

The Future of Security and Reliability

Secret Sharing Systems

Database Attacks and Protection Methods

Malware Programming and Lockdown Virus

Network Programming with Scapy



AAKAKAPI

Hello world!

would like to start by thanking all of you, dear readers for your support and love for our magazine, and the staff who work non-stop to bring this magazine to light. Behind the scenes, there is a lot going on to deliver what we believe is beneficial to the world. Even if there is one person who could see the beauty in the cybersecurity and informatics world through this magazine, we could not be any happier!

On March 8, we will be celebrating International Women's Day. Yet, the origin of the date makes us appreciate what we have today and commemorate what some women did to make us live this way. The origin of the day is March 8, 1857, where some garment workers in New York City protested against the working conditions and low wages. The protests continued, i.e., on March 8, 1908, women marched again in New York City for voting rights, ending child labor and better wages.

As of this significant date, we would like to remind you of some women who rewrote history and without whom the tech world - simply the *world itself*- would never have been the way it is now. The long list starts with Ada Lovelace and continues with Hedy Lamarr, Grace Hopper, and Top Secret Rosies, and so on...

In the last issue's Editor's Note, we talked a bit about the Universal Declaration of Human Rights - *UDHR*. Supporting, respecting and maintaining women rights means respecting the humankind and our future: ourselves, as the UDHR applies to everyone and each and every woman has rights as any other person on this planet does. The value of a person does not depend on their gender, religion, language, skin color, age, etc., but only on the things they do.

As of this issue, you can find interesting articles on encryption, database attacks, viruses, network programming and much more! To learn is to protect yourself. Read so you can learn, learn so you can protect yourself.

Special thanks to Netsparker Ltd. for sponsoring this issue!

Enjoy!

Cansu TOPUKÇU editor@arkakapimag.com

ARKAKAPI MAG

Cyber Security Magazine YEAR: 1 - MARC-APR ISSUE: 2 Bimonthly - ISSN: 2645-906X www.arkakapimag.com

Editor in Chief: Ziyahan Albeniz • ziyahan@arkakapimag.com

Editorial Operations Manager: Cansu Topukçu • cansu@arkakapimag.com

Chief Business Officer: Oğuz Aydınyılmaz • oguz@arkakapimag.com

Publishing Coordinator: Şahin Solmaz • sahin@arkakapimag.com

Director of Web: Ömer Çıtak • omer@arkakapimag.com

Legal Advisor: Mehmet Pehlivan • mehmet@arkakapimag.com

Assistant research editor: Ayşenur Burak • nurayse47@gmail.com

Translators: Hakan Özer, Zekvan Arslan, Atalay Keleştemur, Nuri Çilengir, Enes Özen

Social Media: twitter.com/arkakapimag instagram.com/arkakapimag facebook.com/arkakapimag

We are proud to secure all our emails with Tutanota.



CONTENT

CYBER SECURITY CONFERENCES - Ayşenur Burak	4
THE FUTURE OF SECURITY AND RELIABILITY - Chris Stephenson	6
CRYPTOLOGY FRONT OF WORLD WAR II THE ENIGMA ENCRYPTION MACHINE - Bayram Gök	10
SECRET SHARING SYSTEMS - Ceren İnce	18
DATABASE ATTACKS AND PROTECTION METHODS - Ömer Faruk Colakoğlu	22
MALWARE PROGRAMMING AND LOCKDOWN VIRUS - Bener Kaya	46
NETWORK PROGRAMMING WITH SCAPY - Güray Yıldırım	51
SIBER YILDIZ 2019 WRITEUP - Esra Nur Soylu	57
A SECURITY GUIDE FOR YOUR ANDROID DEVICE - Arka Kapı	78
SIGNAL INTELLIGENCE SIGNAL LISTENING AND ANALYSIS METHODS - Murat Şişman	84

Meb Application Security Scanner

Use Netsparker to Identify Exploitable Vulnerabilities and Other Security Flaws in Your Websites, Web Applications & Web Services Before Hackers Do.

Netsparker scanners employ the unique, dead accurate & fast Proof-Based Vulnerability Scanning Technology that automatically verifies the identified vulnerabilities with a proof of exploit, so you do not have to manually verify them.

🗏 ERNST & YOUNG 💦 🔬 就

SAMSUNG 🛞

ISACA

Microsoft ING

Booz | Allen | Hamilton SIEMENS

Cyber Security Conferences

INTERNATIONAL CONFERENCE ON BIG DATA & DATA SCIENCE

March 04-05, 2019 Hotel Augusta Barcelona Valles Barcelona, Spain

EuroSciCon is organizing the 8th Edition of International Conference on Big Data & Data Science 2019 which will be held between March 04-05 at Barcelona.



DEVOPSDAYS LOS ANGELES

ARKAKAPI

March 08, 2019 Pasadena Convention Center, United States

This conference is dedicated to the DevOps community, and professionals.

Info: <u>https://www.devopsdays.org/</u> events/2019-los-angeles/welcome/



CLOUD & CYBER SECURITY EXPO 2019

EuroSciCon &

March 12-13, 2019 ExCeL London

It is the only place that gives you everything you need to learn, wherever you are in your digital transformation journey and to stay safe in an increasingly hostile digital environment. It's quite simply the industry-leading event for digital-age guardianship.

Info: <u>https://www.cloudsecurityexpo.com/</u>

AAKAKAPI

FIRST CYBER THREAT INTELLIGENCE SYMPOSIUM 2019

March 18-20, 2019 BT Centre London, United Kingdom

There will be one day of training followed by two days of plenary sessions. This event will be open to both FIRST members and non-members.

Info: <u>https://first.org/events/symposium/london2019/</u>



CYBER SECURITY FOR ENERGY & UTILITIES MASTERCLASS 2019

April 09-12, 2019 Singapore, Malaysia

It will provide power, electricity, energy & utilities company attendees with the tools and know-hows of how to plan and strategically develop a cyber security strategy.

Info: <u>http://www.equip-global.com/</u> cyber-security-for-energy-amp-utilities-2019

HARTFORD CYBERSECURITY CONFERENCE

April 18, 2019 Hartford, United States

Data Connectors is host the Cybersecurity Strategies Conference.

Includes Keynote Session and CISO Panel

Info: https://dataconnectors.com/events/hartford2019/



IOT TECH EXPO GLOBAL

April 25-26, 2019 Olympia London, United Kingdom

The World's Largest IoT Conference Series; the IoT Tech Expo Global event in London will bring together key industries from across the globe for 2 days of top level content and discussion. Exploring the latest innovations within the Internet of Things and



covering the impact it has on many industries including Manufacturing, Transport, Supply Chain, Insurance, Logistics, Government, Energy and Automotive, this conference is not to be missed.

Info: https://www.iottechexpo.com/global/

The Future of Security and **Reliability**

This article is a call. On behalf of security, the question of "patch or treatment?" needs to be answered.

ARKAKAPI

We're dealing with patches for now. For the future, this will not be enough!

The size and complexity of operating systems and software are continually increasing; the Linux kernel contains more than 20 million lines of code, and that is just the core. The operating system is a whole lot more than that.

Your equipment is equally sophisticated. There are chips with up to 20 billion (you read it right; it is billions, not millions) transistors; 10 billion transistor processors are now becoming standard.

In both areas, we have systems designed for ancient needs. C language thus Unix is 45, Microsoft Windows is 32, Linux is 27, Intel x86 architecture is 40, and ARM 33 years old.

Therefore, it is challenging to consolidate these systems, which had not been designed due respect to safety or reliability.

With the word security, we want to express the immunity of a system against possible attacks. With reliability, we mean how much a system can do without stopping the work it promises.

Considering that the computer manages aircraft, cars, medical devices that keep us alive, and more, both security and reliability are crucial.

In the future, IoT (Internet of Things) will increase our dependence on reliability and security of software.

Past and Present Solutions

Among the software history, the software that has the oldest history of high security have been those of airplanes and spacecraft. In the past, they tried to solve this problem by augmenting the number of computers. Votes were taken for critical operation between several computers that owned different hardware and separately written software. Space Shuttle had five control computers in two different types. Generally, numerous computer systems are used in the field of Avionics (aircraft electronics). Even though it saves the day up to a point, it had never been the ultimate solution. In addition to multiple systems, it is necessary to perform tests that are systematic and to try to predict every possible situation as in mathematics.

Here, unfortunately, you must pause for some readers. In some countries, the *proof* subject is not in the high school syllabus.

For example, I have the following theorem: "This computer system does not allow the aircraft to stall" - an important theorem. Preconditions, axioms, assumptions, are all crucial, of course. However, the theorem just existing is way safer than flying the plane a few times and saying "Look, it's not down!". However, the methods usually used for software are more like the second one.

Nevertheless, in addition to systematic tests, formal methods, i.e., methods requiring proof, have been used for these critical systems.

For example, if you look at the Airbus 330/340 software guide, we see how formal methods are being used.

30.13 Development Environment

The development of each Airbus Industrie aircraft has been supported by an Iron Bird whole-aircraft systems rig, and by supporting systems rigs that enable work to proceed simultaneously, without mutual interference. The A330/A340 model is no exception, and a number of facilities have been constructed specifically for this programme. These methods are now being used by other airframe manufacturers.

Proper software development is an essential part of systems development throughout the aircraft, and a number of software tools have been developed, notably in the areas of formal methods, rapid prototyping, automatic coding, and rapid data recovery and analysis. These are supplemented by large, fast data recording and telemetry facilities on the test aircraft fleet, associated with real-time and rapidplayback test data displays for the benefit of the flight test observers on board the test aircraft and for the test and systems engineers on the ground.

The result of this environment, the proper use of features from previous programmes, and the proper management of test data flow and the resulting decision process, has created an aircraft that has had a remarkable trouble-free period of introduction into service. This is true both in terms of customer satisfaction and in terms of measurable parameters such as delay rate, which have been up to an order of magnitude better for A340 than for the previous derivative long-range aircraft that entered service.

The Avionics Handbook

Another field that is currently using formal methods is the robot spacecraft that go to Mars.

In an article by a NASA Department, the JPL (Jet Propulsion Laboratory), it describes how the practical application of the software in the vehicle by formal methods can be practiced by various mathematical techniques. In any case, a vehicle that is 100 million kilometers away should be prevented from entering a vicious circle.

Commercial software is both expensive and not practical because of the size of the software with formal methods.

Solved in the Future

In the fifth edition of Arka Kapi Dergi, I mentioned the seL4 kernel. Such initiatives represent the future of safety and reliability.

It was a nice coincidence that a scientific article about a system using the seL4 kernel was published in CACM magazine after my article was published.

Boeing's AH-6 autonomy, the unmanned helicopter is not a small drone or UAV; it is a full-size helicopter. This system has always been tested for its reliability, but a red team hacked the helicopter system successfully in 2013. The attackers managed to direct the helicopter to any location or to crash the helicopter via a USB device attached to the helicopter. The original helicopter system is based on Linux. Linux could not be completely eliminated. However, a virtual machine was created under the seL4 kernel to isolate Linux and the non-critical software, for instance, the camera control of the helicopter, was kept there. This software was blocked from accessing other software flying the helicopter.

Besides, a White Box attack has been attempted - White Box attacks are the attacks in which the attacking team is provided with all the source code and documentation of the system as well as root access to the weaker camera system. Despite all this, the red team could not affect the helicopter's flight systems.

So how was this accomplished? First, a proven operating system, seL4 microspheres, was used. The core itself, the C compiler, and other software are systems proven with formal methods. The proofs have been tested on the software under the virtual machines isolated one by one under the core. Since they were not isolated from each other, the same criteria were not applied to each software.

By implementing such methods, the project implementers could retrofit an existing system and make the system more secure.

Chris Stephenson • The Future of Security and Reliability



Boeing Little Bird flying - did you notice the pilot's absence?

Of course, this is possible under certain conditions: the seL4 microsphere is not a 20 billion line like a Linux kernel, but rather 10-thousand-line C code. Such an attempt for Linux is impossible.

The Future of Proofs

ARKAKAPI

How are security and reliability ensured outside space and aircraft? This cannot be done with software consisting of millions of lines and languages such as C. Even if there are no other factors, the "undefined behavior" trap of the C language alone is enough to make it difficult. In many cases, programs written in C may exhibit different behaviors. This is a disaster for security. In practice, to avoid the poor results of this quality of the C language, both programs, and compiler behavior should be severely restricted. It would be enough to read John Regehr's articles to understand the severity of this problem. While there are 200 different undefined behaviors in C, it is very difficult to prove the behavior of pure C programs.

Formal methods are now becoming more widely accepted. As an example of highly critical problems, we can mention the programs running on browsers. Typically, these programs are written in Javascript. Unfortunately, Javascript is not challenging about variable types, is also complicated, and does not have a clear formal system to recognize the meaning of programs. That's why WebAssembly has been developed for client programs with the joint venture of Google, Apple, Mozilla, and Microsoft. Unlike other languages, the primary feature of WebAssembly is its formal form, mathematical semantics (definitions that define the meaning of programs in language) and type system. We will explain the importance of the types in a moment.

Proof and type systems will be important. New languages and new operating systems are yet to come. New concepts such as proof, type system, formal semantics in new languages will be important. We have to get used to and learn from them.

The importance of types

If we desire security and reliability, we have to say goodbye to our 40-year-old friends, Unix, and C language. Instead, we should adopt provable micro-cores like seL4, as an operating system. However, what will be our solution for the programming languages?

It is not a language that makes it easy for us to write good programs. What we need is a language that makes it impossible for us to write the wrong programs. It's a target. For theoretical reasons, we may

not reach this goal fully at 100%. However, we still have to protect this goal. Adding some important attributes to our languages will make it easier for us to use proofs in larger programs.

In programs, there has to be referential transparency, i.e., when a function is evaluated with the same parameters, it must be guaranteed to produce the same result. Therefore, in our language, mutation (changing the value of the variable) should be impossible.

In our software language, behaviors that may cause undefined behavior should be banned, i.e., rejected by the compiler. This requires a powerful type system.

To realize these, we need a functional language. Nowadays, the languages we already have at hand may not be enough; they are complex and robust too much. Some undesired uncertainties come with Turing Completeness.

However, it is no coincidence that the seL4 operating system reference application was written in Haskell; Haskell is a *pure functional typed* language.

The necessity of types can be explained with two simple examples. We have two major security vulnerabilities. One is Buffer Overflow, and the other is SQL injection. Both of them are due to type mismatch.

If a user enters a text and an SQL command is not of the same type, our compiler may block SQL injection attacks without any further measure. So it becomes impossible to write a program that might be exposed to SQL injection. Buffer Overflow is a more difficult issue. Of course, in environments such as Java language, it is possible to prevent vulnerabilities - such as Buffer Overflow - during runtime, but what our main issue is to prevent it in the compilation stage.

We have to solve these problems so that we can trust the software which occupies more and more space each day in our everyday lives. There will be compromises just like every engineering problem. Nevertheless, proven software will gain more importance. Our old operating systems and programming languages will not be enough.

Conclusion

As usual, I would strongly recommend that you read the original articles that I refer to as references.

Learn programming languages with powerful type systems such as Haskell and Rust. Learn about proof systems such as Coq. If you want to work with security and reliability, this is the future.

References:

- 1. https://www.linuxcounter.net/statistics/kernel
- 2. EPYC: A Study in Energy Efficient CPU Design Nathan Brookwood
- https://www.amd.com/system/files/documents/ The-Energy-Efficient-AMD-EPYC-Design.pdf
- 3. Architecture of the space shuttle primary avionics software system Gene
- D. Carlow Communications of the ACM CACM Volume 27 Issue 9, Sept. 1984 pp 926-936
- 4. New Avionics Systems —Airbus A330/A340 J. P. Potocki de Montalk
- http://www.davi.ws/avionics/TheAvionicsHandbook_ Cap_30.pdf
- Exploiting Traces in Static Program Analysis, Alex Groce, Rajeev Joshi https://agroce.github.io/sttt08. pdf
- Formally Verified Software in the Real World, Gerwin Klein, June Andronick, Matthew Fernandez, Ihor Kuz, Toby Murray, Gernot Heiser, Communications of the ACM Volume 61 Issue 10, October 2018
- 7. Mathematically Verified Software Kernels: Raising the Bar for High
- Assurance Implementations Dr. Daniel Potts, Rene Bourquin, Leslie
- Andresen, Dr. June Andronick, Dr. Gerwin Klein, Prof Gernot Heiser
- 8. Meltdown, Spectre ve Foreshadow, Yaklaşan Devrimin Ayak
- Sesleri, Chris Stephenson, Arka Kapı Dergi Sayı 4
- 9. A Guide to Undefined Behavior in C and C++, John Regehr, https://blog.regehr.org/archives/213
- 10. Bringing the web up to speed with WebAssembly Andreas Rossberg, Ben L. Titzer, Andreas Haas, Derek L. Schuff, Dan Gohman, Luke Wagner, Alon Zakai, J. F. Bastien, Michael Holman Communications of the ACM Volume 61 Issue 12, December 2018 Pages 107-115

Cryptology Front of World War II The Enigma Encryption Machine

t is one of the most famous machines humans have invented. It's the unforgettable star of cryptology. Its story has been the subject of several films from Hollywood. We all know it as the Enigma ciphering device used by the Nazi army during the Second World War. Also, many of the cryptographic devices that developed after enigma have inspired by it. Enigma is the cause of many young people who are interested in cryptology.

When the Second World War was over, the German army had about a hundred thousand Enigma devices in its hands. It is now possible to see the Enigma device, where all the intelligence units have sacrificed their lives to capture one, and the famous cryptanalysts spent years trying to solve them, in museums. You can also find many sites sell replicas of enigma machine on the internet. Speaking of buying, look carefully to the typewriters you see at junk dealers. One of them can be an Enigma device worth 45 thousand euros.



Image 1 : Enigma Device with Three Rotor

ΑЯКАКАРІ



Image 2: Electro-mechanical scheme of Enigma Device [1]



Image 3: Electro-mechanical scheme of Enigma Device [2]

History

The Enigma machine was patented and manufactured by Dr.Arthur Scherbius on February 23, 1918. The first model weighed about 50 kg and was quite bulky. Marketed with the Enigma brand, which means "Riddle" in Greek, the device was developed to be used as a typewriter in its wooden box and in the form of portable 12-pound mobile military models.

As a device designed for commercial purposes, the Enigma did not show the desired sales success until the German Army showed interest. In 1926, the German Navy (Reichsmarine) began using the Funkschlüssel C model, which was specially adapted for them. After some improvements, The Enigma G model, designed for the German Army (Reichswehr) in 1928, was widely used by all German military units and other government agencies after 1930 as Enigma I.

How Does Enigma Work?

To help us understand, we can imagine that the Alberti disk is an advanced continuation of Caesar cipher, the Vigenere cipher is the advanced continuation of Alberti disk, and The Enigma cipher is the advanced continuation of the Vigenere cipher. Each of them has been developed to address the lack of the previous method. While the Caesar cipher was satisfied with a single key (letter shift), multiple keys (letter shift) could be used on the Alberti disk. With the help of a selected keyword in Vigenere cipher, it was possible to encrypt each letter using a different key (different characters shift). In each method, the key mechanism was somewhat complicated. Enigma is the most perfect and last of this series.

The most obvious difference of Enigma is that when each letter is encrypted, it automatically changes the keyword to be used for the next letter to be encrypted. In practice, the method allowed the use of key number close to infinite. It is therefore almost impossible to find repeated strings attached to the same key, such as the Vigenere cipher, in encrypted text. The first key must be known or found to decrypt it.

Enigma is an electromechanical device that works with a battery. They all work on the same basic principle and chassis, although it contains mechanical differences according to the model.

Let's look at the parts of the device.

Keyboard

The enigma is equipped with a 26-letter QWERTY keyboard. They probably wanted it to be compatible with the Morse code. Each key is associated with both a switch and a mechanical pedal that allows the rotor to move step by step. The electrical switch is connected directly to the letter input on the plugboard and to the lamp panel. It does not have a function in the encryption process, it is for data entry purposes.

Plugboard

Is the section where the encryption process begins. This model has a letter change board that provides additional security that is not available in previous models. There are plug entries representing each of the 26 letters on the board. It allows swapping a pair of letters both on the keyboard and on the lamp panel. As can be seen in Figure 4, the letters A and M are replaced by a patch cord attached between the letters A and M. When we press A we will get M and vice versa, so A becomes M and M becomes A, and we get the letter itself if the letter change cable is not attached. A = A; M = M. The number of joining according to the number of patch cables to be used is given in Table 1. The German Army usually used 10 patch cables. This means about 48 bits. The air force was using the UHR (clock) plug attached to the plugboard. With the help of a rotatable key on the UHR plug-in, they were able to easily change the pre-set combinations.

Cable(n)	Combinations
0	1
1	325
2	44.850
3	3.453.450
4	164.038.875
5	5.019.589.575
6	100.391.791.500
7	1.305.093.290.000
8	10.767.019.640.000
9	53.835.098.190.000
10 *	150.738.274.900.000
11	205.552.193.100.000
12	102.776.096.500.000
13	7.905.853.580.550
Toplam	532.985.208.200.000

Table 1: Number of plugboard patch cord



Table 2: Plugboard

Stationary Rotor

The static rotor has conductive surfaces that allow the cables coming from the plugboard to contact the pins on the moving rotor. It has no effect on the encryption process.



Image 5: Black Round Track is Stationary Rotor, silver colored 3 Piece is Latches

Rotor

The heart of the Enigma device, the most complex part, can be easily removed, replaced or mounted on an axis side by side in different order according to the encryption key. There are pins on the right side of the rotor that come in contact with the conductor surfaces of the previous rotor, and pins on the left side that come in contact with the conductor wires that transmit the signal to the next rotor through the cross-connected wires. The German army units have differentiated the cross-links and have used various rotors numbered by Roman numerals. The German Army and Air Force used the enigma device with three rotors numbered I, II and III. In 1938, the number of rotors was increased to 5 by adding rotors IV and V. During encryption, 3 of these 5 rotors were selected and used. Selecting 3 of 5 rotors gives 5x4x3 = 60 combinations.

The Germans were trying to surround the British with their submarines as they did in World War I. Special attention was therefore paid to the communication of the naval forces. In February 1942, the Enigma machine was specially modified for naval forces and coded as M4. The reflector was made thinner and the 4th rotor, which was thinned could be mounted between the reflector and the left-most rotor. There are two types of additional rotor called beta and gamma. The fourth rotor was not moving automatically, unlike the other three rotors, but was manually fixed to one of the 26 positions. The naval forces initially used 6 rotors in the same spaces as the three-rotor version. Later, rotors VII and VIII were added.

All rotors have 26 special notches on the right side and 1 special notch on the left side. When the rotor is mounted on the axis, the right side of the rotor is attached to the left side of the neighbor rotor. As seen in Image 5, there are three latches that center the joining line of the rotor, with a nail on the tip, depending on the key mechanics. When pressing any key, three latches rise upwards simultaneously. With the rising movement, the tip of the right-hand latch is attached to one of the 26 pins to the right of the rotor and moves the rotor one step further. During the nascent movement, if the tip of the center latch is aligned with one of the 26 notches to the right of the central rotor and the single notch on the left of the rotor on the right; it falls into the slot formed by two notches and locks the two rotors. The two locked rotor moves one step together. Since there is only one notch to the left of the rotor on the right, this deadlock occurs once after a lap rotation after every 26 steps of the rotor on the right. In simple term, in order to rotate the rotor in the middle, the rotor on the right should rotate 26 turns. There is also the same mechanical relationship between the third latch, the middle rotor, and the left rotor. In the M4 model, there is no latch for the fourth rotor and it's fixed because it is not connected to the mechanism. In order for the rotor to return to the start position, it is necessary to press a key 26x26x26=17576 times. This is 17 thousand 576 combinations. Since the step-by-step movement changes the contact conductor pins and surfaces,

the encryption key also changes continuously. If we had pressed letter "A" 17.576 times in succession, we might have encountered a series of repetitive letters. You can watch the video of the mechanism through the <u>link</u>.

Rotors VI, VII, and VIII used in the navy have 2 notches on the left side, unlike others. While the normal rotors advance the rotor on the left side of each turn, because of the 2 notches they have the rotors VI, VII and VIII rotate the rotor on the left side of the rotor by two-step for each turn.

In the first rotor produced, the letter ring and conductive pin/surface were fixed. Later, to make the encryption process more complex, the letter rings have been made rotatable through the rotor. And after rotate the ring to the needed position, it was fixed with a small lock. This simple change allowed pin/surface connections and letter relating to variable rotors. Since there is no rotor to the left of the leftmost rotor, only the ring setting of the middle and right rotor will affect the encryption. Because each ring can be set to 26 different positions, 26x26 gives 676 combination.

Pin/surface connection while Ring adjustment is at position **A** :

ABCDEFGHIJKLMNOPQRSTUVWXYZ

EKMFLGDQVZNTOWYHXUSPAIBRCJ

If the ring is set to position **B**, the pin/surface connection be as follows :

ZABCDEFGHIJKLMNOPQRSTUVWXY

EKMFLGDQVZNTOWYHXUSPAIBRCJ



Image 6: Side surfaces of the rotors, pins, and notches



Image 7: Internal connections of rotors, pins, and surfaces cross-linking cables, letter ring



Image 8: Letter ring lock (<u>http://www.cryptomuseum.</u> com/crypto/enigma/working.htm)

Reflector

The reflector passes through the rotors and sends the encrypted message back to the last rotor over the cross-linked return pins. The encrypted signal reaching the reflector is sent back to the last rotor from the cross-connected pin. The signal is re-encrypted by re-adding all the rotors. The customized reflector types were produced for Army intelligence (Abwehr) and the Marine Corps. The cross-linked pins of the reflector are active in the encryption process.



Image 9: Reflector

Lamp Panel

The lamp panel is an output device that reports the encrypted letter to the operator by lighting a lamp. The operator sends the encrypted message via telegraph or radio as Morse code or by courier in writing. It is connected to the plug board, such as a keyboard. Changing the letters made in the plug panel is also valid in the Lamp panel.



Image 10: Lamp Panel

To summarize, Enigma is a highly complex device. Improvements to reinforce the device later made the device more complicated. If we calculate the number of combinations given by the plug panel, rotor, ring setting, we will get $150.738.274.900.000 \times 17576 \times 676 = 1.643.9946.58.58.345.893.248$.

Usage

Enigma is a bidirectional device. Let's explain: For example, when the Enigma device is set and the letter T is pressed, it will appear that the G lamp is lit. This means that the letter T is encoded as a letter G. Again when the letter G is pressed in the same setting, the letter T will light up on the lamp panel. In other words, the Enigma device is capable of encrypting text as well as decrypting the encrypted text. There is no need for a separate device for decoding. Each night, operators set the parameters of the enigma device according to a pre-distributed code booklet, and this setting would be valid for a full day. The rotor set for that day is selected, the letter ring is set and placed in the slot with the specified sequence. Again according to the code booklet, letter replacement settings are made. Then the message Key was created. Since the Nazis thought that tens of thousands of messages to be sent through the day would provide the statistical data needed to break the password, they designed a procedure whereby each operator could determine his or her own message key. The procedure for creating the message key implemented until 1940 was as follows.

Encryption operator

After setting the enigma device according to the code booklet:

- **a**) The operator randomly chose three letters. For example, **RNF** was called the main setting (Grundstellung).
- **b)** Then the operator would rotate the rotor manually from left to right, turning it to the **RNF** position.
- c) The operator would choose another random three letters. For example, **JRM**, it was called the message key.
- d) Then the operator presses the letters JRMJRM respectively and from the lamp panel, for example, notes the letters **BKTRFQ**. The **BKT** letters were called encrypted messages.
- e) Then the operator sets the rotors back to **JRM** letters and begins to encrypt the message.
- f) When the message was encrypted, some additional information (header) was transmitted to the opposite side in a specific format.

Decrypting operator

The operator on the other side also set the rotors, letter rings, and plugboards according to the parameters of the day and according to the code booklet. They use additional information (header) to resolve the message received and, respectively, follows the following procedure.

After setting the enigma device according to the code booklet:

a) Sets the rotors to **RNF** (Grundstellung), which arrives with the message.

- **b)** Again, they enter **BKTRFQ**, the encrypted message setting found in the message attachment information.
- c) Obtained the JRMJRM message key from the lamp panel.
- d) The rotors would set the message key JRM.
- e) Enters the encrypted message and obtains the text that has been decoded from the lamp panel.

Gab.	ine Ri	-	dana)	e,	,	Ira	ice	Stab	s-A	las u o	chin	en3	ch li	isse	N	r. 21	8		-3	6. RF	1885
-	1.77.99		in the second		1.00		-	1			444		1		1					-1027	
11	- 14	19	×.	1	1. 22	11	14	#1.	11	74	28	111	38	18	-18	18	09	jke.	181	111	810
計算数	18. 18. 10.	07.7	in a	N-1	140	12.1	10.0	10 10 14	122.7	122	1000	0A 10 78	118.6	12.2	14.10	14	1140	881 852 944	114 114 117	101	ate state

Image 11: One page from the codebook

In fact, the M1, M2, M3 and M4 codes given to Enigma devices are said to be referred to the encryption procedures rather than the technical specifications of the devices.

How was the legend of Enigma defeated?

There were many historical bad memories of the Polish people to be vigilant. Poland has always been crushed by the eternal competition between Russia and the leading countries of Europe. The only woman with two Nobel Prizes, Marie Curie and the Musician Chopin, were the two famous Polish people who had to leave their country because of the occupation. For this reason, the Polish people have always had good news service and skillful password breakers. Germany was followed by pure attention after the Second World War. They were the first to solve the Enigma. Commercial Enigma was already known. The Poles and the British had already decoded it. However, it is said that the Germans ' military Enigma shocked the Polish. They gathered their best mathematicians and established the Biuro Szyfrom, a password cracking base near Warsaw. Until 1940, the Germans changed encryption procedures several times. Biuro Szyfrom managed to break down every procedure until Poland was occupied. Both developments helped them a lot. First, the former German police, Hans-Thilo Schmidt, stole the Enigma user manual, key lists, and operating instructions from the German military cipher center, where he found work through his brother and sold it to the French secret

service. But the French failed to break the enigma. The French gave the information to Biuro Szyfrom. The second development was when the German government sent a diplomatic Enigma device to the embassy in Warsaw with an ordinary cargo. The Poles took this opportunity. They opened the package and examined the enigma device for two days and took pictures. Then they delivered the package to the embassy as if it had never been opened. The Germans didn't realize anything. The Poles even made them two enigma devices. It is also reported that the poles have developed these devices by purchasing commercial enigma. On September 15, 1938, the Germans changed the encryption procedure once again. Marian Rejewski, who worked at Biuro Szyfrów in October 1938, and his friends developed the first cryptoanalysis device in history to decode Enigma. They called it a cryptographic bomb. As explained in Enigma usage, the encrypted message setting was transmitted in BKT in the header section. To avoid errors in the procedure used until May 1, 1940, the message key JRM was encrypted as JRMJRM twice in a row and transmitted as BKTRFQ. The first 6 letters to get the JRMJRM decoder operator were entered BKTRFQ. This procedure, which was originally designed as security, was itself vulnerable. Key transmission problems will lead to the development of open key understanding in the future. Since all documents were destroyed during the occupation, there is no detailed information about how this gap was broken. However, we have passed the Enigma settings for a full day. This procedure, which was originally designed as a security check was a security breach. Key transmission problems will enable the development of open key understanding in the future. Since all documents were destroyed during the occupation, there is no detailed information about how this vulnerability was broken. However, the enigma settings are valid for a full day.

If sufficient message keys were collected, it was possible to access the message key without the receipt board and rotor information. You can read detailed information from this <u>link</u>. Marian Rajewski also took advantage of the initial positions chosen by lazy operators such as "AAA", "BBB", and"CCC". The number I, II, III rotors produced six combinations. They produced a cryptographic bomb for each combination. They quickly learned the internal structure of the IV and V rotors that were added about a month after the device was completed. However, five rotors produced 60 combinations. They needed more cryptological bombs. Yet they had no way of making so many cryptological bombs. For about 7 years, The Poles decoded Enigma codes without telling the French and the British until the start of the Second World War, listening to German communication. They thought they should now share their information with the British, and handed over all the information, including two copies of The Enigma device to the British. Biuro Szyfrom destroyed all documents and cryptographic bombs before the Germans invaded Poland. The Germans never realized that the Enigma was resolved.

The British, who took over the work of solving Enigma codes from the poles and some Biuro Szyfrom workers, set up a base in Bletchley near London. They specifically targeted M4 to get rid of the German U-boats 'blockade. They gathered the best mathematicians, chess masters, puzzle enthusiasts in the country. This 8000-strong team was directly linked to Churchill, The Prime Minister of the period. In Betchley, privacy was so important that the source of the information obtained from the Decrypted Enigma codes was said to be a spy with the code name "Boniface".Gordon Welchman and especially Alan Turing came forward from inside this team. Turing was inspired by the Polish cryptological bomb and managed to develop a cryptographic device itself. The British also called the device "bomb" to honor the Poles. Weighing about 1 ton, this device simulates dozens of Enigma devices at the same time. 2 cryptological bombs produced by British Tabulating Machine Factory started working in March 1940. They produced 200 of these.

Alan Turing followed a different path than Marian Rejewski and his friends to break the Enigma code. Alan Turing applied "known Open Text attack" to Enigma passwords that changed every day with an automatic machine and succeeded. Frequently used words and codes such as "immediately", and "Hitler", etc. were scanned for in the ciphered text. In other words, if there is one of these words in the text, the machine understood that the message was resolved. The Turing bomb, equipped with Welchman's diagonal board, then eliminated the possibilities and accelerated the process, began to decode messages in less time. The British sought help from the Americans to break the M4, equipped with four rotors in 1942. The Americans developed their own Bombe's.

In Enigma's thrilling adventure which was invented by talented inventor Dr. Arthur Scherbius. It is our duty to discuss which of the Marian Rejewski and Alan Turing approaches is more artistic. Hail to all three geniuses!

SECRET SHARING SYSTEMS

ata storage systems have become an indispensable part of today's technology. Some companies such as You-Tube, Google, and Amazon often need data storage systems that require large scale data processing. The way large-scale data is stored is probably to threaten Institution/Organization and even country security. It's very important to develop methods to secure the storage of this type of data that may threaten the institutions or organizations.

A common method of data security and encryption systems, the secret sharing systems are simply the case where the "secret" data is shared by more than one person. In other words, the secret is known only when a predetermined number of people gather together. In these systems, a distributor designs the system and determines which part of each user in the system will receive the secret.

The need for systems that don't trust a single authority has caused the development of secret sharing systems. We can think of a situation where at least 7 people from a group of 10 should give their authorization for the operation of a nuclear weapon.

$$= \{A_1, A_2, A_3, A_4, A_5, A_6\}$$

$$= \{A_1, A_2, A_3, A_7, A_8, A_9\}$$

$$= \{A_1, A_4, A_5, A_7, A_8, A_{10}\}$$

$$= \{A_2, A_4, A_6, A_7, A_9, A_{10}\}$$

$$= \{A_3, A_5, A_6, A_8, A_9, A_{10}\}$$

Liu's problem caused the secret sharing systems to emerge in 1968. The problem is as follows: "11 scientists work on a secret project in which information is kept in a secure box. How many locks should we use to prevent the box from opening without at least 6 or more scientists? At this requirement, at least how many keys should each scientist have ?"

For the solution of the problem; Without at least 6 scientists, the box should be locked with 462 locks so that the box can't be opened, and each scientist must have at least 252 keys.

The solution to this problem can be found simply with combinatorial calculations but for the most effective solutions, the problem was solved by Shamir and Blakely independently of each other in 1979. Shamir solved this problem using the interpolation formula.

Let's make an example of this problem with smaller numbers and try to understand how Shamir's method works and how effective it is by observing it again through the same example.

The Problem is as follows: 5 scientists are working on a secret project where information is kept in a safe box. How many locks should the box have to prevent the box from opening without at least 3 or more scientists? At this requirement, at least how many keys should each scientist have?

The solution can be easily solved by combinatorial methods. Without at least 3 scientists the box should be locked with 10 locks so that the box can't be opened, and each scientist must have at least 6 keys.

In the image, 10 keys are distributed so that each of them has 6 keys. When the keys of any three scientists are combined, the A_1, \dots, A_{10} keys will be obtained and the box will be opened.

Let's examine Shamir's Secret Sharing System to understand the effective solution that Shamir provides. This system based on Lagrange interpolation, which was developed to distribute a switch with certain shares within a group, is shown as follows.

The system architecture is consist of a D distributor that builds the secret sharing system, S key set, and P={P1, P2,..., Pn} users set. The D distributor selects s key from the S set to split it up and distribute the parts to the users according to the algorithm.

Construction Of Shamir

- Let number p be a prime number larger than the number of people n.
- Select the key to corresponding to the a0(Mod p) coefficient as a secret.
- Let random a1, a2,..., ak-1 (mod p) coefficients be chosen to create the following polynomial:

$$f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1}$$

- Calculate the corresponding yi = f(xi) values in the polynomial for different $xi \pmod{p}$ values to distribute the key to the users. The resulting pairs can now be distributed to the users.

The set of users consists of $P = \{(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)\}$ pairs. In the system built, any k user count finds the

$$f(x) = \sum_{i=1}^{k} y_i \prod_{i \neq j}^{k} \frac{x - x_j}{x_i - x_j} (mod \ p)$$

polynomial using the Lagrange interpolation formula and creating the key. Through the Lagrange interpolation formula, a polynomial with the degree of k-1 can be found by knowing the coordinates of k different points.

Ceren İnce • Secret Sharing Systems



For example, let's create a system with Shamir's method, where the secret is distributed to 5 people, and it can't be found unless 3 people get together.

1. We accept as $S = 3 \mod(11)$.

ARKAKAP

2. Let's create a polynomial $f(x) = x^2 + 2x + 3$ consisting of quadratic random numbers.

3. $P = \{(x_1, y_1), (x_2, y_2), \dots, (x_5, y_5)\}$ is the set of user, given to each user (x, y) pairs is calculated as: 5 (mod 11); $x_4 = 6 \Rightarrow y_4 = 7 \pmod{11}$; $x_5 = 9 \Rightarrow y_5 = 3 \pmod{11}$

4. $P = P = \{P_1 = (1, 6), P_2 = (2, 0), P_3 = (5, 5), P_4 = (6, 7), P_5 = (9, 5)\}$ is a set of users consisting of

pairs, where any 3 users can find the key by creating polynomial using Lagrange interpolation formula.

5. For example, $P = \{P_1, P_3, P_5\}$ users want to come together and find the secret. Using the Lagrange interpolation formula, the X polynomial is created and the key is found as s = f(0) = 3. The Lagrange interpolation formula is used here to form a second-degree polynomial known as the three different points it passes through.



Visual Secret Sharing Systems

Let's briefly mention the Visual Secret Sharing System through an example. The interesting aspect of the visual secret sharing system is that the information shared is an image. In this system, which was introduced by Naor and Adi Shamir in 1994, the images are matrices consisting of black and white pixels. Black pixels are expressed with "1" and white pixels are expressed with "0". The following example shows the matrices created in this manner.



The first image is a picture obtained from random pixels.

The second image is an image obtained from the first image and a hidden image.

The hidden image will be revealed by adding the two matrices which correspond to the first and second image

Sources:

Shamir, A., (1979). " How to Share a Secret ", Communications of the ACM, 22: 612-61

M. Naor and A. Shamir, 'Visual cryptography', Advanced in Cryptography- Eurocrypt94 ,vol.950, no.7, 1995, 1-12.

http://www.matematikdunyasi.org/arsiv/PDF/13_04_75_77_sir.pdf

яякака

http://www.wikizeroo.net/index.php?q=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnL3dpa2kvU2hhbWlyJ3NfU2V-jcmV0X1N oYXJpbmc

Database Attacks and Protection Methods

hat first comes to mind when cybersecurity is mentioned are the web attacks, that is to say, external attacks. Let me confuse you a bit.

"What if the enemy is inside?"

AAKAKAPI

That is to say, what if the person who is after your data is whom you drink coffee with every day?

However, life does not go on with this paranoia, a state of a vast incredulity nearly drifting one into becoming mad. Of course, we won't suspect everyone, yet this does not prevent us from taking action.

Now, let's say that we have a database, let there be an MSSQL server. Here reside some very significant data of your company, such as finance, accounting, R&D, product design. These data may be subject to significant dangers; the data can be:

- 1. Deleted
- 2. Changed
- 3. Compromised by the rival company



Which one is more dangerous, or riskier changes depending on company and individuals. The risk is something not to take.

Database attacks can be made through various methods. However, I am going to mention the random password trying ways; the Brute Force attacks.

Usually, on a database system, it is expected that the system detects it when too many wrong passwords are entered.

The scene below is from the Şabanoğlu Şaban movie of Kemal Sunal, where a password is asked.

The talk between the two is as follows:

-I am going to count to 3, tell the password right now! 1!

+Password. Umm!

The password is not "Umm". 2!

-Password. Stop, I'm going to find it!

-The password is neither "I'm going to find it"!

-Oh! I found it, "Başak".

-You didn't, and it's "Şafak"



This dialogue is an example of how it should be. If a person enters an incorrect password three times, he/she should be blocked.

Let's take a look at how things work in real life.

In an MSSQL database, you are allowed to enter an incorrect password as many times as you wish. That is to say; it does not detect if your actions are malicious. There exist no such setting relevant to this. If the system gives this opportunity, all that is is left to the attacker is to try and find different combinations until the password is found.

Here are what you need to log into an MSSQL database.

1. Physical connection

- 2. For the 1433 port to be open
- 3. Username
- 4. Password

Let's think.

Our SQL server is not open to the internet, so the attacker can not attack from outside since there is no physical connection.

The SQL server can connect to the internet, but the port 1433 is closed; there is a physical connection, but the port is closed, so the access is once again denied.

The SQL is connected to the internet, and you opened the port 1433 to connect without VPN. In this case, the attacker should guess the username and password. Almost 99% of MSSQL users in Turkey do not disable the default admin account "SA". So what is left? To guess the password.

The password "safak" can be found using a 5-combination of the 26 characters of the English alphabet. That is to say, 26x26x26x26x26 = 11,881.376 different password combinations.

Let's suppose that the attacker can try ten passwords per second over the internet, which means 11,881,376 / 10 = 1188137.6 seconds, 19.802 minutes, 330 hours, 13.75 days.

Okay, so what will it be like when the attacker attacks from within?

In many businesses, there are computers with GBit connection speed and i5, i7 CPU.

In this case, you can try up to 5000 passwords a second, which means that - 11,881,376 / 5,000 = 2,376 sec., 39 min.- you can crack the password in 39 minutes.

Right now we have the following question pop up in our minds: "Why would the password be five characters long?" right?

Right, it would not be. The time needed to crack a password would take a little longer than five characters, containing uppercase and lowercase letters. Maybe one day, maybe one week, maybe one month.

However, at the end of the day, in case of such attack, what us, the system administrators need to do is to:

- 1. Detect,
- 2. Record,



- 3. Block the attack
- 4. Distract and if possible catch the attacker on the job

In this article, I will be explaining how to do this.

Below you see the picture of an application which performs continuous password attempts on the target system. The passwords it tries are not a combination, but rather a password dictionary of 2,000,000 passwords you can find online.

It is a simple application I wrote. It uses one thread and cracked the password by trying approximately 500 passwords a second.

🛃 Bağlandı. Passwo	ord=Password1			_		\times
Sunucu	192.168.182.135		Bru	ite Ford	e	
Kullanıcı	SA					
Database	MASTER	1		1000		
Bağlandı. Pa	ssword=Password1 Süre:00:01					
eldiablo6662 cajolantes6 ricky arnejo abbeyeli adriandumitro Password1	escu					

uniqpass_preview.txt 😐 🗙
8997394
RAP
amazing_me_2010
pwalkershit
emjhayarca
fackz95
greatness_personified
kaamasmukka
doveystar
b4rn0n3
blondetweetysweety
8a76e1
challex828
chandramouli 3 0
amos_rosenthal
fatoyfood123
mary claire d
leonleon667
76grigny
squeakie_101
déracinai4
bmforlove
cerradajonathan
91ut@m@te\$
manota2009
161 % -

A screenshot from the password dictionary.



So, are we going to sit there while someone is trying to crack our password?

Of course not!

When you click on the Server Properties on the SQL Server, you can see a part named "Login Auditing".



Server Properties - DESKTO	2-5E3LKN1\sql14	_		\times
Select a page	🔄 Script 🔻 🛐 Help			
Memory Processors Security Connections Database Settings Advanced Permissions	Server authentication Windows Authentication mode SQL Server and Windows Authentication mode Login auditing None Failed logins only Successful logins only Both failed and successful logins Server proxy account			
	Enable server proxy account			
Connection	Password:			
Server: .\sql14 Connection: DESKTOP-5E3LKN1\omerc	Options Enable Common Criteria compliance Enable C2 audit tracing Cross database ownership chaining			
Progress				
Ready				
	[ОК	Cance	el

Here, we specify which login processes we would like to log.

Nothing is logged if None is chosen.

When Failed logins only option is chosen -which is the default option- just incorrect login attempts are logged.

In the Successful logins option, only successful entries are logged.

Both failed, and successful logins option logs them both.

Now let's see how we display these logs.

To see these logs, one needs to go to the SQL Management Studio Management part, enter the SQL Server Logs tab and click on the Current Logs menu.

Object Explorer	▼ ∓ ×	SQLQuery1.sql - 192.
Connect 🕶 🛱 🗮 🝸 🖒 🔸		
😑 🐻 192.168.182.135 (SQL Server 14.0.1000.169 -	sa)	
🕀 📕 Databases		
표 📕 Security		
🕀 🛑 Server Objects		
🕀 📁 Replication		
🕀 💼 PolyBase		
표 📕 Always On High Availability		
🖃 📕 Management		
🗄 🧣 Policy Management		
🕀 📷 Data Collection		
🕀 👦 Resource Governor		
Extended Events		
🕀 🛑 Maintenance Plans		
🖃 🛑 SQL Server Logs		
Current - 4.11.2018 20:46:00		
Archive #1 - 4.11.2018 20:46:00		
Archive #2 - 4.11.2018 20:34:00		
Archive #3 - 4.11.2018 19:33:00		
Archive #4 - 4.11.2018 19:33:00		
🗗 Database Mail		
Distributed Transaction Coordinator	r	
🕀 📕 Legacy		
Integration Services Catalogs		
🗄 💀 SQL Server Agent		
If XEvent Profiler		
		100 % -
		📲 🏟 Connected. (1/1)

uery1.aqf - 192.768.182.135.mast	The second second second second				100
View Project Debug	Log File Viewer - 192,168,182,133			- 0	×
18 - 6 - 🖾 🖬 🥔 🕼	Select logs	Load Log Export	Refresh	Thiter 4. Search I Stop D Help	
under .	20 mert - 4 11 2018 21 56 60	Log file summary: No filter appl	ed		
	Archive #1 - 4,11,2018 20:46:00	Date T	Source	Message	14
irer .	Archive #2 - 4 11 2018 20 34 00	4 11 2018 21:56:06	Logon	Login failed for user SA', Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.	11 110
9 19	Archive #3 - 4.11.2018 19:33-00	4.11.2018 21:56:06	Logen	Error: 18456, Severity: 14, State: 8.	4
	Archive #4 - 4.11.2018 19:33:00	4.11.2018 21.56:06	Legen	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CUENT: 192.168.182.1	灯じ
168.182.135 (SQL Server 14.0.100	III SQL Server Agent	4.11.2018 21:56:06	Logen	Error: 18456, Severity: 14, State: 8.	1
Jacabases	E Wodows NT	4.11.2018 21:56:06	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.]	11
ecunty		4 11 2018 21 56:06	Logon	Error: 18456. Severity: 14, State: 8.	- P
rerver Objects		4.11.2018 21:56:06	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1	1 :
heb @asa		4 11 2018 21 56:06	Logon	Error: 18456, Severity: 14, State: 8.	1
Usuant On Minh Availability		4 11 2018 21 56:06	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1	11
Ananement		4.11.2018 21:56:06	Logon	Error 18455. Severty: 14, State: 8	12
Policy Management		4.11.2018 21:56:06	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CUENT: 192 168.182.]	1] !
E Data Collection		4.11.2018 21.56.06	Logon	Error: 18456, Severity: 14, State: 8.	t i
Resource Governor		4.11.2018 21.56.06	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192 168 182 1	11 :
Extended Events		4.11.2018 21.56.06	Logon	Error: 18456, Severity: 14, State: 8.	10
Maintenance Plans		11 2018 21 56.06	Logon	Login failed for user 'SA' Reason: Password did not match that for the login provided. [CUENT: 192 158 182	1] :
SQL Server Logs	Cinton	4 11 2018 21 56.06	Logon	Error 18456, Seventy 14, State 8.	É.
Current - 4.11.2018 20:46		E 4.11.2018 21.56.06	Logon	Login failed for user 'SA' Reason: Password did not match that for the login provided, [CUENT, 192 168 182 1	11 :
Archive #1 - 4.11.2018 20:	Last Hefresh:	E 4 11 2018 21 56 06	Logon	Error 18455, Seventy 14, State 8	6
Archive #2 - 4.11.2018 20	4 11 2018 21 58 30	E 4 11 2018 21 56 06	Logon	Login failed for user 'SA' Reason: Password did not match that for the login provided [CUENT 192 168 182	1] :
Archive #3 - 4.11.2018 19:		4 11 2018 21 56:06	Logon	Error 18456, Severity 14, State 8	1
Archive #4 - 4.11.2018 19	Hiter: None	100			
V Database Mail	W. Manufika antistan	Polyanta di mur dista fari			1
Distributed Transaction Cool		Date 4.11.2018	21/56/06		12
Legacy	Progress	Log SQL Serve	r (Current	- 4.11.2018 21:56:00)	<u> </u>
ntegration Services Catalogs	Done (1035 records).	Seame Lanan			
QL Server Agent	•	Source Logon			
Event Profiler		Message			¥
				-	5224871

It can be seen that there a lot of "Login Failed for user 'SA' Reason: Password did not match that for the login provided. [CLIENT:192.168.182.1]" log.

This case shows us that a password trying attacks has been made. Furthermore, we also have the IP address the attack is made from.

So, to notice this attack, do we need to look at this screen continually?

In the background, the SQL Server understands nothing but the SQL language.

That is to say, to create the log table we see, there is an SQL query made in the background.

"EXEC XP_ReadErrorLog"

Qu	ery2.sql - 19235.master	(sa (54))* 👳	🔀 SQLQuery1.sql - 19235 master (sa (67))	
1	exec xp_readerrorlo	g		
5 %	: 1			
II B	esuits (Messages			
	LooDate	Processinfo	Test	
97	2018-11-04 21:56:03.110	Logon	Login failed for user SA', Reason: Password did not match that for the login provided. ICLIENT: 192,168,182,11	
88	2018-11-04 21:56:03 110	Logon	Entry 18456. Seventy: 14. State: 8.	
19	2018-11-04 21:56:03.110	Logon	Login failed for user SA', Reason: Password did not match that for the login provided. ICLIENT, 192,168,182,11	
100	2018-11-04 21:56:03.120	Logon	Error: 18456. Seventy: 14. State: 8.	
101	2018-11-04 21:56:03 120	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
02	2018-11-04 21 56:03.130	Logon	Error 18456, Severty, 14, State, 8,	
03	2018-11-04 21:56:03.130	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
104	2018-11-04 21:56:03.140	Logon	Error: 18456, Severity: 14, State: 8.	
105	2018-11-04 21 56:03 140	Logon	Login failed for user SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
106	2018-11-04 21:56:03.150	Logon	Error: 18456, Seventy: 14, State: 8.	
107	2018-11-04 21:56:03.150	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
80	2018-11-04 21:56:03 150	Logon	Error: 18455, Seventy: 14, State: 8.	
09	2018-11-04 21:56:03.150	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. (CLIENT: 192.168.182.1)	
10	2018-11-04 21:56:03.160	Logon	Error: 18456. Seventy: 14. State: 8.	
11	2018-11-04 21:56:03 160	Logon	Login failed for user 'SA', Reason: Password did not match that for the login provided. [CL/ENT: 192.168.182.1]	
12	2018-11-04 21:56:03.170	Logon	Error: 18456. Severty: 14. State: 8.	
13	2018-11-04 21:56:03.170	Logon	Login failed for user SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
14	2018-11-04 21:56:03.180	Logon	Enor: 18456, Seventy: 14, State: 8.	
115	2018-11-04 21 56:03 180	Logon	Login failed for user 'SA', Reason: Password did not match that for the login provided. [CLIENT: 192,168,182,1]	
16	2018-11-04 21 56:03 180	Logon	Error: 18456. Seventy: 14, State: 8.	
17	2018-11-04 21:56:03.180	Logon	Login failed for user SA', Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
118	2018-11-04 21:56:03 190	Logon	Error, 18456, Seventy: 14, State: 8.	
119	2018-11-04 21:56:03.190	Logon	Login failed for user 'SA', Reason: Password did not match that for the login provided, [CLIENT: 192.168.182.1]	
20	2018-11-04 21:56:03.200	Logon	Error: 18456, Severity: 14, State: 8.	
21	2018-11-04 21:56:03 200	Logon	Login failed for user 'SA' Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
22	2018-11-04 21:56:03.210	Logon	Enor: 18456, Severty, 14, State, 8,	
23	2018-11-04 21:56:03.210	Logon	Login failed for user SA', Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
24	2018-11-04 21:56:03.220	Logon	Error: 18456, Severity: 14, State: 8.	
25	2018 11-04 21 56:03 220	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192,158,182.1]	
26	2018-11-04 21:56:03:220	Logon	Enor: 18456, Severty: 14, State: 8.	
27	2018-11-04 21:56:03.220	Logon	Login failed for user SA', Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
128	2018-11-04 21:56:03.230	Logon	Error: 18456, Severity: 14, State: 8.	
129	2018-11-04 21:56:03.230	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
130	2018-11-04 21:56:03.240	Logon	Error: 18456, Seventy: 14, State: 8.	
31	2018-11-04 21:56:03:240	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
132	2018-11-04 21 56:03 250	Logon	Entri 18456, Severty: 14, State: 8.	

Now that we have a command let's suppose a scenario. Let the system:

- Work every 3 minutes
- Read the relevant log lines
- Detect that there is an attack if there are more then 100 logs containing the sentence "Login Failed for user 'SA' *Reason: Password did not match that for the login provided.*"

ΑЯКАКАРІ

Here, 100 is a symbolic number. You may as well make it less or more.

All right, so how do we filter a prepared query like "EXEC XP_ReadErrorLog"?

Quickly, we can do it using the Temp Table. Temp Tables are tables which are created in the memory and disappear later.

CREATE TABLE #SQLErrorLog

```
(
  LogDate DATETIME ,
  ProcessInfo VARCHAR(20) ,
  Text VARCHAR(500)
 );

INSERT INTO #SQLErrorLog
  EXEC xp_readerrorlog 0;
SELECT * FROM #SQLErrorLog
WHERE Text LIKE '%Login failed for user%'
AND LogDate >= DATEADD(MINUTE, -1 * 3, GETDATE())
```

As can be seen, 476 password attempts had been made the last 3 minutes.

ACR C	wery1.sql = 192tit.maste	a (PV (260), X	Object Explorer Defails	
	CREATE TABLE	#SQLErro	orLog	*
	(
	LogDa	te DATE	TIME ,	
	Proce	ssInfo)	ABCHAR(20)	
	Taxt	VARCHAR	(500)	
	TEAL	VANCHAN	500)	
	-13			
	TNSERT TNTO	#SOLEnn	and and and and and and and and and and	
	EXEC	xp reade	errorlog 0:	
1	SELECT . FROM	#SOLE	torl or	
	UNERE Tout 11	WE WIN	the failed for user?"	
	WHERE TEXT LI	KE ALO	in failed for user%	
	AND LogDate >	= DATEAL	DD(MINUTE, -1 * 3, GETDATE())	
00 %				
	Results 🔄 Messages			
	LogDate	Processinfo	Text	- A
4	2018-11-07 01:11:13 820	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	100
5	2018-11-07 01:11 13:830	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192 168.182.1]	
6	2018-11-07 01:11:13:840	Logon	Login falled for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
7	2018-11-07 01:11:13.850	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CUENT: 192.168.182.1]	
8	2018-11-07 01:11:13.850	Logon	Login falled for user SA: Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
5	2018-11-07 01:11:13.860	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192.168.182.1]	
10	2018-11-07 01:11 13:870	Logon	Login failed for user 'SA'. Reason: Password did not match that for the login provided. [CLIENT: 192 168.182 1]	
11	2018-11-07 01:11:13.880	Logon	Login failed for user 'SA', Reason: Password did not match that for the login provided. [CLIENT: 192 168.182.1]	
12	2018-11-07 01:11:13.890	Logon	Login failed for user 'SA', Reason: Password did not match that for the login provided. [CUENT: 192 168.182.1]	
13	2018-11-07 01:11.13.900	Logon	Login failed for user 'SA'. Reason. Password did not match that for the login provided. [CLIENT: 192 158.182 1]	
č	3010 11 07 01 11 12 010	1	To and Education cannot CAT Discussion Discussional distances and also the the the basis and address of the TCOT. TOO 1000 100 11	- × *
20	uery executed successful	br.:	192.168.182.138 (14.0 RTM) SA (56) master 00:00:00	476 rows



Now, what we need to do here is to detect the IP address and inform the database manager. To do this, DB Mail in the SQL Server needs to be activated. SQL DB Mail installation can be done as follows:





👫 Databa	se Mail Configu	iration Wizard - DESKTOP-5E3L	(N1\sql14		_	
Select Select	Configurations setup or maintena	on Task ance tasks.				
If you are in	nstalling Database	e Mail for the first time, select the se	tup option.			
💿 Set ι	ıp Database Mail	by performing the following tasks:				
1. Cre	ate a new e-mail	profile and specify its SMTP accou	nts			
2. Sp	ecify profile secur	ity				
3. Co	nfigure system pa	rameters				
🔿 Mana	age Database Ma	il accounts and profiles				
🔿 Mana	age profile securit	у				
O View	or change system	n parameters				
Help			< Back	Next >	Finish >>	Cancel
						.::
ſ	Patabase Ma	il Configuration Wizard - DESKTOP-	5E3LKN1\sql14		-	
	New Profile					
	Specify the p	rofile name, description, accounts, and f	ailover priority.			
	Profile name:	salegitim				
	Description:	and a Rest t				~
						4

A profile may be associated with multiple SMTP accounts. If an account fails while sending an e-mail, the profile uses the next account in the priority list. Specify the accounts associated with the profile, and move the accounts to set the failover priority.



🔡 Database Mail Configuration Wizard - DESKTOP-5E3LKN1\sql14 — 🛛 [
Manage Existin Choose the accourt	g Account nt to view, change	, or delete.					H
Account name:	sqlserver.egitim@	gmail.com			~	Delete	
Description:							
Outgoing mail server (S	MTP)						-
E-mail address:		sqlserver.egitim@gma	il.com				
Display name:		sqlserver.egitim@gma	il.com				
Reply e-mail:		sqlserver.egitim@gma	il.com				
Server name:		smtp.gmail.com			Port number:	587	
This server requi	ires a secure conn	ection (SSL)					3
SMTP Authentication							
O Windows Auther	ntication using Dat	abase Engine service	credentials				
Basic authentica	ition						
User name:		sqlserver.egitim@gma	ail.com				
Password:							
Confirm passwor	d:						
Anonymous auth	nentication						
Help			< Back	Next >	Finish >>	Cancel	

Specify the	e profile name, de	scription, accounts, and failover priority.	
			6
ofile name:	sqlegitim		
scription:			
rofile may be	associated with	i multiple Sivi i Placcounts, if an account fails while sending an e-	mail, the profile uses the next
count in the p	nonty list. Specif	ty the accounts associated with the profile, and move the accour	nts to set the failover priority.
ITP accounts	:		
ITP accounts iority Acco	: ount Name	E-mail Address	Add
ITP accounts iority Acco sqls	: punt Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove
ITP accounts iority Acco sqls	: punt Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove
ITP accounts iority Acco sqls	: ount Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up
ITP accounts iority Acco sqls	: ount Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: punt Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: punt Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: punt Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: ount Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: ount Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: ever.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down
ITP accounts iority Acco sqls	: ount Name erver.egitim	E-mail Address sqlserver.egitim@gmail.com	Add Remove Move Up Move Down

Ömer Faruk Colakoğlu • Database Attacks and Protection Methods

ΑЯΚΑΚΑΡΙ

🔓 Database	Mail Configuration Wizard - DESKTOP-5E3LKN1\sql14	_	
Manage Specify d	Profile Security atabase users or roles that have access to profiles.		
Public Profile	Private Profiles		
A public p	ofile can be accessed by all users of any mail-host database.		
Select pub	lic profiles. You can also specify the default public profile.		
Public	Profile Name	Default Profile	
	sqlegitim	No	
Show o	nly existing public profiles	Boids and	Cancel
<u>H</u> elp	< <u>B</u> ack <u>N</u> ext >	<u>F</u> inish >>	Cancel

Ŀ	Dat	tabase Mail Configuration Wizard - DESKTOP-5E3LKN1\	sql14			. [⊐ ×
С	on Ci	figuring ick Stop to interrupt the operation.					
	0	Success	4	Total Success	0) Error) Wami	ng
D)etai	ls:					
		Action	Status		Message		
	0	Create new account 'sqlserver.egitim@gmail.com' for SM	Success				
	0	Create New profile 'sqlegitim'	Success				
	0	Add account 'sqlserver.egitim@gmail.com' to profile 'sqleg	Success				
		Grant 'guest' access to 'sqlegitim'	Success				
				Sto	p	Re	eport 🔻
							Close

Now, let's send a test email.

AAKAKAPI



E Send Test E-Mail from DESKTOP	P-5E3LKN1\SQL14 —	×
Database Mail <u>P</u> rofile:	sqlegitim	\sim
<u>T</u> o:	sqlserver.egitim@gmail.com	
<u>S</u> ubject:	Bu bir deneme mailidir.	
<u>B</u> ody:	This is a test e-mail sent from Database Mail on DESKTOP-5E3LKN1\SQL14.	^
		\vee
	Send Test <u>E</u> -Mail	
	Close	:

ΑЯКАКАРІ

The mail we sent is received by the SQL Server.

=	M Gmail		Q. Postalarda arayın					•
+	E-Posta Yaz		□- c :					
-			D Birincii		Sosyal		ø	Tanituriar
	Gelen Kutusu	10		_	(1853%) (1957)			
*	Vildizik		🗀 🏦 ben	Bu	bir deneme maili	dir This is a test	e-ma	all sent from Database Mail on DESKTOP-SE3LKN1\SQL14.
0	Ertelendi							
>	Gönderilmiş Poştalar							
B	Taslaklar							
~	Diğer							
۲	SQL Server -	+						

EXEC msdb.dbo.sp_send_dbmail

@profile_name = 'sqlegitim',

@recipients = 'sqlserver.egitim@gmail.com',

@subject = 'Brute Force Saldırısı',

@body='Sisteminize 01:30:00 ile 01:33:00 saatleri arasında 192.168.189.1 ip li makineden 475 kez Şifre denemesi yapılmıştır.'

After activating the mail system, we need to send a mail to the database manager with a meaningful message. The mail sending process is again actually a T-SQL command.

🗏 M Gmail	Q Postalarda arayın	Χ.
E-Posta Yaz		2 ileti dizisinden 1. < >
Gelen Kutusu 1	Brute Force Saldırısı Gelen Kanunu x	
 ★ Yıldızlı ♦ Ertelendi > Gönderilmiş Postalar ♦ Taslaklar > Diöer 	sqlserver.egitim@gmail.com <sqlserver.egitim@gmail.com> Aloc ben + Sisteminize 01:30:00 ile 01:33:00 saatieri arasında 192:168.189.1 ip li makineden</sqlserver.egitim@gmail.com>	01:32 (0 dakika önce) - 475 kez şifre denemesi yapılmıştır.
SOL Server · +		4
Let's write a query which will do this operation automatically.

```
CREATE PROC BRUTFORCE_CONTROL @MINUTE AS INT = 3
AS
BEGIN
CREATE TABLE #SQLErrorLog
(
LogDate DATETIME ,
ProcessInfo VARCHAR(20) ,
Text VARCHAR(500)
);
```

INSERT INTO #SQLErrorLog

EXEC xp_readerrorlog 0;

DECLARE @TEXT AS VARCHAR(1000); DECLARE @COUNT AS INT; DECLARE @MINDATE AS DATETIME; DECLARE @MAXDATE AS DATETIME;

SELECT @TEXT = Text , @COUNT = COUNT(*) , @MINDATE = MIN(LogDate) , @MAXDATE = MAX(LogDate)

FROM #SQLErrorLog

WHERE (Text LIKE '%Login failed for user%')

AND LogDate >= DATEADD(MINUTE, -1 * @MINUTE, GETDATE())

GROUP BY Text

HAVING COUNT(*) > **5**;

DECLARE @USER AS VARCHAR(100); DECLARE @IP AS VARCHAR(100);

--ORDER BY LogDate DESC

ARKAKAPI

DECLARE @POS AS INT= 0; DECLARE @POS2 AS INT= 0;

DECLARE @STR1 AS VARCHAR(1000)= REPLACE(@TEXT, 'Login failed for USER',

");

SET @POS = CHARINDEX('. Reason:', @STR1); SET @USER = LEFT(@STR1, @POS - 1);

SET @POS = CHARINDEX('[CLIENT: ', @TEXT); SET @POS2 = CHARINDEX(']', @TEXT);

SET @IP = SUBSTRING(@TEXT, @POS, @POS2 - @POS); SET @IP = REPLACE(@IP, '[CLIENT: ', '');

DECLARE @MSG AS VARCHAR(1000);

SET @MSG = CONVERT(VARCHAR, @MINDATE, 109) + ' VE '

+ CONVERT(VARCHAR, @MAXDATE, 109) + '

TARİHLERİ ARASINDA ' + @USER

+ ' KULLANICISI ' + CONVERT(VARCHAR, @COUNT)

+ ' KEZ YANLIŞ ŞİFRE GİRDİ';

IF @COUNT > 5

BEGIN

EXEC msdb.dbo.sp_send_dbmail @profile_name = 'sqlegitim', @recipients = 'sqlserver.egitim@gmail.com',

@subject = 'Brute Force Saldırısı', @body=@MSG

END;

SELECT @MSG;

DROP TABLE #SQLErrorLog;

END;



Now let's do a brute force attack on the system several times.

🖳 Bağlandı. Passw	vord=Password1			_		×
Sunucu	192.168.182.138		Bru	ute Forc	e	
Kullanıcı	SA					
Database	MASTER	1		1000		
Bağlandı. Pa	assword=Password1 Süre:00:01					
eldiablo6662 cajolantes6 ricky arnejo abbeyeli adriandumitu Password1	2 rescu					

Run the BRUTFORCE_CONTROL query manually.

SQLQuery3.sql - 19238.master (SA (56))*	× SQLQuery2.sql - 19238.master (SA (72))*	SQLQuery1.sql - 19238.master (SA (56))* Obje
BRUTFORCE_CONTROL		
100 % -		
🔢 Results 📑 Messages		
(No column name)		
1 Nov 7 2018 1:43:38:030AM VE Nov 7	2018 1:44:03:110AM TARIHLERI ARASINDA 'SA'	KULLANICISI 1073 KEZ YANLIŞ ŞIFRE GIRDI

The response of the query came like this.

Below, the mail received can be seen.

Q	Postalarda ar	ayın										*					
÷	0 0	Î	0	0	Þ		;				8 ile	ti dizisir	iden 1.	<	>	-	
	Brute Fo	rce S	aldırı	SI Gele	n Kutusu	i X										i	ę
*1	sqlserver.egi Alici: ben 👻	tim@gn	nail.com	n <sqlserv< td=""><td>/er.egitim</td><td>@gmail</td><td>.com></td><td></td><td></td><td></td><td></td><td>01:4</td><td>6 (0 dakil</td><td>ka önce</td><td>Ľ</td><td>7 4</td><td>ŀ</td></sqlserv<>	/er.egitim	@gmail	.com>					01:4	6 (0 dakil	ka önce	Ľ	7 4	ŀ
	Nov 7 2018 1	:43:38:0	30AM VI	E Nov 7	2018 1:4	44:03:11	0AM TAI	RİHLERİ A	ARASIND/	A 'SA' KULL	ANICISI 1	073 KE	Z YANL	IŞ ŞİFR	E GIR	Dİ	
	🔶 Yanıtla	i n	Yön	lendir													

What comes next is to do this operation automatically rather than manually.

In order to do this, writing a job to the SQL Server Agent is the most practical way.

🖃 📸 SQL Sei	ver Agent	
 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	New Job Manage Schedules Manage Job <u>C</u> ategories View History Fil <u>t</u> er Start PowerS <u>h</u> ell Reports Refresh	•



📧 New Job			_		×
Select a page	🕵 Script 🔻 📭 Help				
Schedules Alerts Notifications	Name: Owner:	BRUTE FORCE CONTROL			
🚰 Targets	Category: Description:	[Uncategorized (Local)]		~	
Connection					

		S New Job Step			
New Job		Select a page	Scipt + 🖸 He	b	
electapage P General	🕼 Script 👻 🚺 Help	Arranced	Step name. BRUTE FORCE CO	NTROL	
Steps Schedules	Job step list		Type:		
Alerts	St Name		Transact-SQL script	(T-SQL)	10
Targets	65.353218300183501		Run as.		
			Database:	master	~
			Command	exec BRUTEFORCE_CONTROL	~
			Open		
			Select Al		
		Connection	Сору		
onnection		Server. 192.168.182.138	Paste		
Server: 192, 168, 182, 138		Connection: SA	Parse		
Connection:		Wew connection properties			V V V V V V V V V V V V V
Mew connection properties		Progress		4	2
rogress	Move step:			Final.	
(Ready	* *	1			
111	New			OK	Cancel

	New Job Schedule				
and the second	Nene:	3 DAKIKADA 1			(Janaya Seriedare)
New John	Schedule type	Recounter		-	D England
Selecta page Procession	3				
P Steps P Schedules P Aleta	S Date	7.11.2018 U	01 52 17	3	
Notficatione	Frequency				
2 radez	Occurs:	Daly 🗸			
	Recurs every:	1 day(s)			
	Daily frequency				
	O Occurs once at	00:00:00			
	Occurs every:	→ (a)eturin 🔄 E	Starting at 00	00:00	(R)
			Ending at: 23	59.59	(\$)
	Ouration	12 20			
	Start date:	7.11.2018	O End date:	7,11	2018 [] - []
Connection			No end date:		
Server	Sunnay				
192.158.182.138 Connection: SA	Description:	Occurs every day every 3 minute() starting on 7.11.2018.	s) between 00:00:00 and	23 59 59	Schedule will be used A
		-			County Links
riogress					verver mop
O Peady	New	Pok.,	i Henry	3	
			OK Ca	ncel	

📑 New Job								-		×
Select a page Page General	Scrip	t 🔻 📑 Help					6			
Steps Schedules	Schedu	ıle <u>l</u> ist:								
Merts	ID	Name			Enable	ed I	Description	n		
Targets	New	3 DAKI	KADA 1		Yes		Occurs ev	very day e	every 3 minu	rte(s) b
Connection										
Server: 192.168.182.138										
Connection: SA										
View connection properties										
Progress										
Ready	<	<u>N</u> ew]	<u>P</u> ick		<u>E</u> dit			<u>R</u> emove	>
							(Ж	Canc	el

ΑЯКАКАРІ



ARKAKAPI

When we attack again, it can be seen that the system automatically sends us a mail in 3 minutes.

\leftarrow		9 ileti dizisinden 1. <	> =	•
	Brute Force Saldırısı Gelen Kutusu x			•
*	sqlserver.egitim@gmail.com <sqlserver.egitim@gmail.com> Alıcı: ben ╺</sqlserver.egitim@gmail.com>	01:55 (0 dakika önce)	☆	*
	Nov 7 2018 1:53:43:770AM VE Nov 7 2018 1:53:47:550AM TARIHLERI ARASINDA 'SA' KULLA	ANICISI 475 KEZ YANLIŞ ŞİFRE C	SIRDI	
	K Yanıtla 🕨 Yönlendir			

Now that we have detected the attack automatically, all we need to do is to block the entries coming from this IP address automatically.

You may as well write a rule with Powershell for Windows Firewall, or more efficiently, you can use the Server Logon Triggers.

It is indeed logical: now that we got the IP address of the attacker, we might as well create a blacklist table and write this IP within. Afterward, let us write a Logon Trigger and if the IP exists in this blacklist table, do not even allow him/her enter the password even if one knows it.

For this, we are going to make a change in a Stored Procedure named BRUTEFORCE_CONTROL.

First of all, let's create a database named AUDITLOG.

📋 New Database					_	
Select a page P General	Script 👻 📑	Help				
Poptions Filegroups	Database name:		AUDITLOG	à.		
	Owner:		<default></default>			
	Use full-text in	dexing				
	Database files:					
	Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Max	size
	AUDITLOG	ROWS	PRIMARY	8	By 64 MB, Unlimi	ted
	AUDITLOG	LOG	Not Applicable	8	By 64 MB, Unlimit	ted
Connection						
Server: 192.168.182.138						
Connection: SA						
View connection properties						
Progress						
Ready	<			Add	F	> Remove
					ОК	Cancel

Create a table named blacklist in this database.

CREATE TABLE [dbo].[BLACKLIST](

```
[ID] [int] IDENTITY(1,1) NOT NULL,
[DATE_] [datetime] NULL,
[IPADDRESS] [varchar](50) NULL
)
```

Now, update the Stored Procedure named BRUTEFORCE_CONTROL as follows, and add this code right before sending an email.

INSERT INTO AUDITLOG.dbo.BLACKLIST (IPADDRESS, DATE_) VALUES (@IP, GETDATE())

Finally, write a server trigger so that an IP found in this blacklist cannot enter the system.

However, before doing this operation, I highly recommend you to backup the system database, since in case of an error, neither you can enter the SQL Server.

Backup the master.mdf and master.ldf files inside the C:\Program Files\Microsoft SQL Server\MSSQL12\MSSQL\ DATA directory. You need to stop the SQL service to be able to backup.

Later, you block the entry of the computers in the blacklist by executing the query below.

create TRIGGER [connection_limit_trigger]

ON ALL SERVER

FOR LOGON

AS

BEGIN

IF CONNECTIONPROPERTY ('client_net_address') IN (SELECT IPADDRESS FROM AUDIT-LOG.DBO.BLACKLIST)

ROLLBACK;

END

The trigger we created can be seen in the Server Objects part like this:







Now we see that the IP address is written into the blacklist when we attack.

)LQuery6.sql - 19238.master (SA ((75))* 🗙 SQLQuery5.sql - 19238.master (SA ((70))* SQLLo
SELECT * FROM AU	DITLOG.DBO.BLACKLIST	
0% -		
🛾 Results 📑 Messages		
ID DATE_	IPADDRESS	
1 2018-11-07 02:08:37.890	192.168.182.1	

Moreover, even if you enter the right password, access is denied.

	gy connect to serve			
	Microsoft	SQL Server 2014		
	Server type:	Database Engine	~	
	Server name:	192.168.182.138	~	
	Authentication:	SQL Server Authentication	~	
	Login:	SA	~	
essfully.	Password:	******		
		Remember password		
nnect to Se	rver			>
Can	not connect to 192, 168	. 182. 138.		
Ado Ado	ditional information:			
l ,	Logon failed for login 'sa Changed database cont Changed language sett	a' due to trigger execution. text to 'master'. ing to us_english. (Microsoft SQL Server, Error: 17)	392)	

I hope that this article has been informative.

Take care...

Malware Programming and Lockdown Virus

There are many different motivations for virus developers. Some of them develop viruses for cyber vandalism, earning money, damaging a company or taking revenge from somebody. Some, on the other hand, roll up their sleeves to this issue for developing antiviruses or for understanding how to create a virus, or how they work to take the necessary countermeasures.

ARKAKAPI

Whatever reason leads these people to develop viruses, there is a problem that while you are doing researches for this issue, you encounter with fancy advertisements or phishing sites which pretend to be useful.

When I was a university student, I was into Java programming in my spare times. One day, I developed software which I also designed as a media player that acts like a virus because of its small error on the GUI. Multiple windows opened over and over and locked the computer like a Fork Bomb virus.

That day, I realized that there is no need, fund of knowledge or professional education to develop malware. The only thing you need is thinking simple! For instance, using Java.awt.Robot class with an infinite loop, you can fix the mouse cursor to 0,0 point of the screen. And if you run this software in the background, it can be used as a malware. Another example is creating software which copies itself to Windows Start Up while booting the computer, which creates new files and folders simultaneously and writes random bytes for bloating up the free storage area of the disk.

In this article, I am going to explain the steps to starting and following the right path for creating a virus. We will be covering a virus I have named as Lockdown.

Choosing the Ideal Programming Language

All programming languages have advantages and disadvantages, so we can't say a single programming language is the best for creating a virus. At this point, it is important to decide the programming language depending on what kind of a virus you plan to develop. Most especially the programming languages I recommend are Object Oriented, high-level languages such as C# and Java. If you use basic scripting languages, the features of your virus will be limited and because those languages can't be compiled, the source code will be open which is also a great problem. To run a virus created with a scripting language such as Perl and Python, an interpreter is needed to be installed on the victim's computer.

Another important factor is, in which language you are good at. For example, if you can't make a decision between C# and Java, and let's say that you are better at Java, you can easily choose it since both languages are Object Oriented. My personal choice has always been Java. This is also an advantage because it is relatively harder for anti-viruses to scan JAR files. Because Java is supported by all popular operating systems, it will run on all platforms apart from Windows. Unless you add a feature to make it only work in the Windows operating system.

Start-up Stage

First, you have to decide the features of the virus that you want to develop. In our example, the virus should copy itself to the computer and lock it continuously. What can be done for the virus to lock the computer? An encryptor to encrypt the files or a virus which will move the files to a hidden folder as the famous Wanna-Cry does? This is totally up to your imagination. In my example, my preferred method is thinking simple and creating something which prevents the user from using the computer and in order to recover it, something that requires a password like an encryptor.

We can make the virus to copy itself to the Windows Startup folder. That way, the virus will be run each time the computer is turned on. Another method would be letting the virus copy itself to random folders and create a Registry Key. But in this article, my preferred method is the first one. As a bonus feature, we might want to hide the metadata of the virus. Metadata contains details such as the infection time of the virus. Therefore, it will be a good surprise for the victims if the virus changes the creation, modification and last access when it runs for the first time.

About the coding of the virus.. From now I will be explaining the functions with the codes, so you can download the source code of our example virus from the link below. That way you can follow the steps easily.

Download Link

https://drive.google.com/file/d/16DNydtUz91sDP53SdOQNk3waZixRNR8e/view?usp=sharing

You even can compile and test the source code, but you will have to use your own image files instead of the ones I have used for the virus.

MetaStealth()

This function is for hiding the metadata. You can use FileTime for a specific date, but our example function sets all 3 metadata information to 1970.

About the other functions;

makeadminaccount()

This function executes terminal commands by using the Java process and runtime classes. This function also creates a new user with admin permissions and deletes the process log records. For doing all this work, the virus should be running with admin permissions.

copytostartup()

In this function, the virus first checks its own location and if it is not already in the StartUp folder, it decides to copy itself to the specified folder. After it copies itself, whenever the computer starts, the virus will also trigger itself. But as you can see, the copied virus is a JAR file, not an EXE. If the file was an EXE which contains admin manifest, it would request admin permissions as it did before while being infected. Thereby, the user would be aware of the issue and deny it. So, the virus would not be executed. Briefly, the virus will finish the processes that need to have admin permissions when it is first copied, so it won't make any administrative requests. That way, as a bonus we will make the antivirus software harder to detect our virus.

getSHA256()

The aim of this function is to calculate the SHA256 table of a given string value. By this way, the software will compare the table to the SHA256 table instead of the password entered to the textbox by the victim.

So why did we store the password that way? If we stored the correct password as a string in the program, anybody who decompiles the software would get the password. But now the only thing that he may see is the SHA256 hash of the password and that will be useless for the decompiler.

Lock()

We can say that this is the main function of the virus. The *requesting password after locking the computer* and *unlocking it if the correct password is entered* processes will take place in this function.

As you can see in the code, we first calculate the screen resolution and then create a new iFrame which has the same size as the screen. So we can cover the whole screen and make the computer unserviceable. That way, we also get rid of the minimize button. After that, we set the JFrame upmost using the setAlwaysonTop method in the GUI layer matrix. This way, we prevented other programs and the desktop from being seen with Windows and TAB keys.

Now we create the password input screen over this black panel. When the user enters the password and clicks on the unlock button, if the password is wrong, we display the cookie monster on the screen and if it is correct, we set our action listeners and start a daemon thread to protect the virus while running. Now, let's talk about the context of the daemon thread.

DaemonThread:

When the virus is running, the victim will try to fight against the virus instead of trying to enter the password. For such a situation we have to think about the actions to be taken against the virus and take the countermeasures to protect the virus by itself. So what can the potential moves be? For instance, the victim can start a process from the task manager, which can stop the virus working or end the relative process. Or he may use CMD (Windows Command-line) and take the same actions. There are some methods that can be used to prevent the process of our virus from not being ended. For example, we can create a second virus process and let both processes check each other. That way, if one of the processes ended, the other can start it once again. If the victim cannot access the CMD or Task Manager, he/she already cannot take these actions and there will not be any problem for our virus.

When the virus runs, this daemon thread will also run with it every 300 milliseconds, it will close the Task Manager, CMD and File Explorer. Thus, when the victim tries to open those tools, they will be automatically closed before they even come up to the screen. That means, our virus is safe for now.

Lastly, you may ask why daemon thread but not normal thread, I can say that daemon threads are better in GUI software on Java. Because they use fewer system resources than the normal threads and because it won't cause a bug to the Event Dispatch thread, our virus will work properly.

After completing the coding process of the virus and got the JAR output, our virus is almost ready. But we have something missing...

When the JAR file is running, because the virus is not working with admin permissions, copying itself to the StartUp folder and creating admin account features will not work. That means that when the victim restarts their computer, she/he can save himself from the virus. So how can we make the virus demand admin permissions?

At this point, EXE wrapping comes to play. What we need to do is converting the JAR file - namely the virus - into EXE and make it request admin permissions. We convert the file because only EXE files can request admin permissions. The reason for this is that the other file types are not executable. Our JAR file is like a command list that works on Java Virtual Machine. So the admin permissions can't be given to the JAR file itself, but to the javaw.exe.

For the wrapping process, you can search for different software on the internet. My choice is Launch4j.

Download Link: http://launch4j.sourceforge.net

Packaging Stage

Dasic Classpath Hea	der Singleinstance JRE Set env. variables Splash Version Info Messag	es
* Output file:		0
• Jan		6
	Dont't wrap the jar, launch only	
Wrapper manifest:		6
lcon:		
Change dir:	÷	
Command line args:		1
Process priority:	Normal Oldle O High	
Options	Stay alive after launching a GUI application	
	Restart the application after a crash	
Java download and si	ipport -	_
Error title:		1
N 17 N N N N	http://java.com/download	1
Java download URL:		1
Java download URL: Support URL:		
Java download URL: Support URL: Log		
Java download URL: Support URL: Log		

You will see the below screen when you download and run the software:

Here we have to enter the JAR file which we've exported and the wrapped EXE output addresses. Then we need the admin manifest file for the EXE file that the software will prepare to request admin permissions. You can find that file on the internet, but it is already included in the file that you've downloaded to get the source code of our virus. For that, download the .ico file and use it with Launch4j. Last, To export the EXE, you have to enter to the JRE tab and enter the min and max JRE versions. You can set them to 1.00 and 8.00 and click on Build Wrapper (gear icon) to create the EXE file.

When you make the configuration, the program will look like below:

You may even want to change the icon of the software.

🕌 Launch4j 3.11 - untitled — 🛛	x c
Basic Classpath Header Single instance JRE Set env. variables Splash Version Info Mes	sages
* Output file: F:\LockDown malware\LockDown.exe	
* Jar: F:\LockDown malware\LockDown.jar	
Dont't wrap the jar, launch only	
Wrapper manifest: F:\LockDown malware\AdminManifest.manifest	
Icon: F:\icons\winrar-logosu_1133244.ico	D
Change dir: .	
Command line args:	
Process priority: Normal O Idle O High	
Options 🗌 Stay alive after launching a GUI application	
Restart the application after a crash	
Java download and support	
Error title:	
Java download URL: http://java.com/download	
Support URL:	



Now that we have the EXE file, our virus is ready to go!

When you run the virus, it will demand admin permissions, and if you accept that, it will first infect itself to the Windows StartUp folder and lock your computer as seen on the image below. To get rid of the virus, you have to enter the correct password. This will stop the virus from working and after you will have to delete it, or you can delete the virus by using a Live Linux distro.



As you can see, we created a virus similar to an encryptor.

Although it is an EXE file, the antivirus software and Windows defender cannot easily detect it because it actually is a wrapped JAR file.

The desktop cannot be reloaded in some computers because of a simple bug. In such a situation open the Task Manager and restart Explorer.exe.

Warning: The context of the article and the source code of the Lockdown virus is for educational purpose only. I hereby declare that any damage that is caused by the virus is not under my responsibility.

P.S.: If you run a compiled version of the virus accidentally, recovery password is "Adem1234".

Network Programming with Scapy

Even though the simplified version of the packet structures on the network is constantly in our hands, we may have new discoveries when we examine these packages bit by bit. In order to listen to the desired packages through the network and see the details of the bits we want, we can use the visual interface part of the programs like Wireshark and the command line tools like tcpdump among the terminal user interfaces.

If we included the concepts we mentioned on the network to programming, it would be effortless for us to experiment, make changes as we wish, or examine the parts of our interest in depth. In fact, if a request did not go the way we want, we could take measures related to it. It would even make it possible to change the packages we listened to and put them on the line again. If we could use a language such as Python, interactively from the command line, or if we wanted to write the code into a file and pack it as we wanted, we could have brought it to a format useful in detecting many problems.

Scapy is a package manipulation library that can analyze and parse many protocols, including those mentioned, making it possible to manually generate packages, disassembling layers on the package, replacing them with other layers, and much more.

Speaking of such concepts, it is important not to forget that we are able to do the work of many programs such as Nmap, traceroute, tcpdump with Scapy. For example, we can determine different TTL values in the packets that we create and provide similar functions to traceroute functions according to the responses before certain amount of time runs out. As a matter of fact, there are many different libraries written with Scapy. This includes Wi-Fi traffic injection or those which go to such high levels enough to make an HTTP request with Scapy.

ARKAKAPI

When the tools used in cyber security do not provide the desired feature or there is no suitable tool to do the desired job, it usually takes a very short time to complete these deficiencies with Scapy and produce very understandable results.

Scapy can save packages in PCAP format. It can even read saved PCAP files or other programs by itself and make it possible to play with them by transferring them to their own data structures.

Scapy automatically performs checksum calculation, which can be an exhausting process, even though if done correctly, during package creation or when bits on the packages are changed or overlooked. When creating a package, you can work with Scapy to define the requested fields, often without any additional requirements.

Installation and Usage

Since it may take a lot longer to talk about Scapy, mentioning the areas of use, let's move forward hoping that I drew the necessary attention. In this section, we are going to talk about installing Scapy on the system. For this we will work on Ubuntu 16.04. Pre-installation and using some of common commands on the terminals of GNU/Linux systems shall make it easier for you. Finally, you will need an internet connection to implement the commands here.

Since many dependency needs can occur during installation, let's move forward by seeing the errors we may

encounter. We will proceed to learn how to correct these errors, even if we are addressed with too many error messages. Therefore, we will consciously write some commands incorrectly until the installation is complete and talk about what should be done.

We will install Scapy using Python 3 and use PIP for package installations. In addition, since we would not like to do the installation all over the whole system, we are going to install a virtual environment and install packets in this environment as much as we can. An advantage of doing so is that you will find the chance to work with two different versions of Scapy. Besides, this also shall enable us to create a medium where you will question the project-specific dependencies. The virtual environment and the files we will run will be the directory called **workshop** created under the home directory. Let's move forward by creating it and setting up Pip and virtualenv:

```
sudo apt update
sudo apt install python3-pip
pip3 install virtualenv
pip3 install --upgrade pip
```

```
mkdir workshop
cd workshop
```

The commands are: setting pip for Python3 up, and then installing the virtual environment package using pip, and updating of Pip using itself, respectively. Finally, we create and open the directory called workshop. Now we create and activate a new virtual Python environment (virtual environment) in workshop:

virtualenv -p python3 venv
source venv/bin/activate

To verify it, you can check to see if *venv* is written at the beginning of the command line.

This statement will be useful to check which virtual environment you are working on if the name of the virtual environment you are creating is different from the name of the environment you are working on :

which pip # /home/\$USER/workshop/venv/bin/pip

If you typed the commands in your home directory from the beginning, the output of the command will be similar to the one given above. Only your username would be written instead of *\$USER*. After verifying that Pip is on the project-specific virtual environment, let's install Scapy:

```
pip install scapy
```

With this command, Scapy will be installed on the system. Let's try running it now:

Scapy

If you pay attention to the output, Scapy opens with a lot of warnings are given in between. So are these warnings critical? Although the answer to this question depends on the things you want to do, the fact that there are no modules such as *ipython* or *cryptography* increases the chances of having problems. Therefore, we will try to move forward by establishing as many dependencies as possible. Now, to exit, let's type exit() or use CTRL+D, then install the missing packages using pip:

pip install matplotlib pyx cryptography ipython

If we try to run Scapy again after completing the installation, we can see a warning like texlive or ... in the output. While we're at it, let's load it. We will install texlive with apt :

sudo apt install texlive

Note: Of course, we have to get out of Scapy before we write this command.

After all this effort, let's open it up to enjoy Scapy :

scapy

When working with Scapy, we can use the conf command to verify which settings are currently running and also to test the setup we have done in simple terms:

>>> conf

One of the most important areas to be considered in this output is the section in which iface is written section. It is useful to edit it if the connection interface we want to use is not selected. For example, while wanting to work on an Ethernet card, you may see the interface for the wireless internet connection in this section; to edit this :

>>> conf.iface = "enp0s3"

In this command, enp0s3 is actually the interface name, so it is useful to edit it according to your system and purpose (for example, your system can have values like eth0, wlan0).

Let's try to listen to a packet while we're all set up. Since listening is often referred to as sniffing, the name of the function that makes it on the Scapy is called sniff. Now let's try to listen to a package by keeping it simple :

>>> sniff(1)

If you want to write and run the command, you must encounter an error message like "Operation not permitted" (although most of the time it is not recommended, you are expected to not receive this error if you are working as a root user). To solve this problem, you need to open Scapy with a user with administrator privileges. Let's remember that this package is based on the virtual environment inside the workshop directory and we want to open this environment with root. After leaving Scapy, let's run the scripts that are prepared to simplify the installation:

sudo su cd /home/\$USER/workshop/
source venv/bin/activate
scapy
>>> sniff(1)

In the first line, you are switching to root, and you can use your own username instead of *\$USER* in the second line. In the next lines, there is a small example of the expressions that we took a look at so far. In the last line, we want to



catch 1 packet with a sniff and we leave it to listen. If you have active network traffic, this line runs so fast that it may be hard to notice it takes time. If your network traffic is stagnant, the program will wait on this line until a packet is gone.

If you are using Ubuntu on a virtual machine while your sniff () function is running and your network traffic does not have an incoming-out packet, you can try to open a new terminal and ping an IP address. It will appear here when the first ping request is gone. You should get a printout similar to this:

<Sniffed: TCP:0 UDP:0 ICMP:1 Other:0>

Optionally, you can also apply BPF filters during network monitoring. They will be similar to the ones in the tcpdump command. For example:

```
>>> sniff(1, filter="tcp port 80")
```

After you receive the packages, you may want to assign it to a variable to examine:

```
>>> pkt = sniff(1)
```

>>> pkt

```
<Sniffed: TCP:0 UDP:0 ICMP:1 Other:0>
```

In order to capture more than one packet with sniffer, we can write down how many packets we want to capture instead of the number 1 in it. Let's play a little:

```
>>> pkt[0] # Details of the first packet in sniffed packet list
```

>>> pkt[0]/"HELLO" # Add "HELLO" as payload

In the first line, we get a summary about the first package in the PKT structure. In the second line, we add "hello" to the package as content.

It is possible to save packages in PCAP format and then open them with programs such as both Scapy and Wireshark.

```
wrpcap("filename", variable_name)
variable_name = rdpcap("filename")
sniff(offline="filename") # Directly save to a file
```

The wrpcap in the example is actually used as write pcap, and rdpcap as read pcap. In the last line, the function we write will be saved directly in the file that we named.

We can use the IP () class to generate an IP packet from scratch. In the previous example, as we add "HELLO" letters to a package, we can combine the network layers in this way:

>>> IP()
>>> IP(dst="IP.AD.RE.SI")
>>> pkt = IP(dst="IP.AD.RE.SI")/ICMP() # Ping packet

In the first line, we looked at how to create an empty IP packet, and in the second line how to give the target IP address, but we didn't assign it to a variable or something. In the last line, an ICMP packet is generated after determining the destination address of the structure we have set up. The default packet generated of type ICMP echo request, which is often referred to as Ping. If we want to send this package to the real network:

>>> send(pkt)

It will be suffice. Since there are a few other parts that we need to set up, the package will probably not reach its destination even if it is actually dropped into the network.

While being able to create each part of the packet manually, we can also specify the target IP address. For example, if we want to send a ping package from 172.17.0.2 to 172.17.0.3;

>>> send(IP(src="172.17.0.2", dst="172.17.0.3")/ICMP()/"hello",

iface="enp0s3")

The ability to determine the source IP allows us to use whichever we want when we have more than one IP address and this can be used when running some tests in network management. To track what this command does, write tcpdump -vv and watch the packets from a separate terminal or track them with an application like Wireshark. We can also specify how many jumps we can allow on the network by giving a TTL to IP packets:

>>> send(IP(src="172.17.0.2", dst="172.17.0.3",

TTL=10)/ICMP(type=13)/"hello", iface="enp0s3")

In this example, we have identified 13 as the ICMP type. Just in case that it may the first time you encounter with this type, let's talk about what it does; it is used to ask the timestamp to the server over the network.

Before concluding the first part, let's talk about how we can send a request and get back a response. By using the initials of Send-Receive, it is possible to send a packet and wait for response(s). Now let's take a look at an example:

```
>>> pkt = IP(dst="172.17.0.2", ttl=10)/ICMP(type=8)
>>> sr(pkt) # Sends and receives the responses, Layer 3
```

The last line we wrote deals with packets in the third layer of the OSI model. An example can be like:

```
>>> sr(pkt)
Begin emission:
*Finished sending 1 packets.
Received 1 packets, got 1 answers, remaining 0 packets
(<Results: TCP:0 UDP:0 ICMP:1 Other:0>,
```

<Unanswered: TCP:0 UDP:0 ICMP:0 Other:0>)



Sent packets, incoming responses and missed packets can be seen in detail in this output. The output above corresponds to a ping (ICMP echo request) that has been responded to.

As in this example, SR1 gives a much simpler output if we are just waiting for an answer. The number 1 in the function name means that we expect only one answer. Example of usage and sample output:

```
>>> sr1(pkt) # Returns one answer, Layer 3
Begin emission:
*Finished sending 1 packets.
```

```
Received 1 packets, got 1 answers, remaining 0 packets
```

```
<IP version=4 ihl=5 tos=0x0 len=28 id=15563 flags= frag=0 ttl=64 proto=icmp
chksum=0xe5f0 src=172.17.0.2 dst=172.17.0.1 options=[] |<ICMP type=echo-re-
ply code=0 chksum=0xffff id=0x0 seq=0x0 |>>
```

In the next issue, we will examine how to produce packages in the second layer of the OSI model, how to display the details of packages at different levels of detail and to examine the packages more clearly, to make TCP connections starting with three-way handshake with Scapy, to develop port scanning application in a fast and practical way with Scapy and the filtering of received answers, and see a way to create packets with only desired flags being set. Besides, we will mention how to set a timeout and an auto-retry limit to the responses, how to create a DNS request, and perform some simple attacks that are related to cybersecurity in Scapy. We will also recommend some resource suggestions for those who want to get to know Scapy further.

For more examples about this article, please see to Scapy's documentation at https://scapy.readthedocs.io/en/latest/.



Siber Yıldız 2019 Writeup

Preparation Question 1: Do you want to work with our IT company? (Bilişim şirketimizde çalışmak ister misin ?)

When the page's source code is examined

```
   © Maxim Theme. All rights reserved.
   <div class="credits">
        <!-- !!! Yonetici Panelini tespit edebilecek misin? -->
        <a href="https://bootstrapmade.com/">Free Bootstrap Themes</a> by BootstrapMade.com
   </div>
```

It wanted us to find the admin panel. I decided to run dirb, found the admin panel and claimed the flag:

```
    ← → C ① Not Secure | 85.111.95.17/c76b3bd64481c9f391372497fa7c9275/webadmin/
    Tebrikler bayrak senindir :
```

RUp2cWFJNHNmekYvQVUyemZXQXRYbFV6T114cEQ0UFJGYTVLb25MN3EwdW8ra3VxNncrVFNtRFRNenJ1V1VEVFJBQ1RySk1HWkU5eGw4Z3o0dW1KSEE9PQ==

Preparation Question 2: If you examine well you can find the answer. (Dikkatle incelersen cevabi bulabilirsin.)

Bakalım beni bulabilecek misin?



When you take a look at the page's source code, it says that you need to look at another URL.



🎔 twitter 🔞 Hack The Box :: Access 🚯 Bugcrowd 🔯 Outlook 💽 protonmail 🔛 Discord 🔥 Udemy 👩 reddit 🔋 s

Bu algoritmayı çözersen bayrağı kapabilirsin :

//basindaki HTTP'yi unutma
url =BU_SAYFANIN_URL_ADRESI
anahtar =url.split("/")
//0 dan baslayan bir dizi
bayrak = md5(anahtar["4"])

When we go to the URL, you see an algorithm structure we need to solve. The key (*'anahtar'*) implies that we need to use *'/'* to move in the directories and that the flag is in the fourth *'/'*. When we examine the URL, as the algorithm explains, the part after the fourth key shall give us the flag. After hashing the expression "87habyth-i15ng151.php" with md5, we got the flag.

COMPETITION QUESTIONS

Question: This really is easy (Bu gerçekten kolay)

It made us download a file named dikkatli.bak.dms. When this file is opened with any text editor, we see the following expression:

flag: RDcxVWV3SUFLM29RazBGV1Rnb0dsbURpWDJnckg1MUgv209WWF2mbkFBWmhjczk3S291TGprSnZEMENtYmxnd2R6d0tOc2pKeH2KVW8zVHczSUtIRUE9PQ==

Question: Still warming up (Hala ısınmalardasın)



When we examine the source code of the question, we see some scripts. When decoded with the charcode decoder, the flag got extracted.

Question: Respect for labor (Emeğe Saygı)

Emeğe saygı. Toplam Puan:200	Göreve Başla				
GÖREV KODU					
					KODU GÖNDER

Answer:



		Sabahçı Kahve	si - Mozilla Firefox				
🔿 Telegram Web	× B Siber Yildiz 2019 - Türkiyi ×	 Sabahçı Kahvesi 	× +				
\leftrightarrow × \diamond	Q, 85.111.95.20/d6(6b368d7c039d	ae9bee3e0c7cfa93e-02/inc	iex.php	Q, Search	¥	10	(
A Most Visited M Offens	ilve Security 🥆 Kali Linux 🥆 Kali Docs	🔨 Kali Tools 🥌 Exploit-E	08 🐚 Aircrack-ng 🗾 Kal	li Forums 🥆 NetHunter 👼 Getting Started			
			Allen and and a				
		Cok calistik, cok. Emo belirtin.	ege saygi gosterin, ka	aynak			

When I opened the page, there was a sentence: "Cok calistik,cok. Emege saygi gosterin, kaynak belirtin." (We worked so hard. Have some respect for labor and specify source)

				Mozilla Fire	fox	
🕤 Telegram Web	×	8 Siber Yıldız 2019 - Türkiyi 🗙	New Tab	×	+	
$\leftarrow \rightarrow \times \diamond$	Ē	Q about:blank				Q. Search
A Most Visited M Off	fensive Se	ecurity 🔨 Kali Linux 🥆 Kali Docs	🔨 Kali Tools 🍝 Exp	loit-DB	Aircrack-ng 🛛 Kal	li Forums 🥆 NetHunter 🧕 Getting Stan

		Burp S	uite Free Ed	ition v1.7.2	27 - Tempor	ary Project	t		0	Θ	0
Burp Intruder Repeater	Window Help	ler T Repeater	Tsequencer	Decoder	Comparer	Extender	Project options	Luser options	Alerts	8	-
Uttercedt HTTP histor	y WebSockets hist	ory Options]	- ensurer	Cecupiater	Contender	Lucies options	- one options	Ecolics		_
Request to https:: Forward	/siberyildiz.com:443 Drop	[85.111.95.1 ercept is on	2] Action				Ē	Comment this it	əm .		2
Raw Params Heade	Hex Hex										-
<pre>dost: siberyildiz.com Jser-Agent: Mozilla/5. kccept: text/html.appl kccept-Language: en-US kccept-Encoding: gzip. Veferer: https://siber Connection: close Contai: PMPSESSID-7dlc Doprade Insecure.Reque</pre>) (X11: Linux x86 ication/xhtml+xml. en:q=0.5 deflate /ildiz.com/sorular 17nn84074osiv4gieg	64; rv:65.0) application/: tt42	Gecko/20100 ml;q=0.9,im	101 Firefo age/webp.*	x/65.0 /*;q=0.8						

So I decided to analyze with Burp; there was a cookie value as well as a Referer part. When I made random changes to the Referer part and sent the request, you can see "Kaynak belirtenlere hediyelerimizi gönderdik. Sağolun varolun." (We gave prizes to those who specified the source. Thank you so much.) written in the response part. When we saw this part we thought that we were in the right place; only had to change the Referer part. So we tried various changes to the Referer. The "Sabah Kahvecisi" title of the website might as well have been a hint, so we googled that and found the *Sabahçı Kahvesi* song by Ferdi Tayfur and gave the YouTube link of it to the Referer but failed.



Burp Intruder Repeater	Window H	elp									
Target Proxy Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	
Site map Scope											
Filter: Hiding not found ite	ms; hiding	CSS, imag	e and gene	ral binary con	tent; hidin	g 4xx respo	nses; hiding	empty folders			?
 http://85.111.95.19 http://85.111.95.20 http://detectportal.fir http://dimsemenov.cc http://dimsemenov.cc http://github.com http://sileryildiz.com http://sileryildiz.com http://startbootstrap. 	re.com efox.com pm bis.com om			Host https://siberyi https://siberyi https://siberyi https://siberyi https://siberyi Request R Raw Parar POST /ajax/ar lost: siberyi Jser-Agent: N Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200 Accept = 200	Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idiz.com Idi	Method POST GET GET GET GET rs Hex .php HTTP/ 0 (X11; Li ,en;q=0.5 deflate yildiz.com ion/x-www- ttpRequest 17nn840740	URL /ajax/answer /go.php?s=5 / /ajax/answer /go.php 1.1 nux x86_64; /sorular form-urlence siv4giegtt4;	Pa Group.php Group.php rGroup.php rv:65.0) Gecko oded; charset=U	rams Status ✓ 200 ✓ 302 □ 0 ✓ 302 □ 0 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100 ✓ 100	Length 315 453	MIME ty text text HTML

When I looked at the site map section of Burp, I saw a section called Cevap (Answer) by the QuestionId. But that was just unnecessary thrill :) What we had to do so was to prepare a file that records the requests that came with the sniffer, thinking that it made a request to the Referer. The flag came when we looked at the file.

[HTTP_REFERER] => işte ödülün (here's your flag) : aFZPL0hkSjhvaThneGdIdkFMcUd1UFZLO-GNhMGxGSG1lak1VbXIROFVGO

FdxVWI3bjFYTW10bVVFMk5ZdTVQV3daRSsxWFZsbmZWZ3dLOFMveHZxQnc9PQ==

Hersey sanal, ağ gerçek. Toplam Puan:150 Göreve Başla	
GÖREV KODU	
	KODU GÖNDER

Question: Everything is virtual, the network is real.

As the start, we downloaded a wireshark file.

# Jught	warm the					Correstant - Correstant -
-	Time	Bouria .	2millador-	Probabili	tangt bin	
	10.000000	172.16.114.134	172.15.114.1	085	72 Standard (proy BellDr A was, bing.com	
	2 1.049/73	177.10.134.134	172.15.334.3	185	72 Standard query Bollle A unsubing.com	
	3.2.055471	177.16.114.1.04	172.10.114.1	105	72 Standard geory Relate A seeching.com	
	8-4.090521	322.38.334.134	172.10.134.1	ENG.	72 Standard garry Bol33e & searching.com	
	3 8.889(21	377.10.114.134	172.18.134.1	ERN .	22 Standard query Bollite A ann.birg.com	
	8 12.399666	377.36.114.134	172.16.134.132	310	26 2409 + 80 [SV5] Secol simeR292 Lenet PSS-5468 MS-626 SOCK FERE-1	
	7 12.358125	172.16.114.132	122.10.114.114	TCP	00 80 + 2400 [SVN, ACK] Segrill Ack-1 Min-29200 Lini-0 MSS-1000 SACK_FEBH-1 M	i=128
	8 12, 200175	372.10.114.134	177.15.334.332	10*	54 2469 + 80 [ACK] Sep-1 Ack-1 Win-525064 Len-0	
	9 12.334323	172.16.114.134	172.10.114.113	NULTR-	473 467 /wsim.jpg NTTP/1.1	
	18 12.350118	172.16.114.132	177,16,114,134	TCP	00 80 + 2450 (ACK) Sep-1 Ack-420 Mis-30136 Lam-0	
	11 12:354816	\$72.16.114.132	172, 36, 334, 134	BUILDA	236 BITDY1.1 384 Ref. PodiFied	
	12 12,416369	372.10.114.134	172.15.134.132	TEP	54 2460 + 80 [ACK] See-420 Ack-183 Hin-525312 Lar-8	
	11 17.353720	Manara Michiele .	Weare_Eat21tSe	ARP	60 Mbo has 172.16.114.144/ [#11 172.16.114.112	
	14 17:35317	smaare_sat23the	Vmuint_66138171	689	42.372.38.334.334.334.34 38.45.46(0)(29)(6)(29)(6)(2)(5e)	
	15 17. 899730	173.16.214.134	172,18,114,107	3CP	54 2460 + 80 [FDN, XCN] Seq-420 Ack-188 HDA-525812 LDR-0	
	15 17 178662	172 10 114 132	177.18.118.118	TCP	10.50 + 3450 [FDN, ACK] Sept181 Acked23 Min(30136 Level	
	17 17. 170/48	377.16.334.134	172.18.114.112	HP	56.2469 + 89 [ACK] 50g-623 Acks366 Minu525312 Limid	
	13 20.803796	Wmare_60173/3e	Resident	JRP	42 Mbs Fes. 172.16.114.1327 Tell 172.18.114.134	
11.1	19 28,894557	Vessely_d5(3d;7)	Venere_64.2375e	. 422	(# 172,16,114,132,15 et.@;0;:25.06;14:7c	
	28.28,815243	177.10.114.134	177.15.334.332	110	20 20200 * 120 [240] 2eb-0 Min-2020 [642-2600	
	21 20.005831	177.10.114.134	172.10.114.112	scr	26 26240 × 22 12/81 202-8 Min 2824 129-6 702-2400	
	12 AP (07518)	3 (2.10.314,134	1/2,10,334,932	11.0	CALCUMENT AND AND SEARCH AND AND A LONG ADDRESS OF	
	12 26 2802020	102.10.114.142	172-19-114-104		on the worker light work ped-t works when rease	
	24.20.820919	100 Britherin	102110-110.104	100	60 22 + 50540 (KD), FKK) 500+1 ACK+1 NUT+0 LAT+0	
	D R. TANK	101404104104	17271971147114	10	to as a pepter (ks), numbers access access access	
10000	ALL ALL ADDRESS.	ALL DE LANGERA		10.0	De Service e las lavait de la des constantes en la constantes	
	IT W. SHERT	117.10.101.118	177.18.138.133	10.0	All Parket + an United and a market that a supervised	
	20 20.08(347	-102.10.110.100	177.13.118.118			
-	32.30 436213	171.16.114.113	122 16 314 114	70.0	IN SEA A SALES THAT ANY A CARD A LAST MAN AND A REALTING	
-	THE REPORT OF	117. DO. 114. 194	172.1.0.1.0.2.0	100	THE FULL AND AND AND AND AND AND AND AND AND AND	
-	11.10.000171	122 04 114 132	172 16 114 114	3/8	MANUAL SALES (SCI. 1971) South Michael Sales and Sales	
_	TRUE AND AND	170 M. 114 T M	121114 1014 121	100	AN ADDRESS AND A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRIPTION OF A DESCRI	
1.8.		- In the last	** 6		Iteshark Export IIIII objectust	•••
Pac	k 👻 Hos	stname	Content	Туре	Size Filenan	ne
	,		1	-1	104 bytes /	

427		text/html	104 bytes	/
512	172.16.114.132	application/x-www-form-urlencoded	88 bytes	/
515	172.16.114.132		441 bytes	sdk
534	172.16.114.132	text/html	104 bytes	/
537	172.16.114.132	text/html	281 bytes	sdk
539		text/html	104 bytes	/
541	172.16.114.132	text/html	288 bytes	robots.txt
550	172.16.114.132	text/html	316 bytes	/
552	172.16.114.132	text/html	302 bytes	nmaplowercheck1505200568
556	172.16.114.132	text/html	104 bytes	/
559	172.16.114.132	text/html	316 bytes	/
568	172.16.114.132	text/html	287 bytes	HEAD
617	172.16.114.132	text/html	104 bytes	/
618			153 bytes	
619	172.16.114.132	text/html	316 bytes	/
621	172.16.114.132	text/html	283 bytes	HNAP1
629		text/html	282 bytes	
655	172.16.114.132	text/html	104 bytes	/
687	172.16.114.132	text/html	289 bytes	favicon.ico
853	172.16.114.132		223 bytes	sslkeylog.log
856	172.16.114.132	text/html	289 bytes	favicon.ico

Examining the package, it could be seen that there had been a few URL clicks and meaningless packages and nmap logs. When I exported the files within, there were again some senseless files except the sslkeylog.log which could be of use. In this way, even if we do not have a server key we can resolve the traffic passing over ssl.



inchero	io 150 pcap Vice Go. Capture Analy	er Statistes	lelephony Wheless Too	i Hep				-	3
1	Copy	1	12 H 4 4 4 5	[
10.4	Find Packet.	Crish	and the second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second s	7413.01				D • 9	(const
	Find Preside	CHI-S	bedratut.	Tubbal .	Distantiant score Ballin & say blog con				
	Marithanak Rodet	rolat	172.16.114.1	045	72 Standard query 8x333r & sea bleg.com				
	Mark All Displayed	CR+Svit+M	172.16.114.1	D//5	72 Standard query 6x113r & mar.bleg.com				
	Device Nt Dittraped	CHI-MI-M	172.16.114.1	Diff	72 Standard overy Bollin A new blog com				
	Beet Mark	CD-Shiteli	172.16.114.112	1729	WE 2009 + 88 (SVS) Sepid MinuRISC Locus PSS-1400 MS-256 54	00,99893			
	Farenza Maia	DESIMA	172.16.114.114	777.PP	45 M + 2468 [SWL ACK] Sequel Arkit 5010-20200 Linio 1955-14	IND SACK PERMIT INSULT			
	Ignore/Enigrose Packet	CHI-D	172, 16, 114, 132	7139	54 2008 + 38 [A/N] Seq=1 A/N=3 300-325564 (Jmin)				
	Ranner All Glassered	Cui+Shitt+D	172.16.114.114	TINE.	68-98 + 2661 (ACK) Separt Ackar20 Minu10336 Lowall				
	radiancer controled	ANDAROAD	172.16.114.114	HITE	238 HTTP/S 3 300 But Hodified				
	Set/Unset lime Reference	CHI-F	172.16.114.111	TIP	54.2669 + BR [ACK] Seq=620 Acks[83.30]ar/525312 Lon-0				
	Total Long Removers	CRAME-1	Vessere di VIT	410	42 172 16 116 116 116 10 00 00 20 10 12 173				
	FRENDLA TIMA ROMANNA	Develop-10	172.16.114.112	TOP	54 2009 + 38 [ftb, 4(4] Seg-620 dc8-183 bls-525312 los-0				
	Time Shift	Co-Sub-T	172.16.114.114	7139	NR 80 + 2449 [FIN, A(F] Sec-18) Ack-421 win-30104 Lorost				
	Darket Commont	Children.	Broadcast	AND	42 who have 172 bit 114 1102 Tell 172 16 114 114				
	Desete All Packet Communits	Carriere	Visiere Ba 22:5e	ANP	68 172 16 116 113 14 at 69 9c :29:28:34 7c				1
	Contractor in the	(multiple)	109.10.110.007	TOM	58 SPAR - 176 [SV9] Seget Hindald Level Monitole				
Unter Doer Doer	net II, Src: Vesare So net Protocol Version & Datagram Protocol, Src in Nome System (query)	23:5e (00:0e , Src: 172.0 Part: 50460,	(2064(2) 5c), Osti (114.154, Osti 172, Det Part: 53	Veure cil 36.134.1	98-99, (81:97:56:c0:98-93)			2	_
	Wireshark • Pr	eference	25					? X	<
	SMP SMPP SMRSE SMTP SMUX SNA SNMP Snort SoulSeek SoupBin ^T SPDY Spice SPRT SRVLOC SSCOP SSDP SSDP SSH SSL STANAG STANAG	e TCP	Secure Sc RSA keys lit SSL debug Reasse Reasse Reasse Messag Pre-Shared (Pre)-Maste C:\Use	st file mble SS mble SS e Autho -Key [er-Secro	Edit Edit Bro	owse			
						ОК	Cancel	Help	

After embedding sslkeylog.log in the SSL part of the Protocols section in Wireshark settings, the decrypted logs appeared in the Pcap, and when these were examined, it could be seen that there had been entries to some places.

Esra Nur Soylu • Siber Yıldız 2019 Writeup

			470 46 444 400	NTTO	444 GET /00037E03130E0E7330E47032 okt UTTD/1 1
	798 69.609191	172.16.114.134	1/2.10.114.152	ni ie	444 del /9905/502150505/2105/12954/025.pkt h11P/1.1
	799 69.618844	172.16.114.132	172.16.114.134	HTTP	339 HTTP/1.1 200 OK
	800 69.666286	172.16.114.134	172.16.114.132	TCP	54 2499 + 443 [ACK] Seq=652 Ack=1914 Win=65280 Len=0
	801 69.676105	172.16.114.134	172.16.114.132	HTTP	392 GET /favicon.ico HTTP/1.1
	802 69.676812	172.16.114.132	172.16.114.134	HTTP	589 HTTP/1.1 404 Not Found (text/html)
	803 69.728932	172.16.114.134	172.16.114.132	TCP	54 2499 + 443 [ACK] Seq=990 Ack=2449 Win=64768 Len=0
	808 74.679636	172.16.114.134	172.16.114.132	TLSv1.2	85 Alert (Level: Warning, Description: Close Notify)
	809 74.688029	172.16.114.134	172.16.114.132	TCP	54 2499 -> 443 [FIN, ACK] Seq=1021 Ack=2449 Win=64768 Len=0
	810 74.680418	172.16.114.132	172.16.114.134	TLSv1.2	85 Alert (Level: Warning, Description: Close Notify)
	811 74.688475	172.16.114.134	172.16.114.132	TCP	54 2499 + 443 [RST, ACK] Seq=1022 Ack=2480 Win=0 Len=0
	812 74.680557	172.16.114.132	172.16.114.134	TCP	60 443 → 2499 [FIN, ACK] Seq=2480 Ack=1822 Win=32512 Len=0
F	rame 798: 444 byt	es on wire (3552 bit	s), 444 bytes capture	d (3552 bits	.)
E E	rame 798: 444 byte thernet II, Src:)	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Sec: 172	s), 444 bytes capture 0c:29:6a:23:5e), Dst: 16.114.134, Dst: 172	d (3552 bits Vmware_d6:3	;) id:7c (00:0c:29:d6:3d:7c)
F	rame 798: 444 byte thernet II, Src:) nternet Protocol) ransmission Contro	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. al Protocol. Src Por	<pre>cs), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499. Dst Port: 44</pre>	d (3552 bits Vmware_d6:3 16.114.132 3. Sec: 262.	;) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629. Len: 390
F	rame 798: 444 byta thernet II, Src:) nternet Protocol) ransmission Contro ecure Sockets Lave	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er	s), 444 bytes capture 0c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262,	;) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390
F	rame 798: 444 byta thernet II, Src: 1 nternet Protocol 1 ransmission Contru- ecure Sockets Lays ypertext Transfer	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol	:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262,	i) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390
FI E	rame 798: 444 byte thernet II, Src: 1 nernet Protocol 1 ransmission Contri ecure Sockets Lay ypertext Transfer GET /99837582138	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol S585721057129547823.	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44 pkt HTTP/1.1\r\n</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262,	i) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390
F	rame 798: 444 byte thernet II, Src: 1 ransmission Contri- ecure Sockets Lay ypertext Transfer GET /99037582137 Host: 172.16.114	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol SSB5721057129547823. 4.132\r\n	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44 pkt HTTP/1.1\r\n</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262,	;) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390
F E I I S I H	rame 798: 444 byte thernet II, Src: 1 nternet Protocol 1 ransmission Contrr ecure Sockets Lay ypertext Transfer GET /99037582133 Host: 172.16.11 User-Agent: Nozi	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol 8585721057129547823. 4.132\r\n 111a/5.0 (Windows NT	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44 pkt HTTP/1.1\r\n ' 18.8; Win64; x64; rv</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko	:) dd:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390 //20100101 Firefox/55.0\r\n
F E T S H	rame 798: 444 byte thernet II, Src: 1 nternet Protocol 1 ransmission Contre cure Sockets Lay ypertext Transfer GET /99037582133 Host: 172.16.114 User-Agent: Moz: Accept: text/htm	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol 5585721057129547823. 4.132\r\n illa/5.0 (Windows NT al,application/xhtml	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. 't: 2499, Dst Port: 44 pkt HTTP/1.1\r\n ' 10.0; Win64; x64; rv +xml,application/xml;</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko q=0.9,*/*;q=	;) d:7c (00:0c:29:d6:3d:7c) Ack: 1629, Len: 390 /20100101 Firefox/55.0\r\n 0.8\r\n
F E I T S H	rame 798: 444 byte thernet II, Src: 1 ransmission Contre ccure Sockets Lay ypertext Transfer GET /9903758213 Host: 172.16.11/ User-Agent: Mozi Accept: text/ht Accept-Language	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol S585721057129547823. 4.132\r\n illa/5.0 (Windows NT al,application/xhtmal : en-U5_en;q=0.5\r\n	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. 't: 2499, Dst Port: 44 pkt HTTP/1.1\r\n ' 10.0; Win64; x64; rv +xml,application/xml;</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko q=0.9,*/*;q=	;) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390 //20100101 Firefox/55.0\r\n 0.8\r\n
F.E.I.I.S	rame 798: 444 byte thernet II, Src: 1 ransmission Contre ccure Sockets Lay ypertext Transfer GET /9903758213 Host: 172.16.11/ User-Agent: Mozi Accept: text/htm Accept-Language Accept-Encoding	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol SSB5721057129547823. 4.132\r\n al,application/xhtel : en-US,en;q=0.5\r\n : gzip, deflate, br\	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44 pkt HTTP/1.1\r\n</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko q=0.9,*/*;q=	;) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390 /20100101 Firefox/55.0\r\n 0.8\r\n
FEIT	rame 798: 444 byte thernet II, Src: 1 nternet Protocol 1 ransmission Contr- ecure Sockets Lay ypertext Transfer GET /99037582130 Host: 172.16.114 User-Agent: Mozi Accept-Language Accept-Language Connection: keep	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. 01 Protocol, Src Por er Protocol ssa5721057129547823. 4.132\r\n illa/5.0 (Windows NT ml,application/xhtml : en-US,en;q=0.5\r\n p-alive\r\n	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44 pkt HTTP/1.1\r\n 10.0; Win64; x64; rv +xml,application/xml; r\n</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko q=0.9,*/*;q=	;) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390 /20100101 Firefox/55.0\r\n 0.8\r\n
> F > E > T > S	rame 798: 444 byte thernet II, Src: 1 nternet Protocol 1 ransmission Contrr ecure Sockets Lay ypertext Transfer GET /99037582133 Host: 172.16.11 User-Agent: Host Accept: text/hts Accept-Language Accept-Encoding: Connection: keep Upgrade-Insecure	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol 8585721057129547823. 4.132\r\n 111a/S.0 (Windows NT al,application/xhtel : en-US,en;q=0.5\r\n : gzip, deflate, br\ o-alive\r\n e-Requests: 1\r\n	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. t: 2499, Dst Port: 44 pkt HTTP/1.1\r\n 10.0; Win64; x64; rv +xml,application/xml; r\n</pre>	d (3552 bits Vmmare_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko q=0.9,*/*;q=	:) id:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390 ./20100101 Firefox/55.0\r\n 0.8\r\n
F E T S S	rame 798: 444 byte thernet II, Src: 1 nternet Protocol 1 ransmission Contre cure Sockets Lay ypertext Transfer GET /99837582133 Host: 172.16.114 User-Agent: Mozi Accept: text/htm Accept: text/htm Accept: text/htm Accept-Language Accept: Lext/htm Accept-Encoding Connection: keep Upgrade-Insecure \r\m	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Por er Protocol S585721057129547823. 4.132\r\n illa/5.0 (Windows NT al,application/xhtml : en-US,en;q=0.5\r\n : gzip, deflate, br\ o-alive\r\n e-Requests: 1\r\n	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. 't: 2499, Dst Port: 44 pkt HTTP/1.1\r\n '10.0; Win64; x64; rv +xml,application/xml; r\n</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko q=0.9,*/*;q=	:) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390 //20100101 Firefox/55.0\r\n 0.8\r\n
> FE > IT > S	rame 798: 444 byte thernet II, Src: 1 rensmission Contre ccure Sockets Lay ypertext Transfer GET /99837582133 Host: 172.16.114 User-Agent: Hozi Accept: text/ht Accept: text/ht Accept-Language Accept-Encoding Connection: keeg Upgrade-Insecure \r\n [Full request U	es on wire (3552 bit Vmware_6a:23:5e (00: Version 4, Src: 172. ol Protocol, Src Pore er Protocol SSB5721057129547823. 4.132\r\n illa/5.0 (Windows NT illa/5.0 (Windows NT il,application/xhtml : en-US,enjq=0.5\r\n : gzip, deflate, br\ o-alive\r\n e-Requests: 1\r\n RI: https://172.16.1	<pre>:s), 444 bytes capture @c:29:6a:23:5e), Dst: 16.114.134, Dst: 172. 't: 2499, Dst Port: 44 pkt HTTP/1.1\r\n ' 10.0; Win64; x64; rv +xml,application/xml; 'r\n 14.132/99037582138565</pre>	d (3552 bits Vmware_d6:3 16.114.132 3, Seq: 262, :55.0) Gecko q=0.9,*/*;q= 721057129547	:) d:7c (00:0c:29:d6:3d:7c) . Ack: 1629, Len: 390 //20100101 Firefox/55.0\r\n 0.8\r\n



```
GET /99037582138585721057129547823.pkt HTTP/1.1
Host: 172.16.114.132
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
HTTP/1.1 200 OK
Date: Tue, 12 Sep 2017 03:32:08 GMT
Server: Apache/2.4.27 (Debian)
Last-Modified: Tue, 12 Sep 2017 03:30:18 GMT
ETag: "0-558f5a993e8bf"
Accept-Ranges: bytes
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
GET /favicon.ico HTTP/1.1
Host: 172.16.114.132
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
HTTP/1.1 404 Not Found
Date: Tue, 12 Sep 2017 03:32:08 GMT
Server: Apache/2.4.27 (Debian)
Content-Length: 290
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=iso-8859-1
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
The requested URL /favicon.ico was not found on this server.
<hr>>
<address>Apache/2.4.27 (Debian) Server at 172.16.114.132 Port 443</address>
</body></html>
```

Http Stream Image

A file in pcap (99037582138585721057129547823.pkt) drew our attention thus we downloaded it from the server.



We have seen a programming language file called Dyalog. After some further research, we found a packet tracer file, downloaded the program and opened the 99037582138585721057129547823.pkt file.



After examining the router, we exported the Startup config file from the Config section.

```
ARKAKAPI Esra Nur Soylu • Siber Yıldız 2019 Writeup
```

```
1
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
1
hostname Router
1
no logging console
1
1
1
1
I
1
1
ip cef
no ipv6 cef
l
1
1
username usom password 7 0200085A0C5C022519061B49100317193C2439386D
1
I
1
Type 7 Password: 0200085A0C5C022519061B49100317193C2439386D
 Crack Password
Plain text: flag:md5(r0uterP@ss)
```

When we gave it to Cisco Password Cracker (Type 7), we got r0uterP@ss

Question: Password of OBELIX (OBURIX'in şifresi)

ΑЯΚΑΚΑΡΙ

OBURIX'in şifresi Toplam Puan: 200	Göreve Başla			
GOREV KODU				
				KODU GÖNDER

Again, it made us download a pcap file.

	bex					
No.	Time 141 23.169022 142 23.169078 146 23.251235 149 23.276221	Source LgElectr_01:94:84 (_ localhost () LgElectr_01:94:84 (_ LgElectr_01:94:84 (_	Destration localhost () LgElectr_61:94:64 (localhost () localhost ()	Protocol OBEX OBEX OBEX OBEX	Length Wo 26 Rcvd Connect 25 Sent Success 36 Rcvd OBEX fragment 316 Rcvd OBEX fragment	
	122 23, 355229 155 23, 355229 156 23, 202485 156 27, 153897 166 27, 153897 166 27, 153951 187 27, 159517 189 27, 257529 199 27, 267795	LgLiett & 1/84/84 LgLiett & 1/84/84 LgLiett & 1/84/84 LgFlectr & 1/84/84 LgElectr & 1/84/84 LgElectr & 1/84/84 Localhost () LgElectr & 1/84/84 Localhost ()	localbost () localbost () localbost () localbost () localbost () lgElectr_01:34:84 (_ localbost () LgElectr_01:34:64 (_	OVEX ODEX OBEX OBEX ODEX ODEX ODEX	316 Revel COEX fragment 316 Revel OBEX fragment 367 Revel Put continue "usom.png" (PWS) 16 Semt Continue 25 Revel Put final 16 Semt Success 22 Revel Ulsconnect 16 Semt Success	
	Arrival Time: Se [Time shift for Epoch Time: 1505 [Time delta from Time delta from Time since refe Frame Lemath: 31 Capture Length: [Frame Langth: [Frame is infore Point-to-Point 0 [Protocol in fr	p 13, 2017 88:27:43.13; this packet: 0.00000001 080603.12202000 secon: previous captured fran previous displayed france: rence or first frame: 2 2 6 bytes (2528 bits) 326 bytes (2528 bits) 10 False] 40 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 False] 41 F	1922000 EDT 10 seconds] 16 19 099409000 second 19 335029000 seconds] 19 054 BC 191220001110	is] uis]	ex: fata 24.	
- R 000	0 02 00 11 17 01 4 c0 a8 f9 a4	de 74 d5 Bc 6c 60 46 1 f3 bc 25 72 c8 2a e4	Of 24 c1 d07 B3 8f 7d f8 J	11.F. .8 r.1.	4	

I reviewed the pcap and the word *obex* caught my eye due to its resemblence to the with the question; thus I started by writing *obex* into to filtering section.

4 U:	iom1.pcap					
File	Edit View Go Ca	pture Analyze Statistics	Telephony Wireless To	iols Help		
41	I 🖉 🕘 📔 🎗	2 9 + + H T :	1 = a a a a	12		
II po	d .					
No.	Time	Source	Destination.	Protocol	Length brio	
·	156 23.418651	LgElectr_61:94:84	(. localhost ()	OBEX	307 Rcvd Put continue "usom.png" (PNG)	



	ST GROOT ST			
and a				GIC - Hermony
Tere	Storue	fertilister.	Tracal und the	
199 27,419031	Lightheory of Swiths (-	tocethoed (1	range yan wund and contraine inner bell (uwn)	
	Collacte Subtrees	Shift-Right Shift-Seft		
	Expend A3 Column A1	Chi+Tupit Chi+Inft		
	Apply as Column	Or-Skit-F		
	Apply million Descent a Triber	1		
Historth History	Centerubon filter			
Blastooth HCL	Calcium with Filter Tollow	1		
Blastooth RFCO	Cepy			
 IProfile: 0 	Show Rectary Bytes	CRI-SBR+O CRI-SBR+O		
D 15 OREX Frei	Well Pressoul Page		152(590), #155(590), #156(292)]	
.000 0010 -	Riter Ford Parleners of Pertoxol Parlenerson			
WITE THE PARTY	Character Sec.			

We see Bluetooth traffic after examining the pcap file. After investigating further, usom.png caught our eye so we tried to download with binwalk. However, the file got downloaded corrupt, so while looking for other download alternatives, we wrote png into the filter part and tried to download directly from the pcap file.

Right-clicking and downloading from the Export Packet Bytes option, the image told us the flag:

K0JwaTdxRUoydk9Ea3VpTW8rRVM1UT09

Question: There is a beholder, and a sought-after (Bir bakan var, bir de aranan)

At the start of the quest, we were faced with the following hash value: "0827206450376af3dce61d788dde-ba21f58dba35257fdb43c1872c096a36287f"



LeoncioBecerraMacavei

The malware tries to retrieve this file from a server:

http://85.111.95.19/a5d8bccb8e1255fc72340eddab8be601-mobile01/cyb3rStar.zip (Pass: Cyberstar_2018!.)

We saw a comment when we searched this hash value with VirusTotal:

ARKAKAPI



When we downloaded and opened the zipped file, a file called puzzles.apk appeared.

		cyb3rStar puzzles	puzzles				
riş Paylaş	Görünüm						
↑ 📑 > pu	↑ 📑 > puzzles						
	Ad	Değiş	tirme tarihi T	ür	Boyut		
işim	assets	5.02.2	019 11:55 D	osya klasörü			
ler 🖈	lib	5.02.2	019 11:55 D	osya klasörü			
lenler 🖈	META-INF	5.02.2	.019 11:55 D	osya klasörü			
nler 🖈	res	5.02.2	.019 11:55 D	osya klasörü			
güzel-uzun	AndroidManifest	5.02.2	.019 11:55 X	ML Belgesi	17 KB		
3irim (D:)	📄 classes.dex	5.02.2	.019 11:55 D	EX Dosyası	2.450 KB		
dasör	resources.arsc	5.02.2	.019 11:55 A	RSC Dosyası	535 KB		

After changing the file's extension to .zip, we saw files inside, and inside /res/drawable, there were some image files.

DECIMAL	HEXADECIMAL	DESCRIPTION
9	0x0	JPEG image data, JFIF standard 1.01
115805	0x1C45D	Zip archive data, at least v2.0 to extract, name:
gizlidosya/		
115878	0x1C4A6	Zip archive data, at least v2.0 to extract, uncomp
ressed size:	7620, name: gi	zlidosya/thankyoucyberstar.gif
123023	0x1E08F	Zip archive data, at least v2.0 to extract, uncomp
ressed size:	7620, name: gi	zlidosya/thankyoucyberstar_1.gif
130170	0x1FC7A	Zip archive data, at least v2.0 to extract, uncomp
ressed size:	7620, name: gi	zlidosya/thankyoucyberstar_2.gif
137317	0x21865	Zip archive data, at least v2.0 to extract, uncomp
ressed size:	7620, name: gi	zlidosya/thankyoucyberstar_3.gif
144464	0x23450	Zip archive data, at least v2.0 to extract, uncomp
ressed size:	7620, name: gi	zlidosya/thankyoucyberstar_4.gif
151611	0x2503B	Zip archive data, at least v2.0 to extract, uncom
ressed size:	7620, name: gi	zlidosya/thankyoucyberstar_5.gif
158758	0x26C26	Zip archive data, at least v2.0 to extract, uncomp
cessed size:	7620. name: qi	zlidosva/thankvoucyberstar 6.gif

When we looked through it with binwalk, there was the "thankyoucyberstar.gif" content that we see on most pictures.

DECIMAL	HEXADECIMAL	DESCRIPTION
0 30 directory: 8	0x0 0x1E	JPEG image data, JFIF standard 1.01 TIFF image data, big-endian, offset of first image
145579 gizlidosya/	0x238AB	Zip archive data, at least v1.0 to extract, name:
145648 ct, compressec ul.b64	0x238F0 J size: 1342466,	Zip archive data, encrypted at least v2.0 to extra uncompressed size: 2100998, name: gizlidosya/hadib
1488383	0x16B5FF	End of Zip archive, footer length: 22

Yet, there was a zipped file in the ortakoy.jpg. When we tried to extract it, we saw that it was ciphered.

Görünen yol buraya kadar, Ama gitmen lazım ileri. Vakitler az, vakitler dar, Buraya gelmişsin, dönme geri.



Meaning:

The path seen is only up to here, But you need to go further. Little is time, You've come up to here, do not turn back.

: (Binary data 68 bytes,
: AMP COLE 5.5.0 · _2ufb15%T7P2mCv0U2 <p< td=""></p<>
: 1360x575
: 0.782

The password of the zip file was found after looking into *sairnedemis.png* with ExifTool. When we opened the file, we found the hadibul.b64 file and the flag was found when we ran the apk file.

Question: Ad breaks have ended, the movie's starting. (Reklam arası bitti film başlıyor.)

Reklam arası bitti film başlıyor Toplam Puan:200 <u>Come Hasa</u>	
GÓREV KODU	
	кори обнося

We were given the dump.scm file at the beginning. To open the .scm file, when we did a search on google, we found and downloaded the appropriate editor and opened the file.
😰 dump (1).scm - Cha	innel Lis	t PC Editor							
File Edit Hel	lp								
Air		Cable	e		Satellite			отн	2012-01
Channel Category			5	0	× 12			4 5	
Y All									
Turksat 42E				Number	Name	My Favourites Locked	Satellite	Provider	Frequ
> TV				312	USOM T	♥1	Turksat 42E	TURKSAT	126
> Radio				1	TRT1 HD		Turksat 42E	TRT	110
> Data/Other				2	ATV HD		Turksat 42E	TURKUVAZ	120
				3	A2		Turksat 42E	TURKUVAZ	120
My Favourites				4	KANAL		Turksat 42E	DOGAN TV	122
				5	STAR T		Turksat 42E	DOGUS	120
				6	SHOW HD		Turksat 42E	CINER ME	122
		k		7	SHOW		Turksat 42E	SHOW MAX	110
				8	FOX HD		Turksat 42E	FOX	123
				9	TV8 HD		Turksat 42E	TV8	123
				10	TV8 5		Turksat 42E	TV8 5	123
				11	KANAL		Turksat 42E	KANAL 7	121
				12	teve2 HD		Turksat 42E	DOGAN TV	122
				13	FIL TV		Turksat 42E	Platformturk	117
nannels in list: 583 0 channels selected Swap Mode									

USOM TV came up. Opening this up with the editor, it gave us a scene from the Interstellar movie. While being so tired, it was so nice watching a scene from a movie I adore :)

There were morse codes on a scene, so we grabbed a paper and a pen and started to take notes, but that was a waste of effort.

There was a sizzling corruption later in the video, so we decided to investigate the voice file using a powerful forensic tool namely Audacity.

In Audacity, we clicked *live* on the left, then *split* and started to examine the corrupt part. The flag was the md5 encoded version of *iyikivarsineren* - the result we obtained from the previous actions.



Question: QR Code Reader (Karekod Okuyucu)

There was a login screen on the page and a part where the users were listed. When we tried to take a look at the users, we got the "sadece yöneticinin QR Kodu kabul edilir" (only the QR code of the admin is allowed) message. Therefore I quickly generated a QR Code and embedded an SQL Injection as text, saved as png and it worked when I uploaded it to the website.



We got the following sentence:

1 admin 6b71dfdc4c5603272482f5b80db96a0a 5e14ce1f1fa3524ba07cb109549c594e

After decoding with md5, we saw that the password was admin1234567890. Logging in again as admin with this password, we got the flag.

Question: Do you like Kahramanmaraş ice cream? (Kahramanmaraş dondurması sever misin?)

P.S.: Kahramanmaraş ice cream is a renowned ice cream known especially by staying hard/rigid for a long time.

There was a game. When the game was over, we got directed to this URL:

yenibasliyor.php?r=6FAD329DF3870D30696C93460EBB7C29_498D3C6BFA033F6DC1BE4FC-C3C370AA7_

348DF46154717306D71E71C277E71082_

What came to our attention when playing the game is that we did not always have the control. If we tried to die intentionally, the game took over and made us not get killed. Thinking that there was something fishy with this, we took a look at the URL and the source code.



state success a second state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state state s
L Potab
and a function of the second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second s
titisooyun Tahani (/titiso
cntyle>* (pedding: 0; margin: 0;) canvas (background: #eee; display: block; margin: 0 sute;)//style>
4 Cinab
II dotta
13 ocanvas libvingCanvas' wighter 320 sc/canvas
<pre>10 cicript.type="test/javascript".nue="geme/04.js"></pre>
II a service and a filmed and the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the service of the se
CI Summer , Summer ,
at 'mminutat's 'mpiy's
15 Section Generalized Sec
The second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second secon
TEL Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control of Control
23 'error', 'error',
24 Summity they's
25 "optilementByIO",
1.2.2. "Physicanomy", "Restances," We With State of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Constant of the Const
23 Settion a same a
23 Vicinitian',
31. Specification interaction account of the second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second second sec
32. PeeginWath(, 'arts')
JI ************************************
Ta transfer harden h
 transf, "Ispa azial".
in 'fillfear's 'nomen 's
JT "Electrect", "Laws GEST,
TD failureaf
4.0 B.
11 0 thurstion (_1x5725kc, _0x27c087) (
The callentic function (0.15407) (
Series (OKIMETA) (
AND ADDRESS TO ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS

There were so many hex expressions, all written in a script. When we converted from Hex to ASCII, we obtained a base64 encoded expression and after decoding it we were left with a text. Because it would be very difficult to convert them one by one, we wrote a script and by doing so, we got the source code.

Found : **baglanti**

(hash = 6fad329df3870d30696c93460ebb7c29)

2

Found : **son**

(hash = 498d3c6bfa033f6dc1be4fcc3c370aa7)

6

Found : lekle

(hash = 348df46154717306d71e71c277e71082)

We saw 3 md5 encoded texts in the URL section and decoded them. Later, we got:

yenibasliyor.php?r=6FAD329DF3870D30696C93460EBB7C29_

498D3C6BFA033F6DC1BE4FCC3C370AA7_348DF46154717306D71E71C277E71082_C4CA4238A0B-923820DCC509A6F75849B

When we added the md5 encoded version of 1 (C4CA4238A0B923820DCC509A6F75849B) at the end of the URL.

Esra Nur Soylu • Siber Yıldız 2019 Writeup

\leftrightarrow \rightarrow \sim Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/yer
Ваугаğı Кар
↔ C () Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi1.php
Hadi bakalım.
← → C
sonu yok bu gidisin
← → C ③ Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi3.php
bence vazgec
$\leftarrow \rightarrow C$ (i) Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi4.php
somma kadar ilarlavabilirim 2
sonuna kauar heneyeonninn ?
← → C ③ Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi5.php
vakit varken bırak bu işleri
G ③ Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi6.php
benim limitim max url karakter sayısı kadar !
← → C () Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi7.php
pof, senle ugrasmak zaman kaybi.
← → C (Güvenli değil 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi8.php
404 Not Found



← → C () Güvenli değil | 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/simdibasladi9.php

Buradan devam et.

2

← → C ③ Güvenli değil | 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/yenibasliyor.php?r=6FAD329I

Bayrağı Kap



← → C () Güvenli değil | 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/gercektenbasladi.php

Web Uygulamalari

- Gizli Portal
- <u>Sistem Yonetim Arayuzu</u>

b ← → C O Güvenli değil | 85.111.95.22/c98/16450d4754cd6fde30be9d0cfe84-mix03/bu_cok_gizli_bir_portal/index.php

bu portal sevdiginiz dondurmalar hakkinda bilgi vermek amacli kurulmustur.



, ← → C () Güvenli değil | 85.111.95.22/c98f16450d4754cd6fde30be9d0cfe84-mix03/akillidusun.php

ΑЯКАКАРІ



After wandering through the pages, we found somewhere we could execute commands.

There was a textbook, and we could run *ls*. Looking through with ls /tmp, we saw *flag* and *ozel/ (special)* files. Just as we got excited, thinking we got so close, cat /tmp/flag did not make us read the file: only a response which said that the file could be read. We could not even execute ls /tmp. Unfortunately, without being able to finish this question, we ran out of time

A Security Guide for Your Android Device

he Android operating system, supported by Google; is an operating system used in many different devices, from mobile phones to televisions to tablets.

The instructions stated below may vary depending on the type of device used.

Minimize the data Google collects

On most Android devices, it is not mandatory for you to sign in to your Google account. It is possible to skip this option you'll see during installation. Yet, this may result in limited use of certain services. Besides, you can also edit your Google activity profile via https://myactivity.google.com/myactivity, determine which data is stored, or delete your activity data.

Set a PIN to your device

To protect your device, set a pin or an alphanumeric password.

To set a PIN/Password go to Settings > Security > Screen lock



Encrypt Your Device to Protect Your Data

Differing from PIN/Password, you can encrypt the data inside your device with this setting. In order to do so, you first need to activate the PIN or Password and enter this information at each unlock. Since the encryption process wastes energy intensely, it is recommended you connect the device to the charger. In order to encrypt your device, you can also use the *Settings > Security > Encrypt phone/tablet* menu.

P.S. After encryption, it would not be possible to decrypt your data if you forget the PIN/Password. In this case, you can use the *return to factory settings* option but this will end up with all your data being deleted.

🗐 🖓 🗢 🔿 17:48	🖬 🛛 🖗 🖓 🛜 🔿 21:21	🗳 🗘 🗟 21:23
🔅 Settings	(😂 Security	C 🔅 Encrypt phone
	SCREEN SECURITY	
More	Screen lock None	You can encrypt your accounts, settings, downloaded apps and their data, media and other files. Once you encrypt your
PERSONAL	Owner info	phone, you need to type a
😕 Profiles 🛛 OFF	ENCRYPTION	numeric PIN or password to decrypt it each time you switch it on. You can't decrypt your
Cocation OFF	Encrypt phone	phone except by performing a
Security	Require a numerical PIN or password to decrypt your phone each time that you turn it on	your data.
O Privacy	PASSWORDS	Encryption takes an hour or more. You must start with a
👗 Language & input	Make passwords visible	charged battery and keep your phone plugged in until
Backup & reset	DEVICE ADMINISTRATION	
ACCOUNTS	Device administrators	Encrypt phone

Keep your device and applications up to date

We also recommend you to keep all your devices' operating system and applications up to date, not only for Android devices. You can use the Settings > About phone/tablet > System Update menu settings for updating the device.





Do not download applications from untrusted sources

Do not download applications from untrusted, unknown sources. You can arrange the settings so that only applications which are from trusted sources are downloaded. To enable this feature, disable the setting at *Settings* > *Security* > *Unknown sources*.





Review the application permissions

Definitely look over the permissions the application asks for during installation. Does the application require authorization other than its aim? For instance, does the application demand permissions to the microphone, camera, speakers or other sensors even though it has nothing to do with them?

Check the permissions of all applications including the old ones. If an app is granted excess permissions, question why and uninstall if necessary. Some apps may have requested extra permissions during an update, you may have missed some permissions or there may be an app you no longer use. You may change an app you already use for another which does the same thing but requires fewer permissions.



Arka Kapi ARKAKAPI



Decide and review which data should be backed up in the cloud

Not synchronizing the applications restricts the data sent to cloud servers like Google Drive. For example, WhatsApp backs up the data to the Google Drive <u>unencrypted</u> even though it is an application which encrypts the data with end-to-end encryption by default. Review such synchronization settings - you can use the options found in *Settings* > *Accounts section* > [app name].

Hide personal notifications

Your phone is locked but is an incoming notification reveals who you are chatting with? Is the caller information seen although the PIN is active? If so, it is time to review the notification settings; you can prevent the data from being seen when the screen is locked (only viable for newer versions).

Settings > Sound & notification







Review the default applications

Which application does your device use by default for sending a text message? Or when you click a link, which web browser will display the website by default? Review such default application settings. You can change the default applications with trusted applications.

 $Settings > Apps > \Box$ icon > Default



Do not share your location with the apps!

Control which applications can access your location information.

Settings > *Apps* > \Box *icon* > *App permissions* > *Location*

6 0	"≱r Q 5:08	00	2 🛙 5:09	≝ ● ¹ 2/ D 5:04		j 2/0 st
Settings	٩	÷	Apps 🗘 🌣 🗄	← Configure apps	4	App permissions
Device			Android Keyboard (AOSP) 140 KB	App permissions	*	Body Sensors 0 of 0 apps allowed
Display		lia:	API Demos 4.96 MB	App links		Calendar 3 of 4 apps allowed
Sound & notific	ation	0	Browser 0.00 B	Advanced Default Apps	0	Camera 2 of 6 apps allowed
Apps		100	Calculator	Draw over other apps		Contacts
Storage & USB		89	0.00 B	Modify system settings		6 of 12 apps allowed
	5	120	Calendar 36.00 Kil	Battery optimization	0	Location 4 of 9 apps allowed
Battery			Camera			Microphone
Memory			6.00.6			a tot to appear assound

Arka Kapı ARKAKAPI

Do not share your location information with Google

In the step above, we have determined whether the applications will access our location information or not. These applications/services include Google. ADINT, a research made by the University of Washington reveals how you can watch someone step by step using mobile advertisements with a budget of approximately a thousand dollars¹. You can prevent this by inhibiting the applications from accessing your location information. With the following menu options you can check whether your applications can access your location:

Settings > *Location* > *Google Location History*

		🖫 🚨 5:37
Sett	ings	٩
8	Memory	
Perso	nal	
•	Location	
ê	Security	
8	Accounts	
G	Google	
		-



You can install a custom Android version on your device

You can install a custom Android version such as CyanogenMod based LineageOS etc. However, technical information is required for this process. Please note that after installation, your device may no longer be covered by the warranty.

You may use DuckDuckgo or Startpage as default browser

You can use DuckDuckgo or Startpage as the default browsers. They are browsers which do not store your search history and care for your privacy.

Reset MAID (Mobile Advertising ID)

MAID is a cookie-like value uniquely assigned to devices, used in ad tracking. In mobile advertising, ads can be targeted using MAID. For instance, ads can be set so that only those with a specific MAID value can see it. The ad display information, date and time can be correlated with the location information and your location can be found. You can be watched step by step.

Reset the MAID value by clicking *Google Settings > Ads > Reset advertising ID*

P.S. Android Privacy Tips blog post published by DuckDuckGo has been utilized.

Source: https://spreadprivacy.com/android-privacy-tips/

1 https://adint.cs.washington.edu/

Signal Intelligence Signal Listening and Analysis Methods

Today, when wireless communication takes up every aspect of our lives, the signals emitted by many devices surround us. Radios, mobile phones, wireless modems, Bluetooth devices, communication satellites, GPS satellites, and many other devices are continually emitting signals at different frequencies. It is possible to listen, analyze and even decode these signals with the necessary hardware and software.

ARKAKAPI

With the help of computers, much different hardware can be used to listen for signals. The equipment is available in many different options, from professional equipment to mini USB devices. Using the Realtek RT-L2823U chipset, the RTL-SDR hardware is one of the most inexpensive and efficient hardware solutions with a price of \$ 20. This equipment is commercially available to monitor terrestrial TV broadcasts via computers and can operate at all frequencies between 24 and 1766 Mhz. With this feature, in addition to terrestrial TV broadcasts, FM-AM can listen to radio channels, police, lifeguards, firefighters, coast guard radios, amateur radio frequencies, GSM signals, and many satellite signals.

To benefit from this equipment efficiently, the antenna must be suitable for the data to be received. The RTL-SDR equipment can only listen to a signal, not to transmit signals. More expensive alternative equipment such as HackRF and BladeRF can perform both receive (Rx) and send (Tx) operations.



(RTL-SDR Hardware Images)

AAKAKAPI

Some of the things that can be done with RTL-SDR Hardware

- Police, ambulance, fire radio, and EMS communication can be heard (legally public frequencies)
- Air traffic control conversations can be listened to.

- The locations, speeds and direction information (ACARS) of the aircraft in the air can be heard and displayed on the map.

- By listening to sea traffic, the ship name information, direction, and location information can be processed on the map.

- Amateur radio speakers can be listened to.
- Digital audio communication can be heard and decrypted. (DMR digital radios)
- Wireless security camera, baby monitor, Bluetooth devices such as signals can be monitored.
- POCSAG / FLEX Pager systems can be displayed and displayed as text.
- Satellite imagery and weather information can be obtained from meteorology satellites. (NOAA Satellites)
- Analog terrestrial TV broadcasts can be viewed.
- FM and AM radio channels can be played back.
- GSM signals can be rested and analyzed.
- RF signals can be rested and analyzed.

Listening of signals with software

RTL-SDR hardware can run on all operating systems. SDRSharp or Gqrx software can be used to listen to signals simply. The most widely used Gqrx software for Linux and MacOS operating systems. When the desired frequency is reached, listening can be performed if there is an audio communication or Gqrx can be converted to a UDP server and the data of the given frequency can be shared with other applications via the UDP port.



(Gqrx Software Image)



Listening to Police Radios

Some radio frequencies used by traffic or public order policemen broadcast publicly, and listening to them is not a legal offense. In general, journalists listen to these frequencies and know about crimes such as traffic accidents or theft. Police radio frequencies can be found on the internet.



(Gqrx Police Radios image)

Listening to Digital Radios

Police, fire brigades, ambulances or even security guards in shopping malls have now started to use digital radios due to security and other issues. However, these digital conversations called DMR can be decoded with some software.

			CONTRACTOR DE LA CALLARIA			-
Die Tech	Oferen Made		CONTRACTOR OF			
Line Jocca	the life and	an a'				
		<u>x_</u>			11	
	42212	6 100 MHz	11 H. H. H. H	140.4	Receiver Options	No. No. No. of Concession, Name
	TEELLE	0 100	aters .		450.6	00.00
					runness herr	\$21.675500 PB Q
					Filter width User (29.8 41 +
					Titler shape. Norma	C 24
12	a second of the				Mode Nation	effit + -
Approval	an appendice of the Area and Area and Area and Area and Area and Area and Area and Area and Area and Area and A	a there are made	down which have been a set	5 desperson	AGC Fed	100
					Squette -50	A MPS 2 A
					Noise barner 1452	N82
	10 +1115	4.12.19	4115	472.0	Contraction of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the local division of the loc	Contraction in the second
BEATTERN		The second second			Toput L. Receiu	er_ UNISL
					Audo	100
					Audo Anto	
			night -		Auto Contra	
Fie fot two	Search Terring Here and SFSK Intel	15 (9400) 1041			Audo Control	
Fig. bot toos Spec 1000	Search Terroral Inc.	Dis (SLOTE) start	Terigitat -		Auto	
File fort Vere Sync: - 4048 Sync: - 4048 Sync: - 4048	Learn Termina Junp and GFSK Intv11 and CAPH Intv11 and CAPH Intv11 and CAPH Intv11	125 (SLOTE) slor1 116 (SLOTE) slor1 116 (SLOTE) slor1 116 (SLOTE) slor1	Heights -		Auto	
Fie fort wee Sync: 40HR Sync: 40HR Sync: 40HR Sync: 40HR	Learn Termin Jury and SFSK IntV1 word CETH IntV1 word CFSK IntV1 word CFSK IntV1 word CFSK IntV1	126 (9.076) sleri 116 (9.076) sleri 116 (9.076) sleri 116 (9.076) sleri 116 (9.076) sleri 116 (9.076) sleri				
Fie Ant Vee Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048	Meetin terminal leng and SFSK intv1 mod: CETM intv1 mod: CETM intv1 mod: CETM intv1 mod: CETM intv1 mod: CETM intv1 mod: CETM intv1	126 (9.676) sheri 116 (9.676) sheri 116 (9.676) sheri 116 (9.676) sheri 116 (9.676) sheri 126 (9.676) sheri 126 (9.676) sheri 126 (9.676) sheri	VOICE -			
Fire Dath Verse Synta ADHE Synta ADHE Synta ADHE Synta ADHE Synta ADHE Synta ADHE Synta ADHE Synta ADHE Synta ADHE	Seven hereina long and SFix Intvi est SFix Intvi est SFix Intvi est SFix Intvi est SFix Intvi est SFix Intvi est SFix Intvi est SFix Intvi	125 (9.076) 11041 115 (9.076) 11041 115 (9.076) 11041 115 (9.076) 11041 115 (9.076) 11041 105 (9.076) 11041 115 (9.076) 11041 115 (9.076) 11041 115 (9.076) 11041				8
Tie fet vee Sync stille Sync stille Sync stille Sync stille Sync stille Sync stille Sync stille Sync stille	Level: Personal Jung and SPSK Intvil end 2478 (allvil end 2478 (allvil) end 2478 (allvil) end 2478 (allvil) end 2478 (allvil) end 2478 (allvil) end 2478 (allvil) end 2478 (allvil)	120 (9.076) (1001) 130 (9.076) (1001) 134 (9.076) (1001) 134 (9.076) (1001) 134 (9.076) (1001) 135 (9.076) (1001) 135 (9.076) (1001) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.076) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) 135 (9.071) (9.071) (9.071) 135 (9.071) (9.071) (9.071) 135 (9.071) (9.071) (9.071) (9.071) 135 (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071) (9.071	VALUE :			88
Fire Test Value Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M Syntc x04M	Search Permise Jong and SPSK Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi- ent CRM Intivi-	12% (9.070) 11041 11% 9.070) 11041 11% 9.070 11041 11% 9.070 11041 11% 9.070 11041 11% 9.070 1007 11% 9.070 1071 11% 9.070 9.071 11% 9.070 9.071 11% 9.070 9.071	VOICE :			8
File 2014 Nove File 2014 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048 Sync 4048	Jaurin Perman Jang and SFSK Intvi- ed. CAPH (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- ed. CAPK (stvi- str))))))))))))))))))))))))))))))))))))	IA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (4076) theri IIA (40				
The fatt wave Sync alwa Sync alwa Sync elwa Sync Sauch Termina Inag and SFR Influi- nest SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi- est SFR Influi-	124 (9.076) steri 114 (9.076) steri 115 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri 116 (9.076) steri					
Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre Ant Vor Fre A	Least Ferners leng and GFM Inivi- med GFM Inivi- ed GFM Inivi- ed GFM Inivi- ed GFM Inivi- ed GFM Inivi- ed GFM Inivi- ed GFM Inivi- ed GFM Inivi- ed GFM Inivi-	125 (9.078) start 155 (9.078) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) start 155 (9.076) s				8
File Tell Tell Fyric -2004 Syric -2004	Search Personal Jong and SPSK Initial Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalina Book Of Kalin	In Story Steel Starts Story Steel Starts Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story Story S	Telegistic - WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I WHICE I			
First Table Water Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948 Sync 4.0948	Search Termine Image and: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi- ent: SFSK Intivi-	IA (RATE) sheri IA (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RATE) sheri IK (RA				
Ган Тата тана Ган Тата тана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана Ган Салана	Jacob Fernera Jacq and GFM Intvi- med GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi- ed GFM Intvi-	124 (9.078) sileri 114 (9.078) sileri 115 (9.078) sileri 115 (9.078) sileri 116 (9.078) sileri 116 (9.078) sileri 116 (9.078) sileri 116 (9.078) sileri 127 (9.078) sileri 128 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9.078) sileri 129 (9				
Гас. Тот. учис. забия чулс. - 1.0948 - - чулс. - 1.0948 - - чулс. - 1.0948 - - чулс. - 1.0948 - - чулс. - 1.0948 - - чулс. - 1.0948 - - чулс. - 1.0948 - - чулс. - 4.0948 - - чулс.	Search Demma Deg and SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold eff. SFR Infold	12% (9.07%) 11041 13% (9.07%) 11041 13% (9.07%) 11041 13% (9.07%) 11041 13% (9.07%) 11041 13% (9.07%) 11041 13% (9.07%) 11041 13% (9.07%) 11051 13% (9.07%) 11051 13% (9.07%) 11051 13% (9.07%) 11051 13% (9.07%) 11051 13% (9.07%) 11051 13% (9.07%) 11051 13% (9.07%) 11051 14% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 11051 15% (9.07%) 1				8

(Decoding digital radios with Gqrx and other software)

Monitoring and Analysis of Ship Traffic

Each ship over a certain size and carrying passengers uses the AIS (Automatic Identification System) tracking system. VHF is constantly broadcasting at 161.975Mhz and 162.025Mhz channels with GMSK modulation. In these signal broadcasts, information such as the name of the ship, call code, coordinates, route, speed, ship size, destination port and time of arrival are sent. It is not a crime to listen to these signals or to analyze them with the help of computers, but it is forbidden to broadcast on these external frequencies. This field is full of weaknesses because the signals can be manipulated easily, and the radar of a high-tonnage ship can be displayed as if there was another ship with false AIS signals. AISMON and OpenCPN software help to mark the ships on the map with the signals received.



(Vessel traffic listening and analysis image)

Monitoring and Analysis of Air Traffic

All aircraft ready for take-off or active in the air must transmit their information to the stations on the ground via signals. This information includes many data such as speed, altitude, location, destination, and direction of travel, as in marine traffic and is called ADS-B. This data is propagated by a device called the transponder. The 1090Mhz frequency can be listened and analyzed and all the airplanes that were on us at that time can be displayed.





Listening and Analyzing Satellite Signals

Hundreds of different satellites pass through each day, and many of them transmit data to the ground via signals through which they pass. NOAA satellites designed to be used in the meteorological field openly broadcast these signals to the whole world. Many NOAA satellites are continually circulating in different locations in orbit and can be instantly displayed on the internet. Almost all satellites can be displayed at http://www.n2yo.com.

Turnstile, Quadrifilar Helix, V-Dipole or Double Cross type antenna must be used to receive NOAA satellites efficiently. The antenna that comes with the RTL-SDR equipment is not sufficient.









Turnstile

Quadrifilar Helix (QFH)

V-Dipole

Double Cross Antenna (DCA)

When the NOAA-19 satellite passes through, it sends signals at a frequency of 137.100Mhz with SDRSharp software, and the signals are transferred to WXtoImg software and converted into photographs.

Murat Şişman • Signal Intelligence

AAKAKAPI



(Satellite Listening and Analyzing image)

Listening and Analyzing GSM Base Stations

With the RTL-SDR hardware, just like what mobile phones do, GSM signals can be listened to. Each wireless communication system has a standard. The systems used for GSM communication are still ancient and contain many vulnerabilities. By listening to signals easily and analyzing these signals using some software, threats may arise.

Instead of reading conversations or chats in GSM communication, it alone creates a significant vulnerability to listen to the signals and to learn the codes which belong to every mobile phone user called IMSI. Kevin Mitnick, the famous hacker whom dozens of books and films have been dedicated to, managed to escape from the FBI for a long time. Mitnick had acquired the complete IMSI code of the FBI staff by using his social engineering brilliance. He was always listening to the base stations on his computer and checking his IMSI numbers. If the IMSI code of one of the FBI employees entered the base station around him, his computer would give him a warning, and he was able to get away and escape. This method used in the early 1990s can still be used. Mitnick, who listened to GSM signals, also got captured in a similar manner. Tsutomu Shimomura, a computer security expert, set up a counterfeit GSM base station to catch Mitnick, allowing Mitnick to communicate and record all his communications.

When combined with social engineering and GSM weaknesses, open-ended and impossible to prevent threats arise. If the GSM technologies are not overhauled, these vulnerabilities will continue to pose significant threats.

With RTL-SDR and Gr-GSM software, IMSI numbers can be displayed by analyzing the signals from GSM base stations.



(Listening and Analyzing GSM Base Stations - 1)

	root@kali: ~/Desktop/IMSI	• • •
File Edit View Search Terminal He	p	
<pre>root@kali:-/Desktop/IMSI# pythor Nb IMSI ; TMSI-1 ; TMSI-2 2 ; ; ; 3 ; oxb98f97c1; 5 ; ; ; ; 6 ; ; ; ; 7 ; ; ; ; 8 ; ; ; ; 9 ; ; ; ; ; 10 ; ; ; ; ; ; 11 ; ; ; ; ; ; ; ; ;</pre>	<pre>IMSI_yakalama.py ; IMSI ; Ulke ; Marka ; Operator ; MCC ; MNC ; LAC ; 286 02 0325755075 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 0370235819 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 2450086628 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 2312217628 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 055590028 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 055590028 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 0357048449 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 0357048449 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 0357418449 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 0337418449 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 4960228905 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone Turkey ; 286 ; 02 ; 5341 ; 286 02 3650041109 ; Turkey ; Vodafone ; Vodafone ; Vodafone ; Vodafone ;</pre>	; CellId 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151 0 ; 9151

(List of Listening and Analyzing GSM Base Stations - 2)



Do you want your article to be published on Arka Kapi Magazine? Submit now to be featured in the next issue! Your article can be of any title as long as it fits to the cyber security context. Make sure it's an original article that isn't previously published elsewhere.

> Email your articles to: editor@arkakapimag.com



Got any feedback about Arka Kapi Magazine? Found a bug? Want us to add or remove something? Let us know!

follow us

Don't miss the news!

