Hack Teknikleri

Ahmet BERKAY
Gebze Yüksek Teknoloji Enstitüsü
aberkay@bilmuh.gyte.edu.tr

1. Giriş

Hazırlanan bu çalışma sonucunda, özellikle internet kavramının gelişmesi ve yaygınlaşması sonucunda ortaya çıkan bigisayar saldırıların (hack) nasıl yapıldığı ve ne gibi teknikler kullanılarak gerçekleştirildiği açıklanmaya çalışılacaktır. Bu sebepten dolayı bu saldırıları yapan saldırganlar (hacker) ve saldırgan çeşitlerinden de konunun özüne bağlı kalınarak değinilecektir.

Hazırlanan çalışma kapsamında öncelikle *hack*, *hacker* kavramları tanımlanacaktır. Bu tanımlama sonrası hacker'lerin kullandığı ve süreçsel sınıflandırma ile ele alınan temel saldırı teknikleri açıklanarak, bu tekniklerin nasıl yapıldığı konusunda detaylı açıklama yapılacaktır.

Anahtar kelimeler :

Hack, Hacker, Hack Teknikleri, Engelleme, Dinleme, Değiştirme, Oluşturma

2. Önsöz

Bu bölüm altında *hack*, *hacker* gibi kavramlar tanımlanarak bu konunun daha iyi anlaşılabilmesi için çeşitli istatistiksel çalışmalara yer verilecektir.

2.1. Jargon Dosyası

Hacker kavramının çıkış noktası incelendiği zaman ilk olarak Massachusetts Institute of Technology'de (MIT) 1960 yıllarında ortaya çıktığı görülmektedir. Kelime, MIT'de okuyan ve hobi olarak "telefon veya tren yolu model yapımı, amatör radyo yapımı, amatör radyo yayıncılığı" seçtikleri alanları, uç noktalara da "sadece zevk amaçlı olarak" test eden kişiler için kullanılmaktaydı. Yaptıkları bu testlere ise hack etmek anlamına gelen hacking denmekte idi. Mikro bilgisayarlar ve mikro işlemcilerin gelişmesi ve yaygınlaşması sonucu hobi alanları olarak seçilmeye başlanması hack kelimesine günümüzde kullanılan anlamını kazandırmıştır. Hacker ve hacking işlemlerinin kayıtlı hale getirilmesi sonucunda hecker'ler ilk ve en geniş sözlük olan Jargon Dosyası'nı oluşturmuşlardır.

Jargon Dosyası, hacker kültürü içinde yer alan terim, folklor ve gelenekleri anlatan bir tür sözlüktür. Jargon Dosyası'nın ilk versiyonları MIT AI Lab, SAIL (Stanford AI Lab) gibi yerlerde 1975'lerde başlamıştır. Adı da doğal olarak AIWORD.RF idi. Jargon dosyası 2 kez kitap halinde basılmıştır. Bu dosyaya göre hack ve hacker kelimelerinin anlamı aşağıdaki gibidir.

Hack :

Çok geniş anlamda kullanılmaktadır. Jargon dosyasının hack için verdiği tanım:

1. Orijinalinde, gerekeni ortaya çıkaran, ama iyicene yapılmayıp çabuk kotarılmış iş.
2. Tam gerekeni ortaya çıkaran son derece güzel, ve olasılıkla çok zaman yiyen iş.
3. Duygusal ve fiziksel olarak tahammül etmek. *"I can't hack this heat!"*
4. Bir şey (tipik olarak bir program) üzerinde çalışmak. -*"What are you doing?"* - *"I'm hacking TECO."*. Daha genel olarak, *"I hack `foo'"* yaklaşık olarak "`foo' benim esas ilgi alanımdır." cümlesine denktir.
5. Zeka ürünü şaka.
6. Bir bilgisayarla bir hedefe-yönelik olarak değil de oyuncu ve araştırmacı şekilde etkileşmek.
7. "hacker" için bir kısaltma.
8. Bir tür zindan oyunu olan Nethack için kullanılan kısaltma.
9. [MIT] Büyük, kurumsal bir binanın merdivenlerini, çatı kenarlıklarını ve buhar tünellerini, çalışanları ve (genellikle bu eğitim kurumlarında gerçekleştirildiğinden) kampüs polisini tedirgin edecek şekilde araştırmak. Bu faaliyet Dungeons & Dragons ve Zork gibi macera oyunları oynamaya benzer bulunmaktadır.

Hacker :

Orijinal anlamı balta ile mobilya yapan anlamında kullanılmaktadır. Yine Jargon dosyasında göre anlamı:

1. Programlanabilir bir sistemin detaylarını keşfetmekten ve sınırlarını zorlamaktan zevk alan kişi.
2. Büyük bir zevkle hata saplantı olacak şekilde program yazan kişi veya programcılığın teorisinden çok pratiğinden hoşlanan kişi.
3. Hack değerlerini “yarasız amaçlar için denenen programlar” kabul etmiş kişi
4. Hızlı program yapabilen kişi
5. Bir program üzerinde ustalaşmış veya işlerini onun aracılığı ile yada onun üzerinde yapan kişi
6. Bir konu üzerinde uzmanlaşmış kişi yada çok hevesli kişi
7. Entelektüel olarak yaratılan sınırlara yada yaratıcı sınırlara meyden okumayı seven kişi
8. Zaralı amaçlar için hassas bilgileri ele geçirmeye çalışan.

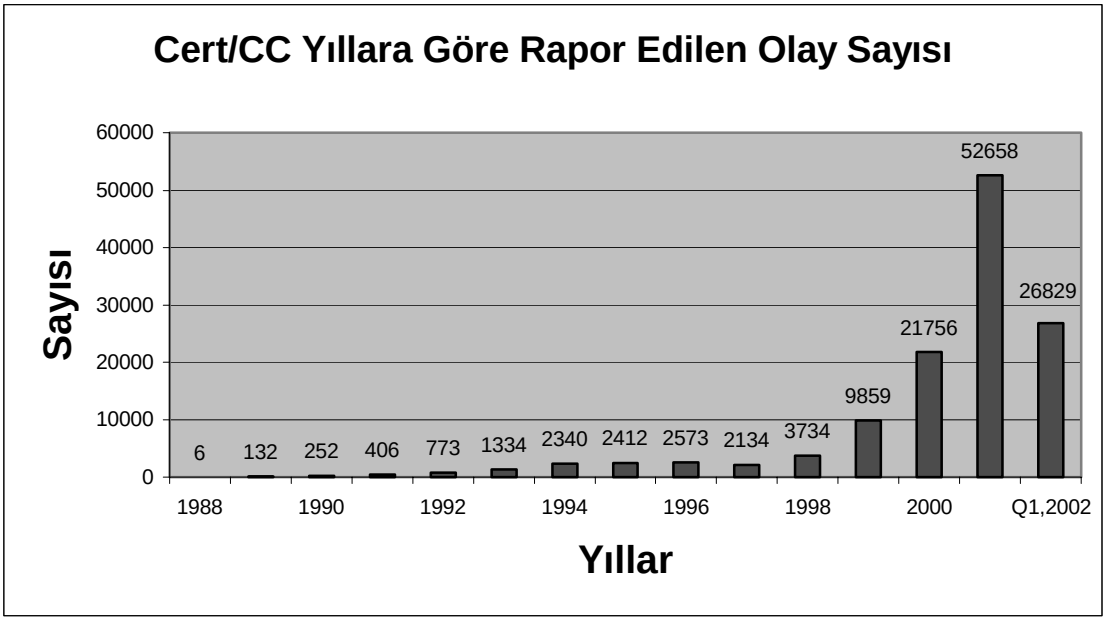
Hack kelimesi ve bunu yapan kişi anlamına gelen hacker kelimesi için tam bir türkçe karşılık bulmak güçtür. Fakat kavramları yaşadığımız toplum içerisinde değerlendirdiğimiz taktirde, bu kavramların çıkışında veya oluşumunda herhangi bir “türkçe içerik oluşturabilecek” katkımız olmadığı için olayı tanıma yada başka bir anlamada popüler hale getiren internete bağlı bilgisayarlara yapılan saldırılar olmuştur. Bu sebepten dolayı hack veya hacker kelimeleri türkçe de bilgisayara saldırı veya saldırgan, bilgisayar korsanı olarak anlam bulmaktadır. Fakat kavramların doğuşu ve orijinal dilinde kullanılan anlamlarına bakılacak olursak türkçedeki kullanımının tam doğru olduğu söylenemez. Bu sebepten dolayı çalışmanın

devamında hack ve/veya hacking, hacker kelimeleri orijinal lisanında kullanıldığı şekilde yazılacaktır.

2.2. Hacking ve Hacker'liğin Gelişimi

Kişisel bilgisayarların zaman içerisinde ucuzlamaları sonucu kullanımlarındaki artışı internet kullanıcılarının sayısını da artırmıştır. Intenet kullanımının artışı internet üzerinde gerçekleşen hacking olaylarının artışını da doğru orantılı olarak artırmıştır (Tablo 2.1.).

Tablo 2-1 Hack Miktarının Yıllara Göre Oranı



Rapor edilen bu hacking olaylarının miktarları dikkatlice incelenecek olursa kaydedilen hack olaylarının belirli periyotlarda anormal artışlar yaptığı gözlenmektedir. Fakat bu artışı hacker sayısındaki bir artmanın sonucu olarak açıklamak doğru olmayacaktır. Bunun sebebi ise dünya üzerinde bulunan hacker'lerin sayısı ve yetenekleri bu artışı sağlayamaz olmasıdır. (Şekil 2.1.).

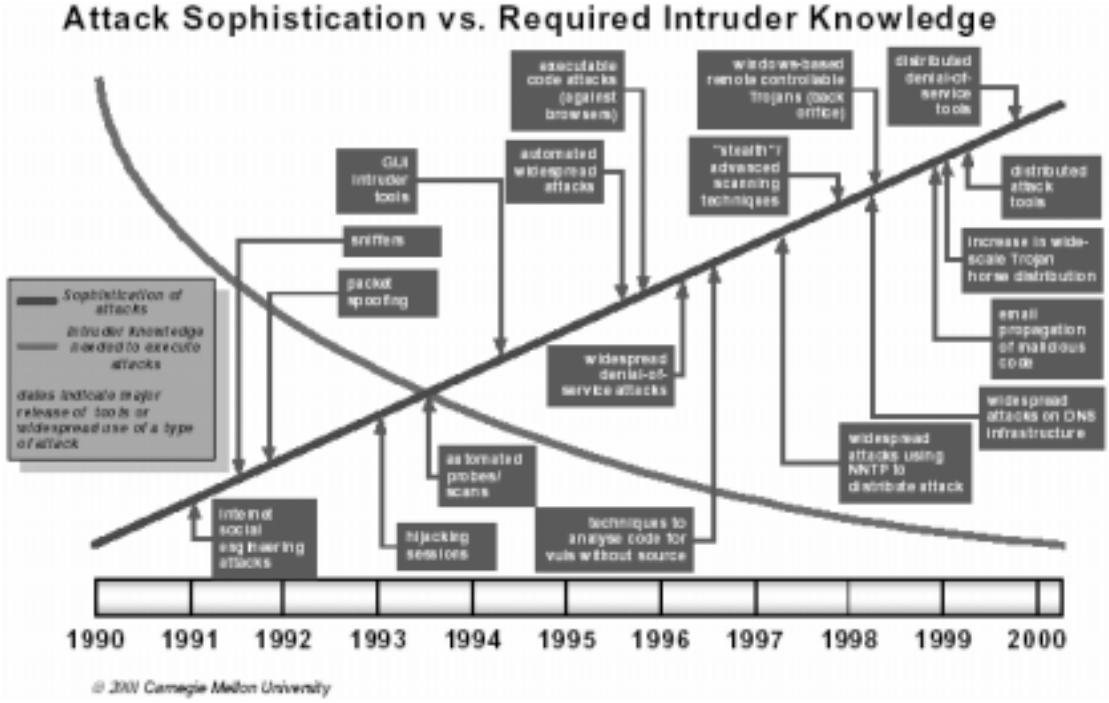
Şekil 2-1 Hacker Kaliteleri Ve Tahmini Sayıları (CERT/CC)

Hack miktarlarının bazı yıllarda gösterdiği büyük altışarların temel sebebi aslıda çok daha tehlikeli ve önlenmesi güç sebepler içermektedir. Bu sebeplerin

başında ise hacking tekniklerinin artık elle yapılmaktan çıkıp tamamen otomatik hale gelmesinden dolayıdır.

Önceleri hack edilecek bilgisayarlar ve o bilgisayar üzerinde çalışan işletim sistemleri, o sitemi ve bilgisayar tiplerini çok iyi tanıyan uzun süre kullanıcısı olan ve bu sistemler hakkında akademik bilgi yanında çok fazla pratik bilgiye sahip olan hacker'ler tarafından satır satır kod yazma "elle" yolu ile hack edilirlerdir. Fakat zaman içerisinde bu yetenekli hacker'ler kendi işlerini kolaylaştırabilmek için elle yaptıkları işlemleri otomatik olarak yapabilen programlar yada program parçaları haline getirdiler. Asıl tehlikede bu noktadan sonra ortaya çıktı. Çünkü bu programlar sayesinde konu ile ilgili çok az hatta hiç bilgiye sahip olmayan kişiler rahatlıkla hacking işlemlerine girişmeye başladırlar. Hacking kalitesi ve hacker yeteneklerinin gelişimi (CERT/CC) hakkında verilen Tablo 2.2. yukarda sözü edilen tehlike ve geliştirilen temel tekniklerin detaylı olarak belirtilmektedir.

Tablo 2-2 Hacking kalitesi ve hacker yeteneklerinin gelişimi (CERT/CC)



3. Bilgilendirme

3.1. Hack Türleri

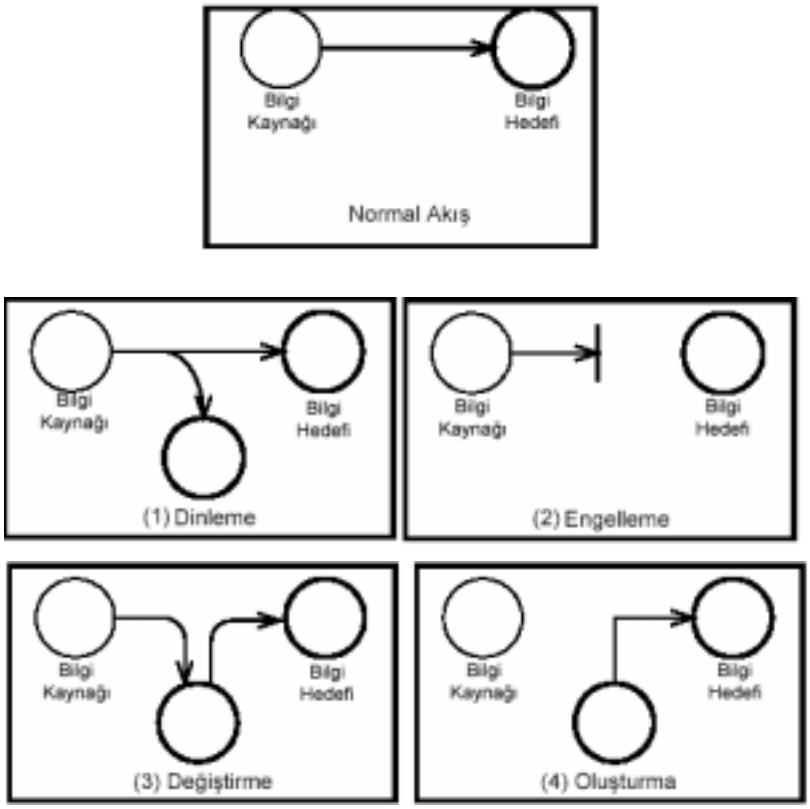
Hack olayının türlerini sınıflandırılmak aslında oldukça güçtür. Bu güçlüğün temel nedeni ise hack türlerinin gerçekte tek başlarına bir hacking tekniği olması yanında birkaç türünün bir araya getirilmesi sonucu yine bir hacking tekniği olmasından kaynaklanmaktadır. Bu sınıflandırma yapılırken Yrd. Doç. Dr. İbrahim Soğukpınar'ın Veri ve Ağ Güvenliği ders notları temel alınmıştır.

Adı geçen çalışmada hack sınıflandırılması, süreçsel ve işlemsel sınıflandırmaya ayrılmıştır. Bu çalışmada ise temel olarak işlemsel sınıflandırma içerisinde yer alan ve "araçlar" başlığını oluşturan teknikler detaylandırılacaktır.

3.1.1. Süreçsel Sınıflandırma

Internet'te gerçekleştirilen hack'ing teknikleri temel olarak dört kategoriye sokulabilir.

Şekil 3-1 Hack Türleri



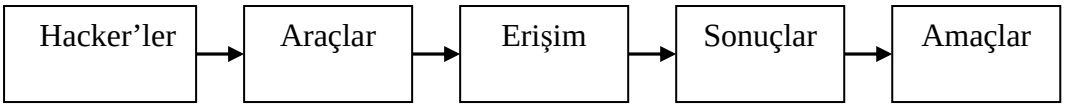
1. Engelleme: Sistemin bir kaynağı yok edilir veya kullanılamaz hale getirilir. Donanımın bir kısmının bozulması iletişim hattının kesilmesi veya dosya yönetim sisteminin kapatılması gibi.
2. Dinleme: İzin verilmemiş bir taraf bir kaynağa erişim elde eder. Yetkisiz taraf, bir şahıs, bir program veya bir bilgisayar olabilir. Ağdaki veriyi veya dosyaların kopyasını alabilir.
3. Değiştirme: İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklik yapar. Bir veri dosyasının değiştirilmesi, farklı işlem yapmak üzere bir programın değiştirilmesi ve ağ üzerinde iletilen bir mesajın içeriğinin değiştirilmesi gibi.
4. Oluşturma: İzin verilmemiş bir taraf, sisteme yeni nesneler ekler. Ağ üzerine sahte mesaj yollanması veya bir dosyaya ilave kayıtlar eklenmesi.

3.1.2. İşlemsel Sınıflandırma

Genel anlamda bir hack; yöntemler, kullanılan yollar ve sonuçları açısından düşünülebilir. Bilgisayar yada bilgisayar ağını hack etmeye çalışan kişi, istediği

sonuca çeşitli adımlardan geçerek ulaşmak zorundadır. Bu adımlar aşağıdaki şekilden de görüldüğü gibi araçlar, erişim ve sonuçlar şeklindedir.

Şekil 3-2 İşlemsel Sınıflandırma



3.2. Araçlar

Bu çalışmanın temelini oluşturan hack tekniklerini belirten genel yapı, araçlar bölümü içerinde değerlendirilecektir. Daha öncede belirtildiği gibi günümüzde hacking olayları belirli araçlar yardımı ile yapılmaktadır. Bu araçlar ise aşağıda listelenen hack tekniklerine ulaşabilmek için kullanılmaktadırlar. Söz edilen hack tekniklerin, ve yazıda araçlar olarak değerlendirilen ve sınıflandırılan hack türleri bu türlerin açıklamaları Tablo 3.1. detaylı olarak verilmektedir.

Tablo 3-1 Hack teknikleri, Hack Türleri .

Hack Türleri	**Dinleme**	**Engelleme**	**Oluşturma**	**Değiştirme**
Hack Teknikleri	Sosyal Mühendislik	DOS	Virüs	Spoofing
	Ping Tarama	Email Bombardment	Trojon	IP spoofing
	Port Tarama	IP Servis Durdurma	Worm	Email spoofing
	İşletim Sisteminin Belirlenmesi	SYN seli		
	Sniffer	NFS		
	Firewalking			

3.3. Hack Teknikleri ve Türleri

Tablo 3-1'de verilen hack türleri bu bölüm altında incelenecek ve ne tür yapı içerisinde gerçekleştirildiği açıklanmaya çalışılacaktır. Bu açıklama sistematik bir şekilde ve Tablo 3-1'e bağlı kalınarak yapılacaktır. Tablo 3-1'de verilen "Hack Türleri" ve bu türlerin alt başlıklarını toplayan "Hack Teknikleri", detaylandırılacak fakat olayın teorik yapısına girilmeyecektir "Teorik yapılara Bölüm 4'te incelenecektir".

3.3.1. Dinleme

Aslıda kedi başına bir hack türü olmasına rağmen bütün hack yöntemlerinin temelini oluşturan olgudur "CERT/CC". Bir çok kaynak tarafından hacking

olaylarının artmasının en büyük nedeni olarak gösterilmektedir. Bunun temel nedeni ise hacker'ler kullandıkları dinleme yöntemleri sayesinde hack edeceği sistem hakkında hemen hemen tüm bilgiyi elde eder yada istediği bilgiyi direkt olarak ağ üzerinden alır.

Dinleme yöntemi aslında temel olarak, ağdaki bileşenleri dinlemek veya ağı üzerindeki bilgiyi dinlemek olarak iki başlık altında toplanabilir. Bunlardan birincisi Tarama, "Scan" ikincisi ise Dinleme'dir "Sniffer"

Scan işlemi, temel olarak hedef ağda bulunan bileşenleri ve bu bileşenlere erişim haklarını saptamak için yapılmaktadır. Aktif sistemlerin belirlenmesi, işletim sistemlerinin saptanması, ve bu bileşenlerin ağ üzerindeki konumlarının belirlenmesi gibi aşamalardan oluşur. Scan, hedef ağın yöneticisi ile aynı bilgi seviyesine ulaşana kadar bu süreç devam eder. Ağ haritalamasının yapılma sebepleri aşağıda sıralanmaktadır:

- Hedef ağdaki tüm bileşenler.
- Hedef ağa ait olan alan adı, IP aralığı ve internet erişim hattının ait olduğu kurumlar, kişiler, bitiş süreleri.
- Hedef ağdaki aktif bileşenlerin işletim sistemleri, sürümleri, yama seviyesi.
- Sunucu sistemler üzerinde çalışan servisler, kullanılan uygulamalar ve yama seviyeleri.
- Hedef ağdaki tüm bileşenlere ve servislere erişim haklarının belirlenmesi.
- Hedef ağdaki tüm güvenlik uygulamaları, erişim listeleri, sürümleri, yama seviyeleri sürümleri.
- Hedef ağdaki aktif bileşenlerin ağdaki yerleşimi

Sniffing ise ağ üzerinden gidip gelen bilgilerin dinlenmesine dayanmaktadır. Sniffing işlemini temel olarak detaylandırmak gerekirse TCP/IP protokolünü kullanan bir Ethernet ağında bilgisayarlar birbiriyle haberleşirken IP numarasını kullanırlar. Her bilgisayar konuşacağı bilgisayarın ip numarasını öğrenir ve göndereceği paketlere o bilgisayarın ip numarasını yazarak yollar. Ancak ağ üzerinden gelen binlerce paket içerisinde ise sadece kendi ip numarası geçen paketleri dinler diğerlerini filtreler. Böylece her bilgisayar kendisiyle ilgili olan bilgileri alıp göndermiş olur. Sniffer programlar ise bu filtreleme olayını software olarak devre dışı bırakır ve ağdaki tüm paketleri dinler.

Dinleme temel olarak aşağıdaki konu başlıklarını içerir:

1. Sosyal Mühendislik ,
2. Ping Tarama
3. Port Tarama
4. İşletim Sisteminin Belirlenmesi
5. Sniffer
6. Firewalking

3.3.1.1. Sosyal Mühendislik

Sosyal mühendislik “Social Engineering” olarak adlandırılan temel hack tekniğinin, Hack Türleri sınıflandırması içerisinde bulunan “Dinleme” başlığı altında yer almasının temel sebebi insan “operatör” faktörünün ağ elemanlarından biri olarak kabul edilmesindedir.

Sosyal mühendislik temel olarak insan ilişkilerini veya insanların dikkatsizliklerini kullanarak kurum hakkında bilgi toplamak olarak tanımlanabilir. Bu olayda amaç kurum yapısı, kurumsal ağın yapısı, çalışanların/yöneticilerin kişisel bilgileri, şifreler ve saldırıda kullanılabilecek her türlü materyalin toplanmasıdır. Kuruma çalışan olarak sızmak, çalışanlarla arkadaş olmak, teknik servis yada destek alınan bir kurumdan arıyormuş gibi görünerek bilgi toplamak, bilinen en örnekleridir.

3.3.1.2. Ping Taraması

Ping Sweep “ICMP sweep olarakta bilinir” belirli bir IP aralığında ağa bağlı olan host’ların çalışıp çalışmadığını kontrol eden temel ağ tarama tekniğidir. Tek bir ping genelde host’un ağa bağlı olup olmadığını belirtirken, ping sweep birçok host’a ICMP (Internet Control Message Protocol) ECHO isteği gönderir ve cevap için ağı dinler. Eğer yollanılan adresteki host aktif halde ise ICMP ECHO cevabı geri döner. Ping sweep yöntemi, ağı taramak için kullanılan en yavaş ve en eski yöntemlerden biridir.

3.3.1.3. Port Taraması “Port Scan”

Günümüz dünyasında birçok işletim sistemi birden fazla programın aynı anda çalışmasına izin vermektedir. Bu programlardan bazıları dışarıdan gelen istekleri (istemci-client/request) kabul etmekte ve uygun gördüklerine cevap (sunucu-server/response) vermektedir. Sunucu programları çalışan bilgisayarlara birer adres verilir (IP adresleri) ve bu adresler kullanılarak istenilen bilgisayarlara ulaşılır. Ulaşılan bu bilgisayar üzerindeki hangi sunucu programdan hizmet almak istendiği belirlemek ise port’lar sayesinde sağlanır.

Bunun için bilgisayarlar üzerinde birtakım soyut bağlantı noktaları tanımlanır ve her birine, adresleyebilmek için positif bir sayı verilir (port numarası). Bazı sunucu programları, daha önce herkes tarafından bilinen port’lardan hizmet verirken (örn: telnet->23. port) bazıları da sunucu programını çalıştıran kişinin türüne ve isteğine göre değişik port’lardan hizmet verir. Dolayısıyla, ağ üzerindeki herhangi bir sunucu programa bağlanmak istenildiğinde, programın çalıştığı bilgisayarın adresinin yanında istekleri kabul ettiği port numarasını da vermek gerekir.

Port numarası genellikle 2 byte olarak tutulur. Bu nedenle 65536 adet port numaralamak mümkündür. Genellikle 1024’ten küçük olan port numaraları özel hakları olan kullanıcılar (root) tarafından kullanılırken, büyük olanlar genel kullanıma açıktır.

Port Scanner’ler ise varolan bu port’lar otomatik olarak tarayan yazılımlardır. Scan işleminin birçok çeşidi vardır. Bu çeşitler, hacker ve hacking yöntemlerine karşı

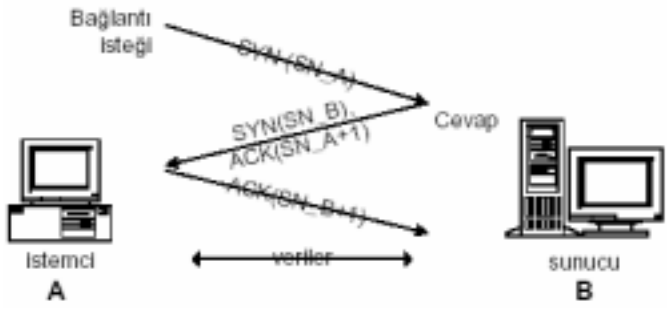
koymak için geliştirilen yöntem ve tekniklerin gelişimi ile doğru orantılı olarak artmıştır.

Temel Port Scan türleri aşağıda verilmiştir:

1. TCP Connect Scan
2. TCP SYN Scan
3. TCP FIN Scan
4. SYN/FIN scanning using IP fragments (bypasses packet filters)
5. TCP Xmas Tree Scan
6. TCP Null Scan
7. TCP ACK Scan
8. TCP ftp proxy (bounce attack) scanning
9. TCP Windows Scan
10. TCP RPC Scan
11. UDP Scan
12. Ident Scan

Fakat bu Scan çeşitleri anlatılmadan önce konunun daha iyi anlaşılması için bilgisayarların İnternet üzerinden bir birleri ile bağlantısını sağlayan bir dizi ağ protokolü olan Transmission Control Protocol'nün "TCP" nasıl çalıştığı incelenmelidir. TCP oturumu, ilk olarak, bir sunucu bilgisayardan servis isteyecek diğer bilgisayar (istemci), bağlantı kurmak istediğini göstermek için SYN bayrağı kalkık(set) paketini, sunucu bilgisayara gönderir. Bu paketi alan sunucu SYN paketi aldığını ve bağlantı isteğini onayladığını yine SYN bayrağı kaldırılmış(set) paketi (SYN-ACK paketi) istemci bilgisayara gönderir. Üçüncü aşamada ise sunucu bilgisayarın gönderdiği SYN-ACK paketini alan istemci bilgisayar sunucuya bu paketi aldığını bildiren bir paket gönderir(ACK).

Şekil 3-3 Port Taraması "Port Scan"



3.3.1.3.1. TCP Connect Scan

Bu tarama yukarıda bahsi geçen oturum açma işlemini tamamıyla yapar ve oturum açıldığında bağlantıyı kesip bize port'un açık olduğu bilgisini verir. Bu tarama türünün iyi yanı, oturumun açık olduğunu bire bir test etmesi olduğu gibi kötü tarafı da karşı sistemin açılan bütün oturumları kaydetmesi durumunda oturum açma isteğini gönderen tarafın IP bilgisin karşı sistemin veri tabanında yerini almış olmasıdır. Sadece zorunlu durumlarda yada emin olunması gereken durumlarda risk alınarak yapılan bir tarama türüdür fakat kesin sonuç verir.

3.3.1.3.2. TCP SYN Scan

Yukarıda bahsi geçen riski almamamız için oturumu açmadan taramamız gerekir. Bu tarama türü yarı-açık tarama olarak ta anılır. Sebebi yukarıda anlatılan oturum açma işleminin ilk 2 aşaması olan SYN bayraklı paketi gönderme ve SYN/ACK bayraklı paketi alma işlemini başarıyla yapmasına rağmen ardından RST/ACK bayraklı bir paket göndererek oturumun açılmasını reddetmesidir. Port'un açık olduğu sonucuna SYN/ACK bayraklı paketi alındığında karar verilir. RST/ACK bayraklı paket oturumun resetlenmesi için gönderilen pakettir. Böylece oturum açılmadığından kayıtlara geçme ihtimalimiz azalır.

3.3.1.3.3. TCP FIN Scan

Eğer bir port'u oturum açma işlemlerini kullanmadan taramak istiyorsak kullanabileceğimiz yöntemlerden biri FIN taramadır. Eğer bir sistemin port'larından birine FIN bayraklı bir paket gönderilirse RFC793'e göre sistem kapalı olan portlar icin RST cevabı gonderir. Bize de açık olan portların bilgisi kalır.

3.3.1.3.4. SYN/FIN Scanning Using IP Fragments

Bu Scan tip aslıda yeni bir yöntem değildir. SYN ve FIN yöntemlerinin geliştirilmiş bir türüdür. Bu yöntemde bir araştırma paketi göndermek yerine paketi daha küçük iki üç IP fragmenti olarak gönderilir. Kısaca TCP paketlerinin başlıklarını paket filtreleşicilerinin işini zorlaştırmak ve yapılan işin anlaşılmaması için çeşitli paketlere bölmektir.

3.3.1.3.5. TCP Xmas Tree Scan

Noel ağacı anlamına gelen bu tarama türünde hedef sistemin portuna FIN "No more data from sender", URG "Urgent Pointer field significant" ve PUSH "Push Function" flaglı paket gönderilir ve kapalı olan port'lardan RFC 793'e göre RST cevabı beklenir. Cevapsızlar yine açık port'lardır.

3.3.1.3.6. TCP Null Scan

Bu tarama türü ise Xmas Tree'nin tersine hiçbir bayrak taşımayan bir paket gönderir. RFC 793'e göre sistemin kapalı olan portlarından RST cevabı gelir.

3.3.1.3.7. TCP ACK Scan

Bu tip taramada temel mantık statik yada dinamik paket filtreleme de firewall'ların bağlantıyı ilk başlatan tarafı hatırlayamamasıdır. Bazı firewall'ların onaylanmış bağlantılara izin verdiğini de düşünürsek bu ACK “Acknowledgment field significant“ paketin firewall yada router’ların içinden engellenmeden geçmesi ve hedefe ulaşması mümkün olabilir. Bu şekilde Firewall'ları bypass ederek hedefe ulaşıp hedefin port’larını tarama şansı kazanırız.

3.3.1.3.8. TCP Ftp Proxy (Bounce Attack) Scanning

RFC 959 tanımına göre ftp protokolünün dikkat çekici bir özelliği de proxy ftp bağlantısına izin vermesidir. Bu tür scan tipi ise bu özelliğin yarattığı açığı kullanır. Çünkü bu özellik hacker.com’dan, kurba.com’un FTP server-PI (protocol interpreter) aracılığı ile kontrol haberleşme bağlantısı kurulabilir. Bu bağlantı sayesinde, server-PI’e ağdaki her hangi bir yere dosya yollayabilecek server-DTP (data transfer process) isteği aktif edilebilir. Bu açık özellikle firewall arkasında bağlı bulunan bir ftp’ya bağlandığımız zaman sunucuya kendi port’larını taratması sağlandığı için çok tehlikeli bit tarama türüdür. Çünkü firewall baypas edilmiş olur.

3.3.1.3.9. TCP Windows Scan

Bu scan türü TCP Windows Scan raporlarındaki kusurları dikkate alarak bazı işletim sistemlerinde portların açık olup olmadığını yada filtreli olup olmadığını kontrol eder.

3.3.1.3.10. TCP RPC Scan

Bu tarama yöntemiyle RPC (Remote Procedure Call - Uzak işlem çağrıları) port’larından çalışan işlemleri ve sürümlerini anlama şansımız olabilir.

3.3.1.3.11. UDP Scan

Bu teknik hedef porta udp paketi göndererek kapalı olan porttan "ICMP port unreachable" mesajının alınması temeline dayanır. Eğer bu mesaj gelmezse port’un açık olduğu anlaşılır. Bu işlemi yaparken oldukça yavaş davranmak gerekir. Özellikle de yoğun işlemlerin olduğu bir filtreleme cihazının üzerinden scan yaparken.

3.3.1.3.12. Ident Scan

RFC 1413'te tanımlanmış bir protokol olan Ident protokolü üzerine inşa edilen bir tarama türüdür. Diğer taramalar ile birlikte kullanılır. Hedef sistem üzerinde Identd aktif ise sistemde çalışan servislerin tam listesine ve bu servisleri çalıştıran kullanıcıların isimlerine ulaşılması için yapılır. Identd aktif durumda değil ise bu tarama türü işlevsiz olmaktadır.

3.3.1.4. İşletim Sisteminin Belirlenmesi

İşletim sistemlerinin belirlenmesi, temel olarak her işletim sisteminin belirli komutlar karşısında sadece kendine has cevaplar vermesinin kontrolü ile yapılmaktadır. bulunmaktadır. Birkaç yöntem kullanılarak hedef sistemlerin işletim sistemleri saptanabilmektedir, bunlar Banner yakalama, Aktif TCP parmakizleri saptama, Pasif TCP parmakizleri saptama ve son olarak ICMP kullanarak işletim sistemi saptamadır.

3.3.1.4.1. Banner Yakalama

Bu tekniğin temeli bazı sistemlerde bağlanılan portlarda giriş mesajlarıyla karşılaşılmasına dayanmaktadır. Fakat buna ek olarak giriş yaptıktan sonra basit yöntemlerle işletim sistemini saptamaya çalışmak gerekebilir. Aşağıdaki örnekte Washington Universitesi FTP sunucusu kullanılan sunucuya bağlanarak SYST komutunu verildi ve işletim sistemi tipi hakkında ufak bir bilgi edinildi.

```
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 localhost.localdomain FTP server (Version wu-2.6.1-16) ready.
SYST
215 UNIX Type: L8
```

Karşılama mesajları içerisinde çalışan servis türü , işletim sistemi türü ve hatta üzerinde yüklü olan yamalar yeralabilir ; ancak bu bilgilere güvenmekte çok sağlıklı değildir. Çünkü bu servislerde yapılabilecek ufak değişiklikler (kodunda yada ayar dosyalarında) bu bölümlerin sahte bilgilerle doldurulmasını sağlayabilir.

3.3.1.4.2. Aktif TCP Parmakizleri Saptama

Temel fikir işletim sistemlerine bazı TCP paketleri gönderilerek verdikleri cevapları incelemek ve bu sayede işletim sistemini saptamaktır. Gönderilecek paketler içerisindeki çeşitli flag'larla oynanarak , parçalanma işareti ile oynayarak , ack değeri yada servis türü gibi bilgilerle oynayarak gönderilir. Karşılığında gelen paketlerdeki cevaplar içinde flaglara bakmak, pencere boyutuna bakmak yada gönderilen ve alınan

ISN/ACK numaralarını incelemek gibi yöntemlerlede hedefin işletim sistemi saptanmaktadır. Bu tekniğin kullanılabileceği araçlar içerisinde Nmap ve Queso başı çekmektedir. Nmap bu aktif işletim sistemi saptama konusunda gerçekten oldukça ilerlemiştir, ciddi bir parmakizi veritabananınıda barındırmaktadır.

3.3.1.4.3. Pasif TCP Parmakizlerini Saptama

Yukarıda bahsi geçen yöntemle arasındaki en önemli fark ; aktif parmakizi saptamasında hedefe çeşitli paketler göndermek ve cevabını beklemek esastır, ancak pasif parmakizi saptamasında hiçbir özel paket gönderilmez ve böylece saldırı tespit sistemi gibi sistemlerce yakalanma işlemi gerçekleşmez. Normal bir ftp, telnet, pop3, smtp, http gibi bir protokol kullanılarak hedefe bağlanırken çalıştırılan pasif parmakizi saptama yazılımı da gelen ve giden paketleri yakalayarak işletim sistemini saptamaya çalışır.

3.3.1.4.4. ICMP kullanarak İşletim Sistemi Saptama

Bu fikir Ofir Arkin tarafından ortaya atılmıştır ve ICMP'nin taramalarda sağlayabileceği yararları *Sys-Security Group* adresinde yayınladığı ve 200'ün üzerinde sayfa sayısına sahip olan bir dökümanda açıklamıştır. Basitçe echo, timestamp, info, address mask gibi çeşitli ICMP istekleri ile hedef sistemlerden bilgi toplamaya çalışmak birinci yöntemidir. Birinci yöntemde broadcast'e , hedeflere yada router'lara gönderilecek ICMP isteklerine verilen cevaplarla işletim sistemlerini saptamaya çalışır. Örneğin windows versiyonları broadcast'e atılan echo isteklerini gözardı ederken kendilerine atılan echo isteklerini cevaplamaktadırlar. İkinci yöntemde ise bozuk IP paketleri göndererek hedef sistemden gelebilecek olası cevapları yorumlayarak işletim sistemini saptamak hedeflenmektedir. IP başlıklarının boylarıyla oynayarak ICMP parameter problem hata mesajını hedeften almak , IP başlıklarında geçersiz kayıtlar kullanarak gelen ICMP Destination Unreachable (Hedef ulaşılamaz) hata mesajını hedeften almak, Paket parçalama sistemini kullanarak bir ICMP Fragment Reassembly Time Exceeded (Paket birleştirme zamanı aşıldı) hata mesajını hedeften almak ve son olarak UDP paketleri göndererek hedefin kapalı portlarından gelen ICMP Port Unreachable (Port ulaşılamaz) hata mesajlarını incelemek temellerine dayanır. Ofir Arkin , ICMP ile hedefin işletim sistemini saptamaya çalışan "Xprobe" isimli bir araçta hazırlamıştır.

3.3.1.5. Sniffer

Sniffing ise ağ üzerinden gidip gelen bilgilerin dinlenmesine dayanmaktadır. Sniffing işlemini temel olarak detaylandırmak gerekirse TCP/IP protokolünü kullanan bir Ethernet ağında bilgisayarlar birbiriyle haberleşirken IP numarasını kullanırlar. Her bilgisayar konuşacağı bilgisayarın ip numarasını öğrenir ve göndereceği paketlere o bilgisayarın ip numarasını yazarak yollar. Ancak ağ üzerinden gelen binlerce paket

içerisinde ise sadece kendi ip numarası geçen paketleri dinler diğerlerini filtreler. Böylece her bilgisayar kendisiyle ilgili olan bilgileri alıp göndermiş olur. Sniffer programlar ise bu filtreleme olayını software olarak devre dışı bırakır ve ağdaki tüm paketleri dinler. Temel olarak iki türü bulunmaktadır.

3.3.1.5.1. Network Sniffing

Yukarda tanımlanan temel sniffing işlemine verilen isimdir. Geleneksel Ethernet ağına yerleştirilene bir sniffer programı ile ağ üzerindeki tüm trafik dinlemektedir. Fakat Switch kullanımından sonra çok zor bir hale gelmiştir.

3.3.1.5.2. Server Sniffing

Bu yöntem ise ağ üzerindeki server ulaşarak bu server üzerinden ağın dinlenmesine dayanmaktadır. Ağ üzerindeki server kurulacak olan sniffer ağ üzerindeki tüm bilgiyi kullanıcısına rahatlıkla yönlendirtebilmektedir.

3.3.1.6. Firewalk

Bu teknik sayesinde Firewall ile korunmakta olan ağlar hakkında ve Firewall hakkında daha ayrıntılı bilgi sahibi olunabilir. Ayrıca ağın güvenliğini ve potansiyel riskleri daha iyi görme fırsatı da kazanılmış olur. Bu teknik gelişmiş bir ağ ve TCP/IP altyapısı gerektirmektedir. Firewalk traceroute gibi IP paketlerini analiz ederek , hedefe paket filtreleme cihazının içinden geçerek ulaşmayı sağlar. Paket filtreleme cihazlarındaki erişim kontrol listelerini yada Firewall üzerindeki izin verilen portları saptamayı sağlayan bir yöntemdir. Ayrıca bu teknik kullanılarak Firewall`un arkasındaki ağın bir haritasını da çıkartma imkanına kavuşulur. Bu tekniğin nasıl çalıştığını anlamak için öncelikle traceroute`un nasıl çalıştığını anlamak gerekmektedir.

Firewalk TCP ve UDP paketlerinin IP TTL`lerini hedeflenen ağ geçidinden geçtikten sonra 0 olacak şekilde değiştirerek taramalar yapar. Eger ağ geçidi trafiğe izin veriyorsa paketi sonraki atlama noktasına verecek, paketler geçersiz olacak ve gelen TTL exceded mesajı ile de bu ortaya çıkacaktır. Eger ağ geçidi bu paket trafiğine izin vermiyorsa muhtemelen bu paketleri görmezden gelecek ve hiçbir cevap göndermeyecektir. Bu şekilde birbirini takip eden araştırmalarla ve hangilerinden cevap geldiği hangilerinden gelmediğinin kaydedilmesiyle Firewall üzerindeki erişim kontrol listesi belirlenmiş olacaktır.

3.3.1.6.1. Traceroute

Traceroute , hedef bilgisayarlara giden en kısa yolu bulmak ve paketin geçtiği ara sistemleri saptamak için tasarlanan bir ağ sorun giderme aracıdır. UDP ve

ICMP paketleri göndererek IP paketlerinin TTL (Time to Live - Yaşam Süresi) bilgilerini analiz eder. Varsayılan deneme sayısı 3`tür. Eger UDP paketi göndererek traceroute yapılıyorsa port belirtme imkanıda bulunmaktadır. TTL bilgisi paketlerin geçtikleri Router'larda sürekli olarak azaltılan bir değerdir. Eğer paketlerin TTL`si her hangi bir aşamada 0 olursa Router bir ICMP hata mesajı gönderir ve taşıma sırasında yaşam süresinin dolduğunu belirtir. Bu hata geri geldiğinde paketin hedefe ulaşamadığı anlaşılır. TTL 1`den başlar ve 2 sistem arasında Router sayısı kadar artar ve ICMP cevapları izlenir. Böylece paketlerin filtrelenip filtrelenmediği yada paketlerin kaybolup kaybolmadığı görülebilir. Hedeften gelecek cevaba göre (ICMP Port Unreachable yada ICMP Echo Reply) traceroute UDP portunu bir arttırarak denemeye devam eder.

3.3.2. Engelleme

Tek başına bir hack sınıflandırması olmasına karşın büyük ve belirli bir sistem içerisinde gerçekleştirilecek olan hack olaylarında dinlemeden sonra gerçekleştirilen ikinci adım olduğu gözlenmektedir. Bu bölüm içerisinde engellemeyi amaç edinen temel hack yöntemlerinden bahsedilecektir.

3.3.2.1. DOS

Denial-of-Service yada kısaca DoS olarak adlandırılan hack yöntemi yazılımlardaki hataları kullanarak ya da sunucu veya ağ kaynaklarını tüketme yoluyla,normal kullanıcıların erişimlerini engelleyecek şekilde,bilgisayar sistemlerini ulaşılamaz hale getirme amacıyla yapılır. Bu tip hacking'lar yapılış tarzına bağlı olarak sistemi veya sistemin sunduğu hizmet yada hizmetleri tamimiyle devre dışı bırakabilir. DoS tipindeki hacking'leri tehlikeli kılan bir başka yön ise çok eski tip makineler ve modemler ile çok karmaşık ve sofistike sistemlerin devre dışı bırakabile olanağıdır. DoS tipindeki hacking'ler sistemler ve sistemlerin sunduğu servislerin çeşitliliği göz önüne alındığı zaman çok fazla çeşide sahip olduğu sonucu ortaya çıkar. Fakat DoS tipi hackin'leri üç temel biçime ayırabiliriz.

3.3.2.1.1. Kısıtlı Kaynakların Tüketilmesi

Bilgisayarlar ve ağlar hizmet verebilmek için bant genişliği, hafıza ve disk alanı, CPU time, veri yapısı, diğer bilgisayarlar ve ağlara giriş olanağı gibi temel işlevlere ihtiyaç duyarlar. DoS hacking'lerin en genel görülen türü ise bu kaynaklara yapılanlarıdır.

3.3.2.1.1.1. Network Bağlantısı

Kaynaklara yönelik hack'lar arasında en çok rastlanan DoS tipi hacking türüdür. Bu türde amaç servis sağlayıcının yada ağın haberleşmesini engellemektir. Bu tip hacking'lere en iyi örneklerden biri ise daha sonra detaylı olarak açıklanacak olan SYN seli saldırısıdır. Bu yöntemde temel olarak dikkat edilmesi gereken husus

hackerin band genişliği ile iş görmemesidir. Yani hacker çok yavaş bir bağlantıdan çok hızlı bir ağa rahatlıkla ağ bağlantısını yok etmeyi hedefleyen saldırıları yapabilmesidir.

3.3.2.1.1.2. 5K

5K saldırısı, kullanıcı kaynaklarının kullanıcının kendisine karşı kullanılmasına dayanmaktadır. Bu yönteme en iyi örneklerden bir UDP Port üzerinden gerçekleştirilen hacking'dir. Bunun sebebi ise her hangi bir UDP servisi üzerinden bağlantı kurulması sırasında bağlantının kendi doğasından dolayı bu servis çok sayıda paket üretir. Bu yöntem ise bu paketlerin hedefe yönlendirilmesi ile gerçekleştirilir. 5K yönteminin bir diğer yan etkisi ise kullanılan makine sayısına bağlı olarak ağın kendisinde de bir yavaşlama olmasıdır.

3.3.2.1.1.3. Band Genişliğini Tüketmek

Bu hacking şekli ise direkt olarak hedef ağın çok fazla sayıda paket ile yoğunlaştırılmasına dayanmaktadır. Genelde üretim kolaylığından dolayı ICMP ECHO paketleri kullanılır fakat teorik açıdan her türlü paket bu yöntem için kullanılabilmektedir. Hacker'ler genellikle bu işlem için çok sayıda makineyi belirli bir ağa yönlendirirler.

3.3.2.1.1.4. Diğer Kaynaklar Tüketmek

Yurda da bir çoğunu belirttiğim gibi DoS' uygun birçok kaynak bulunmaktadır. Örneğin sistemler process bilgilerini (process identifiers, process table entries, process slots, etc.) kısıtlı veri yapılarında tutarlar. Hacker'ler ise bu yapıları şişirerek sistemi devre dışı bırakmak için bilgileri kopyalayarak şişiren çok küçük programlar veya script'ler kullanmaktadır. Diğer bir kısıtlı kaynak olan disk alanı ise yine gereksiz yer oluşturulan "çok sayıda mail mesajı üretmek, log dosyalarının sayısın çok hızlı artırmak, ağa paylaşıma açılmış olan veya ftp sevisine izin verilmesi sonucunda kaynakların doldurulması" veri yapısı sayesinde doldurulmasın ve sistemin çökmesine sebep olmaktadır.

3.3.2.1.2. Configuration Bilgilerinin Değiştirilmesi Veya Silinmesi

Bu tür DoS hacking yönteminin kullanımı sistemin iyi şekillendirilmememsi veya yönetilememesine dayanmaktadır. Hacker bu açıkları kullanarak sistem içindeki ayarlar ile oynar ve aslında normal olan fakat kullanılan sistemin şekline yada konumuna uymayan bilgileri girerek sistemi çalışmaz veya ulaşılamaz duruma getirir. Bu yönteme verilecek olan en iyi örnek router bilgilerinin değiştirilmesidir. Bu işlem sonucunda hedef alınan ağ tamamen yok edilir. Windows NT tip makinelerinde registry üzerinde yapılacak olan değişiklikler sayesinde bir çok servis devre dışı bırakılabilir.

3.3.2.1.3. Fiziksel Değişiklikler Veya Silmeler

Bu tip hack türü fiziksel güvenlik kavramı içerisinde yer almaktadır. Fakat sonuçları bakımından bir DoS hacking şeklidir. Bu tür; yetkisiz bilgisayar girişine, router'lere fiziksel erişimi, kablo alt yapısına erişimi, enerji ve soğutma birimlerine ve sistemimiz için gerekli olan kritik birimlerin erişimine dayanmaktadır.

3.3.2.2. Email Bombardment

Temel olarak bir DoS metodu gibi görülmekle birlikte aslında bir sistem kaynağına yok etmediği için gerçekte başka bir engelleme hacking yöntemidir. Bu metodun aslı kurbanın mail adresine normalden çok fazla ve sürekli olarak kurbanın istemediği Email mesajı yollanmasına dayanmaktadır. Yollanan bu mesajlar sayesinde kurban Email'ini temel amacı olan istediği kişi ile haberleşmesi engellenmiş olur. İnternet üzerinde kullanılan teknoloji ve yazılımların gelişmesi sayesinde artık bir çok gurup, topluluk veya kuruluş yeni ürün, haber veya oluşumlarının otomatik olarak üyeleri veya müşterilerine Email sayesine haberdar eder. Hacker'in bu metotta kullandığı teknik ise kurbanını sürekli olarak bu uyarı mesajlarını almasını sağlamaktır.

3.3.2.3. IP Servis Durdurma

Yanlış kaynak adresi bilgisiyle oluşturulmuş ICMP 'echo request" paketleri kullanılarak gerçekleştirilen, çoğu durumda hedef bilgisayarın kilitlenmesine sebep olan, ayrıca hedef olarak kullanılan ağlarda önemli derecede performans sorunları yaratabilen bir hack tekniğidir. Hedef alınan bilgisayarın IP adresinin "kaynak adres" olarak kullandığı sahte ICMP "echo request" paketlerinin hazırlanması ve bu paketlerin herkese yayınlanacak (broadcast) şekilde tüm bilgisayarlara yönlendirmesinin sağlanmasıdır. Paket herkese yayın adresini taşıdığından, ağ üzerinde yer alan ve açık olan bütün bilgisayarlar tarafından alınacaktır. ICMP 'echo request' paketi olduğundan, paketin kaynak adres kısmında yer alan bilgisayara (hedef bilgisayar) ara hedef ağ üzerinde yer alan her bilgisayar ICMP 'echo reply' paketi gönderecektir. Bu paketler de ara hedef ağ trafiği üzerinde etkili olacak, performansı kötüleştirecektir. Saldırganın kullandığı paket boyu, gönderilme süresi ve ağda bulunan aktif bilgisayar sayısı arttıkça performans düşüşü daha fazla olacaktır.

3.3.2.4. SYN seli

Bu metotta , bir bilgisayarın istemci olarak bir bilgisayara el sıkışma mekanizmasını başlatacak SYN paketini göndermesi, buna karşılık sunucu bilgisayardan SYNACK paketini aldıktan sonra son paketi (ACK) göndermemesi ile oluşur. Böyle bir durumda sunucu tarafında açılmış fakat tamamlanmamış bir bağlantı isteği oluşacaktır. Bu bağlantı isteği uzun bir süre dolumuna kadar açık tutulacaktır. Bu tür bağlantılara yarı açık bağlantılar denir. Bu mekanizmanın kötüye kullanılabilecek noktası, arka arkaya belirtilen bu işlemlerin yapılmasıyla ortaya çıkar. Böyle bir durumda yarı açık birçok bağlantı oluşacaktır. Herhangi bir hizmet bir

port üzerinden verilmektedir. Buraya gelen istekler bir kuyruğa alınır ve istemciden üç yollu bağlantıdaki son paket gelene kadar kuyrukta tutulur. Dolayısıyla kuyruktaki tamamlanmayan bağlantı isteklerinin artması kuyruğun dolmasına sebep olacaktır. Kuyruk dolduğunda ise yeni gelen bağlantı isteklerine cevap veremeyecektir. Dolayısıyla servis kilitlenecektir. Bazı sistemlerde bellek taşmasına sebep olacağından bu durum sunucu bilgisayarı

3.3.2.5. Network File System

NFS (Network File System), ağ üzerindeki bilgisayarların dosyalarını birbirleriyle paylaşmalarını sağlayan bir protokoldür. Ancak bu protokolün açıklarının kullanılmasıyla, sistemi büyük zararlar verilebilecek bir saldırıya açmış olursunuz. NFS uzun zamandır üzerinde çalışılan bir protokoldür ve saldırı programları internette yaygın olarak bulunmaktadır. NFS'e yönelik saldırılar değişik sonuçlar doğurabilir. Saldırgan hedef bilgisayar üzerinde super kullanıcı yetkisiyle işlemler yapabilecek duruma gelebilir. Alınabilecek önlemeler; Güvenlik duvarından NFS servislerine ait paketlerinin geçişi engellenebilir. Aynı şeklide internet üzerinden bu servislere ulaşım yasaklanabilir. Bu önlemeler NFS'e dışardan gelebilecek saldırılar içindir. İç ağdan gelebilecek saldırılara hala açıktır.

3.3.3. Oluşturma

Bu hacking türü aslında amacı olarak tanımlana bilinir. Bu aşamadan sonra hacker sisteme sızmış ve amacına ulaşmış olmaktadır. Daha önceki bölümler içerisinde detaylı olarak bahsettiğim araçlar sayesinde bu tür çok rahat gerçekleştirilebilir hale gelmiş ve tehlikesi had safhaya ulaşmıştır.

3.3.3.1. Virus

Virüsler, kendi kodlarını başka programlara veya program niteliği olan dosyalara bulaştırabilme özelliği olan (kendi kodunu kopyalayabilen) bilgisayar programlarıdır.Bulaştıkları bilgisayarda genelde hızlı bir şekilde yayılırlar.Belli bir amaca yönelik olarak yazılmış, zarar vermeye yönelik olabilecekleri gibi eğlence amacıyla da yazılmış olabilirler.

Virüsler çoğunlukla Assembly gibi düşük seviyeli bir programlama dili ile yazılırlar.Bunun asil 2 sebebi vardır.

1- Assembly'in çok güçlü bir dil olması:
2- Yazılan programların derlendikten sonraki dosya boylarının çok küçük olması

Bu özelliklerin her ikisi de virüs yazarlarının assembly dilini kullanması için yeterli ve gerekli sebeplerdir. Virüsleri özelliklerine göre sınıflandırmak pek mümkün olmasa da aşağıdaki şekildeki gibi bir sınıflandırma yapmak yanlış olmayacaktır. Ancak pek çok virüs, pek çok özelliği bünyesinde barındırabilir. Bulaşma hızını arttırabilmek amacıyla yapılan bu durum sonucu virüs, bot sektörlere, mbr kayıtlarına, programlara bulaşabilir. Simdi de bu virüs türlerinin isleyişlerine bakalım

1. Disk virüsleri :
    i. Boot
    ii. MBR
2. Dosya virüsleri :
    i. Program (TSR ve nonTSR)
    ii. Makro virüsleri
    iii. FlashBIOS virüsleri

3.3.3.1.1. Disk Virüsleri

Disk virüsleri, adından da anlaşılacağı üzere, disk ve/veya disketler üzerinde işletim sistemi için özel anlamı olan bölgelere (boot sektör, MBR) yerleşen virüslerdir. Disk virüsleri, hakkında en çok yanlış bilginin olduğu virüs türüdür.Boot ve MBR virüsleri, aşağıda da göreceğiniz gibi işletim sisteminden önce hafızaya yüklenir. Bu yüzden işletim sistemini kolaylıkla atları. Disk virüslerini boot ve MBR (partition) virüsleri olarak 2 gurupta incelenecektir.

3.3.3.1.1.1. BOOT Virüsleri

Boot virüslerinin ne olduğuna geçmeden önce boot sektör nedir, disk üzerinde nerede bulunur, önce bunlara bir bakalım; Boot sektör, bir diskin veya disketin işletim sistemini yüklemeye yarayan 1 sektör (512 byte) uzunluğundaki bir programdır.Boot sektörler, disketlerde 0.ci iz, 0.ci kafa,1.ci sektör üzerinde bulunur. Hard disklerde ise boot sektörü 0.ci iz, 1.ci kafa ve 1.ci sektör üzerinde bulunur.Boot sektör, açılış için gerekli sistem dosyalarının yükleyen programdır.Ayni zamanda disk (veya disket) ile ilgili bilgileri saklar.DOS buradaki bilgileri kullanarak cylider hesaplarını yapar.

Normal koşullarda, bilgisayarı başlatabilecek durumdaki bir sistem disketini (virüssüz) sürücüye takip bilgisayarı açtığımızda, bilgisayar ilk olarak disket sürücüye bakar.Eğer sürücüde bir disket var ise bu disketin boot sektörü hafızanın 0000:7C00 (hex) adresine okunur ve okunan boot sektör çalıştırılır.Boot sektör, işletim sistemini yükleyerek denetimi işletim sistemine bırakır.Eğer bilgisayarı boot edecek disket bir boot virüsü içeriyorsa o zaman durum değişir.Bilgisayar, boot sektörü yine 0000:7C00 adresine okur ve akısı bu adrese yönlendirir.Disketten okunan boot kaydı, yapı olarak değiştiğinden dolayı, 0000:7C00'daki kod virüsü hafıza içine yükleyip, hafızadaki konumunu garanti altına alacaktır.Virüs aktivitesi için gerekli interrupt servislerini de kontrol altına aldıktan sonra orijinal boot kadidini okuyarak işletim sisteminin yüklenmesini sağlayacaktır.

3.3.3.1.1.2. MBR (Partition) Virüsleri

MBR virüsleri esas olarak, boot virüslerinden pek de farklı değildir.Ancak can alici bir nokta vardır ki, bu boot ve mbr virüsleri arasındaki en önemli noktadır. Hard diskler kapasite olarak çok farklı ve büyük kapasitede olduklarından diskin DOS'a tanıtılması amacıyla MBR - Master Boot Record (Ana açılış kaydı) denilen özel bir açılış programı içerirler.Bu kod diskin 0.ci iz, 0.ci kafa ve 1.ci sektörü üzerinde bulunur.Yani disketlerde boot sektörün bulunduğu konum, hard diskler için MBR

yeridir.Master boot record, hangi disk partitionundan bilgisayarın açılacağını gösterir.Bu yüzden çok önemlidir.Eğer bilgisayar hard diskten boot ediliyorsa, o takdirde mbr ve partition table okunur.Aktif partitiona ait boot sektör okunur.Bundan sonrası boot sektör kısmındaki sistemin aynisidir.

3.3.3.1.2. Dosya Virüsleri

Dosya virüsleri açıkça anlaşılacağı gibi hedefi dosyalar olan virüslerdir.Dosya virüsleri çoğunlukla COM, EXE, SYS olmak üzere OVL, OVR, DOC, XLS, DXF gibi değişik tipte kütüklere bulaşabilirler.

3.3.3.1.2.1. Dosya Virüsleri

Dosya virüsleri açıkça anlaşılacağı gibi hedefi dosyalar olan virüslerdir.Dosya virüsleri çoğunlukla COM, EXE, SYS olmak üzere OVL, OVR, DOC, XLS, DXF gibi değişik tipte kütüklere bulaşabilirler.

3.3.3.1.2.1.1. Program Virüsleri

Program virüsleri, DOS'un çalıştırılabilir dosya uzantıları olan COM ve EXE türü programlar basta olmak üzere SYS, OVL, DLL gibi değişik sürücü ve kütüphane dosyalarını kendilerine kurban olarak seçip bu dosyalara bulaşabilirler.Dosya virüsleri bellekte sürekli kalmayan (nonTSR) ve bellekte yerleşik duran (TSR) olarak 2 tipte yazılırlar.

3.3.3.1.2.1.1.1. NonTSR Virüsler

Bellekte sürekli olarak kalmazlar.Kodları oldukça basittir.Bellekte sürekli kalmayan virüsler sadece virüslü bir program çalıştırıldığında başka programlara bulaşabilirler.Virüslü program çalıştırıldığında programın basında program kontrolünü virüs koduna yönlendirecek bir takım komutlar bulunur.Virüs kontrolü bu şekilde ele aldıktan sonra virüs kendisine temiz olarak nitelendirilen virüssüz programlar aramaya koyulur.Bulduğu temiz programların sonuna kendi kodunu ekler ve programın basına da virüsün kontrolü ele alabilmesi için özel bir atlama komutu yerleştirir ve kendisine yeni kurban programlar arar.Virüs bulaşma isini bitirdikten sonra çalıştırmak istediğimiz program ile ilgili tüm ayarları düzenleyerek kontrolü konak programa devreder

3.3.3.1.2.1.1.2. TSR Virüsler

TSR virüsler yapı olarak TSR olmayan virüslerden çok farklıdır.TSR virüsler, 2 temel bölümden oluşurlar.1.ci bölüm; Virüsün çalışması için gerekli ayarlamaları yapar ve TSR olacak kodu aktifleştirir.2.bölüm TSR olan kodun kendisidir ve TSR virüslerin hayati önemdeki bölümüdür.Bu tip virüsler, çalışmak için sadece TSR

olmakla kalmazlar.Ayni zamanda çeşitli Interruptlari (kesilmeleri) kontrol altına alırlar.Böylece DOS üzerinden yapılan işlemleri bile kontrol altına alabilirler.Örnek vermek gerekirse; TSR bir virüs DIR, COPY gibi DOS komutları ile yapılan -daha doğrusu yapılmak istenen- işlemleri kontrol altına alabilir.Kullanıcı DIR komutunu kullandığında dosya boylarının 0 olarak gösterilmesi, dosya boylarının eksik gösterilmesi gibi işlemler TSR bir virüs için çok kolaydır.

3.3.3.1.2.1.2. Makro Virüsleri

Makro virüsleri Word, Excel gibi programların makro dilleri ile (mesela VBA-Visual Basic for Applications) yazılırlar.Aktif olmaları bazı uygulamalara (word, excel vs) bağlı olduğundan program virüslerine oranla çok daha az etkilidirler.

3.3.3.1.2.1.3. FlashBIOS Virüsleri

FlashBIOS virüsleri tekrar yazılabilir özellikteki BIOS ciplerine bulaşırlar.

3.3.3.2. Trojan

Truva atları, virüslerden oldukça farklı bir yapıya sahiptir.Asla başka programlara bulaşmazlar. Belli olaylara bağlı olarak tetiklenen bir rutindirler. Kendilerini kopyalayamadıkları için bazı programların içine bilinçli olarak yerleştirilirler. Trojanlar, ilgi çeken, utility gibi programların içine yerleştirilirler. Trojan kodu, trojanin içine gizlendiği programın yazarı tarafından yazılmış olabileceği gibi sonradan da programa eklenmiş olabilir.Trojanlar aslında kopya koruma amacıyla hazırlanırlar.

3.3.3.3. Worm

Kurt (worm) bağımsız bir programdır. Kendi kendine çoğalarak, bir bilgisayardan ötekine kopyalanır, genellikle de bir network sistemine yayılır. Virüslerden farklı olarak, diğer programlara sıçramaz. Kutlar, veri yok etmemekle birlikte, network içinde dolaşarak, iletişimi yok edebilir. Ancak, bir kurt veri yok edicisine de dönüştürülebilir. Virüslerden farklı olarak e-posta ve yedekleme ortamlarına ek olarak sunucuların zayıflıklarını da kullanan, sunuculara zarar verip, çeşitli saldırılar için arka kapılar bırakan, virüslerden daha zeki programcıklardır. Verdiği zararlar ise yerel ağdaki tüm sistemlere e-posta kullanmaksızın bulaşmak, Sunucuları servis dışı bırakmak, Web sayfası içeriğini değiştirmek, Yerel ağda yüksek miktarda trafik oluşturmak, İnternet’teki belirli sunuculara veya rastgele sunuculara saldırmak.

3.3.4. Değiştirme

İzin verilmemiş bir taraf bir kaynağa erişmenin yanı sıra üzerinde değişiklik yapar. Bir veri dosyasının değiştirilmesi, farklı işlem yapmak üzere bir programın değiştirilmesi ve ağ üzerinde iletilen bir mesajın içeriğinin değiştirilmesi bu yönteme verilecek örneklerden bir kaçıdır. Fakat yöntem en etkin şekilde Spoofing tipinde görülmektedir.

3.3.4.1. Spoofing

Spoof'un kelime anlamı oyun/parodi/kandırmaktır. Internet ortamında ise Spoofing birkaç alanda karşımıza çıkar. Spoof genel olarak IP'deki (Internet Protokolü) değerlerin olduğundan farklı olarak gösterilmesi demektir.

3.3.4.2. IP Spoofing

IP paketlerinin kaynak IP' sini değiştirmekle sağlanmaktadır. Böylece paketi alan hostun, paketin geldiği kaynak adresini bilmesini engellenmiş olur. Host gelen paketin saldırgandan değil de kullanıcıdan geldiğini sanır.

4. Sonuç

Günümüz sistemlerinin çoğu, sistem tasarımında tüm sistemi kontrol edebilen bir **root** kullanıcısına sahip olduğu için, uzak yada yerel root erişim zayıflığı sorununu içermektedir. Hacking tekniklerinin çoğu da root erişim hakları ile çalışan process'lerdeki zayıflıklardan yararlanmaya çalışırlar, çünkü bir sistemde root erişimini elde etmek her şey demektir. Kısacası günümüz işletim sistemlerinden herhangi biri hakkında "en güvenli sistem" tabirini kullanamayız, tabiki Microsoft platformlarını zaten en güvensiz ve kararsız sistemler olduğu için bu konu dışında tutuyorum.

Basit olarak bir buffer uzunluğunun test edilmemesi, buffer overflow hatasına neden olacaktır ve bu da bir root erişim zayıflığına neden olacaktır. Bu nedenle, eğer güvenli bir işletim sistemi var olduğunu kabul etsek bile, o sistem yararlanılabilir bir buffer overlfow hatası bulunana kadar en güvenli sistem olarak kalacaktır ve bu zayıflık yamalanana kadar ise en güvensiz sistem konumuna düşecektir.

Ancak tüm bu problemlerden etkilenmeyen bir işletim sistemi vardır! En son network işletim sistemi olarak nitelendirilen, Bell Labs'tan **Plan 9**. Benim fikrime göre Plan 9 güvenlik konusu düşünülerek sıfırdan üretilmiş şimdilik en güvenli işletim sistemidir. Bell Labs yaklaşık 35 yıl önce UNIX işletim sistemini tasarladığında güvenlik konusu hemen hemen hiç gündemde değildi, ancak 1990'larda Bell Labs, bu sefer yaklaşık 25 yıllık tecrübesiyle yeni bir sistem üzerinde çalışıyordu ve en son network işletim sistemini üretti, Bell Labs'ın Plan 9 işletim sistemi.

Plan 9 neden güvenli? Öncelikle Plan 9 bir UNIX yada UNIX türevi bir işletim sistemi değildir. Plan 9 tamamen yeni bir işletim sistemidir. Görünüş olarak UNIX işletim sistemine benzemekle birlikte (dosya sistemi ve shell kullanımı gibi), aslında alt yapısı tamamen farklıdır ve farklı bir şekilde tasarlanmıştır.

Plan 9'daki en önemli değişiklik tüm objelerin (dizinler, dosyalar, processler..) bir dosya gibi düşünülmesidir. Aslında UNIX sistemlerinde de bu böyledir ama Plan 9 sistemindeki kadar değil.

Aşağıdaki paragraf Plan 9 ile ilgili basında yayınlanan bir makaleden alınmıştır:
"Plan 9 başından beri bir network işletim sistemi olarak tasarlanmıştır. Plan 9, istemci-sunucu modeline dayanan bir ağda dağıtılmış işlem fikrine dayanmaktadır. Uygulamalara sağlanan tüm kaynaklar dağıtılmış sistemde transparant olarak herkese aynı şekilde sağlanmaktadır."

Plan 9 process , file storage ve makine kavramlarını ayırmaktadır. Bu şekilde merkezi bir dosya sistemi vardır ve bu güvenlik açısından bir avantaj sağlamaktadır. Bu yapı dosya yönetimini, dosya haklarının kontrolü ve değişiklik gösteren dosyaların yakalanması işlevlerini kolaylaştırmaktadır.

Ancak Plan 9'un asıl güzelliği, sistemde root fikrinin hiç bulunmayışıdır. Evet Plan 9 sisteminde root diye bir kullanıcı yoktur. Kullanıcılar ayrıcalıklı dosyalara yada processlere erişim sağlamak için MIT Kerberos benzeri bir sistemle onaylanmaktadırlar. Bu sistemde şifreler ağ üzerinden hiç bir zaman geçmemektedir. Ve kullanıcı processleri dosya sunucusu üzerinde hiçbir zaman çalıştırılmamaktadır.

Cracking ve hacking tekniklerinin büyük çoğunluğu root hakları ile çalışan processlerdeki zayıflıklara dayanır, çünkü bu haklara sahip bir processte bulunan bir zayıflıktan yararlanılarak sistemde istenilen kodlar yine root erişim hakları ile çalıştırılabilmektedir. Ancak Plan 9 sisteminde root olmadığı için bu şekilde bir processte yoktur. Bu nedenle UNIX sistemlerine karşı kullanılan gelişmiş teknikler Plan 9 karşısında başarısız olarak kalmaktadırlar.

Kısacası günümüz geleneksel işletim sistemlerini en güvenli en güvensiz diye sınıflandırmak yersizdir, zira bu işletim sistemlerinin tümü güvenlik problemlerine karşı aynı tasarımı ve yaklaşımı paylaşmaktadırlar. En güvenli sistem olarak nitelendireceğimiz sistem başından beri güvenlik konusu düşünülerek tasarlanmış, gerçeklenmiş olan bir sistem olmalıdır.

Fakat günümüzde kullanılan işletim sitemleri ve yaygınlıkları düşünüldüğü zaman kısa vadede alınacak tedbirler arasında bence en etkin olanı CERT/CC tipi yapılanmaların hızla başlatılması ve geliştirilmesi olacaktır.

Kaynaklar

1. Jargon Dosyası, MIT, http://www.tuxedo.org/jargon/jargon.html, 2002
2. Dr. Thomas A. Longstaff, Information Systems New Threats, New Responses Plenary Session 2: Panel Discussion, CERT® Coordination Center Software Engineering Institute Carnegie Mellon University, 2002
3. Fatih Özavcı, Güvenlik Riskleri ve Saldırı Güvenlik Riskleri ve Saldırı Yöntemleri, http://www.siyahsapka.com, 2002
4. Çağıl Şeker, Hacker Kültürü Civarlarında Karalamalar, http://www.core.gen.tr/, 2002
5. Brian Harvey, What is a Hacker, University of California, Berkeley, http://www.cs.berkeley.edu/~bh/hackers.html, 1985
6. Yrd. Doç. Dr. İbrahim Soğukpınar, Veri ve Ağ Güvenliği ders notları, http://www.bilmuh.gyte.edu.tr/?d=./docs/kisiler/ispinar.htm, 2002
7. Jeffrey S. Havrilla, CERT/CC Overview Incident and Vulnerability Trends, CERT® Coordination Center Software Engineering Institute Carnegie Mellon University, http://www.cert.org/present/cert-overview-trends/cert-trends-modules.zip, 2002
8. Christopher Klaus, Sniffer FAQ, Internet Security Systems Inc., http://www.boran.com/security/sniff.html, 1995
9. Mustafa ATAKAN, Internet Teknolojileri Güvenliği ,ODTU Bilgi İşlem Daire Başkanlığı, http://security.metu.edu.tr/belge.php?what_is_port.txt, 2001.
10. Stuart McClure, Joel Scambray, George Kurtz, The Hacking Exposed, http://www.hackingexposed.com/home.html, 2001
11. David Goldsmith, Michael Schiffman, Firewalking, Cambridge Technology Partners Enterprise Security Services, Inc., http://www.es2.net, 1998
12. Jeffrey S. Havrilla, Denial of Service Attacks, CERT/CC, http://www.cert.org/tech_tips/denial_of_service.html , 2001
13. Email Bombing and Spamming , CERT/CC, http://www.cert.org/tech_tips/email_bombing_spamming.html, 1999