ÖN BİLGİ

Bir makale internetten bulunup şu adreste yedeklenmiştir.

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/S%C3%BCleyman%20Demirel%20%C3%9Cniversitesi%20Tezi.pdf

Bu belge ise yedeklenen bu makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

DNS Sunucu: İsimden IP, IP adresinden isim çözümleyen sistemdir. UDP 53. portu kullanır.

Web Sunucu: Html, php, asp ve benzeri sunucu taraflı betik dil ile yazılmış web sayfalarını üzerinde bulunduran sunucu olup TCP 80. portu kullanmaktadır.

FTP Sunucu: Dosya paylaşımını sağlayan sunuculardır. TCP 20. ve TCP 21. portları kullanırlar.

Mail sunucu: Mail hizmeti sunan sunuculardır.

SQL sunucu: Veri tabanlarının bulunduğu sunucudur.

DHCP sunucu: Otomatik IP dağıtmaya yarayan sistem olup; UDP 67 ve UDP 68. portları kullanır.

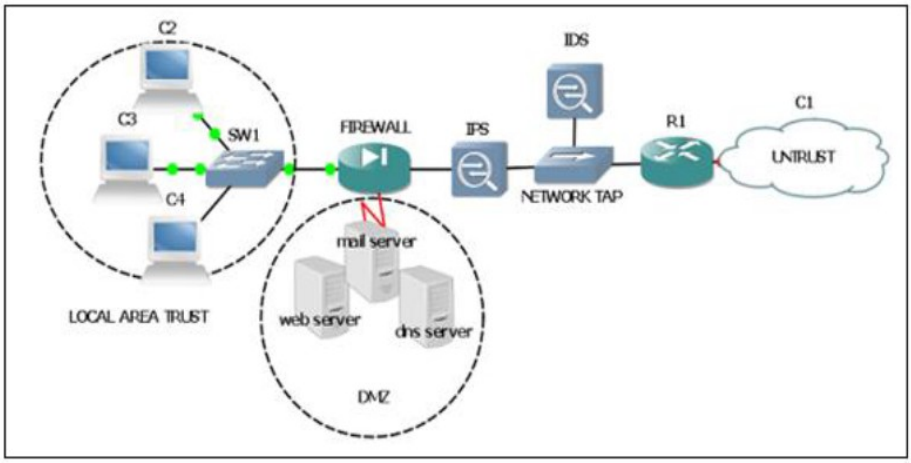
SNMP sunucu: Ağ bilgi protokolü SNMP protokolüdür. Çalışan cihazlar hakkında merkezi bir sunucudan bilgi alınabilmesi için kullanılan sunucudur. Örneğin sıcaklık bilgisi gibi UDP 161. portu kullanır.

IPS (Intrusion Prevention Systems - Sızmayı Engelleyici Sistem): 7. Katmanda denetleme yapan ve üzerindeki imzalardan yararlanarak zararlı trafiği durduran cihazdır.

IDS: Üzerindeki imzalar ile zararlı trafiği kayıt altına alan cihazdır.

WAF (Web Application Firewall - **Web Güvenlik Duvarı):** Web tarafında yapılacak SQL injection XSS gibi atakları kesen cihaz.

Aşağıdaki resimde standart ağ cihazları ile dizayn edilmiş örnek bir ağ yapısı görülmektedir.



(Page 31-32)

2)

Sızma Adımları

Adım 1, İnternet üzerinden, arama motorlarından, mail gruplarından, DNS ve Whois kayıtlarından ve Google map'den bilgi toplanması.
Adım 2, Port taratmak, banner yakalamak, versiyon belirlemek, çalışan servislerin bulunması, kullanılan yazılımın bulunması.
Adım 3, zafiyet tarama araçları ya da manuel olarak zafiyetlerin bulunması.
Adım 4, zafiyetlerin istismar edilmesi.
Adım 5, sistemin ele geçirilmesi.
Adım 6, izlerin temizlenmesi.

(Page 33)

3)

Bilgi Toplama Aşaması

Aktif ve pasif olarak bilgiler toplanabilmektedir. Pasif bilgi toplama yönteminde sistemde iz brakılmadan açık servisler üzerinden bilgi toplanılırken, aktif bilgi toplama yönteminde sistem ile birebir iletişime geçilmektedir. Mesela domain kayıtlarını ortaya döken Netcraft sitesi pasif bilgi toplama araçlarından birisidir.

(Page 33-34)

4)

Google Hacking Dorkları

Site bazlı arama yapar.

> site: www.includekarabuk.com

Yedeği alınarak unutulmuş ve erişimi olan veritabanlarını arar.

> mysql dump filetype:sql

XLS, PDF, PPT gibi dosya uzantılarını kullanarak arama yapılmasına olanak verir.

> filetype: xslt

“robots” dosyalarını arar.

> intitle:index.of robots.txt

Konulan tüm kelimelerin birlikte yer aldığı URL’leri arar.

> allinurl: kalem kağıt defter

Com uzantılı URL’ler içerisinde /etc/passwd yazısı geçen sayfaları arar.

> inurl:/etc/passwd site:com

Title içerisindeki aramaları yapar.

> intitle:

(Page 34-35)

5)

DNS Protokolü Aracılığı İle Bilgi Toplanması

Domain Name System (DNS) isimleri IP, IP'leri de isimlere çevirmeye yarar. DNS üzerinde birtakım kayıtlar tutulur. Linux makinalarda DNS ile ilgili kayıtlar /etc/resolv.conf, /etc/hosts gibi dosyalar içerisinde tutulurken, Windows makinalarda ise c:\windows\system32\drivers\etc\hosts gibi dosyalar içerisinde tutulur. Anılan kayıt türleri aşağıda Tablo 1.2'de görülmektedir. Zone transfer yapılarak, DNS üzerinden bilgi toplanılabilir.

Ns : DNS Kayıtları

Mx: Mail Sunucu Kayıtları

Ptr: IP adresinden domaine dönüşüm kayıtları

A : Domain'den IP adresine dönüşüm kayıtları

Txt: DNS hakkında bilgi verir.

(Page 36)

6)

Nmap'in çalışma prensibinin anlaşılabilmesi için üçlü el sıkışma bayraklarının ve mantığının anlaşılması gerekir. TCP bayrakları aşağıdaki şekilde özetlenebilir:

SYN (Senkronizasyon Bayrağı): Üçlü el sıkışmanın başlaması ve senkronizasyon sağlanması için gönderilen pakettir.

SYN/ACK (Onay Paketi): Syn paketi alındıktan sonra paketi aldığına dair karşının gönderdiği pakettir. Syn/ack paketinin sıra numarası syn paketinin sıra numarasından bir fazladır.

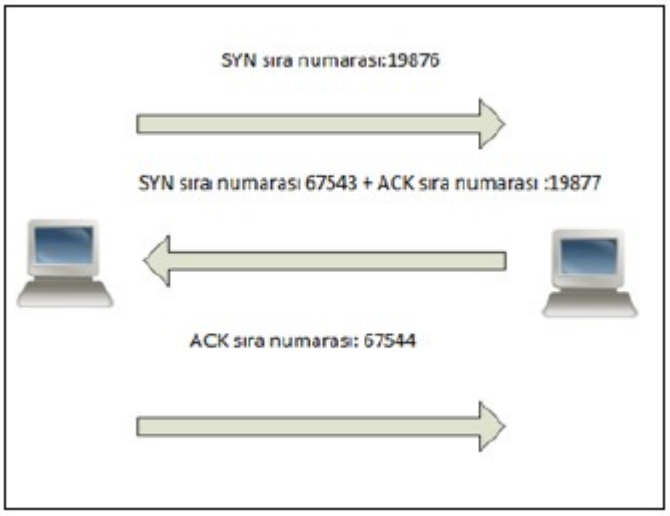
RST (Yeniden Gönderme): Datanın gönderilmesi sırasında oluşan bir sıkıntıdan dolayı yeniden gönderilmesi için gönderilen pakettir. Aynı zamanda kurulan TCP bağlantısını ani olarak sonlandırmak için de kullanılır.

PSH (Push): Datanın hızlı bir şekide tcp katmanında daha fazla bekletilmeden gönderilmesini belirten pakettir.

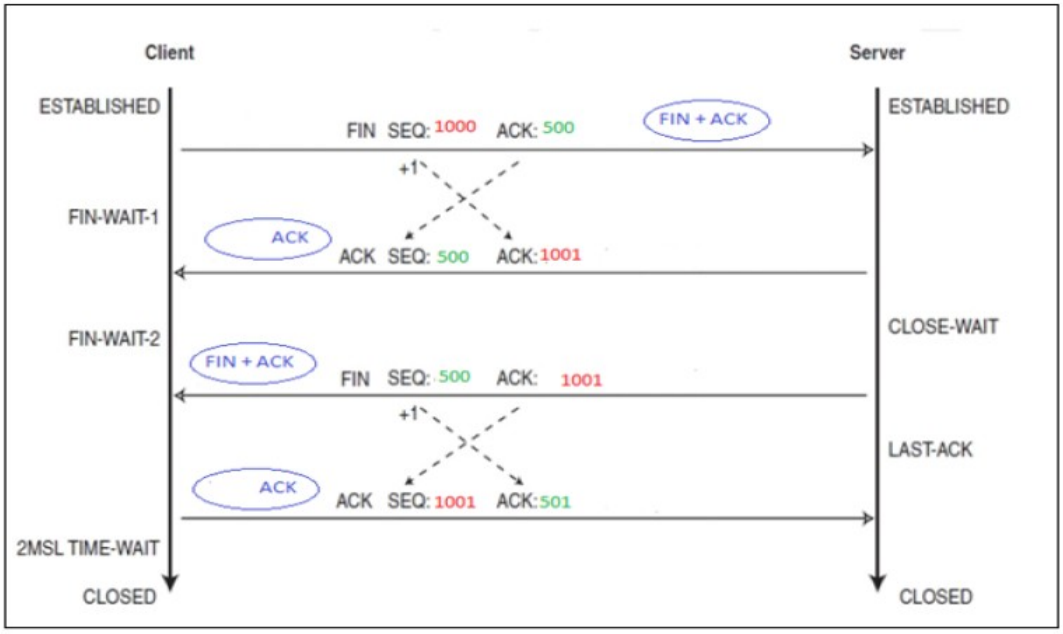
URG (Acil): Acil olarak iletilmesi gereken veriyi içeren pakettir.

CWR (Congestion Window Reduced): Tıkanmaya bağlı olarak pencere boyutunun küçültülmesi gerektiğini belirten paket.

ECE (Explicit Congestion Notification Echo): Tıkanmanın var olduğunu belirtir.



TCP oturumları yukarıdaki üçlü el sıkışma ile kurulur. Bu oturumları sonlandırabilmek için iki yöntem vardır. Bunlardan birincisinde oturumu sonlandırmak isteyen makina RST paketi yollayarak iletişimi ani bir şekilde sonlandırır. İkinci yöntemde ise iletişimi sonlandırmak isteyen makina karşı tarafa fin+ack paketi yollar. Talebi (paketi) alan karşı taraftaki makina buna karşlık önce ack paketi yollar. Hemen ardından fin+ack paketini yollar. İletişimi sonlandırmayı talep eden taraf ise ACK paketini yollayarak iletişim sonlandırılmış olur. Bu işleyişi aşağıdaki resimde görebilirsin (Client iletişimi sonlandırmak isteyen tarafı temsil etmektedir):



Nmap baz alınarak port tarama türleri ve açıklamaları kısaca aşağıdaki gibi özetlenebilir:

SYN tarama (-sS) : Hedef porta SYN paketi yollanır. Eğer port açık ise SYN+ACK paketi döner. Böylece portun açık olduğu tespit edilmiş olur ve tarama yapan taraf üçlü el sıkışmayı tamamlamamak için karşıya RST paketi göndererek bağlantıyı keser. Eğer port kapalı olsaydı karşıdan RST paketi dönerdi. Eğer karşıdan hiçbir yanıt gelmeseydi hedefin önünde bir güvenlik duvarı var olduğu düşünülürdü ve bu durumu ifade etmek için de porta filtrelenmiş(filtered) denirdi.

UDP tarama (Nmap –sU): Tarama daha yavaştır ve sonuçlar bazen yanlış çıkabilmektedir. Karşıdaki makinaya UDP paketi yollanır. Eğer karşıdan UDP cevabı geliyorsa port açık (open) olarak algılanır. Karşıdan UDP paketine cevap olarak ICMP port unreachable paketi geliyorsa (ICMP type 3 code 3) port kapalı (closed) olarak algılanır. ICMP port unreachable (type 3 code 1, 2, 9, 10, 13) mesajı dönerse port filitrelenmiş (fıltered) olarak algılanır. UDP paketine karşı herhangi bir paket gelmediği zamanlarda açık ya da filitrelenmiş (open|fıltered) olarak Nmap yorumlar.

TCP tarama (Nmap –sT): “-p” parametresi ile (–p 1-65535 şeklinde) portlar özellikle belirtilmez ise Nmap 1-1024 arasındaki portları tarayacaktır. Tarama için önce SYN paketi yollanır. SYN+ACK dönerse port açık (open) demektir. Eğer ICMP port unreachable cevabı dönerse ya da cevap dönmezse port filtrelenmiş (filtered) demektir. Eğer RST cevabı gelirse port kapalı (closed) demektir.

ACK tarama (Nmap –sA): Durum denetlemeli (stateful) güvenlik duvarlarında işe yaramaz. Hedefe ACK paketleri yollanır. Amaç açık portları öğrenmekten ziyade ağ haritası çıkartmaktır.

Versiyon tarama (-sV): Versiyon tarama sayesinde önünde SYN cookie bulunan sistemlerde hangi servislerin çalıştığı bulunabilir. Ayrıca bu tarama yöntemi ile portların arkasında çalışan servisler de tespit edilebilir.

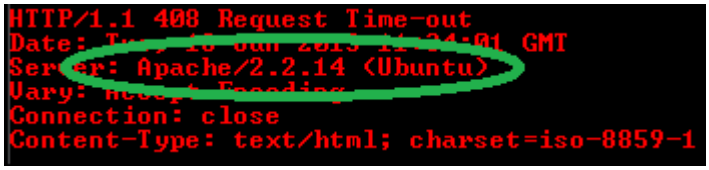
(Page 37-40)

7)

Servis Versiyon Bilgisini Alma

Banner yakalama yöntemi, hedef sistemde çalışan servis hakkında, servisin türü ve versiyonu gibi bilgilerin alınmasını sağlayan bir yöntemdir. Hedef sistemde IPS‘in olup olmadığının anlaşılması gibi husularda da kullanılır. Kullanımı aşağıdaki gibidir:

telnet 192.168.1.23 80



Dönen cevapta web sunucu versiyonu görülebilir. Eğer cevap web sunucudan dönüyorsa arada IPS olmadığı anlşılır. Hedef sistemde neyin çalıştığı bilinirse, o sisteme göre istismar kodu ile atak yapılabilir. Banner yakalamayı engellemek için L7 güvenlik duvarı veya IPS kullanılması gerekir. IPS üzerinde imza yazılarak açık portlardan gelen telnet istekleri kapatılabilir. IDS kullanılarak da gelen istekler loglanmalıdır.

(Page 40-41)

8)

Ağa Giden Yolun Belirlenmesi

Ağa giden yolların belirlenmesi için Traceroute ve tcptraceroute gibi araçlar kullanılabilmektedirler. Traceroute ve Tcptraceroute araçları, ICMP ve UDP tabanlı çalışır. Hedefe gönderilen paketlerin hangi yoldan gittiğinin anlaşılması için kulanılır. Paket yaşam süresi değeri varsayılan olarak routerlarda 256, linux makina ve switchlerde 64, windows makinalarda 128‘dir. Paket her bir cihazın üstünden geçtiğinde TTL değeri 1 birim azalır. Böylece hedefe giderken kaç router atlandığı, hatta Tcptraceroute da kullanılarak, karşı tarafta güvenlik duvarı olup olmadığı anlaşılabilir. Buna karşın, Tcptraceroute karşı sistemdeki cihazda UDP ve ICMP portları kapalı oluğu durumlarda kullanılabilir. Karşıya TCP paketi gönderir. İlk durumda güvenlik duvarı var ise güvenlik duvarının IP adresi görünmez ve **** olur. Tcptraceroute denemesinde güvenlik duvarının IP adresi görülebilir. (Page 41)

9)

IPV6‘ya geçişte ARP protokolünün yerini NDP almıştır. NDP tıpkı ARP gibi yerel ağ keşif protokolüdür.

(Page 42, 44)

10)

SSL (secure socket layer) ağda akan trafiğin gizliliğini sağlamak amacı ile netscape tarafından geliştirilmiş iki anahtarlı şifreleme sistemidir Anahtarlardan biri public, diğeri private'tır.

(Page 46)

11)

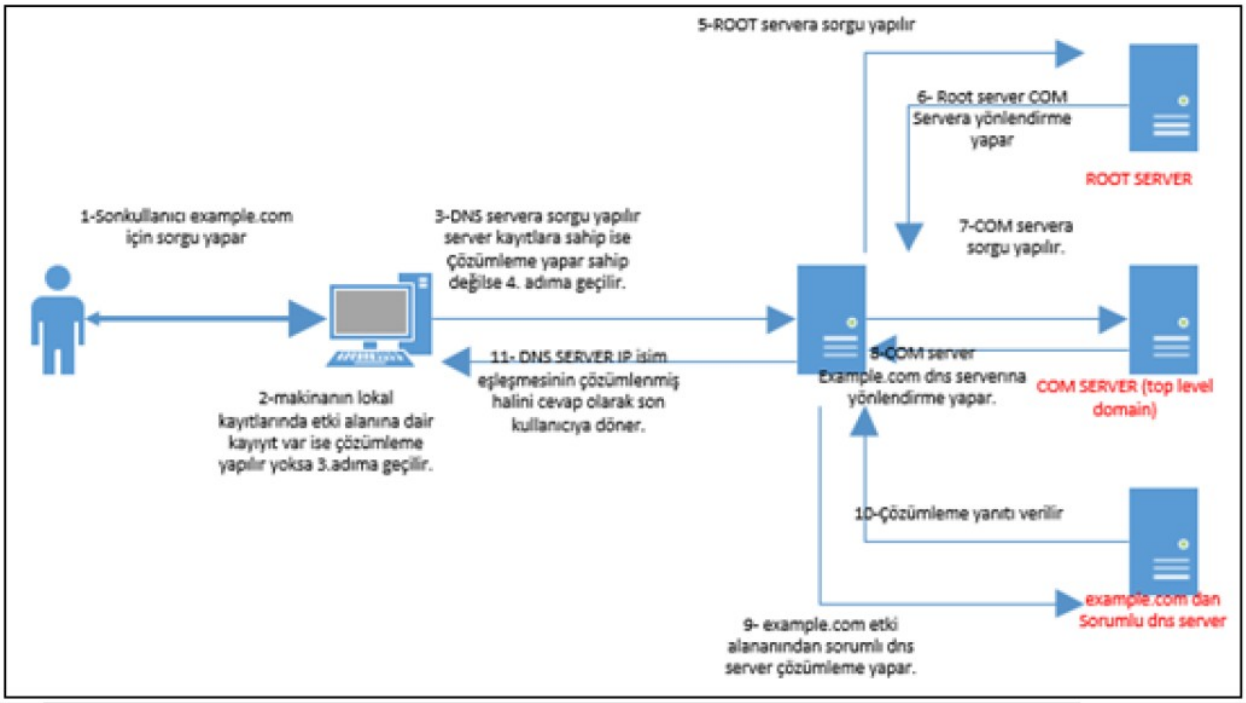
DHCP

DHCP (Dynamic Host Configuration Protocol - Dinamik Host Yapılandırma Protokolü) ağdaki makinaların IP, DNS ve ağ geçidi ayarlarının otomatik olarak yapılandırılması için kullanılır. DHCP, UDP protokolünü kullanır. Bilgisayar ilk açıldığı anda ortamda DHCP sunucu olup olmadığının kontrol edilmesi için DHCP sunucunun 68. portuna son kullanıcının UDP 67. port noktasından discovery paketi yollanılır. Şayet ağda DHCP sunucu var ise discovery paketini alan sunucu kendisine discovery paketi yollayan son kullanıcıya offer paketi yollar. Son kullanıcı offer paketini aldıktan sonra sunucuya request paketi yollar. Sunucu son kullanıcıya ACK paketi yolladığında otomatik IP yapılandırma işlemi tamamlanır

(Page 46-47)

12)

İki çeşit DNS sorgusu yapılmaktadır: İteratif ve recursive sorgular. İteratif sorgu DNS sunucular arasında yapılan sorgulara denir. Recursive sorgu son kullanıcı tarafından DNS sunucuya yapılan sorgulara denir. DNS IP-isim dönüşümü kayıtlarını üzerinde tuttuğu için güvenlik açısından en kritik sistemlerden bir tanesidir.



(Page 49)

13)

Sql açıklıklarından yararlanılarak veritabanı ele geçirilebilir **ve** sistemlere arka kapı enjekte edilebilir.

(page 32)

14)

Kablosuz ağlarda şifreleme çeşidi olan WEP RC4 algoritmasını kullanmaktadır. Orijinal metin RC4 anahtarı ile XOR işlemine tabi tutulur. Paylaşılan anahtar son kullanıcıda da bulunduğu için kendisine gelen kriptolu trafiği XOR işleminden geçirerek açar.

(Page 59)

15)

Windows Utilman.exe zafiyeti

Bu yöntemde bilgisayar Backtrack işletim sistemi ile açılır. C:\\windows\\ system32 dizini altında bulunan cmd.exe, utilman.exe üzerine kopyalanır.

```
root@bt:~# cd '/media/B054605B54602676/Windows/System32'
root@bt:/media/B054605B54602676/Windows/System32# cp cmd.exe Utilman.exe
```

Böylece windows açılırken gelen parola ekranının sağ alt köşesinde bulunan simge kullanılarak terminale erişim hakkı kazanılır.

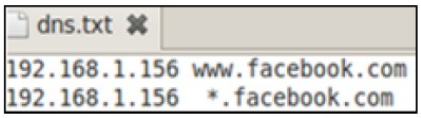
Kullanıcı oluşturularak sisteme admin yetkileri ile giriş yapılabilir. Yani oturumu şifreli olan bir windows'un oturum açma mekanizması bu şekilde bypass edilebilmektedir. (Page 62-63)

16)

DNS Spoofing (*Denedim, Çalışmadı!!! Ama teorik olarak bil*)

Ağın tümüne, yada atak yapılmak istenilen son kullanıcıya arp spoofing yapılır. Böylelikle son kullanıcının DNS isteklerine dnsspoof aracı kulanılarak cevap verilir. Son kullanıcı adres çubuğuna girmek istediği adresi yazıp enter'ladığında

dns kaydında neresi gösterilmişse oraya yönlendirilir. Mesela yönlendirilen site mevcut sitenin fake hali olabilir. Böylece son kullanıcı login bilgilerini fake siteye girerek çaldırabilir. DNS Spoof yapabilmek için önce bir dns dosyası oluşturalım:



Ardından şunlar sırasıyla farklı terminallere girilir:

> arpspoof -t 192.168.2.2 192.168.2.1

(Victim IP) (Router IP)

> arpspoof -t 192.168.2.1 192.168.2.2

(Router IP) (Victim IP)

> echo 1 > /proc/sys/net/ipv4/ip_forward

> dnsspoof -i eth0 -f /root/Desktop/dns.txt

Böylelikle kurban facebook'a giriyorum diye sahte sayfaya yönlendirilecektir. Eğer DNS Spoof yerel ağdaki değil de uzaktaki bir bilgisayara yapılmak isteniyorsa o zaman arp spoof kullanılmaz. Sadece dnsspoof kullanılır:

> dnsspoof -f /root/Desktop/dns.txt host 202.21.22.10

(Victim IP)

(Page 70-71)

17)

Switch MAC adres tablosu doldurularak switch hub cihazı gibi çalışıtırılabilir. Bu atak uzun süre devam ettirildiği zaman servis dışı bırakma atağına dönüşebilmektedir. Atak yapan kişi, switch cihazını huba dönüştürdüğü için broadcast sonucu Wireshark ile kullanıcıların tüm trafiğini görünteleyebilir hale gelmiştir.

(Page 76-77)

18)

Sayfa 40, “**3.2.1.7. Servis versiyonu bilgi alma“** başlığında kaldın.