TASK 3

Network Analiz Raporu

Muhammed Fatih YILMAZ

mfth78@hotmail.com

İçerik

- Public ve Private IP adresleri nedir? Niçin kullanılır?
- Modem IP sine nmap tarama sonuçları
- Shodan üzerinden SMB portu açık sunucuları nmap ile keşif
- SSH, FTP, HTTP, SMB protokollerini araştırıp oluşabilecek zafiyet çeşitleri hakkında bilgilendirme
- Verilen pcap dosyalarının incelenmesi

Public IP adres

Public IP adressleri internete erişim için kullanılır. Public ıp adresleri internete erişim için ISP tarafından routerlara verilir. Routuerlar bu ıp adresleri sayesinde internete erişimi sağlar. Evdeki modem üzerinden örnek vericek olursak herhangi biri internete bağlanmak istediğinde private adresi üzerinden Modemin public ıp adresiyle bağlanır sonra modem gelen isteğe göre bunu kendi içerisinde size atadığı private ıp adres üzerinden size ulaştırır. Bu sayede her cihaza farklı ıp adresi vermek yerine bir cihaza genel ıp adresi verilir ve burada ıp adres sayısından tasarruf edilmiş olunur.

Private IP adres

Private ıp adresi ise her internete erişim olan cihazın telefon,bilgisayar,araba vb. cihazların ıp adresleri vardır. 8 milyarlık dünya nüfusunda 4 milyarlık ıp adress sayısı az gelmektedir. Private ıp adresi kavramı bu noktada önemli bir rol oynamaktadır. Router kendisine bağlı olan her cihaza private bir ip adresi atamaktadır. Bu sayede internete erişim sağlayacağı zaman cihazlar bu ıp adresleriyle routera gelir router public ipsiyle internete erişimi sağlayıp istenilen veriyi o networkteki cihaza yönlendirir.

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

Bu aralıklarda bulunurlar. A,B,C classlarında bulunurlar.

Son kullanıcı internet tarafından direkt olarak erişilmek istemez private ip adresleri sayesinde bu güvenlik sağlanır.

Modem Taraması

Yaptığım Nmap taramasında bütün portları taradım. Bunların 65526 tanesi kapalı olduğundan gösterilmedi.

53 portu domain servisi sağladığından açıktı, aşağıdaki resimde gösterilen portlar açıktı. Genelde zaten 80 portu 53 protu çoğu modemde açık olur default portlar printer portu herhangi bir kullanıcı print işlemini uzak yazıcıya göndermek istediğinde bu port üzerinden haberleşme sağlanıyor. Yaptığımız tarama sonucunda hangi portların aktif olarak açık olduğunu elde ettik.

```
┌──(mfy㉿M0NsTER)-[~]
└─$ nmap -p- 192.168.2.1
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 12:44 +03
Nmap scan report for router.asus.com (192.168.2.1)
Host is up (0.010s latency).
Not shown: 65525 closed tcp ports (conn-refused)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
515/tcp   open  printer
8394/tcp  open  d2k-tapestry2
8838/tcp  open  sos
5473/tcp  open  apsolab-tags
9100/tcp  open  jetdirect
9998/tcp  open  distinct32
18017/tcp open  unknown
37029/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 8.11 seconds
```

Shodandan Bulunan Sunuculara Port Taraması

SMB portu açık olan serverlara tarama gerçekleştirdiğimizde 445 microsoft-ds ve 139 netbios-ssn portları üzerinden SMB servislerinin çalıştığını gördük. Tarama yaptığımızda bazı portlar filtrelenmişti. 25 SMTP gibi. Bu port mail transferini sağladığı için büyük ihtimalle firewall tarafından korunduğundan isteğimizi filtered olarak döndürdü.Aşağıdaki taramalarla açık olan portlara ulaşmaya çalıştım fakat sunucu bilinmeyen host diyip erişimimi engelledi.

```
┌──(mfy㉿M0NsTER)-[~]
└─$ nmap -sV 213.155.110.250
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 14:28 +03
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 45.45% done; ETC: 14:29 (0:00:13 remaining)
Stats: 0:00:28 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 63.64% done; ETC: 14:29 (0:00:15 remaining)
Nmap scan report for 213.155.110.250
Host is up (0.010s latency).
Not shown: 987 closed tcp ports (conn-refused)
PORT      STATE    SERVICE       VERSION
25/tcp    filtered smtp
80/tcp    open     http          Microsoft IIS httpd 10.0
135/tcp   open     msrpc         Microsoft Windows RPC
139/tcp   open     netbios-ssn   Microsoft Windows netbios-ssn
179/tcp   filtered bgp
443/tcp   open     ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
445/tcp   open     microsoft-ds?
1801/tcp  open     msmq?
2103/tcp  open     msrpc         Microsoft Windows RPC
2105/tcp  open     msrpc         Microsoft Windows RPC
2107/tcp  open     msrpc         Microsoft Windows RPC
3389/tcp  open     ms-wbt-server Microsoft Terminal Services
5357/tcp  open     http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.60 seconds
```

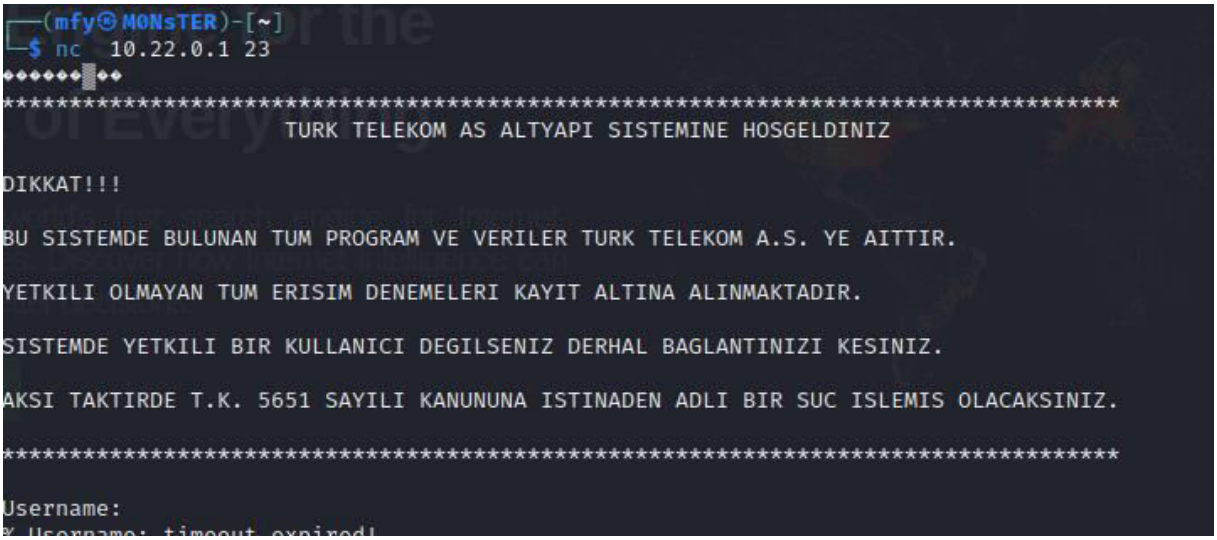
```
Host is up (0.019s latency).
Not shown: 65519 closed tcp ports (conn-refused)
PORT      STATE    SERVICE          VERSION
25/tcp    filtered smtp
135/tcp   open     msrpc            Microsoft Windows RPC
139/tcp   open     netbios-ssn      Microsoft Windows netbios-ssn
445/tcp   open     microsoft-ds     Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp  open     ssl/ms-wbt-server?
4786/tcp  filtered smart-install
5985/tcp  open     http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
11211/tcp filtered memcache
47001/tcp open     http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open     msrpc            Microsoft Windows RPC
49153/tcp open     msrpc            Microsoft Windows RPC
49154/tcp open     msrpc            Microsoft Windows RPC
49155/tcp open     msrpc            Microsoft Windows RPC
49156/tcp open     msrpc            Microsoft Windows RPC
49157/tcp open     msrpc            Microsoft Windows RPC
49158/tcp open     msrpc            Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

```
┌──(mfy㉿M0NsTER)-[~]
└─$ nc -vz 185.162.146.145 139
Warning: forward host lookup failed for hosted-by.bogahost.com: Unknown host
hosted-by.bogahost.com [185.162.146.145] 139 (netbios-ssn) open

┌──(mfy㉿M0NsTER)-[~]
└─$ nc -vz 185.162.146.145 445
Warning: forward host lookup failed for hosted-by.bogahost.com: Unknown host
hosted-by.bogahost.com [185.162.146.145] 445 (microsoft-ds) open

┌──(mfy㉿M0NsTER)-[~]
```

Hocam ayrıca Starbucks'ın wifisine girmeye çalıştım telnet portunda şöyle bi mesajla karşılaştım zorlamadım. :)



SSH nedir ?

SSH internet üzerinden kullanıcıların sunucularını kontrol etmesini sağlayan bir protokoldür. Telnet'in daha güvenli encryptlenmiş halidir. SSH şifreleme teknikleriyle uzaktaki sunucuya giden ve uzaktaki sunucudan gelen ilteşimin şifrelendiğinden emin olur. Uzak makineyle güvenli bir iletişim sağlamak için kullanılır. Uzaktaki kullanıcının kimliğini doğrulamak clientten ana pcye girişleri aktarmak ve çıktıyı geri göndermek için bir mekanizma sağlar.

3 tip şifreleme tekniği vardır

1)Simetrik şifreleme:

Burada şifreyi çözmek ve oluşturmak için gizli anahtar kullanılır oluşturulan anahtarlar sayesinde her iki tarafta şifreyi çözüp güvenliği sağlayabilir. Fakat burada naahatar 3. kişilerle paylaşılmaz. Gönderilen mesajlarda anahtarlar yollanılmaz. Anahtar takas algoritmasıyla 2 ortak verilerini paylaşır bu paylaşılan veriler gizli anahtarları hesaplamak için kullanılır. 3. kişi bu veriyi yakalasada takas algoritması bilinmediğinden anahtarı hesaplayamaz.

2) Asimetrik Şifreleme:

Burada public key dağıtılır private key ile şifre çözülür. Bir makinenin public keyi ile oluşturulan mesaj yine o makinenin private keyi ile çözülür. 3. kişiye private key ulaşmamalıdır. Yalnızca simetrik şifrelemenin anahtar takas algoritmasında kullanılır. Güvenli bağlantı kurmadan önce her iki taraf geçici public private anahtar çifti oluşturur ve bu public anahtarları ortak bir gizli anahtar oluşturmak için paylaşırlar.

3) Hashing

Hash algoritmalarıyla birlikte şifrelenen oturum sonucunda tek yönlü şifreleme gerçekleşir. Hashle oluşturulan şifrelenmiş mesajı eski haline çeviremezsin oluşan hashle hash algoritmasında oluşturulan diğer ifade karşılaştırılarıak şifrelenmenin doğru olup olmadığını kontrol edilir. Bu işlem HMAC'ler ile sağlanır.

FTP Nedir ?

FTP(File Transfer Protocol) adındanda anlaşılacağı üzere dosya transfer işlemleri gerçekleştirilir. 2 ayrı kanal üzerinden iletişim sağlanır İlki komut kanalı olarak adlandırılır. Diğeri ise veri dağıtımının gerçekleştiği veri kanalıdır. FTP basitçe dosyaların internet üzerinde 2 bilgisayar arasında alış-veriş yapmasını sağlayan protokoldür genellikle 21 ve 22 portları üzerinden erişim sağlanır.

HTTP nedir ?

Hyper Text Transfer Protocol bu protocol kullanıcı ve sunucu arasında veri alışverişinin kurallarını belirler. TCP/IP tabanlı bir iletişim protokolüdür. Bu protokol internet üzerinde en sık kullandığımız protokoldür. HTTP durumsuz bir protokoldür. Yani her istek birbirinden bağımsız olarak değerlendirilir. Arama çubuğunda yazılan bir girdinin gelmesi bu protokol sayesinde gerçekleşir. İstediğimiz dökümanı internetten çekmek istediğimizde arka planda oluşan GET komutuyla request atar serverda bu requeste bir response döner bu sayede sayfanının gelip gelmediği anlaşılır.HTTP genellikle 80 portunu kulnanır. HTTP response içinde durum kodları mevcuttur. Bu kodlara göre yapılan requestin nasıl sonuçlandığı anlaşılabilir.

1xx Bilgi

2xx Başarı

3xx Yönlendirme

4xx Tarayıcı Hatası

5xx Sunucu Hatası

HTTP protokolünde istekler vardır. Bu istekler sayesinde veriyi göndermek değiştirme isteme gibi işlemler gerçekleşir POST,GET,DELETE,UPDATE işlemleri örnek verilebilir bunlar genellikle HEADER'a eklenir.

SMB nedir?

Server Message Block protocol bir ağdaki dosyalara, yazıcılara seri bağlantı noktalarına ve paylaşılan diğer kaynaklara erişimi sağlamak için kullanılan protokoldur. Windows tabanlı bir protokoldür. Cihazlar arası mesajlaşma vb işlemlerini sağlamak amacıyla ortaya koymuştur.

Buradan herhangi bir smb protu açık olan uzak sunucuya bağlanıp gerekli işlemleri gerçekleştirebiliriz. Eski versiyonlarında Netbios üzerinden 139 portunda işlem görürken yeni cihazlarda direkt olarak TCP/IP protokolü üzerinden 445 protunda çalışmaktadır. Uçtan uca şifreleme kullanılır.

Oluşabilecek ZAAFİYETLER

Bence bu portların açık olmasında özellikle FTP portunun istenmeyen dosyalar transfer edilip buradaki bilgisayar malware dosyaları aktarılabilir ama bunun için kullanıcı bilgisi ve şifresi de bilinmesi lazım buradaki şifreleme işlmeinide brute forcela kırılabilir. Ayrıca şifreleri encrypt mekanizması olmadığından eğer kullanılmazsa hackerlar tarafından kolayca bulunabilir. Bunula birlikte dizin geçiş saldırılarıyla root kullanıcısını manipüle edip gerçek FTP sahibine istediği izinleri vermeyip kısıtlayabilir. XSS ile hackerlar kullanıcılara zararlı scriptleri FTP üzerinden transfer edebilir. Bunu anlayamayan browser sonucunda hackerlar kendi kodlarını diğer kullanıcılar üzerinde çalıştırabilir.

SSH zaafiyeti olarakta herhangi bir kullanıcı private keyi elde ettiğinde serverlara erişim sağlayabilir. Örneğin şirkette çalışan bir çalışan daha sonrasında ayrılıp ona ait olan keyler silinmediyse ve bu keyler kopyalanıp farklı kullanıcılar tarafından kullanılıp istenmeyen sonuçlar elde edilebilir. Loglar takip edilir fakat sisteme çoktan zarar gelmiştir. SSH configlerini değiştirmekte zaafiyetlere yol açabilir. Şifrelerle giriş açılarak brute force saldırılarına karşı zaafiyet oluşabilir. Man in the middle attackla ele geçirilebilecek keylerle erişilip zaafiyetler ortaya çıkabilir. Burada önemli noktalardan biri keylerin güvenliği, bu da kullanıcı hatasıyla veya remote attackala ele geçirilebilir.

HTTP Zaafiyetleri

En çok kullanılan protokol olduğundan ve kullanıcı girişlerine izin verdiğinden en kritik zaafiyetler bu protokolde oluşur XSS, SQL Injection, Session Hacking, IDOR çünkü genelde kullanıcılar HTTP protokolünü internet üzerinde kullandıklarından ve Application Layerda kullanıldığından HTML dosyalarıda bu protokolle çağırıldığından kullanıcıların inputları önemli bir hal alır, istenmeyen inputlarla kullanıcı bu protokol üzerinden farklı dosyalara ve databaselere erişim sağlayabilir. Örnek verecek olursak arama çubuğuna yazdığımız rastgele bir metin sorgulanmak için HTTP protokollerini de kullanarak database'a bağlanıyor burada yanlış bir kod hatası ile database istenmeyen kişiler tarfından erişim sağlanabilir. Arkada farklı kodlar çalıştırılabilir.

SMB Zaafiyetleri

Smb zaafiyetleri genelde RCE remote code execution dan dolayı kaynaklanır SMB nin amacı zaten local dosyalara veya printer gibi cihazlara kullanıcıların network üzerinden bağlanmasını sağlamaktır. Burada zaafiyet bulunup hedeflenen adreslere zararlı paketler gönderilebilir.

PCAP İnceleme

1.

IM Buddy ismi --- sec558user1

IM mesajlaşmasındaki ilk cümle -- ->Here's the secret recipe... I just downloaded it from the file server. Just copy to a thumb drive and you're good to go >:-)

gönderilen dosyanın adı ---- recipe.docx

transfer edilen dosyanın magic number ı nedir → 50 4B 03 04 14 00 06 00

transfer edilen dosyanın md5 değeri nedir → 8350582774E1D4DBE1D61D64C89E0EA1

transfer edilen dosya kime gönderilmiştir → 192.168.1.159

tshark, tcpdump, argus, strings, rahost, racluster, xxd, foremost, grep, cat, uniq, sort, awk, xxd, tcpflow, vbü

2.

kadının email adresi ve şifresi nedir? --→sneakyg33k@aol.com,

kadının yazıştığı adamın mail adresi nedir. --

→sec558@gmail.com ,mistersecretx@aol.com,

kadın adamdan getirmesini istediği 2 şey nedir --→ Fake pasaport ve mayo

gönderilen dosyanın adı ne → secretrendezvous.docx

gonderilen dosyanın checksum ı ne -->9e423e11db88f01bbff81172839e1923

randevu mekanı neresi? --→ Playa del Carmen, Mexico

dokumandaki imajın checksum ı ne --→ aadeace50997b1ba24b09ac2ef1940b7

3.

appleTV nin MAC adresi --- > 00:25:00:fe:07:c4

appleTV ye giden http isteğinde kullanılan useragent --- > APPLETV/2.4

appletv de search edilen ilk kelime --- > h,ha,hac,hack,s,sn ilk kelime hack tam olarak

appletv de tıklanan ilk film --- > Hocam wireshark kullandım bunu bulmak için grep GET komutuyla tsharktan Http isteklerini çekmiştim tıklananı tahmin ettim Getlerin hepsinde q?=h,ha diye giderken viewMedia id diye bir parametre ortaya çıktı tıklanan filmin id parametresi olarak düşündüm ardından wireshark programına girip getlerin içinden o parametreyi taratıp HTTP stream yaptım ismini buldum Hackers

ikinci filmin fiyatı --- > Bunu diğer tıklanan film olarak düşündüm yine aynı şekil bunun ID'sini getlerin içinde aratıp wiresharktan 9.99 dolar sonucuna ulaştım. Filmin ismi Sneakers

son full arama appleTV --- > iknowyourewatchingme

4.

1) Saldırganın IP adresi – -- > 10.42.253.253

2) ilk gerçekleştirilen portscan ne tip bir portscan --- > Bunu anlamak için Başlangıçta Syn de de TCP connect Scan da da aynı işlem gerçekleşiyor ikisinde de açık olan bir portu buldum ACK SYN bayraklarını 1' e eşit olduğu yerleri getirdim. FAKAT SYN scan daki gibi açık olduğunu görünce direkt RST atmamış bi tane ACK yollamış yani 3 way handshake gerçekleşmiş bu yüzden TCP connect olduğunu düşündüm.

3) hedef olarak tespit edilen IP adresleri, -- >

10.42.42.25 ,10.42.42.50 ,10.42.42.56

4) saldırgan tarafından bulunan windows sistemin IP adresi --- > Windows Sistemini bulmak için araştırdığımda 2 tane fingerprint buldum birisi TTL diğer Length , TTL tablosuna bakıp windowsun 128 olduğunu öğrendim, ICMP paketlerini tshark komutuyla getirip TTL sürelerine baktım bunun sonucunda 10.42.42.50 nin Windowsa ait olduğunu öğrendim

5) bu windows sistemde hangi portlar açık - - → Bunu bulabilmek için TCP connect yaptığından hackerın bağlandığı portla bağlantısını kesebilmesi için RST yollaması lazım bu yüzden tsharkla 10.42.42.50' ye giden RST flaglarını taradım sonucunda 139 ve 135 portlarının açık olduğunu anladım.

6)

saldırgan sizce hangi aracı kullanmış olabilir portscan sırasında. davranış neye benziyor --- >

Benim bildiğim nmap'in -sT opsiyonunu kullanmış olabilir. Çünkü aynı sistem nmap'in TCP connect taramasında da gerçekleştiriliyor.