DENEY FÖY - 4

DERS: WEB LABORATUVAR

KONU: GÜVENLİ YAZILIM GELİŞTİRME VE GÜVENLİK TESTLERİ

ADI:AYŞEGÜL

SOYADI: AKMAN

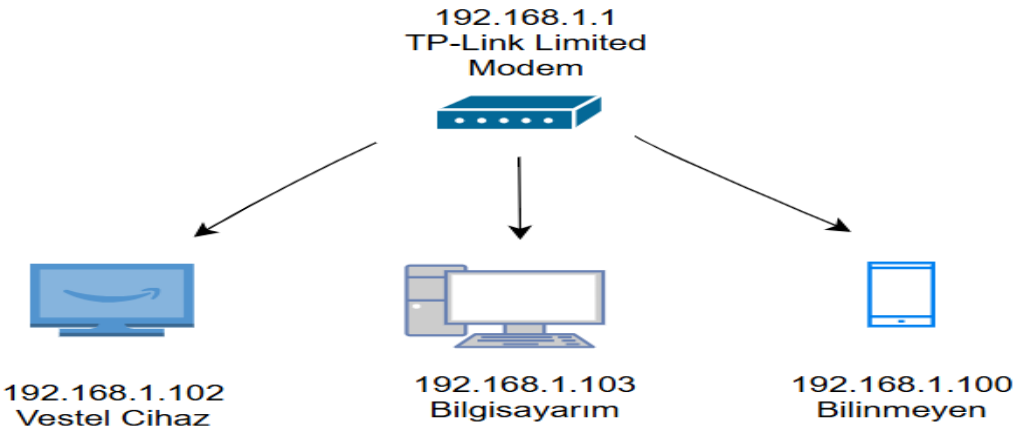
NUMARA: 21060684

Madde 1: Zafiyet testi ve sızma testinin farkları nelerdir?

- Zafiyet testi sistemlerde mevcut olan güvenlik açıklarını hızlıca tespit eder, sızma testi ise bulunan açıkların ciddiyetini ve nasıl kullanılabileceğini belirler.
- Zafiyet testi hızlı, otomatik ve yüzeysel bir test iken sızma testi manuel, derinlemesine ve daha kapsamlı bir testtir.
- Sızma testi zafiyet testinden elde edilen bilgiler eşliğinde yapılır.

Madde 2: Nmap aracı ile yerel ağ üzerinde şu işlemleri gerçekleştiriniz:

a) Ağda bulunan bilgisayarların keşfini gerçekleştiriniz. Basit bir şekil ve tanımlarıyla bu ağı gösteriniz.




```
C:\Users\Aysegul>nmap -sn 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 00:07 T"rkiye Standart Saati
Nmap scan report for 192.168.1.1
Host is up (0.0099s latency).
MAC Address: 40:ED:00:D1:FB:16 (TP-Link Limited)
Nmap scan report for 192.168.1.100
Host is up (0.0070s latency).
MAC Address: 02:86:F6:74:ED:F0 (Unknown)
Nmap scan report for 192.168.1.102
Host is up (0.010s latency).
MAC Address: 90:98:77:99:60:0F (Vestel Elektronik San ve Tic. A.S.)
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.12 seconds
```

```
C:\Users\Aysegul>nmap -sP 192.168.1.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 00:45 Tªrkiye Standart Saati
Nmap scan report for 192.168.1.1
Host is up (0.0056s latency).
MAC Address: 40:ED:00:D1:FB:16 (TP-Link Limited)
Nmap scan report for 192.168.1.100
Host is up (0.039s latency).
MAC Address: 02:86:F6:74:ED:F0 (Unknown)
Nmap scan report for 192.168.1.102
Host is up (0.0070s latency).
MAC Address: 90:98:77:99:60:0F (Vestel Elektronik San ve Tic. A.S.)
Nmap scan report for 192.168.1.103
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.11 seconds
```

Burada iki farklı komut ile aynı sonucu elde ettim:
-sn parametresi ile sadece hangi makinelerin ayakta olduğunu görüntüleriz.
-sP parametresiyle ping scan yapmış olduk. Bu keşfetme işlemlerinden biridir.

Buradaki:
192.168.1.1 -> Router veya Modem
192.168.1.100 -> Aktif herhangi bir cihaz
192.168.1.102 -> Vestel firmasına ait bir cihaz
192.168.1.103 -> Bu kullanmış olduğum bilgisayar

b) Bilgisayarınızda çalışan servislerin kullandığı port numaralarını bularak bu servislerin ne işe yaradıklarını anlatınız. (örneğin SSH) en az 2 servis açmaya çalışınız ve bu servisleri anlatınız.

```
C:\Users\Aysegul>nmap -sT 192.168.1.103
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 03:25 Tªrkiye Standart Saati
Nmap scan report for 192.168.1.103
Host is up (0.0019s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 5.32 seconds
```

```
C:\Users\Aysegul>nmap -sS -v 192.168.1.103
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 00:52 Tªrkiye Standart Saati
Initiating Parallel DNS resolution of 1 host. at 00:52
Completed Parallel DNS resolution of 1 host. at 00:52, 0.02s elapsed
Initiating SYN Stealth Scan at 00:52
Scanning 192.168.1.103 [1000 ports]
Discovered open port 8080/tcp on 192.168.1.103
Discovered open port 3306/tcp on 192.168.1.103
Discovered open port 135/tcp on 192.168.1.103
Discovered open port 139/tcp on 192.168.1.103
Discovered open port 445/tcp on 192.168.1.103
Discovered open port 5357/tcp on 192.168.1.103
Completed SYN Stealth Scan at 00:52, 0.03s elapsed (1000 total ports)
Nmap scan report for 192.168.1.103
Host is up (0.00014s latency).
Not shown: 994 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5357/tcp open  wsdapi
8080/tcp open  http-proxy
```

-sS: Syn taraması yapar.

-v: ekrana gösterilecek detayları arttırır.
-sT: TCP bağlantı taraması yapar.

8080/TCP: HTTP Proxy -> Bir web sunucusu veya proxy çalışıyor.
3306/TCP: MySQL -> Bir MySQL veritabanı sunucusu çalışıyor.
135/TCP: Microsoft RPC
139/TCP: NetBIOS-SSN -> Windows dosya paylaşımı veya NetBIOS hizmeti
445/TCP: Microsoft-DS -> Dosya ve yazıcı paylaşımı için kullanılır.
5357/TCP: WSDAPI -> Web hizmeti algılama protokolü. Genelde cihaz keşfinde kullanılır.

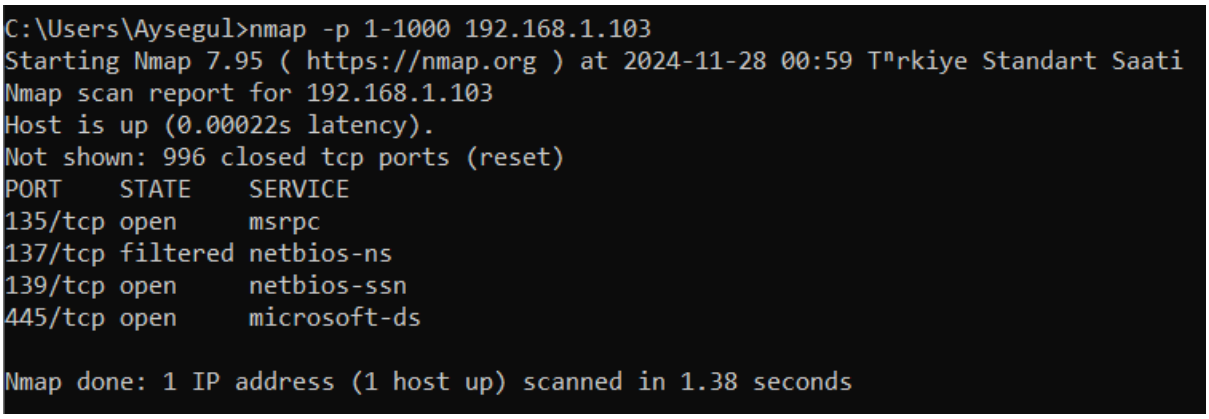
c) Tek bir IP (yerel makine IP adresi) kullanarak port taraması yapınız ve elde edilen sonuçları düzgün bir şekilde yorumlayınız.

```
C:\Users\Aysegul>nmap -p 1-65535 192.168.1.103
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-28 00:53 T"rkiye Standart Saati
Nmap scan report for 192.168.1.103
Host is up (0.0000030s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE    SERVICE
135/tcp   open     msrpc
137/tcp   filtered netbios-ns
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds
3306/tcp  open     mysql
5040/tcp  open     unknown
5357/tcp  open     wsdapi
7680/tcp  open     pando-pub
8080/tcp  open     http-proxy
33060/tcp open     mysqlx
49664/tcp open     unknown
49665/tcp open     unknown
49666/tcp open     unknown
49667/tcp open     unknown
49668/tcp open     unknown
49670/tcp open     unknown
```

-p: Bir IP üzerinden bulunması muhtemele 65535 portun hepsini tarar.
Host is up: Cihazın erişilebilir olduğunu belirtir.
Burada açık portlar görüntülenmektedir.
Geri kalan 65519 tcp portu kapalı.
msrpc: Windows RPC hizmeti
netbios-ns: Ağda cihaz keşfi ve dosya paylaşımı için
netbios-ssn: Windows dosya paylaşım hizmeti
microsoft-ds: dosya ve yazıcı paylaşımı için
mysql: MySQL veritabanı sunucusu
unknown: Belirlenemeyen servis

wsdpapi: Windows cihaz keşfi için
pando-pub: Olası bir medya paylaşım veya yazılım güncelleme servisi
http-proxy: HTTP proxy veya bir web sunucu çalışıyor olabilir
mysqlx: MySQL'in X protokolü - Modern API desteği sunar

d) Yerel makine üzerindeki 1 ve 1000 nolu portlar arasındaki bütün portları tarayan komutu yazınız ve çıkan sonuçları yorumlayınız.

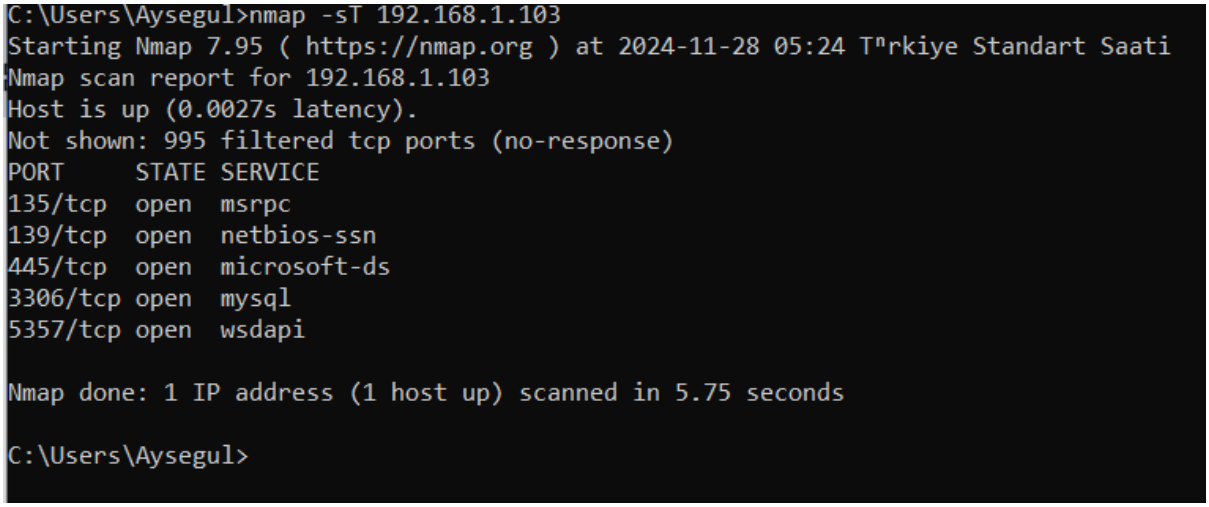


Burada 996 TCP portu kapalı durumda
-p: Bir IP üzerinden bulunması muhtemele 65535 portun hepsini tarar. Ama biz sadece 1000 port tarayacağız.

135 portu Windows RPC hizmeti
137 portu ağda cihaz keşfi ve dosya paylaşımı için
139 portu windows dosya paylaşım hizmeti
445 portu bir SMB protokolü, dosya ve yazıcı paylaşımı için

e) TCP bağlantı taraması nedir? TCP bağlantı taraması gerçekleştiriniz.

Hedef porta bağlanmak için SYN paket gönderir, karşılığında SYN+ACK paketi gelirse ACK paketi göndererek porta bağlanır ve portun açık olduğunu, RST+ACK cevabı gelirse portun kapalı olduğunu rapor eder.
3 farklı parametre ile TCP taraması bulunur:
-sS(TCP SYN taraması), -sA(TCP ACK taraması), -sT(TCP bağlantı taraması)



Madde 3: Vega aracı ile localhost üzerinde çalışan bir web uygulamasına zafiyet testi gerçekleştiriniz ve çıkan sonuçları yorumlayınız. Çıkan hatalardan bir tanesini nasıl kullanabileceğiniz ile ilgili bir örnek veriniz. (Kullanabileceğiniz yerel uygulama önceki föylerde yaptığınız uygulamalardan birisi olabilir.) (Vega indirilmiyor. İşlem uzun sürdü hatası veriyor.)

Madde 4: Kara kutu ve beyaz kutu test yöntemleri nedir? Birbirlerinden farklılıkları nelerdir?

Kara kutu test yöntemi, sistemin, yazılımın iç yapısı hakkında bilgi sahibi olmadan yani koda bakılmadan sistemin işlevselliğini ölçmeye yarayan test tekniğidir. Amaç gereksinimleri karşılayan çıktıların alınıp alınmadığını ölçümlemektir.

Beyaz kutu test yöntemi, şeffaf kutu testi de denmektedir. Yazılımın kodunun iç yapısının bilinerek ve ölçümlenerek test senaryolarının tasarlandığı tekniktir. Ana amaç kod parçacıklarının tek tek test edilerek aslında küçük parçacık halinde bile sağlıklı bir şekilde çalıştırılabildiğinin görülmesidir. Yazılımın işlevselliği test edilmez.

Farkları:

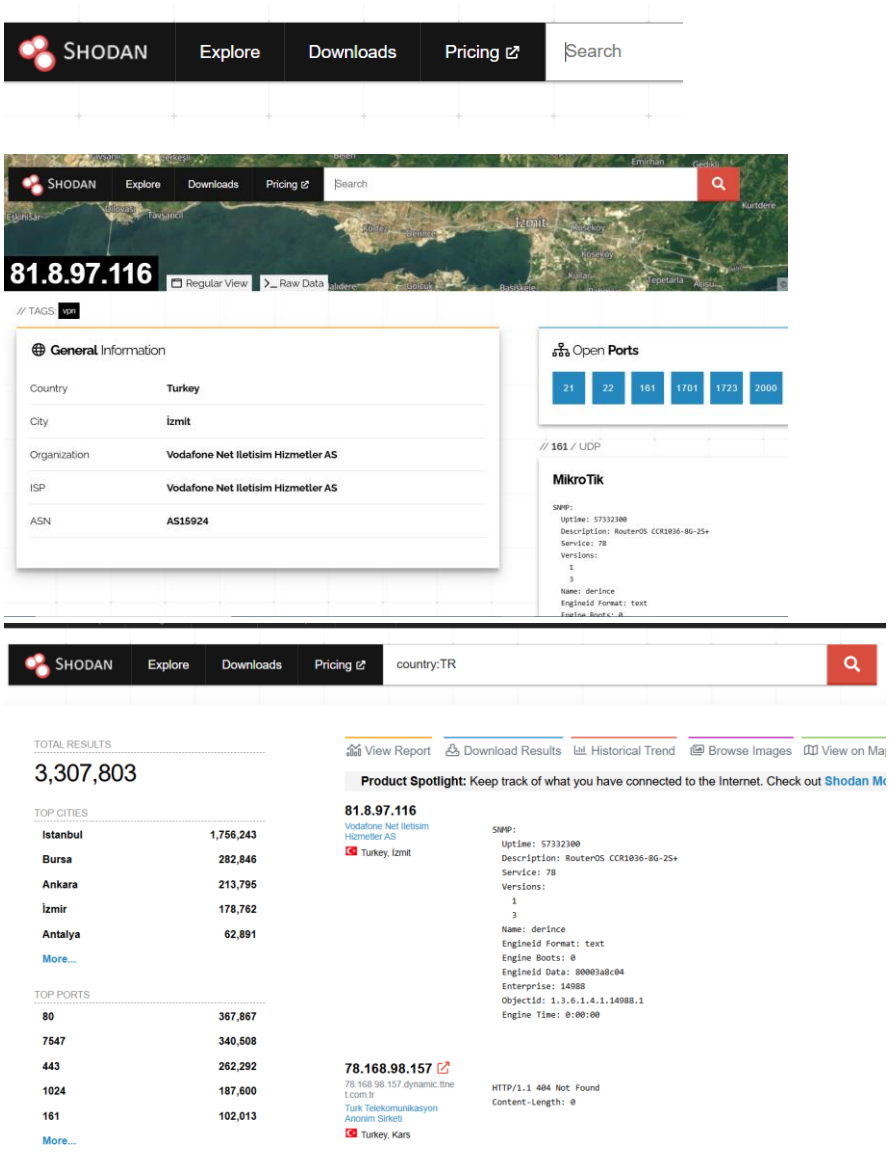
Kara kutu da bir bilgi sahibi olmak gerekmez, beyaz kutu da kodun iç yapısı ile ilgili detaylı bilgilere sahip olmalıyız.

Kara kutu testi hızlıdır ama beyaz kutu testi ayrıntılı ve kapsamlı olduğu için yavaştır bu nedenle çok uzun zaman alabilmektedir.

Madde 5: (Bonus) Shodan.io aracını araştırınız. Örnek bir kullanım senaryosu gösteriniz. Elde ettiğiniz sonuçları yorumlayınız.

Shodan'da internete bağlı her cihazın ya da makinenin bir kaydı vardır. Çok büyük bir veritabanına sahiptir. Bir nevi internet ile ilgili her şeyi bilen bir yapay zeka gibidir.

Shadon' ın parametre yazarak detaylı arama özelliğinden faydalanmak için üye olmak gerekli. Üye olunca bize başka platformlarda da Shodan'ın veri tabanını kullanabilmek için bir API-Key verecektir. Basit aramaları üye olmadan da yapabiliriz.



API –Key'e profil kısmından ulaşabiliriz.

Burada önce üye oldum ve daha sonra arama kısmına "country:TR" yazarak ülkemizdeki ağa erişimi olan cihazları görüntüledim. Eğer istersem bir portu kullanan cihazları ya da bir şehirdeki cihazları görüntülemek gibi işlemler içinde arama yapabilirim.