190541070 - Esra ÇELİK

Merhaba ben Esra Çelik Bilgi Sistemleri Güvenliği dersinde Grup-4 üyesiyim. Nmap araştırmasında Büşra Cin, Fatma Göksu Çalıkoğlu ve Yonca Ray ve arkadaşımla birlikte görev aldım.

Nmap sunumu yaparken bana düşen görev nmap teki tarama türlerini araştırmak ve sunmaktı.

Nmap tarama türleri olarak ;

- **TCP SYN(Stealth) Scan (-sS)**
- **TCP Connect Scan (-sT)**
- **UDP Scan (-sU)**
- **TCP NULL, FIN, Xmas Scans (-sN, -sF, -sX)**
- **TCP ACK Scan (-sA)**
- **TCP Window Scan (-sW)**
- **TCP Idle Scan (-sI)**
- **IP Protocol Scan (-sO)**

bu tarama türlerini araştırdım ve arkadaşlarıma sundum arkadaşlarım kısa ve öz olması için bu araştırmalarım içinde 4 tanesini sunmamı istedi. Kısacası onlarda bunlardı.

1)TCP SYN(Stealth) Scan (-sS) : TCP portlarını taramanın en hızlı yolu olduğu için en popüler tarama türüdür. Hedef sisteme bir SYN bayraklı TCP paketi gönderilerek gelen cevap doğrultusunda portun açık olup olmadığı tespit edilmektedir. Gönderilen SYN paketine, SYN/ACK paketi ile cevap gelirse hedef port açıktır. RST paketi ile cevap dönerse hedef port kapalıdır. Herhangi bir cevap gelmezse port filtreli sonucunu elde edilir. Alınan SYN/ACK paketine RST paketi gönderilip bağlantı düşürülür.

Bu taramayı gerçekleştirmek için aşağıdaki komut kullanılmalıdır : nmap -sS -v [Hedef_IP]

2)UDP Scan (-sU) : Sistemlere yönelik taramalarda sadece TCP portlarına yönelik taramalar gerçekleştirmemek gerekir. Çünkü UDP portlarına yönelik güvenlik açıkları da bulunmaktadır. Nmap üzerinden UDP taraması gerçekleştirmek için –sU parametresi kullanılır. UDP portlarını tespit etmek için UDP paketleri gönderilmektedir. Cevap olarak ICMP port Unreachable hatası döndürülürse port kapalıdır. UDP paketi ile cevap dönerse port açıktır. Herhangi bir cevap alınmadığında port açık veya filtreli olabilir.

3) IP Protocol Scan (-sO): Bu tarama türü teknik olarak port taraması değildir. Hedef sistem üzerinde hangi protokollerin çalıştığını tespit etmek için kullanılır. –p parametresi kullanılarak port numarası yerine protocol numarası yazılmaktadır. –p parametresinin protokol veya port taraması olup olmadığının ayırt edilebilmesi için –sO parametresi kullanılır. –p parametresine atanan protokol numarası ile IP Protocol taraması gerçekleştirilir. Çıktı formatı normal formata benzemektedir. Fakat numaralarının yazıldığı yerde protokol yazılmıştır.

4) TCP Connect Scan (-sT): TCP Connect Scan taraması genellikle yetkisiz Unix makinelerine ve IPv6 hedeflerine yönelik yapılmaktadır. Ayrıca TCP SYN Scan taramasını çalışmadığı veya yetersiz kaldığı durumlarda işlem görmektedir. Nmap aracı, işletim sistemi üzerinden connect system çağrısında bulunarak hedef makine ile port üzerinden bağlantı kurulmasını sağlayacaktır. Böylelikle port taramaları gerçekleştirilmektedir.

Penetrasyon sızma testinde Tüm Grup olarak Muş TSO'yu yapmayı seçtik. Ön raporumuzda sızma test aracı olarak sadece netsparker üzerinde bir tarama yaptık ve tarama sonucundan çıkan zaafiyetleride grup olarak kendi aramızda böldük, buradaki görevim Insecure Frame (External) (Güvensiz Çerçeve) ve Internal Server Error(İç Sunucu Hatası) araştırıp nasıl bir çözüm bulmamız gerektiğini çalışıp sunmayı kararlaştırdık.

Insecure Frame (External) (Güvensiz Çerçeve) :IFrame korumalı alanı, potansiyel olarak kötü amaçlı kodunun, onu gömen web sayfasına zarar vermesini kısıtlamak için bir çerçeve içindeki içerik için bir dizi ek kısıtlama sağlar. Aynı Köken Politikası (SOP), bir kaynaktan gelen JavaScript kodunun, farklı kökenlerin özelliklerine ve işlevlerine ve HTTP yanıtlarına erişmesini engeller. Erişime yalnızca aşağıdaki durumlarda izin verilir: protokol, bağlantı noktası ve ayrıca etki alanı tam olarak eşleşir.

Çözüm Prosedürü
Satır içi çerçevede korumalı alan uygulama Güvenilmeyen içerik için, sorunsuz öznitelik ve sandbox özniteliğinde üstte gezinmeye izin ver, açılır pencerelere izin ver ve komut dosyalarına izin ver özelliğini kullanmaktan kaçının.

Satır içi çerçevede korumalı alan uygulama

<iframe korumalı alan src="framed-page-url"></iframe>

Internal Server Error(İç Sunucu Hatası): Invicti Standard bir dahili sunucu hatası tespit etti. Sunucu, sunucu tarafında bir hata olduğunu belirten bir HTTP durumu 500 ile yanıt verdi. Sebepler değişebilir ve davranış dikkatlice analiz edilmelidir. Invicti Standard bir güvenlik sorunu bulabilirse aynı kaynakta, bunu ayrı bir güvenlik açığı olarak bildirir. Etki, duruma bağlı olarak değişebilir. Genellikle bu, yetersiz kodlama uygulamalarını, yeterli hata denetimi, temizleme ve beyaz listeye alma olmadığını gösterir. Ancak, daha büyük bir sorun olabilir, SQL enjeksiyonu gibi. Bu durumda, Invicti Standard diğer olası sorunları kontrol edecek ve bunları ayrı olarak bildirecektir.

Çözüm Prosedürü

Hatayı aldığınız dizine giriş yaparak dosya veya klasörlerin CHMOD değerlerini kontrol edin ve 777 değerindeki CHMOD değerlerini maksimum 755 olarak güncelleyin.

.htaccess dosyasını kontrol edin ve yedekleyerek dizinden silin. Eğer .htaccess dosyasını sildiğinizde siteniz çalışıyorsa, .htaccess yapılandırmanızı değiştirin.

Ve son olarak Grup-1 Grup-2 ve Grup-4 olarak birleştirtirildiğinde oradaki nmap grubunda yer aldım. Orada da aşağıdaki taramaları yaptım.

Traceroute | nmap –traceroute 151.80.40.80/24 ile Traceroute özelliğini aktifleştirerek hedefe giden paketlerin yol analizini yaptım fakat pek bir sonuç bulunamadı.

```
┌──(kali㉿kali)-[~]
└─$ nmap -traceroute 151.80.40.80/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 10:38 EDT
Traceroute has to be run as root
QUITTING!
```

DNS Keşfi | nmap –system –dns 151.80.40.80/24 ile işletim sistemi üzerindeki dns serverlarını kullanmaya çalıştım fakat pek başarılı bir sonuç alamadım.

```
┌──(kali㉿kali)-[~]
└─$ nmap -system -dns 151.80.40.80/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 11:03 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.04 seconds
```

En çok kullanılan portları taramak için nmap –top-ports 10 151.80.40.80 kullanarak şu çıktıyı elde ettim.

```
┌──(kali㉿kali)-[~]
└─$ nmap -top-ports 10 151.80.40.80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 11:31 EDT
Nmap scan report for mirsoft.com.tr (151.80.40.80)
Host is up (0.15s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   open     http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  open     https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 18.81 seconds
```

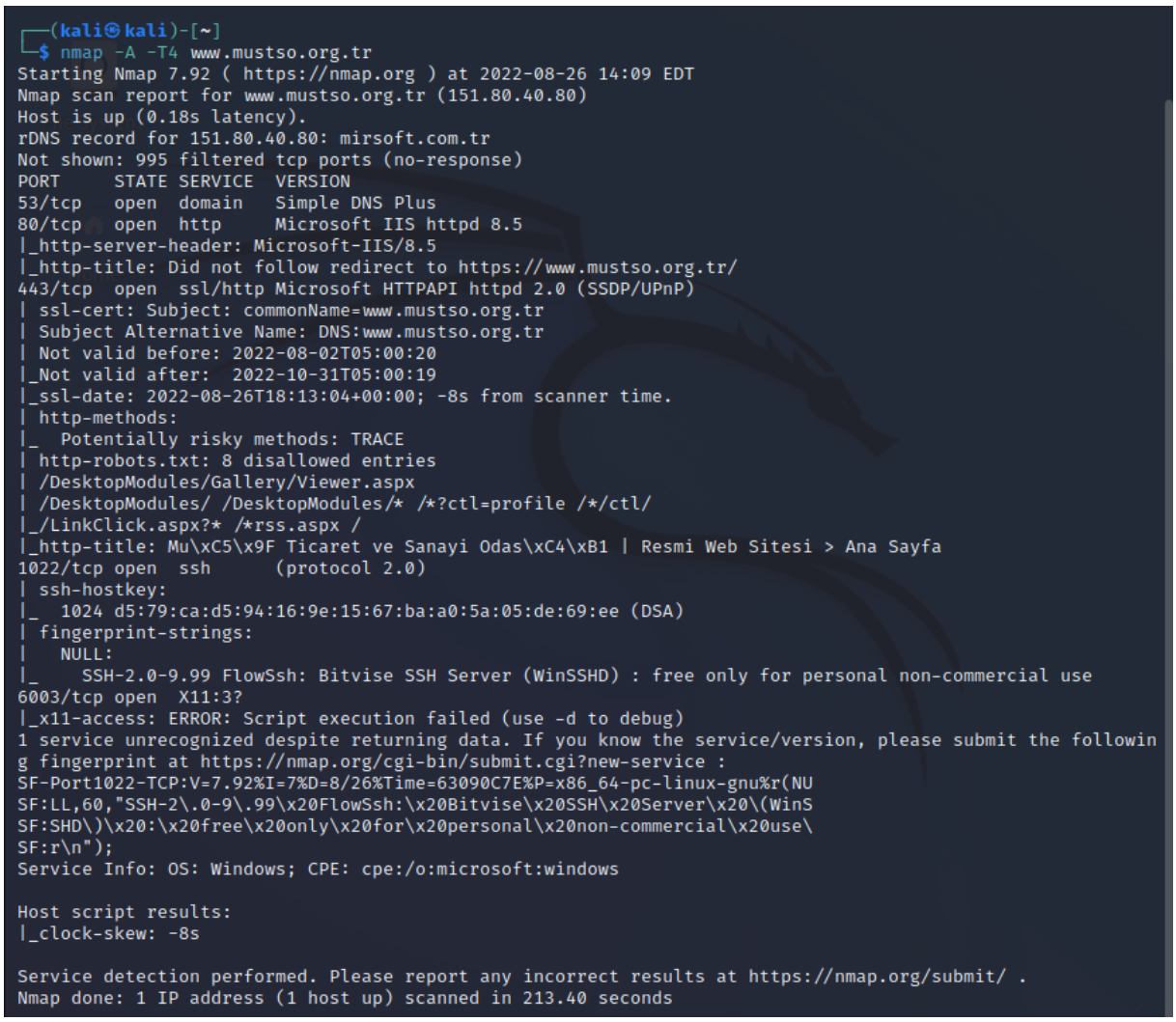
Taranan IP’nin işletim sistemini ve versiyonunu bulmak için nmap –v –A 151.80.40.80 komutunu kullanarak bir tarama yaptım ve sonucunu şu şekilde elde ettim.

```
┌──(kali㉿kali)-[~]
└─$ nmap -v -A 151.80.40.80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 11:43 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:43
Completed NSE at 11:43, 0.00s elapsed
Initiating NSE at 11:43
Completed NSE at 11:43, 0.00s elapsed
Initiating NSE at 11:43
Completed NSE at 11:43, 0.00s elapsed
Initiating Ping Scan at 11:43
Scanning 151.80.40.80 [2 ports]
Completed Ping Scan at 11:43, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:43
Completed Parallel DNS resolution of 1 host. at 11:43, 0.10s elapsed
Initiating Connect Scan at 11:43
Scanning mirsoft.com.tr (151.80.40.80) [1000 ports]
Discovered open port 53/tcp on 151.80.40.80
Discovered open port 443/tcp on 151.80.40.80
Discovered open port 80/tcp on 151.80.40.80
Discovered open port 6003/tcp on 151.80.40.80
Discovered open port 1022/tcp on 151.80.40.80
Completed Connect Scan at 11:43, 7.16s elapsed (1000 total ports)
Initiating Service scan at 11:43
Scanning 5 services on mirsoft.com.tr (151.80.40.80)
Completed Service scan at 11:46, 159.19s elapsed (5 services on 1 host)
NSE: Script scanning 151.80.40.80.
Initiating NSE at 11:46
Completed NSE at 11:47, 78.87s elapsed
Initiating NSE at 11:47
Completed NSE at 11:47, 2.06s elapsed
Initiating NSE at 11:47
Completed NSE at 11:47, 0.00s elapsed
Nmap scan report for mirsoft.com.tr (151.80.40.80)
Host is up (0.088s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE  VERSION
53/tcp    open  domain   Simple DNS Plus
80/tcp    open  http     Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Did not follow redirect to https://www.mirsoft.com.tr/
443/tcp   open  ssl/http Microsoft IIS httpd 8.5
|_ssl-date: 2022-08-26T15:47:14+00:00; -8s from scanner time.
|_http-title: Did not follow redirect to https://www.mirsoft.com.tr/
| ssl-cert: Subject: commonName=*.webdernek.com
| Subject Alternative Name: DNS:*.webdernek.com, DNS:webdernek.com
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
| Public Key type: rsa
| Public Key bits: 3072
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2022-08-04T05:03:09
| Not valid after:  2022-11-02T05:03:08
| MD5:   d3ad 3927 ee32 c867 5608 d0a5 620b 8157
|_SHA-1: a38c ff72 6fc6 6777 00bc 5853 3ada 7a9e 5f60 ef07
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Microsoft-IIS/8.5
1022/tcp open  ssh      (protocol 2.0)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-9.99 FlowSsh: Bitvise SSH Server (WinSSHD) : free only for personal non-commercial use
6003/tcp open  X11:3?
|_x11-access: ERROR: Script execution failed (use -d to debug)
1 service unrecognized despite returning data. If you know the service/version, please submit the followin
g fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1022-TCP:V=7.92%I=7%D=8/26%Time=6308EA21%P=x86_64-pc-linux-gnu%r(NU
SF:LL,60,"SSH-2\.0-9\.99\x20FlowSsh:\x20Bitvise\x20SSH\x20Server\x20\(WinS
SF:SHD\)\x20:\x20free\x20only\x20for\x20personal\x20non-commercial\x20use\
SF:r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -8s

NSE: Script Post-scanning.
Initiating NSE at 11:47
Completed NSE at 11:47, 0.00s elapsed
Initiating NSE at 11:47
Completed NSE at 11:47, 0.00s elapsed
Initiating NSE at 11:47
Completed NSE at 11:47, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 248.37 seconds
```

Hızlı yürütme ile tarama ve işletim sistemi ve servis algılama için nmap -A –T4 www.mustso.org.tr komutunu kullanarak şu şekilde çıktı aldım.“-A” parametresini kullanmak, işletim sistemi ve hizmet algılaması yapmanızı sağlar ve aynı zamanda daha hızlı yürütme için bunu “-T4” ile birleştiriyoruz.



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -T4 www.mustso.org.tr
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 14:09 EDT
Nmap scan report for www.mustso.org.tr (151.80.40.80)
Host is up (0.18s latency).
rDNS record for 151.80.40.80: mirsoft.com.tr
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
53/tcp   open  domain   Simple DNS Plus
80/tcp   open  http     Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_http-title: Did not follow redirect to https://www.mustso.org.tr/
443/tcp  open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| ssl-cert: Subject: commonName=www.mustso.org.tr
| Subject Alternative Name: DNS:www.mustso.org.tr
| Not valid before: 2022-08-02T05:00:20
|_Not valid after:  2022-10-31T05:00:19
|_ssl-date: 2022-08-26T18:13:04+00:00; -8s from scanner time.
| http-methods:
|_  Potentially risky methods: TRACE
| http-robots.txt: 8 disallowed entries
| /DesktopModules/Gallery/Viewer.aspx
| /DesktopModules/ /DesktopModules/* /*?ctl=profile /*/ctl/
|_/LinkClick.aspx?* /*rss.aspx /
|_http-title: Mu\xC5\x9F Ticaret ve Sanayi Odas\xC4\xB1 | Resmi Web Sitesi > Ana Sayfa
1022/tcp open  ssh      (protocol 2.0)
| ssh-hostkey:
|_  1024 d5:79:ca:d5:94:16:9e:15:67:ba:a0:5a:05:de:69:ee (DSA)
| fingerprint-strings:
|   NULL:
|_    SSH-2.0-9.99 FlowSsh: Bitvise SSH Server (WinSSHD) : free only for personal non-commercial use
6003/tcp open  X11:3?
|_x11-access: ERROR: Script execution failed (use -d to debug)
1 service unrecognized despite returning data. If you know the service/version, please submit the followin
g fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port1022-TCP:V=7.92%I=7%D=8/26%Time=63090C7E%P=x86_64-pc-linux-gnu%r(NU
SF:LL,60,"SSH-2\.0-9\.99\x20FlowSsh:\x20Bitvise\x20SSH\x20Server\x20\(WinS
SF:SHD\)\x20:\x20free\x20only\x20for\x20personal\x20non-commercial\x20use\
SF:r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -8s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 213.40 seconds
```

Nmap kullanarak CVE algılama Nmap’in tüm ağ ve sistem yöneticilerinin bilmediği en büyük özelliklerinden biri, “Nmap Scripting Engine” (NSE olarak bilinir) adı verilen bir şeydir. Bu komut dosyası motoru, kullanıcıların önceden tanımlanmış bir komut dosyası kümesi kullanmasına veya Lua programlama dilini kullanarak kendi komut dosyalarını yazmasına olanak tanır. nmap -Pn –script vuln 151.80.40.80 komuduyla aşağıdaki çıktıyı elde ettim.

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn --script vuln 151.80.40.80
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 14:20 EDT
Nmap scan report for mirsoft.com.tr (151.80.40.80)
Host is up (0.12s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp  open  https
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2013-7091: ERROR: Script execution failed (use -d to debug)
|_http-passwd: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
1022/tcp open  exp2
6003/tcp open  X11:3

Nmap done: 1 IP address (1 host up) scanned in 332.76 seconds
```