

6. hét: Aktív információgyűjtés 2.: nmap szkriptek, SMTP enumeráció, SNMP enumeráció, NetBIOS (SMB) enumeráció

Tartalom

1. A labor VPN
2. nmap szkriptek (nmap scripting engine, NSE)
3. SMTP (Simple Mail Transfer Protocol) enumeráció
4. SNMP (Simple Network Management Protocol) enumeráció
5. NetBIOS enumeráció

1. A labor VPN

1.1. A labor VPN szabályai

1. A labor VPN közös, nincs mindenkinek saját, egyelőre még ne bántsátok az ottani gépeket, hadd szkenelgessen mindenki.
2. Szabad otthonról használni.
3. A jelszavadat ne áruld el másnak, ha más visszaél a jelszavaddal, neked kell vállalni a felelősséget.

1.2. Bejelentkezés a labor VPN-be OpenVPN-nel

1. Regisztráció az alábbi adatok megadásával itt: <https://lab.hackthis.xyz/registration.php>

| mező neve | megjegyzés |
|-----------------|-----------------------|
| Neptun kód | DE18SZ |
| Név | (A neved) |
| Felhasználó név | (Szabadon választott) |
| Jelszó | (Szabadon választott) |
| Jelszó újra | |

2. Bejelentkezés itt: <https://lab.hackthis.xyz/login.php>
3. A lab-vpn-config.ovpn nevű OpenVPN "connection profile" állomány (*.ovpn) letöltése innen: <https://lab.hackthis.xyz/lab-vpn-config.ovpn>

4. Kapcsolódás

```
openvpn lab-vpn-config.ovpn
```

Név, jelszó beírása. A kapcsolat ellenőrzése:

```
ping -c 1 10.20.0.101
```

2. nmap szkriptek (nmap scripting engine, NSE)

- ssh-t tartalmazó szkriptek felsorolása

```
ls /usr/share/nmap/scripts/*ssh*
```

2.1. Sérülékenység (vulnerability) keresése

```
nmap -n -vv 10.20.0.2 --script=rmi-vuln-classloader \
-oX 10.20.0.2_rmi-vuln-classloader.xml
```

2.1.1 Több szkript futtatása

1. Szkript lista készítése

```
ls /usr/share/nmap/scripts/*smb-vuln* \
| cut -d"/" -f 6 > scripts.txt
```

2. a.sh

```
#!/bin/bash
for script in $(cat scripts.txt); do
    nmap -v -p 139,445 --script=${script} 10.20.0.2 \
    -oX ${script}.xml
done
```

```
./a.sh
```

3. SMTP (Simple Mail Transfer Protocol) enumeráció

Mire jó: használói nevek keresése.

1. Végrehajtható SMTP parancsok lekérdezése nmap-el:

```
nmap -n -Pn -vv -p 25 10.20.0.2 --script=smtp-command
```

2. SMTP VRFY parancs: emailcím lekérdezése az adott SMTP szerveren.

```
root@deb:~# nc -nv 10.20.0.2 25
(UNKNOWN) [10.20.0.2] 25 (smtp) open
VRFY root
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
252 2.0.0 root
VRFY csattanomaszlag
550 5.1.1 <csattanomaszlag>: Recipient address
rejected: User unknown in local recipient table
^C
root@deb:~#
```

4. SNMP (Simple Network Management Protocol) enumeráció

- Mi ez? Egy UDP 161-en futó alkalmazásréteg protokoll.

4.1. Mire jó?

- A rendszergazdának: eszközöket (routereket, switcheket stb.) konfigurálhatnak távolról. Nézheti a teljesítményüket.
- A támadónak: elsősorban használók neveit olvashatja ki belőle.

4.2. Használata

- Community string: a jelszó. Az alapértelmezett a "public", ez csak olvasható.
- OID-k: <http://www.oid-info.com/>

4.3. onesixtyone

Profi SNMP szkennelő. <http://www.phreedom.org/software/onesixtyone/>

4.3.1 onesixtyone több szerverre

1. community.txt (az utolsó sor utáni sortörés fontos!)

```
public
private
manager
```

2. hosts.txt (részlet)

```
10.11.1.5
10.11.1.7
10.11.1.8
10.11.1.10
10.11.1.13
10.11.1.14
```

3. parancs:

```
onesixtyone -c community.txt -i hosts.txt
```

4.4. snmpwalk

```
snmpwalk -c public -v1 10.20.0.101
```

4.5. snmp-check (máshol: snmpcheck)

```
snmp-check 10.20.0.101 > snmp-check.out
```

4.6. Nmap

- SNMP brute force

```
nmap -n -vv -sU -p 161 10.20.0.101 --script=snmp-brute.nse
-oX 10.20.0.101_snmp-brute.nse.xml
```

- NetBIOS servicekre (135, 137, 138, 139) az alábbiakhoz van szükség: gép doménbe helyezése, hálózat és nyomtató böngészés, ActiveDirectory-ben nem publikált nyomtatók megosztása, mappelt meghajtók, és MS Exchange 2000/2004-hoz.
- NetBIOS neve lehet: domain-nek, számítógépnek, szolgáltatásnak.
- A NetBIOS név formátuma: 16 karakter hosszú, a Microsoft implementációknál a NetBIOS név 16. karaktere a NetBIOS suffix.

5.1. enum4linux

<https://labs.portcullis.co.uk/tools/enum4linux/>

1. Null session keresése enum4linux-szal

```
enum4linux -a -v 10.20.0.2
```

5.2. nbtscan

1. NetBIOS nevek nbtscan-nel.

```
nbtscan -v -r 10.20.0.101
```

◦ Kimenetre példa



Doing NBT name scan for addresses from 10.11.1.229

NetBIOS Name Table for Host 10.11.1.229:

| Name | Service | Type |
|-----------|---------|--------|
| MAIL | <00> | UNIQUE |
| WORKGROUP | <00> | GROUP |
| MAIL | <1f> | UNIQUE |
| MAIL | <03> | UNIQUE |
| MAIL | <20> | UNIQUE |
| WORKGROUP | <1e> | GROUP |

Adapter address: 00:50:56:b8:fe:21

Windows NT által követett NetBIOS suffix konvenciók

NetBIOS Suffixes (16th Character of the NetBIOS Name) 
<https://support.microsoft.com/en-us/help/163409/netbios-suffixes-16th-character-of-the-netbios-name> 

5. NetBIOS enumeráció

Mi ez, mire jó?

- Az 1990-es évekig a NetBIOS API volt a legelterjedtebb a PC-ken hálózatra.
- Ma már a NetBIOS API visszaszorult, de a NetBIOS nevek, és a NetBIOS service-ek használata nem, nyomtató- és meghajtómegosztásra (SMB) ma is elterjedten alkalmazzák.

6. Feladatok

1. Találj egy sérülékenységet nmap-pel a labor VPN bármelyik gépén.
2. Találj egy használati nevet a labor VPN bármelyik gépén.