Windows Attack Lab - Step 2 - Host & Service Discovery

Author

- Knöpfel, Daniel
- Duijts, Michael

NMAP Scan

NMAP Scan durchführen

- -n = Keine DNS Auflösung
- -Pn = Kein Host Discovery durchführen, alle Clients abfragen

```
# nmap -n -Pn --top-ports=10 10.0.1.0/24 -oA nmap_winlab_host_discovery --min-rate=5000
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-17 15:17 CET
Nmap scan report for 10.0.1.1
Host is up (0.00062s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.0.1.9
Host is up (0.0013s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  open   https
445/tcp  closed microsoft-ds
3389/tcp closed ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)
```

```
Nmap scan report for 10.0.1.10
Host is up (0.13s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp open     ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.0.1.100
Host is up (0.062s 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  open     netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp open     ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.0.1.101
Host is up (0.071s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  open     netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp open     ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.0.1.102
Host is up (0.071s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
```

```
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  open     netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp open     ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.0.1.103
Host is up (0.055s 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  open     netbios-ssn
443/tcp  filtered https
445/tcp  open     microsoft-ds
3389/tcp open     ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.0.1.254
Host is up (0.0034s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
23/tcp   filtered telnet
25/tcp   filtered smtp
80/tcp   filtered http
110/tcp  filtered pop3
139/tcp  filtered netbios-ssn
443/tcp  filtered https
445/tcp  filtered microsoft-ds
3389/tcp filtered ms-wbt-server
MAC Address: 12:34:56:78:9A:BC (Unknown)

Nmap scan report for 10.0.1.15
Host is up (0.000023s latency).

PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   closed http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
```

```
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp open   ms-wbt-server

Nmap done: 256 IP addresses (9 hosts up) scanned in 2.23 seconds
```

9 Systeme wurden gefunden

NMAP Service Scan

- `nmap -n -sC -sV -iL hosts_winlab.txt -oA nmap_winlab_script_version_scan --min-rate=5000`
- -sV = Services detektieren
- -sC = Standard Skript verwenden

10.0.1.1

- Keine offenen Ports
- Evtl. Firewall/Router etc.

10.0.1.9

- SSH (22)
- Apache (80,443)
- Apache Tomcat (8080)
- Linux Webserver?

10.0.1.10

- RDP (3389)
- Standard Windows Ports (135, 445) offen
- Windows Client

10.0.1.100

- Viele ldap Services offen
- Domain Controller?

10.0.1.101

- RDP (3389)
- Standard Windows Ports (135, 139, 445) offen
- Windows Client

10.0.1.102

- RDP (3389)
- Standard Windows Ports (139, 445) offen
- Windows Client

10.0.1.103

- Microsoft SQL Server (1433)
- Datenbankserver?

10.0.1.254

- Keine offenen Ports
- Evtl. Firewall/Router etc.