

HACKING- WORKSHOP

Phasen eines Penetrationstests

Ein Penetrationstest ist ein simulierter Angriff aus Sicht eines realen Angreifers

- Planung, Scoping
- Information Gathering
 - Analyse des Scopes, Planung der Scans
 - Passive Reconnaissance
 - Active Reconnaissance
 - Auswertung der Scanner-Ergebnisse
- Exploitation
 - Planung der Angriffe
 - Zugang verschaffen
 - Zugang dauerhaft erhalten, "Lateral Movement"
 - Analyse der Resultate
- Post Exploitation
- Berichterstellung
 - Berichtsübergabe, Meeting, Vorführungen/Demos
 - Fehlernachtests
- Lessons Learned

Netzwerk-Scans

Informationen über Computersysteme innerhalb eines Netzwerks sammeln

- Erster Schritt bei Aktiver Reconnaissance
- „Discovery“ von potentiellen Zielen die verwundbar sind
 - Host Discovery
 - Port Scans
 - Device Enumeration
 - Packet Crafting
 - Vulnerability Scans

Nmap

(network mapper) Der "traditionelle", meistgenutzte Netzwerk-Scanner

- Verfügbar für die meisten Plattformen (Windows, Linux...)
- Die Grundlage der meisten Vulnerability Scan-/Test- Produkte, sowohl kommerziell als auch open source
- Unterstützt Skripte
- Kann IDS (Intrusion Detection Systeme) umgehen
 - Geschwindigkeits- und Performance-Einstellungen

Nmap

- Methoden von Nmap:
 - Host Discovery
 - Port und Service Discovery
 - Betriebssystem-Fingerprinting
 - Service-Fingerprinting
 - Enumeration
 - MAC Adressen-Erkennung
 - Vulnerability-Erkennung
 - Exploit-Erkennung
- **Syntax:** nmap [Scan Type(s)] [Option(s)] <target>

(Mehr zu den Optionen und Skripten folgt später)

Nmap Target

TARGET	BESCHREIBUNG
192.168.1.50	Nur diese IP-Adresse scannen.
scanme.host.tld	Nur diesen Host scannen.
192.168.1.0/24 company.tld/24 192.168.1.*	Gesamtes Subnetz scannen.
scanme.host.tld/24	Subnetz des Hosts scannen.
192.168.1.20-50	IP-Adressen "Range" scannen.
192.168.1.20-25, 7.44	Range 192.168.1.20 bis 25, sowie "192.168.7.44" scannen.

Nmap Scan Arten / Typen

SCAN TYP	BESCHREIBUNG
-h	nmap -h Hilfe-Informationen
-V	nmap -V Nmap-Versionsinformationen anzeigen
-d	Nmap -d 192.168.1.5 Debug-Output aktivieren. Zeigt jeden einzelnen Schritt an den Nmap macht, inklusive Output.
-sS (TCP SYN-Scan)	nmap -sS 192.168.1.50 Sendet einen TCP SYN um zu prüfen ob das Target mit SYN ACK antwortet (Port ist offen), oder mit RST (Reset - Port ist geschlossen). Auch als half-open Scan bekannt, weil es den TCP 3-Wege Handshake nicht vollendet. Das ist Default für Root-User.
-sT (TCP-Connect- Scan)	nmap -sT 192.168.1.50 Komplettiert den TCP 3-Wege Handshake. Nmap lässt das zugrundeliegende Betriebssystem eine Verbindung mit dem Target auf dem angegebenen Port herstellen. Default für reguläre (nicht-root) User.

Nmap Scan Arten / Typen

SCAN TYP	BESCHREIBUNG
-sV	<code>nmap -sV 192.168.1.50</code> "Probe" von offenen Ports um die Service Version festzustellen.
-sU (UDP-Scan)	<code>nmap -sU 192.168.1.50</code> UPD Scan. <ul style="list-style-type: none">• Ports die einen Response senden werden als open (offen) angezeigt.• Ports die keinen Response senden werden als open filtered (unknown) angezeigt.• Ports die einen ICMP Unreachable Error (type 3 code 3) senden werden als closed angezeigt.
-sL	<code>nmap -sL 192.168.1.50</code> Targets auflisten die gescannt werden.
-sA	<code>nmap -sA www.targethost.tld</code> Herausfinden ob ein Host/Netzwerk von einer Firewall geschützt wird. <ul style="list-style-type: none">• "Filtered" bedeutet die Firewall ist aktiv.• "Unfiltered" - Resultate bedeuten der Port ist erreichbar, aber kann offen oder geschlossen sein.

Nmap Optionen

Nmap Option	Beispiel	Hinweis
-p <port range>	<pre>nmap -p 80 192.168.1.50 nmap -p 80,443 www.company.tld nmap -p1024-3000 192.168.1.0/24 nmap -p U:53,111,137,T:21-25,80,139,443 192.168.1.0/24 nmap -p- 192.168.1.50</pre>	<p>Nur den/die spezifizierten Port(s) scannen.</p> <p>Die meisten Implementierungen von Nmap erlauben entweder ein Leerzeichen oder keines nach -p</p> <p>Port Status kann OPEN, CLOSED (Kein Service an dem Port - OS hat ein TCP Reset gesendet), oder FILTERED (Kein Response, vermutlich wegen Firewall) sein.</p> <p>UDP ports: U; TCP ports: T</p> <p>Alle TCP ports: -p-</p>

Nmap Optionen

Nmap Option	Beispiel	Hinweis
-r	nmap -r 192.168.1.0/24	Fortlaufender Scan; keine zufällige Reihenfolge.
--top-ports <number>	nmap --top-ports 200	Scan der Top 200 Ports.
-6	nmap -6 2001:f0d0:1003:51::4 nmap -6 scanme.company.tld nmap -6 fe80::8d50:86ce:55ad:bc5c	Scan der IPv6 Adressen.
-iL <inputfilename>	nmap -iL /tmp/test.txt	Scan der Hosts aus einer Liste (Datei).
--exclude	nmap 192.168.1.0/24 --exclude 192.168.1.5	Bestimmte Hosts ausschließen vom Scan.
-n	nmap -n 192.168.1.0/24	Namen nicht auflösen (spart Zeit).
-R	nmap -R 192.168.1.0/24	Versucht alle Namen mit Reverse DNS Lookup zu auflösen. Selbst wenn der Host (scheinbar) down ist.
-F (fast mode)	nmap -F 192.168.1.50	Scan mit weniger Ports als Default.

Nmap Optionen

Nmap Option	Beispiel	Hinweis
-O	nmap -O 192.168.1.50	"OS Detection" aktivieren. Nmap versucht das OS zu erkennen. Nicht immer akkurat.
-A (aggressive)	nmap -A 192.168.1.50	"OS Detection", Service Version Detection, Skript Scans und Traceroute.
--version-intensity <level>	nmap -sV --version-intensity 9 192.168.1.50	Zu benutzen zusammen mit -sV. Gibt die Prüfungs-Level an von 0 (gering) bis 9 (alle Probes).
--script=<scriptname>	nmap --script=banner.nse 192.168.1.50	Ein NSE Skript benutzen.
-sC	nmap -sC 192.168.1.50	Scan mit allen Default Skripts.
-v	nmap -A -v 192.168.1.50	"Verbosity" des Output/der Ausgabe erhöhen.
-vv	nmap -vv 192.168.1.50	Sehr detaillierte Ausgabe ("verbose").
-oN/-oX/-oS/-oG/-oA <filename>	nmap 192.168.1.50 -oA results.txt	Output speichern als Formate: Normal, XML, Script Kiddie, Grepable, oder alle (außer Script Kiddie), in die angegebene Datei. Standard Speicherort ist das Userprofil (zB. /root/).

Discovery Scans

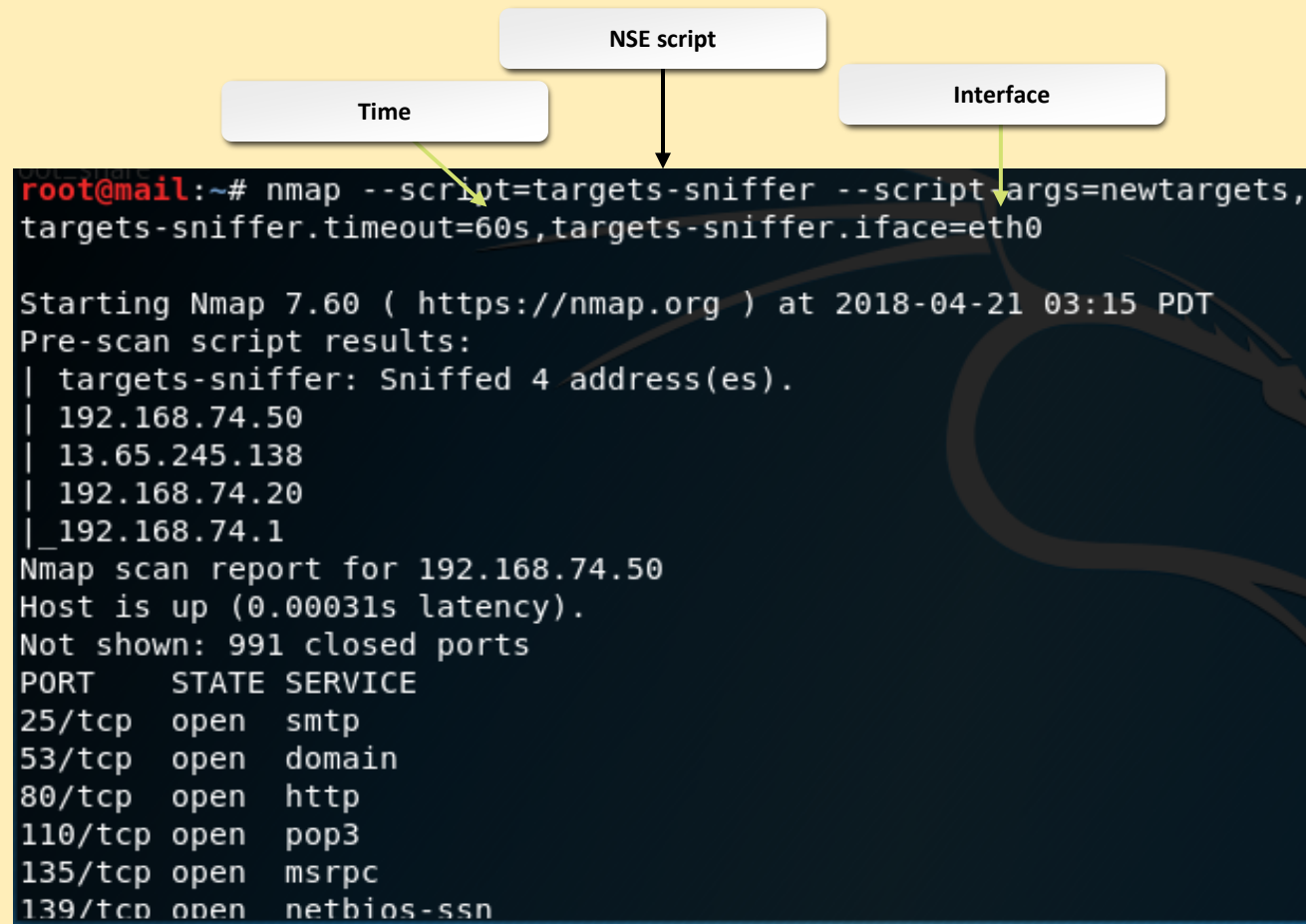
Discovery Scan: Findet aktive IP-Adressen in einem Netzwerk

Ping Sweep: Eine Netzwerk-Scan-Technik die ICMP ECHO REQUEST- Pakete benutzt um aktive Hosts aufzuspüren

Nmap Discovery Scan Syntax	Beispiel	Hinweis
-PR	nmap -PR 192.168.1.50	Sendet einen ARP Request an "Target" um zu prüfen ob es einen Response/eine Antwort gibt. ARPs werden generell nicht von Firewalls geblockt. Das ist die Standard-Discovery-Methode für jeden Nmap Scan im Ethernet LAN.
-sn	nmap -sn 192.168.1.0/24	Kein Port Scan. Nur Discovery, mittels Kombination von ICMP ECHO Request, TCP SYN an Port 443, TCP ACK an Port 80, und einem ICMP Timestamp-Request.
-PS <portlist>	nmap -PS135 192.168.1.0/24	Hosts mittels TCP SYN an angegebene(n) Port(s) entdecken. Default ist 80. Jeder Response (SYN ACK, oder RST) ist Indikator dafür, dass das Target an ist. Es darf kein Leerzeichen zwischen -PS und Portliste stehen. Danach folgt ein Port-Scan, außer -sn wird genutzt.

Es gibt auch andere Tools für Discovery-Scans, aber nmap ist das meistbenutzte Werkzeug.

Discovery Scans



Port Scans


Port Number (TCP, wenn nicht anders angegeben)	Service
21	FTP Befehle
22	SSH
23	Telnet
25	SMTP
53 (TCP oder UDP)	DNS
80	HTTP
88	Kerberos
110	POP3
111 (TCP oder UDP)	*nix portmapper
135	Microsoft Remote Procedure Call (RPC)
139	SMB (legacy)

Port Scans

Port Number (TCP, wenn nicht anders angegeben)	Service
143	IMAP4
161 (TCP oder UDP; z.Zt. nur UDP in Nutzung)	SNMP
162 (TCP oder UDP; z.Zt. nur UDP in Nutzung)	SNMP Traps
389	LDAP
443	HTTPS
445	Microsoft-ds (Authentication von SMB)
3389	RDP

Port Scan Beispiele

```
root@kali:~# nmap 192.168.74.20
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-13 03:17 EDT
Nmap scan report for 192.168.74.20
Host is up (0.000098s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:BA:2C:5D (VMware)
```



Port Scan Beispiele

```
root@kali:~# nmap 192.168.74.50
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-13 03:23 EDT
Nmap scan report for 192.168.74.50
Host is up (0.00019s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
143/tcp   open  imap
445/tcp   open  microsoft-ds
587/tcp   open  submission
MAC Address: 00:0C:29:2D:0C:A3 (VMware)
```

Stealth Scans

Nmap Stealth Option	Beispiel	Beschreibung
-sS	nmap -sS 192.168.1.50	Originaler "Stealth" scan. Sendet ein TCP SYN. Antwortet das Target mit SYN ACK, wird der Handshake nicht vollendet, sondern stattdessen RST gesendet. Wird nicht so leicht entdeckt.
-sA	nmap -sA 192.168.1.0/24	Sendet ein TCP ACK. Wird genutzt um Firewall-Rulesets zu erkennen, erkennt welche Ports gefiltert sind, und ob eine Firewall "stateful" ist.
-sN	nmap -sN 192.168.1.2-10	Sendet ein TCP Segment ohne Flags. Das ist nicht der normale Status bei TCP, dieses hat normal mindestens ein Flag (usually ACK) aktiviert. Damit kann man non-stateful Firewalls umgehen.
-sF	nmap -sF www.company.tld	Sendet ein TCP FIN. Damit kann man non-stateful Firewalls umgehen.
-sX	nmap -sX 192.168.1.0/24	Sendet ein TCP-Paket mit FIN, PSH, and URG Flags aktiv, dadurch <i>"leuchtet das Paket auf wie ein Weihnachtsbaum"</i> . Eine unlogische Flag-Kombination. Wird benutzt um non-stateful Firewalls zu umgehen.

Stealth Scans

Nmap Stealth Option	Beispiel	Beschreibung
-Pn	<code>nmap -Pn -p- 192.168.1.0/24</code>	Discovery-Phase überspringen. Unter der Annahme, dass alle Hosts für den Port-Scan online sind. Nützlich wenn Targets eine Firewall aktiv haben, und ausschließlich Services auf unüblichen Ports anbieten.
-sl <zombie> <target>	<code>nmap -sl -Pn -p- zombie.middle.tld www.company.tld</code>	<i>Blind</i> TCP Port Scan (Idle Scan). <i>Keine Pakete</i> werden direct von der Angreifer-Maschine versendet. Verwendet einen "Zombie"- (Middle Man-) Host um die Informationen über offene Ports des Targets zu erhalten. Man muss erst eine Maschine identifizieren die als Zombie geeignet ist, die man später natürlich auch für weitere Scans verwenden kann.
-b <FTP relay> <FTP target>	<code>nmap -v -b name:password@old-ftp-server.company.tld ftp-target-server.company.tld -Pn</code>	Vollführt einen FTP Bounce Scan. Nutzt FTP Proxy Verbindungen aus in denen ein User einen "Middle Man" FTP Server anfragt, der Dateien zu einem anderen FTP-Server versenden soll. Dieses FTP Relay Feature wurde von den meisten Herstellern deaktiviert.

Stealth Scans

Nmap Stealth Option	Beispiel	Beschreibung
-T <0 - 5>	nmap 192.168.1.0/24 -T 2	Use different timing templates to throttle the speed of your queries to make the scan less noticeable. Choose from T0 (slowest) to T5 (fastest). Nmap also refers to these speeds as paranoid, sneaky, polite, normal, aggressive, and insane, respectively. T0 and T1 are best for IDS evasion, but are VERY slow. T5 has been reported to be unstable because it is too fast. T4 is the recommended choice for a fast scan that is still stable. T3 is the default.
-f	nmap -f 192.168.1.50	Split packets (including pings) into 8-byte fragments to make it harder for packet filtering firewalls and intrusion detection to detect the purpose of packets. MTU is the maximum fragment size.
-D [decoy1, decoy2, decoy3, etc.] <target>	nmap -D 192.168.1.10 192.168.1.15 192.168.1.30 192.138.1.50	Used to mask a port scan by using decoys. Creates bogus packets "from" the decoys so the actual attacker "blends in" with the crowd. It looks like both the decoys and the actual attackers are performing attacks. In this example, 192.138.1.50 is the target. The other IPs are the decoys.

Stealth Scans

Nmap Stealth Option	Beispiel	Beschreibung
-e <interface>	<code>nmap -e eth0 192.168.1.50</code>	Specify the interface Nmap should use.
-S <spoofed source address>	<code>nmap -e eth0 -S www.google.com 192.168.1.50</code>	Spoof the source address. Will not return useful reports to you (target responses will be sent to the spoofed address), but can be used to confuse an IDS or the target administrator.
--spoof-mac [vendor type MAC address]	<code>nmap -sT -PN --spoof-mac apple 192.168.1.50</code> <code>nmap -sT -PN -spoof-mac B7:B1:F9:BC:D4:56 192.168.1.50</code>	Use a bogus source hardware address (also known as Media Access Control or MAC address). You can specify a random MAC based on vendor, or explicitly specify the MAC address. The first example creates a random Apple hardware address.
--source-port <portnumber>	<code>nmap --source-port 53 192.168.1.36</code>	Use a specific source port number (spoof source port) to fool packet filters configured to trust that port. Same as -g <portnumber> option.
--randomize-hosts	<code>nmap --randomize-hosts 192.168.1.1-100</code>	Randomize the order of the hosts being scanned.
--proxies <Comma-separated list of proxy URLs>	<code>nmap --proxies http://192.168.1.30:8080, http://192.168.1.90:8008 192.168.1.50</code>	Relay TCP connections through a chain of HTTP or SOCKS4 proxies. Especially useful on the Internet.

Full Scan

Eine Art von Scan die das Maximum an Informationen von einem Target und über ein Target hervorbringt

- Alle Ports scannen
- Alle Services nach Versionsinformationen befragen/untersuchen
- *OS-Footprinting*
- Weitere Aktionen
- Gibt die meisten Resultate, wird aber am leichtesten entdeckt
 - Evasion-Taktiken sind randomisierte IP-Adressen und Ports, und das Verlangsamen des Scans

Full Scan

Eine Art von Scan die das Maximum an Informationen von einem Target und über ein Target hervorbringt

- Alle Ports scannen
- Alle Services nach Versionsinformationen befragen/untersuchen
- *OS-Fingerprinting*
- Weitere Aktionen
- Gibt die meisten Resultate, wird aber am leichtesten entdeckt
 - Evasion-Taktiken sind randomisierte IP-Adressen und Ports, und das Verlangsamen des Scans

```
nmap -p- 192.168.1.0/24
```

```
nmap -p1-65535 www.example.tld
```

```
nmap -sU -p1-65535 192.168.1.50
```

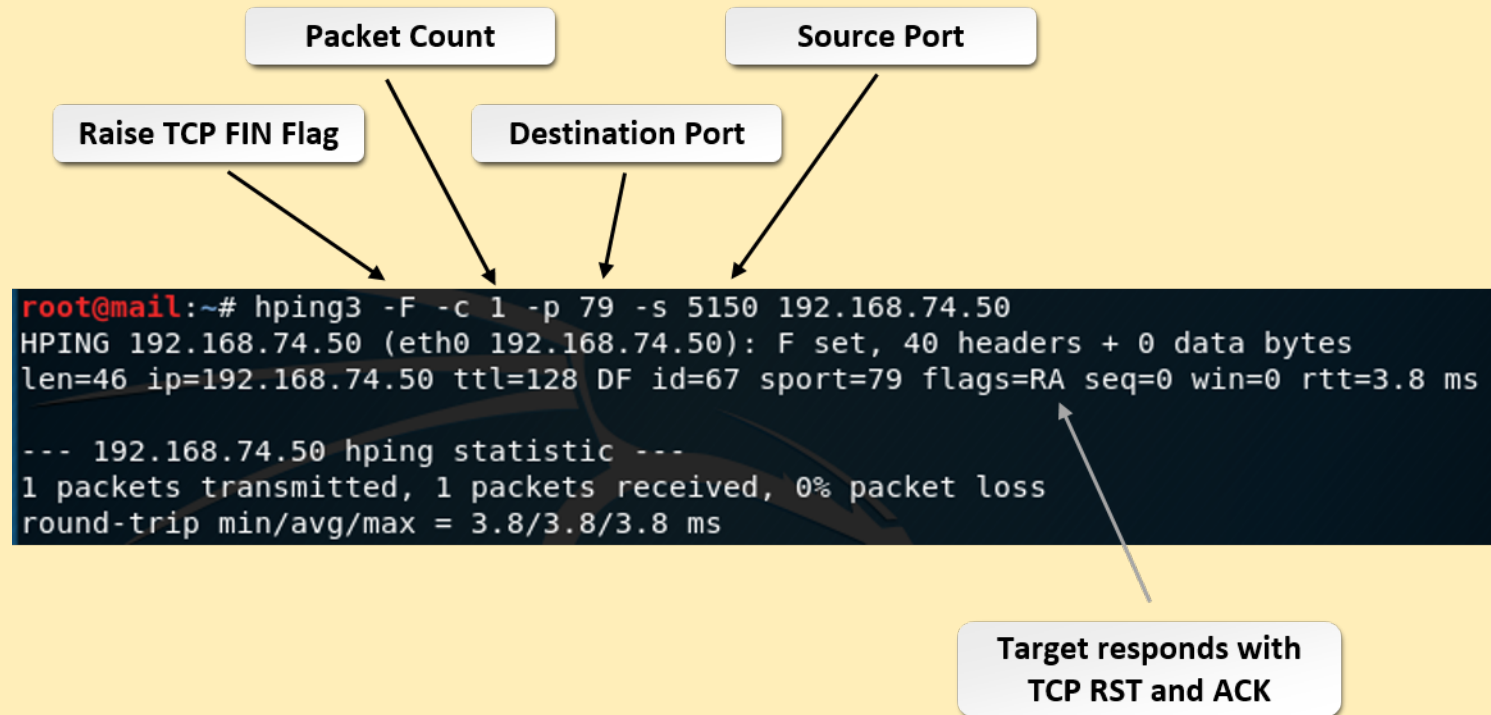
Packet Crafting

Ein normales IP-Paket vor der Übermittlung manipulieren

Um Firewall-Regeln zu testen, die "Intrusion Detection" zu umgehen, oder für DoS-Zwecke

- Man möchte so wenige Pakete als möglich benutzen um die Ziele zu erreichen
 1. Paket generieren
 2. Paket editieren
 3. Paket abspielen
 4. Paket decodieren
- Verschiedene Tools und Skripts
 - Hping
 - Ostinato
 - Scapy
 - Libcrafter
 - Yersinia
 - packETH
 - Colasoft packet builder, Bit-Twist, ...

Packet Crafting



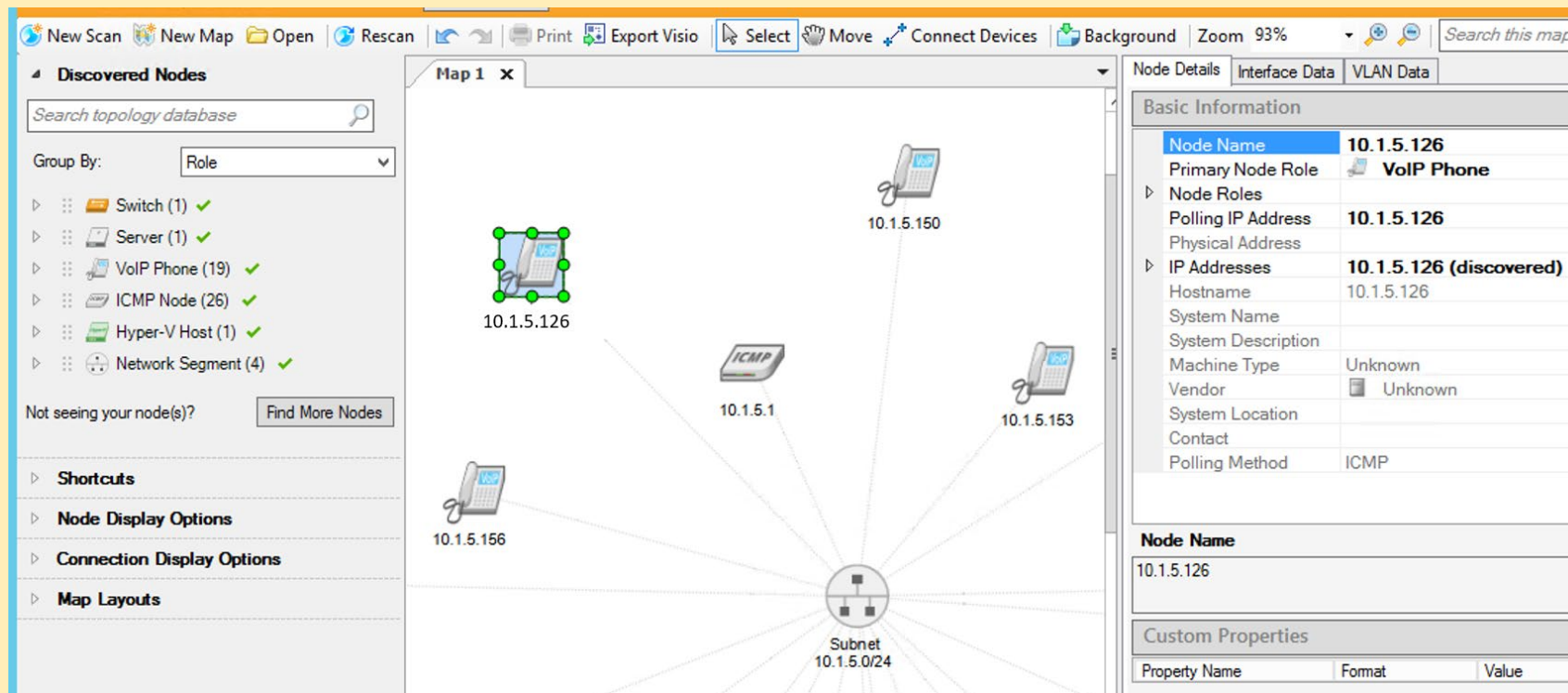
Netzwerk-Mapping

Geräte in einem Netzwerk finden, um das Netzwerk darstellen zu können, und eine logische topologische Map zu erstellen

- Aktives "Probing" um Informationen zu sammeln:
 - MAC und IP-Adressen
 - Ports und Services
 - OSs
 - Device-Arten
 - VMs
 - Hostnamen
 - Protokolle
- Subnetze und die Verbindungen zwischen Geräten identifizieren
- Methoden:
 - Nmap
 - ARP Cache Interrogation
 - Routing und MAC Tables
 - CDP "Neighbor Tables" (CDP = Cisco Discovery Protocol)

Netzwerk-Mapping

- Topologie-Map hilft den Einsatz von benötigten Tools und Strategien zu planen
- Das Standard-Mapping ist normalerweise das lokale Subnetz



Solarwinds
Network
Topology Mapper

Metasploit

Sehr vielseitiges Computersicherheit- und Pentesting-Framework

- Modular, man kann das Toolset sehr spezifisch auf die Bedürfnisse zuschneiden
- Mehr oder weniger ein Exploit-Framework
- Framework und Pro- Editionen
- GUI- Varianten von Rapid7 (offiziell), und zusätzlich Spin-Offs mit GUI von Armitage (kostenlos) und Cobalt Strike (kommerziell)
- Module:
 - Exploits
 - Payloads
 - Post
 - Hilfsmodule (Auxiliary)
 - Encoder
 - NOPs

Exploits und Payloads werden später im Detail besprochen.

Metasploit

Module Type

Target Platform

Target Service

Module Name

exploit/windows/smb/ms17_010_psexec

```
=[ metasploit v4.16.54-dev ]
+ -- --=[ 1757 exploits - 1006 auxiliary - 306 post ]
+ -- --=[ 536 payloads - 41 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/ms17_010_psexec
msf exploit(windows/smb/ms17_010_psexec) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(windows/smb/ms17_010_psexec) >
```

Metasploit

Note: The quickest way to determine the correct module, payload, and options is to conduct a Google search. However, be advised that Metasploit is frequently updated. You are likely to find examples and instructions that are outdated and no longer work.

Metasploit Search

msf> search EternalBlue type:exploit—find every exploit that refers to EternalBlue.

msf> search platform:"Windows XP SP3" type:exploit -o /root/xpsp3_exploits.csv
—find every exploit that applies to Windows XP SP3 and save to xpsp3_exploits.csv.

msf> search Windows/VNC type:payload—find every VNC payload that applies to Windows.

msf> search Windows/MSSQL type:exploit—find every exploit that can be used against Microsoft SQL running on Windows.

msf> search Windows/SMB type:exploit -S great—find all Windows-based SMB exploits that have an excellent (most reliable) ranking (have the string "excellent" in the row results).

msf> search scanner/smb—search for every scanner that has to do with SMB.

msf> search scanner/mssql—search for every scanner that has to do with Microsoft SQL.

Metasploit Beispiel Suche nach MSSQL Scanner

```
msf > search scanner/mssql
```

Matching Modules

=====

Name	Disclosure Date	Rank	Description
----	-----	----	-----
auxiliary/scanner/mssql/mssql_hashdump		normal	MSSQL Password Hashdump
auxiliary/scanner/mssql/mssql_login		normal	MSSQL Login Utility
auxiliary/scanner/mssql/mssql_ping		normal	MSSQL Ping Utility
auxiliary/scanner/mssql/mssql_schemadump		normal	MSSQL Schema Dump

```
msf > use auxiliary/scanner/mssql/mssql_ping
```

```
msf auxiliary(scanner/mssql/mssql_ping) > show options
```

Module options (auxiliary/scanner/mssql/mssql_ping):

Name	Current Setting	Required	Description
----	-----	-----	-----
PASSWORD		no	The password for the specified username
RHOSTS		yes	The target address range or CIDR identifier
TDSENCRYPTION	false	yes	Use TLS/SSL for TDS data "Force Encryption"
THREADS	1	yes	The number of concurrent threads
USERNAME	sa	no	The username to authenticate as
USE_WINDOWS_AUTHENT	false	yes	Use windows authentication (requires DOMAIN option set)

```
msf auxiliary(scanner/mssql/mssql_ping) > set RHOSTS 192.168.74.10-50
```

```
RHOSTS => 192.168.74.10-50
```

```
msf auxiliary(scanner/mssql/mssql_ping) > run
```


Metasploit Sessions

```
msf > sessions -l
```

```
Active sessions
```

```
=====
```

Id	Name	Type	Information	Connection
--	----	----	-----	-----
1		shell	php/php	192.168.74.134:46749 -> 192.168.74.20:3312 (192.168.74.20)
2		shell	cmd/unix	192.168.74.134:26942 -> 192.168.74.20:40154 (192.168.74.20)
3		shell	cmd/unix	192.168.74.134:15900 -> 192.168.74.20:43130 (192.168.74.20)

```
msf > sessions 2
```

```
[*] Starting interaction with 2...
```

Richtlinie für Netzwerkskans

- OSINT oder andere anfängliche Informationen über das Targetnetzwerk nutzen, um die Start-Adresse des Scans zu bestimmen.
- Bestimmen Sie das Level an Detail das Sie entdecken möchten. IP-Adressen, Ports, Services, Versionen, Hostnamen, OS, Device-Status, und wählen Sie ein Tool das in der Lage ist diese Informationen zu beschaffen.
- Starten Sie mit einem Discovery-Scan der verschiedene Techniken einbezieht, nicht nur ICMP ECHO
- Fügen Sie bekannte Netzwerke oder kürzere Subnetzmasken manuell hinzu, und kombinieren Sie mehrere Subnetze in einem einzigen Scan.
- Passen Sie die Scan-Geschwindigkeit an, so dass Performance und Stabilität gut ausgewogen sind.
- Verwenden Sie immer eher langsamere Scan-Geschwindigkeiten (seien Sie sozusagen "höflich"), um nicht zu viel **Noise** im Netzwerk zu erzeugen.

Richtlinie für Netzwerkskans

- Verwenden Sie die langsamsten Scan-Geschwindigkeiten um eine Erkennung durch IDS-Systeme zu vermeiden.
- Benutzen Sie Port Scans um *listening* Ports auf den entdeckten Hosts zu ermitteln.
- Optional: Tools die Ports untersuchen, Banner grabben, und speziell gecraftete Pakete nutzen um Betriebssystem- und Service-Versionen zu identifizieren.
- Optional: Nutzen Sie WMI bzw. SNMP um Geräte auf Service- oder Komponenten-spezifische Informationen hin zu untersuchen.
- Wenn ein standardisiertes Diagramm gewünscht ist, exportieren Sie die Scanner-Ausgaben um sie z.B. in Microsoft Visio zu importieren.
- Google nutzen um schnell Beispiele und Guides für Ihre Tools zu finden. Beachten Sie, dass manche Guides nicht mehr aktuell sein werden. Idealerweise nutzt man Guides unter denen **Kommentare** vorhanden sind. So kann man schnell "outdated" Information aussortieren.