DIGICOMP Hacking Day 2012

Portscanning im Jahre 2012

Martin Rutishauser

DEFCON SWITZERLAND

Agenda

- Vorstellung
- Portscanning im Jahre 2012
- Einführung TCP/IP
- Tipps und Tricks
- Internet Scanning
- Tools
- Referenzen

Vorstellung

- Martin Rutishauser
  - Senior Information Security Consultant
  - Referent CAS/MAS IS
  - Private Homepage: www.indianz.ch
  - Member Defcon-Switzerland

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Defcon-Switzerland

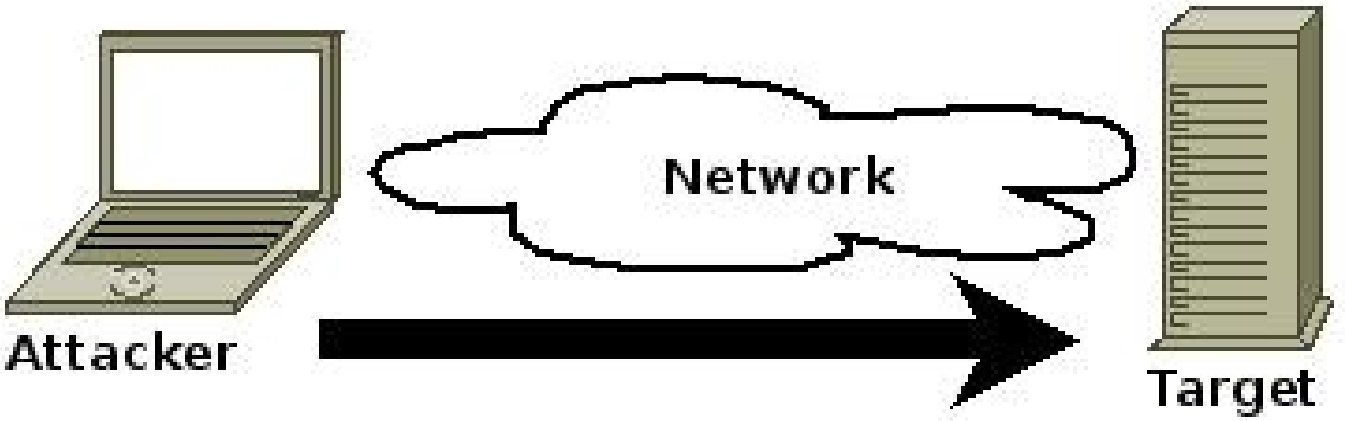
- Verein für Informations-Austausch im Bereich Informationssicherheit
- Existiert seit 2008, etwa 50 Members
- Monatliche Treffen (MS Patch-Tuesdays), abwechselnd in Bern und Zürich
  - https://www.defcon-switzerland.org/
- Organisator “#hashdays” Security Conference
  - https://www.hashdays.ch/

Warnhinweis

- Portscans in der CH noch nicht strafbar
- Kann aber als Angriffsvorbereitung interpretiert werden
- Empfehlungen:
  - Nur eigene Systeme scannen
  - (Schriftlich!) Erlaubnis für Scan einholen
  - Virtuelle Systeme verwenden
  - Öffentliche Systeme verwenden (scanme.insecure.org)

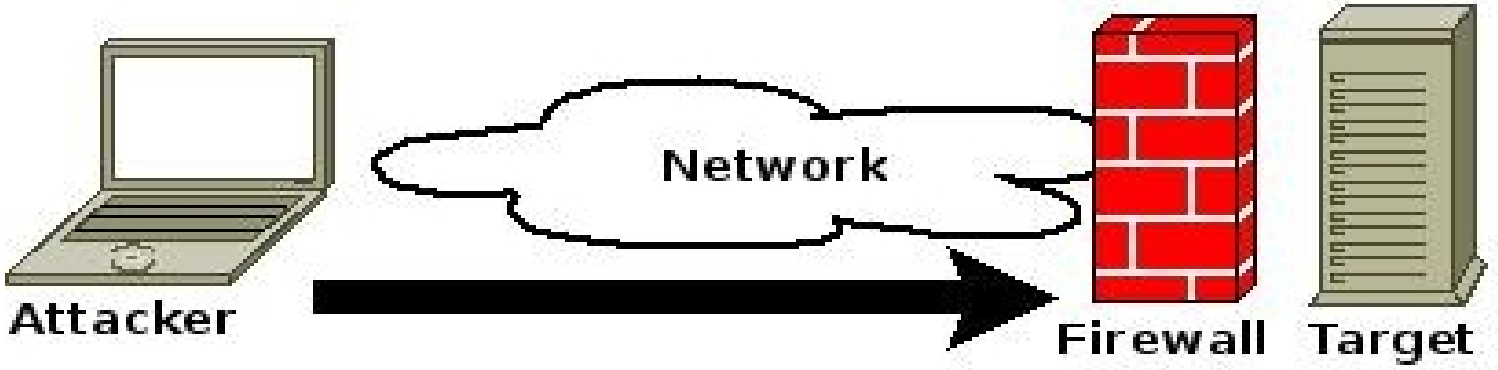
Portscanning im Jahre 2012

- Früher kaum Sicherheit



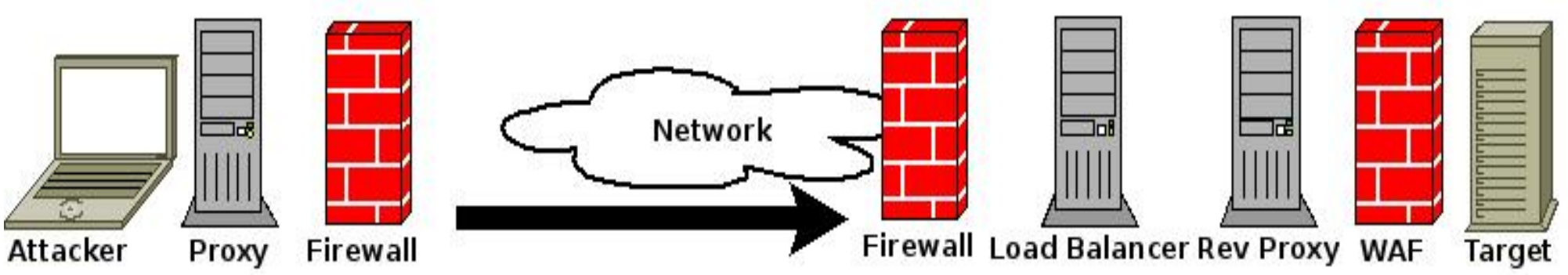
Portscanning im Jahre 2012

- Dann Firewalls als Perimetersicherheit



Portscanning im Jahre 2012

- Heute Firewalls, Gateways, WAF's, Load-Balancers, IDS/IPS, Reverse Proxies, Stateful Packet Filters, …



Einführung TCP/IP

- TCP/IP-Protokoll-Suite:
  - TCP = Transmission Control Protocol
  - UDP = User Datagram Protocol
  - IP = Internet Protocol
  - ICMP = Internet Control Message Protocol
- TCP und UDP bieten je 65'536 Ports an
- Netzwerkdienste werden angeboten
  - 80 = HTTP
  - 443 = HTTPS
  - 22 = OpenSSH

Einführung TCP/IP

- TCP
  - Src-Port = Source-Port
  - Dst-Port = Destination Port
  - TCP Sequenznummer = Reihenfolge Pakete
  - Window-Size = Grösse Sliding Window
  - Data-Offset = Länge TCP-Header, Start Daten
- UDP
  - Src-Port = Source-Port
  - Dst-Port = Destination Port
  - Length = Länge in Oktetten (Minimum 8)

Einführung TCP/IP

- IP
  - Version = v4 (v6)
  - Src-Address = Source IP
  - Dst-Address = Destination IP
  - IP-ID = Reassemblieren von IP Paketen
  - TTL = Time-to-Live
- ICMP
  - Fehlermeldungen
  - Types und Codes
  - Ping, Traceroute, ...

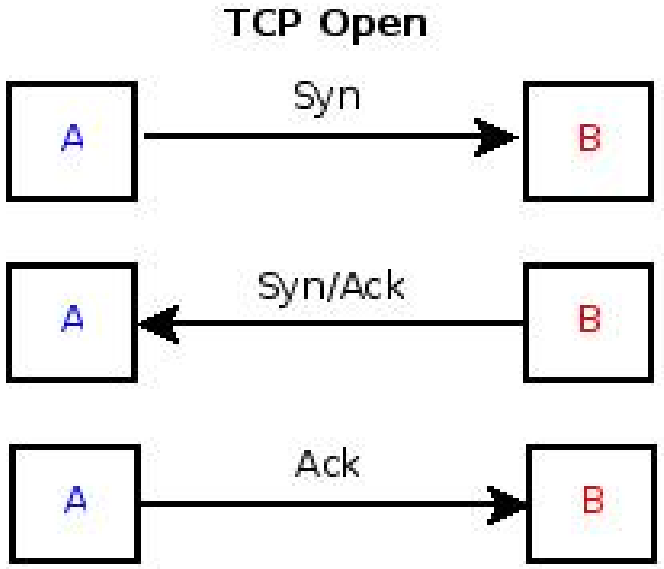
Einführung TCP/IP

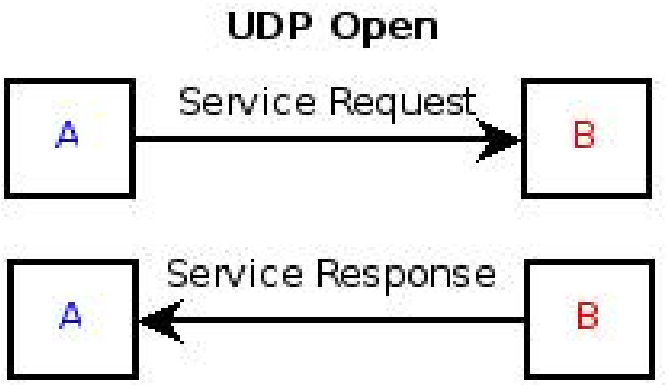
- Flags:
  - Syn = Synchronize
  - Ack = Acknowledge
  - Fin = Finish
  - Rst = Reset
  - Psh = Push
  - Urg = Urgent
  - Alle = Xmas
  - Keine = Null

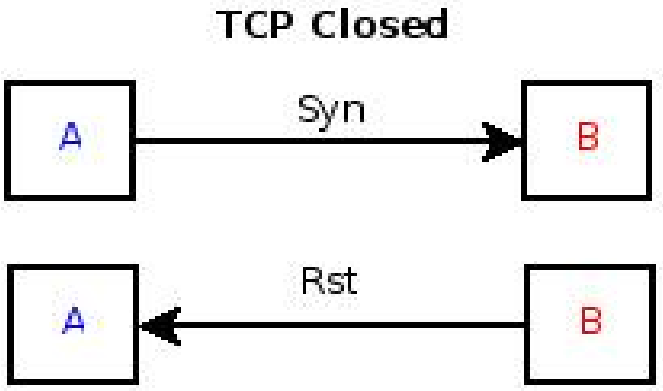
Einführung TCP/IP

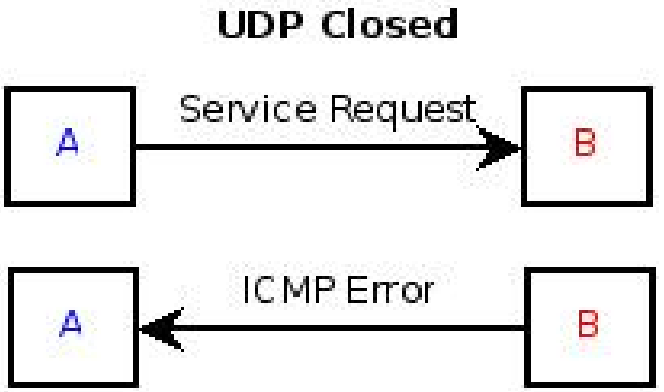
- TCP verbindungsorientiert
  - 3-way Handshake
  - Sitzung (Session) wird aufgebaut
  - Dann Datentransfer
- UDP verbindungslos
  - Fire-and-forget
  - Protokoll/Service reagiert oder eben nicht
  - UDP braucht ICMP Fehlermeldungen

Einführung TCP/IP









Einführung TCP/IP

```
11:52:47.890899 IP (tos 0x0, ttl 45, id 27, offset 0, flags [none], proto TCP (6),
length 44)
    192.168.0.58.61051 > 217.26.52.76.80: Flags [S], cksum 0x66cc (correct), seq
922630471, win 1024, options [mss 1460], length 0
11:52:47.890916 IP (tos 0x0, ttl 52, id 1611, offset 0, flags [none], proto TCP (6),
length 44)
    192.168.0.58.61051 > 217.26.52.76.81: Flags [S], cksum 0x66cb (correct), seq
922630471, win 1024, options [mss 1460], length 0
11:52:47.915335 IP (tos 0x0, ttl 58, id 57788, offset 0, flags [DF], proto TCP (6),
length 44)
    217.26.52.76.80 > 192.168.0.58.61051: Flags [S.], cksum 0x42b6 (correct), seq
1027336913, ack 922630472, win 65535, options [mss 1452], length 0
11:52:47.915361 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto TCP (6), length
40)
    192.168.0.58.61051 > 217.26.52.76.80: Flags [R], cksum 0x8285 (correct), seq
922630472, win 0, length 0
11:52:47.915741 IP (tos 0x0, ttl 58, id 57789, offset 0, flags [DF], proto TCP (6),
length 40)
    217.26.52.76.81 > 192.168.0.58.61051: Flags [R.], cksum 0x8274 (correct), seq 0,
ack 922630472, win 0, length 0
```

Portscanning im Jahre 2012

- Probleme mit Portscanning
  - “Komische” Resultate
  - Lange dauernde Scans
  - Jedes mal andere Resultate
  - False Negatives / False Positives
  - Filter lokal/remote
  - ...

Portscanning im Jahre 2012

- Wichtig bei Port- und Security-Scans:
  - Nicht durch ein NAT (spoofing SRC-Ports)
  - Nicht durch einen aktiven Stateful Packetfilter
  - Nicht durch eine aktive Firewall (lokal egress)
  - Nicht durch einen Proxy (wenn möglich)
  - Nicht durch aktivierte IPS-Module (Evasion ;)
  - ...

Portscanning im Jahre 2012

- Nmap Scans
  - -sS = TCP-SYN-Scan (Stealth Scan)
  - -sT = TCP-Connect-Scan (Handshake, Vanilla Scan)
  - -sU = UDP-Scan (UDP Scan, Linux Timing)
  - -sN = TCP-NULL-Scan (RST, Filter Evasion, UNIX)
  - -sF = FIN-Scan (RST, Filter Evasion, BSD)
  - -sX = Xmas-Scans (RST, Filter Evasion, UNIX)
  - -sA = TCP-ACK-Scan (Filter Detection)
  - -sW = TCP-Window-Scan (Filter Detection)
  - -sM = TCP-Maimon-Scan (RST, Filter Evasion)
  - -sV = Versioning-Scan (Fingerprinting)
  - -O/-A = OS-Detection/OS, Services, Scripts, Traceroute
  - --scanflags = Benutzerdefinierter TCP-Scan

Portscanning im Jahre 2012

- More Nmap Scans
  - -sI <zombie host>[:<probeport>] = Idle-Scan
  - -sO = IP-Protokoll-Scan
  - -sR = RPC-Scan
  - -b <FTP relay host> = FTP-Bounce-Scan
  - -6 = IPv6-Scan
  - -Sc/--script=default/safe/all = Scripting Engine (LUA)
  - --top-ports
  - -sY/-sZ = SCTP INIT/COOKIE-ECHO scans
  - -f = Fragmented Scan
  - -D = Decoy-Scan
  - -S/-g = Spoof Source IP/Port
  - -i = reverse ident scanning (process owner)

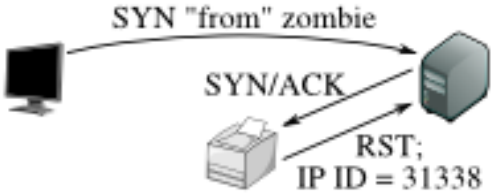
Portscanning im Jahre 2012

- Nmap Idle Scan Open (Quelle: Book)

Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

Step 2: Forge a SYN packet from the zombie.



The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

Portscanning im Jahre 2012

- Nmap Idle Scan Closed (Quelle: Book)

Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

Step 2: Forge a SYN packet from the zombie.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

Portscanning im Jahre 2012

- Nmap Timing und Performance
  - --min-hostgroup/--max-hostgroup <numhosts>
    - Adjust parallel scan group sizes
  - --min-parallelism/--max-parallelism <numprobes>
    - Adjust probe parallelization
  - --min-rtt-timeout/--max-rtt-timeout <time>
    - Adjust probe timeouts
  - --max-retries <numtries>
    - Specify maximum number of probe retransmissions
  - --host-timeout <time>
    - Give up on slow targets

Portscanning im Jahre 2012

- Nmap Timing und Performance
  - --scan-delay/--max-scan-delay <time>
    - Adjust delay between probes
  - --min-rate/--max-rate <number>
    - Directly control the scanning rate
  - --defeat-rst-ratelimit
    - Ignore those rate limits
  - --nsock-engine epoll|select
    - Enforce use of a given nsock IO multiplexing engine
  - -T paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5)
    - Set a timing template

Portscanning im Jahre 2012

- Nmap Scripting Engine
  - Kategorien: auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, intrusive, malware, safe, version, vuln
  - Etwa 350 Scripts derzeit
  - Prerule scripts (vor dem Scan), Host scripts (bei Host-Detektion), Service scripts (bei Service Detektion) und Postrule scripts (nach dem Scan)
- Ndiff
  - Vergleichen von Nmap-Resultaten

Portscanning im Jahre 2012

- Nping
  - Netzwerk-Paket-Generator
  - Protokolle: TCP, UDP, ICMP, ARP, Ethernet, IP
  - Funktionen: Ping, DoS, Stresstest, ARP Poisoning, Firewall-Rules ausmessen, Paket-Korruption entdecken, Senden von Exploit-Payload
  - Echo-Mode: Paket-Informationen (Nping Echo Servermode + Clientmode)
- Ncat
  - Netcat-Ersatz mit mehr Funktionalität
  - SSL-Support, Proxy-Support, Chaining, UDP, TCP, STCP

Tipps und Tricks

- Full Port Range: 0-65535 TCP und UDP
- ICMP Filter erschweren UDP Scans
- UDP nicht vergessen, auch wenn mühsam
- UDP applikatorisch prüfen (App Payloads)
- High-Range Ports TCP/UDP nicht vergessen
- Nur ein Subset von Ports scannen
- Portscans oder Portsweeps?
- Resultate immer verifizieren
- Low-Level-Informationen auswerten
- Portscanning → Fingerprinting → Attacking

Internet Scanning I/II

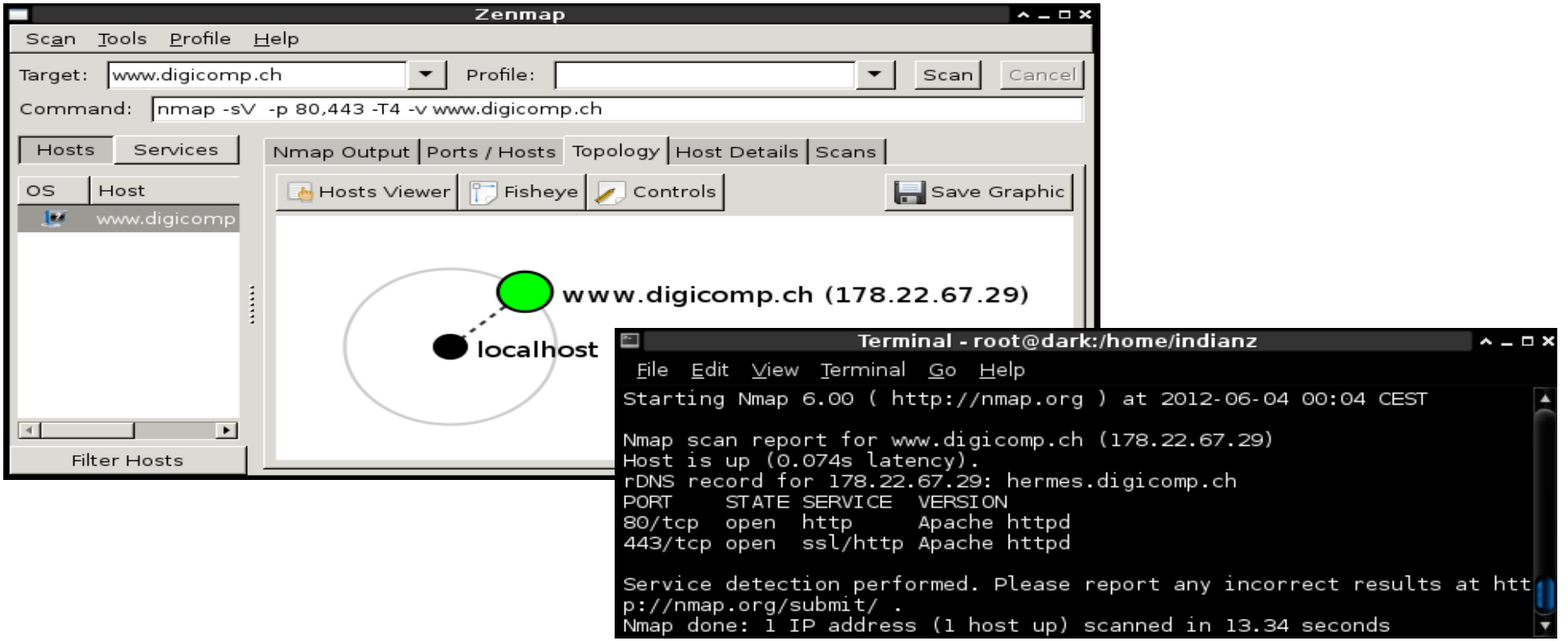
- Das Internet ist voll von RFC-incompliant Hosts (Microsoft, Cisco)
- Es gibt Hosts im Internet, die immer ACK's senden
- Auf ein Syn-Paket an einen Host kann die Antwort von einem anderen kommen (asynchrones NAT)
- Es gibt ganze Class-A Netzwerke im Internet, die leer sind (black holes)

Internet Scanning II/II

- Nie sequentiell scannen, immer Spread Spectrum (Blockweise zB. 256 Hosts, ARP-Flooding!)
- Das erste Syn-Paket geht oft verloren (ARP auf Router, kann droppen)
- Koordiniertes Scannen (ARP-Flooding! wenn zuviele Tester die gleichen Hosts scannen)
- Nie länger als 3 Sekunden pro Host auf Antwort warten (längere Antwortzeit = nicht interessant)
- Rücksicht auf Administratoren nehmen ;)

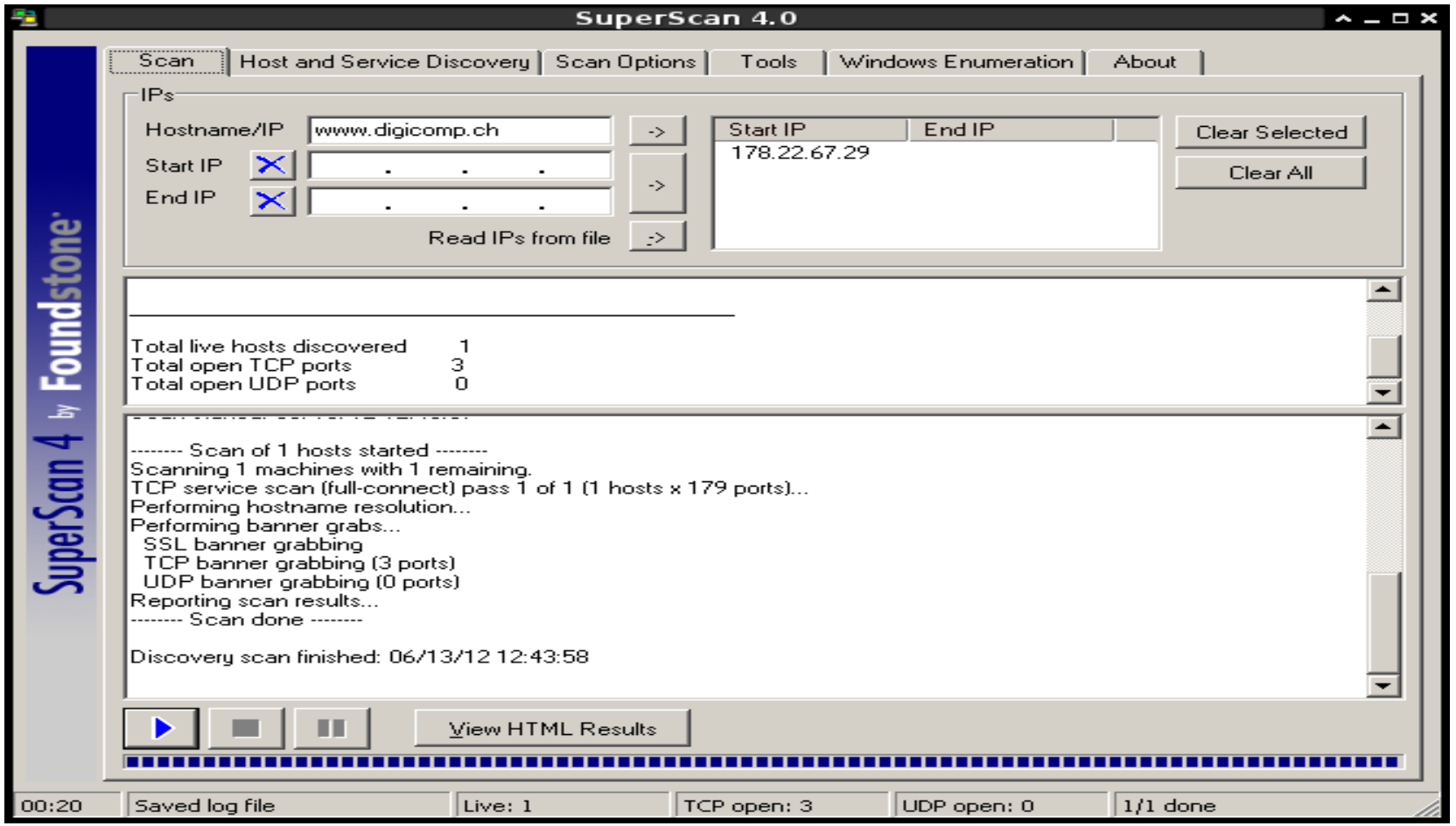
Tools I/III

- Insecure.org Nmap
  - Windows/Linux/Mac GUI/Commandline



Tools II/III

- (McAfee/Foundstone) Superscan
  - Windows-GUI / Wine unter Linux

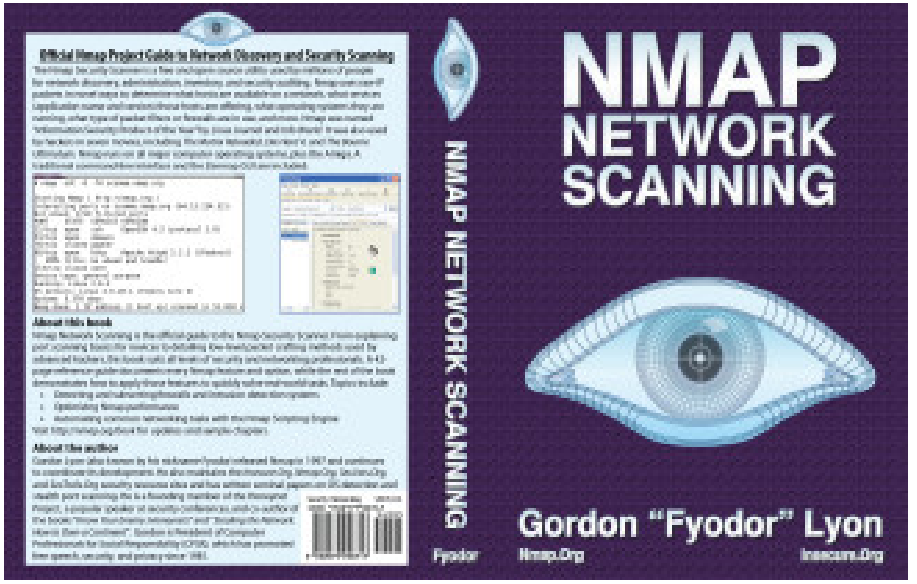


Mehr Tools (Open Source) III/III

- Unicornscanner (Linux)
  - Fast Network Scanner
- Metasploit Module (Linux/Windows)
  - Scanners und Discovery-Tools
- Hping (Linux/Windows)
  - Low-Level TCP/IP-Manipulation
- Angry-IP (Windows/Linux/Mac)
  - Portscanner
- Advanced IP Scanner (Windows)
  - Network Mapping

Referenzen

- Nmap
  - http://nmap.org/
  - http://nmap.org/book/toc.html
  - http://nmap.org/nping/
  - http://nmap.org/book/nse.html
  - http://nmap.org/nsedoc/



- Superscan
  - http://www.mcafee.com/us/downloads/free-tools/superscan.aspx

Fragen / Diskussion

- Wem darf ich noch eine Frage beantworten?