Scanning Techniques

Hendrik Spiegel
hendrik.spiegel@rub.de
Tobias Füchtler
fuchtler@et.rub.de

Ruhr-Universität Bochum
Lehrstuhl für Kommunikationssicherheit
Ahmad-Reza Sadeghi
Netzwerksicherheit

Überblick

- Motivation
- Protokolltypen (kurze Wiederholung)
- Ping Sweeps
- Portscanning Varianten
- Portscanning Techniken
- Betriebssystemerkennung
- Scannen durch Firewalls
- Die Praxis: NMAP
- Fazit

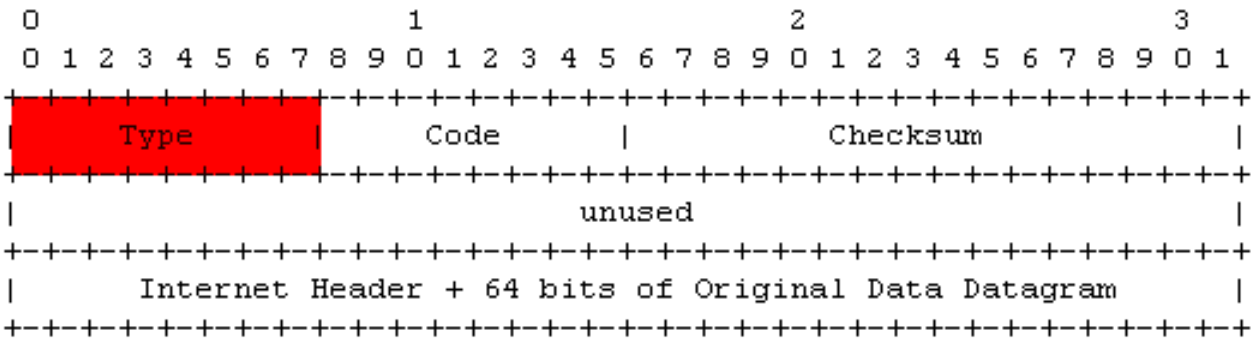
Motivation

- Unter welchen IP Adressen eines Netzwerkes sind Rechner erreichbar?
- Welche Dienste laufen auf diesen Rechnern?
- Welche System Architektur (z.B. Sparc, Alpha, x86) liegt zugrunde?
- Welches Betriebssystem wird verwendet?

Vorgehensweise

- Ermitteln der erreichbaren Hosts durch Pingen
- Portscans identifizieren:
  - Aktive Dienste
  - System Architektur
  - Betriebssystem
- Die gewonnenen Informationen liefern evtl. Schwachstellen im Betriebssystem

ICMP (RFC 972)

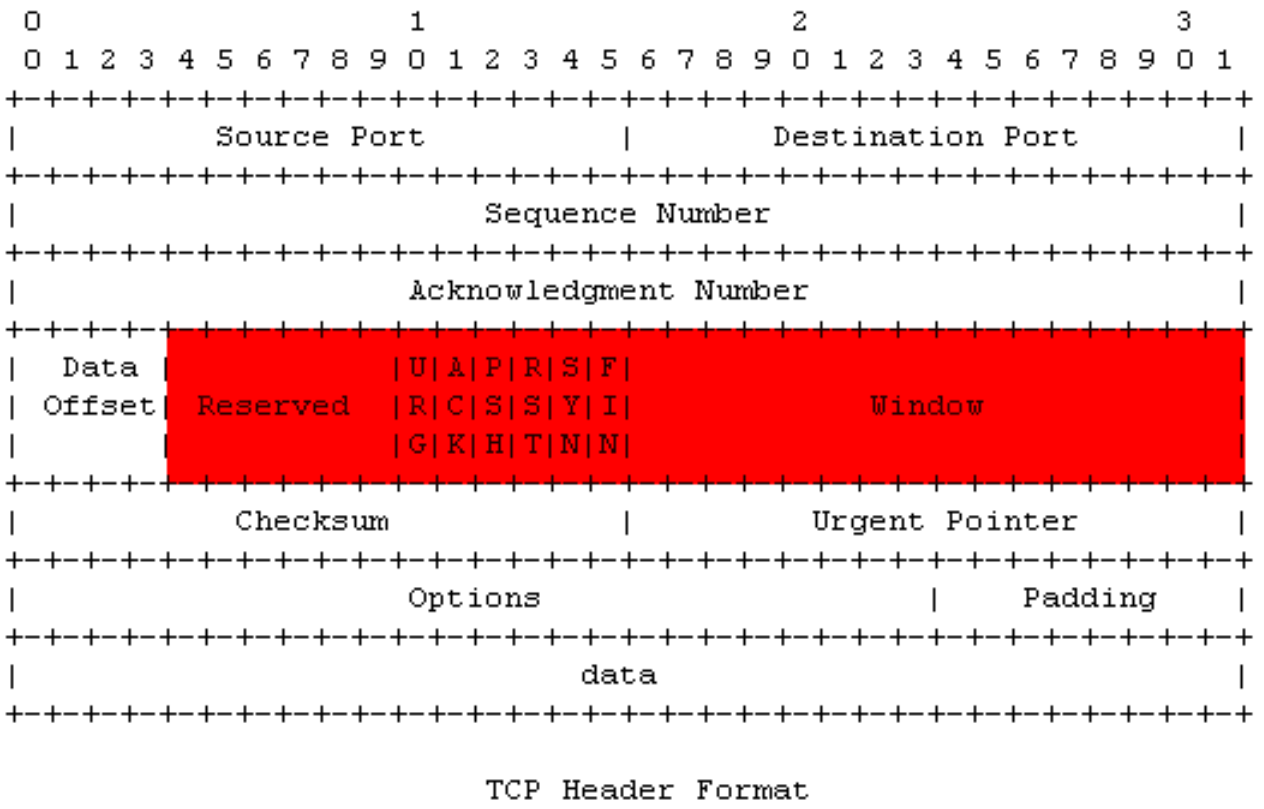


Verschiedene Typen z.B.

- ICMP ECHO request (Typ 8)
- ICMP ECHO reply (Typ 0)

TCP (RFC 973)

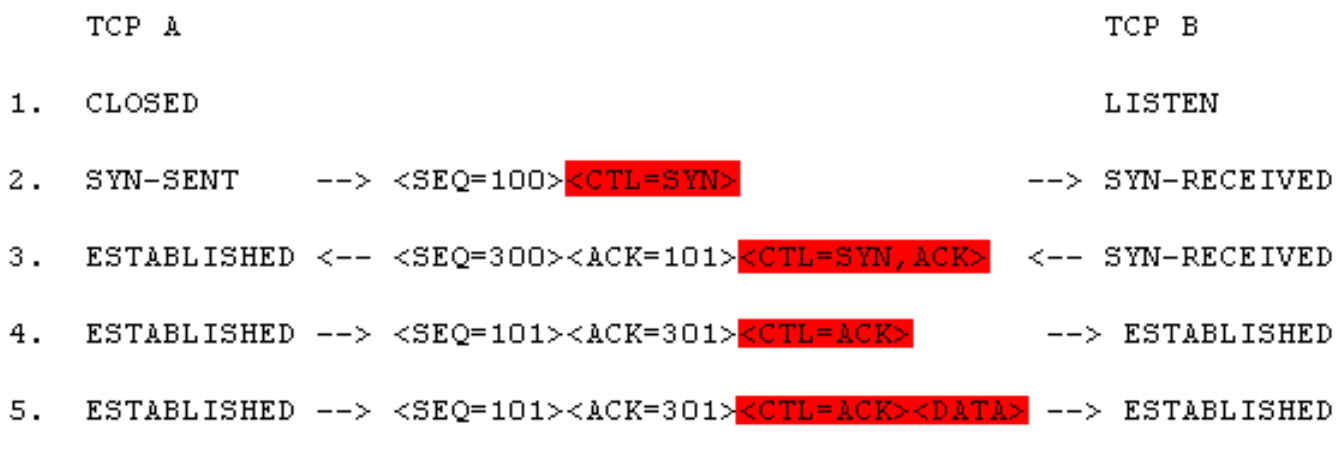
- Flags



TCP Header Format

TCP (RFC 973)

- “three-way handshake“



Basic 3-Way Handshake for Connection Synchronization

Ping Sweeps

- ICMP Sweeps (ICMP ECHO requests)
  - Testet ob Ziel IP erreichbar
- Broadcast ICMP
  - ICMP ECHO request an Broadcastadresse
  - Testet ganze Netze
- Non-ECHO ICMP
  - ICMP timestamp um aktuelle Zeit zu erfahren
  - ICMP address mask um Subnetmask zu erfahren

Ping Sweeps

- UDP Sweeps (UDP Scans)
  - Basiert auf ICMP PORT UNREACHABLE
  - Nicht zuverlässig, weil:
    - Firewalls und Router oft UDP Pakete verwerfen
- Falls ICMP Pakete gefiltert werden, muß ein Angreifer alle IP Adressen eines Netzes Portscannen, was sehr zeitaufwändig ist

Portscanning Übersicht

- Offenes TCP Scannen
  - TCP connect()
- Stealth TCP Scannen
  - Halb-offenes SYN Flag Scannen
  - Inverses TCP Flag Scannen
  - ACK Flag Probe Scannen
  - TCP Fragmentation Scannen

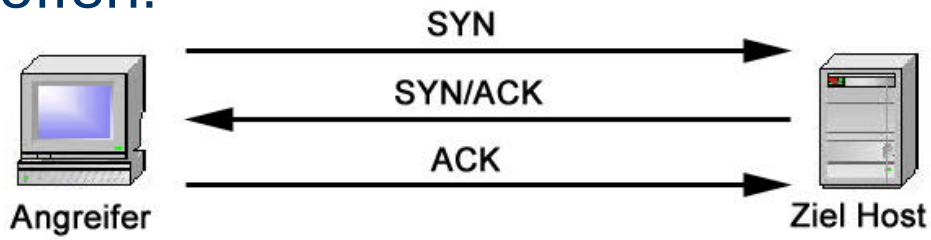
Portscanning Übersicht

- Third-party und spoofed TCP Scannen
  - FTP bounce Scannen
  - Proxy bounce Scannen
  - Sniffer-based spoofed Scannen
  - IP ID Header scannen

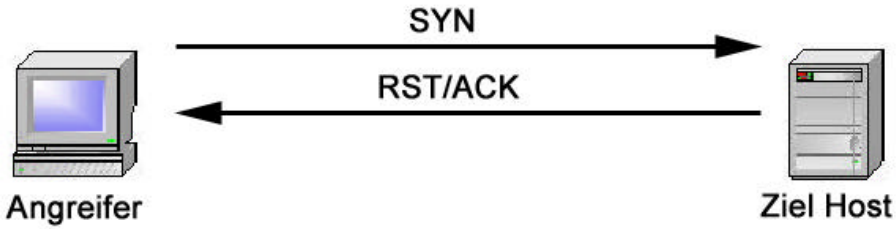
Offenes TCP Scannen

- TCP connect()

  Port offen:



  Port geschlossen:

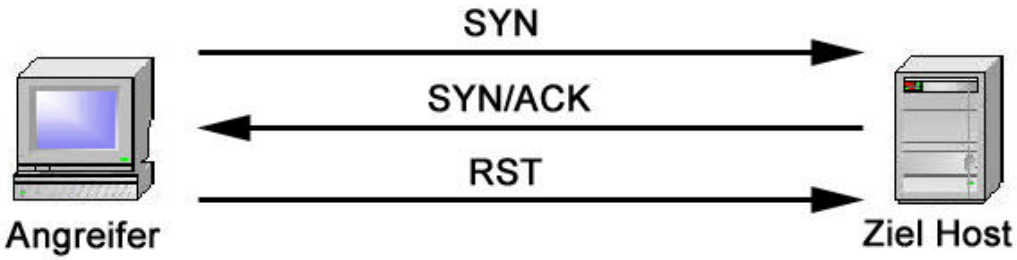


- Vorteil: Sehr genaue Ergebnisse
- Nachteil: Wird durch Logging erkannt

Stealth TCP Scannen

- Halb-offenes SYN Flag Scannen

  Port offen:



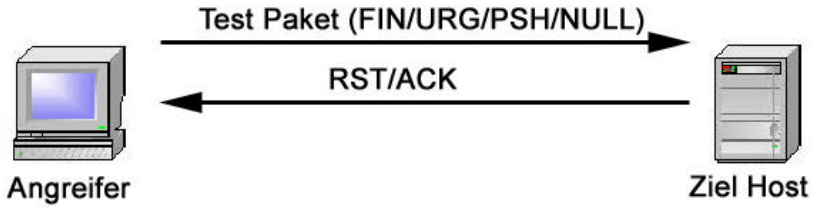
- Vorteil: geringere Gefahr durch Logging
- Nachteil: Nur als Super-User möglich, da RST Pakete „erstellt“ werden müssen

Stealth TCP Scannen

- Inverses TCP Flag Scannen

  Port offen:

  Port geschlossen:



- Vorteil: Schwer aufzuspüren
- Nachteil: Nicht möglich bei Windows Rechnern

Stealth TCP Scannen

- ACK Flag Probe Scannen

- Analyse des TTL oder Window Feldes, der Pakete
- Die Werte unterscheiden sich bei offenem/geschlossenem Port
- Vorteil: Schwer aufzuspüren
- Nachteil: Zeitaufwändige Analyse und basiert auf Implementierungsfehler

Port Scanning Techniken

- Motivation
- Exkurs: Intrusion Detection Systeme
- Verfahren
  - Slow Scan
  - Fragmentation Scan
  - Decoy
  - Coordinated Scans
- Gegenmaßnahmen

Motivation

- Erkannte Scans können als Vorbereitung eines Angriffs erkannt werden
- Abwehrmaßnahmen und Maßnahmen gegen Angreifer sind nicht erwünscht
- Konsequenz: Scans bzw. Urheber müssen verschleiert werden

Exkurs: Intrusion Detection Systeme

- Intrusion Detection Systeme (IDS) suchen in Echtzeit oder in Logfiles nach Mustern eines Angriffs
- Muster heißt z.B. auffällige Häufung von Anfragen in einem begrenzten Zeitraum

Verfahren

- Slow Scan
  - nur wenige Pakete in langem Zeitraum $\Rightarrow$ taucht nicht in Statistiken auf bzw. nicht in auswertbaren Umfängen
- Fragmentation Scanning
  - IP Pakete werden fragmentiert
  - Erstes Fragment enthält nur Source und Destination, keine Flags oder Payload
  - Paketfilter leiten ohne Überprüfung zum Ziel weiter

Verfahren

- Decoy
  - Falsche Adressen werden übermittelt, zufällige TTL
  - IDS kann einen Angriff feststellen, nicht aber den Verursacher
- Coordinated Scans
  - Gruppe von Angreifern koordiniert Scan
  - In Kombination mit „Slow Scan“ sehr schwer erkennbar, da keine auswertbaren Muster auftreten.

Gegenmaßnahmen

- Verfahren werden verwendet um Gegenmaßnahmen auszuhebeln
- Möglichkeit: Filter feiner einstellen
- Gefahr von „false positives“ steigt mit feineren Filtern

Betriebssystemerkennung

- Motivation
- Verfahren
- Gegenmaßnahmen

Motivation

- Viele Exploits funktionieren nur auf bestimmten Betriebssystemen oder auf verschiedenen Serverversionen
- IP Adressen werden auf „Vorrat“ gescannt für spätere Exploits

Verfahren

- Banner Grabbing
  - Server geben Betriebssystem in „Bannern“ an

```
~> telnet ftp.rub.de
Trying 134.147.32.70...
Connected to sun218.rz.ruhr-uni-bochum.de
Escape character is '^]'.


SunOS 5.8
```

Verfahren

- Stack fingerprinting – der OS TCP/IP-Stack wird getestet
  - FIN Probe – FIN Paket wird an offenen Port gesandt, nach Standard darf nicht geantwortet werden
  - BOGUS Flag Test – undefinierter TCP-Flag im TCP Header eines SYN-Paketes

Verfahren

- Sammeln von TCP Sequenznummern – verschiedene TCP/IP-Stacks verwenden verschiedene Verfahren
- Don't Fragment bit gesetzt oder nicht
- TCP Initial Window – überprüfen der „window size“ von Antwortpaketen

Verfahren

- ICMP Error Message Quenching – wie wird die Wiederholungsrate der Error Messages begrenzt
- TCP Optionen – freiwillige Implementation, Anfrage mit bestimmten Argumenten $\Rightarrow$ unterschdliche Stacks reagieren verschieden

Gegenmaßnahmen

- Banner abstellen oder fälschen
- Keine „verräterischen“ Host-Namen verwenden
- Application Proxies verwenden
- Langfristig: TCP/IP-Stacks stärker standartisieren
- Kurzfristig: Wenn möglich selbst Parameter des Stacks ändern

Scannen durch eine Firewall

- Non-Echo-Request ICMP Pakete für Anfragen verwenden, diese werden von Firewalls oft nicht geblockt
- Ports von Firewalls mit verschiedenen Protokollen testen, um Regelsatz der Firewall nachzuvollziehen
- Anschließend kann man mit verschiedenen Verfahren die Struktur hinter der Firewall testen (Firewalking)

NMAP - Quelle

- Nmap - DER Portscanner schlechthin, bietet eine Vielzahl von Optionen zum Scannen und eine recht zuverlässige Betriebs-systemerkennung - www.insecure.org (unixoide Plattformen), www.eeye.com/html/Research/Tools/nmapNT.html (Windows Plattformen)

NMAP – Scan Typen

- NMAP unterstützt alle oben genannten Scanmodi; z.B. führt:
  - Nmap –sU Ziel_IP einen UDP Scan durch
  - Nmap –sT Ziel_IP einen TCP connect() aus
  - Nmap –sS Ziel_IP einen TCP SYN Scan aus
  - Nmap –sP Ziel_IP einen ICMP Sweep durch
  - Nmap –sO Ziel_IP einen IP Protocol Scan aus

NMAP – Scan Typen

- Weitere unterstütze Scan Typen sind:
  - SYN Sweep
  - FIN/ACK Sweep
  - XMAS/NULL Flag Scanning
  - FTP Bouncing
  - Reverse Ident Scanning
  - Fragmentation Scanning
  - Decoy Scanning

NMAP – Timing Optionen

- NMAP bietet verschiedene Timing Optionen, um:
  - Intrusion Detection Systeme zu hintergehen (Slow Scan)
  - Scanvorgänge in Bezug auf die vorliegende Netzwerk Infrastruktur zu opimtieren (Bandbreite)
- Folgende Optionen sind möglich:
  - -host_timeout: Dauer, für die ein Host gescannt wird

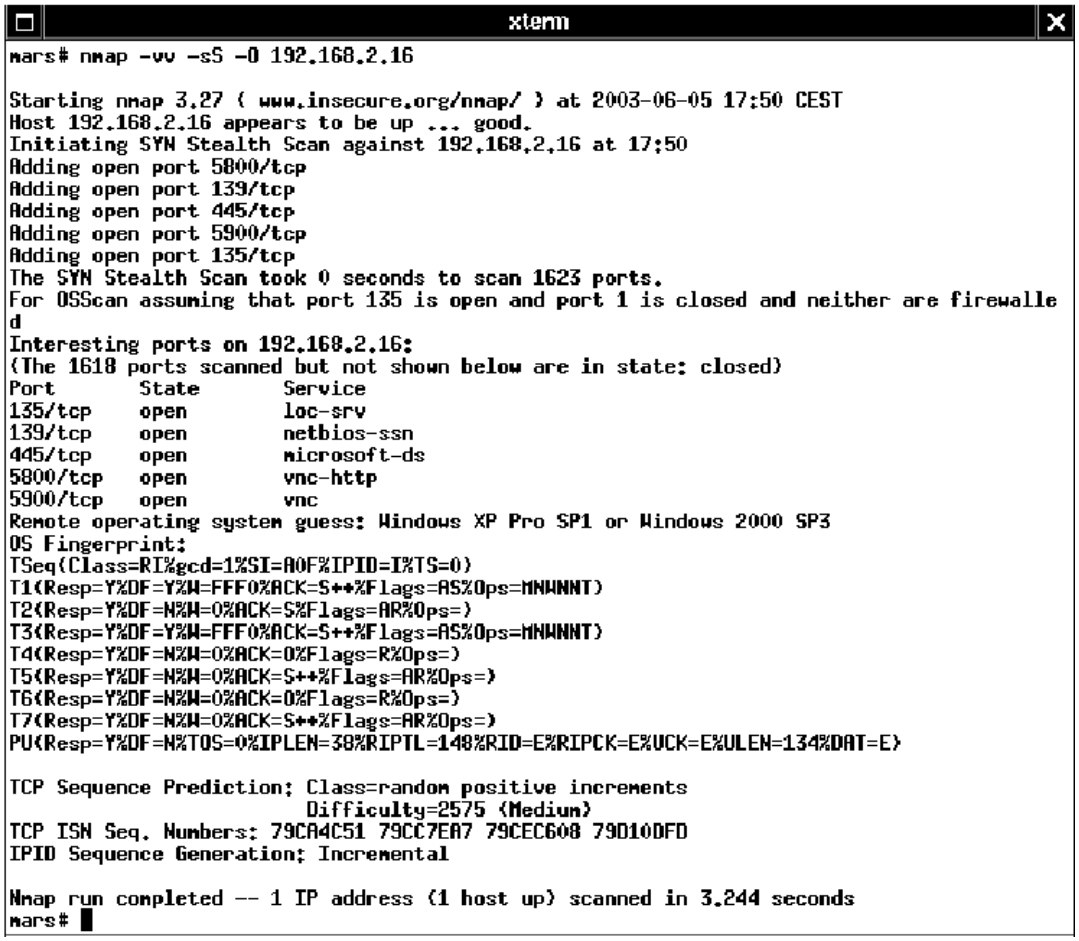
NMAP – Timing Optionen

- -max_/min_/initial_rtt_timeout: maximale/minimale/anfangs Zeit, die auf eine Antwort gewartet werden soll, bevor ein Timeout gemeldet wird
- -max_parallelism: maximale Anzahl paralleler Scans
- -scan_delay: Pause zwischen zwei Testpaketen
- -T: legt eine vordefinierte Timing Policy fest, die alle o.g. Parameter beinhaltet

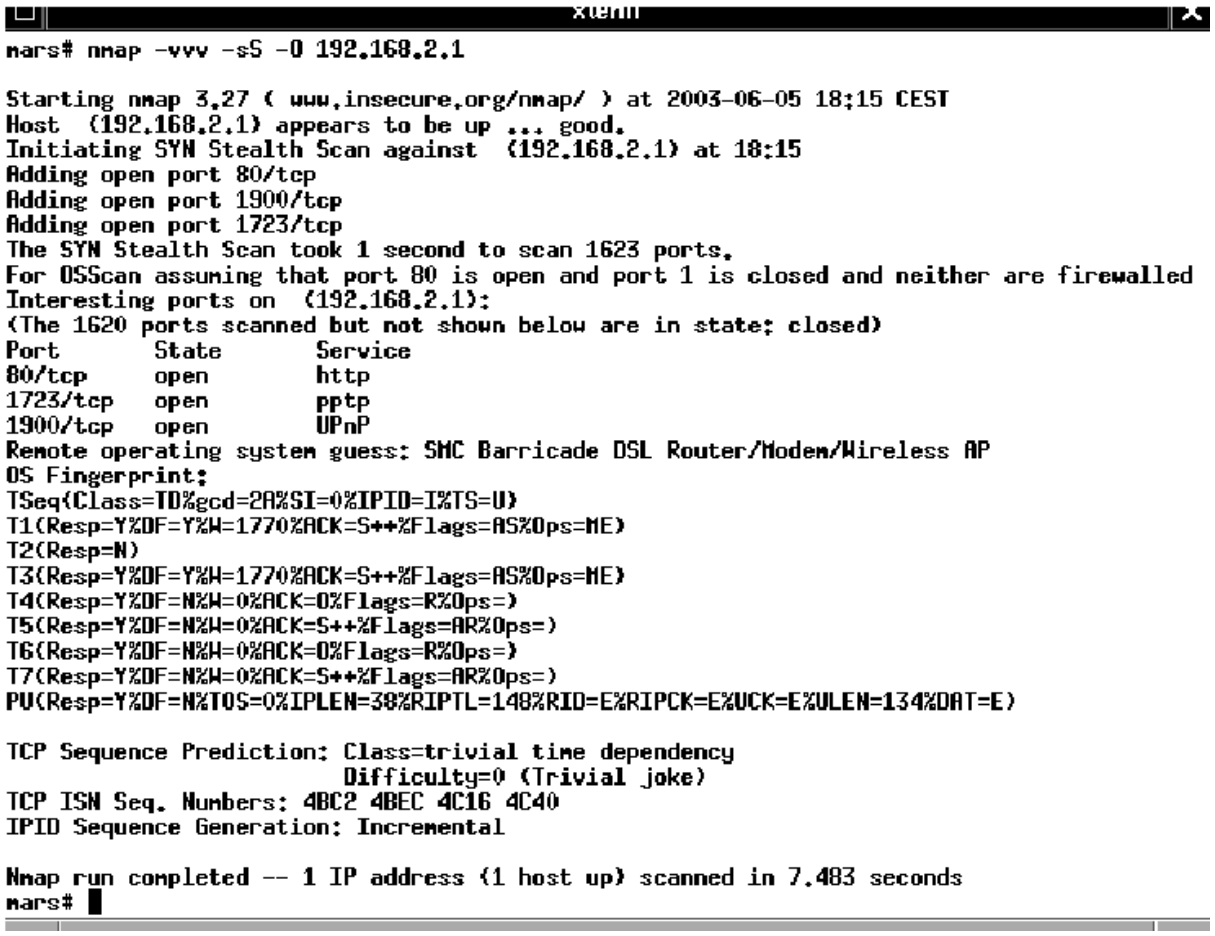
NMAP für den Administrator

- NMAP hilft nicht nur Angreifern
- Durch scannen des „eigenen“ Netzes kann ein Admin die Hosts finden, die von „außen“ sichtbar sind
- Die Konfiguration bzw. das Regelwerk einer Firewall können mit NMAP Scans überprüft werden
- Die Anfälligkeit gegenüber DoS Attacken kann geprüft werden

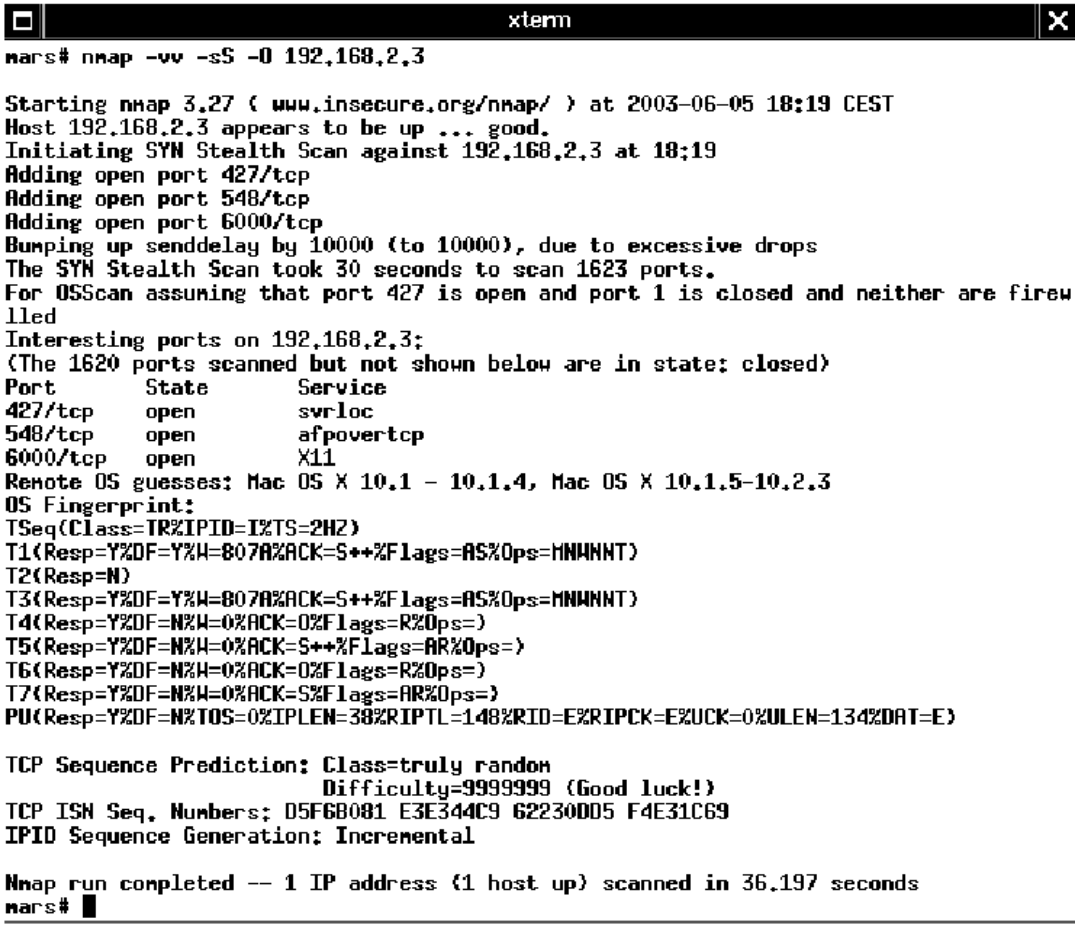
NMAP Scan: Windows XP SP 1



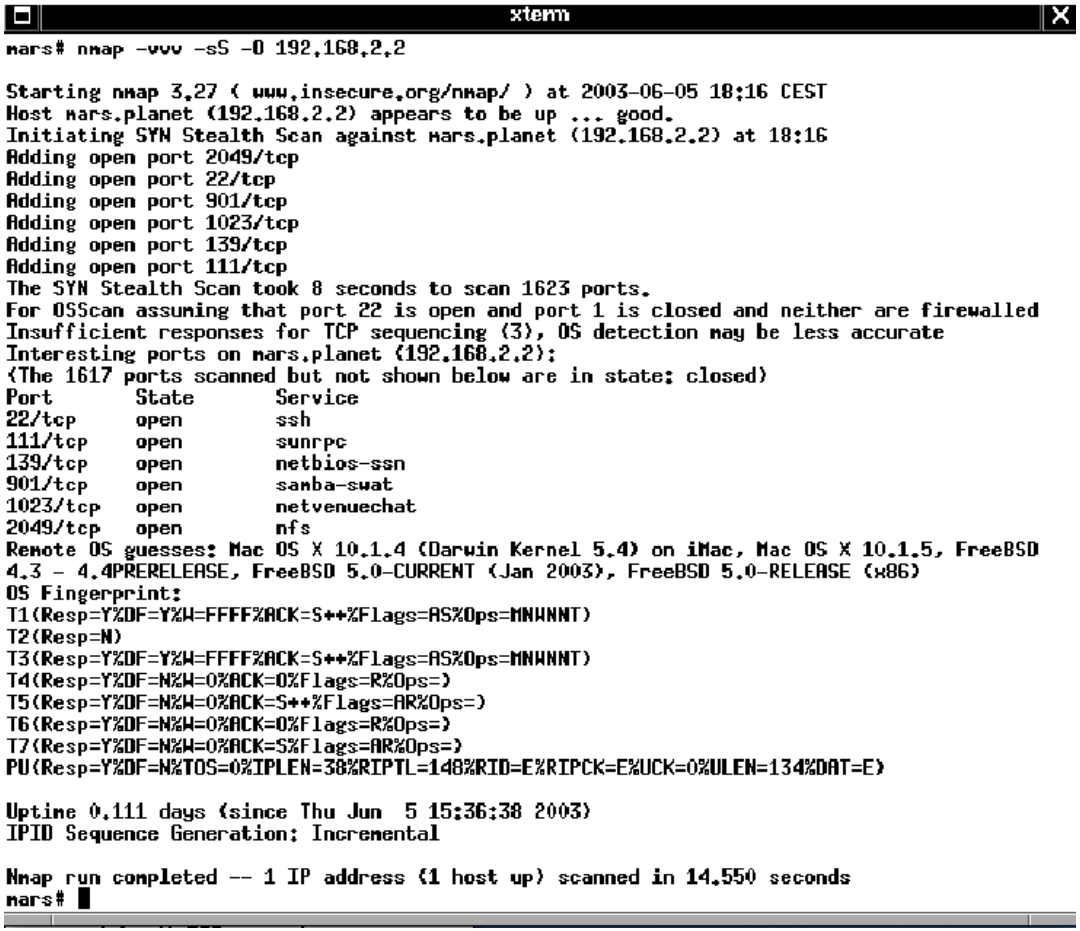
NMAP Scan:
SMC Barricade DSL Router



NMAP Scan: Mac OS X



NMAP Scan: FreeBSD 5.1



Fazit

- Scannen von Netzwerken kann verschiedenen Zwecken dienen: defensiv, zum Absichern des eigenen Systems, oder offensiv, zum Ausspähen eines Ziels für Cracker
- Scanner sind Alltag geworden, sowohl automatisierte, als auch manuelle Varianten
- Kenntnisse von Verfahren und Funktionen wichtig, um Sicherheit der eigenen Hosts zu gewährleisten