

Einführung in die Informationssicherheit

Florian Mendel

Institute for Applied Information Processing and Communications (IAIK)

Graz University of Technology
Inffeldgasse 16a, A-8010 Graz, Austria



<http://www.iaik.tugraz.at/>

L4 – Netzwerksicherheit

Einführung in die Informationssicherheit

Übersicht

- Vorfälle
- Wie greift man ein Netzwerk an:
 - Social engineering
 - OS Fingerprinting
 - Attacking Internet protocols
- Wie schützt man ein Netzwerk:
 - Intrusion detection systems – Firewalls
- Was kann man mit SSL, SSH etc. erreichen

Berühmte Vorfälle – The Internet Worm

- Geschrieben von Robert Morris, Jr., ein Computer Science Student in Cornell, in 1988
- Das erste experimentelle, sich selbst replizierende, selbst verbreitende Programm (Wurm)
- Lustigerweise hat das Programm sich viel schneller verbreitet als Morris das berechnet hat – es gab einen Bug 😊
- Der Schaden pro infiziertem Computer betrug \$200 bis zu \$53,000

The Internet Worm

- Der Morris-Wurm nutzte:
 - eine Lücke im debug mode des Unix sendmail Programms, und
 - eine Lücke im finger daemon fingerd
- Mehrere Teams an Universitäten arbeiteten mehrere Tage daran den Wurm unter Kontrolle zu bringen
- Robert T. Morris wurde im Sinne des Computer Fraud and Abuse Act (Title 18) schuldig gesprochen und das Urteil bestand aus:
 - 3 Jahre auf Bewährung,
 - 400 h Wohltätigkeitsarbeit,
 - Geldstrafe \$10.050,
 - Sein Gesuch auf Begnadigung 1990 wurde abgelehnt

Weitere Vorfälle

Love Letter Worm (2000)

- Infizierte Systeme mit Microsoft Windows die den Windows Scripting Host enabled hatten
- Der “*Love Letter*” Wurm war ein schadhaftes VB-Script das mehrere Wege der Verbreitung hatte:
 - E-mail,
 - Windows file sharing,
 - IRC, USENET news, etc.
- Der Wurm modifizierte alle möglichen Dateien um sich weiterzuverbreiten

SQL-Slammer (2003)

- Nutzte Schwachstellen im Microsoft SQL Server 2000 und Microsoft Desktop Engine (MSDE) 2000
- Sobald der Wurm einen Rechner infiziert hat, versucht er sich weiterzuverbreiten
 - Der Wurm versendet sich über speziell aufbereitete 376-bytes und sendet diese an zufällige IP Adressen über Port 1434/UDP
 - Wenn so ein Paket auf einen anfälligen Rechner trifft, beginnt dieser auch, Pakete an zufällige IP Adressen zu versenden
- Der hohe 1434/udp traffic durch die infizierten Hosts führte zu großen Leistungseinbußen (inkl. denial-of-service)

Stuxnet (2010)

- Mit Stuxnet wurde ein neues Zeitalter der Cyberwarfare eingeläutet
- Nutzte 4 Zero-Day-Exploits in 32-bit Windows-Systemen
- User-Mode und Kernel-Mode Rootkits
 - Device-Treiber wurden digital unterschrieben mit gestohlenen privaten Schlüsseln
- Zudem maßgeschneidert auf Steuerungssoftware für Industrieanlagen von Siemens
- 60% der infizierten Rechner standen im Iran
- Hoher Grad an technischem Knowhow und Manpower notwendig (Regierungsbeteiligung?)

Flame (2010)

- Großteil der infizierten Rechner standen im Nahen Osten
- Großes Programm $\approx 20MB$, breitet sich über LAN oder USB aus
- “Encrypted” Malware
- Unterstützt einen Kill-Befehl – löscht alle Spuren der Malware auf dem Computer
- Die Entwickler verwendeten hochentwickelte kryptographische Angriffe “*Rogue CA*” um ein gültiges Code Signing Zertifikat von Microsoft (basierend auf MD5) verwenden zu können (Regierungsbeteiligung?)


CERT Definition of “Incident”

“The act of violating an explicit or implied security policy:”

- Versuch, (erfolgreich oder erfolglos) unerlaubten Zugang zu einem System oder seinen Daten zu erhalten
- Unerwünschte Unterbrechungen oder Denial-of-Service
- Das unerlaubte Benutzen eines Systems zum Verarbeiten oder Speichern von Daten
- Änderungen der System-Hardware, Firmware, oder Software ohne das Wissen, die Zustimmung des Eigentümers

<http://www.cert.org>

SANS – SysAdmins, Audit, Network, Security



[why SANS?](#)[pick a course](#)[why certify?](#)[register now](#)

The most trusted source for computer security training, certification and research.

[training](#)[certification](#)[resources](#)[vendor](#)[portal](#)[storm center](#)[college](#)[developer](#)[about](#)

Top 20 Internet Security Problems, Threats and Risks

Check out the new Top Cyber Security Risks document.
www.sans.org/top-cyber-security-risks

Featuring attack data from TippingPoint intrusion prevention systems protecting 6,000 organizations, vulnerability data from 9,000,000 systems compiled by Qualys, and additional analysis and tutorial by the Internet Storm Center and key SANS faculty members. [more >>](#)

For a continuous update on the SANS Top 20 vulnerabilities, subscribe to [@Risk](#). If you would like the Executive Summary pointing out newsworthy highlights of the SANS 2007 Top Internet Security Risks, [click here](#).

Client-side Vulnerabilities in:

- C1. Web Browsers
- C2. Office Software
- C3. Email Clients
- C4. Media Players

Server-side Vulnerabilities in:

- S1. Web Applications
- S2. Windows Services
- S3. Unix and Mac OS Services
- S4. Backup Software
- S5. Anti-virus Software
- S6. Management Servers
- S7. Database Software

Security Policy and Personnel:

- H1. Excessive User Rights and Unauthorized Devices
- H2. Phishing/Spear Phishing
- H3. Unencrypted Laptops and Removable Media

Application Abuse:

- A1. Instant Messaging
- A2. Peer-to-Peer Programs

Network Devices:

- N1. VoIP Servers and Phones

Zero Day Attacks:

- Z1. Zero Day Attacks

Best Practices for Preventing Top 20 Risks

<http://www.sans.org/top20/>

Social Engineering

- Der Mensch scheint in den meisten Systemen am anfälligsten zu sein
- Es gibt verschiedene Definitionen:
 - *“The art and science of getting people to comply to your wishes”*
 - *“... getting needed information from a person rather than breaking into asystem”* – <http://packetstorm.deceptions.org/>
 - *“An outside hacker’s use psychological tricks on legitimate users of a computer system, in order to obtain information one needs to gain access to the system”* – <http://www.sans.org/>

Ziele von Social Engineering Attacken

- Physical access
 - Angriff auf Vertraulichkeit, Integrität, Authentizität, etc.
- Remote access credentials
 - Passwörter und andere Zugangsdaten (z.B. Handy, etc.)
- Information
 - Kundendaten, Source Code , Pläne, etc.
- Umgehen von Sicherheitskontrollen
 - Opfer führen Code aus, überweisen Geld, etc.

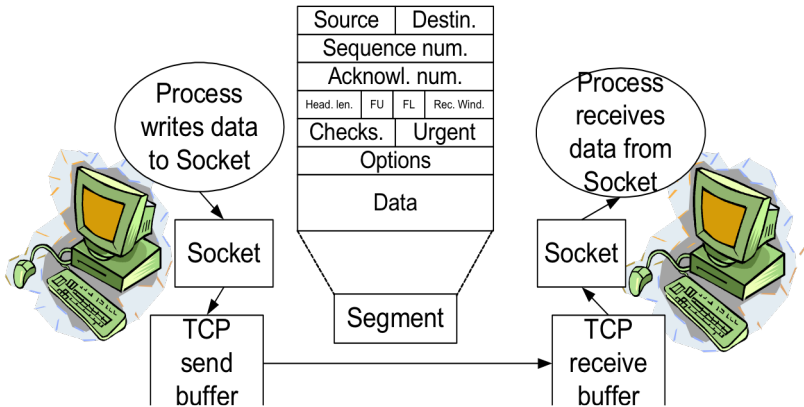
OS Fingerprinting

- Ist eine Methode um das Betriebssystem eines Rechners herauszufinden
- Ist sehr oft der erste Schritt in einer Attacke
 - Kennt der Angreifer das OS, dann weiß er auch, auf welche Sicherheitslücken er schauen soll
- Plumper Versuch: Öffnen einer Telnet Session
 - Viele Telnet-Server geben viel Info über OS preis
- Andernfalls, kann man TCP dazu benutzen

TCP –Transmission Control Protocol

- Ist ein Verbindungs-orientiertes Protokoll
- Features
 - Stream data transfer
 - Die Applikation braucht sich nicht um große Datenmengen kümmern, das macht TCP
 - Reliability
 - Data bytes werden acknowledged
 - Full duplex
 - Gleichzeitiges Senden und Empfangen

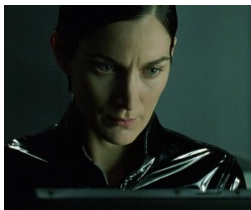
TCPSegments



- Flags: URG, PSH, ACK, RST, SYN, FIN

TCP Stack Fingerprinting

- OS implementieren den TCP Stack zum Teil sehr unterschiedlich
 - Indem man spezielle Pakete an einen TCP-Server schickt, kann man anhand der Antworten des Servers das OS erkennen
- Tools die diesen Ansatz implementieren gibt es im Netz:
 - Nmap ist eines der Bekanntesten (www.insecure.org)



```
60/tcp open      http
61/tcp open      http2-ns
62/tcp open      [mobile]
10 # nmap -v -sS -O 10.2.2.2
11
12 Starting nmap V. 2.54BETA25
13 Insufficient responses for TCP sequencing (3). OS detection
13 accurate
14 Interesting ports on 10.2.2.2:
15 (The 1539 ports scanned but not shown below are in state: c)
51 Port      State      Service
52 /tcp      open       ssh
53
54 No exact OS matches for host
55
56 Nmap run completed -- 1 IP address (1 host up) scanned
57 # schuko 10.2.2.2 -rootpw="210H0101"
58 Connecting to 10.2.2.2:ssh ... successful.
59 Attempting to exploit SSHv1 CRC32 ... successful.
60 IP Reseting root password to "210H0101".
61 System open: Access Level (9)
62 # ssh 10.2.2.2 -l root
63 root@10.2.2.2's password:
64
```

ACCESS CONTROL:
ACCESS GRANTED

Movie: The Matrix Reloaded

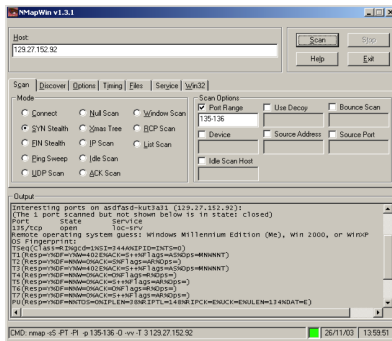
TCP Stack Fingerprinting

Typische Attacken die über TCP auf OS schließen:

- FIN probe
 - Sendet FIN Paket an offenen Port, laut RFC 793 soll der Server darauf nicht antworten, aber die Windows-Implementierung tut es
- ACK value
 - OS benutzen unterschiedliche hex-Werte im ACK-Feld des TCP-Pakets
- ICMP error messages
 - Die Anzahl an Fehlermeldungen ist beschränkt und hängt vom jeweiligen OS ab

Nmap

- Tool für TCP stack Fingerprinting
- Nmap liest aus einem File mit Fingerprint Templates:
 - Die Antworten des Servers werden mit den Fingerprints verglichen und das wahrscheinlichste OS bestimmt



<http://nmap.org/book/osdetect.html>

Attacking Internet Protocols



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

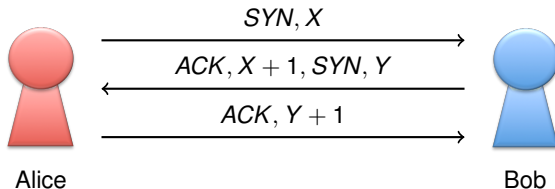


Software Engineering Institute
Carnegie Mellon

SYN Flooding

- Angriff auf TCP-Handshake

- Der Angreifer sendet eine große Menge SYN Pakete an einen Host und lässt die Repls un-acknowledged
- Bekannt seit den 1980er Jahren



- Technische Lösung: SYNcookie

- Das von Bob gesendete $Y = Enc(X)$

Smurfing Attacks

- Nutze eine Lücke im ICMP Protokoll:
 - Echo-Pakete können benutzt werden um zu überprüfen, ob ein Host am Leben ist
 - Implementierungen reagierten auf Pings an Broadcast-Adressen
- Der Angreifer produziert Pakete mit gefälschter IP Adresse:
 - Die gefälschte Adresse ist die des Opfers
 - Das Opfer wird durch Echo-Replys überflutet
- 1999 wurde der ICMP-Standard abgeändert um diese Attacke nicht mehr zuzulassen

DDoS Attacks

- Distributed denial-of-service Angriffe gehören zu den verheerendsten Angriffen
- Ein Angreifer
 - übernimmt eine große Anzahl an Remote-Rechnern (Bot-Net)
 - installiert darauf die Attack-Software
- Auf ein Signal wird das Opfer mit Angriffen bombardiert
- Gegenmaßnahme: ICMP traceback messages
- Muss nicht immer bösartig sein:
 - Univ. of Wisc.-Madison: ≈ 100.000 packets per second due to 700.000 routers requesting the time (2003)

Spoofing

- Eve will sich für Alice ausgeben und will eine Verbindung mit Bob herstellen:
 - Kombination aus mehreren Techniken
 - DDoS-Attacke um Alice handlungsunfähig zu machen
 - Erraten der Sequence Numbers die zwischen Alice und Bob benutzt würden (um sich als Alice auszugeben)
 - Das funktioniert wegen schlechten Implementierungen
- Gegenmaßnahme: Inspizieren der Antwort auf SYN+ACK Pakete

Attacken auf andere Protokolle

- DNS cache poisoning

- Server validiert DNS responses nicht (z.B. über DNSSEC)
- Server fügt gefälschte Einträge im Cache hinzu
- Server verteilt gefälschte Einträge weiter

- BGP route hijacking

- youtube.com wurde von pakistanischem ISP versehentlich gehijacked
- Sollte eigentlich 3 IP-Adressen blocken
- `https://www.arbornetworks.com/asert/2008/02/internet-routing-insecuritypakistan-nukes-youtube/`

Attacken auf andere Protokolle

- TCP Sockstress – durch grundsätzliche Probleme in TCP kann jeder beliebige Server der TCP Verbindungen annimmt sehr einfach vom Netz genommen werden.
 - Viele Möglichkeiten: Zero window stress, small window stress, ...
 - <http://www.checkpoint.com/defense/advisories/public/announcement/090809-tcpip-dos-sockstress.html>
- ARP cache poisoning
 - Viele LANs verwundbar
 - Man schickt gefälschte ARP messages in ein LAN
 - Ziel ist es, die MAC-Adresse des Angreifers mit der eines gültigen Hosts zu verbinden
 - Traffic für den Host geht dann zum Angreifer

IDS und Firewalls

- Firewall

- Policy based
- Soll Attacken verhindern

- Intrusion Detection System (IDS)

- Traditionellerweise wird versucht, Angriffe nachträglich aufzuspüren
- Moderne Systeme: Pro-aktiv, blockiert Angriffe

Firewalls

- Packet filtering
 - Inspizieren der Header-Information eines jeden Pakets
- Application gateways
 - Inspiziert den Traffic einer Verbindung oder eines Service
- Circuit-level gateways
 - Steht wirklich zwischen Host und Netzwerk

Intrusion Detection Systems

- Versuchen abnormales Verhalten mit verschiedenen Methoden zu entdecken:
 - Statistische Methoden
 - Regel-Basiert
 - Neuronale Netzwerke
- Arten von IDS:
 - Logfile monitors
 - Integrity monitors
 - Signature matchers
 - Anomaly detectors

Was kann SSL, SSH, etc. für uns tun?

- Diese Tools (Protokolle) stellen kryptographische Techniken zur Verfügung und garantieren daher:
 - Vertraulichkeit
 - Integrität
 - Authentizität
 - Non-repudiation
- Sie helfen nicht gegen DDoS, spoofing, etc.
- Früher: Protokolle für jede App:
 - POP, IMAP, TELNET, FTP, ...
- Heute eher: HTTP mit Schutz über SSL/TLS

Transport Layer Security (TLS) – SSL

- Session basierte Authentication und Verschlüsselung
 - Bietet einen sicheren Kanal zwischen Sender und Empfänger
- Setzt am Transport Layer an:
 - Unabhängig von der Applikation
- Basierend auf X.509v3 Zertifikaten
- Benutzt eine Vielzahl kryptographischer Techniken und Algorithmen (Cipher-Suites)
- Sichert nur die Verbindung, nicht den Sender/Empfänger

Transport Layer Security (TLS) – SSL

- Sicherheitsprobleme:

- Offene WLANs
- ARP cache poisoning
- HTTP session stealing (XSS)
- Angriffe auf den Browser
- Amazon '10 (switched zurück auf HTTP)

Secure Shell – SSH

- Wurde als Alternative zu komplett unsicheren Protokollen eingeführt:
 - rlogin, ftp, telnet, etc.
- SSH Version 2 ist der aktuelle Standard
 - SSH1 wurde ziemlich überarbeitet
- Hat auch eine große Zahl Algorithmen zur Verfügung für
 - Authentication
 - Confidentialty
- Basiert NICHT auf X.509 Zertifikaten
 - Kann sie aber benutzen, ebenso PGP Zertifikate

Internet Protocol Security – IPSec

- Kombiniert Standards um Network Security zu gewährleisten
 - Authentication und Verschlüsselung am Network layer
- IP Pakete werden verschlüsselt (re-formattiert)
- Zwei grundlegende Protokolle:
 - Authentication header protocol
 - Encapsulating security protocol
- Sehr umfangreich und komplex!

Zusammenfassung

- Netzwerksicherheit wird gefährdet durch:
 - DAUs
 - Böswillige Software
- Gegenmaßnahmen können nicht auf Kryptographie alleine basieren
 - Firewalls
 - Intrusion detection
- Kryptographie kann Verbindungen sicher machen, aber nicht Computer!

Vielen Dank für Ihre Aufmerksamkeit!