Security

D. Schüler

Lokale Sicherheit

- Tagesarbeit nicht als Admin/Root!
  - Nutze sudo und su stattdessen
- Nutze starke Passwörter
  - Mindestens 8, besser 10 Zeichen
  - Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen
  - Für jeden Zweck ein anderes Passwort
- /etc/passwd und /etc/shadow enthalten die Logins und Passwörter sowie Gruppen-zuordnungen

Softwarebezug

- Software nur aus vertrauenswürdigen Quellen verwenden → Repository der Distribution
- RPMs und DEBs sind nur gepackte Binary-Pakete → was macht die Software im Hintergr.
- Quellcode (wenn aus nicht vertrauenswürdiger Quelle) immer inspizieren oder alternative suchen. → Foren lesen, Experten fragen
- Was Viele verwenden ist meist vertrauens-würdig → große Projekte (Apache, MySQL, ...)

Dateisicherheit

- Rechteverwaltung
  - Lesen/Read
  - Schreiben/Write
  - Ausführen/Execute
  - Sticky bit
  - SUID (set user id)
  - SGID (set group id)

Dateisicherheit (Mehrnutzersysteme)

- /home und /var müssen keine ausführbaren Dateien enthalten → nosuid, noexec, nodev mounten
- „*last*“ zeigt die Loginzeiten und -orte aller Nutzer → ein regelmäßiger Blick lohnt
- Regelm. Integritätscheck über Systemdateien als Angriffsfrüherkennung → tripwire, osiris
- Hashes der Systemdateien als USB-Stick mit Schreibschutz am Server/Workstation

Sichere Kommunikation

- PGP/GPG → unsymetrische Verschlüsselung für alle Daten, meist eMail oder Dateien
  - Vertrauen durch persönlichen Kontakt oder durch Kontakt über Dritte
  - Ende zu Ende Verschlüsselung. Sehr Sicher, aber auch recht Umständlich.
- HTTPS → HTTP über SSL
  - Vertrauen durch Root-Zertifikate im Browser
  - Anfällig für Man-In-The-Middle Attacken

Remote Zugriff

- Keinesfalls rlogin, rsh oder telnet verwenden!
  - Übertragung aller Daten unverschlüsselt.
- Stattdessen ssh, scp, sftp → immer Version 2!
  - Verschlüsselung aller Daten (unsym. Schlüssel)
  - Login über Login/Passwort oder Public-Key
  - Login nur von vertrauenswürdigen Quellen

Grundlegende Netzwerksicherheit

- Aktivierung der Firewall → iptables
  - Nicht unbedingt bei Workstations nötig
  - Wichtig bei Servern und Routern → Logging
- Schutz gegen SYN-Floods durch SYN-Cookies
  - Nutzen die Sequence-Number im TCP-Header
  - Keine Servereigenen Ressourcen werden benötigt

Packet Sniffing

- NIC akzeptiert alle Datenpakete (promiscuous mode)
- Sniffing im „switched Network“ mittels ARP-Spoofing → wir geben uns als Router aus.
- Anreifer sucht nach Daten mit z.B. „passwd“ „login“ oder „su“ um Logins zu sniffen.
- Besonders gefährlich im WLAN → macht nicht an der Mauer halt und funktioniert wie ein Hub
- Tools: wireshark, tcpdump, (kismet)

Firewall

- iptables
  - Nutzt Ketten („chains“) für die Regulierung der Datenpakete
  - INPUT, OUTPUT, FORWARD
  - Jede chain wird Zeile für Zeile abgearbeitet
  - Passt ein Paket auf eine Zeile wird es akzeptiert, verworfen, zurückgewiesen oder geloggt
  - Tabellen für FILTER, NAT, MANGLE und RAW

Application Security

- Buffer Overflow

```
void input_line() {
        char line[1000];
        if (gets(line))
                parse_line(line);
}
```

XSS & CSRF

- Eingaben in Web-Formularen werden nicht auf HTML-Code geprüft.
- Angreifer schreibt JavaScript-Code in ein Gästebuch/Forum/Blog-Comment/etc.
- Code wird bei jemdem Besucher ausgeführt → z.B. stehlen von Session-IDs des Nutzers
- Mittels CSRF z.B. Bestellungen oder Einstellungen auslösen auf Seiten auf denen der Nutzer gerade eingeloggt ist.

SQL Injection

- Ungefiltertes einfügen von Datensätzen in SQL

```
INSERT INTO gb (`name`,`greet`)
VALUES ('$name','$greet')
```

- Was passiert wohl nun?

```
…&greet=');SELECT * FROM `logins`;--
```

- Beliebiger SQL-Code einschleusbar.
- Immer auf Typ prüfen → Zeichenketten escapen (\') → Zahlen typisieren (intval($x)).

- Local & Remote (root) Exploit
- DoS & DDoS / PoC
- Rootkits
- Drive-by-Download
- XSS & CSRF
- SQL Injection
- Buffer Overflow
- Hash Tables, Brute Force
- HIDS & NIDS, snort
- MITM
- DNS spoofing
- Botnet
- Trojan horse
- Teardrop Attack
- Eavesdropping
- Packetsniffing
- Blue-/Airsnarfing
- Vulnscanner
- Pentests