TCP/IP Penetrationsmöglichkeiten

Vortrag: *Felix von Leitner* <fefe@ccc.de>

Bericht: *Dieter Kirchner* <dieter@roko.goe.net>

Es gibt mehrere verschiedene Klassen von Penetrationsmöglichkeiten bei Rechnern in TCP/IP-basierten Netzen:

1. Fehlkonfigurationen, Dienste sind nicht abgeschaltet.

Dies ist die häufigste einzelne Ursache von Angriffen. Oft sind Patches und Updates der Serversoftware nicht eingespielt, gelegentlich braucht der (proprietäre) Hersteller der Software auch einige Zeit, um diese Bugfixes zu entwickeln. Oft werden unnötige Dienste nicht abgeschaltet, was teilweise auch durch die Linux-Distributionen begünstigt wird, die alle möglichen Dienste erst einmal defaultmäßig starten, aber nicht unbedingt sicher konfigurieren. Firewalls und Router sind dabei besonders tückisch, z.B. werden default-Paßwörter nicht geändert oder Standardaccounts eingetragen. Beispiel für eine Fehlkonfiguration: ist das Relaying von Mails nicht abgeschaltet, so ist es Spam-Mailern möglich, den Server zu mißbrauchen. Einige Dienste sind inhärent unsicher wie NFS, NIS, telnet und rlogin.

2. Buffer Overflows.

Beispiel im Code:

```
void bla (char *s) { char buf[199]; strcpy (buf,s); }
```

Sehr häufig, teilweise auch in Library -Funktionen (z.B. syslog()). Dieses Phänomen ist ein Bug im Programm oder dessen Bibliotheken, betroffen sind beispielsweise MS-Exchange, wu-ftpd, Netscape, MSIE, sendmail, Outlook, Outlook Express, MS IIS usw. Diese Bugs finden sich in allen Betriebssystemen. Auf diese Angriffsmethode wurde auch in einer anderen Veranstaltung eingegangen (-> Stack Exploits).

3. Metazeichen nicht "escaped".

Beispiel für eine URL:

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

Wenn Shellscripte oder andere Scriptsprachen benutzt werden, müssen alle Metazeichen escaped werden. Viele Freeware CGI-Scripte haben damit Probleme, aber auch das ::$DATA-Problem bei NT-Webservern wird dadurch verursacht. Der Ansatz ist die Übertragung von Steuersequenzen an Programme, die vom Webserver ausgeführt werden. Dies umgeht der Programmierer der Scripte durch eine Liste von Ausdrücken, die er als Programmeingabe durch den Webserver zuläßt. Richtig ist eine Whitelist, also nur erlauben, was nötig ist, nicht aber blacklisten, wo nur weniges explizit verboten wird. Liberale Einstellungen lohnen sich nicht in diesem Bereich :-)

4. Passwörter gesnifft

Alle Programme, die unverschlüsselte Authentifizierung benutzen, sind gefährdet, also ftp, telnet, pop3 und imap. Der Angriffspunkt ist dabei ein Rechner, der physikalischen Zugriff auf die Kabel hat, also dort über eine Netzwerkkarte angeschlossen ist. Da alle Pakete in einem ungeswitchten Netz auch bei dieser Netzwerkkarte ankommen oder über den Computer geroutet werden (deswegen sind Router ein Hauptziel für Angriffe!), können sie mitgelesen werden. Passwörter/Loginkombinationen stehen im Klartext in den Datenpaketen und verraten damit die Accounts von Nutzern.

5. Passwörter gecrackt

Viele Fehler in Software erlauben zwar nicht, als root Code auszuführen, aber sie machen es möglich, die /etc/passwd zu lesen oder aber die NIS -Datenbank abzufragen. Damit können dann Accounts auf dem Zielsystem geknackt werden, über die weitere Angriffe ausgeführt werden können. Der empfohlene Passwort-Cracker ist John the Ripper, zu finden unter ftp.congress.ccc.de/pub/unix/security, um aus der passwd mit Hilfe eines Wörterbuches die Paßwörter zu knacken.Passwortsynchronisation zwischen vielen Rechnern reißt oft aber Lücken, die sichere Paßwortsysteme wie das shadow-Verfahren aushebeln. Alternativen sind in diesem Bereich Tivoli oder Kerberos, wobei Kerberos ebenso wie NIS+ Schwächen aufweist.

6. TCP-Hijacking

Gemeint ist damit die Übernahme von TCP/IP-Verbindungen, speziell die von One-Time-Passwortschemata, bei denen nur einmal das Paßwort abgefragt wird. Dabei übernimmt man nach der Authentifizierung der Verbindung durch den ursprünglichen Nutzer dessen Verbindung. Dabei wird die Eigenschaft des TCP/IP-Protokolls ausgenutzt, daß die Datenpakete durchnummeriert gesendet werden. Jemand, der in der Mitte der Verbindung nun entsprechend manipulierte Pakete an beide an der Verbindung beteiligten Rechner sendet, kann beiden Rechnern vormachen, er sei der jeweils andere, und übernimmt damit die Kontrolle über die Verbindung (man in the middle). Unter Umständen genügt es auch, parallel zu einem anderen Rechner im Netz zu sein, um einen Versuch zur Übernahme der Verbindung durchzuführen.

7. Hintertüren

Back Orifice und Netbus als Trojaner sind aktuelle Hintertüren für Windowssysteme. Aber es sind auch andere Trojaner für andere Betriebsysteme bekannt. Gelegentlich hinterlassen auch Systemadministratoren und Programmierer Hintertüren in ihren Programmen.

Wie schützt man sich ?

Folgende Regeln helfen:

-Nicht auf die Firewall verlassen.

-Verbindung verschlüsseln.

-Ständige Scans der eigenen Rechner sind nötig.

-Open Source hilft gegen offensichtliche Hintertüren.

-No Microsoft.

-Paßwörter selber cracken, um unsichere vor anderen zu finden.