

IT-SECURITY

Portscanning: Guck' mal, wer da spricht!

Jede Woche beantworten Sicherheits-
experten Leserfragen und geben
Ratschläge, wie sich die Sicherheit in
einem Unternehmen erhöhen lässt.

Frage: Wie funktioniert Portscanning? Wann stellt es eine Bedrohung der Sicherheit dar?

TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) sind bedeutende Protokolle der TCP/IP-Protokoll-Suite. Beide bieten je 65536 (0 bis 65535) Ports, worüber Software angesprochen werden kann (man spricht in diesem Fall von Server-Deamons).

Die Ports 1 bis 1023 werden als «well-known» bezeichnet. Sie benötigen administrative Privilegien, um eine Software an sich zu binden. Die Ports 1024 bis 49151 sind bekannt als registrierte Ports, die Ports 49152 bis 65535 heissen dynamische oder private Ports. Die Internet-Organisation IANA verwaltet die Zuordnung von Applikationen auf Ports.

TCP ist verbindungsorientiert, was bedeutet, dass eine

Verbindung mittels Paketen initialisiert und von der Gegenseite bestätigt wird (three-way handshake). Im Gegensatz dazu ist UDP verbindungslos (fire and forget), es wird keine Bestätigung des Kommunikationspartners erwartet. ICMP (Internet Control Message Protocol) ist ein weiteres Protokoll der TCP/IP-Suite, welches für Verbindungskontrolle und Fehlermeldungen eingesetzt wird.

TCP funktioniert so: Es wird ein Syn-Paket vom Computer A zum Computer B geschickt, dieser bestätigt mittels Syn- oder Syn/Ack-Paket. Als Bestätigung schickt Computer A ein Ack-Paket zu Computer B. Falls kein Daemon auf dem Zielcomputer existiert, wird meist ein Rst-Paket geschickt, um die Verbindung abzubrechen.

Wenn über das Protokoll UDP ein Paket geschickt wird, erfolgt trotz vorhandenem Daemon meist keinerlei Bestätigung, allenfalls kann man die dahinter lauschende Applikation beobachten, ob sie auf das gesendete Paket reagiert. Wenn kein Daemon auf diesem Port lauscht, schickt der Zielcomputer meist eine ICMP Fehlermeldung «Port Unreachable» zurück.

Ports können offen (Daemon) oder geschlossen (kein Daemon) sein – aber was bedeutet «gefiltert»? Gefiltert heisst, dass beispielsweise auf eine Anfrage eine ICMP Fehlermeldung

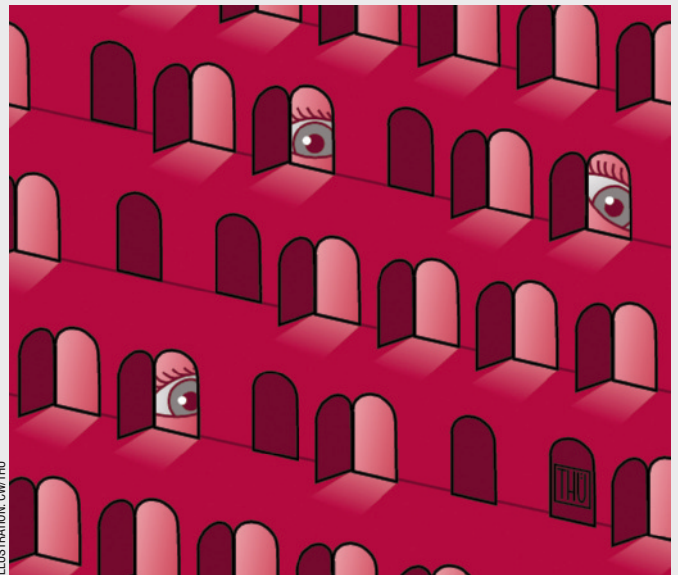


ILLUSTRATION: GW/THU

«Admin Prohibit» zurückkommt oder ICMP-Meldungen des Zielcomputers gar nicht beim scannenden System ankommen.

Portscanner fragen Ports an und analysieren die Antworten des Zielsystems, um Rückschlüsse auf offene, gefilterte oder geschlossene Ports zu ermöglichen. Dabei ermöglicht die Nutzung von TCP-Flags (SYN = Synchronize, ACK = Acknow-

«Einer der bekanntesten Portscanner ist Nmap, der die verschiedensten Scan-Arten unterstützt.»

ledge, PSH = Push, URG = Urgent, FIN = Finish und RST = Reset) die Analyse von widersprüchlichen Antworten. Bei UDP ist es aufgrund fehlender Bestätigungen und oftmals gefilterter ICMP-Nachrichten schwierig zu sagen, ob ein Port offen oder geschlossen ist. In diesem Fall empfiehlt es sich, mittels der entsprechenden Client-Applikation den Daemon manuell zu testen.

Einer der bekanntesten Portscanner ist Nmap von www.insecure.org/nmap/, der die verschiedensten Scan-Arten unterstützt: Connect-Scan, um den «three-way handshake» abzuschliessen; Syn-Stealth-Scan ohne das letzte Ack zu senden, um keine erfolgreiche und oft auf der Firewall protokollierte

Sitzung zu initiieren; Idle-Scan, um selbst kein einziges Paket an den Zielcomputer zu schicken; Xmas-Scan, wo alle TCP-Flags gesetzt werden; Null-Scan ohne TCP-Flags zu setzen; Ack-/Fin-/Rst-Scan, um nur einzelne TCP-Flags zu setzen, und viele andere mehr. Weil Portscanning die Vorstufe eines Netzwerk-basierten Angriffes sein kann, kann dies als

Bedrohung wahrgenommen werden. Wenn Portscanning jedoch präventiv von Sicherheitsexperten angewendet wird, können unnötige offene Ports entdeckt und geschlossen werden.

Es gilt die Regel: Je mehr offene Ports ein System bietet, desto grösser ist in der Regel die Gefährdung. Wenn die Anzahl offener Ports minimiert wird, verringert dies die Angriffsfläche des Systems. ■



Der Autor
Martin Rutishauser
ist Consultant und
OPST/OPSA bei
der Sicherheitsbe-
raterin Oneconsult,
Bern, www.oneconsult.com

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikeln finden Sie im Internet: www.computerworld.ch

IN EIGENER SACHE

Das Computerworld-Kompaktseminar

Am 1. März 2007 findet in Bassersdorf das Seminar «Hacking für Security-Beauftragte» statt. Es vermittelt Theorie- und Praxis-Wissens rund ums Thema Hacking sowie das OSSTMM (Open Source Security Testing Methodology Manual).

➔ **Anmeldungen unter:** www.computerworld.ch/seminare