

## Portscans im Internet

Autoren: Sebastian Schreiber, Stefan Arbeiter

Klassischerweise muss ein Angreifer, der es direkt auf ein bestimmtes System im Internet abgesehen hat, erst herausfinden, welche Funktion dieses erfüllt um sich eine erfolgreiche Taktik überlegen zu können. Er kann sich dabei zunutze machen, dass Systeme im Internet sich an standardisierte Verhaltensweisen zum Verbindungsaufbau halten müssen.

Im Rahmen von TCP ist dies sehr einfach, da hier jeder Dienst einen Port verwenden muss, auf dem er auf Verbindungsversuche wartet, wenn er denn von der Allgemeinheit erreichbar sein soll.

Eine TCP-Verbindung wird durch den 3-Wege-Handshake aufgebaut: Der Client schickt als Signal, das er mit einem Dienst kommunizieren will, ein einzelnes SYN-Paket an den jeweiligen Port auf dem Server. Dieser antwortet mit einem SYN/ACK-Paket, und signalisiert so, dass er für den Verbindungsaufbau bereit ist - der Client bestätigt dies mit einem ACK-Paket.

Wird der Handshake nicht vollendet, weil z.B. der Server überlastet ist (Kein SYN/ACK wird verschickt) oder der Client mittlerweile abgestürzt ist (Kein ACK-Paket wird verschickt) kommt kein Verbindungsaufbau zustande.

Daher muss ein Angreifer also nur SYN-Pakete an alle Ports verschicken, auf denen er Dienste erwartet oder die ihn besonders interessieren. Sofern die Verbindung mit dem Zielsystem stabil ist, wird er von jedem Port, auf den Dienst aktiv ist, ein SYN/ACK Paket erhalten. Wenn kein Dienst auf dem entsprechenden Port aktiv ist, verschickt das System ein RST-Paket, das zum Abbruch des Verbindungsversuches auffordert – Paketfilter können aber auch verhindern, dass überhaupt eine Antwort verschickt wird.

Selbstverständlich muss der Angreifer eine gewisse Zeitspanne einkalkulieren, die er auf Antworten warten muss - er wird daher nicht alle Ports absuchen, sondern nur diejenigen, die ihn speziell interessieren. Ein Angreifer, der z.B. in Angriffen auf MySQL spezialisiert ist, wird nur nach Port 3306 suchen und anderen Ports links liegen lassen.

Portscans gelten aber juristisch nicht als Angriff, da es sich um völlig standardkonforme Aktivitäten innerhalb des jeweils verwendeten Protokolls handelt.

Tatsächlich sind sie auch für einen Administrator unersetzlich, der überprüfen will, ob Firewall-Regeln korrekt gesetzt sind, oder ob auf einem System mehr Dienste laufen als zulässig. Würmer, die dem Angreifer eine Hintertür öffnen, können über Portscans ebenfalls gefunden.

Da Portscans bis auf den sog. Idle-Scan<sup>1</sup> zu einem System zurückverfolgt werden, sind Sie im Vergleich zu der Bedrohung durch vollautomatisierte Einbruchswerkzeuge („Würmer“) unerheblich geworden. Würmer führen keinerlei Prüfung durch, ob ein Ziel oder der von ihnen ausgenutzte Dienst tatsächlich erreichbar sind, sondern „feuern“ direkt Ihren Exploit-Code ab..

Daher ist das Risiko, das durch das blockieren von IP-Adressen, von denen Portscans ausgehen, weitaus höher ist als der Nutzen. Daher läuft man Gefahr, befreundete Systeme zu blockieren, wenn die Quelladressen eines Portscans gefälscht sind, was z.B. die Decoy-Option von nmap<sup>2</sup> ermöglicht, stattdessen sollte Energie darin investiert werden, die einzelnen Dienste sicher zu halten.

1. Siehe Network Computing, Ausgabe X, Seite Y

2. Der bekannteste und an Features reichste Portscanner ist nmap (<http://www.insecure.org>) von Fyodor, der sowohl auf Windows als Unix-Systemen läuft. Mit ihm kann ein Administrator schnell und flexibel auch größere Netze überprüfen.