Nmap: Firewalls umgehen mit Ping- und TCP-ACK-Scans

Nmap: Firewalls umgehen mit Ping- und TCP-ACK-Scans

Nmap zeigt schon mit einfachen Scans, welche Ports von außen erreichbar sind. Neben Ports, die sich eindeutig als offen oder geschlossen identifizieren lassen, gibt es solche, die als gefiltert gelten. Dies ist der Fall, wenn sich Systeme hinter einer Firewall befinden. Hier liefern spezialisierte Scans zusätzliche Informationen.

Um die Methoden für TCP-Port-Scans besser zu verstehen, sollten Sie elementare Konzepte des TCP-Protokolls wie den TCP-Verbindungsaufbau kennen. Im Wesentlichen gibt es dabei zwei reguläre Szenarien.

Offene Ports

Bei einem Szenario mit offenem Port lauscht eine Anwendung auf eingehende Verbindungen vom Client. Der Port befindet sich somit im Status TCP LISTEN.

Beim Empfang einer eingehenden Verbindungsanfrage in Form eines Synchronisationspakets (SYN) antwortet das Zielsystem (Server) mit einem SYN/ACK-Paket (Acknowledge), um die Synchronisation zu bestätigen.

Sobald der Client, von dem die Anfrage ausging, mit einem ACK-Paket antwortet, ist die Verbindung auf beiden Seiten hergestellt. Das ist der klassische TCP-3-Way-Handshake.

Verlauf eines TCP-Handshakes

Verlauf eines TCP-Handshakes

Die Sequenznummern spielen für die weiteren Erläuterungen erstmal keine Rolle. Details dazu finden Sie in meinem Artikel zu Wireshark.

Geschlossene Ports

Bei einem zweiten möglichen Szenario lauscht gerade keine Anwendung auf eingehende Verbindungen auf einem bestimmten Port. Daher gilt er als geschlossen, der Status ist somit TCP CLOSED.

Kommt es zu einer eingehenden Verbindungsanfrage, dann weist der Server diese mit einem RST- oder Reset-Paket zurück.

Gefilterte Ports

Im Zusammenhang mit einer Firewall ergibt sich ein drittes mögliches Szenario. Die an den Server gesendeten Pakete werden hierbei einfach verworfen - entweder von einer dedizierten Firewall oder dem Ziel-Server selbst bzw. von dessen Paketfilter. Als Folge davon antwortet der Server überhaupt nie.

Weil aber das Zielsystem nicht antwortet, wenn nmap ein Testpaket an den Port sendet, gilt der Port als "gefiltert". Ein Paketfilter ist aber in einigen Fällen so konfiguriert, dass die verworfenen Pakete durch ICMP-Fehlermeldungen (Internet Control Message Protocol) signalisiert werden.

Bei Ports mit dem Status FILTERED müssen Sie sich in der Rolle des "Angreifers" folgende Frage stellen, wenn auf ein Testpaket keine Antwort erfolgt: Ist der Port gefiltert oder wurde das Testpaket etwa wegen eines überlasteten Netzwerks verworfen?

Selbst wenn Letzteres auszuschließen ist, sollten Sie auf jeden Fall länger auf eine Antwort warten als bei OPEN oder CLOSED und können dadurch zum Ergebnis kommen, dass der Port FILTERED ist.

Spezialisierte Port-Scans

Mit Hilfe des gewöhnlichen Port-Scans ermittelt nmap im Wesentlichen offene Ports und weiß in der Regel auch, zu welchen Anwendungen diese gehören.

Spezialisierte Port-Scans dagegen helfen in Situationen weiter, wenn zum Beispiel eine Firewall umgangen werden soll. Hier provozieren Sie absichtlich Reaktionen, die tiefergehende Erkenntnisse über den Port-Status liefern, beispielsweise durch einen Ping-Scan.

Dieser provoziert eine Antwort des Zielsystems mit Hilfe eines TCP-ACK-Pakets. Er macht sich dabei zunutze, dass einfach gestickte zustandslose Firewalls wie Linux-Iptables zwar meist eingehende SYN-Pakete filtern, aber keine (streng genommen unzulässigen) ACK-Pakete.

Genau das bewirkt eine Rückmeldung des Ziels etwa in Form eines RST-Pakets. Der Status des betroffenen Ports ist dann eben nicht mehr FILTERED (also durch Firewall blockiert), sondern UNFILTERED.

Letztes heißt dann für den Angreifer, dass der Port doch erreichbar ist, aber nicht weiter bestimmt werden kann, ob er offen oder geschlossen ist. Aktivieren können Sie den TCP-ACK-San mit dem Parameter -sA.

Mit dem Schalter -PN können Sie zudem jedes System scannen, unabhängig davon, ob dieses Pings blockiert oder nicht, weil damit das Host-Discovery übersprungen wird und Scans auch gegen Ziele erfolgen, ohne dass ihre Erreichbarkeit verifiziert wurde.

Scan-Timings

Möchten Sie Ihre Firewall testen, bietet sich der TCP-ACK-Scan also durchaus an. Allerdings sollten Sie das System dann auf jeden Fall mit unterschiedlichen Timings scannen. Hierzu stellt Nmap den Schalter -Tx zur Verfügung. Für x können Sie eine Ziffer von 0 bis 5 verwenden.

Die Ziffern stehen für:

0 paranoid

1 sneaky

2 polite

3 normal

4 aggresive

5 insane

So könnten Sie zum Beispiel mit

nmap -T4 -F

einen aggressiven Scan starten. Sie müssen nicht unbedingt alle sechs Timings ausprobieren, aber zwei oder drei unterschiedliche sind ratsam, um eventuell verschiedene Reaktionen der Firewall zu provozieren.

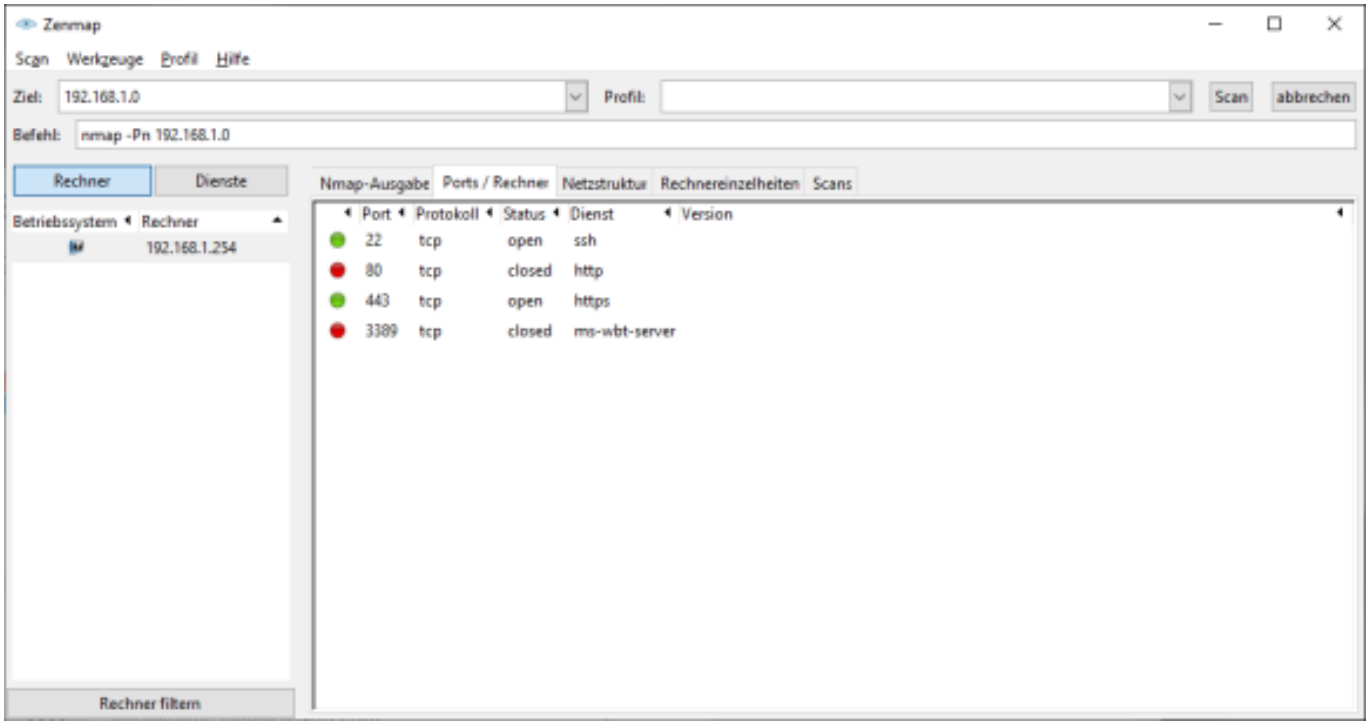
Scannen mit unterschiedlichen Timings

Scannen mit unterschiedlichen Timings

Zenmap zeigt Ihnen im Reiter Ports / Rechner schließlich die Detailinformationen zu den ermittelten Ports.

Detailinformationen zu den untersuchten Ports in Zenmap

Detailinformationen zu den untersuchten Ports in Zenmap



Zusammenfassung

Während sich offene und geschlossene Port über einen TCP-Handshake recht einfach erkennen lassen, fällt es schwieriger, eine ausbleibende Antwort verlässlich einzuordnen.

In dieser Situation helfen spezialisierte Port-Scans weiter, die absichtlich Reaktionen provozieren, die mit denen sich tiefergehende Erkenntnisse über den Port-Status gewinnen lassen.

Eindeutige ID: #1019
Verfasser: n/a
Letzte Änderung: 2022-10-25 10:24