„Der Idle Scan“ oder wie man beim Portscannen nicht entdeckt wird

(Micha Borrmann <Borrmann@SySS.de>)

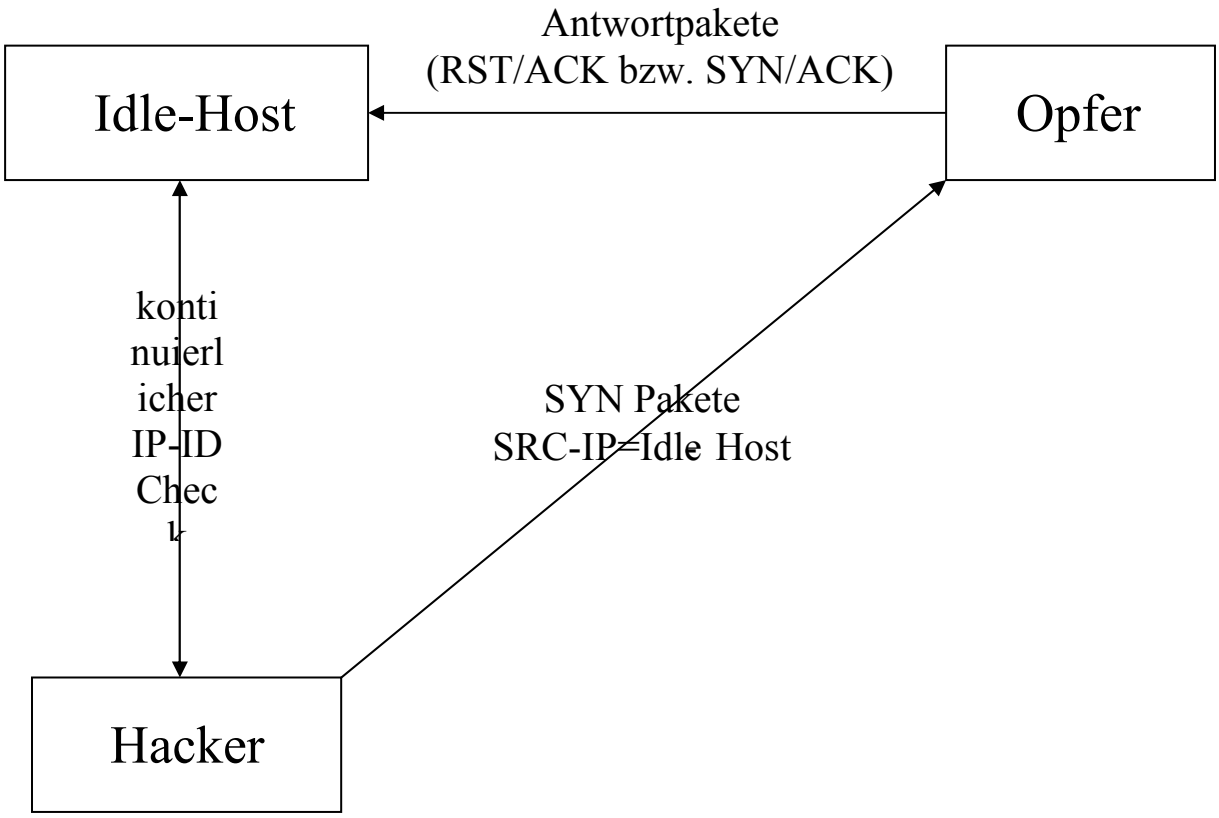
Das Port-Scanning von Systemen im Internet erfolgt immer ähnlich: man schickt unterschiedliche Pakete zur IP-Adresse eines Systems und prüft die Beschaffenheit etwaiger Antwortpakete. Im Lauf der letzten fünf Jahre sind neue - äußerst trickreiche - Scanning-Techniken entwickelt worden; z.B. lässt sich ein System scannen, ohne dass man von diesem System auch nur ein einziges Antwortpaket erhält.

Beim „traditionellen“ Portscanning wird beim Verbindungsaufbau die eigene IP dem zu attackierenden Host als Source-IP bekannt gemacht. Firewalls bzw. Intrusion Detection Systeme sowie einfache Portscan-Detektoren können den Verursacher leicht identifizieren.

Jedes IP Paket hat eine Identification (IP-ID) im Header, die für das korrekte Handling fragmentierter Pakete vorgesehen ist. Da zahlreiche IP Stacks diese ID bei jedem versendeten Paket lediglich um eins erhöhen, kann man diese Tatsache nutzen, um unerkannt ein Opfer zu scannen. Dies beruht auf folgenden Eigenschaften:

- Ein SYN wird von einem geschlossenen Port mit RST/ACK, von einem offenen Port mit SYN/ACK beantwortet
- Ein unerwünscht eingehendes SYN/ACK Paket wird mit RST beantwortet
- Ein unerwünscht eingehendes RST bzw. RST/ACK wird ignoriert
- Jedes IP-Paket enthält eine ID, die bei zahlreichen Hosts bei jedem IP-Paket fortlaufend erhöht wird.

Der Angreifer benötigt einen Host, der keine Netzwerkaktivität aufweist, d.h. *idle* ist und der vorhersagbare IP-IDs hat. Der Angreifer prüft mit einem beliebigen Datenpaket die IP-ID des Idle-Hosts und merkt sich diese. Danach sendet der Angreifer ein SYN Paket mit der Absender IP-Adresse des Idle-Hosts an das Opfer und prüft die IP-ID des Idle-Hosts erneut. Ist die IP-ID des Idle-Hosts nur um eins erhöht, so hat das angegriffene System entweder ein RST oder kein Paket an den Idle-Host geschickt. Ist die IP-ID des Idle-Hosts dagegen um zwei erhöht, so hat das angegriffene System ein SYN/ACK zum Idle-Host geschickt, der wiederum mit einem RST dem Opfer antwortete. Auf diese Weise kann ein Angreifer die offenen Ports des Opfers detektieren, ohne daß die IP-Adresse des Angreifers auch nur ein einziges mal zum Opfer geschickt wird: der Angreifer erhält niemals ein Antwortpaket vom getesteten System. Der Angreifer kann danach die Dienste des Systems identifizieren. Diese Technologie zeigt, dass ein Portscan-Detektor den tatsächlichen Verursacher nicht identifizieren kann. Mit dem bekannten Portscanner nmap (siehe www.insecure.org) lassen sich auch Idle-Scans durchführen.



Es ergeben sich folgende Konsequenzen:

- IP-basierte Authentifikation alleine ist nicht ausreichend - aber dennoch sinnvoll. Es empfiehlt sich, darüber hinaus z.B. zertifikatsbasierte Authentifikation einzusetzen.

- Es ist davon auszugehen, dass ein Angreifer unerkannt Angriffe durchführt.

- Den IDS- oder Firewall-Logfiles ist nicht unbedingt zu trauen. Bei einer Strafverfolgung bzw. bei disziplinarischen Maßnahmen gegen Mitarbeiter ist zu beachten, dass die Fährten auch bewusst falsch gelegt worden sein können.