Kontrollfragen

Angriffe und Firewalls

Die Angriffe

Denial of Service

Ein *"Denial of Service"*-Angriff kann wie folgt umschrieben werden:

- □ Der angreifende Host sendet ein *"Ping of Death"*-Paket an das Opfer. Das verfälschte ICMP-Netzwerkpaket, welches die maximale Paketgrösse (MTU; Maximum Transmission Unit) von 1500 Bytes klar überschreitet, wird beim Opfer-Host durch einen Fehler in der Implementierung des *Internet Protocols* einen *Buffer Overflow* verursachen.
  → Folge: Bluescreen bzw. Systemabsturz.

- □ Der angreifende Host muss zuerst einige Vorkehrungen treffen. Er infiziert mehrere PCs mit einem Trojaner oder mietet sich für einige Stunden ein sogenanntes Botnetz (Verbund von infizierten Hosts, welche sich via Konsole fernsteueren lassen). Mit diesen Zombie-PCs wird nun ein *"Denial of Service"*-Attacke auf einen bestimmten Host gestartet, i.d.R. handelt es sich hierbei um Webserver, welche druch die Flut von Anfragen kollabieren.

- □ Der angreifende Host startet, unter Verwendung eines speziellen Skripts oder Programms, einen Angriff auf einen ausgewählten Zielhost. Die Attacke selbst besteht darin, dass das Opfer mit unnatürlich vielen Netzwerkpaketen kontaktiert wird, sodass eine normale Abarbeitung der Anfragen nicht mehr gewährleistet werden kann und der attackierte Host seinen Dienst quittieren muss.

Brute Force

Welche Aussage würden Sie im Bezug auf eine *Brute Force*-Attacke unterschreiben?

- □ Mittels einer speziellen Software (oder auch eines Skripts mit entsprechenden Arrays und Programmschleifen) werden die unterschiedlichsten Benutzernamen und Passwörter kreiert, welche durch den Angreifer in den entsprechenden Eingabefeldern (z.B. Web-Shop, eBanking etc.) der anzugreifenden Plattform eingegeben werden können.

- □ Die *Brute Force*-Attacke kann auch als pures Ausprobieren von Benutzername und/oder Passwort umschrieben werden. Opferseitig kann man sich mittels sogenannter *"Counter"* schützen, welche das Benutzerkonto nach drei falschen Eingaben sperrt (was natürlich die Benutzerfreundlichkeit einschränken kann).

- □ Durch das automatische Ausprobieren von Benutzernamen und Passwörtern, welche durch ein speziell dafür kreiertes Programm durchgeführt werden, kann ein Opfer-Host mittles dieses Angriffs kollabieren. Durch die Flut von Anfragen wird eine Überlast auf dem attackierten Host erzeugt, welcher über kurz oder lang seinen Dienst, auf Grund zu hoher Menge von Anfragen, quittieren muss.

Distributed Denial of Service

Der grosse Bruder des *Denial of Service*. Welche Aussagen stimmen?

- □ Für einen erfolgreichen DDoS-Angriff benötige ich nur zwei, drei performante Hosts um genug Anfragen generieren zu können.
- □ Damit meine DDoS-Attack erfolgreich durchgeführt werden kann, benötige ich eine Netzwerkkarte, welche den *Promiscuous-Mode* (empfangen von nicht direkt adressierten Netzwerkpaketen; meist über Hubs oder Portmirroring auf Switches) beherrscht.
- □ Für einen erfolgreichen DDos-Angriff auf eine moderne Infrastruktur benötige ich mehrere 100'000 Zombie-Hosts.

IP-Spoofing

Eine weitere Disziplin ist IP-Spoofing. Doch welche Aussage stimmt im Bezug auf IP-Spoofing?

- □ Unter Spoofing versteht man grundsätzlich die Verfälschung von Paketinhalten bzw. Paketheader. Somit kann zum Beispiel eine zu versendende *setup.exe* als *HTTP-Request* getarnt werden, was ein Einschleusen von Schadcode auf einem Webserver ermöglicht.
- □ Mittels IP-Spoofing (verfälschen der Source-Adresse) können Sie einen *Denial of Service*-Attacke an einem Zielhost innerhalb Ihres Netzwerkes druchführen. Da Sie die Quelle-Adresse z.B. von Ihren PING-Anfragen (ICMP) abändern, erhalten nicht Sie als Anfragender den ICMP-Request, sondern die IP-Adresse bzw. MAC-Adresse Ihres Opfers. Mit der nötigen Menge an antwortenden Hosts, können Sie ihr Opfer in die Knie zwingen.
- □ Unter Spoofing, zu deutsch *Manipulation* bzw. *Verschleierung*, wird die Manipulation von IP-Paketinhalten verstanden. Die Manipulation wird meist auf Basis von Zieladressen durchgeführt. Durch diese Verfälschung kann in einem Netzwerk viel Verwirrung gestiftet werden, da alle Paket mit der richtigen Quelladresse unterwegs sind, aber kein Paket sein gewünschtes Ziel erreichen kann.

Rund um den Angriff

Welche Statements würden Sie als Fachfrau/-mann ebenso wiedergeben?

- □ Unter einem **False Positiv** verstehen Sie, innerhalb der Warntechnologie von Angriffen, eine falsche Meldung. Sprich, Ihnen wird ein Angriff gemeldet, welcher gar keiner war.
- □ Frühwarnsysteme und Abwehrmechanismen gehören in das Grundset einer jeden Firewall. Sie gehören zum absoluten Minimum der Basisfunktionen.
- □ Sie haben als Netzwerk- und Firewalladmin die Auswahl zwischen einem **Intrusion Detection System** und einem **Intrusion Prevention System**. Sie entscheiden sich logischerweise für die IDS-Lösung, da Sie Angriffe nicht nur erkennen, sondern auch automatisch abwehren möchten.
- □ Die Signaturerkennung eines Warnsystems, kann mit den Paternfiles, welche zyklisch aktualisiert werden, eines Virenschutzes verglichen werden. Die Signaturerkennung erkennt nur bereits bekannte Angriffsmuster.
- □ Bei der Anomalieerkennung werden Abweichungen des normalen Betriebszustandes erkannt. Sie gilt als wartungs- und administrationsarm.
- □ Unter einem **False Negativ** verstehen Sie, innerhalb der Warntechnologie von Angriffen, eine falsche Meldung. Sprich, Ihnen wird ein Angriff gemeldet, welcher gar keiner war.
- □ Um mich gut vor Angriffen schützen zu können, sollte mein Netzwerk gut konzipiert und geplant sein. Nur so kenne ich die exponierten Stellen innerhalb meines Netzwerkes und kann diese entsprechend schützen.
- □ Die meisten Angriffe haben als primäres Ziel die Firewall im Visier, denn wenn die Firewall erst mal überwunden ist, gehört das Netzwerk mir.
- □ Der durchschnittliche Mitarbeiter ist für einen Angreifer, welcher durch wirtschaftskriminelle Treiber motiviert ist, das wichtigere Ziel, als eine gut geschützte Firewall- und Serverinfrastruktur.
- □ Sie haben als Netzwerk- und Firewalladmin die Auswahl zwischen einem **Intrusion Detection System** und einem **Intrusion Prevention System**. Sie entscheiden sich logischerweise für die IPS-Lösung, da Sie Angriffe nicht nur erkennen, sondern auch automatisch abwehren möchten.