SecLab

Praktikum IT-Sicherheit

- Versuchshandbuch -

Aufgaben

Angriffstechniken

In diesem Versuch werden verschiedene Angriffstechniken anhand von Beispielen vorgestellt. Die Ausarbeitung der Übungen soll einen kurzen Einblick in das mögliche Vorgehen eines Angreifers im Internet aber auch in lokalen, geswitchten Netzwerken bieten.

B.Sc. AI, WI
M.Sc. AI
M.Sc. EB

IT-Sicherheit

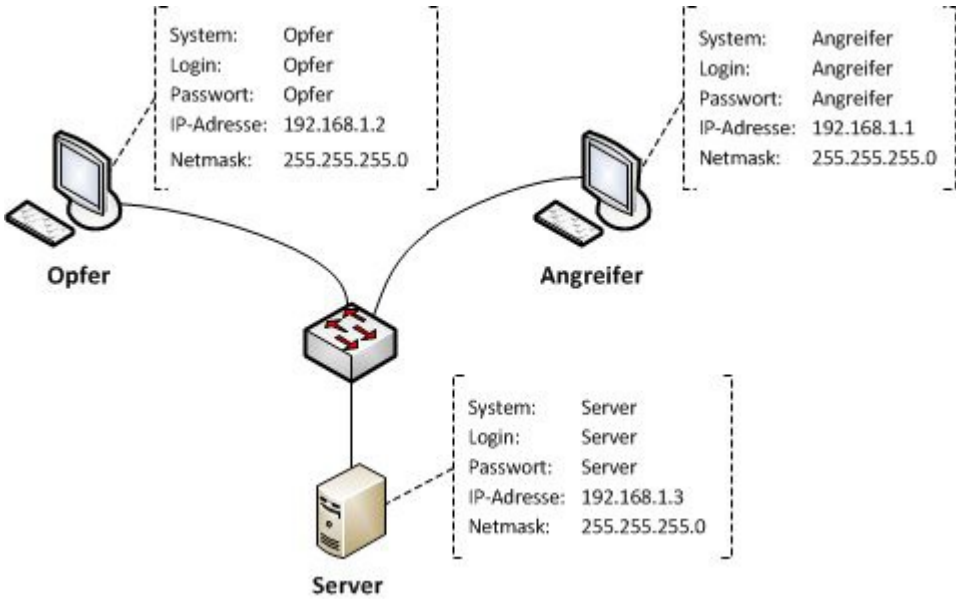
Einleitung

In diesem Versuch lernen Sie verschiedene Arten von Angriffen auf Rechner im Internet oder in lokalen, geswitchten Netzwerken sowie deren Vorbereitung kennen. Dazu stehen drei per virtuellem Switch vernetzte, virtuelle Maschinen – ein Server, ein Client (Opfer) und der Rechner des Angreifers – zur Verfügung. Die benötigten Zugangsdaten und die verwendete Netzwerk-konfiguration finden Sie im folgenden Abschnitt.

Zugangsdaten

- Systeme: Windows XP
- Benutzer: <Name der virtuellen Maschine>
- Passwort: <Name der virtuellen Maschine>

Netzwerkplan



Aufgabe 1: Port-Scanning

a) Führen Sie als *Angreifer* einen Portscan der Ports 0 bis 1024 auf das Opfersystem durch. Nutzen Sie dazu den *Open Port Scanner* der *NetTools Suite*. Nennen Sie alle geöffneten Ports des Opfers sowie die dazugehörigen Dienste.

.....

.....

.....

.....

b) Beschreiben Sie knapp, wie Portscanning funktioniert und nennen Sie verschiedene Arten von Portscanning.

.....

.....

.....

.....

.....

.....

Aufgabe 2: DoS-Attacke

a) Öffnen Sie auf dem Server mit Hilfe der NetTools Suite den *„Local http Server"* (*Start → Network Tools → Create Local HTTP Server*) und starten Sie ihn durch Anklicken der Schaltfläche *„Start"*. Welcher Port sollte nun offen sein?

.....

b) Versuchen Sie nun mit einem Webbrowser vom Rechner des Opfers auf die Webseite des Servers zuzugreifen. Lassen Sie sich nicht durch den Inhalt der Webseite verwirren. Schließen Sie anschließend den Webbrowser wieder. War der Aufruf der Webseite erfolgreich?

.....

c) Was versteht man unter einer Flood-Attacke und zu welcher Art von Angriff wird eine solche Attacke gezählt?

.....

.....

.....

.....

.....

d) Führen Sie nun vom Rechner des Angreifers einen Flood-Angriff auf den *Local http Server* durch. Verwenden Sie dazu den *http flooder* der NetTools Suite.
(Verwenden Sie folgende Einstellungen: Connections 100 (ggf. mehr), Active 0)

e) Wiederholen Sie nun Aufgabe b. Schließen Sie Internet Explorer zuvor, um den Cache zu leeren. Was ist zu beobachten? Begründen Sie ihre Aussage.

.....

.....

.....

.....

.....

f) Bringen Sie alle Rechner in den Ursprungszustand zurück, bevor Sie mit der nächsten Aufgabe fortfahren.

Aufgabe 3: ARP-Poisoning

a) Lassen Sie sich die ARP-Einträge auf dem Rechner des Opfers anzeigen. Verwenden Sie den Befehl „arp –a" in der Windows-Konsole. Welche ARP-Einträge sind vorhanden?

.....

.....

.....

b) Starten Sie nun das Programm *Ettercap* auf dem PC des Angreifers und führen Sie einen ARP-Poisoning Angriff durch. Gehen Sie wie folgt vor:

- Wählen Sie im Menü (*Sniff* → *Unified Sniffing*) den Netzwerkadapter *VMware Adapter* aus
- Scannen Sie das Netzwerk nach anderen Rechnern (*Hosts* → *Scan for hosts*)
- Wählen Sie im Menü den ARP-Poisoning Angriff aus (*Mitm* → *Arp poisoning*) und starten Sie diesen (Markieren Sie keine weiteren Optionen).

c) Lassen Sie sich auf dem Rechner des Opfers erneut die ARP-Einträge anzeigen und versuchen Sie den Server anzupingen. Was stellen Sie fest? Begründen Sie Ihre Beobachtung.

.....

.....

.....

.....

.....

.....

d) Beenden Sie nun den ARP-Angriff (*Mitm → Stop mitm attack(s)*), schließen Sie Ettercap und sehen Sie sich die ARP-Einträge auf dem PC des Opfers erneut an. Was stellen Sie fest?

.....

.....

.....

.....

e) Erzeugen Sie jetzt einen statischen ARP-Eintrag zum Server auf dem PC des Opfers. Verwenden Sie dazu das Kommando „arp -s". Wiederholen Sie anschließend den Angriff (Aufgaben b und c) und erklären Sie Ihre Beobachtungen.

.....

.....

.....

.....

.....

.....

f) Bringen Sie alle Rechner in den Ursprungszustand zurück, bevor Sie mit der nächsten Aufgabe fortfahren.

Aufgabe 4: FTP-Sniffing

a) Starten Sie auf dem *Server* den Dienst FTP-Server. Verwenden Sie dazu das Programm *ftpserv.exe*, das Sie auf dem Desktop finden.

b) Führen Sie einen Portscann auf den Server durch. Welche Ports sind geöffnet?

.....

.....

.....

c) Führen Sie nun die FTP-Sniffing Attacke durch. Gehen Sie wie folgt vor:

- Starten Sie das Programm *Ettercap* auf dem PC des Angreifers
- Wählen Sie im Menü (*Sniff → Unified Sniffing*) den Netzwerkadapter *VMware Adapter* aus
- Scannen Sie das Netzwerk nach anderen Rechnern (*Hosts → Scan for hosts*)
- Lassen Sie sich die Ergebnisliste des Scans anzeigen (*Hosts → Hosts list*)
- Markieren Sie den *Server* und fügen Sie ihn als Target hinzu (*Add to Target 1*) Das *Opfer* wird ebenfalls als Target hinzugefügt (*Add to Target 2*)
- Lassen Sie sich nun über das Menü die Ziele anzeigen (*Targets → Current Targets*). Sie sollten zwei IP-Adressen sehen
- Lassen Sie sich die Konsole zur Überwachung der Verbindung zwischen den Zielen anzeigen (*View → Connections*)

- Führen Sie jetzt einen ARP-Poisening Angriff durch (*Mitm* → *ARP poisening*)
- Starten Sie nun den Angriff (*Start* → *Star sniffing*)
- Bauen Sie eine FTP-Verbindung vom Opfer zum Server auf. Verwenden Sie dafür den Internet-Explorer mit der Adresse ftp://192.168.1.3. Das Passwort für die FTP-Verbindung lautet „opfer".

d) Was können Sie in der Konsole von Ettercap beobachten? Begründen Sie Ihre Beobachtung und machen Sie Vorschläge zur Vermeidung des Problems.

.....

.....

.....

.....

.....

.....

.....

.....

.....