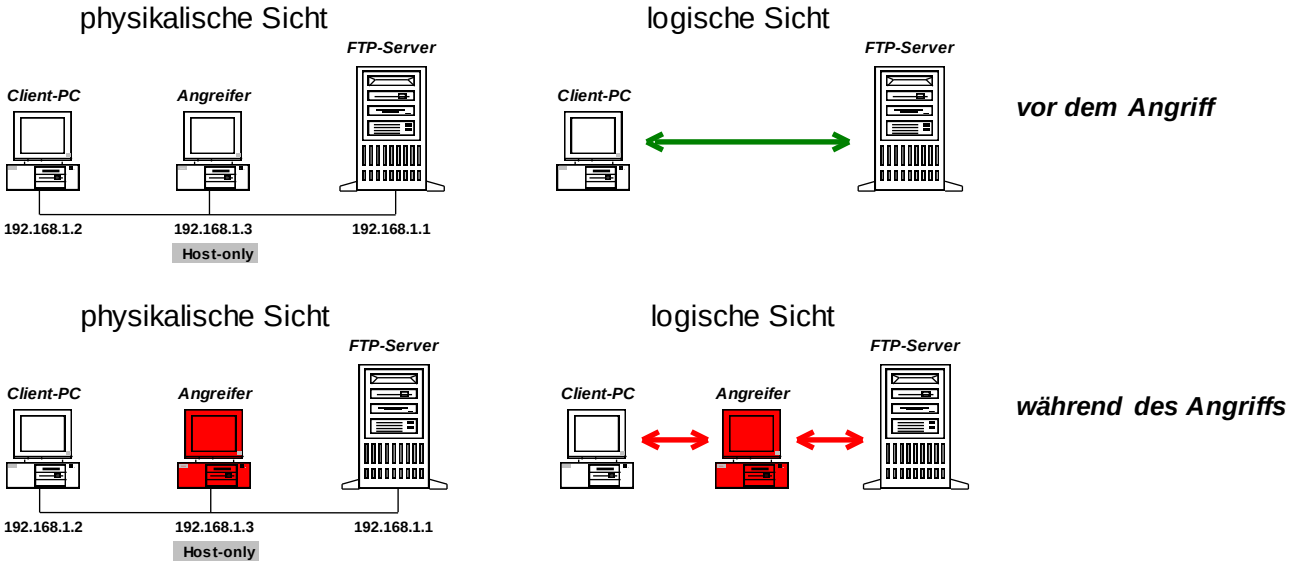
Einfache lokale Angriffe

ARP-Poisoning und Man-in-the-Middle mit Ettercap



Bei einem Man-in-the-middle-Angriff (MITM) steht der Angreifer zwischen den Kommunikationspartnern und hat dabei mit seinem System die vollständige Kontrolle über den Datenverkehr. Er kann die übertragenen Informationen nach Belieben einsehen und sogar manipulieren.

Beispiele für populäre MITM-Angriffe:

- im Ethernet modifiziert der Angreifer durch ARP-Spoofing/-Poisoning die ARP-Tabellen der Opfersysteme
- durch DNS-Poisoning gibt der Angreifer zu einem angefragten Rechnernamen eine falsche Ziel-IP-Adresse vor

VMs vorbereiten

Wir arbeiten unter VMware mit drei Virtuellen Maschinen (VM).

Wichtig: Stellen Sie sicher, dass auf dem Host-PC unter *Start - Einstellungen - Netzwerkverbindungen* die Netzwerkkarte "*VMware Host-Only-Adapter VMnet1*" aktiviert ist (Das ist des VMware Host-Only-Adapter).

1.) Eine VM ist bereits als selbstextrahierendes ZIP-Archiv unter http://intranet/files/VMs/XP-Netz.vm65.exe vorbereitet. Bitte laden Sie das Archiv vom Intranet herunter und führen Sie es aus.

Beim Extrahieren wird die VM nach "C:\VMs\XP-Netz\" kopiert. Danach wird sie mit VMware geöffnet.

Klicken Sie jetzt auf den virtuellen Netzwerkadapter der VM und weisen Sie ***Host-only*** zu.

2.) Wir benötigen drei VMs: "FTP-Server", "Client-PC" und "Angreifer".
Diese VMs erhalten wir, indem wir die vorhandene VM "XP-Netz" **clonen**:

Über das Kontextmenü der XP-Netz-VM in der Favoritenliste oder über *VM - Manage - clone - weiter - The current state... - weiter - **create a linked clone*** - unter *Virtual machine name* "FTP-Server" eingeben.

Die VMs "Client-PC" und "Angreifer" erhalten Sie genauso.

3.) Starten Sie die drei geclonten VMs und setzen Sie die Rechnernamen "FTP-Server", "Client-PC" und "Angreifer" entsprechend den Namen der VMs. Setzen Sie auch die IP-Adressen wie im Bild oben dargestellt.

4.) Laden Sie das Archiv http://intranet/files/ettercap.rar und entpacken Sie es auf dem Desktop des Host-PCs

Ziehen Sie das Verzeichnis "ftpsrv110" mit der Maus in den Desktop der laufenden VM "FTP-Server" hinein (oder mit copy-and-paste).

Erstellen Sie dort das Verzeichnis C:\TEMP und erstellen Sie dort eine Datei mit dem Namen test.txt.

Starten Sie jetzt auf dem Desktop des FTP-Servers das Programm ftpserv.exe das sich in "ftpsrv110" befindet.

Testen der VMs

5.) Testen Sie den FTP-Server vom Client-PC aus, indem Sie dort in einer Kommandozeile die **fett** gedruckten Kommandos eingeben:

```
ftp 192.168.1.1
Verbindung mit 192.168.1.1 wurde hergestellt.
220 TYPSoft FTP Server 1.10 ready...
Benutzer (192.168.1.1:(none)): root
331 Password required for root.
Kennwort:geheim
230 User root logged in.
ftp> dir
200 Port command successful.
150 Opening data connection for directory list.
-rw-rw-rw-   1 ftp      ftp            0 Dec 03 21:52 test.txt
226 Transfer complete.
FTP: 64d Bytes empfangen in 0,00Sekunden 64000,00KB/s
ftp> bye
221 Goodbye!
```

6.) Pingen Sie von jeder VM jede andere an, lesen Sie mit **arp -a** die ARP-Caches aus und ergänzen Sie nachfolgend die ARP-Tabellen für die drei VMs. Geben Sie jeweils auch die Mac-Adressen der VMs an.

Client-PC

MAC-Adresse
00-0c-29-ad-5a-7c

ARP-Tabelle

IP-Adresse	*MAC-Adresse*
192.168.1.1	00-0c-29-80-5e-a7
192.168.1.3	00-0c-29-2d-11-12

Angreifer

MAC-Adresse
00-0c-29-2d-11-12

ARP-Tabelle

IP-Adresse	*MAC-Adresse*
192.168.1.1	00-0c-29-80-5e-a7
192.168.1.2	00-0c-29-ad-5a-7c

FTP-Server

MAC-Adresse
00-0c-29-80-5e-a7

ARP-Tabelle

IP-Adresse	*MAC-Adresse*
192.168.1.2	00-0c-29-ad-5a-7c
192.168.1.3	00-0c-29-2d-11-12

Angriff starten

7.) Installieren Sie Ettercap auf der "Angreifer"-VM. Ziehen Sie dazu die Datei "ettercap-NG-0.7.3-win32.exe" in den Desktop der "Angreifer"-VM hinein und führen Sie die Installation dort aus.

8.) Starten Sie Ettercap auf der "Angreifer"-VM unter *Start - Programme - Ettercap NG - ettercap*

Starten Sie das Unified-Sniffing: *Sniff - Unified sniffing* und dort das *VMware Interface* auswählen
Erstellen Sie die Host-Liste: *Hosts - Scan for hosts*

Zeigen Sie mit *Hosts - Hosts list* die Hosts-Liste an.
Wählen Sie die Zeile, die 192.168.1.1 enthält und klicken Sie auf *Add to target 1*
Wählen Sie die Zeile, die 192.168.1.2 enthält und klicken Sie auf *Add to target 2*

Starten Sie jetzt den Angriff über *Mitm - Arp poisoning*
Starten Sie das Sniffing über *Start - Start sniffing*

Pingen Sie vom Client-PC aus den FTP-Server an.
Stellen Sie nachfolgend noch einmal die ARP-Tabelle des Client-PCs dar:

Client-PC

ARP-Tabelle
während des Angriffs

ARP-Tabelle

IP-Adresse	*MAC-Adresse*
192.168.1.1	00-0c-29-2d-11-12
192.168.1.3	00-0c-29-2d-11-12

FRAGE: Was fällt Ihnen jetzt hinsichtlich der ARP-Einträge beim Client-PC auf?

Angriff analysieren

9.) Starten Sie auf dem Host-PC den Sniffer Wireshark und beginnen Sie das Sniffern unter *Capture - Interfaces* auf dem vorher aktivierten *VMware Host-Only-Adapter VMnet1* mit *Start*

Senden Sie jetzt von der Client-PC-VM einen einzelnen Ping an den FTP-Server: **`ping -n 1 192.168.1.1`**

Jetzt sind insgesamt 4 ICMP-Pakete (2x echo-request, 2x echo-reply) vorhanden.

FRAGE: Wie erklären Sie sich dieses Verhalten?

Datenverkehr mitlesen

10.) Der Angreifer kann auch die übertragenen Daten mitlesen.

Aktivieren Sie das Mitlesen in Ettercap unter *Start - Start sniffing*

Starten Sie eine FTP-Session vom Client-PC aus: **`ftp 192.168.1.1`**
Verwenden Sie folgende Einstellungen: Username: *root* Passwort: *geheim*

FRAGE: Was können Sie im unteren Teil des Ettercap-Fensters beobachten?

Datenverkehr manipulieren

11.) Mit Ettercap ist auch eine Veränderung der übertragenen Daten über Filter möglich.

Als einfaches Beispiel soll das Banner des FTP-Servers verändert werden:
Aus "*TYPSoft FTP Server 1.10*" soll "*YOU HAVE BEEN SPOOFED!!!*" werden

Kopieren Sie die Datei "test_filter.txt" aus dem Ettercap-Archiv in die Angreifer-VM nach C:\test_filter.txt
(oder: Schreiben Sie auf der Angreifer-VM dazu Folgendes in die Datei C:\test_filter.txt)

```
if (tcp.src == 21 && search(DATA.data, "TYPSoft")) {
   replace("TYPSoft FTP Server 1.10", "YOU HAVE BEEN SPOOFED!!!");
}
```

Öffnen Sie auf der Angreifer-VM eine Kommandozeile und kompilieren Sie den Filter:

`C:\Programme\EttercapNG\etterfilter.exe C:\test_filter.txt -o C:\test_filter.bin`

Laden Sie den kompilierten Filter "C:\test_filter.bin" in Ettercap unter *Filters - Load a filter..*

Aktivieren Sie Wireshark (wie unter 10.) und schneiden Sie den sich ergebenden Netzwerkverkehr mit, indem Sie noch einmal vom Client-PC aus eine Verbindung zum FTP-Server aufbauen.

to spoof so., to spoof sth. - jemanden hereinlegen, etwas fälschen

Links

www.backtrack-linux.org/forums/backtrack-howtos/1057-ettercap-arp-poisoning.html
openmaniak.com/ettercap_arp.php
openmaniak.com/ettercap_filter.php