# Labor III

*Ziel dieser Übung ist, anhand einiger Beispiele herauszufinden, welche Informationen mit vergleichsweise einfachen Methoden in einem Netz abgehört werden können. Danach wird eine Reihe „klassischer" aktiver Attacken durchgeführt. Protokollieren Sie für jede Aufgabe alle Schritte (auf sinnvoller Abstraktionsebene) mit, beantworten Sie im Protokoll auch die Fragestellungen am Ende jeder Aufgabe.Dieses Protokoll geben Sie bitte auf Moodle bis zum in der Moodle Abgabemaske angegebenen Termin ab.*

## 1 Aufbau der Testumgebung

Mittels VMWare Workstation[1] definieren wir zunächst ein virtuelles Netzwerk für unsere Testumgebung. Die Images der virtuellen Maschinen auf der lokalen Festplatte im Labor zur Verfügung (und unter `http://jrz.fh-salzburg.ac.at/IFS16`).

### 1.1 Topologie

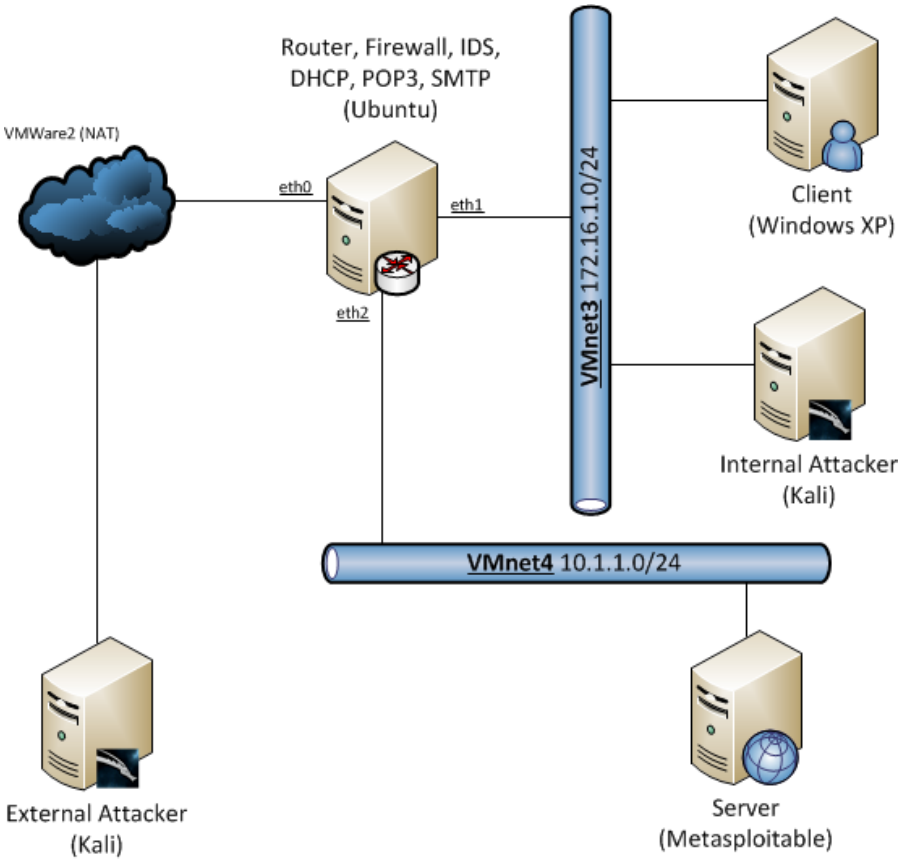


Abbildung 1: Topologie Testaufbau

[1] VMWare Workstation ist auf allen Rechnern im Labor installiert. Versionen von VMare Workstation für Studierende können als akademische Lizenz über "'On the Hub"' bezogen werden.

## 1.2 Einrichtung des virtuellen Netzwerks

Bevor Sie in VMWare Workstation VMs starten, öffnen Sie den *Virtual Network Editor* über Menüpunkt „Edit → Virtual Network Editor“). Ändern Sie zuerst VMNet 8 auf „host-only“ (nur ein Netzwerk kann für NAT verwendet werden, wir möchten dies für VMNet2 machen). Legen Sie dann folgende Einstellungen für die Netze VMNet2, VMNet3 und VMNet4 fest.

**VMNet8**

- Type: host-only

**VMNet2**

- Type: NATs
- Network: 192.168.136.0/24
- NAT Settings: Gateway IP 192.168.136.**2**
- Enable DHCP (Start IP: 192.168.136.128, End IP: 192.168.136.254)
- „Connect a host virtual adapter to this network“ deaktivieren

**VMNet3**

- Type: Host-only
- DHCP deaktivieren
- Network: 172.16.1.0/24
- „Connect a host virtual adapter to this network“ deaktivieren

**VMNet4**

- Type: Host-only
- DHCP deaktivieren
- Network: 10.1.1.0/24
- „Connect a host virtual adapter to this network“ deaktivieren

## 1.3 Konfiguration der virtuellen NICs

Konfigurieren Sie die virtuellen Netzwerkadapter (NICs) der VMs (für jede VM unter Einstellungen) wie folgt:

- Ubuntu Router
  - Erster NIC: VMNet2
  - Zweiter NIC: VMNet3
  - Dritter NIC: VMNet4

- Metasploitable - VMNet4
- Windows XP - VMNet3
- Kali - VMNet3

## 1.4 Starten der VMs

### 1.4.1 Starten der Ubuntu VM

- - Starten Sie die VM „Ubuntu“
  Beim Öffnen in VMWare öffnet sich eine Anfrage ob das Image kopiert oder verschoben wurde, bitte diese unbedingt mit **“I moved it“** beantworten.
- Username: `administrator`, Passwort: `administrator`
- Öffnen Sie die Datei /etc/network/interfaces (Editor nach Wahl, z.b. gedit, nano – dabei sudo nicht vergessen, also z.B. sudo gedit /etc/network/interfaces)
  - `eth0` und `eth2` wurden bereits konfiguriert
  - `eth1` ist zu konfigurieren mit IP Adresse 172.16.1.1/24.
- Danach mittels `sudo /etc/init.d/networking restart` aktivieren
- Prüfen Sie die Einstellungen mittels ifconfig
- Konfiguration des DHCP Servers am Ubuntu Router:
  - Editieren Sie `/etc/dhcp3/dhcpd.conf` (wieder sudo voranstellen)
  - Ergänzen Sie die Einstellungen, damit auch für 172.16.1.0/24 IP-Adressen per DHCP vergeben werden.
  - Starten Sie den DHCP Server neu: `service dhcp3-server restart`
- Network Address Translation (NAT) für den Ubuntu Router wurde bereits konfiguriert.
  - Die entsprechenden Einstellungen finden Sie unter `/etc/init.d/iptables_update`.
  - Falls Sie Änderungen vornehmen, aktivieren Sie die neuen Einstellungen mittels `/etc/init.d/iptab`
- Ein Mailserver läuft auf dem Ubuntu Router. Dieser Server ist bereits konfiguriert.

### 1.4.2 Starten der Windows VM

- Starten Sie die Windows VM
- Aktivieren Sie DHCP Client
- Stellen Sie sicher, dass die Windows VM vom Ubuntu Router die notwendigen Netwzerkeinstellungen erhält

### 1.4.3 Starten der Kali VM

- Starten Sie die Kali VM
- Einloggen mittels Username: `root`, Passwort: `toor`
- Öffnen Sie einen Terminal und prüfen Sie die Netzwerkeinstellungen mittels `ifconfig`

# 2 Network Reconnaissance

## 2.1 Network Ping Sweep

- Starten Sie wireshark in der Ubuntu VM (dient nur dem Monitoring).
- Nun wird versucht über die Kali VM Informationen über das LAN herauszufinden.
- Starten Sie in der Kali VM eine Shell und führen Sie einen `nmap` Ping Sweep durch:
  `nmap -sP 172.16.1.*`
- Welche Informationen können Sie so herausfinden?
- Wechseln Sie zur Ubuntu VM.
  - Können Sie nachvollziehen, wie der Ping Sweep funktioniert hat?
  - Was kann das Ubuntu GW sehen?
- *Advanced: Welche Schlüsse ziehen Sie daraus für Erkennung von Eindringlingen (Intrusion Detection System – IDS)?*

## 2.2 OS Detection

- Im folgenden wird versucht über die Kali VM Informationen über einen Rechner im LAN herauszufinden.
- Starten Sie in der Kali VM eine Shell und führen Sie eine nmap OS Detection für einen der erkannten Rechner im LAN durch:
  `nmap -O -v 172.16.1.X`
- Welche Informationen können Sie so herausfinden?

## 2.3 E-Mail Sniffing

- Starten Sie wireshark in der Ubuntu VM. Diesmal dient wireshark zum Ausforschen von Informationen, die eigentlich nicht für den Lauscher bestimmt sind. Dieses Lauschen ist eine passive Attacke, d.h. es wird nicht ins Protokoll eingegriffen. In den kommenden Laboreinheiten werden aktive Attacken geprobt und Gegenmaßnahmen untersucht.
- Stellen Sie den Filter für wireshark auf das POP3 Protokoll.
- Wechseln Sie zur Windows WM. Starten Sie in der Windows VM den vorinstallierten Thunderbird E-Mail Client und rufen Sie die Nachrichten ab (Passwort für User *rektor*: „rektor“).

- Wechseln Sie zur Ubuntu VM und analyiseren Sie das Wireshark Protokoll. Versuchen Sie die Pakete zu identifizieren, die das Passwort enthalten könnten. Hinweis: Plaintextpasswörter sind BASE-64 kodiert.
- Schicken Sie sich vom Account „rektor“ ein E-Mail. Versuchen Sie dieses E-Mail im Wireshark zu finden und auf der Ubuntu VM zu lesen.
- Versuchen Sie die gleiche Attacken auf der Kali VM durchzuführen.
- *Advanced: Welche Voraussetzungen müssen gelten, damit dieser Angriff erfolgreich ist, bzw. welche Gegenmaßnahmen können getroffen werden, um ihn zu verhindern?*

# 3 Aktive Attacken

## 3.1 ARP Poisoning

- Starten Sie wireshark auf der Kali VM
- Lassen Sie zur Information zuerst das Mapping von IP auf MAC Adresse auf Windows VM (`arp -a`) und Ubuntu VM (`arp -a`) anzeigen.
- Starten Sie ettercap auf der Kali VM mittels `ettercap -G`. Verwenden Sie ettercap um eine ARP Poisoning Attacke durchzuführen (grundlegende Beschreibung siehe Laborfolien) und das POP Passwort des Windows Users auf der Kali VM in Erfahrung zu bringen. Auf Moodle finden Sie ein Howto, das Ihnen weiterhelfen kann.
- Prüfen Sie wiederum auf Windows VM und Ubuntu VM die Zuweisung MAC und IP Adresse. Was hat sich geändert?
- Wenn ARP Poisoning auf der Kali VM erfolgreich war, checken Sie in der Windows VM über Thunderbird den E-Mail Account.
- Wechseln Sie zurück in die Kali VM – Sie sollten nun im Besitz des Passworts sein.
- Beenden Sie die Attacke (MITM → Stop mitm attack).
- Leitfragen für das Protokoll
  - Beschreiben Sie die Funktionsweise der ARP Poisoning Attacke.
  - Welche Rückschlüsse lässt das Wireshark Protokoll zu?
  - Was macht ettercap vor dem Beenden der Attacke?
  - *Advanced: Warum funktioniert die ARP Attacke permanent und wird nicht nach einiger Zeit durch ein (Original-)ARP Paket zurückgesetzt?*
  - *Advanced: Recherchieren Sie mögliche Gegenmaßnahmen.*

## 3.2 DHCP Spoofing (Advanced)

- Stoppen Sie in der Ubuntu VM den DHCP Server.
- Starten Sie vorab wieder wireshark in der Kali VM.
- Starten Sie ettercap.
- Verwenden Sie mitm→ DHCP Spoofing
  - IP Pool: zum Beispiel 172.16.1.50-99
  - Netmask: 255.255.255.0
  - DNS Server: 192.168.136.2
- Wechseln Sie in die Windows XP VM.
- Geben Sie in der Konsole (cmd) den Befehl: `ipconfig /release` gefolgt von `ipconfig /renew` ein.
  -
  - Protokollieren Sie kurz was während der Attacke passiert.
  - *Welche Gegenmaßnahmen sind vorstellbar?*

## 3.3 SSL Capturing (ADVANCED)

In dieser Übung wird eine MITM Attacke am Beispiel ARP Poisoning um SSL Capturing erweitert.

- Stellen Sie sicher, dass die Windows VM die richtigen Einstellungen für Gateway, etc. hat. (Eventuell ist ein `ipconfig /release` gefolgt von `ipconfig /renew` notwendig.)
- Wechseln Sie zur Kali VM.
- Öffnen Sie `/etc/ettercap/etter.conf` in einem Editor.
- Stellen Sie sicher dass der Abschnitt [priv] wie folgt konfiguriert ist:

```
[privs]
ec_uid = 0
ec_gid = 0
```

- Scrollen Sie zum Abschnitt `redir_command_on/off`. Stellen Sie sicher, dass am Anfang der beiden Zeilen, die auf „# if you use iptables:“ folgen, keine Kommentarzeichen (#) stehen:

```
# if you use iptables:
redir_command_on = "iptables -t nat -A PREROUTING ...
redir_command_off = "iptables -t nat -D PREROUTING ...
```

- Starten Sie *ettercap* und führen Sie eine ARP Poisoning Attacke durch, wie oben beschrieben – aktivieren Sie die Checkbox „Sniff remote connections“.
- Wechseln Sie in die Windows VM und starten Sie einen Browser und laden sie eine Webseite über HTTPS. Untersucchen Sie das Zertifikat das vom Remote Server präsentiert wird.
  - Beschreiben Sie kurz wie diese MITM funktioniert.
  - Was kann getan werden um sie zu verhindern?

# 4 Metasploit

Metasploit wird verwendet, um exemplarisch Sicherheitslücken aufzudecken. Als Beispieldistribution dient Metasploitable", eine auf Ubuntu 8.04 basierende Linux Distribution, die sich durch einige gravierende Sicherheitsmängel auszeichnet.
Hilfreiche Informationen zu Metasploit finden Sie unter `http://www.offensive-security.com/metasploit-unleashed/Main_Page`

## 4.1 Vorbereitung

- Starten Sie Ubuntu Gateway
- Starten Sie Metasploitable (nur starten, Sie müssen bzw. können sich nicht einloggen)
- Verschieben Sie die Kali in VMNet 4 (das Server Segement) und starten Sie Kali
- Finden Sie in Kali mittels `nmap` heraus, welche Hosts im Netzwerk sind, im speziellen, welche IP die Metasploitable VM besitzt
- Nachdem Sie die IP festgestellt haben, führen Sie einen OS fingerprint durch (mittels `nmap`).
- Finden Sie heraus, welche Ports offen sind, und welche Services in welcher Version auf den Ports verfügbar sind (`-sV`)
- Starten Sie nun in Kali die *Metasploit console* mittels Eingabe von `msfconsole` in einer Shell

Hinweis: In Metasploit kann über den Befehl `search` nach Exploits zu einem Schlagwort gesucht werden.

## 4.2 Brute-force Attacken

- Suchen Sie mittels `search` in Metasploit nach exploits für "mysql".
- Starten Sie den Login Scanner für MySQL (`mysql_login`) mittels `use` gefolgt vom gesamten Pfad des Scanners (den Sie über die Suche im vorigen Schritt herausgefunden haben sollten).
- In MSF können Sie sich die Optionen für das mittels `use` gewählte Tool immer mit Hilfe des Befehls `show options` ausgeben lassen.
- Für die Brute-force Attacken benötigen wir Files mit möglichen Username und Password Einträgen. Wir begnügen uns, vorerst nur mögliche MySQL Default Settings anzutesten. Legen Sie dazu zwei Dateien an: `/root/pass.txt` und `/root/user.txt` (z.B. mit gedit):
  - user.txt:

    ```
    admin
    sqladmin
    root
    administrator
    rektor
    ```

  - pass.txt:

```
password
admin
root
sqladmin
its
```

- Setzen Sie in msfconsole die Optionen `PASS_FILE` und `USER_FILE` für beide Listen auf den o.a. Eintrag. Verwenden Sie dazu den Befehl `set` (`set` *`OPTION WERT`*) Um das Ziel der Attacke zu spezifizieren setzen Sie die Option `RHOSTS` auf die IP des zu attackierenden Hosts.
- Starten Sie den Scanner mittels `run`
- Nachdem Sie ein gültiges Login gefunden haben, können Sie sich nun über den mysql Client mit der Datenbank verbinden
- Starten Sie dazu einen *neuen Terminal* in der Kali VM.
- Benutzen Sie das Login, um sich mit der mysql Datenbank zu verbinden:
  `mysql -h` *`IP`* `-u` *`USER`* `-p`
- Nun benutzen Sie den Befehl mysql Befehl `load_file` in einem `SELECT` statement, um sich die Datei `/etc/passwd` anzeigen zu lassen.
- Such Sie einen Benutzernamen, der eventuell Rootrechte haben könnte (→ im Beispiel: "admin" kommt im Namen des Users vor!)
- Diesen Benutzer werden wir nun verwenden um eine Bruteforce Attacke über ssh zu starten. Fügen Sie den Benutzernamen zu /root/user.txt und zu /root/pass.txt hinzu.
- Suchen Sie in MSF nach einem geeigneten Scanner für SSH.
- Führen Sie mittels diesem Scanner eine Brute-force attacke durch.

## 4.3 Tomcat

- Sie finden die Standardsetttings für User und Passwörter in Kali mittels folgenden Linuxbefehlen:

```
find / -iname tomcat_mgr_default_pass.txt
find / -iname tomcat_mgr_default_users.txt
```

- Führen Sie mittels MSFConsole eine Brute-Force Attacke auf Tomcat durch.
- Wenn Sie ein Tomcat Login gefunden haben, recherchieren Sie, wie Sie das ausnützen können um eine Shell zu bekommen.

### 4.4 Leitfragen für die Protokollerstellung

- Diskutieren Sie kurz das Resultat dieses Angriffs und die Implikationen die Sie dadurch im Bereich Netzwerksicherheit sehen.
- Diskutieren Sie auch, welche Voraussetzungen für den Erfolg dieses Angriffs gegeben sein müssen (u.a.: lokale LAN Verbindung erforderlich?)
- Was kann der Administrator des angegriffenen Systems/Netzwerks tun, um solche Attacken zu verhindern bzw. einzuschränken?

## 5 Gegenmaßnahmen

### 5.1 Firewall Updates als erste Maßnahmen gegen Brute-force Attacken

Die folgenden Attacken haben die **Ubuntu VM** zum Ziel.

#### 5.1.1 Monitoring am Zielrechner

- Wechseln Sie zur Ubuntu VM
- Führen Sie sudo -s aus um Root-Rechte zu erhalten.
- Beobachten Sie die Datei /var/log/auth.log:
  `tail -f /var/log/auth.log`
- Starten Sie nun von Kali aus eine SSH-Brute-force Attacke auf die Ubuntu VM.

### 5.2 Firewall Update

- Eine schnelle Abhilfe gegen Brute-force Attacken ist das Blocken der IP des Angreifers mittels Eintrag in die Firewall.
- Öffnen Sie die Datei `/etc/init.d/iptables_update` und fügen Sie folgende Filterregeln hinzu (ersetzen Sie dabei `[IP]` mit der IP Adresse des Angreifers):
  `iptables -A INPUT -s [IP] -p tcp -j DROP`
- Führen Sie im Anschluss `/etc/init.d/iptables_update` aus.
- Wechseln Sie zurück zur Kali VM und stellen Sie fest, ob Ihre Maßnahme Wirkungen zeigt.
- Danach löschen Sie die Filterregel wieder und führen `/etc/init.d/iptables_update` erneut aus (damit die Kali VM für die nächste Übung wieder zugelassen ist.)

### 5.3 Dynamische Firewall Updates

- Um auf der Ubuntu VM automatische Firewall Updates vorzunehmen wird *fail2ban* verwendet.
- *fail2ban* überacht `/var/log/auth.log` und blockiert IP Adressen von denen mehrere erfolglose Anmeldungsversuche durchgeführt wurden.

- Installieren Sie fail2ban mittels
  `sudo apt-get install fail2ban`
- Die Standardeinstellungen finden Sie in `/etc/fail2ban/jail.conf`
- Das Überwachen von SSH Loginversuchen in `/var/log/auth.log` ist standardmäßig eingeschalten.
- Starten Sie eine neue Shell und lassen Sie sich die Inhalte von /var/log/fail2ban.log ständig anzeigen:
  `tail -f /var/log/fail2ban.log`
- Wechseln Sie zurück zur Kali VM und starten Sie den SSH Angriff erneut.
- Nach einigen[2] fehlgeschlagenen Versuchen sollte nun die IP des Angreifers automatisch gesperrt werden.
- Lassen Sie sich auf der Ubuntu VM die entsprechenden Regeln anzeigen: `sudoiptables -L`
- Setzen Sie dann die Firewall mittels `/etc/init.d/iptables_update` auf den Ausgangszustand zurück.

# 6 Autopwn & Meterpreter (ADVANCED)

Benutzen Sie in metasploit `browser_autopwn`. Senden Sie dann einen entsprechenden Link an den Benutzer der XP VM, z.B. über E-Mail, um eine Social Eningeering Attacke nachzustellen.
Klicken Sie nun in der XP VM auf den Link. Sie erhalten in der Kali VM eine Meterpreter-Session für die XP VM.
Machen Sie sich mit den Möglichkeiten von meterpreter vertraut:

- Enumeration (PW-Hashes, Firefox, etc.)
- Keylogger
- Screenshots
- Starten und Beenden von Programmen am Zielrechner
- Installieren eines Backdoors (*persistence*)

[2] Das sind nicht immer exakt drei Versuche. Warum?