Emailservereinrichtung und Man in the Middle

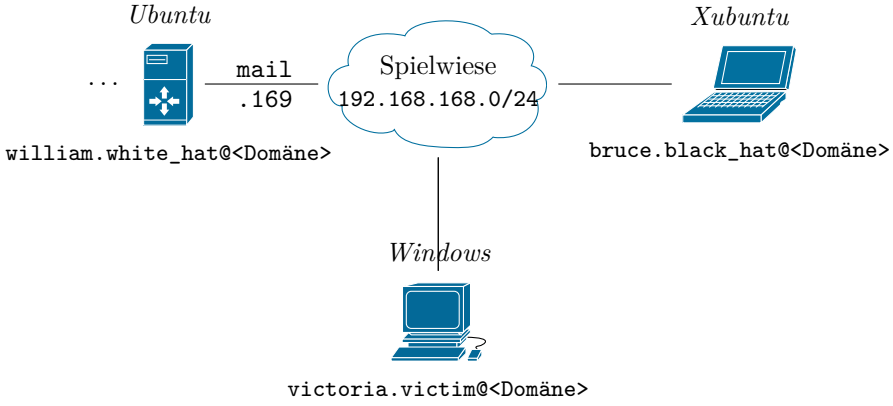
Lösen Sie die nachfolgenden Aufgaben und bereiten Sie diese bis zum nächsten Lehrveranstaltungstermin vor.

01.

a) Fügen Sie als Superuser auf dem *Ubuntu*-Server zwei Benutzer – *bruce* und *victoria* – mit dem Befehl `adduser <Benutzername>` hinzu. Wählen Sie als Passwort den jeweiligen Benutzernamen und geben Sie alle notwendigen Details ein. Loggen Sie sich testweise mit `exit` aus und mit den neuen Benutzerkennungen wieder ein, um die Einrichtung zu überprüfen.

b) Konfigurieren Sie den Mailserver auf dem *Ubuntu*-Server so, dass die IP der in der Grafik unten abgebildeten entspricht und für jeden Benutzer ein Emailkonto eingerichtet ist. Folgen Sie den Hinweisen zur Einrichtung.

c) Installieren Sie *Thunderbird* in der *Windows*-VM und richten Sie ein Emailkonto für `victoria.victim@<Domänenname>` ein. Überprüfen Sie die Einrichtung, indem Sie Emails aus dem Posteingang abrufen, die Sie zuvor auf dem *Ubuntu*-Server mit dem `sendmail`-Befehl (als ein anderer Benutzer) verschickt haben. Schicken Sie aus *Thunderbird* eine Antwortemail und lesen Sie diese auf dem *Ubuntu*-Server mit dem `mail`-Befehl (`n` zeigt die nächste Nachricht, `q` beendet). Folgen Sie den Hinweisen zur Verwendung.



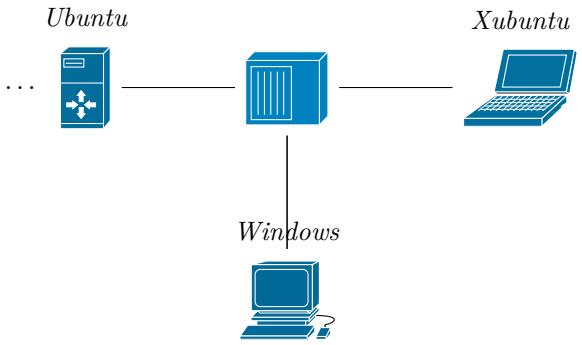
Domäne `spielwiese-<Nachname>.tld.`, z.B. `spielwiese-unterweger.tld.`

02.

a) Starten Sie *Wireshark* auf der *Xubuntu*-VM und versuchen Sie, Emailverkehr aufzeichnen. Folgen Sie den Hinweisen zur Verwendung. Erläutern Sie, welche Daten aufgezeichnet werden können und begründen Sie, warum der Rest nicht aufgezeichnet werden kann.

b) Fahren Sie die *Xubuntu*-VM herunter und konfigurieren Sie für den aktiven Netzwerkadapter in den VM-Einstellungen *erlauben für alle VMs* als *Promiscuous-Modus*, um ein nicht geswitchtes Netz (alle Geräte im Netzwerk *Spielwiese* hängen an einem Hub, wie in der Abbildung unten dargestellt) nachzubilden. Wiederholen Sie den Versuch, Emailverkehr aufzuzeichnen und erläutern Sie die Unterschiede zum geswitchten Netzwerk.

c) Versuchen Sie mit *Wireshark*, Benutzernamen, Passwörter und ausgehende (d.h. über SMTP übertragene) Nachrichtentexte aus dem Emailverkehr von *Thunderbird* mitzulesen. Folgen Sie den Hinweisen zur Verwendung.



03.

a) Aktivieren Sie die Unterstützung für Verbindungsverschlüsselung in den IMAP-Servereinstellungen auf dem *Ubuntu*-Server und ändern Sie die Einstellungen des IMAP- sowie des SMTP-Servers in *Thunderbird* auf der *Windows*-VM entsprechend, d.h. stellen Sie *Connection Security* auf *STARTTLS*. Erläutern Sie, wie viele Informationen aus dem Emailverkehr nun in *Wireshark* auf der *Xubuntu*-VM noch rekonstruierbar sind.

b) Fahren Sie die *Xubuntu*-VM herunter und stellen Sie für den aktiven Netzwerkadapter in den VM-Einstellungen den *Promiscuous-Modus* wieder auf *verweigern*, um den Ursprungszustand eines geswitchten Netzes wiederherzustellen. Verwenden Sie anschließend *Ettercap*, um eine ARP-Poisoning-Attacke durchzuführen, die den Emailverkehr zwischen der *Windows*-VM und dem IMAP-/SMTP-Server auf die *Xubuntu*-VM umleitet. Folgen Sie den Hinweisen zur Verwendung. Erörtern Sie die Rekonstruierbarkeit von Emailverkehr mit und ohne Zuhilfenahme dieser Attacke.

c) Analysieren Sie mit dem Befehl `arp -a` in allen VMs, wie sich der ARP-Cache vor, während und nach einer erfolgreichen ARP-Poisoning-Attacke entwickelt und inwieweit die Attacke als solche in *Wireshark* erkennbar ist. Erötern Sie Sicherheitsimplikationen und weitere Angriffsmöglichkeiten.

Hinweis zur Einrichtung des Mailservers auf einem *Ubuntu*-Server

Stellen Sie sicher, dass Sie eingeloggt sind und führen Sie alle nachfolgenden Befehle als Superuser aus. Öffnen Sie die Konfigurationsdatei des Mailservers mit dem Editor `nano`, indem Sie

```
nano /etc/postfix/main.cf
```

eingeben.
Deaktivieren Sie die Option `alias_maps`, indem Sie eine Raute (`#`) am Beginn der entsprechenden Zeile hinzufügen, um diese auszukommentieren. Fügen Sie anschließend die Zeile `virtual_alias_maps = hash:/etc/postfix/virtual` hinzu, um den Pfad einer Zuordnungsdatei anzugeben, die Emailadressen Benutzernamen zuordnet.
Zusätzlich sollte der von außen erreichbare SMTP-Server auf eine IP-Adresse beschränkt werden, damit er nicht von allen anderen Netzwerkschnittstellen aus erreichbar ist. Dies kann über die Option `inet_interfaces` gesteuert werden, die von `all` auf die gewünschte Mailserver-IP-Adresse geändert wird.
Speichern Sie die Datei und öffnen Sie anschließend die zuvor angegebene Zuordnungsdatei `/etc/postfix/virtual`. Fügen Sie eine Zuordnung pro Zeile nach dem folgenden Muster hinzu:

```
1 bruce.black_hat@spielwiese-unterweger.tld bruce
```

Vor dem Leerzeichen steht hierbei die volle Emailadresse, danach der Name des Benutzers auf dem Server, dem Emails zugestellt werden, die an die angegebene Emailadresse geschickt werden. Speichern Sie die Änderungen und beenden Sie `nano`.
Nach der Konfiguration der Zuordnungen muss die interne Zuordnungstabelle des Mailservers aktualisiert werden:

```
postmap /etc/postfix/virtual
```

Außerdem muss der Mailserver neu gestartet werden:

```
/etc/init.d/postfix restart
```

Abschließend kann mit dem Befehl

```
netstat -4at
```

überprüft werden, ob nur ein SMTP-Port auf der gewünschten IP-Adresse offen ist und keine weiteren Emailprotokolle und/oder IP-Adressen bedient werden.
Um Emails mit gängigen Emailprogramm von außen (d.h. von anderen Rechnern aus) abrufen zu können, muss zusätzlich ein POP3- und/oder ein IMAP-Server eingerichtet werden, wie unten beschrieben.

Hinweis zur Einrichtung des IMAP-Servers auf einem *Ubuntu*-Server

Stellen Sie sicher, dass Sie eingeloggt sind und führen Sie alle nachfolgenden Befehle als Superuser aus. Öffnen Sie die Konfigurationsdatei des IMAP-Servers – `/etc/dovecot/dovecot.conf` – mit `nano`. Ändern Sie die Zeile für die Option `protocols` zu

```
1 protocols = imap
```

ab, um (ausschließlich) IMAP zu aktivieren. Entfernen Sie die Raute (`#`) vor der (**nicht** eingerückten) Zeile für die Option `listen` und ersetzen Sie `*` durch die IP-Adresse, auf der der IMAP-Server lauschen soll.
Entfernen Sie die Raute vor der Zeile für die Option `disable_plaintext_auth` und ersetzen Sie `yes` durch `no`, um Authentifizierung im Klartext zu erlauben. Entfernen Sie analog die Raute vor der Zeile für die Option `ssl` und setzen Sie die Option auf `no`, um SSL zu deaktivieren. *Hinweis: Konfigurieren Sie einen IMAP-Server* ***unter keinen Umständen*** *mit diesen beiden Optionen, wenn Sie ihn praktisch einsetzen möchten. Die hier gezeigten Optionen dienen zum Aufzeigen von Angriffsmöglichkeiten bei falscher Konfiguration.*
Entfernen Sie zuletzt die Raute vor der (**nicht** eingerückten) Zeile für die Option `mail_location` und ändern Sie diese zu

```
1 mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

Dies ist der Standardpfad der Mailbox(-Datei) für Benutzer.
Nach der Konfiguration muss der Mailserver neu gestartet werden:

```
/etc/init.d/dovecot restart
```

Abschließend kann mit dem Befehl

```
netstat -4at
```

überprüft werden, ob nur ein IMAP-Port auf der gewünschten IP-Adresse offen ist und keine weiteren Emailprotokolle und/oder IP-Adressen bedient werden.

Hinweis zur Einrichtung von Thunderbird in *Windows*

Laden Sie *Thunderbird* von `https://www.mozilla.org/en-US/thunderbird/all/` **auf Ihren Hostrechner** herunter. Wählen Sie die aktuellste Version für *Windows* in *English (US)*. Die nachfolgenden Hinweise beziehen sich auf Version 45.7.0 (`https://download.mozilla.org/?product=thunderbird-45.7.0-SSL&os=win&lang=en-US`) und können für andere Versionen abweichen.
Ziehen Sie die Setupdatei per Drag'n'Drop vom Hostrechner auf den Desktop der gestarteten *Windows*-VM. Warten Sie, bis die Datei übertragen wurde, öffnen Sie sie durch einen Doppelklick und installieren Sie *Thunderbird* mit Hilfe des Installationsassistenten. Starten Sie es anschließend und überspringen Sie alle Schritte, die der automatischen Einrichtung dienen.

Öffnen Sie im Einstellungsmenü unter dem Menüpunkt *Options* den Untermenüpunkt *Account Settings*. Klicken Sie auf *Account Actions* und öffnen Sie anschließend den Menüpunkt *Add Mail Account*. Geben Sie im erscheinenden Fenster den vollen Namen, die Emailadresse und das Passwort für den dazugehörigen Benutzer ein. Klicken Sie auf *Continue*, um fortzufahren.
Wählen Sie *Manual config* und stellen Sie sicher, dass die Option *SSL* in allen Fällen auf *None* gestellt ist. Ändern Sie zudem die Benutzernamen *Incoming* und *Outgoing* auf jenen, dem das dazugehörige Emailkonto (sowie das oben angegebene Passwort) gehört. Klicken Sie auf *Re-test* und anschließend auf *Done*. Bestätigen Sie die Sicherheitswarnung mit *I understand the risks* und klicken Sie abschließend auf *Done*. *Hinweis: Bestätigen Sie derartige Sicherheitswarnungen* ***unter keinen Umständen*** *beim Einrichten eines beruflich oder privat verwendeten Emailkontos.*

Hinweis zur Verwendung von `sendmail`

Emails können unter anderem mit dem Befehl `sendmail` vom aktuell eingeloggten Benutzer verschickt werden. Stellen Sie sicher, dass Sie den Befehl nicht als Superuser (`root`) ausführen – in der bisher beschriebenen Konfiguration ist kein gesondertes Emailkonto für ihn vorgesehen.
Öffnen Sie vor dem Aufruf von `sendmail` eine neue Datei, z.B. `/tmp/mail.txt`, mit `nano` und geben Sie eine Nachricht nach dem folgenden Muster ein:

```
1 Subject: Test
2
3 Hallo Victoria!
4
5 Das ist ein Test, durch den du siehst, dass dein Email
     -Account funktioniert. Antworte mir bitte kurz,
     damit ich sehe, ob auch in die Gegenrichtung alles
     funktioniert.
6
7 LG William
```

Zeile 1 beginnt mit `Subject: <Betreff>` und ist verpflichtend. Danach folgt eine Leerzeile und beliebiger Nachrichtentext. Das Versenden der Nachricht erfolgt dann z.B. mit dem Befehl

```
sendmail victoria.victim@spielwiese-unterweger.tld < /tmp/mail.txt
```

Die Emailadresse wird hierbei als Parameter angegeben und der Text als Eingabe ins Programm `sendmail` umgeleitet.

Hinweis zur Verwendung von *Wireshark*

Wireshark kann im Terminal mit dem Befehl

```
wireshark
```

gestartet werden. Alternativ kann das Programm über das Programmmenü des Betriebssystemes gestartet werden.
Eine neue Aufzeichnung kann über einen Doppelklick auf den Netzwerkschnittstellennamen `enp0s8` (oder vergleichbar) gestart werden (wird die Maus über den Namen bewegt, erscheint die IP-Adresse der Schnittstelle zur Überprüfung). Bis die Aufzeichnung durch einen Klick das entsprechende Symbol in der Symbolleiste beendet wird, werden alle Pakete, die an der angegebenen Netzwerkschnittstelle ankommen, aufgelistet und können analysiert werden.
Das Textfeld oben kann dabei zur Filterung verwendet werden. Der Filter `imap` zeigt beispielsweise ausschließlich Pakete an, die zum IMAP-Protokoll gehören. Falls nach der Filterung Pakete übrig bleiben, können diese durch Auswahl per Klick nach Protokollschicht getrennt untersucht werden, wie am nachfolgenden Beispiel illustriert.
Base64-kodierte Daten wie zum Beispiel Authentifizierungsinformationen im *Request Tag* der IMAP-Antwort (in der obersten Protokollschicht, d.h. in der Protokollaufschlüsselung am weitesten unten), können wie folgt (menschen-)lesbar gemacht werden. Zuerst wird der Tag (falls notwendig durch Aufklappen der Baumstruktur bis in die unterste Ebene) ausgewählt. Dann wird im Kontextmenü im Untermenü *Kopieren* der Untermenüeintrag *...als druckbarer Text* gewählt. Anschließend wird im Terminal der kopierte Text (Base64-String) eingefügt und mit dem Befehl `base64` dekodiert (Parameter `-d`):

```
echo "<Eingefügter Text>" | base64 -d
```

Die spitzen Klammern sind **nicht** einzufügen.
Sollen erneut Pakete aufgezeichnet werden, kann über den Menüeintrag *Schließen* im Menü *Datei* die aktuelle Aufzeichnung verworfen werden, was mit *Fortsetzen ohne zu speichern* bestätigt werden muss. Die neue Aufzeichnung kann dann erneut wie oben beschrieben erfolgen.

Hinweis zur Verwendung von *Ettercap*

Ettercap kann im Terminal mit dem Befehl

```
sudo ettercap -G
```

gestartet werden (oder alternativ über das Programmmenü, vgl. oben).
Aktivieren Sie *Unified Sniffing* über den gleichnamigen Menüpunkt im Menü *Sniff* und wählen Sie `enp0s8` (oder vergleichbar) als Netzwerkschnittstelle aus. Wählen Sie anschließend den Menüeintrag *Scan for hosts* im Menü *Hosts*, warten Sie den Scan ab und öffnen Sie dann die *Hosts list* über den gleichnamigen Menüpunkt im Menü *Hosts*. Wählen Sie die IP, die umgeleitet werden soll, aus und klicken Sie auf *Add to Target 1*. Wählen Sie analog die IP des ARP-Poisoining-„Opfers“ und klicken Sie auf *Add to Target 2*.
Wählen Sie anschließend den Menüeintrag *ARP poisoning...* im Menü *Mitm* und aktivieren Sie im erscheinenden Optionsfenster *Sniff remote connections*. Die ARP-Poisoning-Attacke ist nun aktiv, bis der Menüeintrag *Stop Mitm attack(s)* im Menü *Mitm* ausgewählt wird.