Domäneneinrichtung und interne Reconnaissance

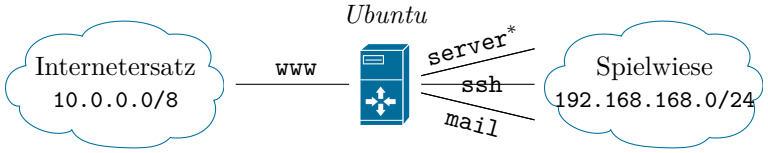
Lösen Sie die nachfolgenden Aufgaben und bereiten Sie diese bis zum nächsten Lehrveranstaltungstermin vor.

01.

a) Konfigurieren Sie den DNS-Server auf dem *Ubuntu*-Server derart, dass die Domänennamen den in der Grafik unten angegebenen entsprechen. Folgen Sie den Hinweisen zur Einrichtung.

b) Überprüfen Sie die Funktionalität der lokalen Namensauflösung per DNS mit den Befehlen `dig` und `host` (Beispielaufruf für die Domäne `google.de`: `host www.google.de.`). Führen Sie die Befehle für **alle** Namen in der Domäne durch und beschreiben Sie die Ausgabe(n).

c) Überprüfen Sie die Funktionalität der Namensauflösung per DNS in der *Kali*-VM analog zum vorherigen Beispiel.



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

`www: 10.1.2.3` (vollständig z.B. `www.spielwiese-unterweger.tld.`),
`server*: 192.168.168.1`, `ssh: 192.168.168.168`, `mail: 192.168.168.169`
* Platzsparende Kurzform von `server-<Nachname>` (z.B. `server-unterweger`)

02.

a) Verwenden Sie `nmap -A <Adressbereich>` (z.B. `nmap -A 10.0.0.0/8`) auf der *Kali*-VM, um den lokalen IP-Adressbereich (*Spielwiese*) zu scannen. Erstellen Sie eine Liste aller gefundenen Rechner nebst Betriebssystemversion und den jeweiligen offenen Ports. Schließen Sie daraus, welche Dienste auf diesen Rechnern laufen. Verwenden Sie die zusätzlichen Parameter `-v` oder `-vv`, um bei Bedarf eine detailliertere Ausgabe zu erhalten.
Hinweis: Starten Sie auch die Windows-VM vor dem Scan.

b) Verwenden Sie `netdiscover -r`, um den lokalen IP-Adressbereich (*Spielwiese*) zu scannen. Schließen Sie aus der Ausgabe, wie viele verschiedene Rechner es im lokalen Netzwerk gibt und gleichen Sie das Ergebnis mit dem `nmap`-Scan ab. Erstellen Sie aus den Erkenntnissen eine Skizze des lokalen Netzwerkes und prüfen Sie diese auf Plausibilität.
Hinweis: Wenden Sie bei Unsicherheiten `traceroute` auf die gefundenen IP-Adressen an, um Ihre Ergebnisse zu präzisieren.

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

Stellen Sie sicher, dass Sie eingeloggt sind. Führen Sie alle nachfolgenden Befehle als Superuser aus, indem Sie

```
sudo su
```

eingeben und mit Ihrem Passwort bestätigen. Öffnen Sie die Konfigurationsdatei des DNS-Servers mit dem Editor `nano`, indem Sie

```
nano /etc/bind/named.conf.local
```

eingeben.
Jede DNS-Zone muss separat konfiguriert werden. Nutzen Sie folgendes Muster für die Beispielzone `spielwiese-unterweger.tld`, für die festlegt werden muss, in welcher Datei (`/etc/bind/db.spielwiese-unterweger`) weitere Konfigurationsinformationen zu finden sein werden:

```
1 zone "spielwiese-unterweger.tld" {
2   type master;
3   file "/etc/bind/db.spielwiese-unterweger.tld";
4 };
```

Für die Unterstützung von Reverse DNS Lookups muss pro IP-Adressbereich zusätzlich eine Zone definiert werden. Im nachfolgenden Beispiel ist die Konfiguration für den beispielhaften Adressbereich `192.168.0.0/16` definiert:

```
1 zone "168.192.in-addr.arpa" {
2   type master;
3   notify no;
4   file "/etc/bind/db.192";
5 };
```

Der Dateiname (im Beispiel `/etc/bind/db.192`) kann frei gewählt werden, muss aber eindeutig sein.
Für jede Zone muss die angegebene Konfigurationsdatei entsprechend befüllt werden. Die Vorgehensweise unterscheidet sich hierbei für „reguläre“ Zonen und solche für Reverse DNS Lookups.
Konfigurationen für „reguläre“ Zonen können auf Basis der lokalen Beispielkonfiguration in `/etc/bind/db.local` erstellt werden, indem letztere kopiert wird, z.B.:

```
cp /etc/bind/db.local /etc/bind/db.spielwiese-unterweger.tld
```

Die kopierte Datei kann wie oben mit `nano` (mit dem Dateinamen als Parameter) bearbeitet werden. Zuerst müssen **alle** Vorkommnisse von `localhost.` durch `<Name>.<Domäne>` (z.B. `server-unterweger.spielwiese-unterweger.tld.`) ersetzt werden, wobei `<Name>` hier mit dem Rechnernamen übereinstimmt. Anschließend muss am Dateiende für **jede** Namen-Adress-Kombination eine Zeile nach dem folgenden Muster hinzugefügt werden:

```
1 test IN A 192.168.0.7
```

Das Beispiel definiert einen `A`-Record (Address Record) für die (Unter-)Domäne `test.spielwiese-unterweger.tld.`, der auf die IP-Adresse `192.168.0.7` verweist.
Für Mailserver muss zusätzlich der `MX`-Record (Mail Exchange Record) gesetzt werden, z.B.:

```
1 @ IN MX 10 mail.spielwiese-unterweger.tld.
```

Der Wert `10` steht hierbei für einen Prioritätswert, der bei Verwendung nur eines Mailservers nicht weiter relevant ist.
Konfigurationen für Reverse-DNS-Lookup-Zonen können auf Basis der lokalen Beispielkonfiguration in `/etc/bind/db.127` erstellt werden, indem letztere kopiert wird, z.B.:

```
cp /etc/bind/db.127 /etc/bind/db.spielwiese-unterweger.192
```

Wieder kann die neue Datei kann wie oben beschrieben mit `nano` bearbeitet werden. Zuerst müssen **alle** Vorkommnisse von `localhost.` durch `<Name>.<Domäne>` (z.B. `server-unterweger.spielwiese-unterweger.tld.`) ersetzt werden, wobei `<Name>` hier mit dem Rechnernamen übereinstimmt. Danach muss die letzte Zeile gelöscht werden. Anschließend muss am Dateiende für **jede** Adress-Namen-Kombination eine Zeile nach dem folgenden Muster hinzugefügt werden:

```
1 7.0 in PTR test.spielwiese-unterweger.tld.
```

Das Beispiel definiert den zum oben definierten `A`-Record passenden `PTR`-Record (Pointer record), der die IP-Adresse `192.168.0.7` (nur der lokale Adressteil – hier im Beispiel `0.7` in entsprechender Reihenfolge – ist anzugeben) mit dem Namen verknüpft, um entsprechende Reverse DNS Lookups zu ermöglichen.
Nach der Konfiguration der Zonen muss der DNS-Server neu gestartet werden:

```
/etc/init.d/bind9 restart
```

Beim Auftreten von Fehlern kann mit dem Befehl

```
tail /var/log/daemon.log | grep named
```

das Log nach nameserverspezifischen Fehlermeldungen durchsucht werden.