Übungsblatt 7 – IT- & Netzwerk-Security

Voraussetzungen: Wie in den vorigen Übungen sollte Sie in der Lage sein ein eigenes statisches Netzwerk aufzubauen. D.h. Ihr Netzwerk sollten den Anforderungen des Übungsblattes 4 genügen – es gibt einen Router der zwei Subnetze verbindet und einen Backbone-Router, der für die Vernetzung der Bankreihen, sowie den Uplink sorgt. Das Adressschema kann der Tabelle 1 entnommen werden.

Tabelle 1: Adressschema für das Labor

	IP || IP-Range
LAN_X	10.0.X.Y/Size
Backbone	10.10.10.100 + ρ
Labornetz	10.0.0.0/8
Uplink	10.10.10.254
DNS	10.10.10.254

Nachdem Ihr Netzwerk aufgebaut ist:

- Überprüfen Sie ob sich Ihre Raspberry Pis untereinander erreichen können.
- Überprüfen Sie ob alle Raspberry Pis den Uplink erreichen können und ob externe Adresse (d.h. IP-Adressen außerhalb des Labors) erreichbar sind.
- Überprüfen Sie ob die Namensauflösung funktioniert.

Aufgabe A – Domain Name System (DNS)

1.)

a.) Fragen Sie mit jedem der vier Tools auf der Kommandozeile jeweils einmal einen Hostnamen (bspw. `www.htw-berlin.de`), einen Domainnamen (htw-berlin.de) und eine IP-Adresse (141.45.5.100) ab.

b.) Schauen Sie sich die Ausgabe von *dig* bei der Abfrage der IP-Adresse genauer an – dort werden Sie in der „Question Section“ sehen, das nach dem A-Resource-Record mit dem Namen 141.45.5.100 gefragt wurde. Wenn Sie den Namen zu dieser IP-Adresse suchen – welchen Resource-Record müssen Sie dann anstelle des A-Records erfragen?

c.) In welcher Form müssen Sie dann die IP-Adresse angeben? (Test mit dig -t <record-type> <richtiges-format-ip-adresse>).

d.) Denken Sie sich einen Domainnamen aus, den es wahrscheinlich geben könnte, aber den noch niemand vom Netzwerk der HTW-Berlin aus innerhalb der letzten Stunden angefragt hat (z.B. `www.uriminzokkiri.com` oder `www.northkoreatech.org`). Erfragen Sie diesen Namen zweimal kurz hintereinander via dig und vergleichen Sie die beiden Ausgaben. Worin unterscheiden sich beide Einträge? Begründen Sie diese Unterschiede!

e.) Erfragen Sie mit host, dig und nslookup den zuständigen Mail-Server für die Domain `htw-berlin.de`.

f.) Erzwingen Sie mit *host, dig* und *nslookup*, das die Namensauflösung nicht mit dem Standard-Nameserver des Betriebssystems, sondern mit einem öffentlichen Nameserver (bspw.: 9.9.9.9) erfolgt. Testen Sie am Besten zuerst mit dig oder nslookup , da diese Ihnen immer sagen, welche Nameserver sie genutzt haben. *host* liefert diese Information nur, wenn Sie explizit eigene Server angefordert haben.

2.) DNS-Resolver: Das Listing zeigt die „resolv.conf“ eines Servers.

```
1 # Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
2 # DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
3 nameserver 141.45.3.100
4 search f4.htw-berlin.de
```

Was bedeuten die Einträge mit den Schlüsselwörtern: „nameserver“ und „search“?

Aufgabe B – SSH Basics

Die folgenden Aufgaben stellen verschiedene Arten der verschlüsselten Kommunikation zwischen Prozessen oder Rechnern dar. Zunächst sollen Sie sich mit dem Umgang mit SSH vertraut machen, anschließend werden einige theoretische Konzepte aus der Theorie in die Praxis umgesetzt. Sodass Sie sich ohne Passwort auf anderen Maschinen einloggen können, bestimmte User sich nur noch einloggen dürfen oder ausschließlich ausgewählte Kommandos verfügbar sind.

1.) Starten Sie Wireshark, sodass Sie den anfallenden Traffic analysieren können.

2.) Überprüfen Sie, ob in Ihrem Heimatverzeichnis bereits der Ordner `.ssh` existiert. Falls ja, löschen Sie diesen!

3.) Lassen Sie vor beginn der eigentlichen Arbeit die beiden Scripte *reset_ssh_config.sh* und *reset_ssh_config.sh* durchlaufen. Somit wird sichergestellt, dass keine alte Konfiguration den Übungsspaß trübt.

a.) Loggen Sie sich via SSH auf dem Uranus-Server (`uranus.f4.htw-berlin.de`) ein! Achten Sie darauf, dass zu viele Fehlversuche dazu führen, dass der Server das gesamte Labor Blocken können.

b.) Was bedeuten die Abfragen zur „authenticity“ die Ihnen beim ersten mal gestellt wird. (Auf den Raspberry Pis sollte dies der Fall sein!)

c.) Wie können Sie den Fingerprint prüfen? Mit welchem Programm können Sie sich diesen anzeigen lassen?
Bspw.: *SHA256:KsUg4lOc91/iJBYFkQhxeI/YGkcnKV2uKUXFNP1ymiw root@xen (ECDSA)*)

d.) Starten Sie in Wireshark einen neuen Traffic-Mitschnitt auf dem Ethernet-Netzwerkinterface. Anschließend soll eine neue SSH-Session von einem anderen Rechner gestartet werden. Analysieren Sie auszugsweise die entsprechenden Pakete! Was wird von Traffic verschlüsselt, was können Sie einsehen?

e.) Sie müssen sich bis jetzt immer via Passwort authentifizieren, d.h. Ihr Login erfolgt aufgrund eines Passworts. Ist Ihr Passwort in einem der ersten Pakete zu finden? Wenn es nicht zu finden ist, wie konnten Sie sich dennoch erfolgreich anmelden? (Welcher kryptografische Mechanismus greift hier ein...)

f.) Wenn Sie die entsprechenden Wireshark Mitschnitte ausgewertet haben, ist Ihnen aufgefallen, dass dort ein „Key Exchange“stattfindet. Welches kryptografische Verfahren wird dort verwendet und ist dies eine symmetrisches oder asymmetrisches Kryptografieverfahren?

4.) Ermöglichen Sie nun den Login mittels SSH zum Linux-SSH-Server **ohne** das Nutzerpasswort angeben zu müssen.
Achtung: Wenn Sie sich auf dem Uranus ohne Passwort anmelden wollen, muss eine bereits existierende SSH-Verbindung auf dem Uranus-Server vorhanden sein, da ihr Home-Directory erst im Anschluss gemountet wird und ihr hinterlegter Public-Key ansprechbar ist.

a.) Generieren Sie sich ein SSH-Schlüsselpaar! Nutzen Sie hierfür die recherchierten Parameter aus Ihren Notizen.

b.) Beim generieren des Schlüssels werden Sie aufgefordert eine Passphrase einzugeben. Der Private-Key ist durch eine Passphrase geschützt, sodass dieser geheime Schlüssel nur von Ihnen geöffnet werden kann. Wie ist die Passphrase zu wählen? Was gilt es zu beachten?

c.) Verbinden Sie sich von Rechner zu Rechner ohne ein Passwort zu nutzen. D.h. Sie sollten über das eigene LAN hinaus auf einem anderen Raspberry Pi via SSH zugreifen können. Sie könne sich hierfür ein neuen Nutzer anlegen (*useradd*).

d.) Setzen Sie die Anzahl der maximalen Login-Fehlversuche auf drei!

e.) Erlauben Sie dem Nutzer *student* nur noch das Auflisten des Home-Verzeichnis, wenn er sich via SSH verbunden hat.

f.) Setzen Sie als Anmeldeverfahren SSH auf reine Public-Key-Kryptografie. Hat dies eventuell auch Nachteile?

5.) Mit SSH können Sie beliebige TCP-Verbindungen über die verschlüsselte SSH-Verbindung „tunneln“. Somit wird es Ihnen möglich, Server zu erreichen, zu denen Sie ansonsten direkt keinen Zugriff haben, weil sie hinter einer Firewall befinden oder der Datenverkehr anderweitig gefiltert wird (Packet-Filtering).
Konfigurieren Sie das Port-Forwarding unter SSH – ermöglichen Sie dazu folgende Zugriffe:

a.) Sie sollen von Ihrem Raspberry Pi aus ein lokales Port-Forwarding auf die Seite der HTW vornehmen. Hierzu soll ein SSH-Tunnel aufgebaut werden mit den Source-Port 8080 und dem HTTP-Port 80 für den Ziel-Port.

b.) Ihr Raspberry Pi logt sich per SSH auf einem anderen Raspberry Pi SSH-Server ein und leitet den lokalen Port 2200 auf den Port 22 des dortigen Systems weiter. Danach sollten Sie sich mit SSH über den lokalen Port mit dem SSH-Server des fremden SSH-Server verbinden können.

c.) Konfigurieren Sie eine Remote Port-Forward – stellen Sie dazu eine SSH-Verbindung vom einem anderen Raspberry Pi zu Ihrem Raspberry PI als SSH-Server her. Leiten Sie den Port 8880 des SSH-Server nun über Ihren Client zum Webserver der URL `www.htw-berlin.de` weiter. Im folgenden kann sich nun jeder Raspberry Pi mit Ihrem Raspberry Pi auf Port 8880 verbinden, um die Webseite der HTW-Berlin zu besuchen.