Übungsblatt 7 – Application Layer & SSH

Über das gesamt Semester hinweg haben Sie ein fundiertes Grundlagenwissen zu Netzwerken erworben. Sie haben mit dem Aufbau der Infrastruktur begonnen, indem Sie eigene kleine und etwas komplexere Netzwerke, samt Routing, aufgebaut und betrieben haben. Daran anknüpfend sind Sie in die Phase gegangen in der Sie sich angeschaut haben was eigentlich übertragen wird, wie sich Geräte im Netzwerk und auch darüber hinaus finden. Anschließend untersuchten Sie wie die Anwendungsebene des OSI-Modells mit einigen täglich genutzten Protokolle, wie HTTP(S), DNS, IMAP und SMTP. Witziger weise stellten fest, dass diese auch ohne schicke grafische Oberflächen ihren Dienst tun – da diese rein textbasiert sind. An dieser Stelle werden Sie sicherlich auch festgestellt haben: Wenn die Application-Layer-Protokolle textbasiert sind, können womöglich auch andere Nutzer einsehen, was über den „Äther“ geht.
Da Sie als angehende InformatikerInnen sich bewusst sind, dass Daten von Ihnen selbst, als auch Daten anderer Nutzer, schützenswert sind, beschäftigen Sie sich im letzten Übungsblatt mit den Themen Kryptografie und Netzwerksicherheit.

Aufgabe A – Domain Name System (DNS)

Das Domain Name System ist ein dezentrales System (verteilte Datenbank nach der Client-Server-Architektur), dessen primäre Aufgabe die Adressauflösung von Domain Name(n) zu IP-Adresse(n) ist. M.a.W. DNS bietet eine Abbildung von Domainname auf IP-Adresse [1]. Im Laufe der Jahre sind hierzu einige Tools entwickelt worden:

- whois
- host
- dig
- nslookup.

In der vierten Übung wurde das DNS bereits kurz angeschnitten, da Ihre Netzwerke im letzten Schritt einen Uplink in Internet erhalten haben und auch Domain Namen auflösen können sollten. Nun schauen wir uns das DNS und einige Tools, die um DNS „gewachsen“ sind, etwas genauer an.

1.) Rekapitulieren Sie Ihr Wissen zu DNS!

a.) Auf welchem Layer des OSI-Modells arbeitet DNS?

b.) Welches Transportprotokoll nutzt DNS?

c.) Auf welchem Port läuft DNS standardmäßig?

2.) Nennen und Erklären Sie die Komponenten des DNS-Systems.

[1] Bzw. als Inverse – die Abbildung von IP-Adresse auf Domainnamen (Reverse-Lookup)

a.) Was wird unter dem Begriff Resolver verstaden?

b.) Was ist ein DNS-Root-Server, was ist ein TLD-Server und was ein Domain-Server?

c.) Was ist ein Stub im Kontext von DNS?

d.) Was ist ein Bind-Server?

3.) Erläutern Sie die Auflösung einer DNS-Anfrage.

a.) Welche beiden Möglichkeiten einer Namensauflösung gibt es? D.h. welche Variante gibt einen Namen aufzulösen.

b.) Wie erfolgt die jeweilige Auflösung eines DNS-Requests?

c.) Verdeutlichen Sie sich anhand eines Beispiels, wie ein DNS-Request bearbeitet wird.

d.) DNS bietet theoretisch eine rekursive und iterative Namensauflösung, praktisch wird eine Mischung aus beiden Verfahren angewandt. Recherchieren Sie, wie diese Auflösung aussieht.

4.) Recherchieren Sie kurz wie die Tools

- whois
- host
- dig
- nslookup.

zu nutzen sind.

a.) Erläutern Sie kurz was jedes der oben genannten Tools leistet.

b.) Nennen Sie für jedes Tool geeignete Einsatzgebiete/ Szenarien.

c.) Recherchieren Sie die Syntax, sowie Semantik der Tools.

d.) Notieren und kommentieren Sie sich entsprechende Beispiele.

Aufgabe B – Kryptografie Grundlagen

Da Sie mit großer Wahrscheinlichkeit keine ausgebildeten Mathematiker sind, beginnen Sie zunächst mit einer kurzen Recherchephase. Dies soll Ihnen helfen Licht ins Dunkel zu bringen.
Hilfreiche Links:

- `https://de.wikipedia.org/wiki/Kryptologie`
- `https://en.wikipedia.org/wiki/Cryptography`
- `https://www.cryptool.org` → sehr schönes Tool! Zeigt visualisiert Chiffren & Verfahren

- Begriffsklärung Kryptografie & Chiffren:

  a.) Recherchieren Sie was sich hinter den Begriffen Kryptologie, Kryptografie und Kryptoanalyse verbirgt.

  b.) Worin besteht der maßgebliche Unterschied zwischen symmetrischen und asymmetrischen Kryptosystemen?

  c.) Welche Aufgaben könne kryptografisch via asymmetrischen Chiffren bewältigt werden?

  d.) Nennen Sie mindestens drei asymmetrische Krypto-Verfahren.

  e.) Nennen Sie mindestens drei symmetrische Chiffrierverfahren.

  f.) Was ist der Unterschied zwischen Stromchiffren und Blockchiffren?

  g.) Recherchieren Sie kurz welche Aufgabe der Diffie-Hellmann-Algorithmus und der Elgamal-Algorithmus haben? D.h. wozu werden diese Verfahren, bspw. in SSH, für gewöhnlich genutzt?

  h.) Was wird unter einem „Man-in-the-Middle-Angriff“ verstanden?

  i.) Beschreiben Sie die Gefahr des Man-in-the-Middle-Angriffs bei Diffie-Hellmann.

  j.) Recherchieren Sie zunächst was unter einer Hashfunktion verstanden wird, im Anschluss daran: Was wird unter einer kryptografischen Hashfunktion verstanden?

  k.) Was ist die Aufgabe einer kryptografischen Hashfunktion?

  l.) Woran bemisst sich die Qualität einer kryptografischen Hashfunktion?

  m.) Nennen Sie mindestens drei (aktuell ungebrochene) kryptografische Hashfunktionen.

  n.) Fakultativ: Warum kann nicht gezeigt werden (d.h. mathematisch bewiesen werden), das ein Hashfunktion Kollisionsresistent ist? (`https://en.wikipedia.org/wiki/Collision_resistance`)

- Public-Key-Kryptografie

  a.) Was wird unter dem Begriff Public-Key-Kryptografie verstanden? [2]

  b.) Warum werden Public-Key-Verfahren eingesetzt? Bzw. Warum sollte/muss ein solches Verfahren genutzt werden?

  c.) Wie läuft eine Public-Key-Verfahren im groben ab? Bspw. in *RSA* oder *Diffie-Hellman*.

- Kryptografische Zertifikate & Public-Key-Infrastruktur

a.) Was wird unter einem kryptografische Zertifikat verstanden? Welchen Nutzen hat dieses Zertifikat?

b.) Recherchieren Sie was unter einer Public-Key-Infrastruktur *PKI* verstanden wird.

c.) Im letzten Übungsblatt ist Ihnen diese des öfteren über den Weg gelaufen. Mit welcher *PKI* hatten Sie es zu tun? Was war die Aufgabe der *PKI*?

d.) Recherchieren Sie was im Zusammenhang mit *PKI*s unter dem Namen *Chain-Of-Trust* verstanden wird.

Aufgabe C – Grundlagen: Secure Shell (SSH) mit openSSH

Das gesamte Semester über haben Sie überwiegend lokal auf der Kommandozeile gearbeitet. Viele Netzwerk- und Serverkomponenten sind jedoch nicht lokal verfügbar (d.h. direkt, physisch), da diese in Rechenzentren unter besonderen Bedingungen ihren Dienst verrichten.[3] Die Administration der Rechner muss also auch entfernt möglich sein – remote.
Früher haben dies die sogenannten *r-Tools* ermöglicht, jedoch ohne kryptografische Schutzmaßnahmen. Heute übernehmen gesicherte Tools wie *SSH* mit verschiedensten Implementierungen, wie *openSSH*, diese Aufgabe.

1.) Lesen Sie folgendes SSH-Tutorial: `https://support.suso.com/supki/SSH_Tutorial_for_Linux`

2.) **Fakultativ:** Lesen Sie die Moodle bereitgestellte Ausarbeitung zu openSSH.

3.) Welche vier Aufgaben, d.h. Zusicherungen in Bezug auf die Sicherheit von Daten, kann SSH mithilfe von kryptografischen Verfahren gewährleisten?

4.) Notieren Sie sich an welchen Orten die verschiedenen Konfigurationsdateien für Server und Client im Normalfall (default) liegen. Notieren sie sich deren Zweck.

5.) Recherchieren Sie, was ein „Fingerprint“ im Sinne von SSH ist und welche Aufgabe dieser übernimmt.

6.) *SSH* kommt ohne Passwörter aus, es können Public-Key-Verfahren genutzt werden,

[3] Sie würden bestimmt nicht direkt in einem Rechenzentrum Ihre Arbeit als Admin ausführen! Da die Temperaturen unangenehm und die Lautstärke recht hoch ist. Auch die Sicherheitsbestimmungen sind enorm hoch.

d.h. Sie können *SSH* auch ohne Zugangspasswort nutzen.[4] Recherchieren Sie welche Verfahren *openSSH* hierfür anbietet.

7.) Recherchieren Sie, wie die Schlüsselgenerierung in openSSH erfolgt. Wie sind Verfahren, Schlüsselgröße und zu speichernden Ort zu wählen? Notieren Sie sich die entsprechende Syntax!

8.) Welche Schlüssellänge und welche Schlüsselarten sind für Ihren Einsatz im Labor sinnvoll? Wie hängen Schlüssellänge und Sicherheit zusammen?

9.) Lassen sich die SSH-Schlüssel zwischen den verschiedenen Clients weiterverwenden/-konvertieren? Oder muss andernfalls für jeden Client ein eigener Schlüssel generiert werden?

10.) Recherchieren Sie die Bedeutung der Passphrase. Ist die Passphrase mit dem Passwort gleichzusetzen?

11.) Wie kann aus Sicherheitsgründen ein Login ohne Passwort eingeschränkt werden, so das nur bestimmte Kommandos via SSH ausgeführt werden können?

12.) In manchen Fällen ist es ratsam den Zugriff via SSH nur auf einige Nutzer zu beschränken. Recherchieren Sie könnte anhand eines Beispiels wie das aussehen.

13.) Recherchieren Sie was „Tunneling“ im Sinne von SSH bedeutet.

Aufgabe D – SSH Port-Forwarding

Mit SSH können Sie beliebige TCP-Verbindungen über die verschlüsselte SSH-Verbindung „tunneln“. [5] Somit wird es Ihnen möglich, Server zu erreichen, zu denen Sie ansonsten direkt keinen zugriff hätten, weil sie hinter einer Firewall stehen oder der Datenverkehr anderweitig gefiltert wird.
openSSH kann nicht nur beliebige TCP-Verbindungen weiterleiten, sondern ein komplettes VPN aufbauen, in dem alle Datenverbindungen, egal ob TCP, UDP oder ICMP, über die verschlüsselte SSH-Verbindung weitergeleitet werden.
Der Nachteil hierbei ist jedoch, das es, im Gegensatz zum SSH-Port-Forwarding, nur durch den root-Nutzer eingerichtet werden kann. Den Tunnel verwenden kann jeder Nutzer/jedes Programm, aber konfigurieren muss dies der Administrator. Normale Port-Forwardings hingegen kann jeder Nutzer für sich selber nach Bedarf einrichten.
Nützliche Links:

[4] Eigentlich ist es ratsam auf Passwörter zu verzichten, da das Brechen von kryptografischen Schlüsseln momentan fast unmöglich ist

[5] `https://de.wikipedia.org/wiki/Tunnel_(Rechnernetz)`

- https://www.ssh.com/ssh/tunneling/example
- https://blog.trackets.com/2014/05/17/ssh-tunnel-local-and-remote-port-forwarding-expl
  html?utm_source=cronweekly.com
- https://marius.bloggt-in-braunschweig.de/2016/01/02/vds-schnell-ein-vpn-aufsetzen/
- https://marius.bloggt-in-braunschweig.de/2016/04/12/ssh-vpn-mit-den-iproute2-tools/
- https://debian-administration.org/article/539/Setting_up_a_Layer_3_tunneling_
  VPN_with_using_OpenSSH

- Recherchieren Sie was unter Port-Forwarding verstanden wird.
  Hinweis: Nutzen Sie die oben genannten Links!

  a.) Welche Arten von Port-Forwarding gibt es bzw. welche können mit SSH realisiert werden? Für welche Einsatzszenarien kann welches Forwarding genutzt werden?

  b.) Verdeutlichen Sie sich jeweils anhand eines Beispiels wie Forwarding genutzt werden kann.

  c.) Finden Sie heraus wie Port-Forwarding unter Linux und SSH funktioniert. D.h. Sie sollten schauen, was die Vorbedingungen sind, und welche Kommandos hierfür notwendig sind. Notieren Sie sich entsprechende Kommandos, sowie deren Bedeutung.

- Recherchieren Sie was ein *Virtual Private Netwrok (VPN)* ist und wie dies sinnvoll genutzt werden kann.

  a.) Recherchieren Sie wie ein VPN unter Nutzung von SSH zu realisieren wäre.

  b.) Notieren Sie sich die dafür notwendigen Kommandos, sowie deren Bedeutung.

Aufgabe E – VPN via Wireguard