Übungsblatt 6 – Netzwerksicherheit

Aufgabe A – Kryptografie Grundlagen

Da Sie mit großer Wahrscheinlichkeit keine ausgebildeten Mathematiker*innen sind, beginnen sie zunächst mit einer kurzen Recherchephase. Bei allen Aufgaben reicht ein grobes Verständnis, die mathematischen Formalismen können sie überspringen! Hilfreiche Links:

- https://de.wikipedia.org/wiki/Kryptologie
- https://en.wikipedia.org/wiki/Cryptography
- https://www.cryptool.org → sehr schönes Tool! Visualisiert Chiffren, Verfahren etc.

1. Begriffsklärung Kryptografie & Chiffren:
   a) Erläutern sie die grundlegende Sicherheitseigenschaften CIA (Confidentiality, Integrity, Availability) und Authenticity im Bereich der IT-Security.
   b) Recherchieren sie was sich hinter den Begriffen Kryptologie, Kryptografie und Kryptoanalyse verbirgt.
   c) Worin besteht der maßgebliche Unterschied zwischen symmetrischen und asymmetrischen Kryptosystemen?
   d) Welche Aufgaben könne kryptografisch per symmetrischen Chiffren bewältigt werden?
   e) Welche Aufgaben könne kryptografisch per asymmetrischen Chiffren bewältigt werden?
   f) Recherchieren Sie **kurz** welche Aufgabe der Diffie-Hellmann-Algorithmus (DH) und der Elgamal-Algorithmus haben? Wozu werden diese Verfahren für gewöhnlich genutzt? (Manschmal auch mit dem Zusatz EC für Elliptic-Curve).
   g) Recherchieren sie zunächst was unter einer Hashfunktion verstanden wird. Im Anschluss daran: Was wird unter einer kryptografischen Hashfunktion verstanden?
   h) Was ist die Aufgabe einer kryptografischen Hashfunktion?
2. 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) Recherchieren sie was im Zusammenhang mit *PKI*s unter dem Namen *Chain-Of-Trust* verstanden wird.

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

Das gesamte Semester über haben sie überwiegend lokal auf der Kommandozeile gearbeitet, also relativ nah an der eigentlich Hardware. Viele Netzwerk- und Serverkomponenten sind jedoch nicht lokal verfügbar (d.h. direkt, physisch), da diese oft in Rechenzentren unter besonderen Bedingungen ihren Dienst verrichten.[1] Die Administration der Rechner muss also auch entfernt möglich sein – remote.
Früher haben dies die sogenannten *r-Tools* ermöglicht, dies jedoch ohne kryptografische Schutzmaßnahmen. Heute übernehmen gesicherte Tools wie *ssh* mit verschiedensten Implementierungen, wie *openSSH*, diese Aufgabe.

1. Lesen Sie folgendes SSH-Tutorial: https://docs.freebsd.org/de_DE.ISO8859-1/books/handbook/openssh.html

2. Welche vier Aufgaben, d.h. Zusicherungen in Bezug auf die Sicherheit von Daten, kann *SSH* mithilfe von kryptografischen Verfahren gewährleisten? M.a.W. welche Sicherheitseigenschaften gewährleistet ihnen die Nutzung von *SSH*?

3. Notieren sie sich an welchen Orten die verschiedenen Konfigurationsdateien für Server und Client im Normalfall (default) unter einem *freeBSD* liegen. Notieren sie sich deren Zweck.

4. Recherchieren sie, was ein „Fingerprint“ im Sinne von *SSH* ist und welche Aufgabe dieser übernimmt.

5. *SSH* kommt ohne Passwörter aus, es können Public-Key-Verfahren genutzt werden. D.h. Sie können *SSH* auch ohne Zugangspasswort nutzen.[2]
   Recherchieren sie welche Verfahren *openSSH* hierfür anbietet – Stichwort Schlüsselbasierte Authentifizierung!

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

7. Welche Schlüssellänge und welche Schlüsselarten sind für Ihren Einsatz im Labor(zu Hause) sinnvoll? Ist die maximale Schlüssellänge angebracht?
   Wie hängen Schlüssellänge und Sicherheit zusammen?

8. Lassen sich die *SSH*-Schlüssel zwischen verschiedenen Clients (Windows, Linux, Solaris,...) weiterverwenden/konvertieren? Oder muss andernfalls für jeden Client ein eigener Schlüssel generiert werden?

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

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

9. Recherchieren sie die Bedeutung der Passphrase. Ist die Passphrase mit dem Nutzer-Passwort gleichzusetzen?

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

11. In manchen Fällen ist es ratsam den Zugriff via *SSH* nur auf einige Nutzer zu beschränken. Wie muss dies unter *openSSH* anhand eines Beispiels aussehen.

Aufgabe C – SSH Port-Forwarding

Mit *SSH* können Sie beliebige TCP-Verbindungen über die verschlüsselte *SSH*-Verbindung „tunneln“. [3] 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, konfigurieren muss dies jedoch der Administrator. Normale Port-Forwardings hingegen kann jeder Nutzer für sich selber nach Bedarf einrichten.
Nützliche Links:

- https://www.ssh.com/ssh/tunneling/example
- https://blog.trackets.com/2014/05/17/ssh-tunnel-local-and-remote-port-forwarding-ex
  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 „Tunneling“ im Sinne von *SSH* bedeutet.
- Recherchieren Sie was unter Port-Forwarding verstanden wird.

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

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

2. Verdeutlichen Sie sich jeweils anhand eines Beispiels wie Forwarding genutzt werden kann.
3. Finden Sie heraus, wie Port-Forwarding unter Linux und SSH funktioniert. Sie sollten schauen, was die Vorbedingungen sind, und welche Kommandos für das Forwarding notwendig sind.
   Notieren Sie sich entsprechende Kommandos, sowie deren Bedeutung!

Aufgabe D – Spoofing

Einige Protokolle stammen aus einer Zeit bzw. in einem Kontext in der Sicherheit in Rechnernetzen anders gedacht wurde. Sicherungsmaßnahmen wurden in diesen Protokollen nicht eingebaut. Im Folgenden betrachten wir verschiedene Spoofing Angriffe.

1. Recherchieren sie zunächst was unter Spoofing verstanden wird.
2. Welche Sicherheitseigenschaft wird durch das Spoofing gebrochen?
3. Im vierten Übungsblatt hatten sie bereits einen Einblick in das *ARP*-Protokoll erhalten. Rekapitulieren sie die Begriffe Cache und ARP-Cache!
4. Rekapitulieren sie was ein Man-In-The-Middle-Angriff (*MITM*) ist.
5. Als Vorbereitung auf die Durchführung eines *MITM*-Angriffs:
   a) Ist es möglich IP-Pakete zu fälschen, sodass Adressen in den Paketen enthalten sind, die nicht ihre sind? M.a.W. hat IP eine Sicherungsmaßnahme für das Spoofen von IP-Adressen?
   b) Rekapitulieren sie wie der ARP-Table befüllt wird.
6. Folgendes Szenario: Drei Rechner befinden sich in einem gemeinsamen Netzwerk. Einer der Rechner ist ein Router. Sie sind der Angreifer und wollen den Verkehr über sich selbst laufen lassen. Dazu greifen sie den übrigen Rechner an und fluten dessen ARP-Cache mit gefälschten Einträgen – sie annoncieren Ihren Rechner als Default-Gateway gegenüber den angegriffenen Rechner.
   Zunächst müssen sie die IP-Adressen des Routers und des anzugreifenden Ziels kennen.
   a) Wie können sie diese herausfinden?
   b) Welcher Mechanismus des ARP-Protokolls kann für das Spoofen genutzt werden?
7. Auch das DNS-Protokoll hatte anfänglich keine Sicherungsmaßnahmen. Recherchieren sie was unter DNS-Spoofing verstanden wird.
8. Erläutern sie wie ein DNS-Spoofing abläuft!

Aufgabe F – ICMP & TCP

Neben den Spoofing-Angriffen sind auch Denial-of-Service-Angriffe für Netzwerke ein echtes Problem. Im Folgenden betrachten wir einige DoS-Techniken.

1. Recherchieren sie zunächst was unter einem DoS verstaden wird.
2. Welche Sicherheitseigenschaft wird bei dieser Art Bedrohung gebrochen?
3. Rekapitulieren sie kurz ihr Wissen zu ICMP. Anschließend:
   a) Was wird unter dem Begriff *Ping-Flood* verstanden? Wie kann dieser im Groben umgesetzt werden?
   b) Was wird unter einem *Smurf-Attack* verstanden? Wie läuft dieser ab?
   c) Was wird unter einem *Teardrop*-Angriff verstanden?
4. Darüber hinaus ist ICMP ein nützliches Protokoll für die Aufklärung fremder Netze (Reconnaissance).
   a) Was verbirgt sich hinter dem Begriff *Ping Sweep*? Welcher Nachrichtentyp wird hier genutzt?
   b) Was verbirgt sich hinter dem Begriff *ICMP Tunneling*? Wie ist dieser Angriff möglich?
5. Rekapitulieren sie kurz ihr Wissen zu ICMP. Anschließend:
   a) Was wird unter einem *SYN-Flood*-Angriff verstanden? Welcher Mechanismus von TCP ermöglicht diesen? Wie ist eine einfache Mitigation möglich?
   b) Was wird unter einem *TCP Reset*-Angriff verstanden?
   c) Was wird unter einem *TCP Session Hijacking*-Angriff verstanden?