Voraussetzung:

Installation zweier virtueller Maschinen (A und B), die miteinander kommunizieren können sollen.
Das Betriebssystem beider Maschinen darf eine Linux-Distribution Ihrer Wahl sein.

Benötigte Anwendungen auf A:
- Apache Webserver mit PHP-Modul und erreichbarer index.php
- MariaDB
- Apache Tomcat
- PostgreDB
- FTP-Server inkl. einem Benutzer
- keine Firewall (iptables o. firewalld)
- snort (Bitte erst, wenn durch Aufgabe erforderlich)

Benötigte Anwendungen auf B:
- nmap
- wireshark
- iptraf

Abgabe

Für einen erfolgreichen Beleg geben Sie bitte die Dokumentation mit Deckblatt der Aufgaben, des Lösungsweges und der Lösung ab. Der letzte mögliche Abgabezeitpunkt ist der 18.07.2018.

Aufgaben

1. Aufgabe (Maschine B):

Starten Sie den ASCII-Sniffer iptraf in einem Shell-Fenster. Rufen Sie in einem anderen Fenster eine nicht verschlüsselte Webseite auf. Loggen Sie die Pakete im iptraf und schreiben Sie das Log in eine Datei.
Zur Lösung geben Sie einen Auszug aus dem Log des mit iptraf gesnifften Traffics ab.

2. Aufgabe (Maschine B und A):

Starten Sie Wireshark und konfigurieren Sie es zum Mitschneiden. Rufen Sie die index.php auf Maschine B auf.
Zur Lösung geben Sie ein Bildschirmfoto ab. Es sollte nur der Webseitenaufruf von A sichtbar sein.

3. Aufgabe (Maschine B und A):

Starten Sie Wireshark und konfigurieren Sie es zum Mitschneiden. Versuchen Sie eine leere Textdatei via FTP auf A zu laden.
Zur Lösung geben Sie ein Bildschirmfoto des mitgeschnittenen Passworts ab.

4. Aufgabe (Maschine B):

Starten Sie Wireshark und konfigurieren Sie es zum Mitschneiden. Rufen Sie die Webseite https://google.de auf. Zur Lösung Beschreiben Sie den Kommunikationsablauf bis zur Auslieferung der Webseite.

5. Aufgabe (Maschine B und A):

Versuchen Sie mit nmap (auf B ausgeführt) so viele Informationen wie möglich über A herauszufinden.
Zur Lösung geben Sie eine Zusammenfassung der positiven nmap-Ergebnisse an und der nmap Befehle (inkl. Paramter) an.

6. Aufgabe (Maschine A):

Installieren Sie snort. Konfigurieren Sie es so, dass es Portscanns erkennt. (Eine Vorlage zur snort.conf finden Sie im etc-Verzeichnis des Tarfiles)
Es müssen mindestens drei Stellen geändert werden:
(a) Betroffene Schnittstelle
(b) Aktivieren der Portscanner-Detektoren
(c) die Reaktion bei Ereignissen, z. B. Schreiben einer Meldung in eine Logdatei
Regeldateien für Snort können nach erfolgter Registrierung unter snort.org heruntergeladen werden. Diese Regeln werden mit „tar zxf snortrules- snapshot-2820.tar.gz“ ausgepackt.
Es werden drei Ordner angelegt: rules, preproc_rules und so_rules.
Zur Lösung geben Sie die geänderten Stellen mit den Änderungen (Endzustand) in der snort.conf an.

7. Aufgabe (Maschine A und B):

Führen Sie Aufgabe 5 erneut durch (exkl. Abgabe der Lösung). Zeichnen Sie auf Maschine A mindestens einen Scann mit snort (Sniffer-Modus) auf (Datei).
Zur Lösung geben Sie einen sinnvollen Auszug aus der Datei des mitgeschnittenen Scann ab.

8. Aufgabe:

Geben Sie an mit welchen Mitteln Sie Ihren privaten (realen oder fiktiven) Rechner/Client schützen. Erläutern welche Angriffsmöglichkeiten damit abgewehrt werden können und welche nicht abgedeckt sind.
Zur Lösung geben Sie die Darstellung des Zustands und die Erläuterung (min. 200 Worte) ab.

9. Aufgabe:

Nennen und erläutern Sie (in Sätzen) je 4 Vor- und Nachteile einer Bring-Your-Own-Device Strategie in einem Unternehmen.

10. Aufgabe:

Erläutern Sie das Kerckhoffs’sche Prinzip und warum es in der Kryptografie sinnvoll angewandt werden kann.

11. Aufgabe:

Nennen Sie zwei mögliche Probleme und deren Auswirkungen, wenn ein Kryptografie-Algorithmus im Black-Box-Verfahren angewandt wird. (Black Box = Algorithmus ist nicht bekannt)

12. Aufgabe:

Nutzen Sie die Viginère Chiffre und das Schlüsselwort „buchsbaeumebrauchenauchwasser“, um den folgenden Text zu verschlüsseln. Leerzeichen werden subtrahiert

erst wenn der zu verschluesselnde text kuerzer oder genauso lang ist wie das verwendete schluesselwort ist das verfahren unknackbar

Als Lösung geben Sie die verschlüsselten Zeichen in Gruppen zu je 5 Zeichen ab.