Hochschule RheinMain, Prof. Dr. Martin Gergeleit

Rechnernetze & Telekommunikation
SoSe 2020
LV 2142

Übungsblatt 3

Bearbeiten Sie diese Aufgaben bitte **vor** Beginn Ihrer Praktikumsgruppe und halten Sie Ihre Ergebnisse **schriftlich** in einem Protokoll Ihrer Versuche fest. Die nötigen Informationen erhalten Sie aus der Vorlesung (https://video.cs.hs-rm.de/course/5/lecture/56/ , Rechnernetze und Telekommunikation > 3. TCP/IP - Grundlagen Teil 2), den man-Pages und natürlich im Internet.

Zu Beginn werden Einzelne vom Praktikumsleiter stichprobenartig gebeten elektronisch abzugeben. Die Bearbeitung der Fragen bildet mit eine Grundlage der Bewertung.

Die Fragen werden anschließend in der Praktikumsgruppe interaktiv besprochen und vorgeführt.

Aufgabe 3.1 (netstat):

Informieren Sie sich, was das Kommandozeilen-Werkzeug „netstat“ leistet.

a) Wieso kann es bei der Erkennung von Malware hilfreich sein?

b) Beobachten Sie mit „netstat -t“ welche TCP-Verbindungen Ihr Rechner geöffnet hat.

c) Loggen Sie sich auf dem login1.cs.hs-rm.de mit `ssh` (`putty`) ein. Was ändert sich jeweils bei der Ausgabe von „netstat -t“? Erkennen Sie, welche lokale TCP-Portnummer Ihre ssh-Verbindung hat?

d) Beenden Sie die ssh-Verbindung wieder und rufen Sie gleich danach nochmal „netstat -t“ auf. Was ist mit der ssh-Verbindung aus c) passiert?

Aufgabe 3.2 (wireshark):

Installieren Sie das Programm „Wireshark“ von https://www.wireshark.org/#download (wenn Sie gefragt werden inkl. der libpcap/winpcap, das ist die Bibliothek um Live-Mitschnitte des Netzwerkverkehrs machen zu können).

a) Was kann man mit dem Wireshark machen? Wieso ist Wireshark ein Programm, das sicherheitskritisch ist und für die volle Funktionalität Administratorenrechte erfordert?

e) Was sind Filter unter Wireshark? Geben Sie ein Beispiel an!

f) Im Praktikums -Verzeichnis des finden Sie einen Netzwerk-Mitschnitt (sog. „Trace“) als Trace1.pcap. Laden Sie diesen Trace mit dem Wireshark. Betrachten Sie das Paket 24 und expandieren Sie den IP-Header. Erklären Sie alle Felder des Headers (Welche Werte sehen Sie und was bedeuten diese?).

g) Betrachten Sie die ganze Folge von Paketen und beantworten Sie folgende Fragen:

   i. Welche IP-Adressen sind beteiligt?

   ii. Welche Protokolle werden genutzt?

iii. Was bedeuten die schwarz eingefärbten Pakete im Wireshark?

iv. Welches Kommando wurde auf welchem Rechner ausgeführt?

v. Erklären Sie die Funktion jedes einzelnen Paketes.

Aufgabe 3.3 (TCP):

Sie können weitere Informationen neber der Vorlesung auch dem im StudIP hochgeladenen Buchausschnitt „TCP.pdf“ entnehmen.

a) Im StudIP-Verzeichnis des Praktikums finden Sie einen weiteren Netzwerk-Mitschnitt als Trace2.pcap. Laden Sie diesen Trace mit dem Wireshark. Betrachten Sie die Paketfolge und beantworten Sie folgende Fragen:

   i. Wie viele TCP-Verbindungen beobachten Sie hier insgesamt?

   ii. Was wurde in diesen TCP-Verbindungen gemacht?

   iii. Können Sie die Inhalte der Pakete lesen?

b) Analysieren Sie die Pakete ab Paket 9 weiter und beantworten Sie folgende Fragen:

   i. Informieren Sie sich über den „Three-Way-Handshake“ beim Start einer TCP-Verbindung. Was ist die Funktion der drei Pakete? Zeigen Sie die Pakete eines Three-Way-Handshakes.

   ii. Wie lauten die dort vereinbarten Sequenz- und Acknowledgement-nummern?

   iii. Wie viele TCP-Segmente werden von 195.72.102.137 übertragen? Wie groß sind diese Segmente? Verfolgen Sie Sequenznummern dieser Segmente.

   iv. Wie viele Bytes werden von 192.168.178.22 in die andere Richtung übertragen?

   v. Beobachten Sie die von 192.168.178.22 bestätigte Window-Size. Was erkennen Sie?