Lsg Vorschlag RuT Ü03 Maximilian Maag

Aufgabe 3.1

a)

Netstat ist in der Lage TCP Verbindungen zu erkennen. Malware sendet Daten von einem PC an einen Angreifer. Eine unerwünschte TCP-Verbindung könnte ein Hinweis auf Maleware sein.

b)

Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 127 Desktop:47986 rs003862.fastroot:https VERBUNDEN
tcp 0 0 Desktop:48654 vps2021339.fastwe:https TIME WAIT
tcp 0 0 Desktop:52588 fra24s02-in-f10.1:https TIME WAIT
tcp 0 0 Desktop:54158 149.154.167.99:https TIME WAIT
tcp 0 0 Desktop:55298 rs003862.fastrootse:ssh VERBUNDEN
tcp 0 0 Desktop:41004 133.247.244.35.bc:https TIME WAIT
tcp 0 0 Desktop:48426 vps2021339.fastwe:https VERBUNDEN
tcp 0 0 Desktop:51548 ec2-34-211-222-43:https VERBUNDEN
tcp 0 0 Desktop:45854 fra16s50-in-f3.1e:https TIME WAIT

c)

Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 Desktop:54970 scooter.cs.hs-rm.de:ssh VERBUNDEN

Gegenüber der Ausgabe aus b ist obige Verbindung hinzugekommen, daher gehe ich davon aus das die die SSH-Verbindung zum Server der Hochschule darstellt.

d)

Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 Desktop:54970 scooter.cs.hs-rm.de:ssh TIME WAIT

Die Verbindung ist nicht mehr aktiv und wird dem Status Time Wait belegt. Der Port ist aber weiterhin reserviert falls die Verbindung erneut genutzt wird.

Aufgabe 3.2

a)

Wireshark ist ein Programm, dass in der Lage ist Netzwerktraffic mitzuschneiden. Es unterstützt alle gängigen und relevanten Netzwerkprotokolle und kann bei missbräuchlichem Umgang verwendet werden um Personen abzuhören.

b)

Filter strukturieren die Ausgabe von Wireshark. Sie Können verwendet werden um nach bestimmten Dingen zu Suchen.
Zum Beispiel könnte man nach dem FTP Protokoll filtern und sich alle Pakete anzeigen lassen, welche dieses Protokoll verwendet haben.

c)

Ein IP Header enthält in der Regel:
Quellport/Adresse: Beschreibt den Ursprung des Pakets.
Zielport/Adresse: Ziel des Pakets.
Sequenznummer: nummeriert Daten in Senderichtung
Ack-Flag: Dient der Bestätigung der Empfangsdaten
Checksum: Fehlerprüfsumme
Window: Fenstergröße für Flutkontrolle

$Frame 24 : 106 bytes on wire (848 bits), 106 bytes captured (848 bits)$
$Encapsulation type : Ethernet (1)$
$Arrival Time : Oct 28, 201310 : 46 : 05.783172000 CET [Time shift for this packet :$
$0.000000000 seconds$
$] Epoch Time : 1382953565.783172000 seconds$
$1 [Time delta from previous captured frame : 0.001849000 seconds]$
$1 [Time delta from previous displayed frame : 0.001849000 seconds]$
$1 [Time since reference or first frame : 7.712425000 seconds]$
$Frame Number : 24$
$Frame Length : 106 bytes (848 bits)$
$Capture Length : 106 bytes (848 bits)$
$1 [Frame is marked : False]$
$1 [Frame is ignored : False]$
$1 [Protocols in frame : eth : ethertype : ip : icmp : data]$
$1 [Coloring Rule Name : ICMP]$
$1 [Coloring Rule String : icmp || icmpv6]$
$Ethernet II, Src : Juniper N1d : 7c : 06$
$(00 : 1f : 12 : 1d : 7c : 06), Dst : Hon Hai Pr 28 : 47 : e6$
$(00 : 23 : 4e : 28 : 47 : e6)$
$Destination : Hon Hai Pr 28 : 47 : e6 (00 : 23 : 4e : 28 : 47 : e6)$
$Source : Juniper N_1 d : 7c : 06 (00 : 1f : 12 : 1d : 7c : 06) Type : IPv4 (0x0800)$
$Internet Protocol Version 4, Src :$
$195.72.102.137, Dst : 10.156.7.72$
$0100.... = Version : 4$
$....0101 = Header Length : 20 bytes (5)$
$Differentiated Services Field : 0x00 (DSCP : CS0, ECN : Not - ECT)$
$000000.. = Differentiated Services Codepoint : Default (0)$
$.....00 = Explicit Congestion Notification :$

$NotECN - CapableTransport(0)$
$TotalLength : 92 Identification : 0x4d1e(19742)$
$Flags : 0x00000..... = Reservedbit : Notset$
$.0..... = Don't fragment : Notset$
$..0..... = More fragments : Notset$
$Fragment offset : 0$
$Time to live : 61$
$Protocol : ICMP(1)$
$Header checksum : 0xf4cd[validation disabled]$
$1[Header checksum status : Unverified]$
$Source$: 195.72.102.137
$Destination$: 10.156.7.72
$Internet Control Message Protocol$

d)

I: beteiligt an der Kommunikation waren: 10.156.7.72 und 195.72.102.137
II: ICMP, IP
III: Die schwarzen Pakete sind verworfene Pakte deren Time-To-Live abgelaufen ist.
IV: stätige Steigerung der Time To Live steht für Traceroute
V: Zusammenfassung über Time-To-Live.

Aufgabe 3.3

a)

I: an Syn in Fin Paket 2 mal = Zwei Verbindungen
II: Die Website der Hochschule wurde aufgerufen.
III: Der Inhalt der Paket ist deutlich Sichtbar. Der übertragene HTMLcode ist vollständig einsehbar

b)

I: Quelle Wikipedia
Der Client, der eine Verbindung aufbauen will, sendet dem Server ein SYN-Paket (von englisch synchronize) mit einer Sequenznummer x. Die Sequenznummern sind dabei für die Sicherstellung einer vollständigen Übertragung in der richtigen Reihenfolge und ohne Duplikate wichtig. Es handelt sich also um ein Paket, dessen SYN-Bit im Paketkopf gesetzt ist (siehe TCP-Header). Die Start-Sequenznummer ist eine beliebige Zahl, deren Generierung von der jeweiligen TCP-Implementierung abhängig ist. Sie sollte jedoch möglichst zufällig sein, um Sicherheitsrisiken zu vermeiden.
Ist der Port geöffnet, bestätigt er den Erhalt des ersten SYN-Pakets und stimmt

dem Verbindungsaufbau zu, indem er ein SYN/ACK-Paket zurückschickt. Zusätzlich sendet er im Gegenzug seine Start-Sequenznummer y, die ebenfalls beliebig und unabhängig von der Start-Sequenznummer des Clients ist.
Der Client bestätigt zuletzt den Erhalt des SYN/ACK-Pakets durch das Senden eines eigenen ACK-Pakets mit der Sequenznummer x+1. . II:
III:
IV:
V: