Fragen zur Theorie - Protokollanalyse

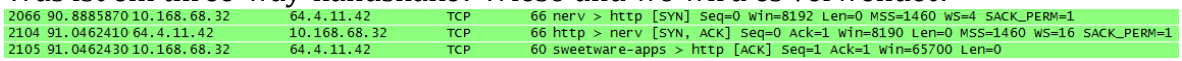
3.5 Kontrollfragen

1. Was ist der Unterschied zwischen Capture und Display Filter?
   Capture -Filter: Es wird nur protokoliert was den Capture Filter entspricht.
   Display-Filter: Es wird alles protokoliert (sofern kein capture filter definiert) und dann nur dasjenige angezeigt, welches dem Display-Filter entspricht.

2. Was für ein Capture Filter muss man verwenden, um nur den TCP und UDP Verkehr von Host 192.168.1.15 zu betrachten? Wie würde man es mittels Display Filter erreichen?
   Capture-Filter: host 192.168.1.15
   Display-Filter: ip.addr == 192.168.1.15

4.2 Kontrollfragen

1. Was ist ein three-way-handshake? Wieso und wo wird es verwendet?



   SYN → SYN-ACK → ACK
   Bei TCP für den Verbindungsaufbau.

2. Welche Flags kennt der TCP header?
   CWR: Congestion Window Reduced
   ECN-Echo
   Urgent
   Acknowledgment
   Push
   Reset
   Syn
   Fin

5.2 Kontrollfragen

1. Welche sind die wichtigsten ICMP-Nachrichtentypen?
   Echo request
   Echo replay
   Destination Unreachable
   Time exceeded

2. Was ist TTL? Wie wird es eingesetzt?
   Time-To-Live, wie lange in Packet noch „gültig“ ist.

3. Was erzwingt tracert -6 ?
   Force using IPv6.
   IPv6 wird verwendet.

4. Was erzielt man mit ping –t ?
   Ping the specified host until stopped.
   “Endlos” Ping

6.2 Kontrollfragen

1. Was ist ein „forward lookup“? Was ein „reverse lookup“?
   DNS forward lookup: Auflösung von DNS-Name nach einer IP Adresse
   DNS reverse lookup: Auflösung von IP-Adresse nach DNS-Hostname

2. Welchen Zweck erfüllt das Programm nslookup?
   DNS Abfragen ausführen (DNS Client)

7.2 Kontrollfragen

1. Wer von den Clients besitzt einen ARP-Cache?
   Alle

2. Wie lautet die Broadcast MAC Adresse?
   FF:FF:FF:FF:FF:FF

8.2 Kontrollfragen

INFORMATION	RIP	EIGRP	OSPF
PERIODICAL SEND-INTERVAL	Ca. 30sec	Ca. 5sec	Ca. 10sec
FRAME LENGTH RANGE	106bytes	60-180bytes	78-166bytes
PAKETS	Request, Response	Update, Hello, Hello (Ack)	Hello, DB Description, LS Request, LS Update
IP PROTOCOL	UDP	EIGRP	OSPF IGP
DESTINATION PORT	520	88	89

ROUTER PROTOCOL PAKET

IP ADDRESSES	192.168.2.0 192.168.3.0 192.168.4.0	Unknown (Cisco proprietäres Protokoll) In Wireshark v1.6.5 nicht unterstützt aber in HexCode ersichtlich	192.168.1.1 192.168.1.2
PROTOCOL SPECIFIC INFORMATION	Version: RIPv1 IP Address: 192.168.2.0 Metric: 1 Address Familiy: IP (2)	Version: 2 Opcode: Hello/Ack, Update Autonomous System: 1 EIGRP Parameters : (werden für die Metric benötigt) Software Version: IOS=6.0, EIGRP=3.0 Route Information: Unknown	Version: 2 Source OSFP Router: 192.168.4.1 Area ID: 0.0.0.1 Link-State Advertisement & ID Advertising Router Number of Links: 4 Attached Router: (ID)

1. Welches der analysierten Routing Protokolle generiert mehr Traffic?
   EIGRP

2. Welches würden Sie einsetzen und weshalb?
   Je nach Anforderung. Bandbreite, Änderungen, Konvergenz-Zeit, etc.

9.3 Kontrollfragen

1. Ports können „open“, „closed“ oder auch „filtered“ sein? Wie kann der Scanner das beurteilen?
   Open: *SYN / SYN-ACK*
   Closed: *SYN / RST (Es wird ein Reset geschickt)*
   Filtered: *SYN / [nichts], Es gibt kein Antwort-Packet und auch kein RST*

2. Bei einem Connect-Scan wie antwortet der Ziel Host?
   SYN-ACK resp. RST

3. Ist es möglich anstatt einem Host das ganze Subnetz zu scannen? Falls ja, wie?
   nmap -sP 172.16.201.0/24

10.3 Kontrollfragen

1. Wieso muss der Angreifer-Host regelmässig Gratuitous ARP Replys senden?
   Damit er weiterhin „Man-in-the-middle“ bleibt.

2. Wie könnte man die Verbindung sichern, sodass sie vor einem Man-in-the-middle Angriff geschützt ist?
   End-2-End Verschlüsselung