Free Questions for 200-201 by ebraindumps

Shared by Mcintosh on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit. Where is the executable file?

Options:

A- info

B- tags

C- MIME

D- name

Answer:

C

Question 2

Question Type: MultipleChoice

Which are two denial-of-service attacks? (Choose two.)

Options:

A- TCP connections

B- ping of death

C- man-in-the-middle

D- code-red

E- UDP flooding

Answer:

B, E

Question 3

Question Type: **MultipleChoice**

What describes a buffer overflow attack?

Options:

A- injecting new commands into existing buffers

B- fetching data from memory buffer registers

C- overloading a predefined amount of memory

D- suppressing the buffers in a process

Answer:

C

Question 4

Question Type: **MultipleChoice**

What is a description of a social engineering attack?

Options:

A- fake offer for free music download to trick the user into providing sensitive data

B- package deliberately sent to the wrong receiver to advertise a new product

C- mistakenly received valuable order destined for another person and hidden on purpose

D- email offering last-minute deals on various vacations around the world with a due date and a counter

Answer:

D

Question 5

Question Type: MultipleChoice

Which tool gives the ability to see session data in real time?

Options:

A- tcpdstat

B- trafdump

C- tcptrace

D- trafshow

Answer:

C

Question 6

Question Type: MultipleChoice

What should an engineer use to aid the trusted exchange of public keys between user tom0411976943 and dan1968754032?

Options:

A- central key management server

B- web of trust

C- trusted certificate authorities

D- registration authority data

Answer:

C

Question 7

Question Type: MultipleChoice

A user received a targeted spear-phishing email and identified it as suspicious before opening the content. To which category of the Cyber Kill Chain model does to this type of event belong?

Options:

A- weaponization

B- delivery

C- exploitation

D- reconnaissance

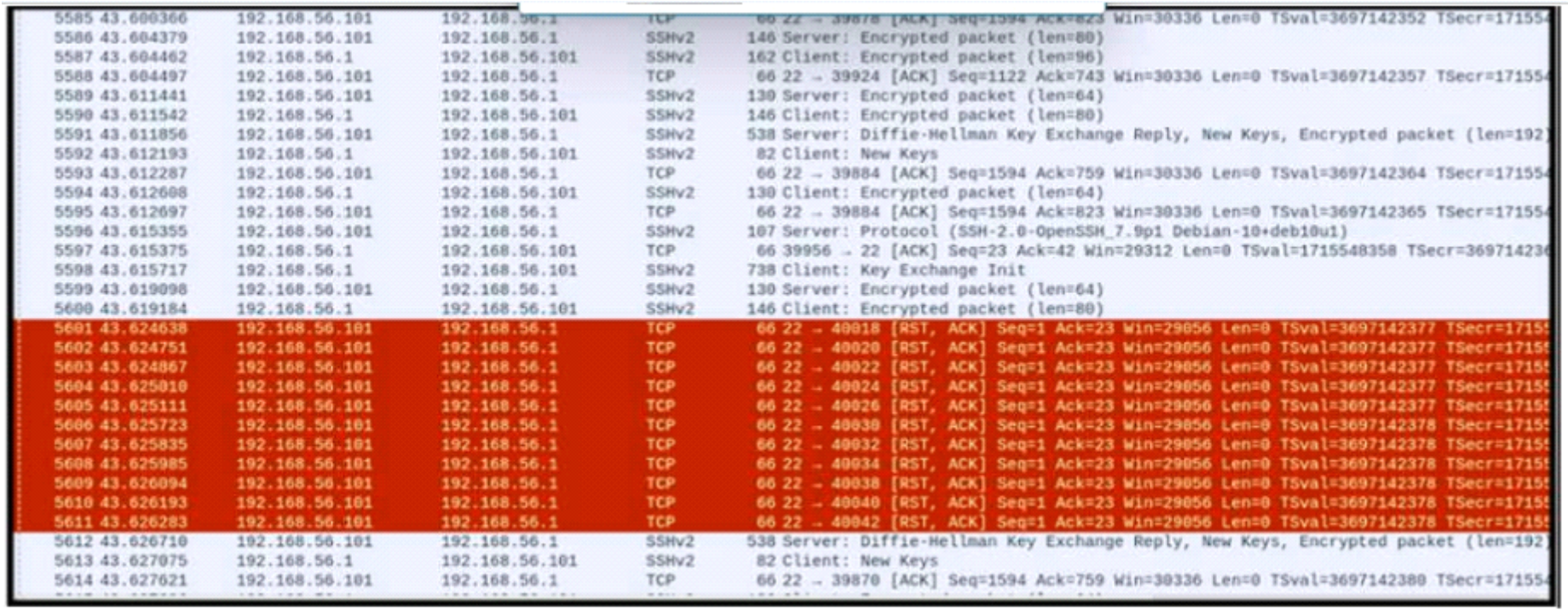
Answer:

B

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



5585 43.600366	192.168.56.101	192.168.56.1	TCP	66 22 → 39878 [ACK] Seq=1594 Ack=823 Win=30336 Len=0 TSval=3697142352 TSecr=17155
5586 43.604379	192.168.56.101	192.168.56.1	SSHv2	146 Server: Encrypted packet (len=80)
5587 43.604462	192.168.56.1	192.168.56.101	SSHv2	162 Client: Encrypted packet (len=96)
5588 43.604497	192.168.56.101	192.168.56.1	TCP	66 22 → 39924 [ACK] Seq=1122 Ack=743 Win=30336 Len=0 TSval=3697142357 TSecr=17155
5589 43.611441	192.168.56.101	192.168.56.1	SSHv2	130 Server: Encrypted packet (len=64)
5590 43.611542	192.168.56.1	192.168.56.101	SSHv2	146 Client: Encrypted packet (len=80)
5591 43.611856	192.168.56.101	192.168.56.1	SSHv2	538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192
5592 43.612193	192.168.56.1	192.168.56.101	SSHv2	82 Client: New Keys
5593 43.612287	192.168.56.101	192.168.56.1	TCP	66 22 → 39884 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142364 TSecr=17155
5594 43.612608	192.168.56.1	192.168.56.101	SSHv2	130 Client: Encrypted packet (len=64)
5595 43.612697	192.168.56.101	192.168.56.1	TCP	66 22 → 39884 [ACK] Seq=1594 Ack=823 Win=30336 Len=0 TSval=3697142365 TSecr=17155
5596 43.615355	192.168.56.101	192.168.56.1	SSHv2	107 Server: Protocol (SSH-2.0-OpenSSH_7.9p1 Debian-10+deb10u1)
5597 43.615375	192.168.56.1	192.168.56.101	TCP	66 39956 → 22 [ACK] Seq=23 Ack=42 Win=29312 Len=0 TSval=1715548358 TSecr=369714236
5598 43.615717	192.168.56.1	192.168.56.101	SSHv2	738 Client: Key Exchange Init
5599 43.619098	192.168.56.101	192.168.56.1	SSHv2	130 Server: Encrypted packet (len=64)
5600 43.619184	192.168.56.1	192.168.56.101	SSHv2	146 Client: Encrypted packet (len=80)
5601 43.624638	192.168.56.101	192.168.56.1	TCP	66 22 → 40018 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5602 43.624751	192.168.56.101	192.168.56.1	TCP	66 22 → 40020 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5603 43.624867	192.168.56.101	192.168.56.1	TCP	66 22 → 40022 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5604 43.625010	192.168.56.101	192.168.56.1	TCP	66 22 → 40024 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5605 43.625111	192.168.56.101	192.168.56.1	TCP	66 22 → 40026 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142377 TSecr=1715
5606 43.625723	192.168.56.101	192.168.56.1	TCP	66 22 → 40030 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5607 43.625835	192.168.56.101	192.168.56.1	TCP	66 22 → 40032 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5608 43.625985	192.168.56.101	192.168.56.1	TCP	66 22 → 40034 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5609 43.626094	192.168.56.101	192.168.56.1	TCP	66 22 → 40038 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5610 43.626193	192.168.56.101	192.168.56.1	TCP	66 22 → 40040 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5611 43.626283	192.168.56.101	192.168.56.1	TCP	66 22 → 40042 [RST, ACK] Seq=1 Ack=23 Win=29056 Len=0 TSval=3697142378 TSecr=1715
5612 43.626710	192.168.56.101	192.168.56.1	SSHv2	538 Server: Diffie-Hellman Key Exchange Reply, New Keys, Encrypted packet (len=192
5613 43.627075	192.168.56.1	192.168.56.101	SSHv2	82 Client: New Keys
5614 43.627621	192.168.56.101	192.168.56.1	TCP	66 22 → 39870 [ACK] Seq=1594 Ack=759 Win=30336 Len=0 TSval=3697142380 TSecr=17155

An engineer is analyzing a PCAP file after a recent breach An engineer identified that the attacker used an aggressive ARP scan to scan the hosts and found web and SSH servers. Further analysis showed several SSH Server Banner and Key Exchange Initiations. The engineer cannot see the exact data being transmitted over an encrypted channel and cannot identify how the attacker gained access How did the attacker gain access?

Options:

A- by using the buffer overflow in the URL catcher feature for SSH

B- by using an SSH Tectia Server vulnerability to enable host-based authentication

C- by using an SSH vulnerability to silently redirect connections to the local host

D- by using brute force on the SSH service to gain access

Answer:

C

Question 9

Question Type: MultipleChoice

What is the difference between the ACK flag and the RST flag?

Options:

A- The RST flag approves the connection, and the ACK flag terminates spontaneous connections.

B- The ACK flag confirms the received segment, and the RST flag terminates the connection.

C- The RST flag approves the connection, and the ACK flag indicates that a packet needs to be resent

D- The ACK flag marks the connection as reliable, and the RST flag indicates the failure within TCP Handshake

Answer:

B