QUESTION 16
Drag and Drop Question
Refer to the exhibit. Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.

source address	10.0.2.15
destination address	50588
source port	443
destination port	192.124.249.9
Network Protocol	Transmission Control Protocol
Transport Protocol	Internet Protocol v4
Application Protocol	Transport Layer Security v1.2

Answer:

	source address
	source port
	destination port
	destination address
	Transport Protocol
	Network Protocol
	Application Protocol

QUESTION 17
Drag and Drop Question
Drag and drop the access control models from the left onto the correct descriptions on the right.

MAC	object owner determines permissions
ABAC	OS determines permissions
RBAC	role of the subject determines permissions
DAC	attributes of the subject determines permissions

Answer:

DAC
MAC
RBAC
ABAC

QUESTION 18
Drag and Drop Question
Drag and drop the technology on the left onto the data type the technology provides on the right.

tcpdump	session data
web content filtering	full packet capture
traditional stateful firewall	transaction data
NetFlow	connection event

Answer:

web content filtering
tcpdump
NetFlow
traditional stateful firewall

QUESTION 19
Which tool is commonly used by threat actors on a webpage to take advantage of the softwarevulnerabilitiesof a system to spread malware?

A. exploit kit
B. root kit
C. vulnerability kit
D. script kiddie kit

Answer: A

QUESTION 20
Which two methods might be used by an analyst to detect SSL/TLS encrypted command-and-control communication? (Choose two.)

A. perform decryption and inspection of SSL/TLS traffic
B. perform firewall HTTP application inspection to detect for the command and control traffic
C. perform IPS HTTP deep packets inspection to detect for the command and control traffic

D. perform analysis of the NetFlow data to detect anomalous TLS/SSL flows

Answer: AD

QUESTION 21
While viewing packet capture data, an analyst sees that one IP is sending and receiving traffic for multiple devices by modifying the IP header.
Which technology makes this behavior possible?

A. encapsulation
B. TOR
C. tunneling
D. NAT

Answer: D

QUESTION 22
When communicating via TLS, the client initiates the handshake to the server and the server responds back with its certificate for identification.
Which information is available on the server certificate?

A. server name, trusted subordinate CA, and private key
B. trusted subordinate CA, public key, and cipher suites
C. trusted CA name, cipher suites, and private key
D. server name, trusted CA, and public key

Answer: D

QUESTION 23
A security engineer has a video of a suspect entering a data center that was captured on the same day that files in the same data center were transferred to a competitor.
Which type of evidence is this?

A. best evidence
B. prima facie evidence
C. indirect evidence
D. physical evidence

Answer: C

QUESTION 24
Which two elements of the incident response process are stated in NIST Special Publication 800-61 r2? (Choose two.)

A. detection and analysis
B. post-incident activity
C. vulnerability management
D. risk assessment
E. vulnerability scoring

Answer: AB

QUESTION 25
Which utility blocks a host portscan?

A. HIDS

B. sandboxing
C. host-based firewall
D. antimalware

Answer: C

QUESTION 26
Which event is user interaction?

A. gaining root access
B. executing remote code
C. reading and writing file permission
D. opening a malicious file

Answer: D

QUESTION 27
An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?

A. social engineering
B. eavesdropping
C. piggybacking
D. tailgating

Answer: A

QUESTION 28
Refer to the exhibit. What information is depicted?

Top 10 Src IP Addr ordered by flows:									
Date first seen	Duration	Src IP Addr	Flows	Packets	Bytes	pps	bps	bpp
2019-11-30 06:45:50.990	1147.332	192.168.12.234	109183	202523	13.1 M	176	96116	68
2019-11-30 06:45:02.928	1192.834	10.10.151.203	62794	219715	25.9 M	184	182294	123
2019-11-30 06:59:24.563	330.110	192.168.28.173	27864	47943	2.2 M	145	55769	48

A. IIS data
B. NetFlow data
C. network discovery event
D. IPS event data

Answer: B

QUESTION 29
Which type of evidence supports a theory or an assumption that results from initial evidence?

A. probabilistic
B. indirect
C. best
D. corroborative

Answer: D