QUESTION 130
At a company party a guest asks questions about the company's user account format and password complexity. How is this type of conversation classified?

A. Phishing attack
B. Password Revelation Strategy
C. Piggybacking
D. Social Engineering

Correct Answer: D

QUESTION 131
How does certificate authority impact a security system?

A. It authenticates client identity when requesting SSL certificate
B. It validates domain identity of a SSL certificate
C. It authenticates domain identity when requesting SSL certificate
D. It validates client identity when communicating with the server

Correct Answer: B

QUESTION 132
An offline audit log contains the source IP address of a session suspected to have exploited a vulnerability resulting in system compromise. Which kind of evidence is this IP address?

A. best evidence
B. corroborative evidence
C. indirect evidence
D. forensic evidence

Correct Answer: B

QUESTION 133
An engineer received a flood of phishing emails from HR with the source address HRjacobm@companycom. What is the threat actor in this scenario?

A. phishing email
B. sender
C. HR
D. receiver

Correct Answer: B

QUESTION 134
What are two denial-of-service (DoS) attacks? (Choose two)

A. port scan
B. SYN flood
C. man-in-the-middle
D. phishing

E. teardrop

Correct Answer: BC

QUESTION 135
An engineer received an alert affecting the degraded performance of a critical server. Analysis showed a heavy CPU and memory load. What is the next step the engineer should take to investigate this resource usage?

A. Run "ps -d" to decrease the priority state of high load processes to avoid resource exhaustion.
B. Run "ps -u" to find out who executed additional processes that caused a high load on a server.
C. Run "ps -ef" to understand which processes are taking a high amount of resources.
D. Run "ps -m" to capture the existing state of daemons and map required processes to find the gap.

Correct Answer: C

QUESTION 136
What is the difference between vulnerability and risk?

A. A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.
B. A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself
C. A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.
D. A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit

Correct Answer: C

QUESTION 137
What is a difference between signature-based and behavior-based detection?

A. Signature-based identifies behaviors that may be linked to attacks, while behavior-based has a predefined set of rules to match before an alert.
B. Behavior-based identifies behaviors that may be linked to attacks, while signature-based has a predefined set of rules to match before an alert.
C. Behavior-based uses a known vulnerability database, while signature-based intelligently summarizes existing data.
D. Signature-based uses a known vulnerability database, while behavior-based intelligently summarizes existing data.

Correct Answer: B

QUESTION 138
A company is using several network applications that require high availability and responsiveness, such that milliseconds of latency on network traffic is not acceptable. An engineer needs to analyze the network and identify ways to improve traffic movement to minimize delays. Which information must the engineer obtain for this analysis?

A. total throughput on the interface of the router and NetFlow records
B. output of routing protocol authentication failures and ports used
C. running processes on the applications and their total network usage

D. deep packet captures of each application flow and duration

Correct Answer: C

QUESTION 139
Which security monitoring data type requires the largest storage space?

A. transaction data
B. statistical data
C. session data
D. full packet capture

Correct Answer: D

QUESTION 140
What is the difference between inline traffic interrogation (TAPS) and traffic mirroring (SPAN)?

A. TAPS interrogation is more complex because traffic mirroring applies additional tags to data and SPAN does not alter integrity and provides full duplex network.
B. SPAN results in more efficient traffic analysis, and TAPS is considerably slower due to latency caused by mirroring.
C. TAPS replicates the traffic to preserve integrity, and SPAN modifies packets before sending them to other analysis tools
D. SPAN ports filter out physical layer errors, making some types of analyses more difficult, and TAPS receives all packets, including physical errors.

Correct Answer: D

QUESTION 141
What is the virtual address space for a Windows process?

A. physical location of an object in memory
B. set of pages that reside in the physical memory
C. system-level memory protection feature built into the operating system
D. set of virtual memory addresses that can be used

Correct Answer: D

QUESTION 142
Which filter allows an engineer to filter traffic in Wireshark to further analyze the PCAP file by only showing the traffic for LAN 10.11.x.x, between workstations and servers without the Internet?

A. src=10.11.0.0/16 and dst=10.11.0.0/16
B. ip.src==10.11.0.0/16 and ip.dst==10.11.0.0/16
C. ip.src=10.11.0.0/16 and ip.dst=10.11.0.0/16
D. src==10.11.0.0/16 and dst==10.11.0.0/16

Correct Answer: B

QUESTION 143
When trying to evade IDS/IPS devices, which mechanism allows the user to make the data incomprehensible without a specific key, certificate, or password?

A. fragmentation
B. pivoting
C. encryption
D. stenography

Correct Answer: C

QUESTION 144
Which evasion technique is indicated when an intrusion detection system begins receiving an abnormally high volume of scanning from numerous sources?

A. resource exhaustion
B. tunneling
C. traffic fragmentation
D. timing attack

Correct Answer: A

QUESTION 145
Which two elements are used for profiling a network? (Choose two.)

A. session duration
B. total throughput
C. running processes
D. listening ports
E. OS fingerprint

Correct Answer: AB

QUESTION 146
An employee reports that someone has logged into their system and made unapproved changes, files are out of order, and several documents have been placed in the recycle bin. The security specialist reviewed the system logs, found nothing suspicious, and was not able to determine what occurred. The software is up to date; there are no alerts from antivirus and no failed login attempts. What is causing the lack of data visibility needed to detect the attack?

A. The threat actor used a dictionary-based password attack to obtain credentials.
B. The threat actor gained access to the system by known credentials.
C. The threat actor used the teardrop technique to confuse and crash login services.
D. The threat actor used an unknown vulnerability of the operating system that went undetected.

Correct Answer: C

QUESTION 147
Which of these describes SOC metrics in relation to security incidents?

A. time it takes to detect the incident
B. time it takes to assess the risks of the incident
C. probability of outage caused by the incident
D. probability of compromise and impact caused by the incident

Correct Answer: A

QUESTION 148
An automotive company provides new types of engines and special brakes for rally sports cars. The company has a database of inventions and patents for their engines and technical information Customers can access the database through the company's website after they register and identify themselves. Which type of protected data is accessed by customers?

A. IP data
B. PII data
C. PSI data
D. PHI data

Correct Answer: B

QUESTION 149
What is an advantage of symmetric over asymmetric encryption?

A. A key is generated on demand according to data type.
B. A one-time encryption key is generated for data transmission
C. It is suited for transmitting large amounts of data.
D. It is a faster encryption mechanism for sessions

Correct Answer: C

QUESTION 150
What is a difference between data obtained from Tap and SPAN ports?

A. Tap mirrors existing traffic from specified ports, while SPAN presents more structured data for deeper analysis.
B. SPAN passively splits traffic between a network device and the network without altering it, while Tap alters response times.
C. SPAN improves the detection of media errors, while Tap provides direct access to traffic with lowered data visibility.
D. Tap sends traffic from physical layers to the monitoring device, while SPAN provides a copy of network traffic from switch to destination

Correct Answer: D

QUESTION 151
What should a security analyst consider when comparing inline traffic interrogation with traffic tapping to determine which approach to use in the network?

A. Tapping interrogation replicates signals to a separate port for analyzing traffic
B. Tapping interrogations detect and block malicious traffic
C. Inline interrogation enables viewing a copy of traffic to ensure traffic is in compliance with security