**Question 1**

**0 / 1.5 pts**

Jared is responsible for network security at his company. He has discovered behavior on one computer that certainly appears to be a virus. He has even identified a file he thinks might be the virus. However, using three separate antivirus programs, he finds that none can detect the file. Which of the following is most likely to be occurring?

The computer has a RAT.

The computer has a worm.

**You Answered**

The computer has a rootkit.

**Correct Answer**

The computer has a zero-day exploit.

**Question 2**

**1.5 / 1.5 pts**

What threat vector is most impacted by how Windows handles autorun.inf files?

**Correct!**

Removable devices

Unsecure Wi-Fi

Watering hole attacks

Open service ports

**Question 3**

**1.5 / 1.5 pts**

Ashley's organization has recently come under attack and has suffered a DNS outage. As she investigated, she found that requests to her DNS servers were sent to open DNS resolvers using spoofed IP addresses with requests that would result in very large responses from the DNS resolvers to the IP addresses that appeared to be making the request. What type of attack targeted Ashley's organization?

A mirrored DDoS

**Correct!**

A reflected DDoS

A DNS flood

A supersized query attack

**Question 4**

**1.5 / 1.5 pts**

Olivia has deployed Microsoft's Intune for her environment. What capability has she gained for her devices?

Code versioning

**Correct!**

Configuration enforcement

Malware detection and response

Web application firewalling

**Question 5**

**1.5 / 1.5 pts**

Geoff believes that a workstation on his network may have been the target of an on-path attack. What indicator is most likely to indicate this type of attack on a local network segment?

Encrypted traffic has been forced to use a less secure algorithm.

A website's URL has been modified.

External DNS resolution shows an improper result.

**Correct!**

The ARP table shows an alternate address for the gateway.

**Question 6**

**1.5 / 1.5 pts**

Helen wants to prevent her staff from sideloading applications to their Android devices. What type of tool is best suited to preventing this type of issue without reducing other functionality for the device?

**Correct!**

Use an MDM solution.

Use an EDR tool.

Disable the manufacturer's store.

Disable the Google Play store.

**Question 7**

**1.5 / 1.5 pts**

Jill's organization has received an advisory about a flaw that could allow software running on a virtual machine to execute code on the system that is running the VM hypervisor. What type of vulnerability is this?

A resource reuse issue

A jailbreaking issue

**Correct!**

A VM escape issue

A sideloading issue

**Question 8**

**1.5 / 1.5 pts**

Sam's organization uses a DNS black hole to prevent access to known malicious sites. The organization relies on a reputation service feed that is used to add the known malicious domains and IP addresses. DNS lookups that would go to those sites is sent to an internal redirect site that lets users know the site is inaccessible. Sam reviews the logs to determine if a system is trying to access those blocked sites regularly. What type of indicator of compromise is Sam looking for?

Published or documented indicators

Resource inaccessibility

**Correct!**

Blocked content

Missing logs

**Question 9**

**1.5 / 1.5 pts**

Users in your company report someone has been calling their extension and claiming to be doing a survey for a large vendor. Based on the questions asked in the survey, you suspect that this is a scam to elicit information from your company's employees. What best describes this?

War dialing

Robocalling

Spear phishing

**Correct!**

Vishing

**Question 10**

**1.5 / 1.5 pts**

Amanda discovers that a member of her organization's staff has installed a remote-access Trojan on their accounting software server and has been accessing it remotely. What type of threat has she discovered?

Weak encryption

Zero-day

**Correct!**

Insider threat

Misconfiguration

**Question 11**

**1.5 / 1.5 pts**

Which of the following best describes a zero-day vulnerability?

A vulnerability that can be quickly exploited (i.e., in zero days)

A vulnerability that has not yet been breached

**Correct!**

A vulnerability that the vendor is not yet aware of

A vulnerability that will give the attacker brief access (i.e., zero days)

**Question 12**

**1.5 / 1.5 pts**

Michelle is modeling threat actor motivation for her organization and wants to describe ransomware actors. What motivation is not commonly associated with ransomware?

Data exfiltration

**Correct!**

Revenge

Financial gain

Blackmail

**Question 13**

**1.5 / 1.5 pts**

Isaac is reviewing IPS rules used by his organization and notices rules that block the use of ' as well as OR 1=1 in HTTP queries. What type of attacks is Isaac's organization attempting to stop?

Buffer overflow attacks

Replay attacks

**Correct!**

SQL injection attacks

Directory traversal attacks

**Question 14**

**1.5 / 1.5 pts**

During a regular review of logs, Jennifer notices that a regularly scheduled script that copies files to another server every hour has run multiple times within the last hour. What indicator of compromise should she categorize this as?

Impossible travel

**Correct!**

Out-of-cycle logging

Concurrent session use

Missing logs

**Question 15**

**1.5 / 1.5 pts**

Neil wants to deploy a host-intrusion prevention system that will use a third-party threat feed to servers in his datacenter. What concern might his system administrators express about the HIPS that he should consider before he makes the decision?

A HIPS may make use of segmentation less effective.

A HIPS may prevent least privilege configurations.

**Correct!**

A HIPS may block traffic, causing an outage or disruption.

A HIPS may bypass application allow lists.

**Question 16**

**1.5 / 1.5 pts**

Kathleen wants to control network traffic between subnets using her Cisco network devices. What built-in capability can she use to allow or deny traffic based on port, protocol, and IP address?

Least privilege lists

VLANs

**Correct!**

ACLs

A HIPS

**Question 17**

**1.5 / 1.5 pts**

Scott discovers that malware has been installed on one of the systems he is responsible for. Shortly afterward passwords used by the user that the system is assigned to are discovered to be in use by attackers. What type of malicious program should Scott look for on the compromised system?

**Correct!**

A keylogger

A rootkit

None of the above

A worm

**Question 18**

**1.5 / 1.5 pts**

What term is used to describe the unwanted but generally harmless programs that are commonly installed on consumer computers when they are purchased?

Logic bombs

**Correct!**

Bloatware

Spyware

Firmware

**Question 19**

**1.5 / 1.5 pts**

Jorge wants to brief his organization's leadership on common email threat vectors. Which of the following common threats should not be in his presentation?

Phishing

Email spoofing

**Correct!**

Cross-site scripting

Malware sent via email

**Question 20**

**1.5 / 1.5 pts**

Christina is reviewing a Linux system that she is responsible for, and notices that the /usr filesystem is 80 percent full. After review, she notices that a single user's home directory has hundreds of files in it that were recently added. What type of indicator of compromise should she categorize this as?

**Correct!**

Resource consumption

Resource inaccessibility

Blocked content

Impossible travel