Question 1:

Which of the following must be combined with a threat to create risk?

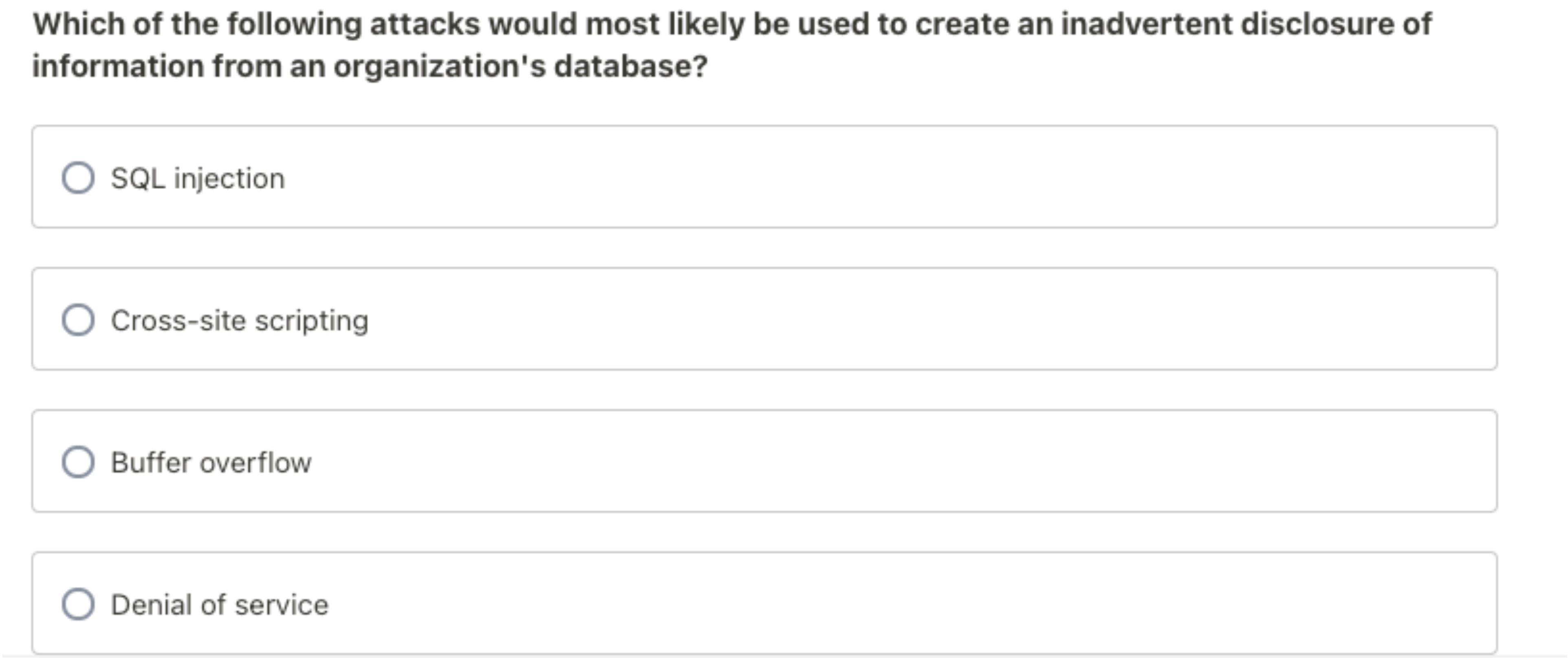
○ Malicious actor

○ Mitigation

○ Vulnerability

○ Exploit

Question 2:



Which of the following attacks would most likely be used to create an inadvertent disclosure of information from an organization's database?

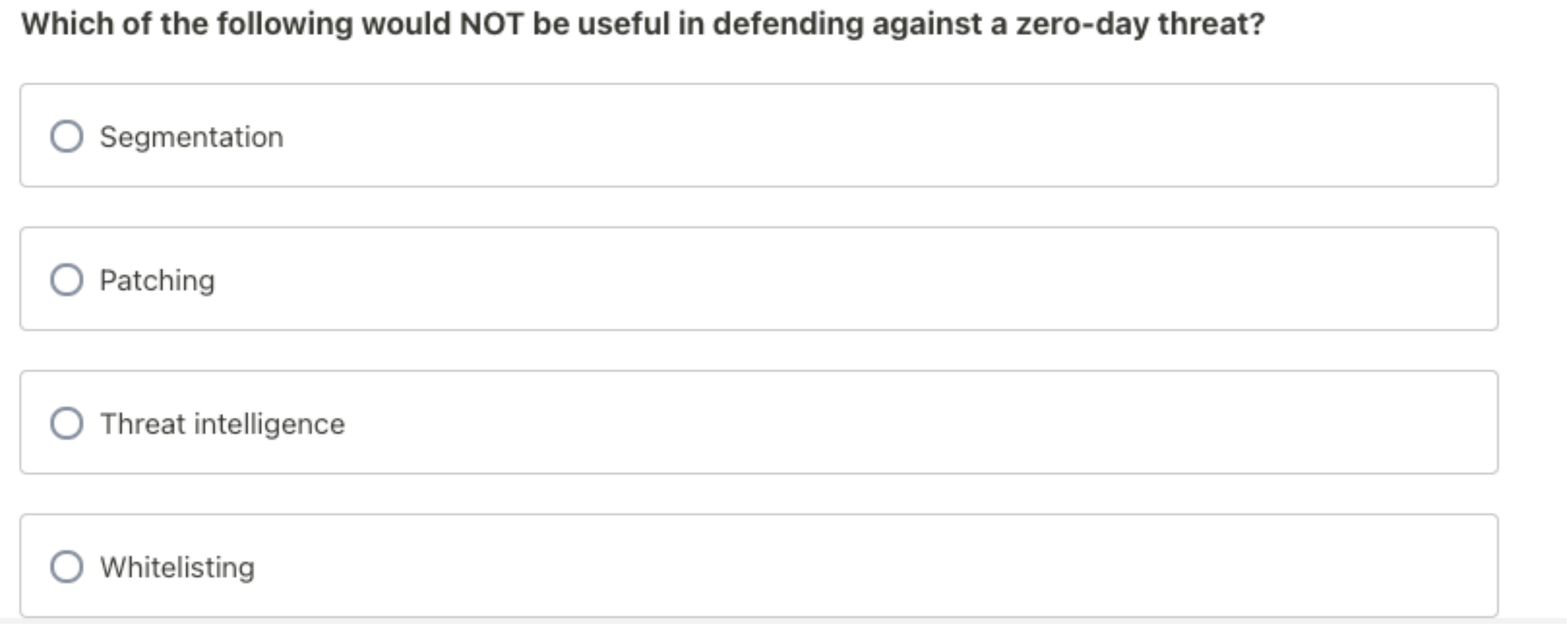
○ SQL injection

○ Cross-site scripting

○ Buffer overflow

○ Denial of service

Question 3:



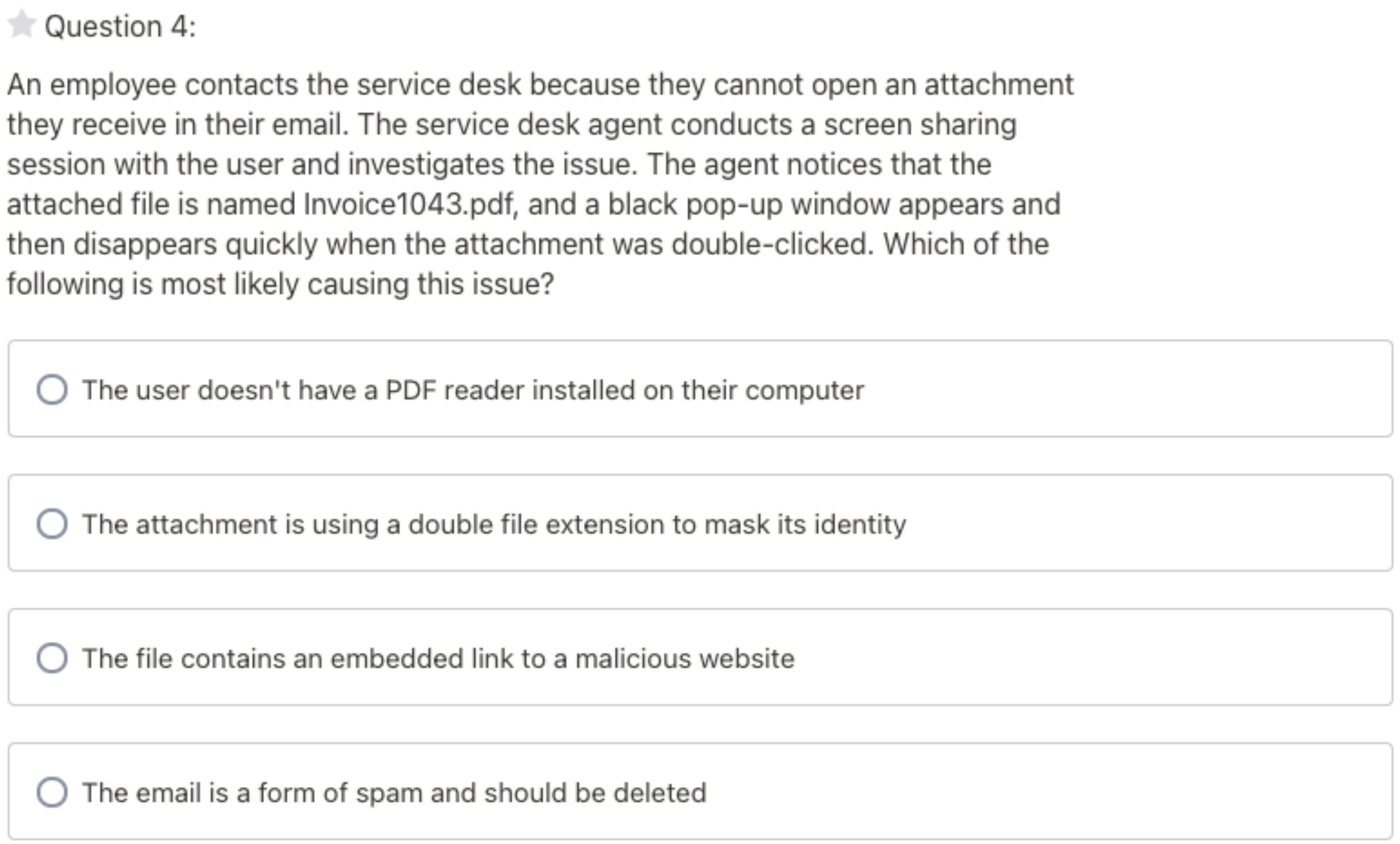
Which of the following would NOT be useful in defending against a zero-day threat?

○ Segmentation

○ Patching

○ Threat intelligence

○ Whitelisting



Question 4:

An employee contacts the service desk because they cannot open an attachment they receive in their email. The service desk agent conducts a screen sharing session with the user and investigates the issue. The agent notices that the attached file is named Invoice1043.pdf, and a black pop-up window appears and then disappears quickly when the attachment was double-clicked. Which of the following is most likely causing this issue?

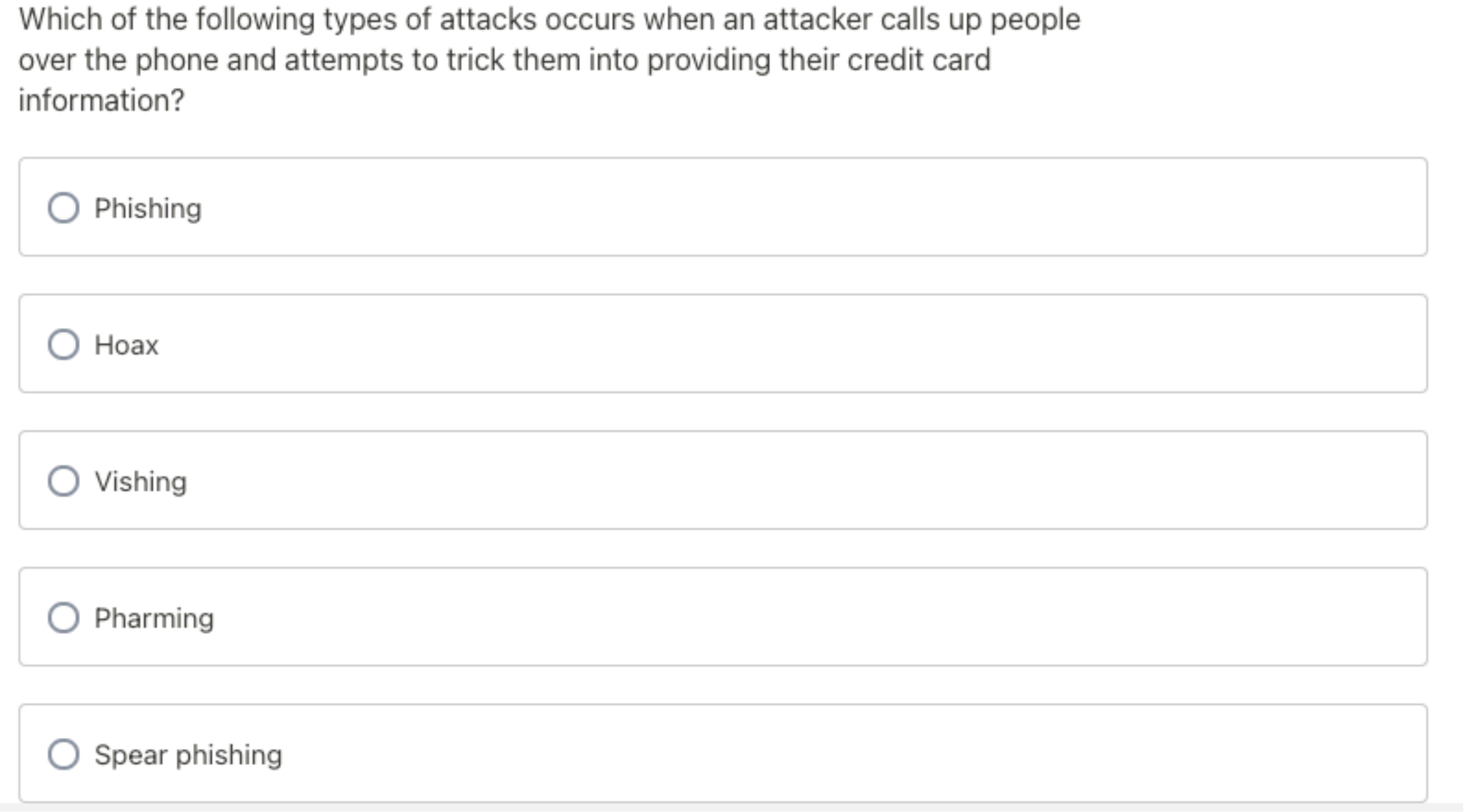
○ The user doesn't have a PDF reader installed on their computer

○ The attachment is using a double file extension to mask its identity

○ The file contains an embedded link to a malicious website

○ The email is a form of spam and should be deleted

Question 5:



Which of the following types of attacks occurs when an attacker calls up people over the phone and attempts to trick them into providing their credit card information?

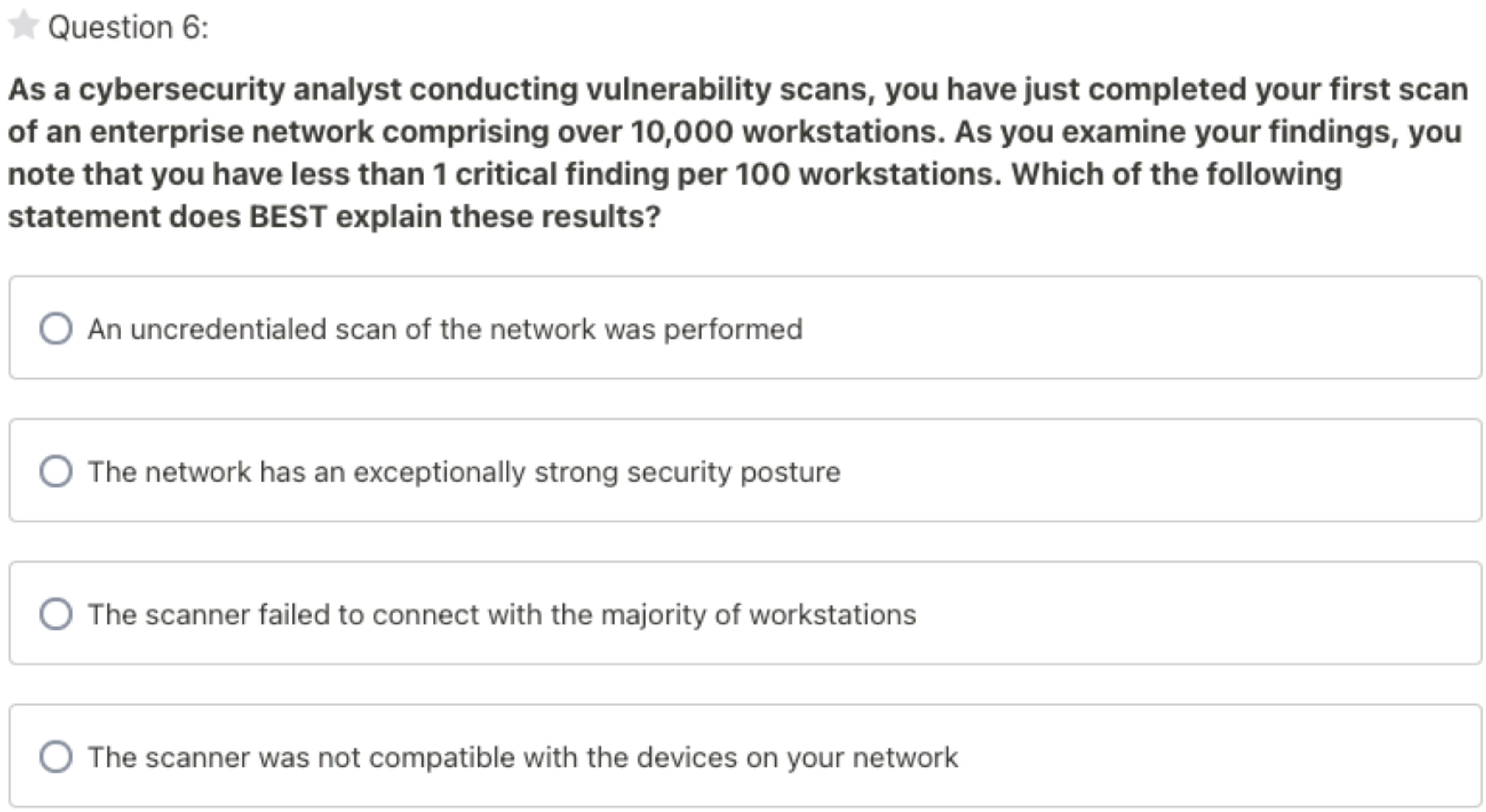
○ Phishing

○ Hoax

○ Vishing

○ Pharming

○ Spear phishing



Question 6:

As a cybersecurity analyst conducting vulnerability scans, you have just completed your first scan of an enterprise network comprising over 10,000 workstations. As you examine your findings, you note that you have less than 1 critical finding per 100 workstations. Which of the following statement does BEST explain these results?

○ An uncredentialed scan of the network was performed

○ The network has an exceptionally strong security posture

○ The scanner failed to connect with the majority of workstations

○ The scanner was not compatible with the devices on your network

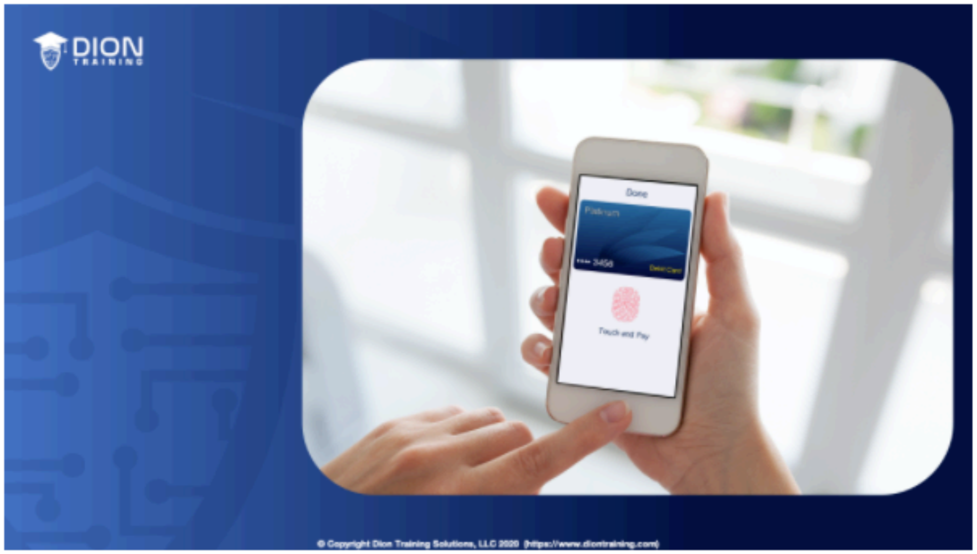
★ Question 7:

Which of the following cryptographic algorithms is classified as asymmetric?

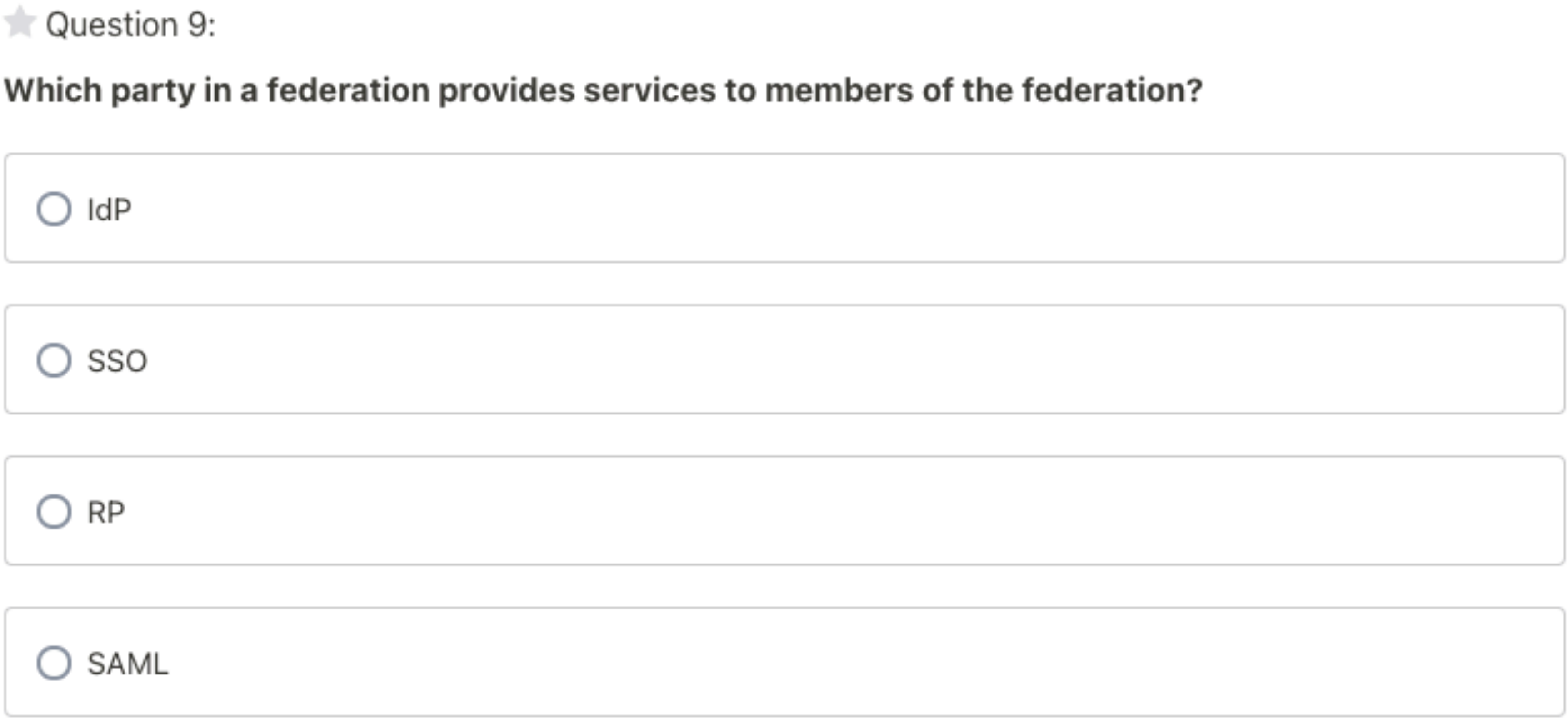
- ○ 3DES
- ○ RRC4
- ○ AES
- ○ PGP

Question 8:

(Sample Simulation – On the real exam for this type of question, you would receive 3-5 pictures and be asked to drag and drop them into place next to the correct term.)



○ Biometric Authentication
○ One-time password Authentication
○ Multifactor Authentication
○ PAP Authentication



Question 9:

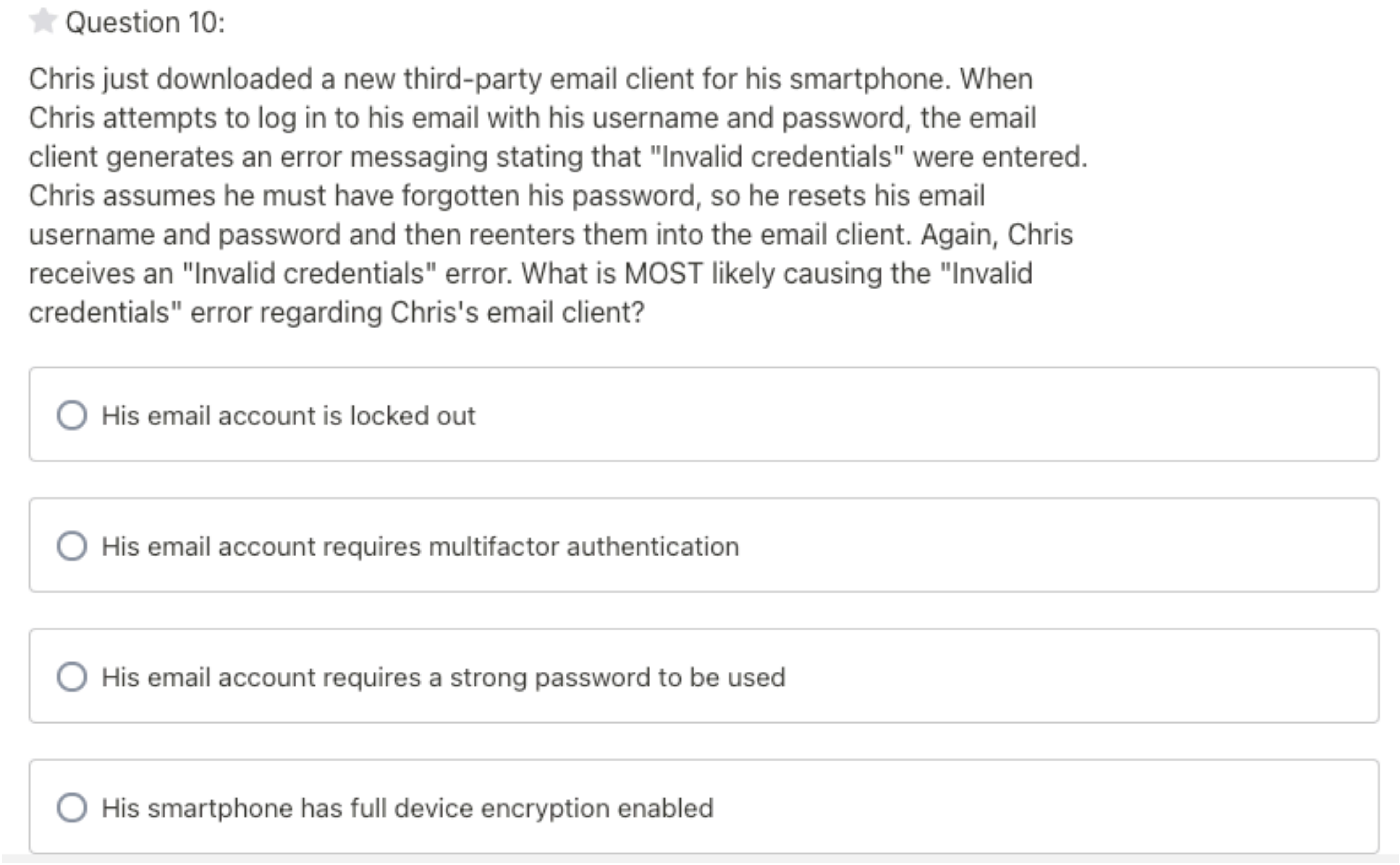
Which party in a federation provides services to members of the federation?

○ IdP

○ SSO

○ RP

○ SAML



Question 10:

Chris just downloaded a new third-party email client for his smartphone. When Chris attempts to log in to his email with his username and password, the email client generates an error messaging stating that "Invalid credentials" were entered. Chris assumes he must have forgotten his password, so he resets his email username and password and then reenters them into the email client. Again, Chris receives an "Invalid credentials" error. What is MOST likely causing the "Invalid credentials" error regarding Chris's email client?

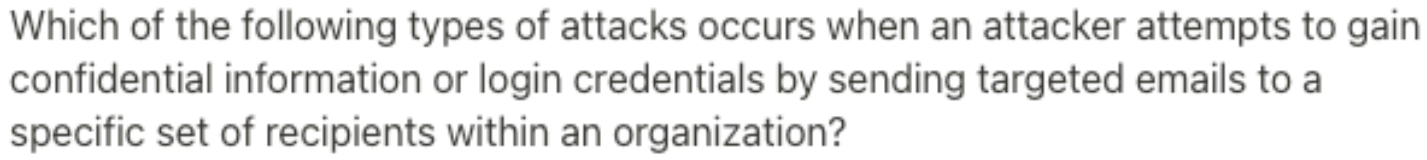
○ His email account is locked out

○ His email account requires multifactor authentication

○ His email account requires a strong password to be used

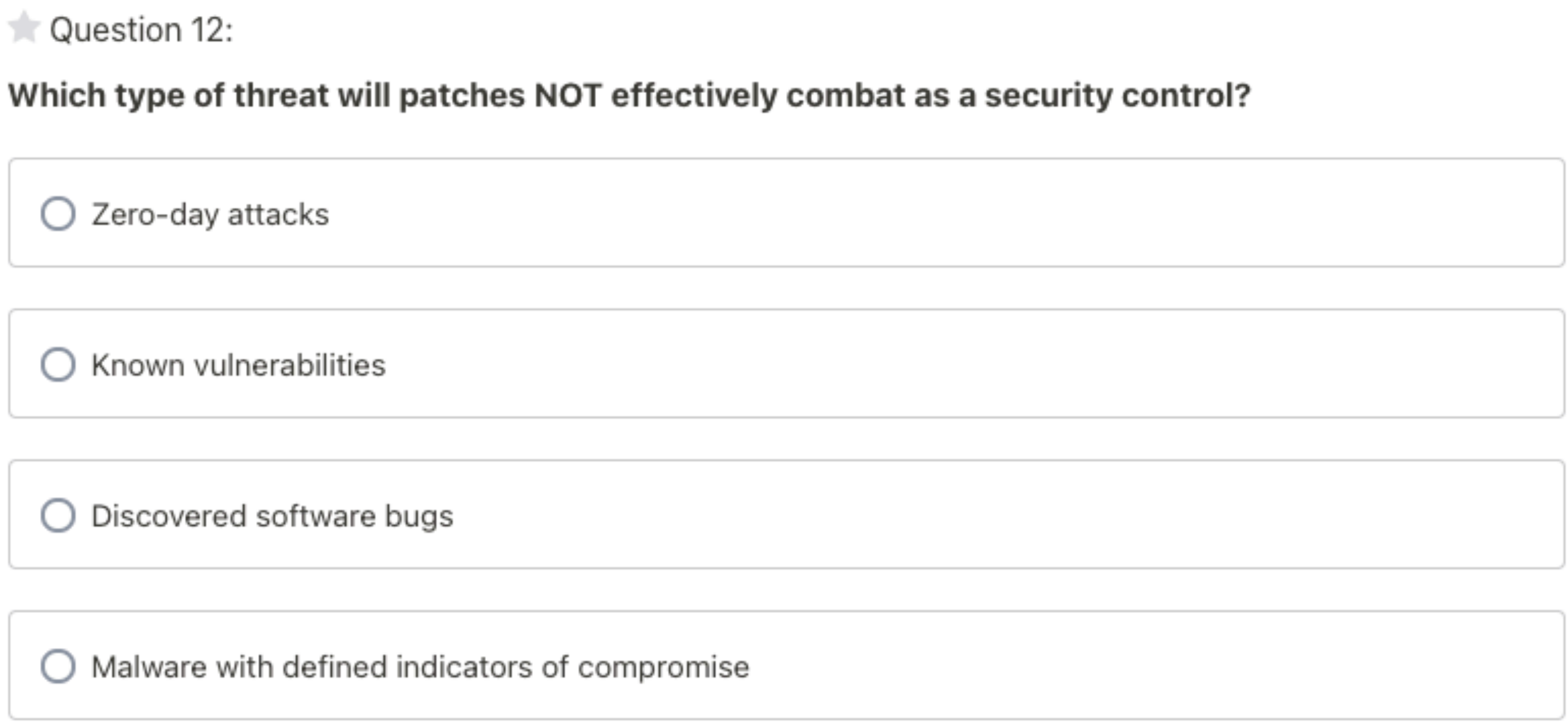
○ His smartphone has full device encryption enabled

Question 11:



Which of the following types of attacks occurs when an attacker attempts to gain confidential information or login credentials by sending targeted emails to a specific set of recipients within an organization?

- ○ Phishing
- ○ HOAX
- ○ Vishing
- ○ Pharming
- ○ Spear Phishing



Question 12:

Which type of threat will patches NOT effectively combat as a security control?

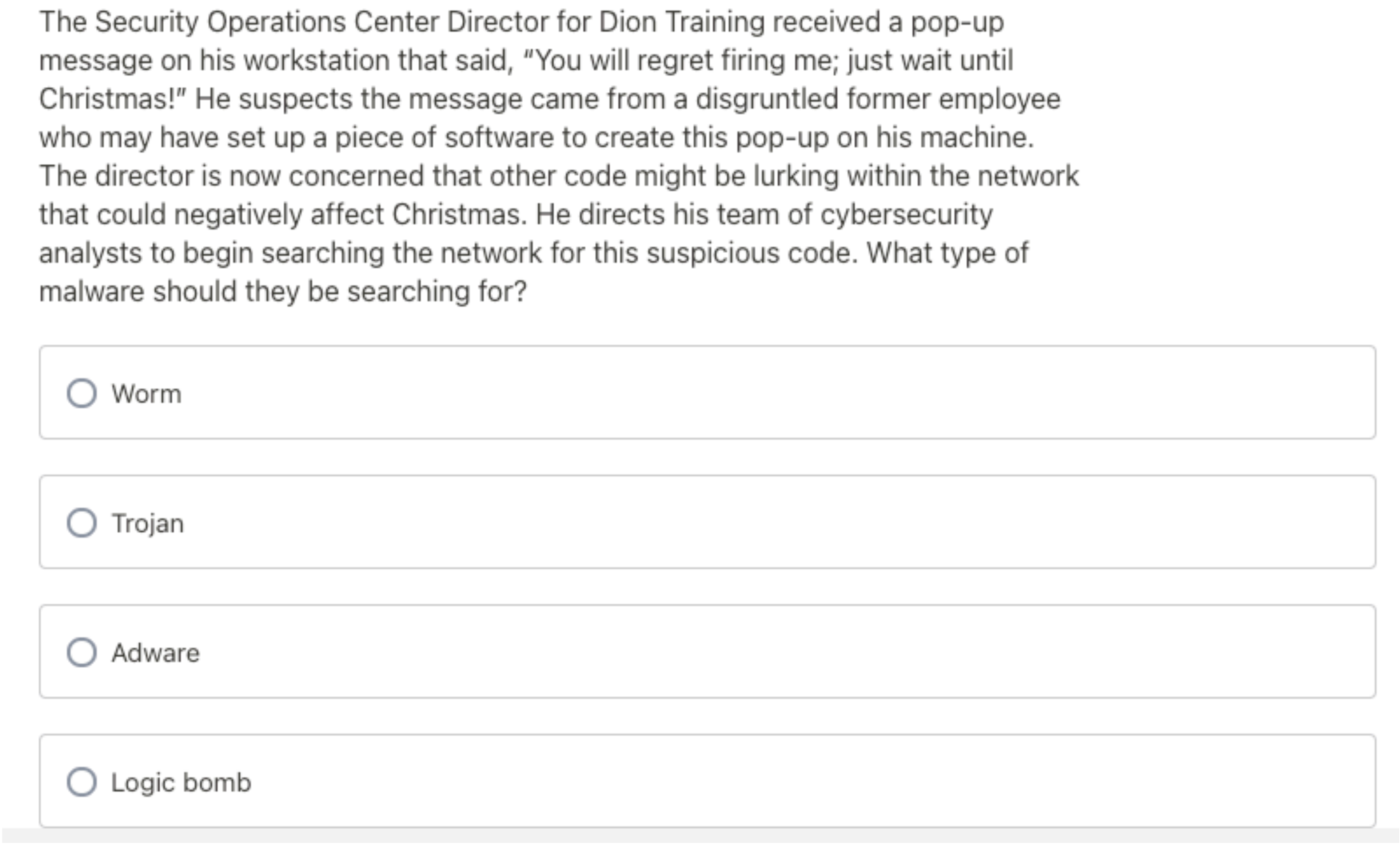
○ Zero-day attacks

○ Known vulnerabilities

○ Discovered software bugs

○ Malware with defined indicators of compromise

Question 13:



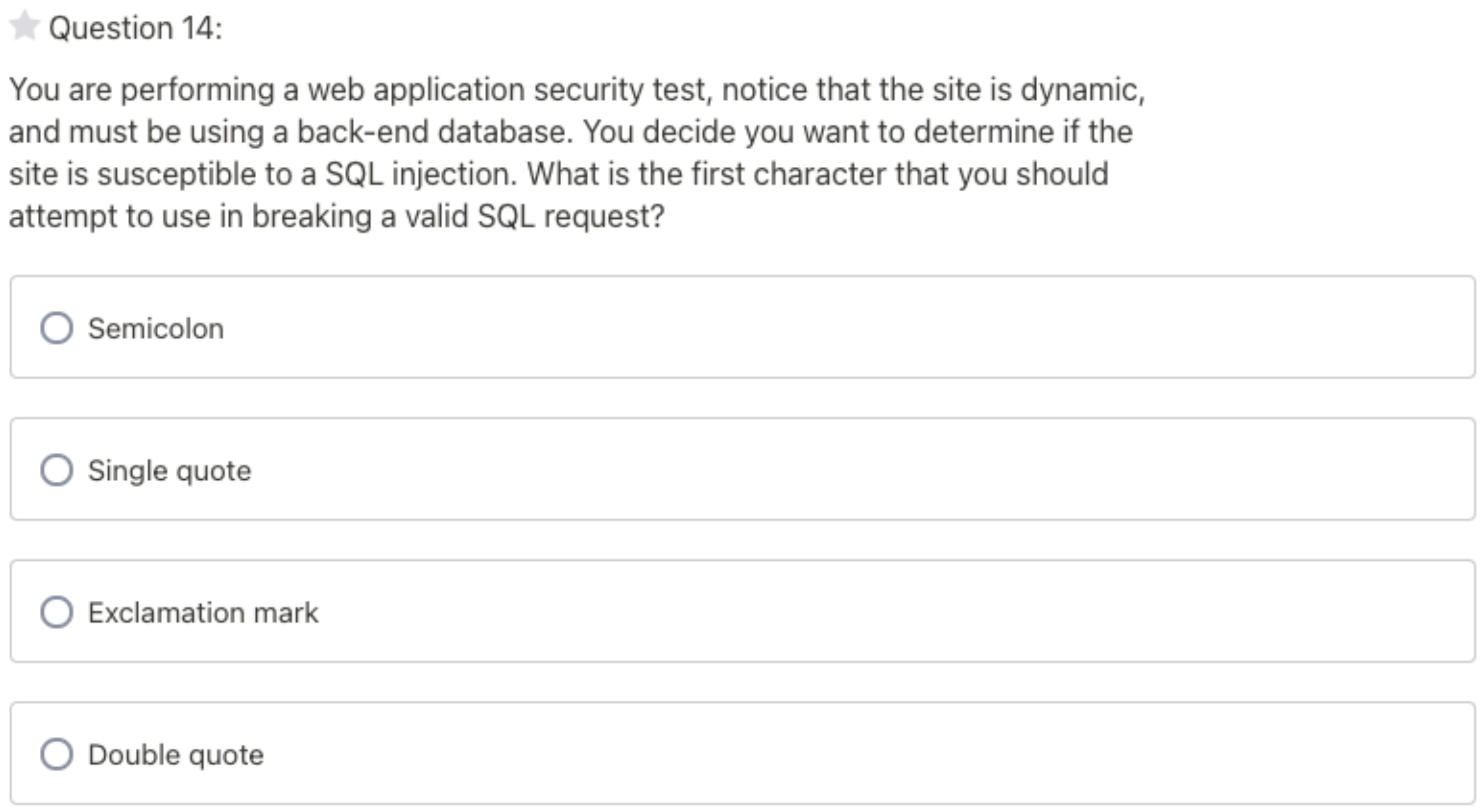
The Security Operations Center Director for Dion Training received a pop-up message on his workstation that said, “You will regret firing me; just wait until Christmas!” He suspects the message came from a disgruntled former employee who may have set up a piece of software to create this pop-up on his machine. The director is now concerned that other code might be lurking within the network that could negatively affect Christmas. He directs his team of cybersecurity analysts to begin searching the network for this suspicious code. What type of malware should they be searching for?

○ Worm

○ Trojan

○ Adware

○ Logic bomb



Question 14:

You are performing a web application security test, notice that the site is dynamic, and must be using a back-end database. You decide you want to determine if the site is susceptible to a SQL injection. What is the first character that you should attempt to use in breaking a valid SQL request?

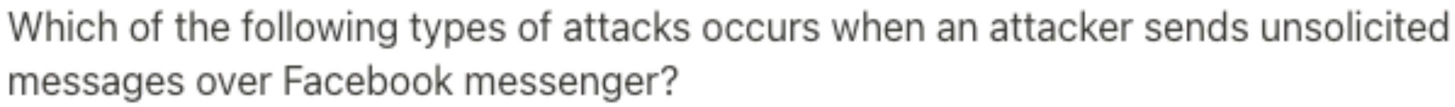
○ Semicolon

○ Single quote

○ Exclamation mark

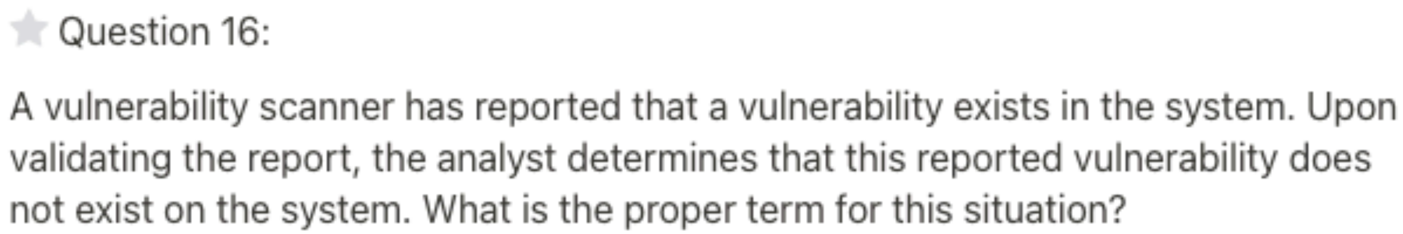
○ Double quote

Question 15:



Which of the following types of attacks occurs when an attacker sends unsolicited messages over Facebook messenger?

○ Pharming
○ Phishinng
○ Spimming
○ Spamming
○ Spear Phishing



Question 16:

A vulnerability scanner has reported that a vulnerability exists in the system. Upon validating the report, the analyst determines that this reported vulnerability does not exist on the system. What is the proper term for this situation?

○ False Positive
○ False Negative
○ True Positive
○ True Negative

★ Question 17:

The paparazzi have found copies of pictures of a celebrity's new baby online. The celebrity states they were never publicly released but were uploaded to their cloud provider's automated photo backup. Which of the following threats was the celebrity MOST likely a victim of?

○ Leaked personal files

○ Unauthorized root access

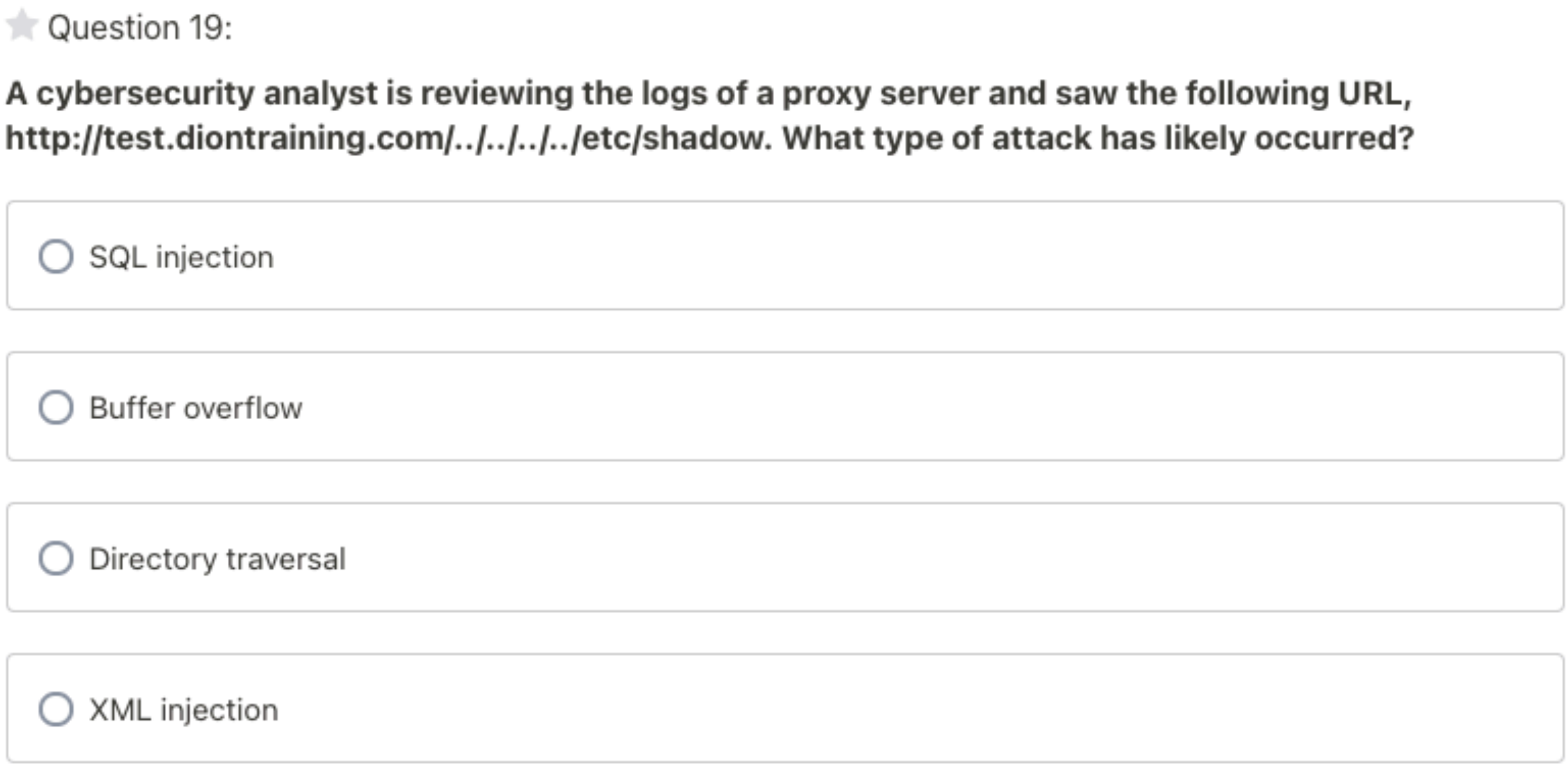
○ Unauthorized camera activation

○ Unintended Bluetooth pairing

Question 18:

What is the utilization of insights gained from threat research and threat modeling to proactively discover evidence of adversarial TTPs within a network or system called?

○ Threat Hunting
○ Penetration Testing
○ Information Assurance
○ Incident Response



Question 19:

A cybersecurity analyst is reviewing the logs of a proxy server and saw the following URL, http://test.diontraining.com/../../../../etc/shadow. What type of attack has likely occurred?

○ SQL injection

○ Buffer overflow

○ Directory traversal

○ XML injection

☆ Question 20:

What type of threat actor is highly funded and often backed by nation-states?

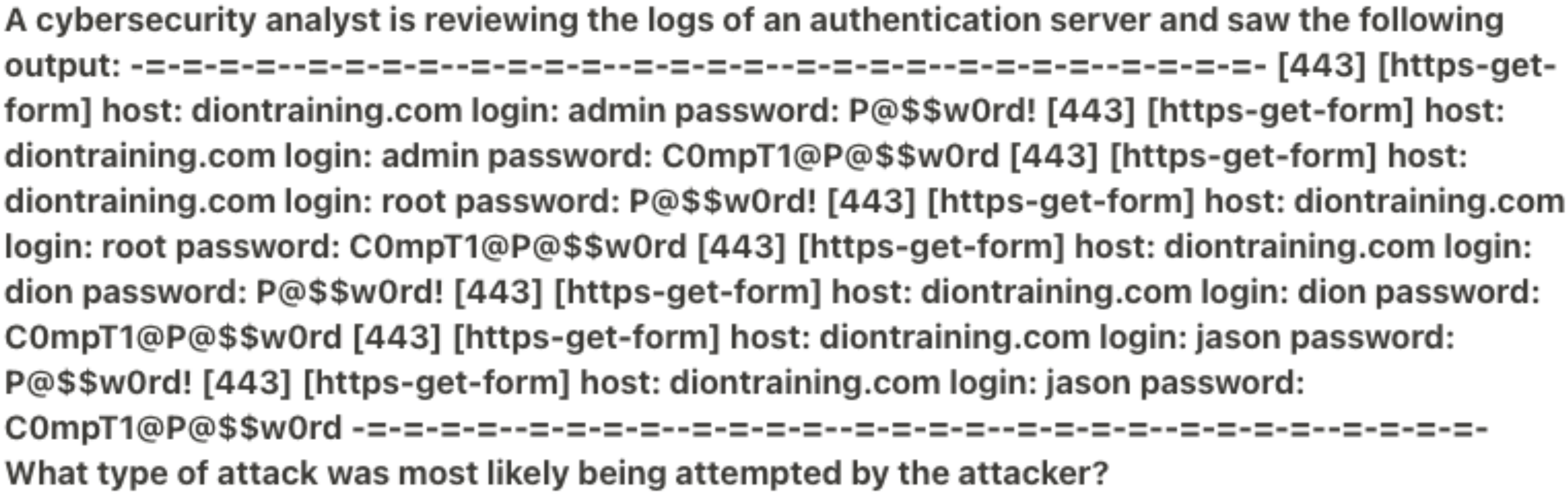
○ APT

○ Hacktivist

○ Script Kiddies

○ Insider Threat

Question 21:



A cybersecurity analyst is reviewing the logs of an authentication server and saw the following output: -=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=- [443] [https-get-form] host: diontraining.com login: admin password: P@$$w0rd! [443] [https-get-form] host: diontraining.com login: admin password: C0mpT1@P@$$w0rd [443] [https-get-form] host: diontraining.com login: root password: P@$$w0rd! [443] [https-get-form] host: diontraining.com login: root password: C0mpT1@P@$$w0rd [443] [https-get-form] host: diontraining.com login: dion password: P@$$w0rd! [443] [https-get-form] host: diontraining.com login: dion password: C0mpT1@P@$$w0rd [443] [https-get-form] host: diontraining.com login: jason password: P@$$w0rd! [443] [https-get-form] host: diontraining.com login: jason password: C0mpT1@P@$$w0rd -=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=--=-=-=-=- What type of attack was most likely being attempted by the attacker?

○ Session Hijacking
○ Password Spraying
○ Impersonation
○ Credential Stuffing

Question 22:

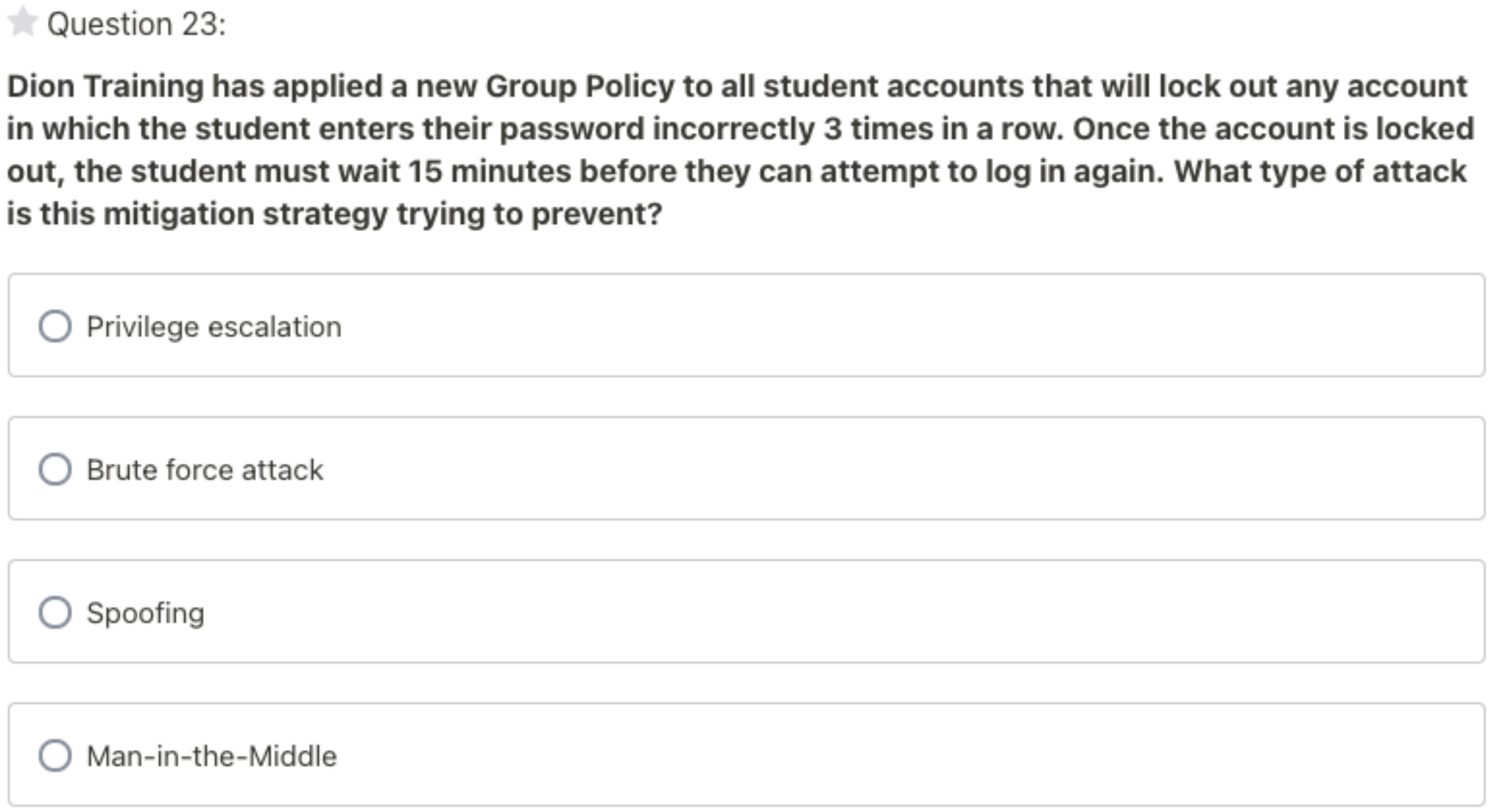
Which of the following types of remote access technologies should NOT be used in a network due to its lack of security?

○ RDP

○ telnet

○ SSH

○ VPN



Question 23:

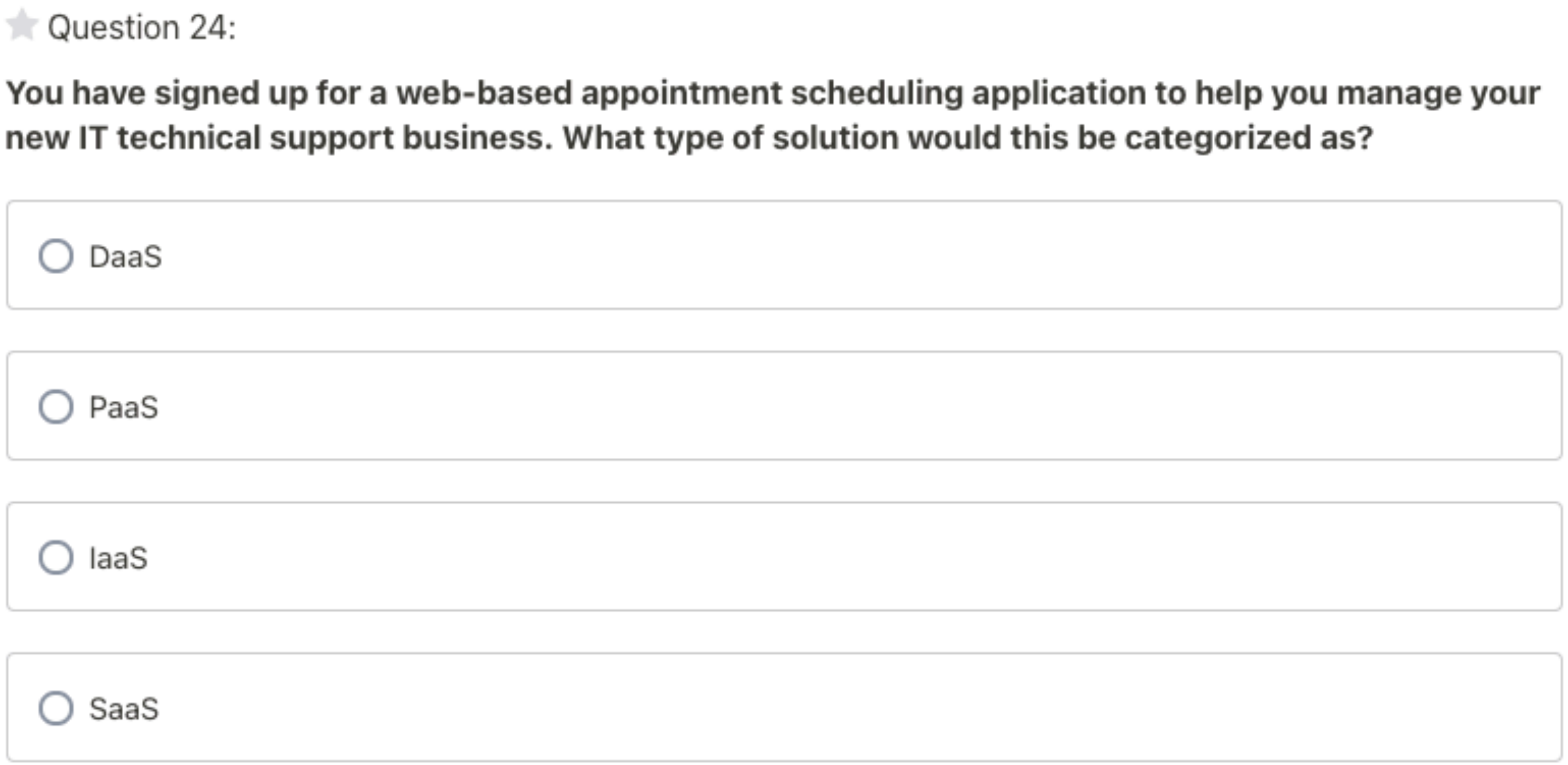
Dion Training has applied a new Group Policy to all student accounts that will lock out any account in which the student enters their password incorrectly 3 times in a row. Once the account is locked out, the student must wait 15 minutes before they can attempt to log in again. What type of attack is this mitigation strategy trying to prevent?

○ Privilege escalation

○ Brute force attack

○ Spoofing

○ Man-in-the-Middle



Question 24:

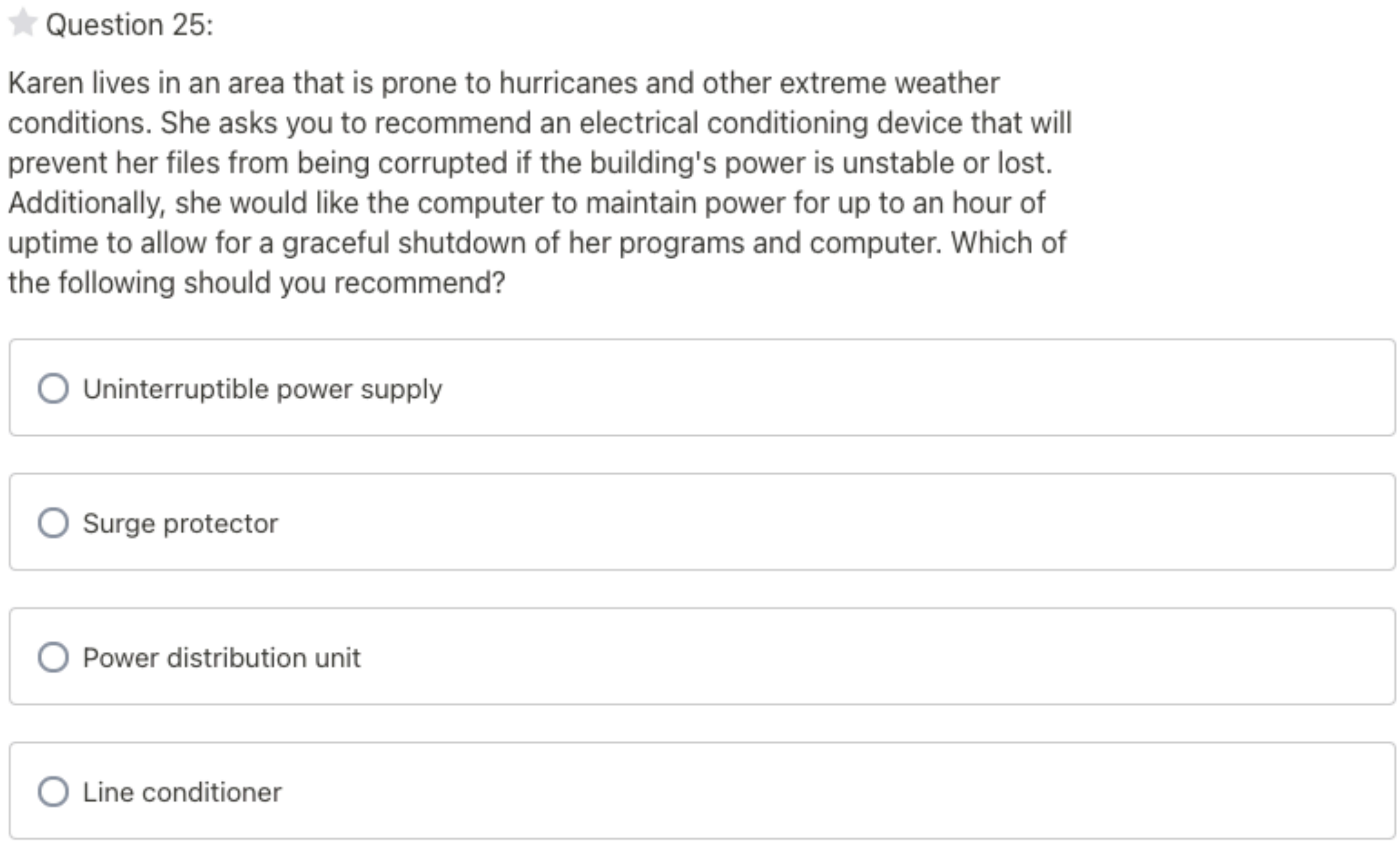
You have signed up for a web-based appointment scheduling application to help you manage your new IT technical support business. What type of solution would this be categorized as?

○ DaaS

○ PaaS

○ IaaS

○ SaaS



Question 25:

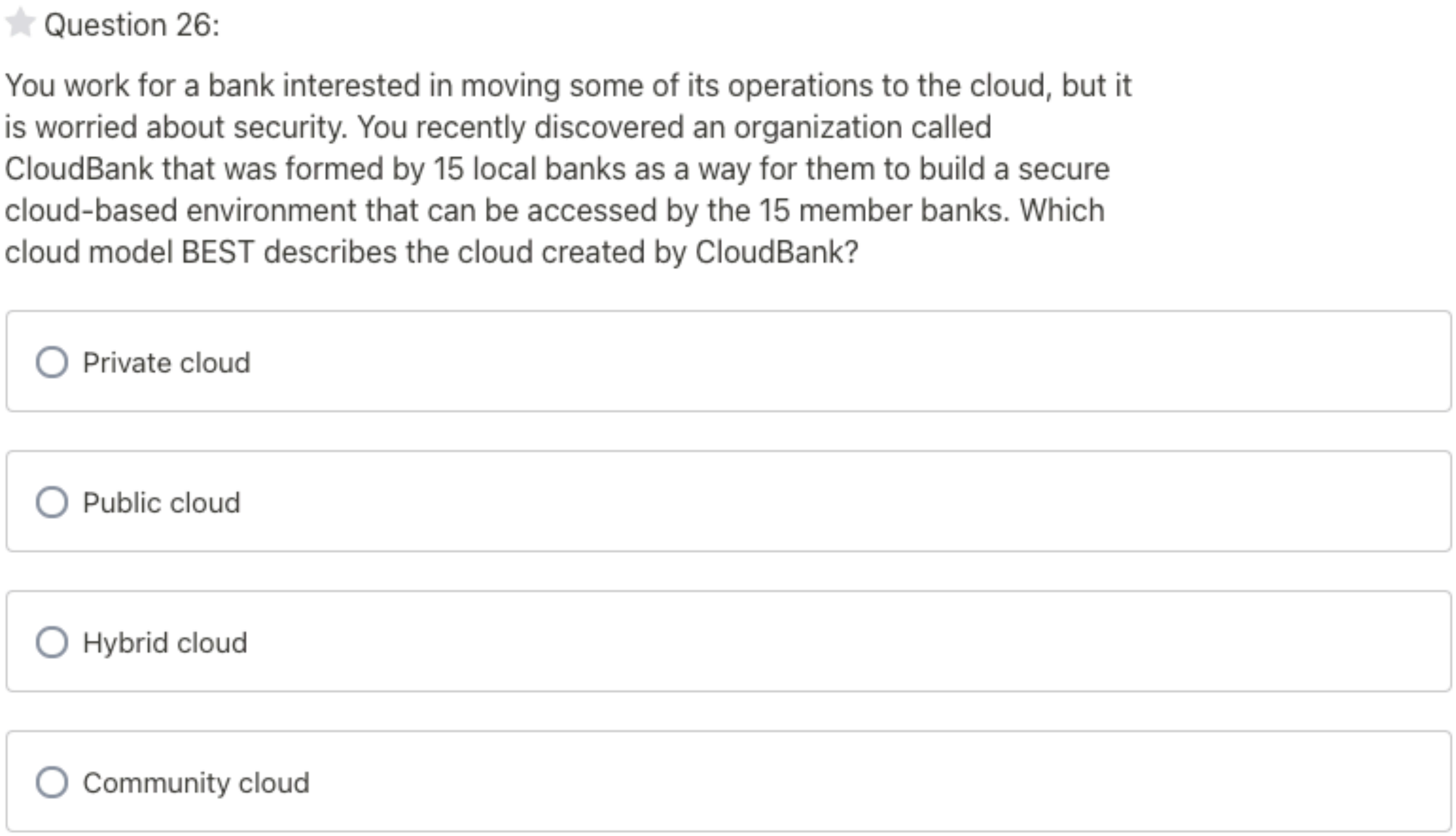
Karen lives in an area that is prone to hurricanes and other extreme weather conditions. She asks you to recommend an electrical conditioning device that will prevent her files from being corrupted if the building's power is unstable or lost. Additionally, she would like the computer to maintain power for up to an hour of uptime to allow for a graceful shutdown of her programs and computer. Which of the following should you recommend?

○ Uninterruptible power supply

○ Surge protector

○ Power distribution unit

○ Line conditioner



Question 26:

You work for a bank interested in moving some of its operations to the cloud, but it is worried about security. You recently discovered an organization called CloudBank that was formed by 15 local banks as a way for them to build a secure cloud-based environment that can be accessed by the 15 member banks. Which cloud model BEST describes the cloud created by CloudBank?

○ Private cloud

○ Public cloud

○ Hybrid cloud

○ Community cloud

Question 27:

You have just received some unusual alerts on your SIEM dashboard and want to collect the payload associated with it. Which of the following should you implement to effectively collect these malicious payloads that the attackers are sending towards your systems without impacting your organization's normal business operations?

○ Honeypot

○ Jumpbox

○ Sandbox

○ Containerization

☆ Question 28:

Nicole's organization does not have the budget or staff to conduct 24/7 security monitoring of their network. To supplement her team, she contracts with a managed SOC service. Which of the following services or providers would be best suited for this role?

○ MSSP

○ IaaS

○ PaaS

○ SaaS

Question 29:

Maria is trying to log in to her company's webmail and is asked to enter her username and password. Which type of authentication method is Maria using?

○ RADIUS

○ Multifactor

○ TACACS+

○ Single-factor

☆ Question 30:

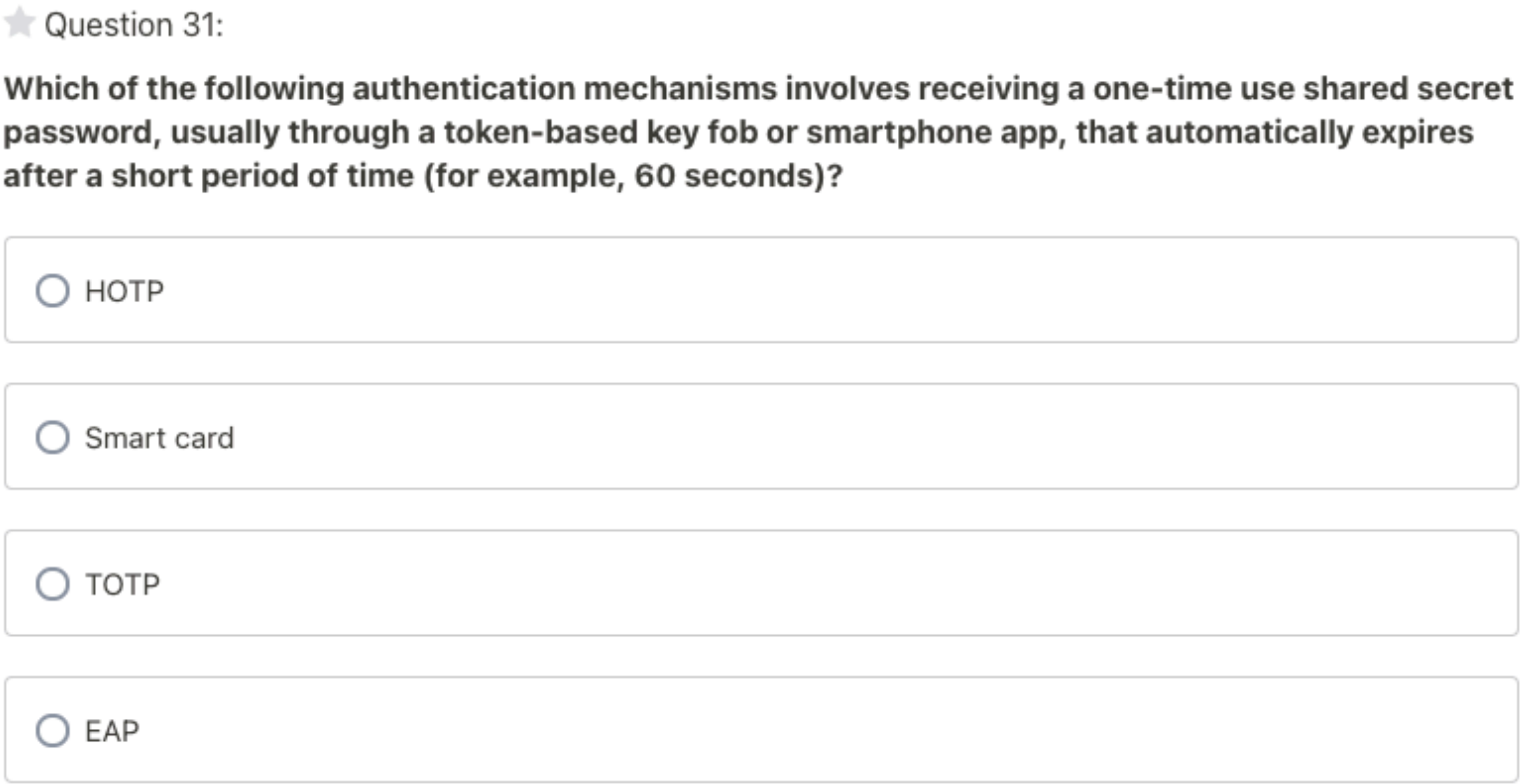
Joseph would like to prevent hosts from connecting to known malware distribution domains. What type of solution should be used without deploying endpoint protection software or an IPS system?

○ Route poisoning

○ Anti-malware router filters

○ Subdomain whitelisting

○ DNS blackholing



Question 31:

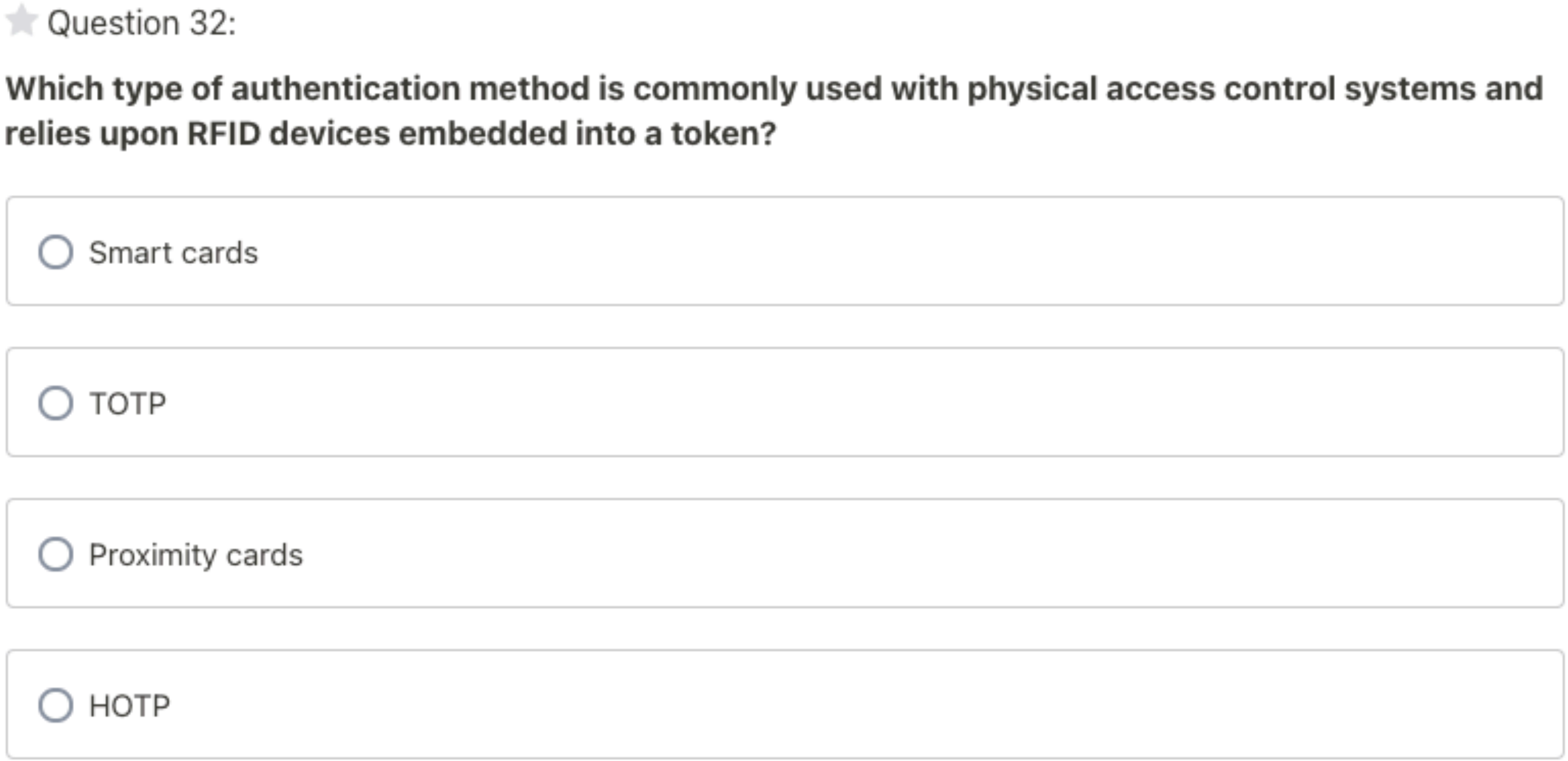
Which of the following authentication mechanisms involves receiving a one-time use shared secret password, usually through a token-based key fob or smartphone app, that automatically expires after a short period of time (for example, 60 seconds)?

○ HOTP

○ Smart card

○ TOTP

○ EAP



☆ Question 32:

Which type of authentication method is commonly used with physical access control systems and relies upon RFID devices embedded into a token?

○ Smart cards

○ TOTP

○ Proximity cards

○ HOTP

Question 33:

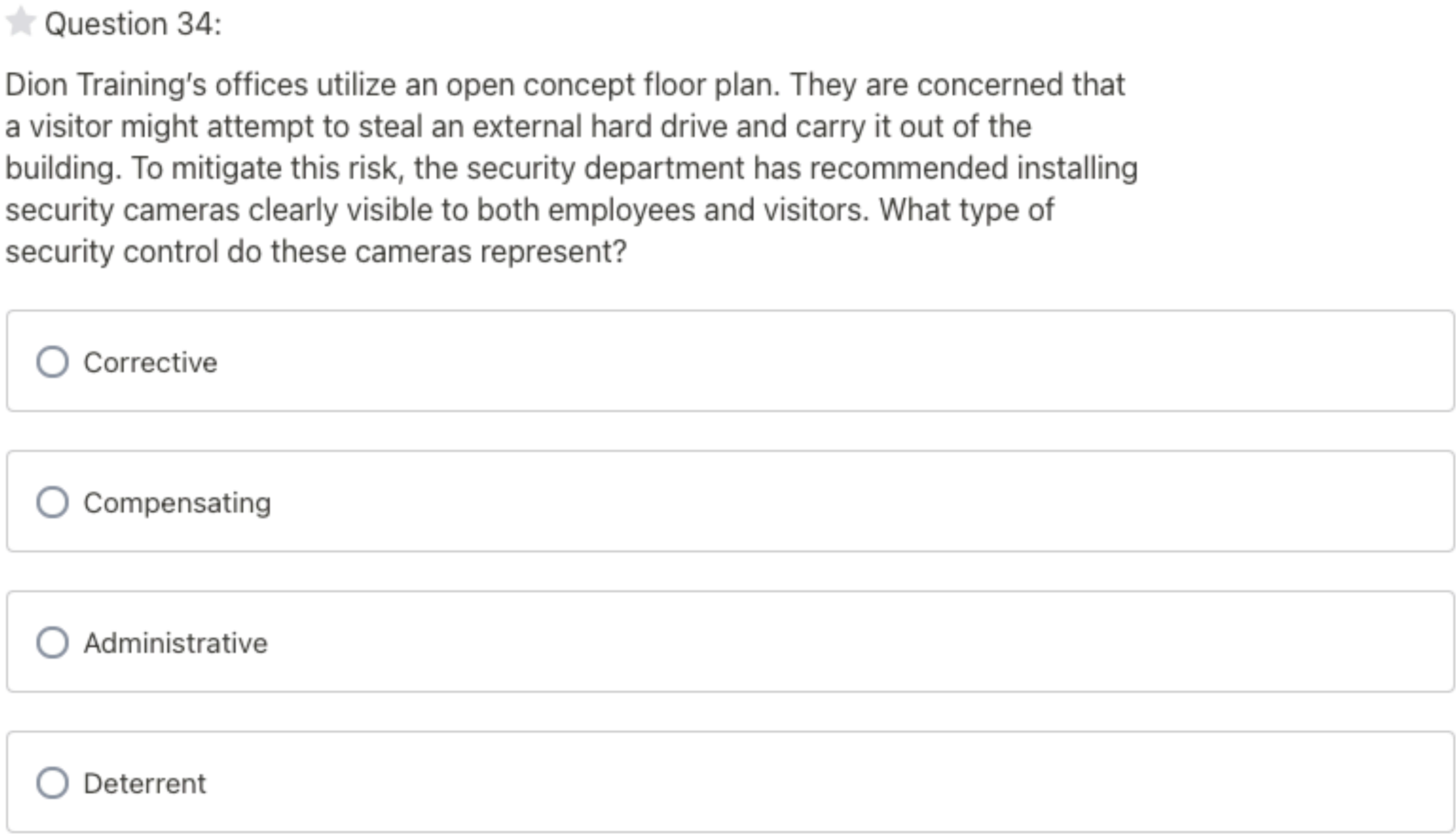
Keith wants to validate the application file that he downloaded from the vendor of the application. Which of the following should he compare against the file to verify the integrity of the downloaded application?

○ File size and file creation date

○ MD5 or SHA1 hash digest of the file

○ Private key of the file

○ Public key of the file



Question 34:

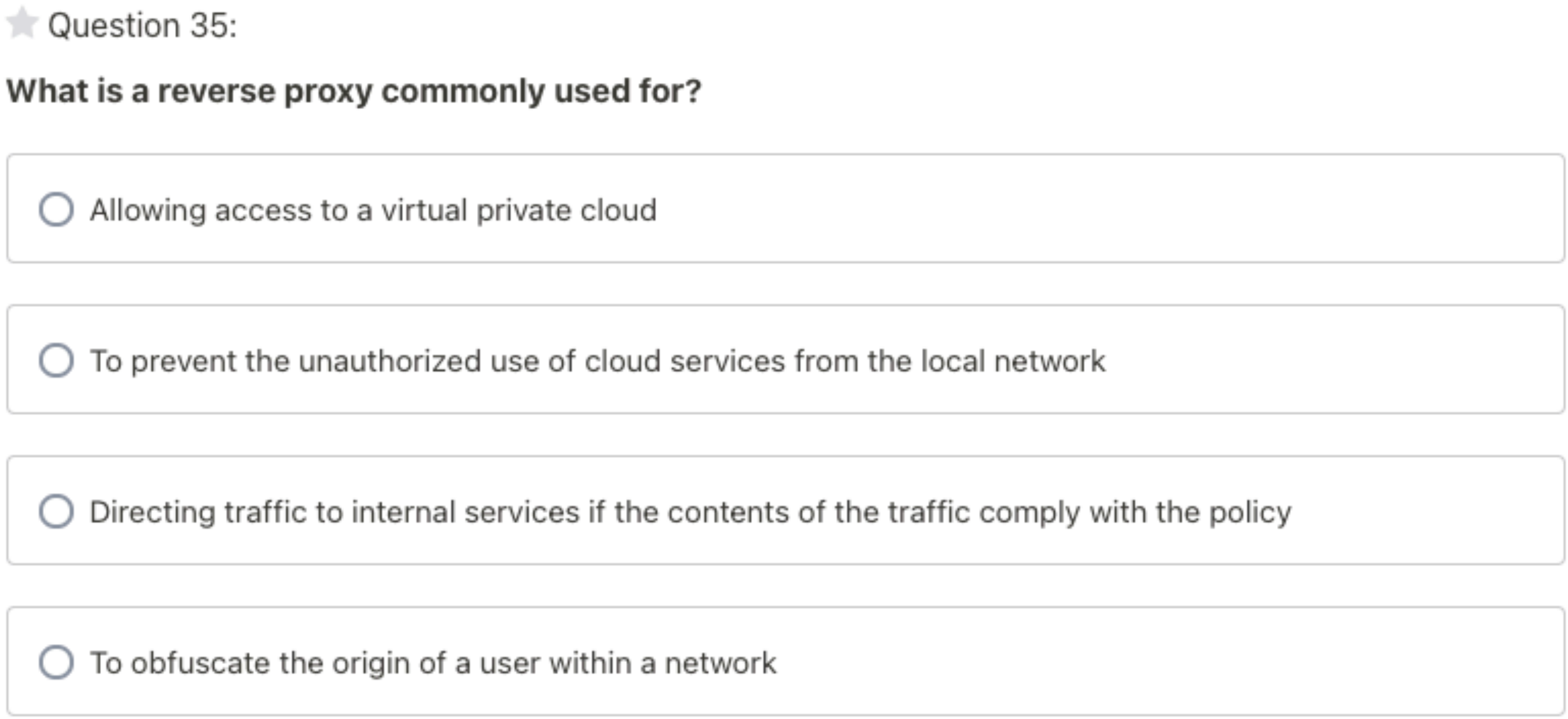
Dion Training's offices utilize an open concept floor plan. They are concerned that a visitor might attempt to steal an external hard drive and carry it out of the building. To mitigate this risk, the security department has recommended installing security cameras clearly visible to both employees and visitors. What type of security control do these cameras represent?

○ Corrective

○ Compensating

○ Administrative

○ Deterrent



Question 35:

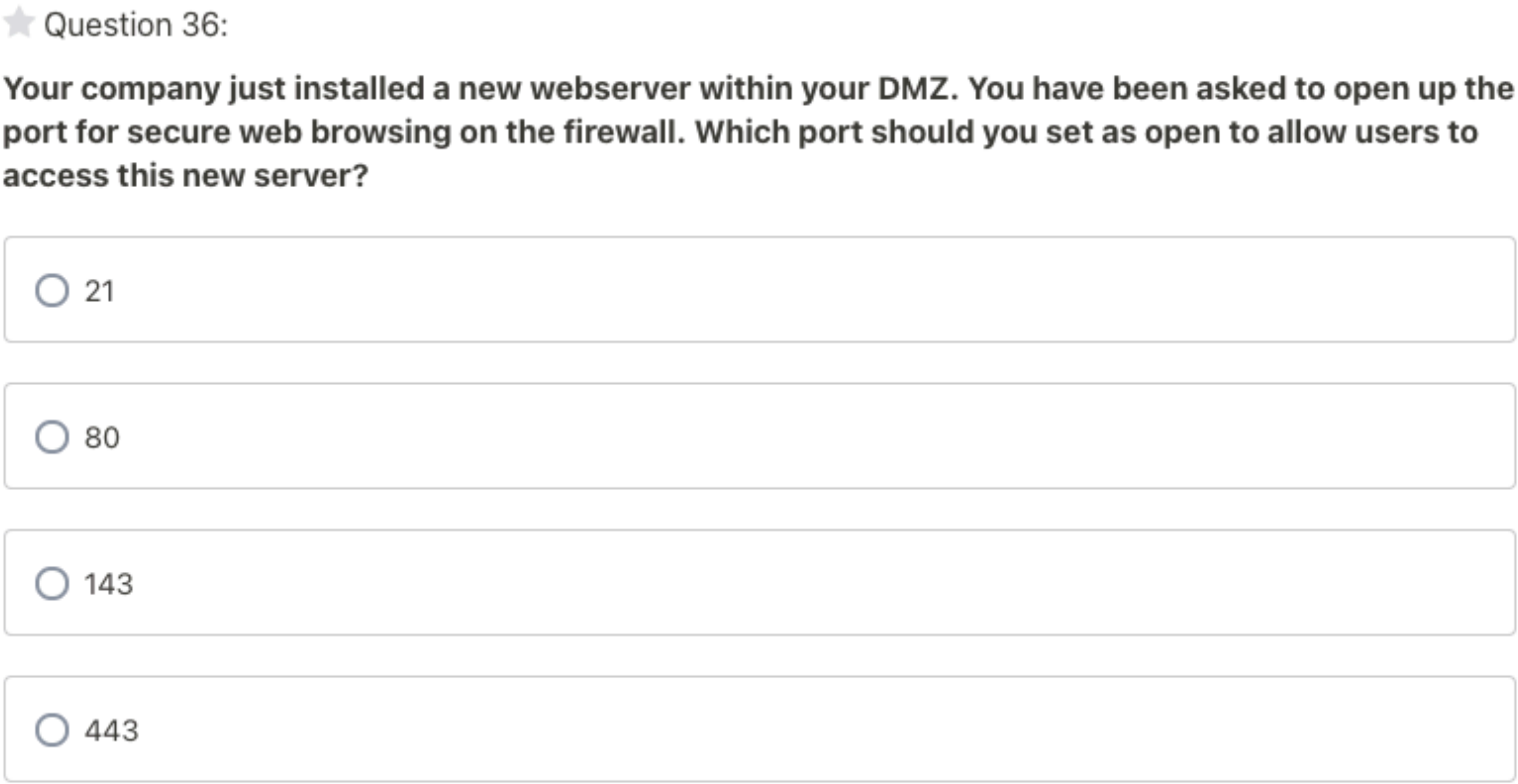
What is a reverse proxy commonly used for?

○ Allowing access to a virtual private cloud

○ To prevent the unauthorized use of cloud services from the local network

○ Directing traffic to internal services if the contents of the traffic comply with the policy

○ To obfuscate the origin of a user within a network



☆ Question 36:

Your company just installed a new webserver within your DMZ. You have been asked to open up the port for secure web browsing on the firewall. Which port should you set as open to allow users to access this new server?

○ 21

○ 80

○ 143

○ 443

Question 37:

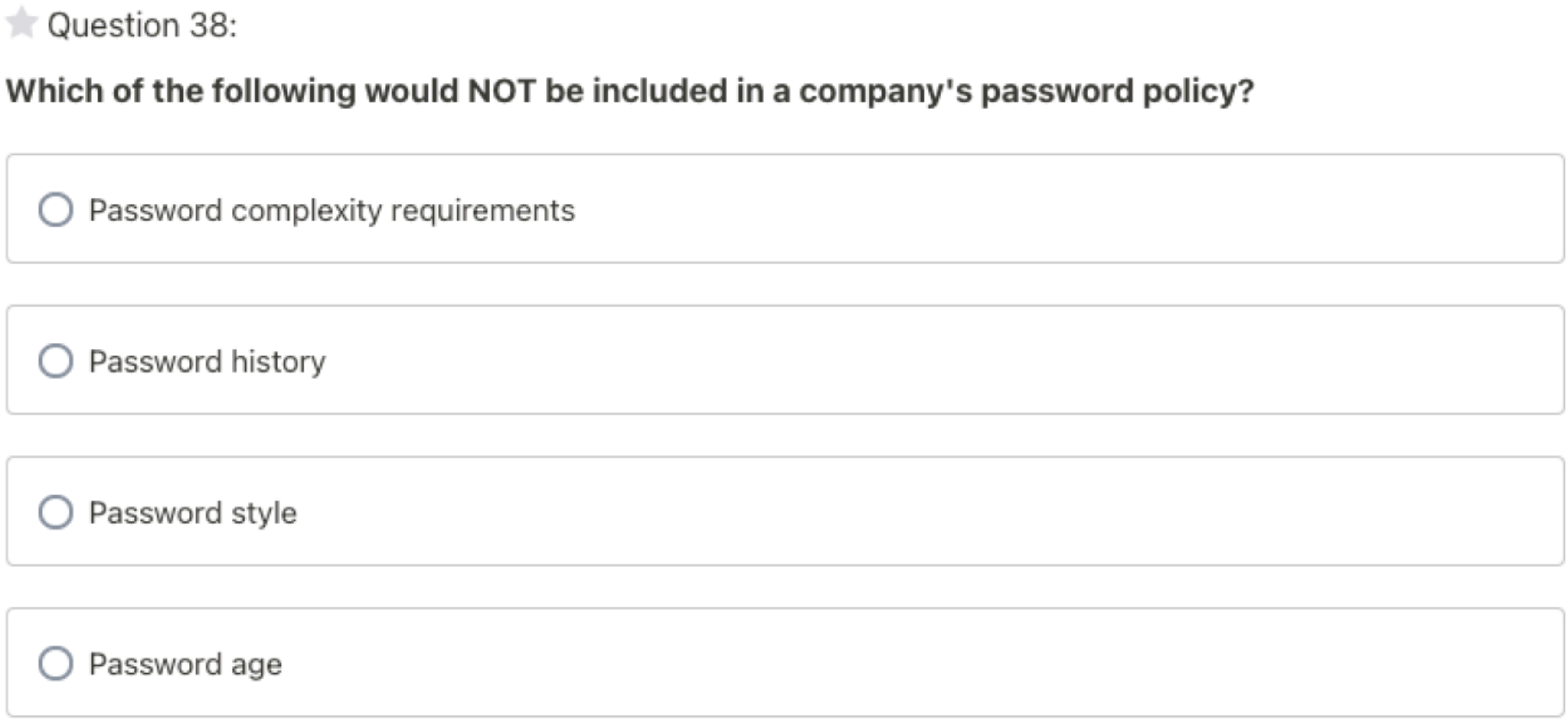
Which of the following is the leading cause for cross-site scripting, SQL injection, and XML injection attacks?

○ Directory traversals

○ File inclusions

○ Faulty input validation

○ Output encoding



Question 38:

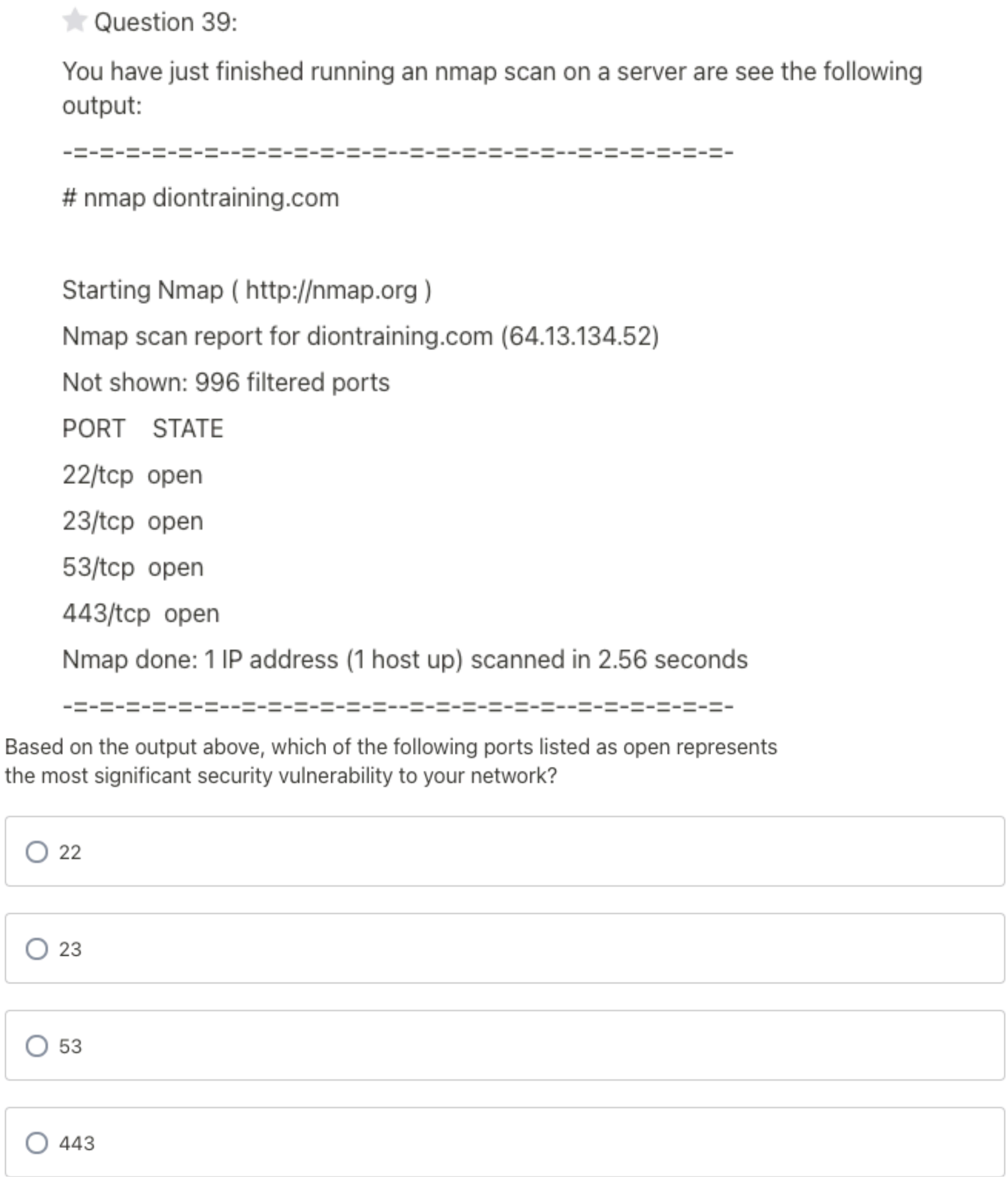
Which of the following would NOT be included in a company's password policy?

○ Password complexity requirements

○ Password history

○ Password style

○ Password age



Question 39:

You have just finished running an nmap scan on a server are see the following output:

```
-=-=-=-=-=-=--=-=-=-=-=-=-=--=-=-=-=-=-=--=-=-=-=-=-
# nmap diontraining.com


Starting Nmap ( http://nmap.org )
Nmap scan report for diontraining.com (64.13.134.52)
Not shown: 996 filtered ports
PORT    STATE
22/tcp  open
23/tcp  open
53/tcp  open
443/tcp  open
Nmap done: 1 IP address (1 host up) scanned in 2.56 seconds
-=-=-=-=-=-=--=-=-=-=-=-=-=--=-=-=-=-=-=--=-=-=-=-=-
```

Based on the output above, which of the following ports listed as open represents the most significant security vulnerability to your network?

○ 22

○ 23

○ 53

○ 443

☆ Question 40:

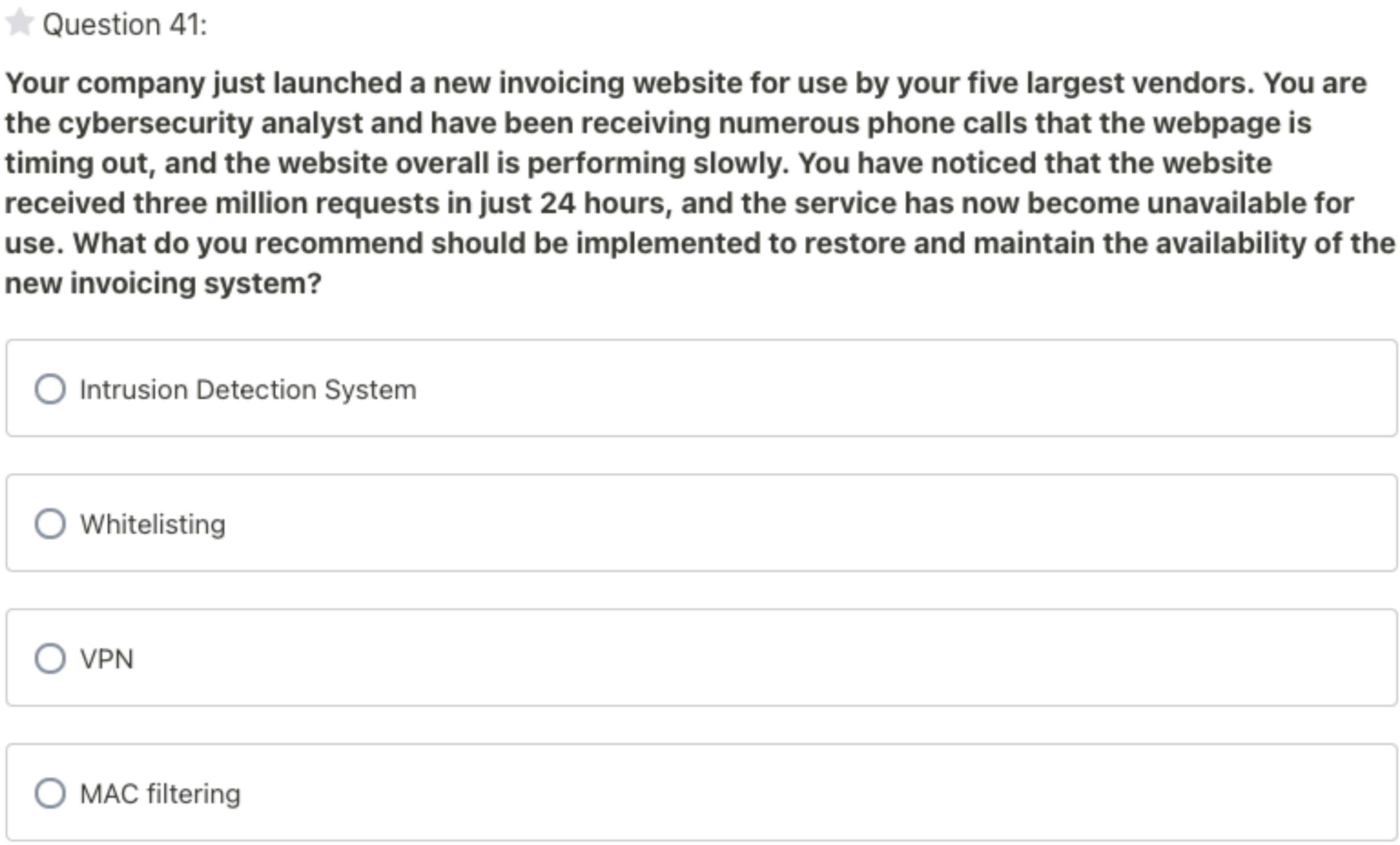
You have been investigating how a malicious actor could exfiltrate confidential data from a web server to a remote host. After an in-depth forensic review, you determine that a rootkit's installation had modified the web server’s BIOS. After removing the rootkit and reflash the BIOS to a known good image, what should you do to prevent the malicious actor from affecting the BIOS again?

○ Install an anti-malware application

○ Install a host-based IDS

○ Utilize secure boot

○ Utilize file integrity monitoring



Question 41:

Your company just launched a new invoicing website for use by your five largest vendors. You are the cybersecurity analyst and have been receiving numerous phone calls that the webpage is timing out, and the website overall is performing slowly. You have noticed that the website received three million requests in just 24 hours, and the service has now become unavailable for use. What do you recommend should be implemented to restore and maintain the availability of the new invoicing system?

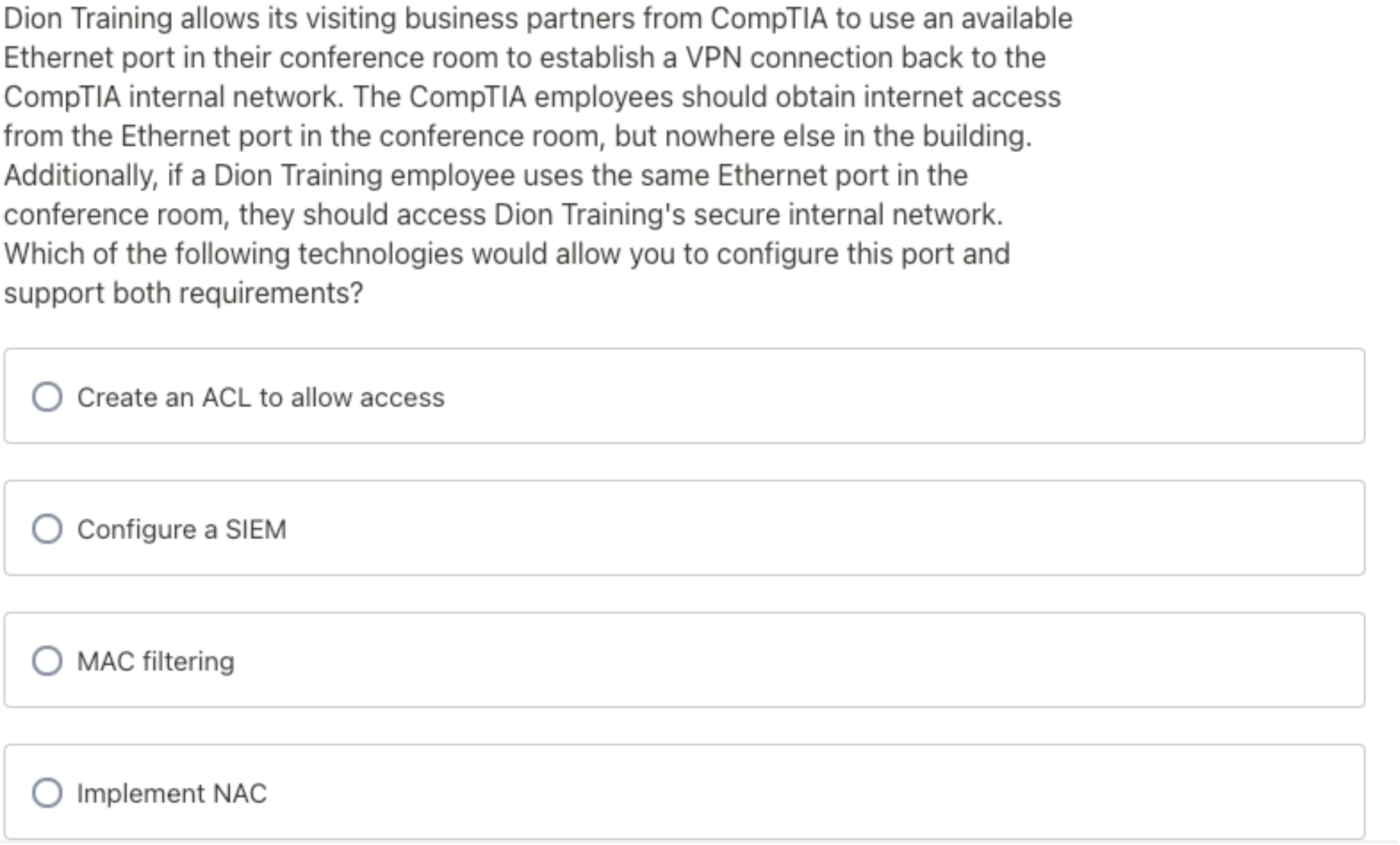
○ Intrusion Detection System

○ Whitelisting

○ VPN

○ MAC filtering

Question 42:



Dion Training allows its visiting business partners from CompTIA to use an available Ethernet port in their conference room to establish a VPN connection back to the CompTIA internal network. The CompTIA employees should obtain internet access from the Ethernet port in the conference room, but nowhere else in the building. Additionally, if a Dion Training employee uses the same Ethernet port in the conference room, they should access Dion Training's secure internal network. Which of the following technologies would allow you to configure this port and support both requirements?

○ Create an ACL to allow access

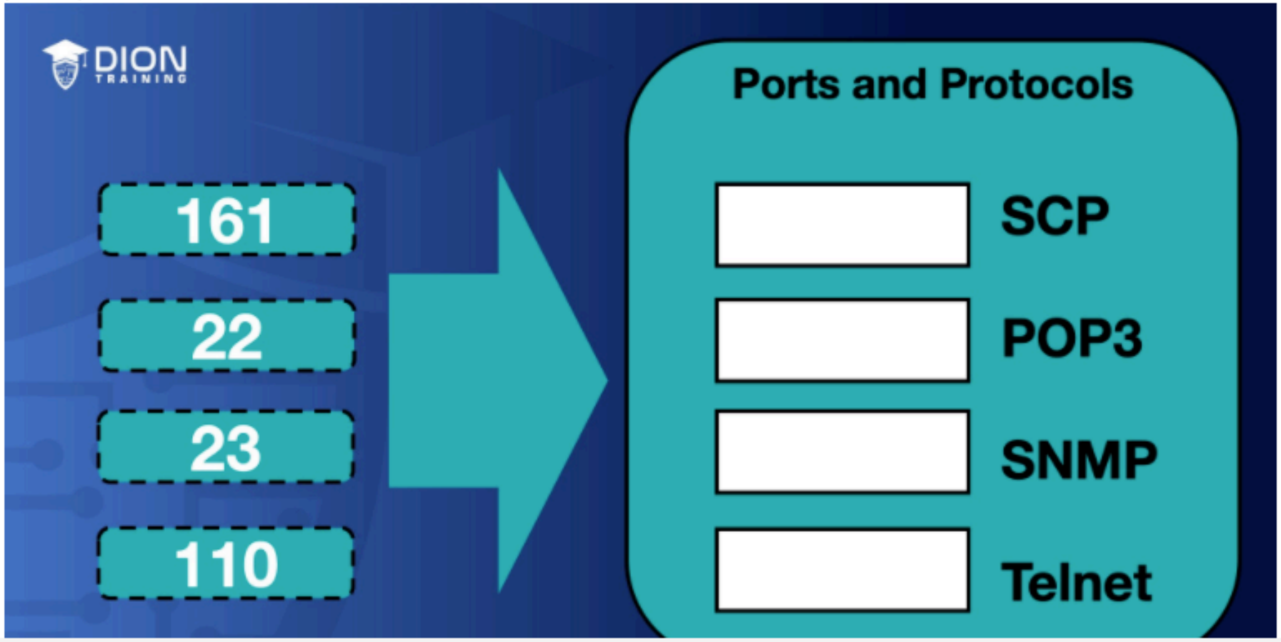
○ Configure a SIEM

○ MAC filtering

○ Implement NAC

Question 43:

(Sample Simulation – On the real exam for this type of question, you would have to rearrange the ports into the proper order by dragging and dropping them into place.)



DION TRAINING

Ports and Protocols

161

22

23

110

SCP

POP3

SNMP

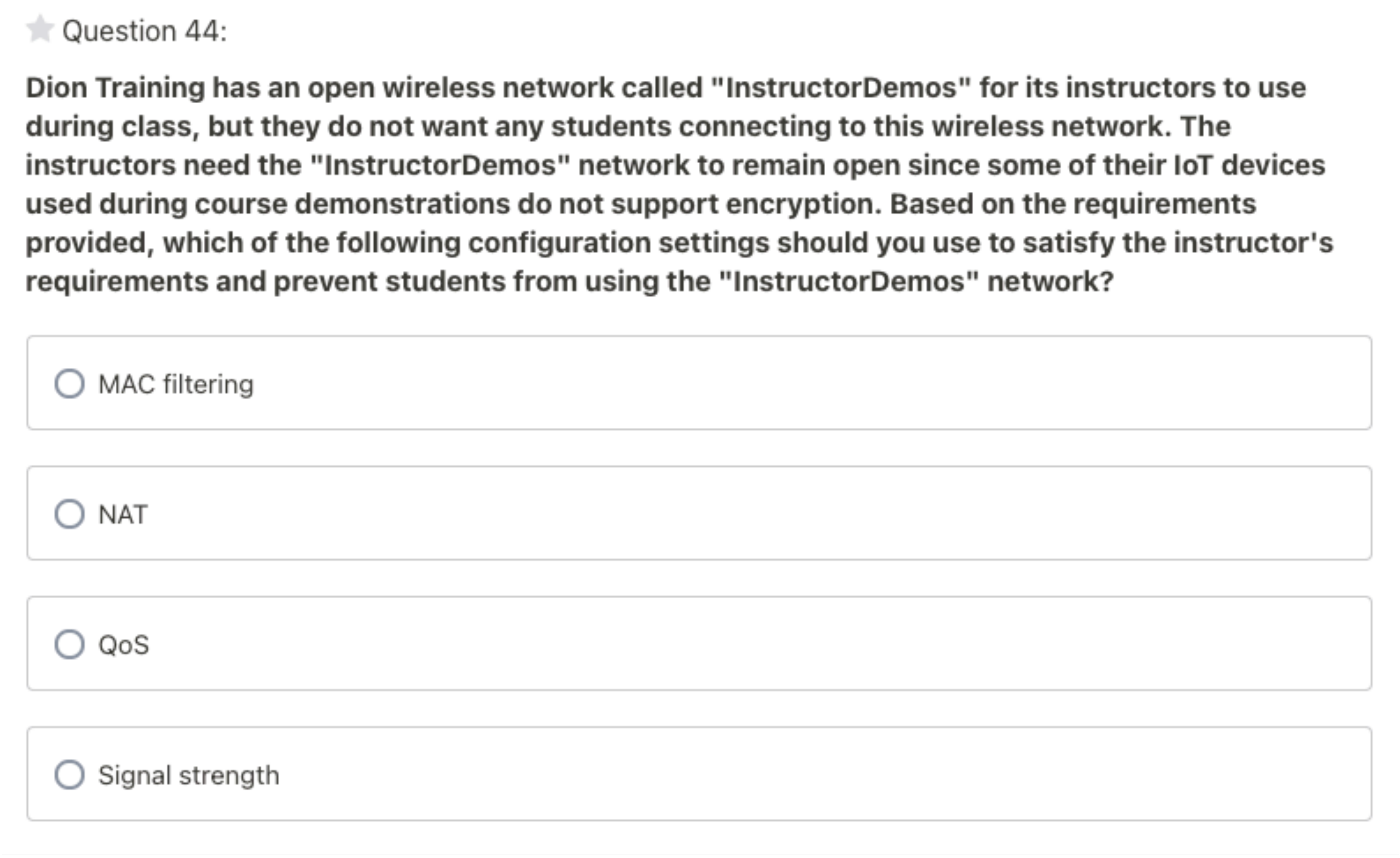
Telnet

○ 161, 22, 110, 23

○ 22, 110, 161, 23

○ 110, 161, 23, 22

○ 23, 110, 22, 161



Question 44:

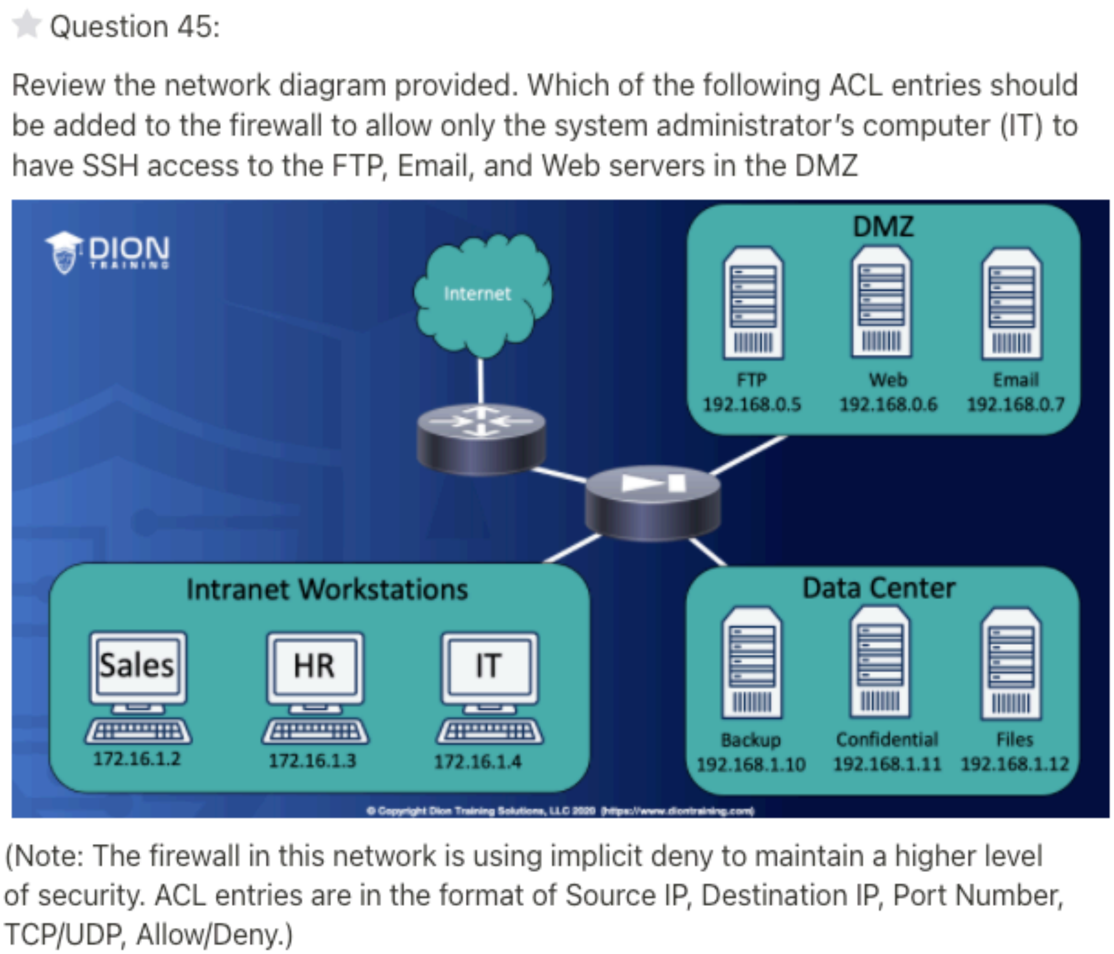
Dion Training has an open wireless network called "InstructorDemos" for its instructors to use during class, but they do not want any students connecting to this wireless network. The instructors need the "InstructorDemos" network to remain open since some of their IoT devices used during course demonstrations do not support encryption. Based on the requirements provided, which of the following configuration settings should you use to satisfy the instructor's requirements and prevent students from using the "InstructorDemos" network?

○ MAC filtering

○ NAT

○ QoS

○ Signal strength



☆ Question 45:

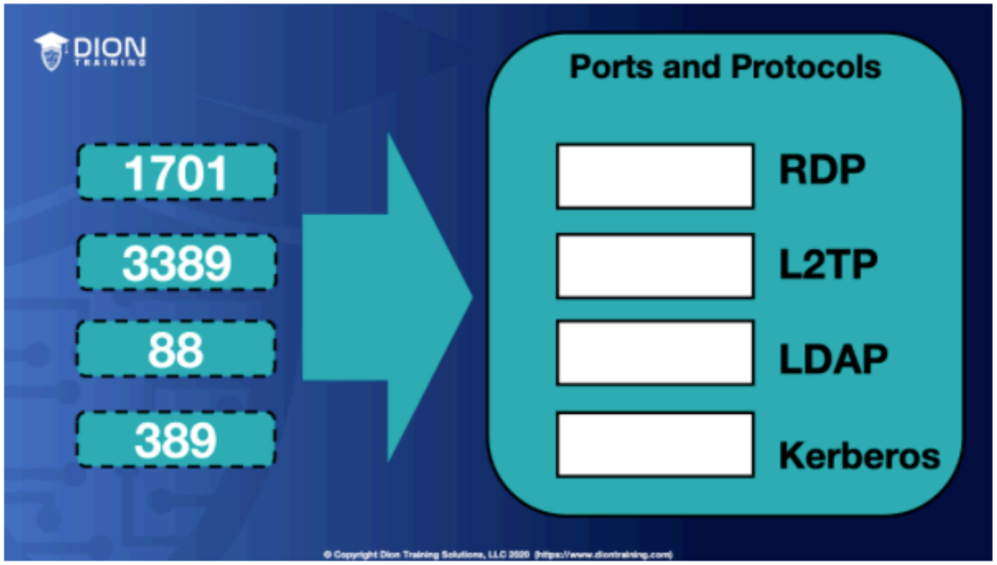
Review the network diagram provided. Which of the following ACL entries should be added to the firewall to allow only the system administrator's computer (IT) to have SSH access to the FTP, Email, and Web servers in the DMZ

(Note: The firewall in this network is using implicit deny to maintain a higher level of security. ACL entries are in the format of Source IP, Destination IP, Port Number, TCP/UDP, Allow/Deny.)

- ○ 172.16.1.0/24, 192.168.0.0/24, Any, TCP, Allow
- ○ 192.168.0.0/24, 172.16.1.4, 22, TCP, Allow
- ○ 192.168.0.3/24, 172.16.1.4, Any, TCP, Allow
- ○ 172.16.1.4, 192.168.0.0/24, 22, TCP, Allow

☆ Question 46:

(Sample Simulation – On the real exam for this type of question, you would have to rearrange the ports into the proper order by dragging and dropping them into place.)



Ports and Protocols

□ RDP

□ L2TP

□ LDAP

□ Kerberos

Using the image provided, place the port numbers in the correct order with their associated protocols

○ 3389, 1701, 389, 88

○ 88, 389, 3389, 1701

○ 1701, 3389, 88. 389

○ 389, 88, 1701, 3389

☆ Question 47:

A financial services company wants to donate some old hard drives from their servers to a local charity. Still, they are concerned about the possibility of residual data being left on the drives. Which of the following secure disposal methods would you recommend the company use?

○ Secure erase

○ Cryptographic erase

○ Zero-fill

○ Overwrite

★ Question 48:

You have been asked to install a computer in a public workspace. Only an authorized user should use the computer. Which of the following security requirements should you implement to prevent unauthorized users from accessing the network with this computer?

○ Issue the same strong and complex password for all users

○ Require authentication on wake-up

○ Disable single sign-on

○ Remove the guest account from the administrator group

Question 49:

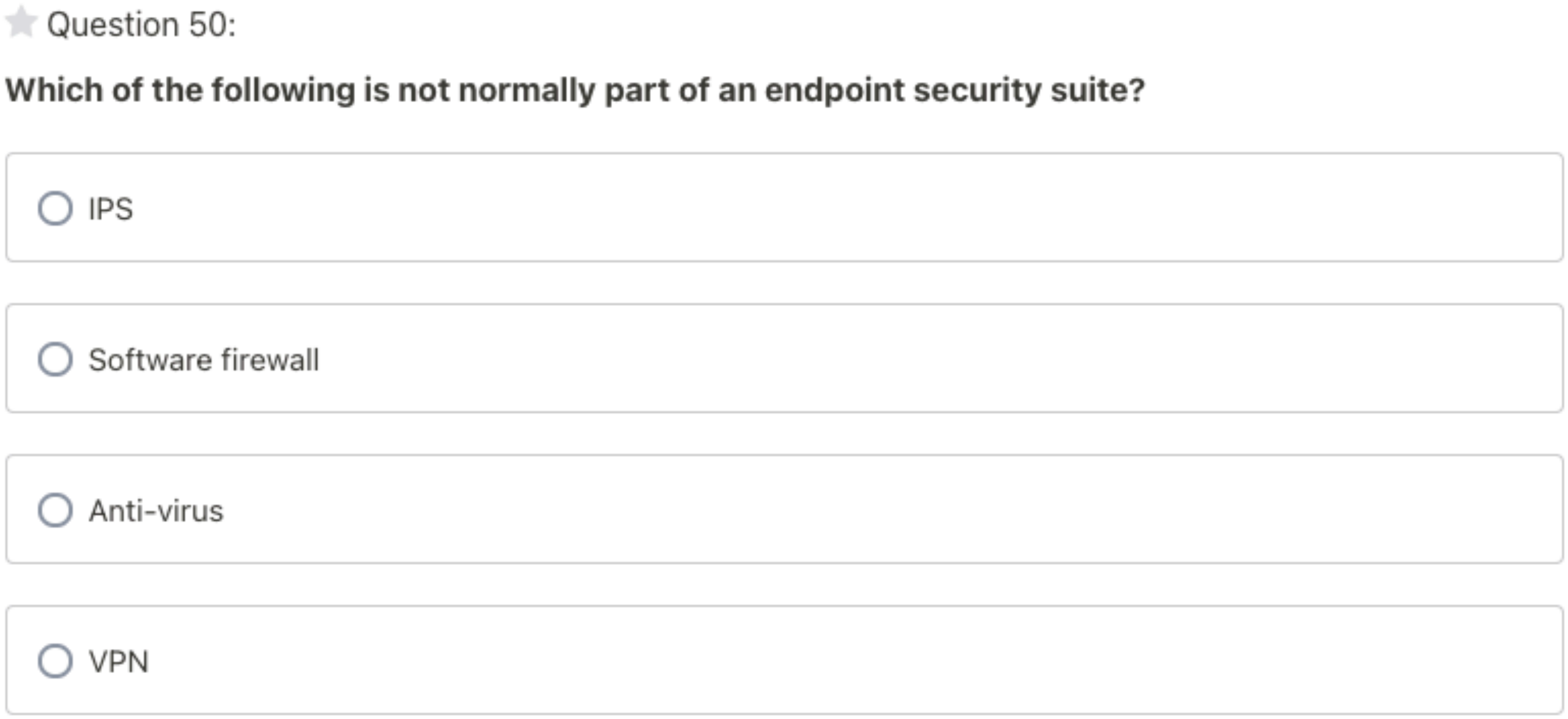
Which of the following is the LEAST secure wireless security and encryption protocol?

○ AES

○ WPA

○ WPA2

○ WEP



Question 50:

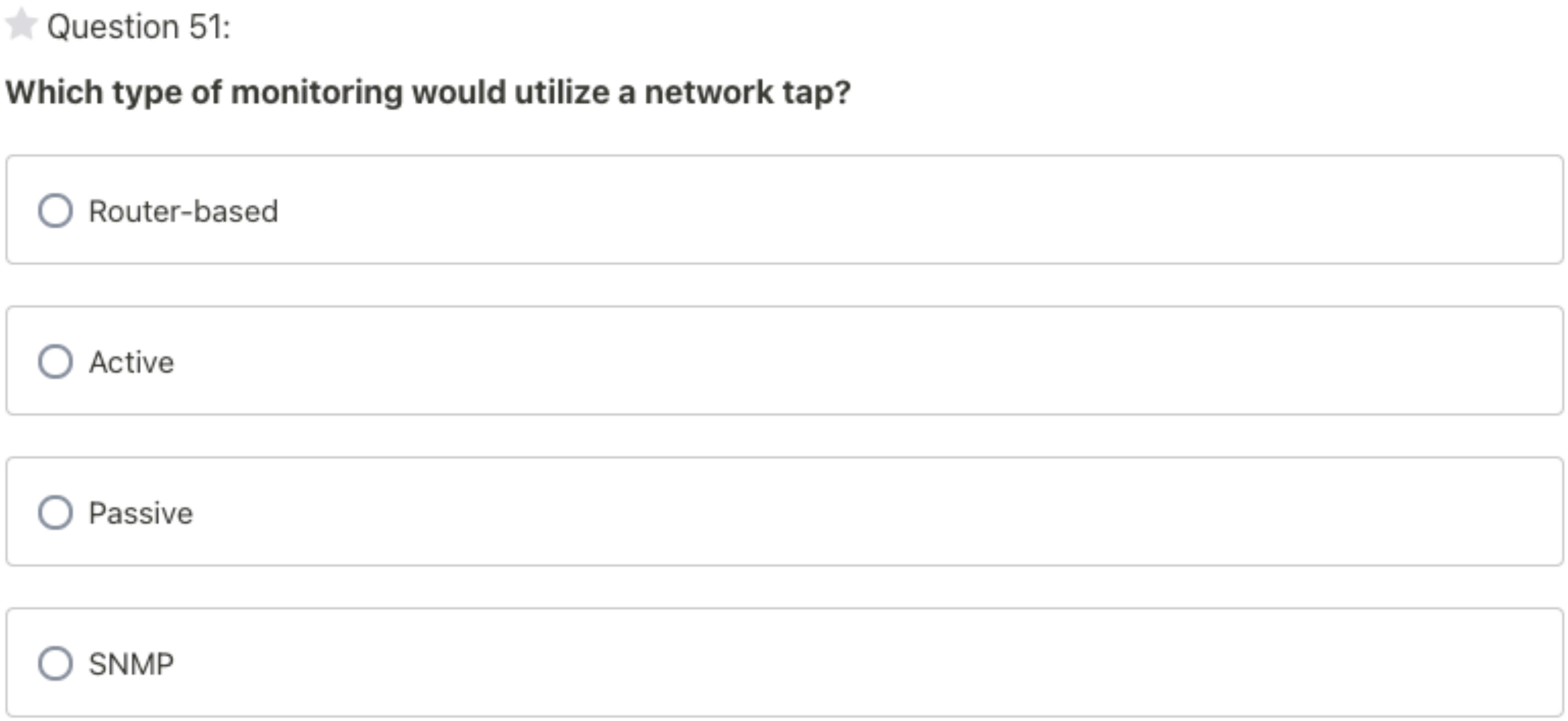
Which of the following is not normally part of an endpoint security suite?

○ IPS

○ Software firewall

○ Anti-virus

○ VPN



Question 51:

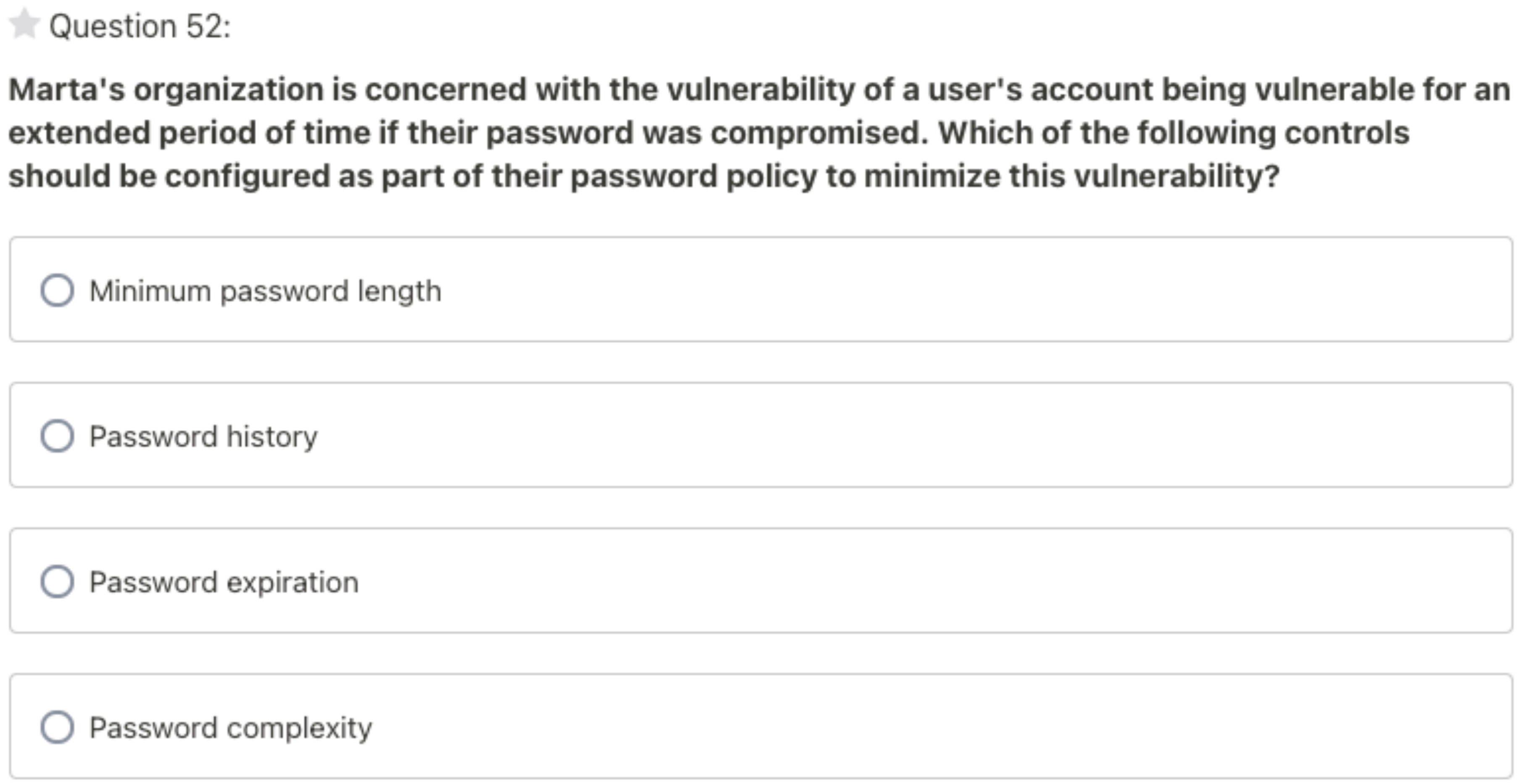
Which type of monitoring would utilize a network tap?

○ Router-based

○ Active

○ Passive

○ SNMP



☆ Question 52:

Marta's organization is concerned with the vulnerability of a user's account being vulnerable for an extended period of time if their password was compromised. Which of the following controls should be configured as part of their password policy to minimize this vulnerability?

○ Minimum password length

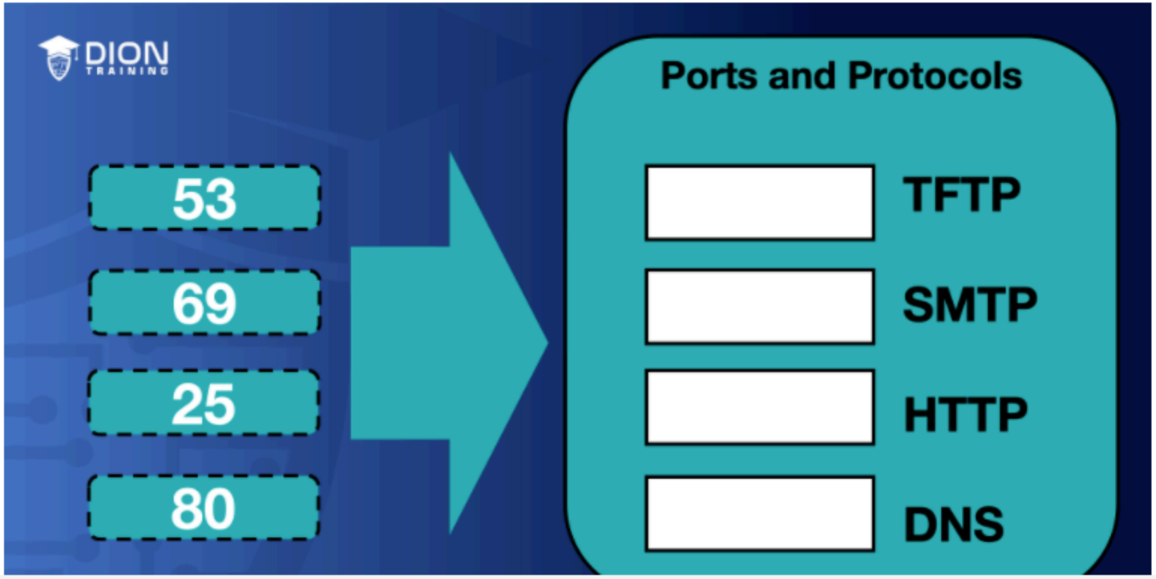
○ Password history

○ Password expiration

○ Password complexity

Question 53:

(Sample Simulation – On the real exam for this type of question, you would have to rearrange the steps into the proper order by dragging and dropping them into place.)



Ports and Protocols

53

69

25

80

TFTP

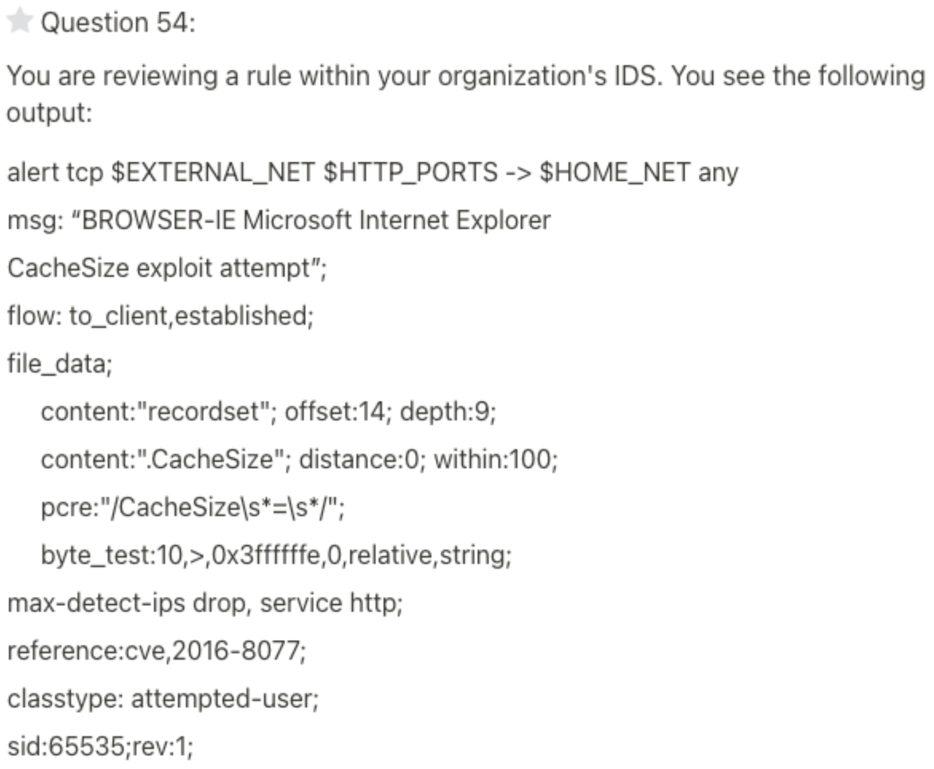
SMTP

HTTP

DNS

Using the image provided, place the port numbers in the correct order with their associated protocols

- ○ 53, 69, 25, 80
- ○ 80, 53, 69, 25
- ○ 69, 25, 80, 53
- ○ 25, 80, 53, 69



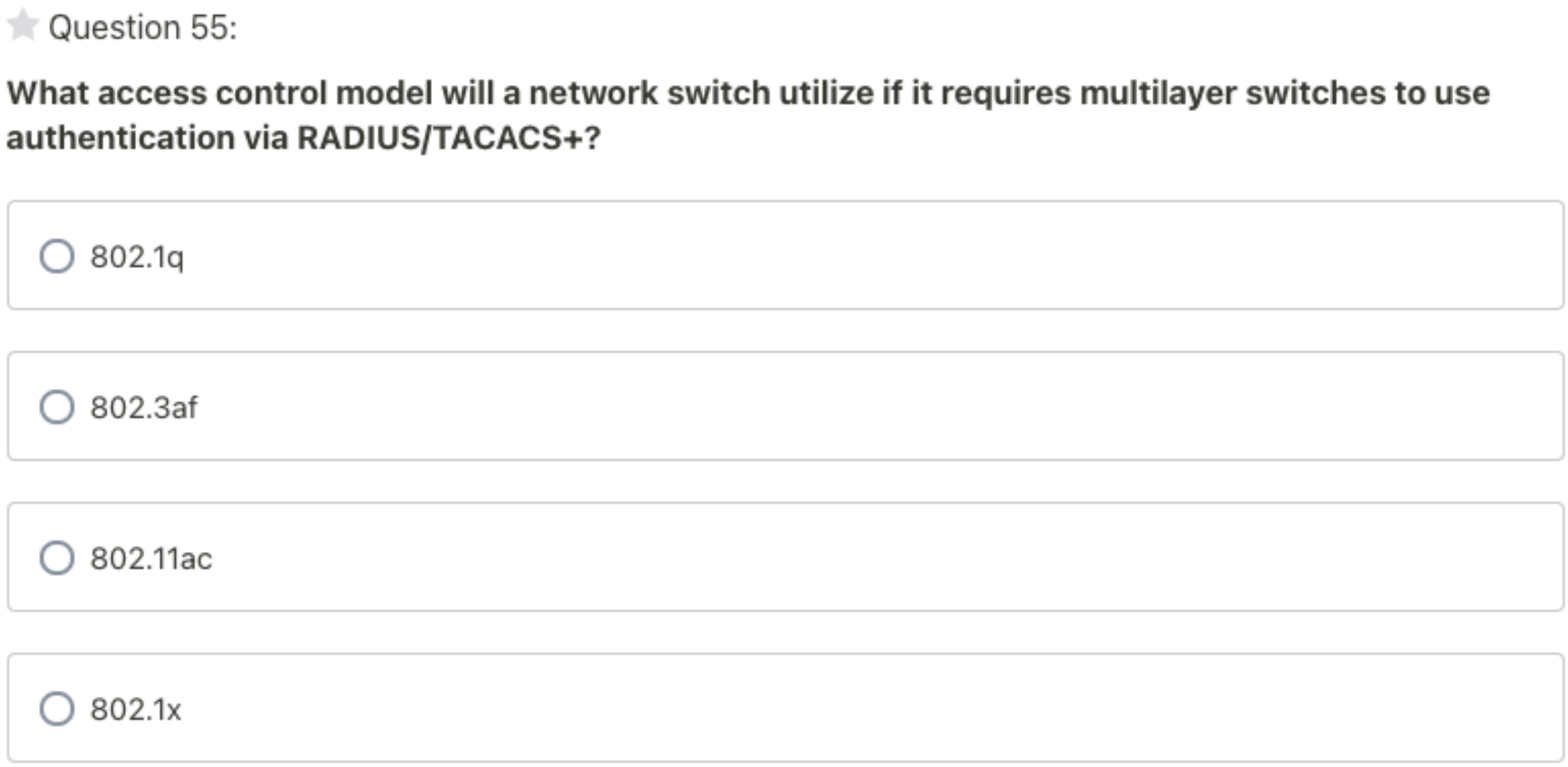
★ Question 54:

You are reviewing a rule within your organization's IDS. You see the following output:

```
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any
msg: "BROWSER-IE Microsoft Internet Explorer
CacheSize exploit attempt";
flow: to_client,established;
file_data;
   content:"recordset"; offset:14; depth:9;
   content:".CacheSize"; distance:0; within:100;
   pcre:"/CacheSize\s*=\s*/";
   byte_test:10,>,0x3ffffffe,0,relative,string;
max-detect-ips drop, service http;
reference:cve,2016-8077;
classtype: attempted-user;
sid:65535;rev:1;
```

Based on this rule, which of the following malicious packets would this IDS alerts on?

- ○ A malicious inbound TCP packet
- ○ Any malicious outbound packets
- ○ A malicious outbound TCP packet
- ○ Any malicious inbound packets



☆ Question 55:

What access control model will a network switch utilize if it requires multilayer switches to use authentication via RADIUS/TACACS+?

○ 802.1q

○ 802.3af

○ 802.11ac

○ 802.1x

Question 56:

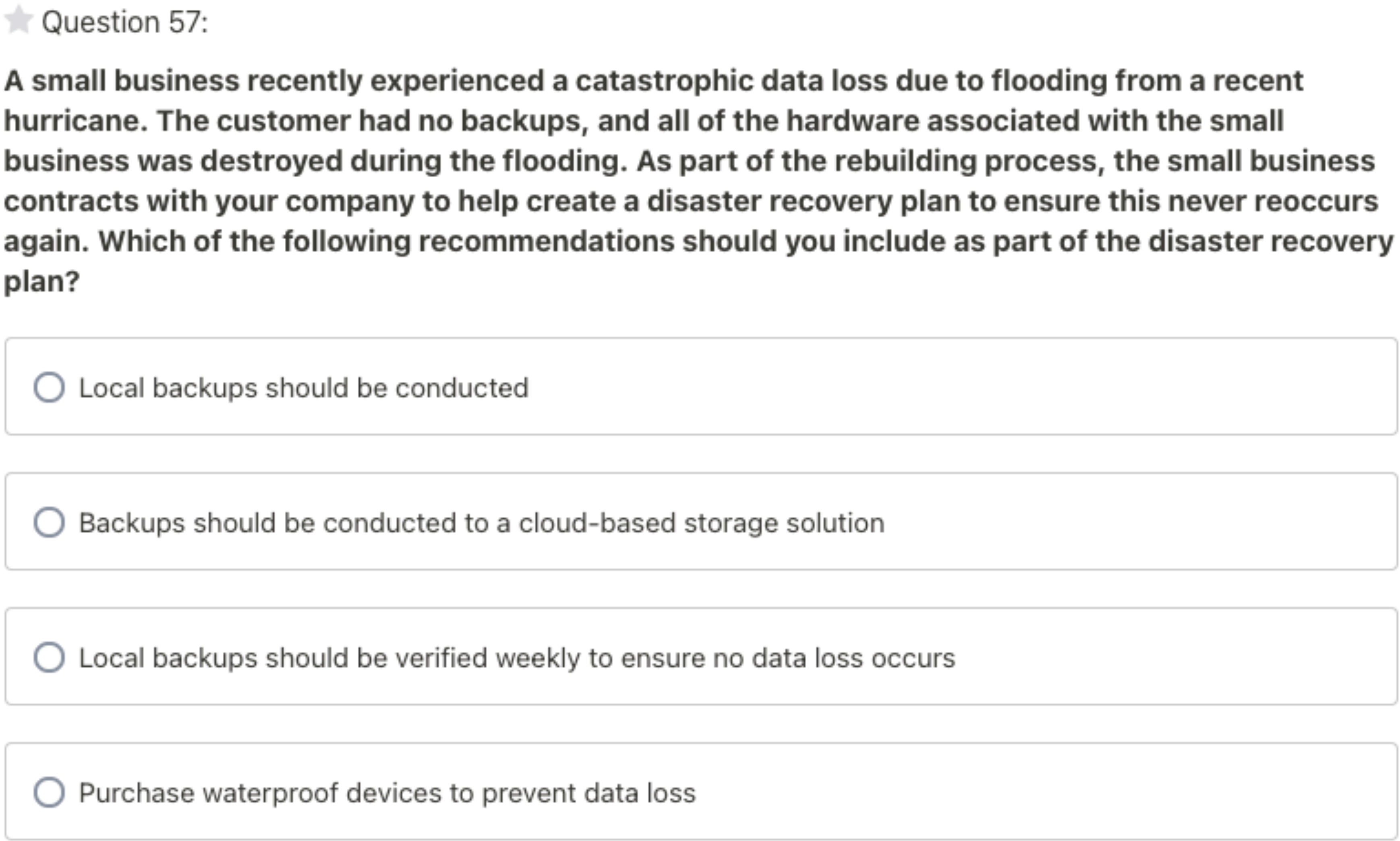
An attacker has compromised a virtualized server. You are conducting forensic analysis as part of the recovery effort but found that the attacker deleted a virtual machine image as part of their malicious activity. Which of the following challenges do you now have to overcome as part of the recovery and remediation efforts?

○ The attack widely fragmented the image across the host file system

○ File formats used by some hypervisors cannot be analyzed with traditional forensic tools

○ You will need to roll back to an early snapshot and then merge any checkpoints to the main image

○ All log files are stored within the VM disk image, therefore, they are lost



Question 57:

A small business recently experienced a catastrophic data loss due to flooding from a recent hurricane. The customer had no backups, and all of the hardware associated with the small business was destroyed during the flooding. As part of the rebuilding process, the small business contracts with your company to help create a disaster recovery plan to ensure this never reoccurs again. Which of the following recommendations should you include as part of the disaster recovery plan?

○ Local backups should be conducted

○ Backups should be conducted to a cloud-based storage solution

○ Local backups should be verified weekly to ensure no data loss occurs

○ Purchase waterproof devices to prevent data loss

☆ Question 58:

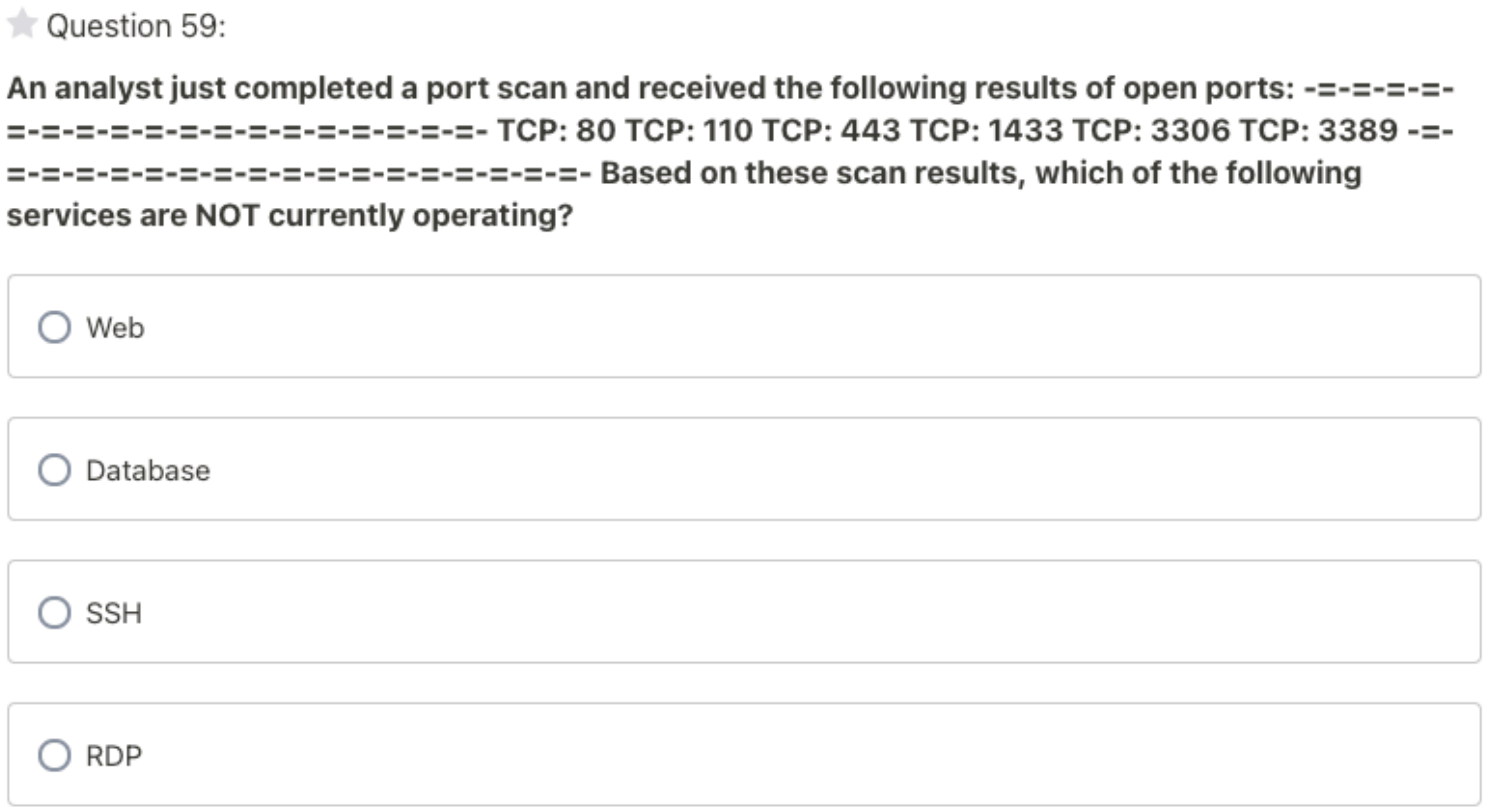
Which of the following items represents a document that includes detailed information on when an incident was detected, how impactful the incident was, how it was remediated, the effectiveness of the incident response, and any identified gaps that might require improvement?

○ Forensic analysis report

○ Chain of custody report

○ Trends analysis report

○ Lessons learned report



Question 59:

An analyst just completed a port scan and received the following results of open ports: -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- TCP: 80 TCP: 110 TCP: 443 TCP: 1433 TCP: 3306 TCP: 3389 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=- Based on these scan results, which of the following services are NOT currently operating?

○ Web

○ Database

○ SSH

○ RDP

Question 60:

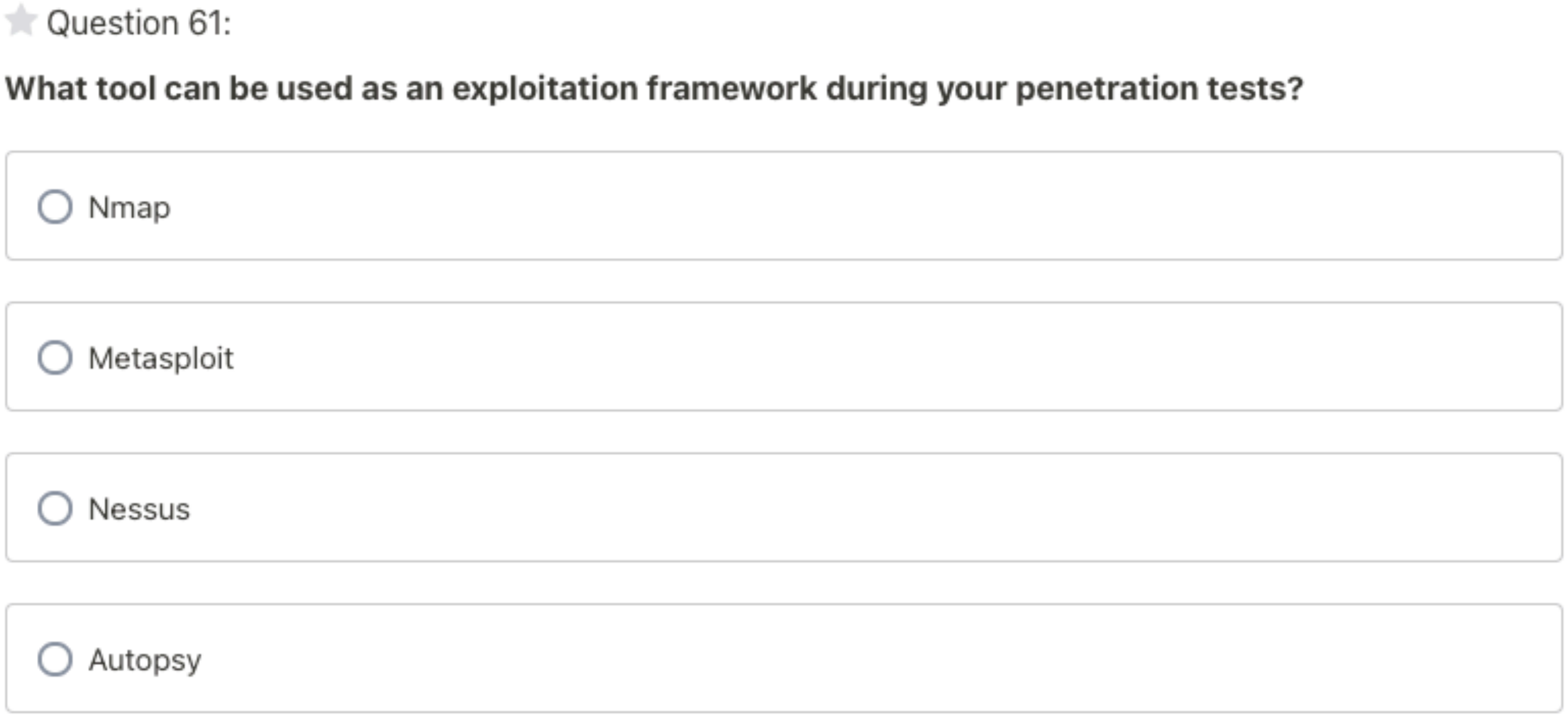
Which analysis framework makes no allowance for an adversary retreat in its analysis?

○ MITRE ATT&CK framework

○ Diamond Model of Intrusion Analysis

○ Lockheed Martin cyber kill chain

○ AlienVault (AT&T Cybersecurity) Cyber Kill Chain



Question 61:

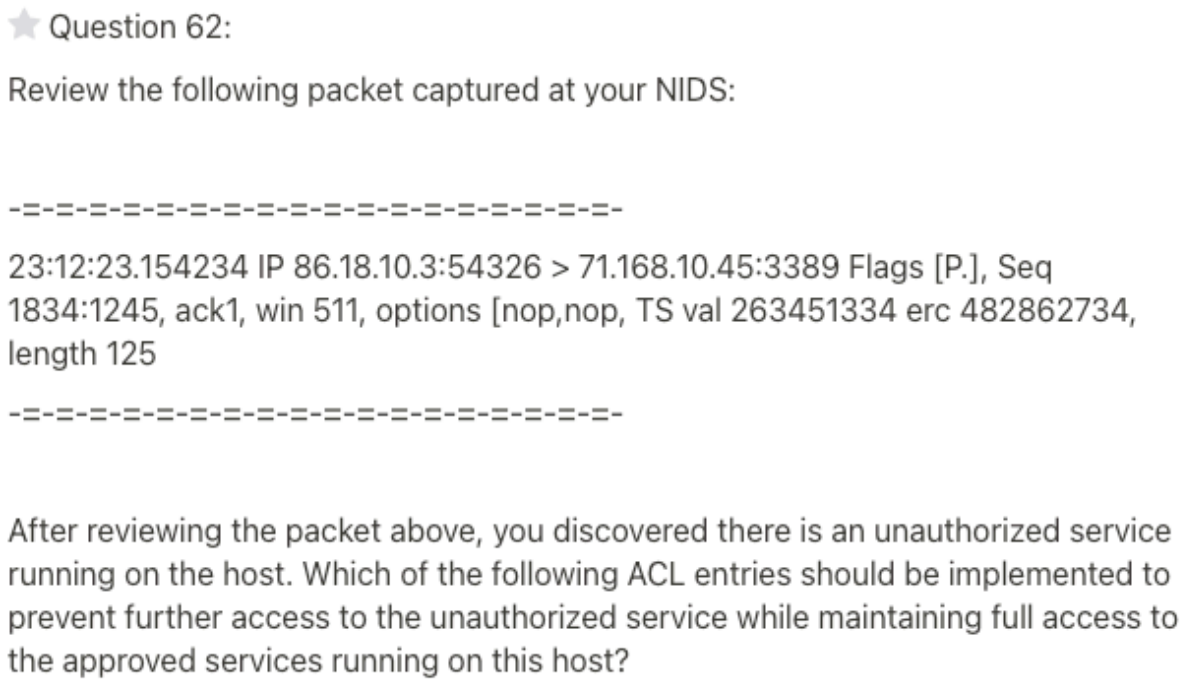
What tool can be used as an exploitation framework during your penetration tests?

○ Nmap

○ Metasploit

○ Nessus

○ Autopsy



Question 62:

Review the following packet captured at your NIDS:

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
23:12:23.154234 IP 86.18.10.3:54326 > 71.168.10.45:3389 Flags [P.], Seq
1834:1245, ack1, win 511, options [nop,nop, TS val 263451334 erc 482862734,
length 125
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

After reviewing the packet above, you discovered there is an unauthorized service running on the host. Which of the following ACL entries should be implemented to prevent further access to the unauthorized service while maintaining full access to the approved services running on this host?

○ DENY TCP ANY HOST 71.168.10.45 EQ 3389
○ DENY IP HOST 71.168.10.45 ANY EQ 25
○ DENY IP HOST 86.18.10.3 EQ 3389
○ DENY TCP ANY HOST 86.18.10.3 EQ 25

Question 63:

During which phase of the incident response process does an organization assemble an incident response toolkit?

○ Preparation

○ Detection and analysis

○ Containment, eradication, and recovery

○ Post-incident activity

☆ Question 64:

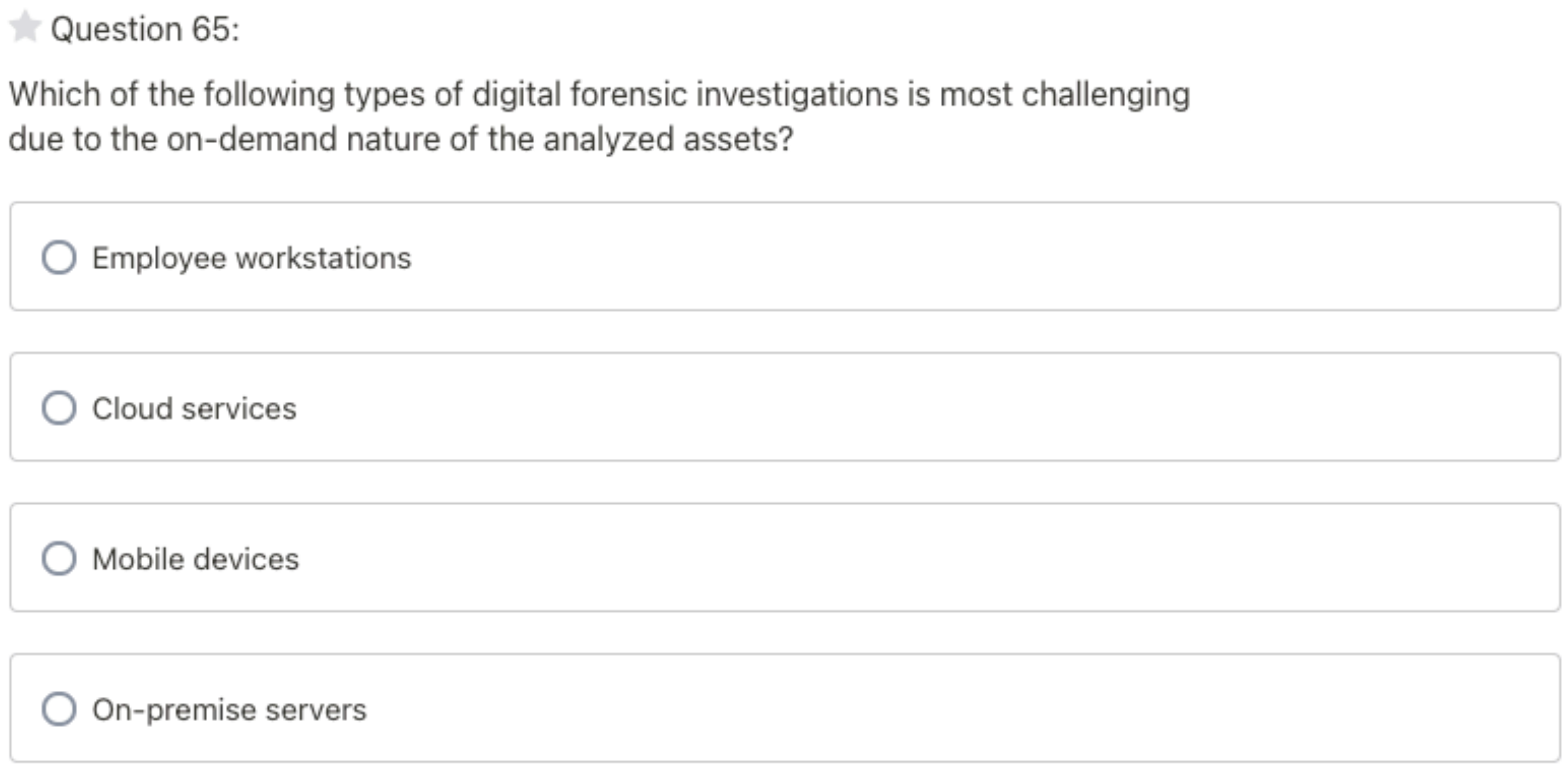
An attacker has issued the following command: nc -l -p 8080 | nc 192.168.1.76 443. Based on this command, what will occur?

○ Netcat will listen on the 192.168.1.76 interface for 443 seconds on port 8080

○ Netcat will listen on port 8080 and output anything received to a remote connection on 192.168.1.76 port 443

○ Netcat will listen for a connection from 192.168.1.76 on port 443 and output anything received to port 8080

○ Netcat will listen on port 8080 and then output anything received to local interface 192.168.1.76



Question 65:

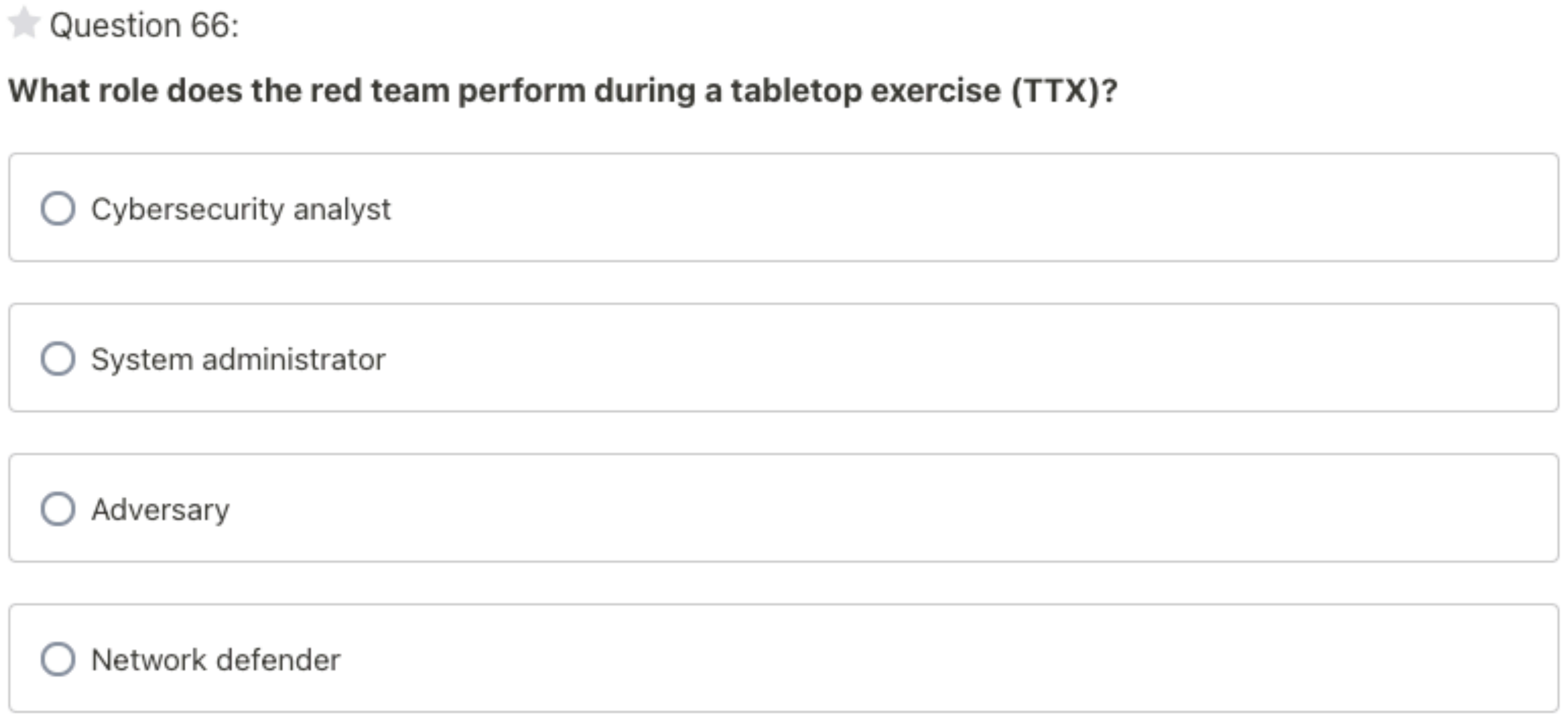
Which of the following types of digital forensic investigations is most challenging due to the on-demand nature of the analyzed assets?

○ Employee workstations

○ Cloud services

○ Mobile devices

○ On-premise servers



Question 66:

What role does the red team perform during a tabletop exercise (TTX)?

○ Cybersecurity analyst

○ System administrator

○ Adversary

○ Network defender

Question 67:

If you cannot ping a target because you are receiving no response or a response that states the destination is unreachable, then ICMP may be disabled on the remote end. If you wanted to elicit a response from a host using TCP, what tool would you use?

○ Hping

○ Traceroute

○ Ptunnel

○ Broadcast ping

Question 68:

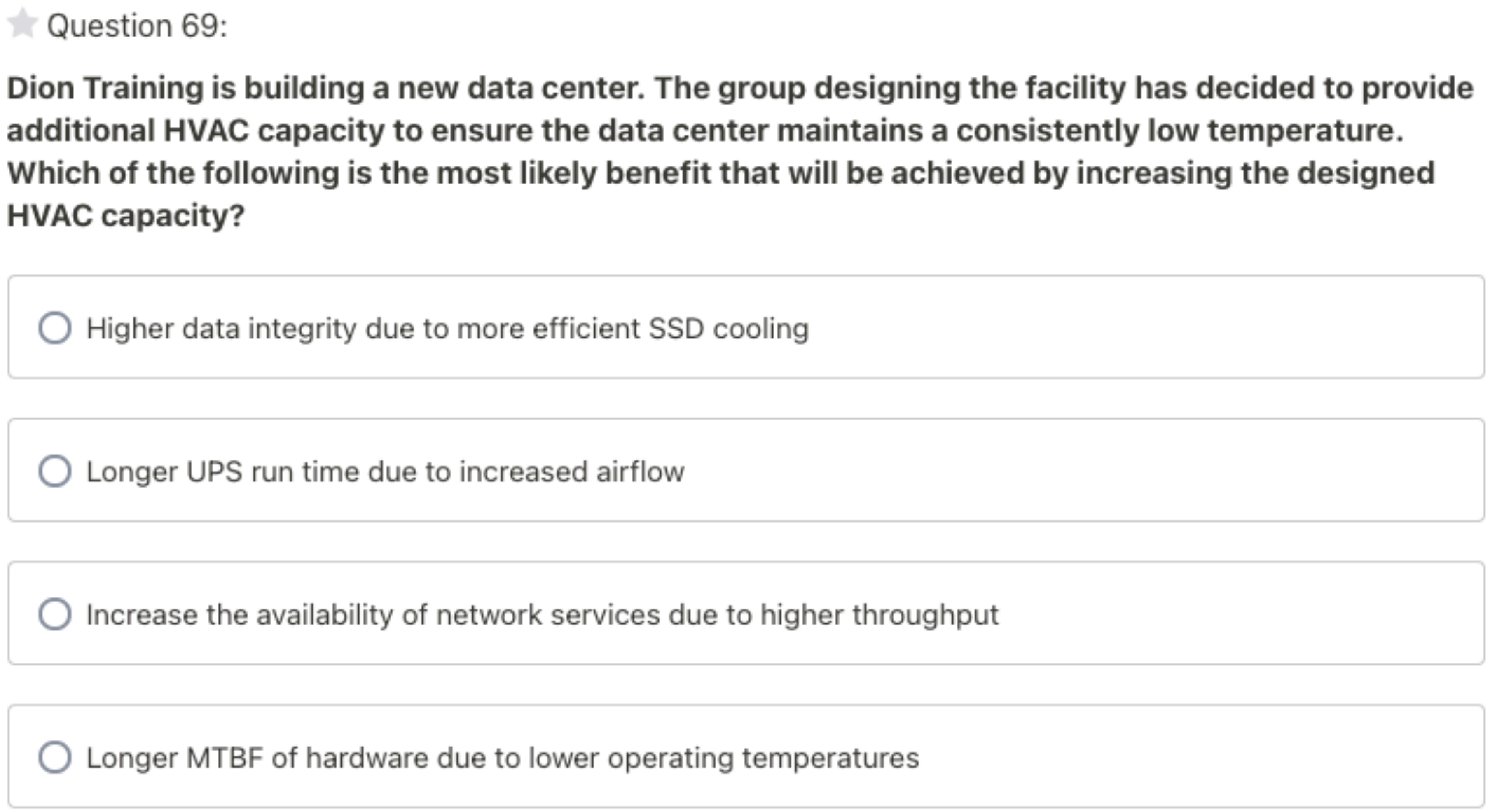
When your credit card data is written to the customer invoicing system at Dion Training, the first 12 digits are replaced with an x before storing the data. Which of the following privacy methods is being used?

○ Data masking

○ Tokenization

○ Data minimization

○ Anonymization



★ Question 69:

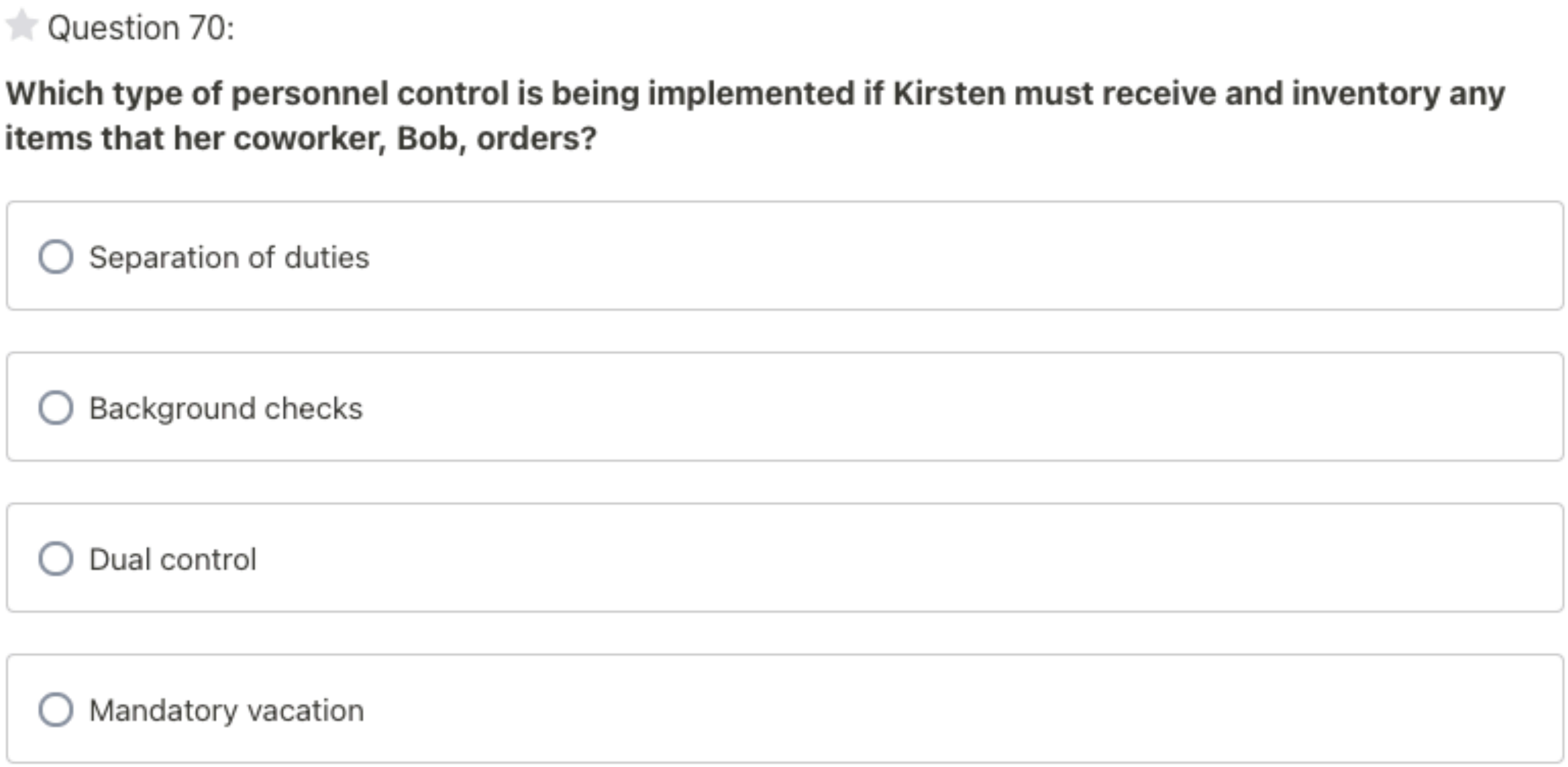
Dion Training is building a new data center. The group designing the facility has decided to provide additional HVAC capacity to ensure the data center maintains a consistently low temperature. Which of the following is the most likely benefit that will be achieved by increasing the designed HVAC capacity?

○ Higher data integrity due to more efficient SSD cooling

○ Longer UPS run time due to increased airflow

○ Increase the availability of network services due to higher throughput

○ Longer MTBF of hardware due to lower operating temperatures



Question 70:

Which type of personnel control is being implemented if Kirsten must receive and inventory any items that her coworker, Bob, orders?

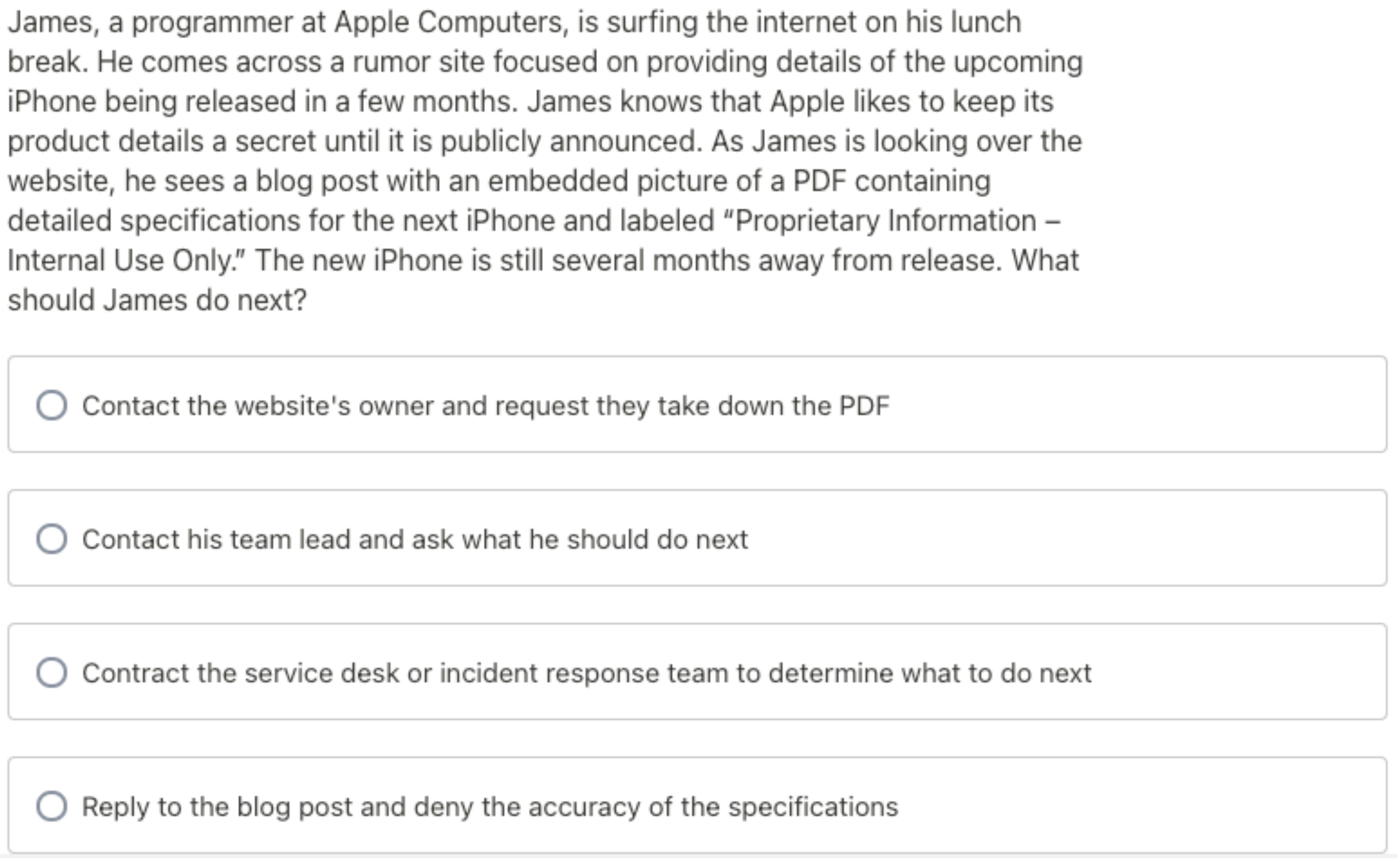
○ Separation of duties

○ Background checks

○ Dual control

○ Mandatory vacation

Question 71:



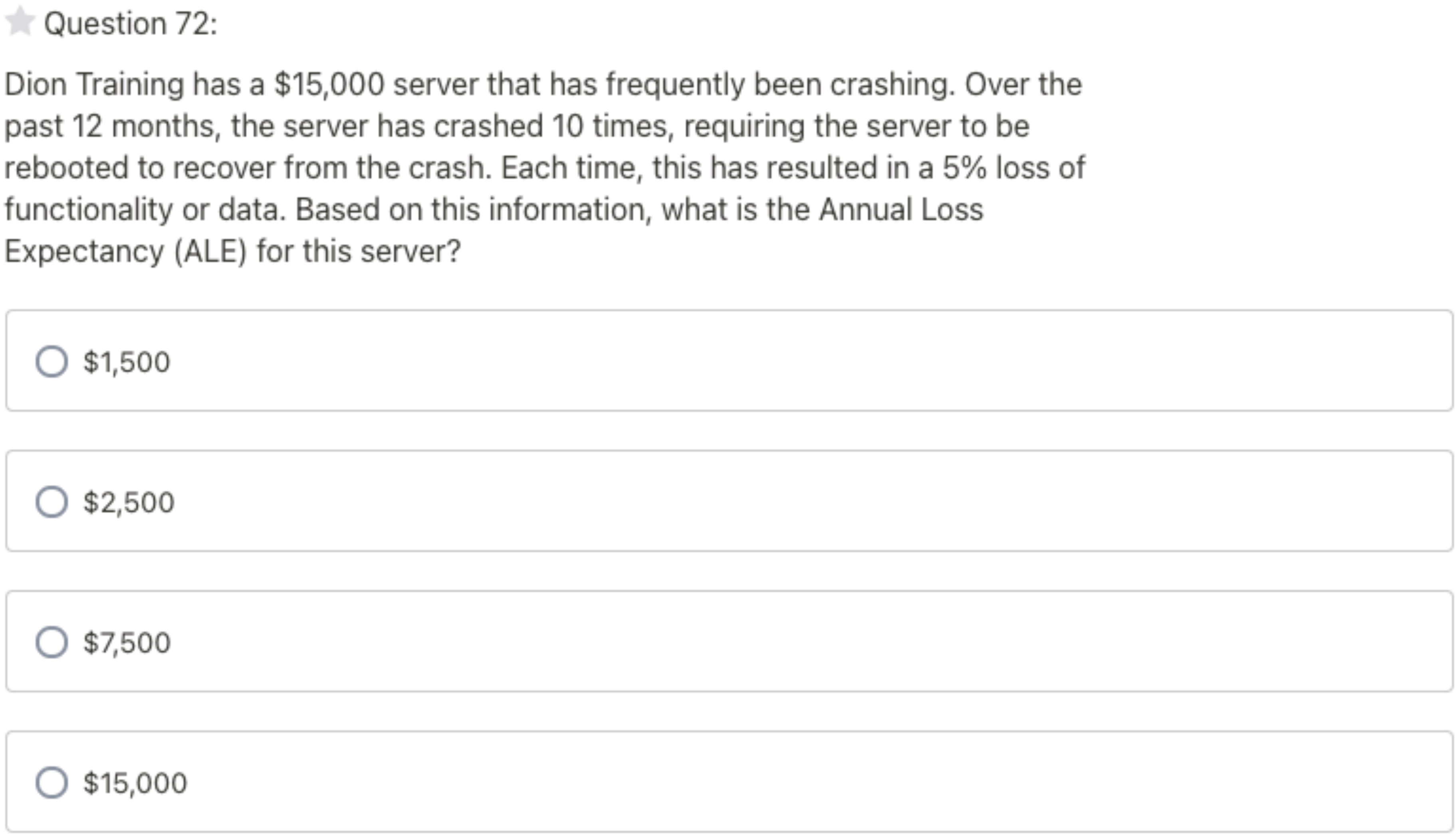
James, a programmer at Apple Computers, is surfing the internet on his lunch break. He comes across a rumor site focused on providing details of the upcoming iPhone being released in a few months. James knows that Apple likes to keep its product details a secret until it is publicly announced. As James is looking over the website, he sees a blog post with an embedded picture of a PDF containing detailed specifications for the next iPhone and labeled “Proprietary Information – Internal Use Only.” The new iPhone is still several months away from release. What should James do next?

○ Contact the website's owner and request they take down the PDF

○ Contact his team lead and ask what he should do next

○ Contract the service desk or incident response team to determine what to do next

○ Reply to the blog post and deny the accuracy of the specifications



Question 72:

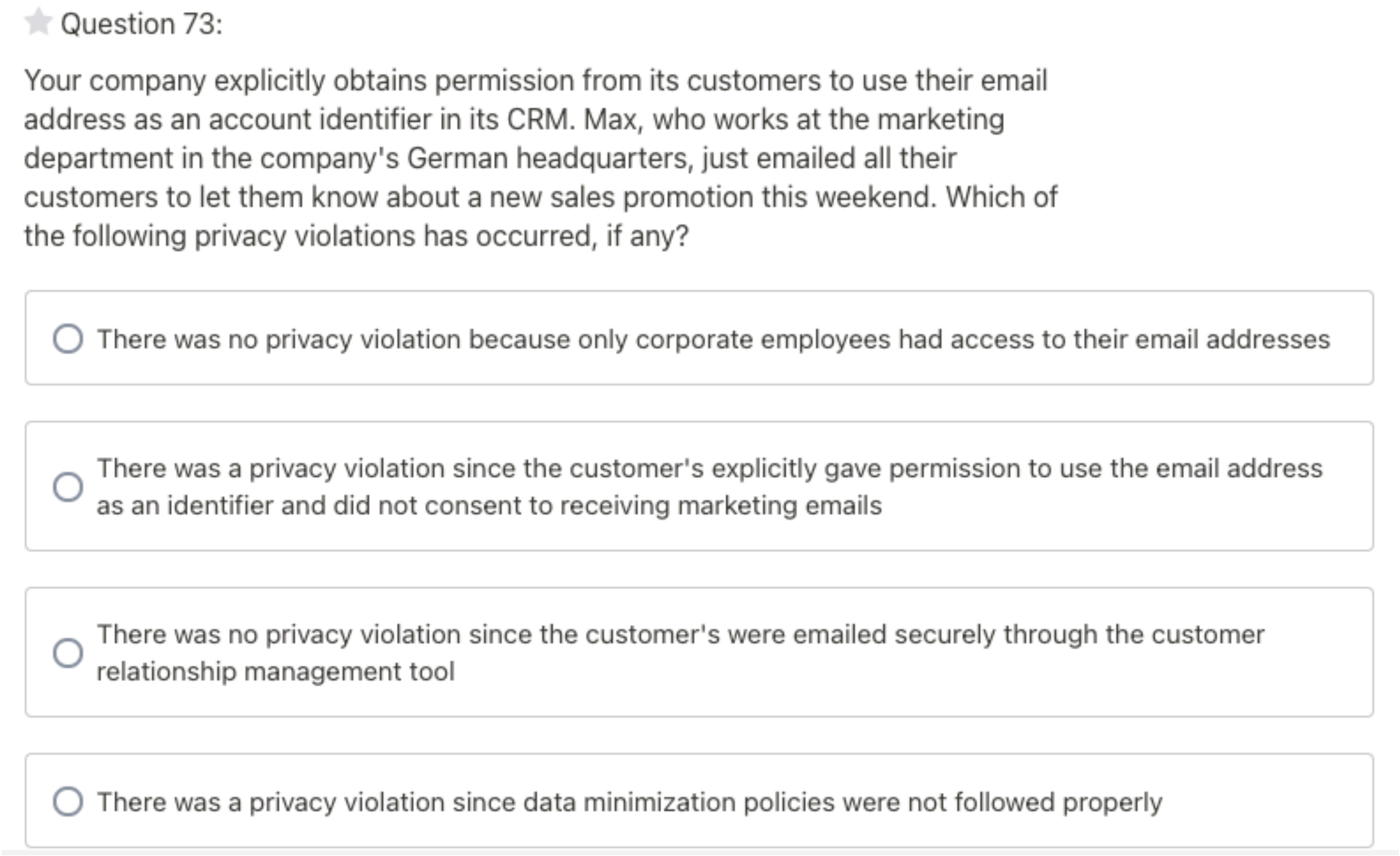
Dion Training has a $15,000 server that has frequently been crashing. Over the past 12 months, the server has crashed 10 times, requiring the server to be rebooted to recover from the crash. Each time, this has resulted in a 5% loss of functionality or data. Based on this information, what is the Annual Loss Expectancy (ALE) for this server?

○ $1,500

○ $2,500

○ $7,500

○ $15,000



Question 73:

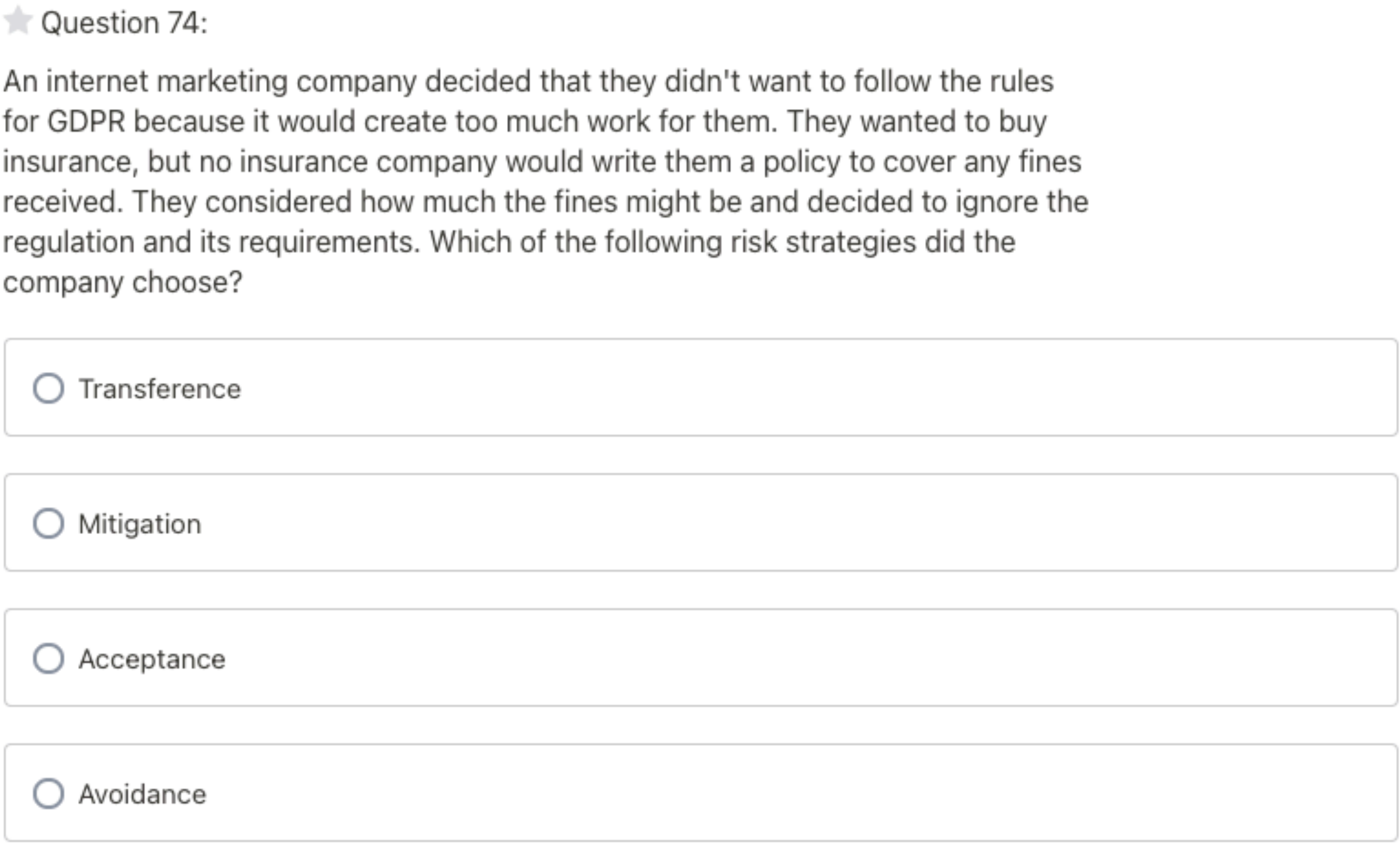
Your company explicitly obtains permission from its customers to use their email address as an account identifier in its CRM. Max, who works at the marketing department in the company's German headquarters, just emailed all their customers to let them know about a new sales promotion this weekend. Which of the following privacy violations has occurred, if any?

○ There was no privacy violation because only corporate employees had access to their email addresses

○ There was a privacy violation since the customer's explicitly gave permission to use the email address as an identifier and did not consent to receiving marketing emails

○ There was no privacy violation since the customer's were emailed securely through the customer relationship management tool

○ There was a privacy violation since data minimization policies were not followed properly



Question 74:

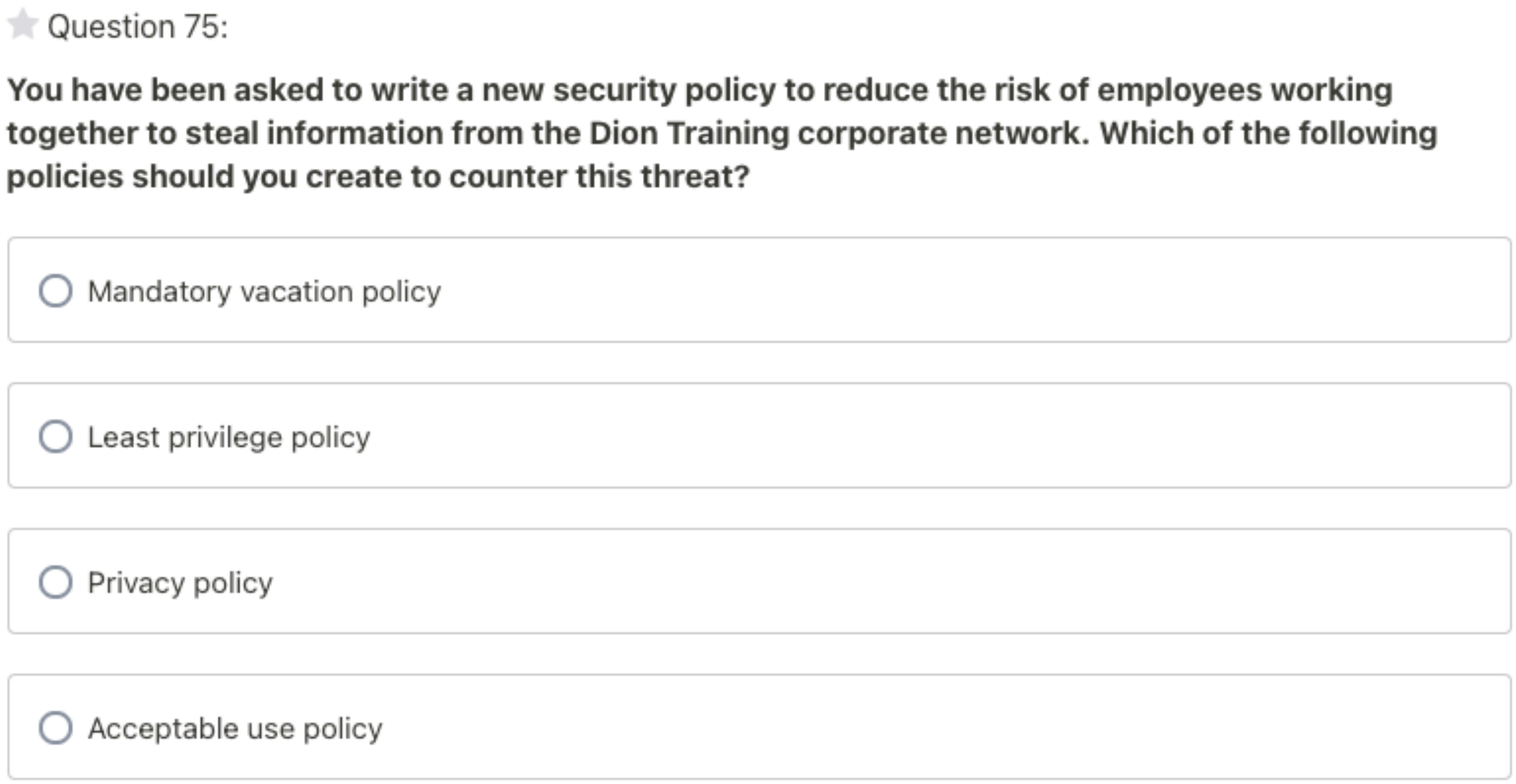
An internet marketing company decided that they didn't want to follow the rules for GDPR because it would create too much work for them. They wanted to buy insurance, but no insurance company would write them a policy to cover any fines received. They considered how much the fines might be and decided to ignore the regulation and its requirements. Which of the following risk strategies did the company choose?

○ Transference

○ Mitigation

○ Acceptance

○ Avoidance



☆ Question 75:

You have been asked to write a new security policy to reduce the risk of employees working together to steal information from the Dion Training corporate network. Which of the following policies should you create to counter this threat?

○ Mandatory vacation policy

○ Least privilege policy

○ Privacy policy

○ Acceptable use policy

☆ Question 76:

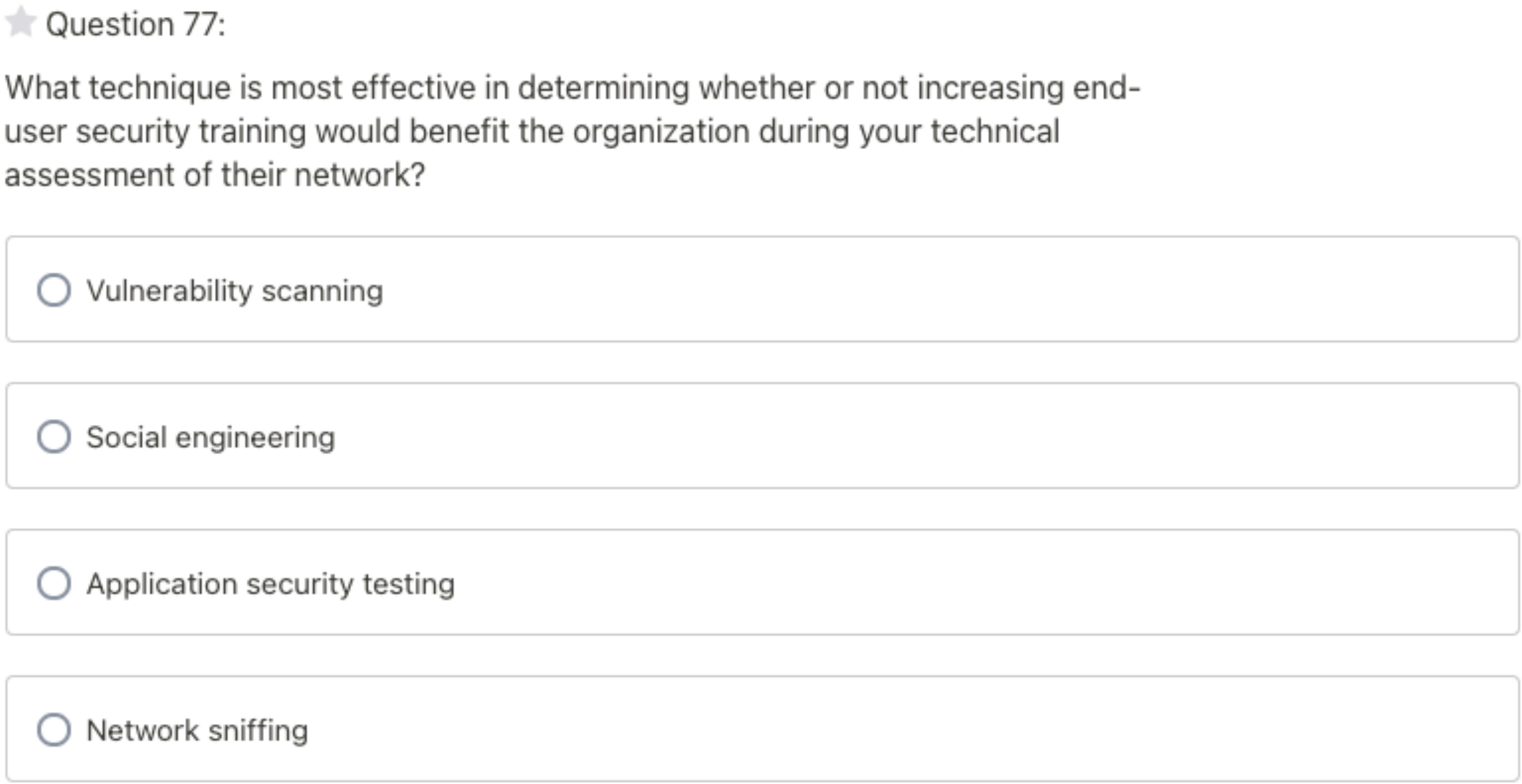
Following a root cause analysis of an edge router's unexpected failure, a cybersecurity analyst discovered that the system administrator had purchased the device from an unauthorized reseller. The analyst suspects that the router may be a counterfeit device. Which of the following controls would have been most effective in preventing this issue?

○ Increase network vulnerability scan frequency

○ Ensure all anti-virus signatures are up to date

○ Conduct secure supply chain management training

○ Verify that all routers are patched to the latest release



Question 77:

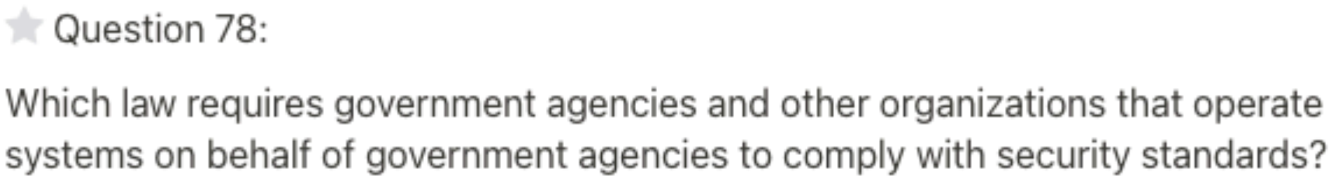
What technique is most effective in determining whether or not increasing end-user security training would benefit the organization during your technical assessment of their network?

○ Vulnerability scanning

○ Social engineering

○ Application security testing

○ Network sniffing



Question 78:

Which law requires government agencies and other organizations that operate systems on behalf of government agencies to comply with security standards?

- ○ FISMA
- ○ SOX
- ○ HIPPA
- ○ COPPA

Question 79:

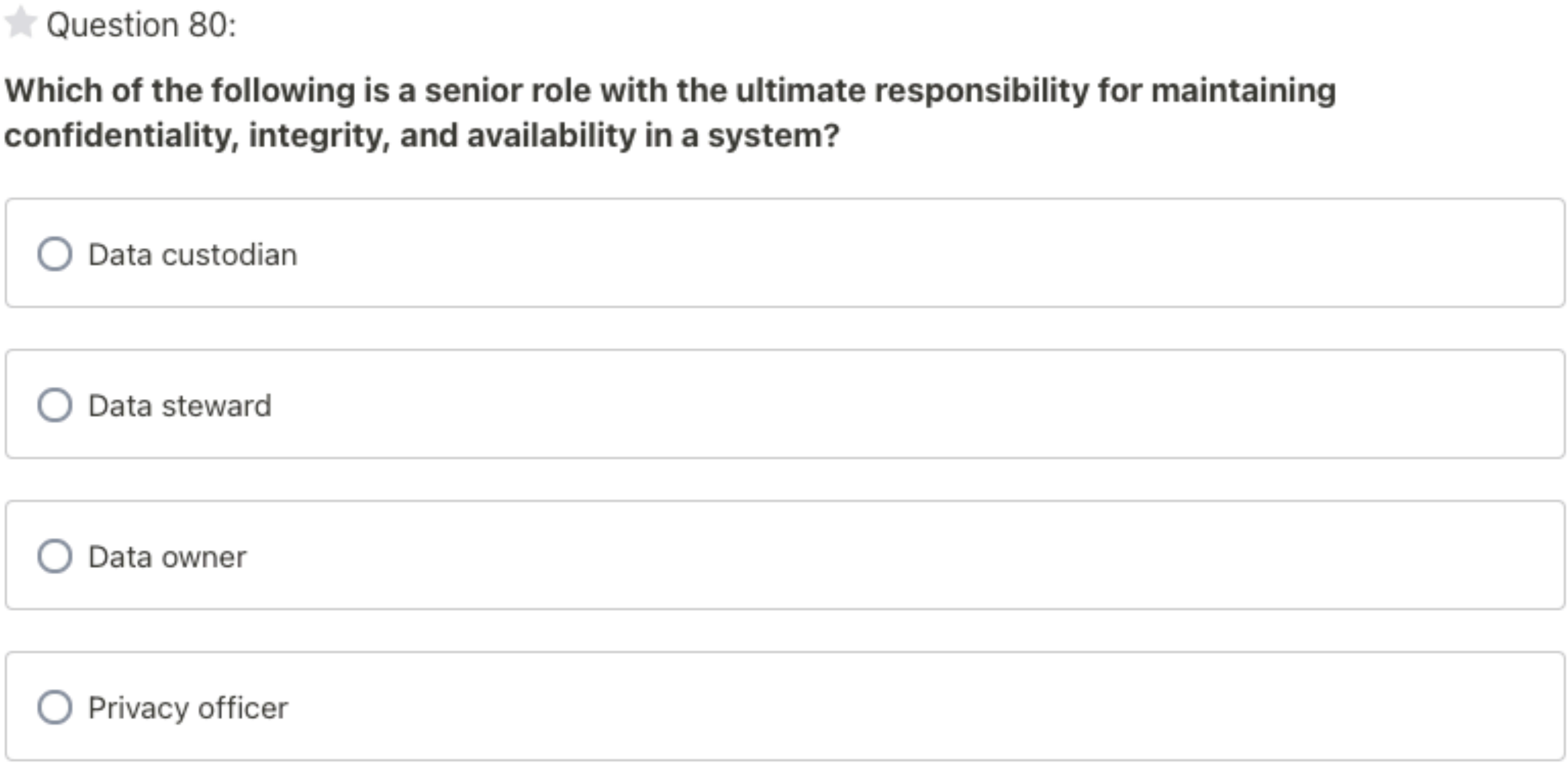
What type of malicious application does not require user intervention or another application to act as a host to replicate?

○ Macro

○ Worm

○ Trojan

○ Virus



★ Question 80:

Which of the following is a senior role with the ultimate responsibility for maintaining confidentiality, integrity, and availability in a system?

○ Data custodian

○ Data steward

○ Data owner

○ Privacy officer

Answer Key

1. vulnerability
2. SQL injection
3. Patching
4. The attachment is using a double file extension to mask its identity.
5. vishing
6. An uncredentialed scan of the network was performed.
7. PGP
8. Biometric authentication
9. RP
10. His email account requires multifactor authentication.
11. Spear phishing
12. Zero-day attacks
13. Logic bomb
14. Single quote
15. Spimming
16. False positive
17. Leaked personal files
18. Threat hunting
19. Directory traversal
20. APT
21. Password spraying
22. Telnet
23. Brute force attack
24. SaaS
25. Uninterruptable power supply
26. Community cloud
27. Honeypot
28. MSSP
29. Single-factor
30. DNS blackholing
31. TOTP
32. Proximity cards
33. MD5 or SHA1 hash digest of the file
34. Deterrent
35. Directing traffic to internal services if the contents of the traffic comply with the policy
36. 443
37. Faulty input validation
38. Password style
39. 23
40. utilize secure boot
41. Whitelisting
42. Implement NAC
43. 22, 110, 161, 23
44. MAC filtering
45. 172.16.1.4, 192.168.0.0/24, 22, TCP, ALLOW
46. 3389, 1701, 389, 88
47. Cryptographic erase
48. Require authentication on wake-up
49. WEP
50. VPN
51. PASSIVE
52. Password expiration
53. 69, 25, 80, 53
54. A malicious inbound TCP packet
55. 802.1x
56. The attack widely fragmented the image across the host file system
57. Backups should be conducted to a cloud-based storage solution
58. Lessons learned report
59. SSH
60. Lockheed Martin Cyber Kill Chain
61. Metasploit
62. DENY TCP ANY HOST 71.168.10.45 EQ 3389
63. Preparation
64. Netcat will listen on port 8080 and output anything received to a remote connection on 192.168.1.76 port 443.
65. Cloud services
66. Adversary
67. Hping
68. Data masking
69. Longer MTBF of hardware due to lower operating temperatures
70. Separation of duties
71. Contract the service desk or incident response team to determine what to do next.
72. $7,500
73. There was a privacy violation since the customer's explicitly gave permission to use the email address as an identifier and did not consent to receiving marketing email.
74. Acceptance
75. Mandatory vacation policy
76. Conduct secure supply chain management training.
77. Social engineering
78. FISMA
79. Worm
80. Data owner