EXAMTOPICS
- Expert Verified, Online, **Free**.

CERTIFICATION TEST
- CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Which of the following is the most important reason why tactics, techniques, and procedures (TTP) are beneficial to a defensive strategy?

A. TTP provides useful insights on the hash values and internet protocol addresses attributed to an attacker.

B. TTP provides useful insights on an attacker's indicators of compromise.

C. TTP provides useful insights on the tools used by an attacker.

D. TTP provides useful insights on the strategy and behavior of an attacker.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Which of the following is the best reason to heavily segment business-critical assets from within the network?

A. Legacy systems

B. Degraded functionality

C. Asset obfuscation

D. Proprietary server

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

A cybersecurity analyst receives an unstructured text document that contains advanced persistent threat (APT)-related indicators of compromise (IoCs). The analyst needs to extract the IPv4 addresses. Which of the following is the best tool to accomplish this task?

A. CyberChef

B. Wireshark

C. Zeek

D. Open Cyber Threat Intelligence (OpenCTI)

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

Which of the following best describes why operational technology (OT) devices use compensating controls?

A. Industrial control systems use significant network bandwidth.

B. Outage windows are usually scheduled.

C. Traditional IT security solutions may not be compatible.

D. OT devices are typically not encrypted.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

The Chief Information Security Officer (CISO) reviews the following security operations metrics from the last month:

Metric	Value	Notes
Alerts	3701	Raw SIEM alerts
Investigations	491	Actively investigated events
Incidents	5	Number of times incident was declared
Analyst hours	1400	Hours analysts spent investigating
Junior analysts	4	Total number of junior analysts
Senior analysts	7	Total number of senior analysts

Which of the following is the best action to improve overall security operations efficiency?

A. Leverage a cloud security posture management tool to add asset context to alerts.

B. Analyze and tune the detections that are causing non-actionable alerts.

C. Implement playbooks for the junior analysts to use during investigations.

D. Perform internal incident training on the most common alerts from security information and event management (SIEM).

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

A public threat intelligence report includes indicators of compromise (IoCs) for threat actors. The threat actors are exploiting a zero-day vulnerability that the vendor has not fixed. Which of the following techniques should be used until a patch is available?

A. Sinkholing

B. Eradication techniques

C. Continuous monitoring

D. Evidence acquisition

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 1*

The Chief Information Security Officer wants to improve internal security measures by continuously validating and verifying access to the production environment. Which of the following concepts best describes this practice?

A. Secure access service edge

B. Next-generation firewall

C. Zero Trust

D. Privileged access management

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

Which of the following allows an organization to leverage AI in various forms while protecting business objectives and data?

A. Usage policies

B. Prompt engineering

C. Non-disclosure agreement

D. Incident response policy

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

A security operations center analyst is using the command line to display specific traffic. The analyst uses the following command:
$tshark -r file.pcap -Y "http or udp"
Which of the following will the command line display?

A. Encrypted web requests and Domain Name System (DNS) traffic

B. Unencrypted web requests and DNS traffic

C. Neither encrypted nor unencrypted web and DNS traffic

D. Both encrypted and unencrypted web and DNS traffic

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which of the following network architectures would best implement a perimeter-less network topology?

A. Hybrid cloud networks

B. Secure access service edge

C. Cloud-native computing

D. Content delivery networks

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

A new security operations center (SOC) manager joins a team that struggles to meet service-level agreements (SLAs). The alert backlog continues to increase daily. Which of the following will the manager most likely need to do?

A. Automate escalation.

B. Improve the triage processes.

C. Upgrade threat intelligence.

D. Enhance the customer service response.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

Which of the following should a cybersecurity analyst utilize when a notification is inaccurate?

A. Data enrichment

B. Dashboard creation

C. Threat hunting

D. Alert tuning

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

A Chief Information Security Officer (CISO) evaluates a threat heat map and notices a substantial increase in custom scanning and enumeration activities. The CISO wants to gather as much information as possible about the activities targeting the company to help prioritize mitigations. Which of the following solutions is the best way to accomplish this goal?

A. Configuring a honeypot in a separate environment to gather attacker techniques

B. Leveraging canary tokens on all production systems to detect valid intrusion attempts

C. Subscribing to information-sharing and threat intelligence reports for the industry

D. Implementing a web application firewall in front of all applications and having it log attacks

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

An analyst uses an AI platform to help correlate events. The AI output contains events that did not happen. This results in inaccurate correlations. Which of the following best describes what has occurred?

A. Hallucinations

B. Data exposure

C. Malicious prompts

D. Model poisoning

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

A security analyst must identify documents that contain encoded ActiveMime payloads in a directory containing thousands of files. The analyst runs the following command: grep -rail ActiveMime *
The command returns no output. Which of the following Yet Another Recursive Acronym (YARA) rules should the analyst use to find the suspicious files?

A.
```
rule activemime {
  strings:
    $p="%PDF"
    $a="ActiveMime" fullword
  condition"
    $p at 0 and $a
}
```

B.
```
rule activemime {
  strings:
    $p="%PDF"
    $a="ActiveMime" nocase
  condition"
    $p at 0 and $a
}
```

C.
```
rule activemime {
  strings:
    $p="%PDF"
    $a="ActiveMime" base64
  condition"
    $p at 0 and $a
}
```

D.
```
rule activemime {
  strings:
    $p="%PDF"
    $a="ActiveMime" ascii
  condition"
    $p at 0 and $a
}
```

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

An analyst executes the top command on a Linux system for an unresponsive application and observes the following output:

```
PID     USER        %CPU        %MEM     COMMAND
6651    xrdp        6.3         0.2      xrdp
7316    comptia     0.3         0.1      top
7583    root        91.2        96       python
6680    comptia     0.7         0.1      kworker
```

Which of the following is the most likely cause of this issue?

A. Service disruption

B. Unauthorized software

C. Resource exhaustion

D. Filesystem changes

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

Which of the following is the most difficult for threat actors to change according to the Pyramid of Pain model?

A. Tactics, techniques, and procedures

B. Tools

C. Domain names

D. Internet Protocol addresses

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

An analyst is assigned to a new cybersecurity improvement project. The analyst wants to better understand the workflow processes and the skill set of the cybersecurity engineers on this task force. The analyst sets up a recurring, weekly conference call. Which of the following best describes the purpose for the conference call?

A. To conduct incident response training

B. To create vendor information sessions

C. To manage and facilitate team coordination

D. To respond to customer requirements

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

A security analyst uses a full pcap solution to extract all traffic from the last two days associated with the 10.213.4.27 file server. This file server is under investigation due to concerns about potential data exfiltration using Domain Name System (DNS) traffic. Which of the following commands should the analyst use to extract any potentially leaked data from the suspicious.pcap file?

A. strings suspicious.pcap | grep 10.213.4.27

B. zeek -r suspicious.pcap ; grep 10.213.4.27 file.log

C. snort -r suspicious.pcap ; grep eve.log 10.213.4.27

D. tcpdump -r suspicious.pcap port 53 and host 10.213.4.27

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

An analyst is configuring a security information and event management system to capture fileless malware execution events. Which of the following log files requires additional configuration to accomplish this task?

A. Microsoft-Windows-Crypto-DPAPI/Operational

B. Microsoft-Windows-PowerShell/Operational

C. Microsoft-Windows-UserPnp/DeviceInstall

D. Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

A binary file that might contain malicious code is hosted on an isolated machine. An analyst wants to quickly detect the malicious code. Which of the following should the analyst use?

A. strings

B. VirusTotal

C. WHOIS

D. Yet Another Recursive Acronym (YARA)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

A security analyst analyzes the output of a web application access log for a company based in the United States. Given the following output:

datetime	username	status	sip_address	region
07-12-2025 09:01:00Z	tlindy	failed	63.102.4.78	US
07-12-2025 09:02:00Z	tlindy	success	63.102.4.78	US
07-12-2025 09:03:00Z	jschott	failed	185.23.154.24	RU
07-12-2025 09:07:00Z	ssanford	success	63.102.4.71	US
07-12-2025 09:08:00Z	mschultz	success	63.102.4.74	US
07-12-2025 09:08:00Z	jschott	failed	185.23.154.22	RU
07-12-2025 09:10:00Z	wlangey	success	63.102.4.79	US
07-12-2025 09:14:00Z	pking	failed	185.23.127.21	RU
07-12-2025 09:15:00Z	tlindy	success	185.87.14.12	RU
07-12-2025 09:13:00Z	jschott	failed	185.28.154.54	RU
07-12-2025 09:18:00Z	oohare	success	63.102.4.70	US
07-12-2025 09:18:00Z	jschott	failed	185.23.127.21	RU
07-12-2025 09:19:00Z	mschultz	success	63.102.4.74	US
07-12-2025 09:20:00Z	qjones	success	63.102.4.71	US
07-12-2025 09:23:00Z	jschott	success	63.102.4.78	US
07-12-2025 09:23:00Z	dmann	failed	185.23.127.21	RU
07-12-2025 09:25:00Z	tlindy	success	63.102.4.71	US
07-12-2025 09:28:00Z	jschott	failed	185.143.137.221	RU
07-12-2025 09:31:00Z	mschultz	success	63.102.4.74	US

Which of the following users should be investigated first?

A. jschott

B. dmann

C. mschultz

D. tlindy

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

An analyst reviews the following system logs from a recent breach attempt:

Time	User	Command	IP
12:51:11	Berry	whoami	10.10.12.13
12:51:12	Berry	netstat -tulpn	10.10.12.13
12:51:13	Berry	sudo su	10.10.12.13
12:51:14	Berry	./linpeas.sh	10.10.12.13
12:51:15	Berry	su Larry	10.10.12.13
12:51:16	Larry	sudo nano	10.10.12.13
12:51:19	Larry	reset; sh1>&0 2>&0	10.10.12.13
12:51:25	root	whoami	10.10.12.13

Which of the following techniques did the attacker attempt to use?

A. Exfiltration

B. Remote code execution

C. Privilege escalation

D. Spoofing

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

An analyst reviews the following log entries:

Time (UTC)	Source Internet Protocol (IP)	Source hostname	Source port/protocol	Destination IP	Destination port/protocol
16:44:53	192.168.1.57	ws-57	49571/client	192.168.1.2	22/ssh
16:44:54	192.168.1.57	ws-57	44236/client	192.168.1.2	23/telnet
16:44:55	192.168.1.57	ws-57	46871/client	192.168.1.2	80/http
16:44:56	192.168.1.57	ws-57	43664/client	192.168.1.2	139/netbios
16:44:57	192.168.1.57	ws-57	50127/client	192.168.1.2	443/https
16:44:58	192.168.1.57	ws-57	48741/client	192.168.1.2	445/smb
16:44:59	192.168.1.57	ws-57	50111/client	192.168.1.2	3389/rdp
16:46:33	192.168.1.2	dc-1	445/smb	192.168.1.57	48741/client
16:52:12	192.168.1.57	ws-57	49853/client	185.167.3.24	53/https
16:59:31	192.168.1.57	ws-57	49953/client	192.168.1.25	25/smtp

Which of the following conclusions should the analyst reach? (Choose two.)

A. Host ws-57 is performing a network scan against dc-1.

B. Domain Controller dc-1 is performing a network scan against ws-57.

C. Host ws-57 delivered a phishing email via Simple Mail Transfer Protocol.

D. Host ws-57 is communicating on a service using a non-standard port.

E. Domain Controller dc-1 is infected with ransomware and initiating connections with ws-57.

F. Domain Controller dc-1 is communicating using a non-standard port.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

Which of the following best explains the purpose of the Pyramid of Pain in threat intelligence?

A. To show that changing to different types of indicators and behaviors is difficult for an adversary

B. To measure how much operational damage a threat actor can cause before detection occurs

C. To compare open-source intelligence (OSINT) with closed-source intelligence based on collection cost

D. To organize attack activity into categories such as spoofing, tampering, and repudiation

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

A security operations center (SOC) analyst investigates the results of a password spray test conducted by the vulnerability management team.
The analyst must:
Identify Linux systems that have successful and unsuccessful logins with username "User1".
Create an output report named "linux-events" of all the events to a flat file.
The analyst issues the following console command:
ls /var/log/
The shortened output of the command is below:

```
alternatives.log  cups              kern.log.2gz
apport.log        dmesg             private
auth.log          sssd              syslog
faillog           sysstat           installer
kern.log
```

Which of the following commands should the analyst use to meet the report output requirements?

A. cat /var/log/sssd | grep "User1" > linux-events.txt

B. cat /var/log/faillog.log | grep "User1" > linux-events.txt

C. cat /var/log/syslog | grep "User1" > linux-events.txt

D. cat /var/log/auth.log | grep "User1" > linux-events.txt

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

Multiple users report unexpected mouse movements and terminal windows opening. An analyst reviewing the network traffic logs observes the following:

```
Source                Destination          Protocol
192.168.12.11:49823   192.168.29.10:5900   TCP
192.168.12.11:52890   192.168.31.10:80     TCP
192.168.100.237:61923 192.168.17.2:443     TCP
192.168.12.11:55641   192.168.31.7:5900    TCP
192.168.12.11:58220   192.168.100.237:3389 TCP
192.168.12.11:123     192.168.34.123       UDP
192.168.100.237:64489 192.168.100.57:3389  TCP
```

Which of the following is the most likely reason for the reported symptoms?

A. Activity is on an internally addressable network.

B. A reverse tunnel is being used to send commands.

C. Remote Desktop Protocol (RDP) is being used to remotely control the impacted computers.

D. Virtual Network Computing is being used to connect to systems.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

Which of the following best explains why sensitive data should be encrypted at rest on laptops?

A. To prevent end users from copying data to other systems

B. To protect disclosure of information if physical devices are stolen

C. To comply with regulatory and legal requirements

D. To ensure the integrity of the data on the company network

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

A security architect works with a client on security operations center (SOC) capabilities. The security architect wants to ensure the log correlation and investigation activities are accurate across the infrastructure. Which of the following is the best for the client to implement?

A. Network Time Protocol (NTP)

B. Zero Trust Network Access (ZTNA)

C. Account federation

D. Secure access service edge (SASE)

E. Application programming interfaces (APIs)

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

A team lead asks an analyst to integrate multiple security tools to provide an enhanced view into data that is not readily available in the tool console. Which of the following will best meet this requirement?

A. Utilizing application programming interfaces

B. Deploying security orchestration, automation, and response

C. Templating with infrastructure as code

D. Using playbooks

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

A cybersecurity analyst requests a paid subscription to a threat intelligence feed relevant to a company's industry. Which of the following best describes this type of feed?

A. Open-source intelligence

B. Threat mapping

C. Threat modeling

D. Closed-source intelligence

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

HOTSPOT -

A systems administrator is reviewing the output of a vulnerability scan.

INSTRUCTIONS -

Review the information in each tab.

Based on the organization's environment architecture and remediation standards, select the server to be patched within 14 days and select the appropriate technique and mitigation.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Vulnerability remediation timeframes | Environment | Output

CVSS risk level	Standard	Applies to		
		OPS	TEST	STAGE
CVSS > 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **7 calendar days**	✔	✔	✘
CVSS > 7.9 < 9.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **14 calendar days**	✔	✘	✘
CVSS > 5.0 < 7.9	Must be patched or remediated and verified by a subsequent vulnerability scan within **30 calendar days**	✔	✘	✘
CVSS > 0 < 5.0	Must be patched or remediated and verified by a subsequent vulnerability scan within **60 calendar days**	✔	✘	✘

Any of these timeframes may be accelerated at the discretion of the Chief Information Security Officer (CISO).

- If patching cannot be completed or a vendor has not made a patch available within the timeframe in the table outlined above, compensating controls must be put in place within the timeframes listed above and the exception process must be followed.
- If a patch requires a reboot for installation, the reboot must occur within the timeframes outlined above.
- All mitigations must be tested in the lower environments before being promoted to operations.
- Appropriate risk management processes should be considered when an applicable timeframe is not required for an environment.

Vulnerability remediation timeframes | Environment | Output

Environment name	Environment location	Subnets	Domain	Publicly accessible	NGFW	Load balancer	MFA required
ops.comptia.org	External	203.17.18.20 203.17.18.30 192.168.60.0/24 192.168.61.0/24	comptia.org	Yes	Yes	Yes	No
stage.comptia.org	Internal	192.168.76.0/24 192.168.75.0/24	comptia.org	No	No	Yes	Yes
test.comptia.org	External	192.168.50.0/24 192.168.51.0/24	comptia.org	No	Yes	Yes	Yes

Vulnerability remediation timeframes | Environment | Output

Title: Microsoft IIS: Unsupported software version detected
Description: The software version detected is no longer supported.
Affected asset: 192.168.76.50
Risk: Unpatched software
Reference: CVE-2022-0155, CVSS 9.2

Title: Sensitive cookie in HTTPS session without "secure" attribute
Description: The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset: 192.168.76.60
Risk: Session sidejacking
Reference: CVE-2021-0462, CVSS 7.4

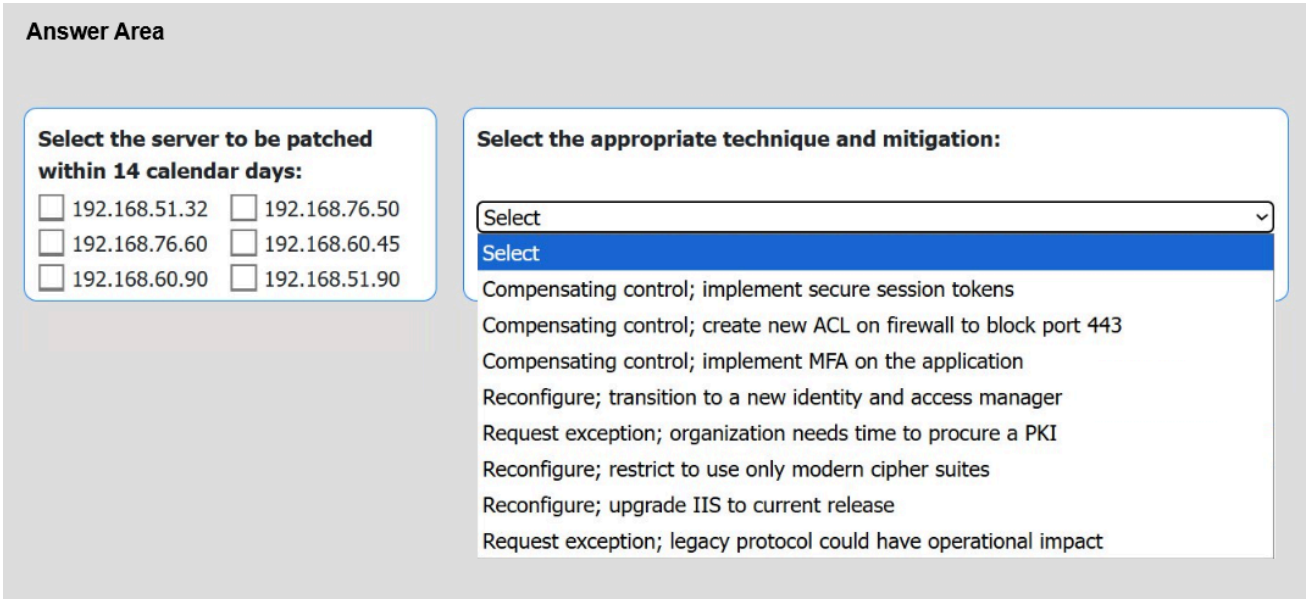
Title: Untrusted SSL/TLS Server X.509 certificate
Description: The server's TLS/SSL certificate is signed by a certificate authority that is untrusted or unknown.
Affected asset: 192.168.51.32
Risk: May allow on-path attackers to insert a spoofed certificate for any distinguished name (DN).
Reference: CVE-2021-1234, CVSS 8.1

Title: Sensitive cookie in HTTPS session without "secure" attribute
Description: The secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the user agent to send those cookies in plaintext over HTTP session.
Affected asset: 192.168.60.45
Risk: Session sidejacking
Reference: CVE-2021-0462, CVSS 7.4

Title: Web server is susceptible to TLS downgrade attacks
Description: The server permits the web client to select and use its own preferences.
Affected asset: 192.168.60.90
Risk: May allow data to be vulnerable.
Reference: CVE-2021-1234, CVSS 8.1

Title: Basic authentication
Description: Website is configured to permit use of `.htaccess` files on directories.
Affected asset: 192.168.51.90
Risk: May allow privileged access to sensitive data.
Reference: CVE-2021-38361, CVSS 5.1

Answer Area



Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 2*

A security team reviews a penetration testing report of a web application that contains multiple cross-site scripting (XSS) and Structured Query Language injection (SQLi) vulnerabilities. Which of the following is most likely causing these to occur?

A. Misconfigured web application firewall (WAF)

B. Lack of secure input validation

C. Lack of a Hypertext Transfer Protocol (HTTP) Strict Transport Security (HSTS) header

D. Lack of endpoint protection in the environment

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 2*

The Chief Information Officer (CIO) is requiring users to phase out a legacy system that no longer receives security updates because the system will be decommissioned soon. Which of the following risk management strategies is the CIO using?

A. Avoidance

B. Mitigation

C. Acceptance

D. Transference

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 2*

A security team deploys a new scanning solution that requires root, domain administrator, and local server administrator permissions on all systems. Which of the following is the best way to help mitigate the risk for this level of access?

A. Enabling single sign-on for all administrators

B. Integrating token-based authentication using a privileged access management (PAM) solution

C. Using temporary, one-time passwords as part of the login process

D. Configuring agentless scanning for critical targets

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 2*

Before merging with a software company, the acquiring company's legal team requires a detailed software scan to determine if all code base is using open-source or paid licensed libraries. The vulnerability management analyst needs to provide this report. Which of the following scan methods will best meet this requirement?

A. Static application security testing (SAST)

B. Dynamic application security testing (DAST)

C. Software composition analysis (SCA)

D. Runtime application self-protection (RASP)

E. Credentialed vulnerability scan

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 2*

Which of the following is the most likely reason an organization might implement compensating controls?

A. A vulnerability does not have a patch, and the system is mission critical.

B. A vulnerability has been fixed, tested, and deployed to production.

C. A vulnerability is being actively exploited in the wild, but the organization does not use the affected system.

D. A vulnerability was detected, but the organization has determined the result is a false positive.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 2*

A vulnerability analyst must perform a security assessment on an edge device running various services. The analyst runs an Nmap port scan and sees the following output:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-15 18:52 UTC
Nmap scan report for 152.203.20.16
Host is up (0.0000050s latency).
Not shown: 998 closed tcp ports (reset)
PORT          STATE           SERVICE
7/tcp         open            bgp
443/tcp       open            https
500/udp       open            ikamsp

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

Which of the following should the analyst do next to validate the discovered remote access service is secure?

A. Verify that the web server certificate is added to certificate store.

B. Verify that the Border Gateway Protocol (BGP) route has been published.

C. Verify that the virtual private network (VPN) service is utilizing Main Mode.

D. Verify that the web server can be pinged.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 2*

An analyst performs Nmap scans to determine which hosts may need to be targeted to deploy a critical Windows patch. The patch for the vulnerability is to address a critical security flaw that targets open Server Message Block (SMB) ports on Windows systems only. The analyst scans with the following command:

$sudo nmap -Pn 10.203.10.0/24

The analyst then receives the following output:

```
Nmap scan report for 10.203.10.11
Host is up, received user-set (0.0065s latency).
Scanned at 2025-05-01 18:50:59 UTC for 8s
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE REASON
22/tcp open ***** syn-ack ttl 128
135/tcp open ***** syn-ack ttl 128
445/tcp open ***** syn-ack ttl 128
3389/tcp open ***** syn-ack ttl 128

Nmap scan report for 10.203.10.12
Host is up, received user-set (0.0028s latency).
Scanned at 2025-05-01 18:50:59 UTC for 2s
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ***** syn-ack ttl 64
53/tcp filtered ***** no-response
80/tcp open ***** syn-ack ttl 64
3389/tcp open ***** syn-ack ttl 64
8080/tcp open ***** syn-ack ttl 64

Nmap scan report for 10.203.10.13
Host is up, received user-set (0.0070s latency).
Scanned at 2025-05-01 18:50:59 UTC for 2s
Not shown: 995 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ***** syn-ack ttl 64
53/tcp filtered ***** no-response
80/tcp open ***** syn-ack ttl 64
3389/tcp open ***** syn-ack ttl 64
8080/tcp open ***** syn-ack ttl 64

Nmap scan report for 10.203.10.16
Host is up, received user-set (0.0065s latency).
Scanned at 2025-05-01 18:50:59 UTC for 8s
Not shown: 997 filtered tcp ports (no-response)
PORT STATE SERVICE REASON
22/tcp open ***** syn-ack ttl 128
135/tcp open ***** syn-ack ttl 128
3389/tcp open ***** syn-ack ttl 128
```

Which of the following hosts should the analyst prioritize for patching?

A. 10.203.10.11

B. 10.203.10.12

C. 10.203.10.13

D. 10.203.10.16

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 2*

An analyst receives the following output:

```
Initiating SYN Stealth Scan
Scanning 16 hosts [3 ports / host]
Discovered open port 22/tcp on 10.203.20.15
Discovered open port 22/tcp on 10.203.20.10
Discovered open port 80/tcp on 10.203.20.15
Discovered open port 22/tcp on 10.203.20.13
Discovered open port 22/tcp on 10.203.20.11
Discovered open port 22/tcp on 10.203.20.14
Discovered open port 80/tcp on 10.203.20.10
Discovered open port 443/tcp on 10.203.20.14
```

Which of the following is the correct number of discovered systems that are allowing unencrypted traffic?

A. 1

B. 2

C. 3

D. 5

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 2*

An incident response team identifies a malicious uniform resource locator (URL) associated with a required business process and performs the following activities:

• Access to the URL has been restricted only to the necessary users through firewall rules and Cloud Security Group rules.

• Additional monitoring has been enabled for traffic related to that site and the allowed users.

• All application servers that need to access that site have been patched with the latest security and software updates.

• Application owners have been notified of the severity and need to remediate this reported issue.

Which of the following best describes the overall mitigation the security team is performing?

A. Patching solutions

B. Configuration management

C. Compensating controls

D. Attack surface management

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 2*

A vendor releases details of a new vulnerability. When an analyst reviews the scheduled scans, no vulnerabilities are identified. The vulnerability is only discovered after a configuration change. Which of the following scan types did the analyst configure?

A. External

B. Credentialed

C. Agent-based

D. Network

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!