compare biometric solutions?

A. FRR
B. Difficulty of use
C. Cost
D. FAR
E. CER

Correct Answer: A

QUESTION 330
A financial analyst has been accused of violating the company's AUP and there is forensic evidence to substantiate the allegation. Which of the following would dispute the analyst's claim of innocence?

A. Legal hold
B. Order of volatility
C. Non-repudiation
D. Chain of custody

Correct Answer: D

QUESTION 331
A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?

A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS

Correct Answer: E

QUESTION 332
An analyst is trying to identify insecure services that are running on the internal network. After performing a port scan the analyst identifies that a server has some insecure services enabled on default ports. Which of the following BEST describes the services that are currently running and the secure alternatives for replacing them? (Select THREE)

A. SFTP FTPS
B. SNMPv2 SNMPv3
C. HTTP, HTTPS
D. TFTP FTP
E. SNMPv1, SNMPv2
F. Telnet SSH
G. TLS, SSL
H. POP, IMAP

I. Login, rlogin

Correct Answer: BCF

QUESTION 333
The security team received a report of copyright infringement from the IP space of lire corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted le. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?

A. HIDS
B. Allow list
C. TPM
D. NGFW

Correct Answer: D

QUESTION 334
A security analyst generated a file named host1.pcap and shared it with a team member who is going to use it for further incident analysis. Which of the following tools will the other team member MOST likely use to open this file?

A. Autopsy
B. Memdump
C. FTK imager
D. Wireshark

Correct Answer: D
Explanation:
Some common applications that can open .pcap files are Wireshark, WinDump, tcpdump, Packet Square - Capedit and Ethereal.

QUESTION 335
Which of the following is the MOST relevant security check to be performed before embedding third-parry libraries in developed code?

A. Check to see if the third party has resources to create dedicated development and staging environments.
B. Verify the number of companies that downloaded the third-party code and the number of contributions on the code repository.
C. Assess existing vulnerabilities affecting the third-parry code and the remediation efficiency of the libraries' developers.
D. Read multiple penetration-testing reports for environments running software that reused the library.

Correct Answer: D

QUESTION 336
As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII
B. TLP
C. TTP
D. STIX

Correct Answer: C
Explanation:
TTPs Within Cyber Threat Intelligence:

- Tactics, techniques and procedures (TTPs) are the "patterns of activities or methods associated with a specific threat actor or group of threat actors."
- Analysis of TTPs aids in counterintelligence and security operations by describing how threat actors perform attacks.
- Top threats facing an organization should be given priority for TTP maturation. Smaller organizations may benefit strategically by outsourcing research and response.

One acronym everyone working on a cybersecurity team should be familiar with is TTPs - tactics, techniques and procedures - but not everyone understands how to use them properly within a cyber threat intelligence solution. TTPs describe how threat actors (the bad guys) orchestrate, execute and manage their operations attacks. ("Tactics" is also sometimes called "tools" in the acronym.) Specifically, TTPs are defined as the "patterns of activities or methods associated with a specific threat actor or group of threat actors," according to the Definitive Guide to Cyber Threat Intelligence.

QUESTION 337
Which of the following holds staff accountable while escorting unauthorized personnel?

A. Locks
B. Badges
C. Cameras
D. Visitor logs

Correct Answer: B

QUESTION 338
A security analyst wants to fingerprint a web server. Which of the following tools will the security analyst MOST likely use to accomplish this task?

A. nmap -p1-65535 192.168.0.10
B. dig 192.168.0.10
C. curl --head http://192.168.0.10
D. ping 192.168.0.10

Correct Answer: C
Explanation:
curl - Identify remote web server

Type the command as follows:$

curl -I http://www.remote-server.com/

$

curl -I http://vivekgite.com/

Output:

HTTP/1.1 200 OK

Content-type: text/html

Content-Length: 0

Date: Mon, 28 Jan 2008 08:53:54 GMT

Server: lighttpd

QUESTION 339
A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions
B. Multifactor authentication
C. A banned password list
D. A complex password policy

Correct Answer: B

QUESTION 340
During an investigation, a security manager receives notification from local authorities mat company proprietary data was found on a former employees home computer. The former employee's corporate workstation has since been repurposed, and the data on the hard drive has been overwritten. Which of the following would BEST provide the security manager with enough details to determine when the data was removed from the company network?

A. Properly congured hosts with security logging
B. Properly congured endpoint security tool with darting
C. Properly congured SIEM with retention policies
D. Properly congured USB blocker with encryption

Correct Answer: D
QUESTION 341
An organization's finance department is implementing a policy to protect against collusion. Which of the following control types and corresponding procedures should the organization implement to fulfill this policy's requirement? (Select TWO).

A. Corrective
B. Deterrent
C. Preventive
D. Mandatory vacations
E. Job rotation
F. Separation of duties

Correct Answer: DE

QUESTION 342
A recent security audit revealed that a popular website with IP address 172.16.1.5 also has an FTP service that employees were using to store sensitive corporate data. The organization's outbound firewall processes rules top-down. Which of the following would permit HTTP and HTTPS, while denying all other services for this host?

A. access-rule permit tcp destination 172.16.1.5 port 80
access-rule permit tcp destination 172.16-1-5 port 443
access-rule deny ip destination 172.16.1.5
B. access-rule permit tcp destination 172.16.1.5 port 22
access-rule permit tcp destination 172.16.1.5 port 443
access-rule deny tcp destination 172.16.1.5 port 80
C. access-rule permit tcp destination 172.16.1.5 port 21
access-rule permit tcp destination 172.16.1.5 port 80
access-rule deny ip destination 172.16.1.5
D. access-rule permit tcp destination 172.16.1.5 port 80
access-rule permit tcp destination 172.16.1.5 port 443
access-rule deny tcp destination 172.16.1.5 port 21

Correct Answer: D

QUESTION 343
Which of the following distributes data among nodes, making it more difficult to manipulate the data while also minimizing downtime?

A. MSSP
B. Public cloud
C. Hybrid cloud
D. Fog computing

Correct Answer: C

QUESTION 344
After a WiFi scan of a local office was conducted, an unknown wireless signal was identified Upon investigation, an unknown Raspberry Pi device was found connected to an Ethernet port using a single connection. Which of the following BEST describes the purpose of this device?

A. loT sensor
B. Evil twin
C. Rogue access point
D. On-path attack

Correct Answer: C

QUESTION 345
A security analyst needs to find real-time data on the latest malware and loCs. Which of the following best describe the solution the analyst should persue?