Question # 1

Two organizations plan to collaborate on the evaluation of new SIEM solutions for their respective companies. A combined effort from both organizations' SOC teams would speed up the effort. Which of the following can be written to document this agreement?

A. MOU

B. ISA

C. SLA

D. NDA

Question # 2

A company is implementing a DLP solution on the file server. The file server has PII, financial information, and health information stored on it. Depending on what type of data that is hosted on the file server, the company wants different DLP rules assigned to the data. Which of the following should the company do to help accomplish this goal?

A. Classify the data

B. Mask the data

C. Assign an application owner

D. Perform a risk analysis

Question #:3

A company is implementing BYOD and wants to ensure all users have access to the same cloud-based services. Which of the following would BEST allow the company to meet this requirement?

A. laaS

B. PasS

C. MaaS

D. SaaS

Question #:4

An organization has decided to purchase an insurance policy because a risk assessment determined that the cost to remediate the risk is greater than the five-year cost of the insurance policy. The organization is enabling risk

A. avoidance

B. acceptance

C. mitigation

D. transference

Question #:5

The database administration team is requesting guidance for a secure solution that will ensure confidentiality of cardholder data at rest only in certain fields in the database schema. The requirement is to substitute a sensitive data field with a non-sensitive field that is rendered useless if a data breach occurs. Which of the following is the BEST solution to meet the requirement?

A. Tokenization

B. Masking

C. Full disk encryption

D. Mirroring

Question #:6

A company is looking to migrate some servers to the cloud to minimize its technology footprint. The company has 100 databases that are on premises. Which of the following solutions will require the LEAST management and support from the company?

A. SaaS

B. IaaS

C. PaaS

D. SDN

Question #:7

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

Question #:8

A SOC operator is analyzing a log file that contains the following entries:

```
[06-Apr-2021 - 18:00:06] GET /index.php/../../../../../../etc/passwd
[06-Apr-2021 - 18:01:07] GET /index.php/../../../../../../etc/shadow
[06-Apr-2021 - 18:00:26] GET /index.php/../../../../../../../../../../etc/passwd
[06-Apr-2021 - 18:02:16] GET /index.php?var1=;cat /etc/passwd;&var2=7865tgydk
[06-Apr-2021 - 18:02:56] GET /index.php?var1=;cat /etc/shadow;&var2=7865tgydk
```

Which of the following explains these log entries?

A. SQL injection and improper input-handling attempts

B. Cross-site scripting and resource exhaustion attempts

C. Command injection and directory traversal attempts

D. Error handling and privilege escalation attempts

Question #:9

The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP

B. USB data blocker

C. USB OTG

D. Disabling USB ports

Question #:10

A penetration tester was able to compromise an internal server and is now trying to pivot the current session in a network lateral movement. Which of the following tools, if available on the server, will provide the MOST useful information for the next assessment step?

A. Autopsy

B. Cuckoo

C. Memdump

D. Nmap

Question #:11

A customer service representative reported an unusual text message that was sent to the help desk. The message contained an unrecognized invoice number with a large balance due and a link to click for more details. Which of the following BEST describes this technique?

A. Vishing

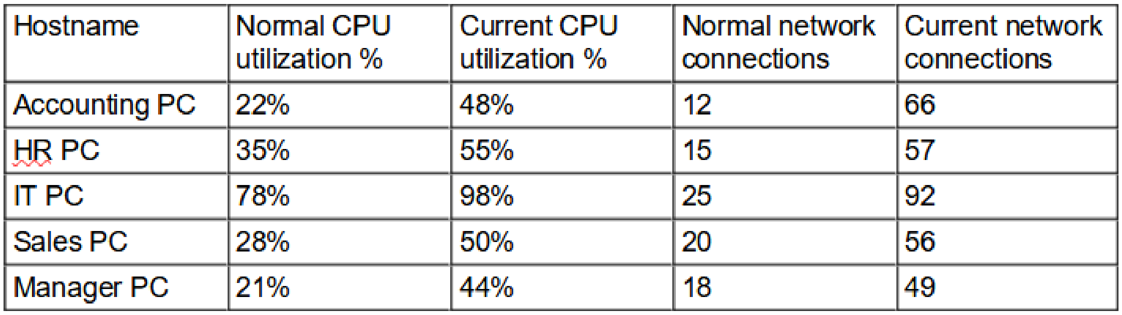
B. Whaling

C. Phishing

D. Smishing

Question #:12

Several users have opened tickets with the help desk. The help desk has reassigned the tickets to a security analyst for further review. The security analyst reviews the following metrics:



Hostname	Normal CPU utilization %	Current CPU utilization %	Normal network connections	Current network connections
Accounting PC	22%	48%	12	66
HR PC	35%	55%	15	57
IT PC	78%	98%	25	92
Sales PC	28%	50%	20	56
Manager PC	21%	44%	18	49

Which of the following is MOST likely the result of the security analyst's review?

A. The ISP is dropping outbound connections

B. The user of the Sales-PC fell for a phishing attack

C. Corporate PCs have been turned into a botnet

D. An on-path attack is taking place between PCs and the router

Question #:13

A company is providing security awareness training regarding the importance of not forwarding social media messages from unverified sources. Which of the following risks would this training help to prevent?

A. Hoaxes

B. SPIMs

C. Identity fraud

D. Credential harvesting

Question #:14

A security administrator is analyzing the corporate wireless network. The network only has two access points running on channels 1 and 11. While using airodump-ng, the administrator notices other access points are running with the same corporate ESSID on all available channels and with the same BSSID of one of the legitimate access ports. Which of the following attacks is happening on the corporate network?

A. Man in the middle

B. Evil twin

C. Jamming

D. Rogue access point

E. Disassociation

Question #:15

An attacker browses a company’s online job board attempting to find any relevant information regarding the technologies the company uses. Which of the following BEST describes this social engineering technique?

A. Hoax

B. Reconnaissance

C. Impersonation

D. pretexting

Question #:16

A penetration tester is fuzzing an application to identify where the EIP of the stack is located on memory. Which of the following attacks is the penetration tester planning to execute?

A. Race-condition

B. Pass-the-hash

C. Buffer overflow

D. XSS

Question #:17

A company has a flat network in the cloud. The company needs to implement a solution to segment its production and non-production servers without migrating servers to a new network. Which of the following solutions should the company implement?

A. internet

B. Screened Subnet

C. VLAN segmentation

D. Zero Trust

Question #:18

While preparing a software Inventory report, a security analyst discovers an unauthorized program installed on most of the company's servers. The program utilizes the same code signing certificate as an application deployed to only the accounting team. Which of the following mitigations would BEST secure the server environment?

A. Revoke the code signing certificate used by both programs.

B. Block all unapproved file hashes from installation.

C. Add the accounting application file hash to the allowed list.

D. Update the code signing certificate for the approved application.

Question #:19

A news article states hackers have been selling access to IoT camera feeds. Which of the following is the Most likely reason for this issue?

A. Outdated software

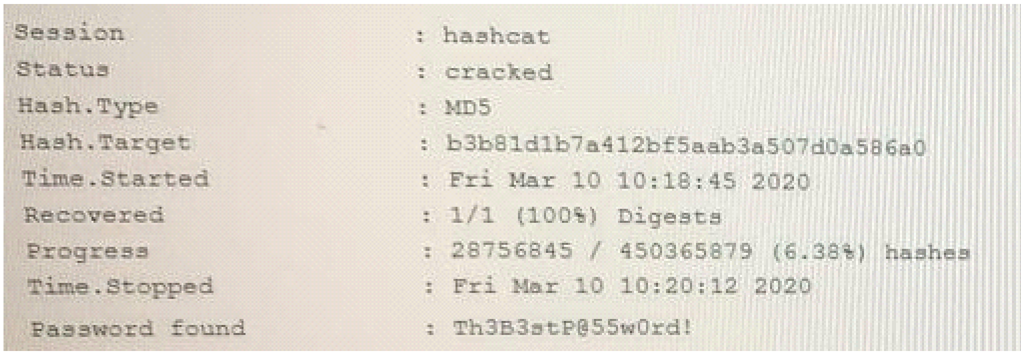
B. Weak credentials

C. Lack of encryption

D. Backdoors

Question #:20

An attacker has successfully exfiltrated several non-salted password hashes from an online system. Given the logs below:



```
Session                 : hashcat
Status                  : cracked
Hash.Type               : MD5
Hash.Target             : b3b81d1b7a412bf5aab3a507d0a586a0
Time.Started            : Fri Mar 10 10:18:45 2020
Recovered               : 1/1 (100%) Digests
Progress                : 28756845 / 450365879 (6.38%) hashes
Time.Stopped            : Fri Mar 10 10:20:12 2020
Password found          : Th3B3stP@55w0rd!
```

Which of the following BEST describes the type of password attack the attacker is performing?

A. Dictionary

B. Pass-the-hash

C. Brute-force

D. Password spraying

Question #:21

While investigating a recent security incident, a security analyst decides to view all network connections on a particular server. Which of the following would provide the desired information?

A. arp

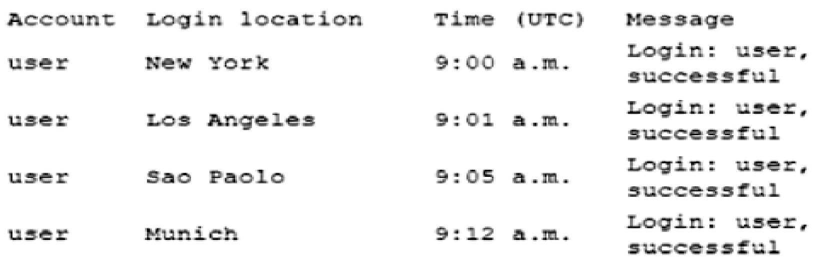
B. nslookup

C. netstat

D. nmap

Question #:22

During a recent security incident at a multinational corporation, a security analyst found the following logs for an account called user:



```
Account  Login location     Time (UTC)   Message
user     New York           9:00 a.m.    Login: user,
                                         successful
user     Los Angeles        9:01 a.m.    Login: user,
                                         successful
user     Sao Paolo          9:05 a.m.    Login: user,
                                         successful
user     Munich             9:12 a.m.    Login: user,
                                         successful
```

Which of the following account policies would BEST prevent attackers from logging in as user?

A. Impossible travel time

B. Geofencing

C. Time-based logins

D. Geolocation

Question #: 23

A recently discovered zero-day exploit utilizes an unknown vulnerability in the SMB network protocol to rapidly infect computers. Once infected, computers are encrypted and held for ransom. Which of the following would BEST prevent this attack from reoccurring?

A. Configure the perimeter firewall to deny inbound external connections to SMB ports.

B. Ensure endpoint detection and response systems are alerting on suspicious SMB connections.

C. Deny unauthenticated users access to shared network folders.

D. Verify computers are set to install monthly operating system updates automatically.

Question #: 24

A security manager for a retailer needs to reduce the scope of a project to comply with PCI DSS. The PCI data

is located in different offices than where credit cards are accepted. All the offices are connected via MPLS back to the primary datacenter. Which of the following should the security manager implement to achieve the objective?

A. Segmentation

B. Containment

C. Geofencing

D. Isolation

Question #:25

A user is concerned that a web application will not be able to handle unexpected or random input without crashing. Which of the following BEST describes the type of testing the user should perform?

A. Code signing

B. Fuzzing

C. Manual code review

D. Dynamic code analysis

Question #:26

An enterprise has hired an outside security firm to conduct a penetration test on its network and applications. The enterprise provided the firm with access to a guest account. Which of the following BEST represents the type of testing that is being used?

A. Black-box

B. Red-team

C. Gray-box

D. Bug bounty

E. White-box

Question #:27

While checking logs, a security engineer notices a number of end users suddenly downloading files with the .tar.gz extension. Closer examination of the files reveals they are PE32 files(Portable-Executable-32 Files). The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an href link a week prior. Which of the following is MOST likely occurring?

A. A RAT was installed and is transferring additional exploit tools.

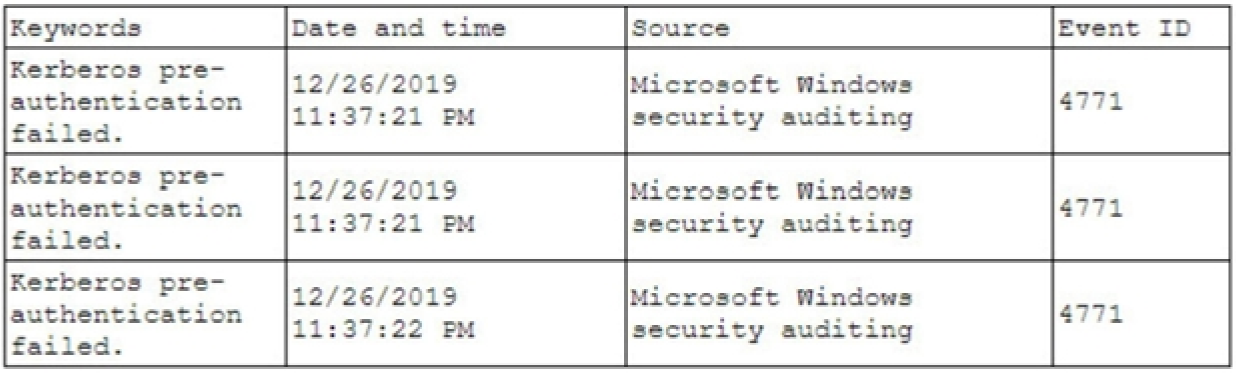
B. The workstations are beaconing to a command-and-control server.

C. A logic bomb was executed and is responsible for the data transfers.

D. A fileless virus is spreading in the local network environment

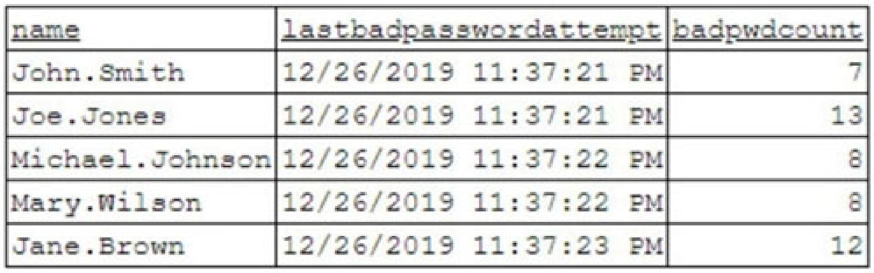
Question #:28

A security analyst has been asked to investigate a situation after the SOC started to receive alerts from the SIEM. The analyst first looks at the domain controller and finds the following events:



Keywords	Date and time	Source	Event ID
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:21 PM	Microsoft Windows security auditing	4771
Kerberos pre-authentication failed.	12/26/2019 11:37:22 PM	Microsoft Windows security auditing	4771

To better understand what is going on, the analyst runs a command and receives the following output:



name	lastbadpasswordattempt	badpwdcount
John.Smith	12/26/2019 11:37:21 PM	7
Joe.Jones	12/26/2019 11:37:21 PM	13
Michael.Johnson	12/26/2019 11:37:22 PM	8
Mary.Wilson	12/26/2019 11:37:22 PM	8
Jane.Brown	12/26/2019 11:37:23 PM	12

Based on the analyst’s findings, which of the following attacks is being executed?

A. Credential harvesting

B. Keylogger

C. Brute-force

D. Spraying

Question #:29

A privileged user at a company stole several proprietary documents from a server. The user also went into the log files and deleted all records of the incident. The systems administrator has just informed investigators that other log files are available for review. Which of the following did the administrator MOST likely configure that will assist the investigators?

A. Memory dumps

B. The syslog server

C. The application logs

D. The log retention policy

Question #:30

A company provides mobile devices to its users to permit access to email and enterprise applications. The company recently started allowing users to select from several different vendors and device models. When configuring the MDM, which of the following is a key security implication of this heterogeneous device approach?

A. The most common set of MDM configurations will become the effective set of enterprise mobile security controls.

B. All devices will need to support SCEP-based enrollment; therefore, the heterogeneity of the chosen architecture may unnecessarily expose private keys to adversaries.

C. Certain devices are inherently less secure than others, so compensatory controls will be needed to address the delta between device vendors.

D. MDMs typically will not support heterogeneous deployment environments, so multiple MDMs will need to be installed and configured.

.

Question #:31

During an internal penetration test, a security analyst identified a network device that had accepted cleartext authentication and was configured with a default credential. Which of the following recommendations should the security analyst make to secure this device?

A. Configure SNMPv1.

B. Configure SNMPv2.

C. Configure SNMPv3.

D. Configure the default community string.   // the name of the device 256 char

Question #:32

Which of the following job roles would sponsor data quality and data entry initiatives that ensure business and regulatory requirements are met?

A. The data owner

B. The data processor

C. The data steward

D. The data privacy officer.

Question #:33

Under GDPR, which of the following is MOST responsible for the protection of privacy and website user rights?

A. The data protection officer

B. The data processor

C. The data owner

D. The data controller

Question #:34

A user recently sent an SMS on a mobile phone that asked for bank delays. Which of the following social-engineering techniques was used in this case?

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Question #:35

An organization’s help desk is flooded with phone calls from users stating they can no longer access certain websites. The help desk escalates the issue to the security team, as these websites were accessible the previous day. The security analysts run the following command: ipconfig /flushdns, but the issue persists. Finally, an analyst changes the DNS server for an impacted machine, and the issue goes away. Which of the following attacks MOST likely occurred on the original DNS server?

A. DNS cache poisoning

B. Domain hijacking

C. Distributed denial-of-service

D. DNS tunneling

Question #:36

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 WAP 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

Question #: 37

A security analyst is performing a packet capture on a series of SOAP HTTP requests for a security assessment. The analyst redirects the output to a file. After the capture is complete, the analyst needs to review the first transactions quickly and then search the entire series of requests for a particular string. Which of the following would be BEST to use to accomplish the task? (Select TWO).

A. head

B. Tcpdump

C. grep

D. tail

E. curl

F. openssl

G. dd

Question #: 38

A user contacts the help desk to report the following:

Two days ago, a pop-up browser window prompted the user for a name and password after connecting to the corporate wireless SSID. This had never happened before, but the user entered the information as requested.

The user was able to access the Internet, but had trouble accessing the department share until the next day.

The user is now getting notifications from the bank about unauthorized transactions.

Which of the following attack vectors was MOST likely used in this scenario?

A. Rogue access point

B. Evil twin

C. DNS poisoning

D. ARP poisoning

Question #:39

An enterprise has hired an outside security firm to conduct penetration testing on its network and applications. The firm has only been given the documentation available to the customers of the applications. Which of the following BEST represents the type of testing that will occur?

A. Bug bounty

B. Black-box

C. Gray-box

D. White-box

Question #:40

Which of the following BEST explains the difference between a data owner and a data custodian?

A. The data owner is responsible for adhering to the rules for using the data, while the data custodian is responsible for determining the corporate governance regarding the data

B. The data owner is responsible for determining how the data may be used, while the data custodian is responsible for implementing the protection to the data

C. The data owner is responsible for controlling the data, while the data custodian is responsible for maintaining the chain of custody when handling the data

D. The data owner grants the technical permissions for data access, while the data custodian maintains the database access controls to the data

Question #:41

A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator MOST likely use to confirm the suspicions?

A. Nmap

B. Wireshark

C. Autopsy

D. DNSEnum

Question #:42

During a security assessment, a security analyst finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permissions for the existing users and groups and remove the set-user-ID bit from the file?

A. ls

B. chflags

C. chmod

D. lsof

E. setuid

Question #:43

A web server administrator has redundant servers and needs to ensure failover to the secondary server when the primary server goes down. Which of the following should the administrator implement to avoid disruption?

A. NIC teaming

B. High availability

C. Dual power supply

D. laaS

Question #:44

A multinational organization that offers web-based services has datacenters that are located only in the United States; however, a large number of its customers are in Australia, Europe, and China. Payments for services are managed by a third party in the United Kingdom that specializes in payment gateways. The management team is concerned the organization is not compliant with privacy laws that cover some of its customers. Which of the following frameworks should the management team follow?

A. Payment Card Industry Data Security Standard

B. Cloud Security Alliance Best Practices

C. ISO/IEC 27032 Cybersecurity Guidelines

D. General Data Protection Regulation

Question #: 45

Which of the following often operates in a client-server architecture to act as a service repository, providing enterprise consumers access to structured threat intelligence data?

A. STIX

B. CIRT

C. OSINT

D. TAXII

Question #:46

A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?

A. An incident response plan

B. A communications plan

C. A business continuity plan

D. A disaster recovery plan

Question #:47

A Chief Information Security Officer has defined resiliency requirements for a new data center architecture. The requirements are as follows:

- Critical file shares will remain accessible during and after a natural disaster. //Geographic dispersal
- Five percent of hard disks can fail at any given time without impacting the data. //RAID
- Systems will be forced to shutdown gracefully when battery levels are below 20%. //UPS

Which of the following are required to BEST meet these objectives? (Select THREE)

A. Fiber switching

B. laC

C. NAS

D. RAID

E. UPS

F. Redundant power supplies

G. Geographic dispersal

H. Snapshots

I. Load balancing

Question #:48

The Chief Information Security Officer wants to prevent exfiltration of sensitive information from employee cell phones when using public USB power charging stations. Which of the following would be the BEST solution to Implement?

A. DLP

B. USB data blocker

C. USB OTG

D. Disabling USB ports

Question #: 49

Which of the following should be monitored by threat intelligence researchers who search for leaked credentials?

A. Common Weakness Enumeration

B. OSINT

C. Dark web

D. Vulnerability databases

Question #:50

In a phishing attack, the perpetrator is pretending to be someone in a position of power in an effort to influence the target to click or follow the desired response. Which of the following principles is being used?

A. Authority

B. Intimidation

C. Consensus

D. Scarcity

Question #:51

Which of the following control types fixes a previously identified issue and mitigates a risk?

A. Detective

B. Corrective

C. Preventative

D. Finalized

Question #:51

Which of the following provides the BEST protection for sensitive information and data stored in cloud-based services but still allows for full functionality and searchability of data within the cloud-based services?

A. Data encryption

B. Data masking

C. Anonymization

D. Tokenization

Question #:52

Which of the following is MOST likely to outline the roles and responsibilities of data controllers and data processors?

A. SSAE SOC 2

B. PCI DSS

C. GDPR

D. ISO 31000

Question #:53

A security analyst must determine if either SSH or Telnet is being used to log in to servers. Which of the following should the analyst use?

A. logger

B. Metasploit

C. tcpdump

D. netstat