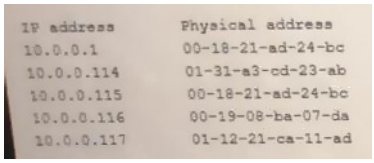
QUESTION 221
A security analyst is investigation an incident that was first reported as an issue connecting to network shares and the internet. While reviewing logs and tool output, the analyst sees the following:



IP address	Physical address
10.0.0.1	00-18-21-ad-24-bc
10.0.0.114	01-31-a3-cd-23-ab
10.0.0.115	00-18-21-ad-24-bc
10.0.0.116	00-19-08-ba-07-da
10.0.0.117	01-12-21-ca-11-ad

Which of the following attacks has occurred?

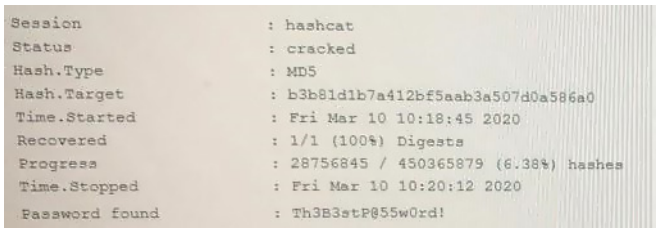
A. IP conflict
B. Pass-the-hash
C. MAC flooding
D. Directory traversal
E. ARP poisoning

Correct Answer: E
Explanation:
https://www.radware.com/security/ddos-knowledge-center/ddospedia/arp-poisoning
QUESTION 222
A security analyst needs to complete an assessment. The analyst is logged into a server and must use native tools to map services running on it to the server's listening ports. Which of the following tools can BEST accomplish this talk?

A. Netcat
B. Netstat
C. Nmap
D. Nessus

Correct Answer: B

QUESTION 223
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

Correct Answer: A

QUESTION 224
A security analyst is logged into a Windows file server and needs to see who is accessing files and from which computers. Which of the following tools should the analyst use?

A. netstat
B. net share
C. netcat
D. nbtstat
E. net session

Correct Answer: A

QUESTION 225
A large enterprise has moved all Hs data to the cloud behind strong authentication and encryption A sales director recently had a laptop stolen and later, enterprise data was round to have been compromised database. Which of the following was the MOST likely cause?

A. Shadow IT
B. Credential stuffing
C. SQL injection
D. Man-in-the-browser
E. Bluejacking

Correct Answer: A

QUESTION 226
A security analyst is investigating an incident to determine what an attacker was able to do on a compromised laptop. The analyst reviews the following SIEM log:

Host	Event ID	Event source	Description
PC1	865	Microsoft-Windows-SoftwareRestrictionPolicies	C:\asdf234\asdf234.exe was blocked by Group Policy
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:powershell.exe Creator Process Name:outlook.exe
PC1	4688	Microsoft-Windows-Security-Auditing	A new process has been created. New Process Name:lat.ps1 Creator Process Name:powershell.exe
PC2	4625	Microsoft-Windows-Security-Auditing	An account failed to log on. LogonType:3 SecurityID:Null SID Workstation Name:PC1 Authentication Package Name:NTLM

Which of the following describes the method that was used to compromise the laptop?

A. An attacker was able to move laterally from PC1 to PC2 using a pass-the-hash attack
B. An attacker was able to bypass application whitelisting by emailing a spreadsheet attachment with an embedded PowerShell in the file
C. An attacker was able to install malware to the CAasdf234 folder and use it to gam administrator nights and launch Outlook
D. An attacker was able to phish user credentials successfully from an Outlook user profile

Correct Answer: A

QUESTION 227
Employees are having issues accessing the company's website. Some employees report very slow performance, while others cannot the website at all. The web and security administrators search the logs and find millions of half-open connections to port 443 on the web server. Further analysis reveals thousands of different source IPs initiating this traffic. Which of the following attacks is MOST likely occurring?

A. DDoS
B. Man-in-the-middle
C. MAC flooding
D. Domain hijacking

Correct Answer: A

QUESTION 228
A user recently attended an exposition and received some digital promotional materials The user later noticed blue boxes popping up and disappearing on the computer, and reported receiving several spam emails, which the user did not open. Which of the following is MOST likely the cause of the reported issue?

A. There was a drive-by download of malware
B. The user installed a cryptominer
C. The OS was corrupted
D. There was malicious code on the USB drive

Correct Answer: D

QUESTION 229
The facilities supervisor for a government agency is concerned about unauthorized access to environmental systems in the event the staff WiFi network is breached. Which of the blowing would BEST address this security concern?

A. install a smart meter on the staff WiFi.
B. Place the environmental systems in the same DHCP scope as the staff WiFi.
C. Implement Zigbee on the staff WiFi access points.
D. Segment the staff WiFi network from the environmental systems network.

Correct Answer: D

QUESTION 230
Which of the following would be the BEST resource lor a software developer who is looking to improve secure coding practices for web applications?

A. OWASP
B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries

Correct Answer: A

QUESTION 231
A security analyst discovers several .jpg photos from a cellular phone during a forensics investigation involving a compromised system. The analyst runs a forensics tool to gather file metadata. Which of the following would be part of the images if all the metadata is still intact?

A. The GPS location
B. When the file was deleted
C. The total number of print jobs
D. The number of copies made

Correct Answer: A

QUESTION 232
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

Correct Answer: A

QUESTION 233
Which of the following is MOST likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report
B. A risk register
C. A business impact analysis
D. An asset value register
E. A disaster recovery plan

Correct Answer: B

QUESTION 234
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

Correct Answer: B
QUESTION 235
An information security incident recently occurred at an organization, and the organization was required to report the incident to authorities and notify the affected parties. When the organization's customers became of aware of the incident, some reduced their orders or stopped placing orders entirely. Which of the following is the organization experiencing?

A. Reputation damage
B. Identity theft
C. Anonymlzation
D. Interrupted supply chain

Correct Answer: A

QUESTION 236
An attacked is attempting to exploit users by creating a fake website with the URL www.validwebsite.com. The attacker's intent is to imitate the look and feel of a legitimate website to obtain personal information from unsuspecting users. Which of the following social-engineering attacks does this describe?

A. Information elicitation
B. Typo squatting
C. Impersonation
D. Watering-hole attack

Correct Answer: D