Correct Answer: A

QUESTION 199
During an investigation, an analyst discovers the following rule in an executive's email client:

IF * TO <executive@anycompany.com> THEN mailto: <someaddress@domain.com>

SELECT FROM `sent' THEN DELETE FROM <executive@anycompany.com>

The executive is not aware of this rule. Which of the following should the analyst do FIRST to evaluate the potential impact of this security incident?

A. Check the server logs to evaluate which emails were sent to <someaddress@domain.com>
B. Use the SIEM to correlate logging events from the email server and the domain server
C. Remove the rule from the email client and change the password
D. Recommend that management implement SPF and DKIM

Correct Answer: A

QUESTION 200
A security analyst is reviewing the following requirements for new time clocks that will be installed in a shipping warehouse:

▪ The clocks must be configured so they do not respond to ARP broadcasts.
▪ The server must be configured with static ARP entries for each clock.

Which of the following types of attacks will this configuration mitigate?

A. Spoofing
B. Overflows
C. Rootkits
D. Sniffing

Correct Answer: A

QUESTION 201
A company's security administrator needs to automate several security processes related to testing for the existence of changes within the environment. Conditionally, other processes will need to be created based on input from prior processes. Which of the following is the BEST method for accomplishing this task?

A. Machine learning and process monitoring
B. API integration and data enrichment
C. Workflow orchestration and scripting
D. Continuous integration and configuration management

Correct Answer: A

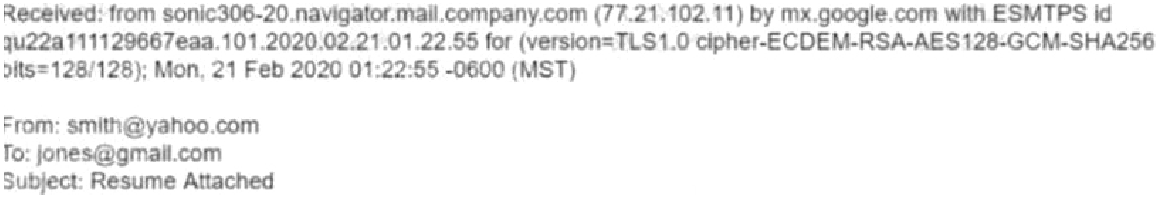
QUESTION 202

Which of the following are reasons why consumer IoT devices should be avoided in an enterprise environment? (Select TWO)

A. Message queuing telemetry transport does not support encryption.
B. The devices may have weak or known passwords.
C. The devices may cause a dramatic Increase in wireless network traffic.
D. The devices may utilize unsecure network protocols.
E. Multiple devices may interface with the functions of other IoT devices.
F. The devices are not compatible with TLS 12.

Correct Answer: BD

QUESTION 203
A security analyst inspects the header of an email that is presumed to be malicious and sees the following:



```
Received: from sonic306-20.navigator.mail.company.com (77.21.102.11) by mx.google.com with ESMTPS id
qu22a111129667eaa.101.2020.02.21.01.22.55 for (version=TLS1.0 cipher-ECDEM-RSA-AES128-GCM-SHA256
bits=128/128); Mon, 21 Feb 2020 01:22:55 -0600 (MST)

From: smith@yahoo.com
To: jones@gmail.com
Subject: Resume Attached
```

Which of the following is inconsistent with the rest of the header and should be treated as suspicious?

A. The subject line
B. The sender's email address
C. The destination email server
D. The use of a TLS cipher

Correct Answer: C

QUESTION 204
A company is experiencing a malware attack within its network. A security engineer notices many of the impacted assets are connecting outbound to a number of remote destinations and exfiltrating data. The security engineer also see that deployed, up-to-date antivirus signatures are ineffective. Which of the following is the BEST approach to prevent any impact to the company from similar attacks in the future?

A. IDS signatures
B. Data loss prevention
C. Port security
D. Sinkholing

Correct Answer: A

QUESTION 205
As part of an Intelligence feed, a security analyst receives a report from a third-party trusted source. Within the report are several detrains and reputational information that suggest the

company's employees may be targeted for a phishing campaign. Which of the following configuration changes would be the MOST appropriate for Mergence gathering?

A. Update the whitelist.
B. Develop a malware signature.
C. Sinkhole the domains
D. Update the Blacklist

Correct Answer: D

QUESTION 206
Which of the following should be found within an organization's acceptable use policy?

A. Passwords must be eight characters in length and contain at least one special character.
B. Customer data must be handled properly, stored on company servers, and encrypted when possible
C. Administrator accounts must be audited monthly, and inactive accounts should be removed.
D. Consequences of violating the policy could include discipline up to and including termination.

Correct Answer: D

QUESTION 207
A web-based front end for a business intelligence application uses pass-through authentication to authenticate users. The application then uses a service account, to perform queries and look up data m a database. A security analyst discovers employees are accessing data sets they have not been authorized to use. Which of the following will fix the cause of the issue?

A. Change the security model to force the users to access the database as themselves
B. Parameterize queries to prevent unauthorized SQL queries against the database
C. Configure database security logging using syslog or a SIEM
D. Enforce unique session IDs so users do not get a reused session ID

Correct Answer: B

QUESTION 208
A software development team asked a security analyst to review some code for security vulnerabilities. Which of the following would BEST assist the security analyst while performing this task?

A. Static analysis
B. Dynamic analysis
C. Regression testing
D. User acceptance testing

Correct Answer: C

QUESTION 209
During an investigation, a security analyst identified machines that are infected with malware the antivirus was unable to detect. Which of the following is the BEST place to acquire evidence to perform data carving?

A. The system memory
B. The hard drive
C. Network packets
D. The Windows Registry

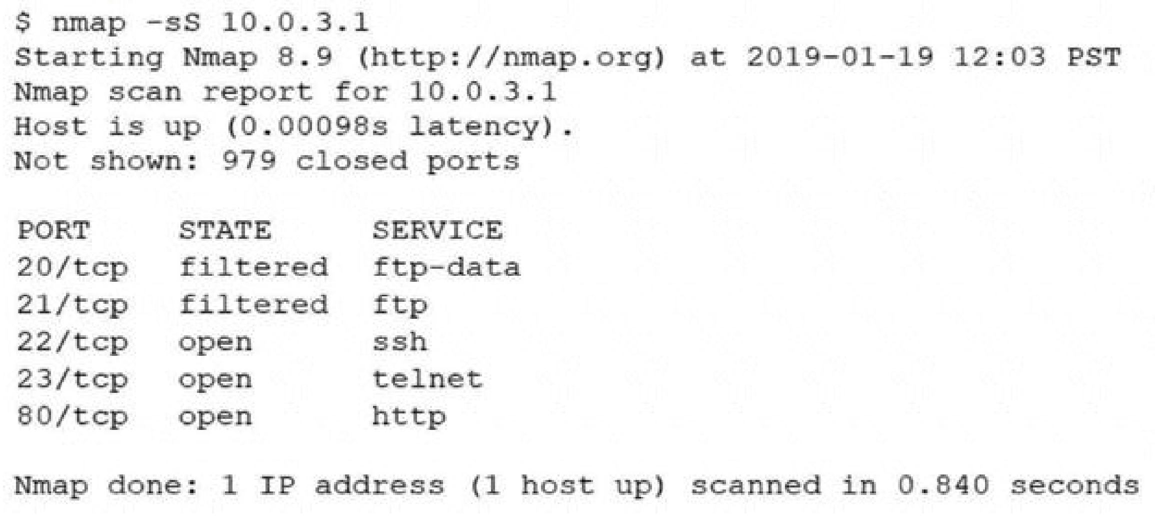
Correct Answer: A

QUESTION 210
A security engineer is reviewing security products that identify malicious actions by users as part of a company's insider threat program. Which of the following is the MOST appropriate product category for this purpose?

A. SOAR
B. WAF
C. SCAP
D. UEBA

Correct Answer: D
Explanation:
UEBA stands for User and Entity Behavior Analytics and was previously known as user behavior analytics (UBA).

QUESTION 211
An analyst performs a routine scan of a host using Nmap and receives the following output:



```
$ nmap -sS 10.0.3.1
Starting Nmap 8.9 (http://nmap.org) at 2019-01-19 12:03 PST
Nmap scan report for 10.0.3.1
Host is up (0.00098s latency).
Not shown: 979 closed ports

PORT     STATE     SERVICE
20/tcp   filtered  ftp-data
21/tcp   filtered  ftp
22/tcp   open      ssh
23/tcp   open      telnet
80/tcp   open      http

Nmap done: 1 IP address (1 host up) scanned in 0.840 seconds
```

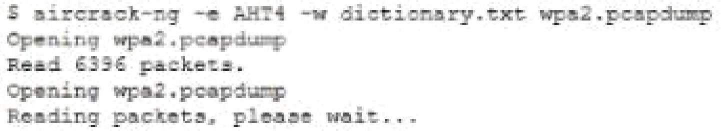
Which of the following should the analyst investigate FIRST?

A. Port 21

B. Port 22
C. Port 23
D. Port 80

Correct Answer: A

QUESTION 212
The help desk provided a security analyst with a screenshot of a user's desktop:



```
$ aircrack-ng -e AHT4 -w dictionary.txt wpa2.pcapdump
Opening wpa2.pcapdump
Read 6396 packets.
Opening wpa2.pcapdump
Reading packets, please wait...
```

For which of the following is aircrack-ng being used?

A. Wireless access point discovery
B. Rainbow attack
C. Brute-force attack
D. PCAP data collection

Correct Answer: B

QUESTION 213
A security analyst is investigating a malware infection that occurred on a Windows system. The system was not connected to a network and had no wireless capability Company policy prohibits using portable media or mobile storage. The security analyst is trying to determine which user caused the malware to get onto the system. Which of the following registry keys would MOST likely have this information?

A. HKEY_USERS\<user SID>\Software\Microsoft\Windows\CurrentVersion\Run
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_USERS\<user SID>\Software\Microsoft\Windows\explorer\MountPoints2
D. HKEY_USERS\<user SID>\Software\Microsoft\Internet Explorer\Typed URLs
E. HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\eventlog\System\iusb3hub

Correct Answer: E

QUESTION 214
Which of me following BEST articulates the benefit of leveraging SCAP in an organization's cybersecurity analysis toolset?

A. It automatically performs remedial configuration changes lo enterprise security services
B. It enables standard checklist and vulnerability analysis expressions for automaton
C. It establishes a continuous integration environment for software development operations
D. It provides validation of suspected system vulnerabilities through workflow orchestration

Correct Answer: B