Vendor: Cisco

Exam Code:210-250

Exam Name: Cisco Cybersecurity Fundamentals

Version: Demo

QUESTION 1

How can the SMB worm self-propagate throughout the network?

A. using Windows Outlook

B. using Windows file shares

C. using Windows remote desktop

D. using Windows PowerShell

Correct Answer: B

QUESTION 2

What does the acronym LDAP represent?

A. lightweight directory access protocol

B. lightweight directory assistance protocol

C. lightweight daemon access protocol

D. lightweight directory access process

Correct Answer: A

QUESTION 3

A change that is low risk and might not need to follow the full change management process is classified as which of the following?

A. Standard

B. Emergency

C. Normal

D. Controlled

Correct Answer: A

QUESTION 4

What are two controls that the Cisco WSA can use to validate web requests? (Choose two.)

A. basic URL filtering that leverages pre-defined, category-based web usage controls

B. AMP for isolating reputable exploits and malware samples to its local disk for further investigation

C. a reputation database that is used to analyze web requests as part of a security control procedure

D. IPS-based signatures that are loaded in the Cisco WSA to prevent intrusions and alert system administrators

E. a reputation database within the Cisco WSA that uses Snort-like rule sets to combat RootKit intrusions

Correct Answer: AC

QUESTION 5

Which two of the following statements are true regarding the DHCP relay agent? (Choose two.)

A. DHCP relay is required if the DHCP clients and the DHCP servers are located in the same broadcast domain

B. The DHCP server uses the ciaddr IP address to select an IP address pool from which to assign the IP addresses to the DHCP client.

C. The primary function of a DHCP relay agent is to relay the DHCP messages from the local DHCP clients to the remote DHCP servers.

D. DHCP discovery messages are broadcasted from the DHCP relay agent to the DHCP servers.

E. When the DHCP relay agent receives a broadcast packet from a connected client, it changes the giaddr field from zero to the relay agent IP address, and forwards the message to the DHCP server.

Correct Answer: CE

QUESTION 6

Cisco AVC uses which of the following technologies to provide deep packet inspection (DPI) technology to identify a wide variety of applications within the network traffic flow, using Layer 3 to Layer 7 data?

A. Cisco NetFlow

B. IPFIX

C. Cisco AMP

D. Cisco Network-Based Application Recognition Version 2 (NBAR2)

Correct Answer: D

QUESTION 7

Which definition of a daemon on Linux is true?

A. error check right afterthe call to fork a process

B. new process created by duplicating the calling process

C. program that runs unobtrusively in the background

D. set of basic CPU instructions

Correct Answer: C

QUESTION 8

Which of the following is not a disadvantage of host-based antimalware?

A. It requires updating multiple endpoints.

B. It does not have visibility into encrypted traffic.

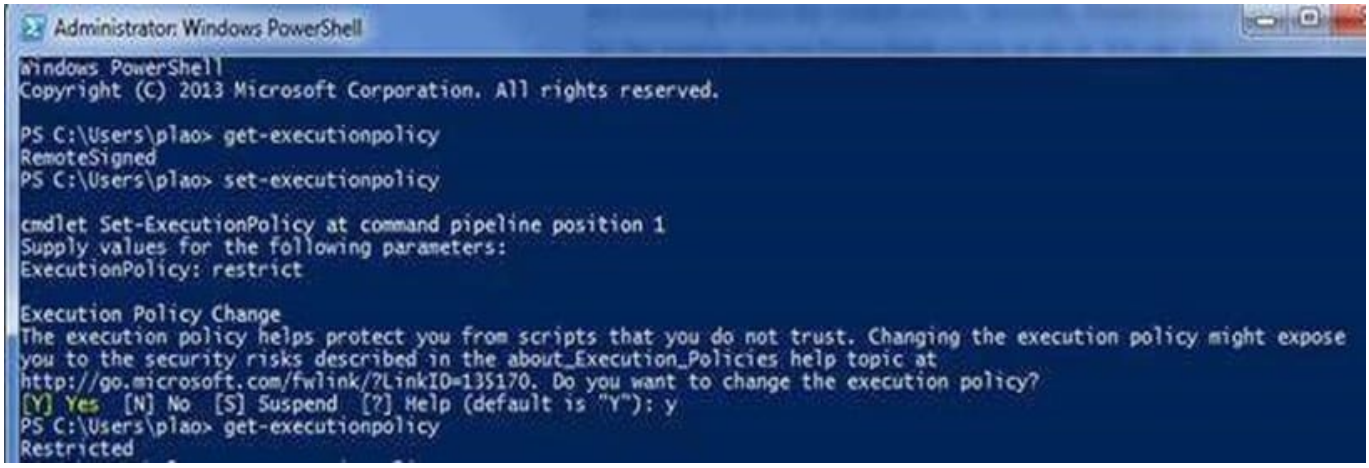
C. It does not have visibility of all events happening in the network.

D. It may require working with different operating systems.

Correct Answer: B

QUESTION 9

Referring to the output shown below, which two statements are correct? (Choose two.)



A. Only the externally downloaded PowerShell scripts must be digitally signed.

B. The user changed the PowerShell execution policy to the default setting.

C. PowerShell was run with administrative privileges.

D. There are no restrictions on running PowerShell scripts.

Correct Answer: BC

QUESTION 10

What is one of the main reasons that it is important for security analysts to understand how ICMP works and what normal ICMP activity looks like?

A. Helps them determine when ICMP is broken

B. Enables them to spot misuses of TCP discovery packets and rogue devices

C. Enables them to spot Denial of Service attacks

D. Enables them to spot ARP Poisoning attacks

Correct Answer: C

QUESTION 11

Which of the following are benefits of system-based sandboxing?

A. It limits the development of an application inside of a region of memory.

B. It limits the impact of security vulnerabilities and bugs in code to only run inside the "sandbox."

C. It prevents software bugs and exploits of vulnerabilities from affecting the rest of the system and from installing persistent malware in the system.

D. It limits the communication of kernel modules within the system, controlling the flow of information and data exchange.

Correct Answer: BC

QUESTION 12

Which Linux component is being affected if the malware is altering the Linux memory management functions?

A. user space

B. kernel space

C. hardware

D. user applications

Correct Answer: B