Download Cisco 300-215 Exam Dumps Free

Shared by Greer on 17-06-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.

Metadata	
Drive type	Fixed (Hard disk)
Drive serial number	1CBDB2C4
Full path	C:\Windows\System32\WIndowsPowerShell\v1.0\powershell.exe
NetBIOS name	user-pc
Lnk file name	ds7002.pdf
Relative path	..\..\..\..\..\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Arguments	-noni –ep bypass $zk = 'JHB0Z3Q9MHgwMDA1ZTJiZTskdmNxPTB4MDAwNjlzYjY7.
Target file size (bytes)	452608
Droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Birth droid volume	c59b0b22-7202-4410-b323-894349c1d75b
Droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
Birth droid file	bf069f66-8be6-11e6-b3d9-0800279224e5
File attribute	The file or directory is an archive file
Target file access time (UTC)	13.07.2009 23:32:37
Target file creation time (UTC)	13.07.2009 23:32:37
Target file modification time (UTC)	14.07.2009 1:14:24
Header flags	HasTargetIdList, HasLinkInfo, HasName, HasRelativePath, HasArguments, HasIcc
MAC vendor	Cadmus Computer Systems
Target path	My Computer\C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Target MFT entry number	0x7E21

An engineer is analyzing a .LNK (shortcut) file recently received as an email attachment and blocked by email security as suspicious. What is the next step an engineer should take?

Options:

A- Delete the suspicious email with the attachment as the file is a shortcut extension and does not represent any threat.

B- Upload the file to a virus checking engine to compare with well-known viruses as the file is a virus disguised as a legitimate extension.

C- Quarantine the file within the endpoint antivirus solution as the file is a ransomware which will encrypt the documents of a victim.

D- Open the file in a sandbox environment for further behavioral analysis as the file contains a malicious script that runs on execution.

Answer:

D

Explanation:

The metadata in the exhibit reveals a strong indicator that this .LNK file (shortcut) is malicious:

The shortcut file is named 'ds7002.pdf' but actually points to the execution of PowerShell:

Full path: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Arguments include:

-noni -ep bypass $z = '...'; indicating an attempt to run a PowerShell script with execution policy bypassed (a known tactic for fileless malware delivery).

The file is masked as a PDF (common social engineering technique), and PowerShell execution via .LNK is a signature technique used by many malware families to initiate second-stage payloads or scripts.

Given this, the correct and safest course of action is to:

Open the .LNK file in a sandbox environment (D).

This enables safe behavioral analysis to observe what actions it attempts upon execution without endangering live systems.

Other options are inappropriate:

A (ignoring the threat due to extension) is dangerous --- .LNKs can trigger code.

B (upload to virus engine) is only helpful for known malware and lacks behavioral context.

C (quarantine) is preventive but not investigative --- sandboxing provides visibility.

Question 2

Question Type: MultipleChoice

Which tool is used for reverse engineering malware?

Options:

A- Ghidra

B- SNORT

C- Wireshark
D- NMAP

Answer:

A

Explanation:

Ghidra is a free and open-source software reverse engineering (SRE) suite developed by the NSA. It includes disassembly, decompilation, and debugging tools specifically designed for analyzing malware and other compiled programs.

The Cisco CyberOps guide references Ghidra as a top tool for reverse engineering binary files during malware analysis tasks, making it ideal for understanding malicious code behavior at a deeper level.

Question 3

Question Type: MultipleChoice

A security team receives reports of multiple files causing suspicious activity on users' workstations. The file attempted to access highly confidential information in a centralized file server. Which two actions should be taken by a security analyst to evaluate the file in a sandbox? (Choose two.)

Options:

A- Inspect registry entries
B- Inspect processes.
C- Inspect file hash.
D- Inspect file type.
E- Inspect PE header.

Answer:

B, E

Explanation:

When analyzing suspicious files in a sandbox environment, a security analyst focuses on identifying and evaluating their behavior in a controlled setting to confirm potential malicious activity:

Inspect processes (B): Observing the processes that the file spawns or injects into during execution helps identify malicious actions or privilege escalation. This is a crucial part of dynamic analysis in the sandbox environment.

Inspect PE header (E): The PE (Portable Executable) header contains metadata about how the file will execute on Windows systems. It reveals details such as the entry point, libraries used, and whether the file is suspiciously crafted or packed, which can be strong indicators of malicious behavior.

The other options (A, C, D) are important in the broader forensic analysis, but within the sandbox dynamic analysis, focusing on process behavior and file execution headers is critical for determining how the file interacts with the system and whether it is indeed malicious.

Question 4

Question Type: MultipleChoice

What are YARA rules based upon?

Options:

A- binary patterns
B- HTML code
C- network artifacts
D- IP addresses

Answer:

A

Explanation:

YARA rules are primarily used for malware classification and detection based on binary pattern matching within files. They describe sequences of bytes, strings, and other file characteristics found in malicious binaries.

The Cisco CyberOps Associate guide explains: 'YARA rules operate by inspecting binary data using conditions and string matches to identify specific patterns that indicate known malware

samples.'.

Question 5

Question Type: MultipleChoice

A security team needs to prevent a remote code execution vulnerability. The vulnerability can be exploited only by sending '${ string in the HTTP request. WAF rule is blocking '${', but system engineers detect that attackers are executing commands on the host anyway. Which action should the security team recommend?

Options:

A- Enable URL decoding on WAF.
B- Block incoming web traffic.
C- Add two WAF rules to block 'S' and '{' characters separately.
D- Deploy antimalware solution.

Answer:

A

Explanation:

When Web Application Firewalls (WAFs) are configured to block specific patterns (like ${), attackers may bypass this using URL encoding (e.g., %24%7B). In such cases, the WAF must decode these patterns before applying matching rules. Enabling URL decoding ensures the WAF recognizes encoded payloads and applies protections appropriately. This is a recommended hardening strategy against bypass techniques for command injection and remote code execution.

Question 6

Question Type: MultipleChoice

What is an antiforensic technique to cover a digital footprint?

Options:

A- authorization
B- obfuscation
C- privilege escalation
D- authentication

Answer:

B

Explanation:

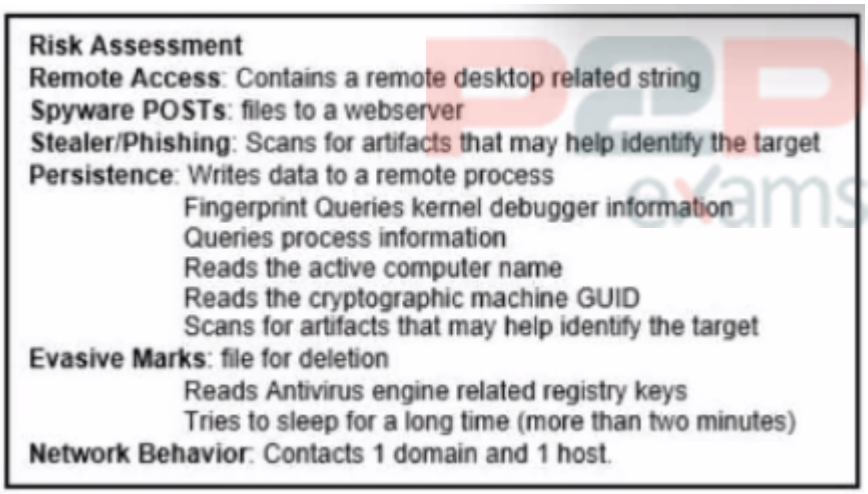
Antiforensic techniques are methods attackers use to cover their tracks. According to the Cisco CyberOps curriculum, ''obfuscation'' refers to techniques such as encoding, encrypting, or otherwise disguising commands, payloads, or scripts to avoid detection and analysis. This is a standard antiforensic tactic used to prevent attribution and hinder forensic investigation.

Options like privilege escalation and authentication are part of attack vectors or access control and not antiforensic methods.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.



The application x-dosexec with hash 691c65e4fb1d19f82465df1d34ad51aaeceba14a78167262dc7b2840a6a6aa87 is reported as malicious and labeled as "Trojan.Generic" by the threat intelligence tool. What is considered an indicator of compromise?

Options:

A- modified registry
B- hooking
C- process injection
D- data compression

Answer:

C

Explanation:

Comprehensive and Detailed

The exhibit lists several behaviors under categories such as Remote Access, Stealer/Phishing, Persistence, and Evasive Marks. Notably, under ''Persistence'' it states:

''Writes data to a remote process''

This behavior is indicative of ''process injection,'' a technique where malware writes or injects malicious code into the address space of another process. This allows the malware to evade detection and run within the context of a legitimate process.

This matches the MITRE ATT&CK technique T1055 (Process Injection), which is also discussed in the Cisco CyberOps Associate guide under evasion and persistence tactics used by malware.

While modified registry and data compression are possible signs of malware, they are not explicitly referenced in the exhibit. The definitive indicator shown is related to process injection.

Therefore, the correct answer is: C. process injection.

To Get Premium Files for 300-215 Visit
https://www.p2pexams.com/products/300-215

For More Free Questions Visit
https://www.p2pexams.com/cisco/pdf/300-215

P2P exams