350-201$^{Q\&As}$

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

QUESTION 1

A security architect in an automotive factory is working on the Cyber Security Management System and is implementing procedures and creating policies to prevent attacks. Which standard must the architect apply?

A. IEC62446

B. IEC62443

C. IEC62439-3

D. IEC62439-2

Correct Answer: B

QUESTION 2

A security analyst receives an escalation regarding an unidentified connection on the Accounting A1 server within a monitored zone. The analyst pulls the logs and discovers that a Powershell process and a WMI tool process were started on the server after the connection was established and that a PE format file was created in the system directory.

What is the next step the analyst should take?

A. Isolate the server and perform forensic analysis of the file to determine the type and vector of a possible attack

B. Identify the server owner through the CMDB and contact the owner to determine if these were planned and identifiable activities

C. Review the server backup and identify server content and data criticality to assess the intrusion risk

D. Perform behavioral analysis of the processes on an isolated workstation and perform cleaning procedures if the file is malicious

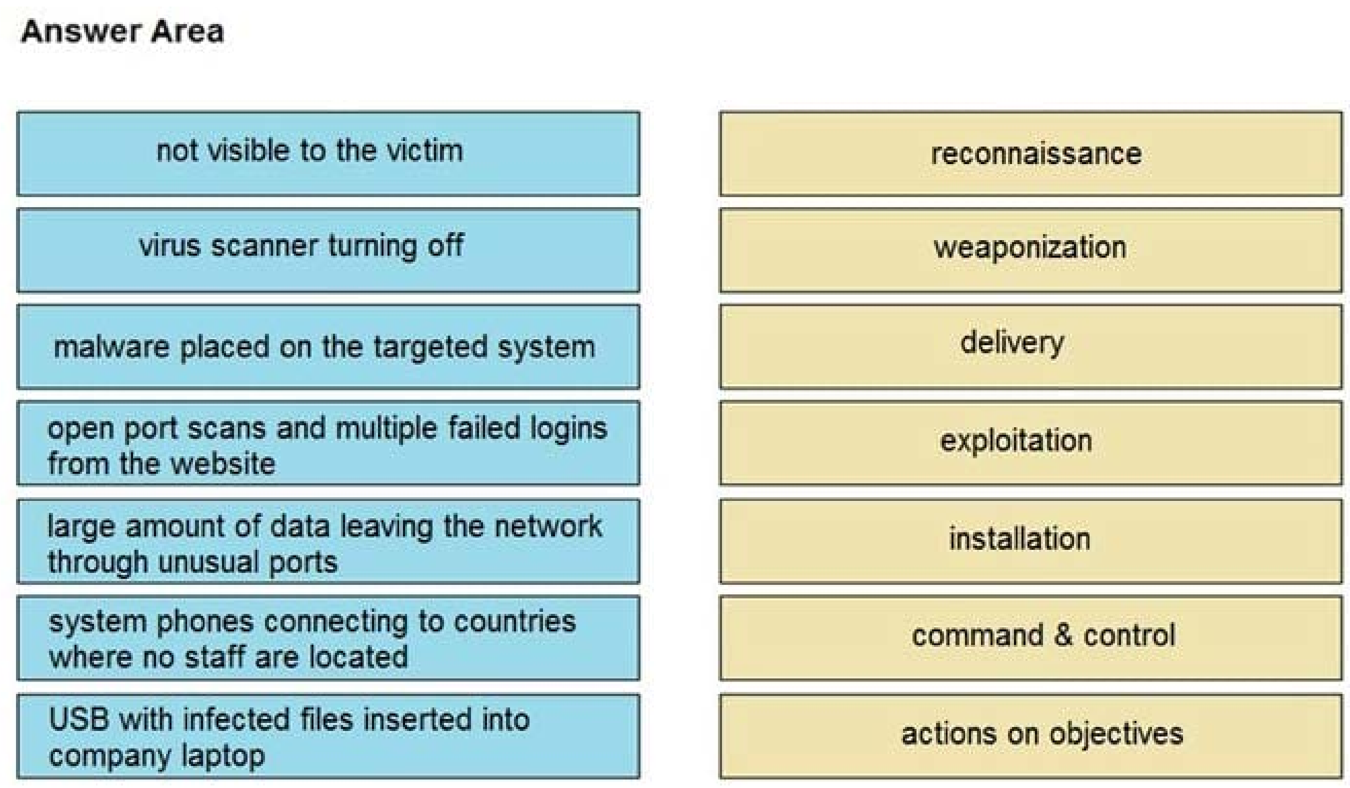
Correct Answer: C

QUESTION 3

DRAG DROP

Drag and drop the type of attacks from the left onto the cyber kill chain stages at which the attacks are seen on the right.

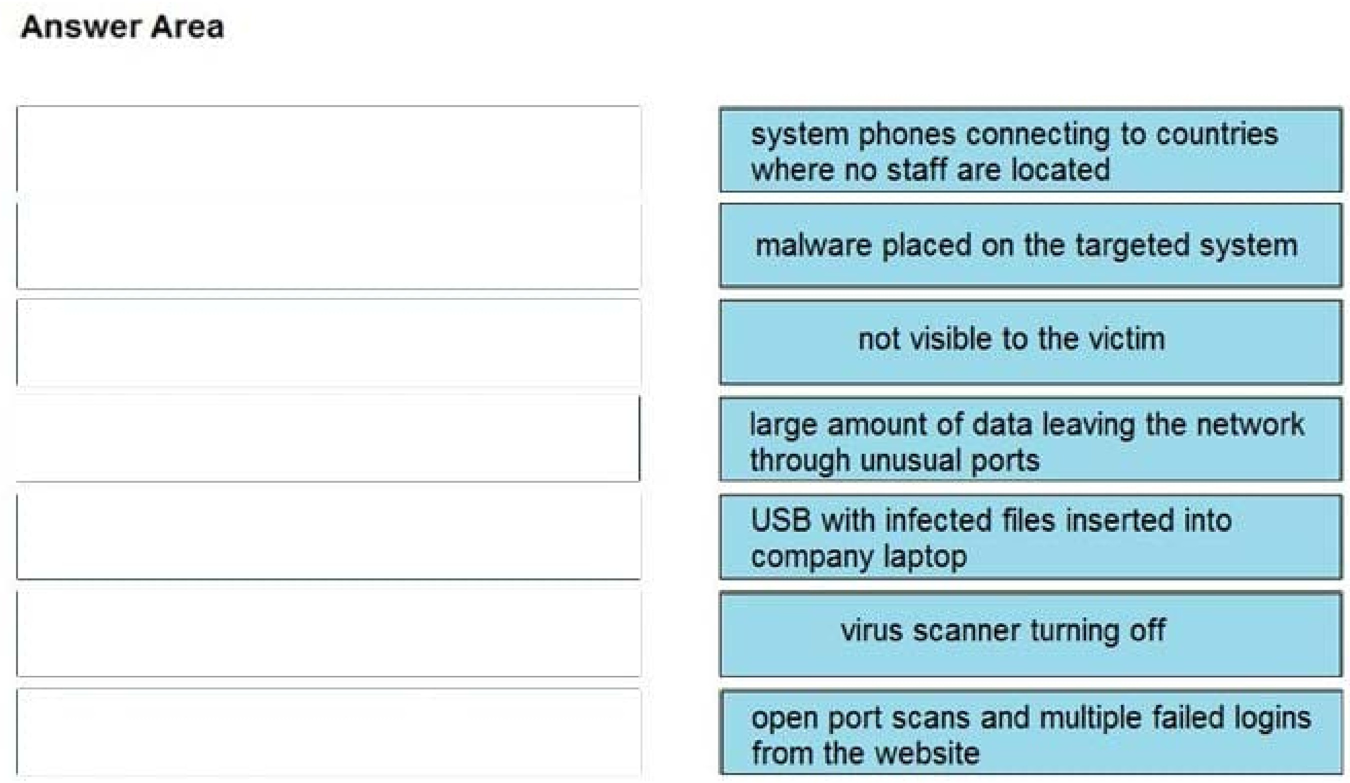
Select and Place:



Answer Area

not visible to the victim	reconnaissance
virus scanner turning off	weaponization
malware placed on the targeted system	delivery
open port scans and multiple failed logins from the website	exploitation
large amount of data leaving the network through unusual ports	installation
system phones connecting to countries where no staff are located	command & control
USB with infected files inserted into company laptop	actions on objectives

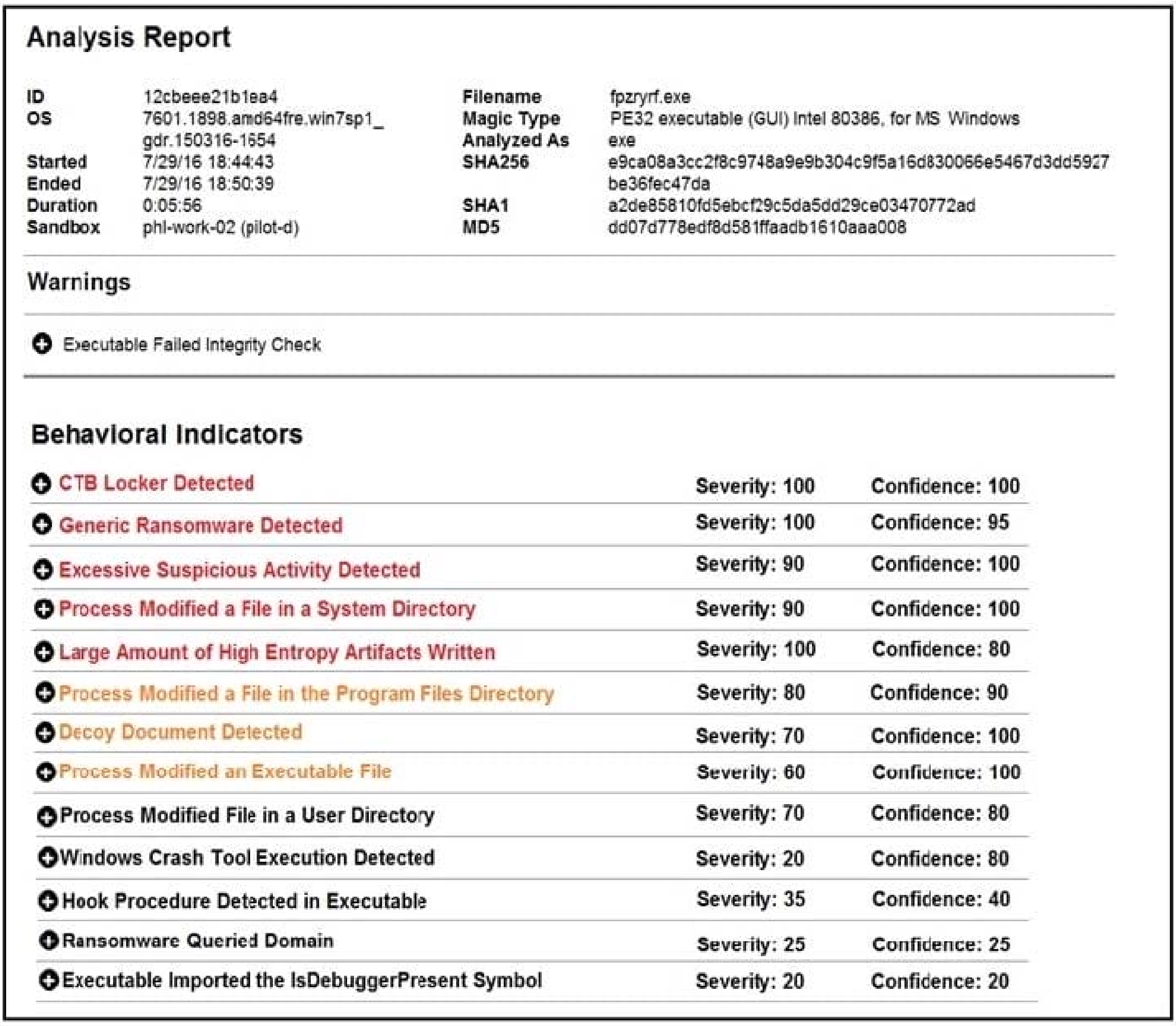
Correct Answer:



Answer Area

	system phones connecting to countries where no staff are located
	malware placed on the targeted system
	not visible to the victim
	large amount of data leaving the network through unusual ports
	USB with infected files inserted into company laptop
	virus scanner turning off
	open port scans and multiple failed logins from the website

QUESTION 4



Analysis Report

ID	12cbeee21b1ea4	Filename	fpzryrf.exe
OS	7601.1898.amd64fre.win7sp1_ gdr.150316-1654	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows
		Analyzed As	exe
Started	7/29/16 18:44:43	SHA256	e9ca08a3cc2f8c9748a9e9b304c9f5a16d830066e5467d3dd5927 be36fec47da
Ended	7/29/16 18:50:39		
Duration	0:05:56	SHA1	a2de85810fd5ebcf29c5da5dd29ce03470772ad
Sandbox	phl-work-02 (pilot-d)	MD5	dd07d778edf8d581ffaadb1610aaa008

Warnings

- Executable Failed Integrity Check

Behavioral Indicators

CTB Locker Detected	Severity: 100	Confidence: 100
Generic Ransomware Detected	Severity: 100	Confidence: 95
Excessive Suspicious Activity Detected	Severity: 90	Confidence: 100
Process Modified a File in a System Directory	Severity: 90	Confidence: 100
Large Amount of High Entropy Artifacts Written	Severity: 100	Confidence: 80
Process Modified a File in the Program Files Directory	Severity: 80	Confidence: 90
Decoy Document Detected	Severity: 70	Confidence: 100
Process Modified an Executable File	Severity: 60	Confidence: 100
Process Modified File in a User Directory	Severity: 70	Confidence: 80
Windows Crash Tool Execution Detected	Severity: 20	Confidence: 80
Hook Procedure Detected in Executable	Severity: 35	Confidence: 40
Ransomware Queried Domain	Severity: 25	Confidence: 25
Executable Imported the IsDebuggerPresent Symbol	Severity: 20	Confidence: 20

Refer to the exhibit. Cisco Advanced Malware Protection installed on an end-user desktop has automatically submitted a low prevalence file to the Threat Grid analysis engine for further analysis. What should be concluded from this report?

A. The prioritized behavioral indicators of compromise do not justify the execution of the "ransomware" because the scores do not indicate the likelihood of malicious ransomware.

B. The prioritized behavioral indicators of compromise do not justify the execution of the "ransomware" because the scores are high and do not indicate the likelihood of malicious ransomware.

C. The prioritized behavioral indicators of compromise justify the execution of the "ransomware" because the scores are high and indicate the likelihood that malicious ransomware has been detected.

D. The prioritized behavioral indicators of compromise justify the execution of the "ransomware" because the scores are low and indicate the likelihood that malicious ransomware has been detected.

Correct Answer: C

QUESTION 5

An engineer received multiple reports from users trying to access a company website and instead of landing on the website, they are redirected to a malicious website that asks them to fill in sensitive personal data. Which type of attack is occurring?

A. Address Resolution Protocol poisoning

B. session hijacking attack

C. teardrop attack

D. Domain Name System poisoning

Correct Answer: D