350-201 Q&As

Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Pass Cisco 350-201 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/350-201.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the exhibit. Which command was executed in PowerShell to generate this log?

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

A. Get-EventLog -LogName*

B. Get-EventLog -List

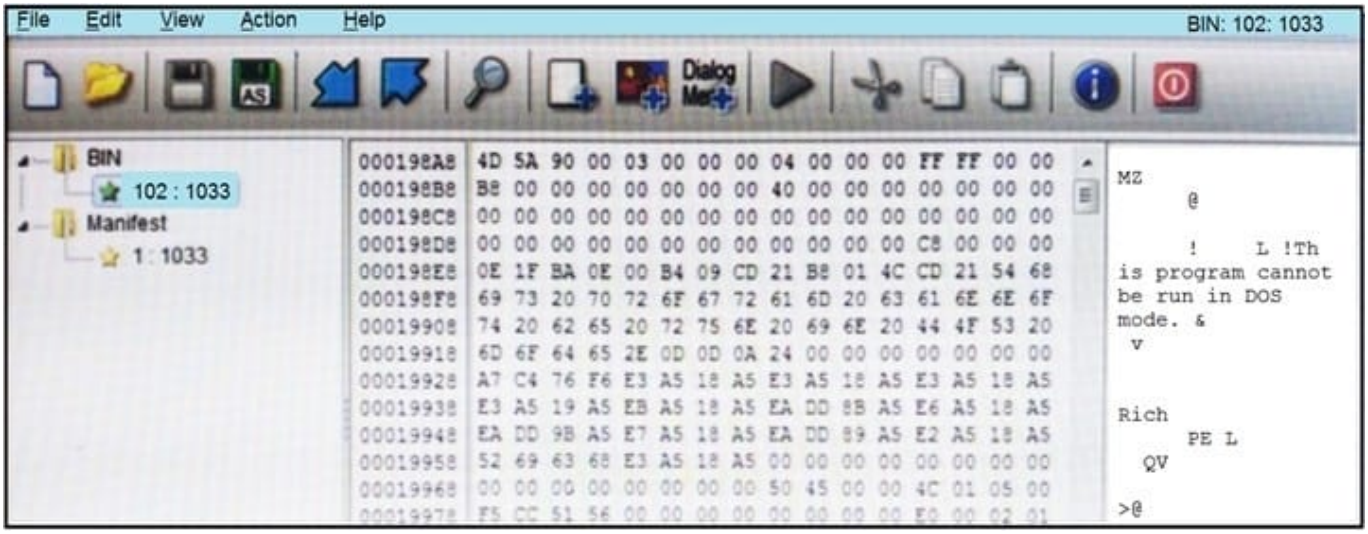
C. Get-WinEvent -ListLog* -ComputerName localhost

D. Get-WinEvent -ListLog*

Correct Answer: A

Reference: https://lists.xymon.com/archive/2019-March/046125.html

QUESTION 2



Refer to the exhibit. An engineer is reverse engineering a suspicious file by examining its resources. What does this file indicate?

A. a DOS MZ executable format

B. a MS-DOS executable archive

C. an archived malware

D. a Windows executable file

Correct Answer: D

Reference: https://stackoverflow.com/questions/2577545/why-is-this-program-cannot-be-run-in-dos-mode-text-present-in-dll-files#:~:text=The%20linker%20places%20a%20default,using%20the%20%2FSTUB%20linker%20option.andtext=This%20information%20enables%20Windows%20to,has%20an%20MS-DOS%20stub.

QUESTION 3

Refer to the exhibit. An engineer is performing static analysis of a file received and reported by a user. Which risk is indicated in this STIX?

```
HttpWebRequest httpWebRequest = (HttpWebRequest)WebRequest.Create("http://freegeoip.net/xml/");
httpWebRequest.UserAgent = "Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0";
httpWebRequest.Proxy = null;
httpWebRequest.Timeout = 10000;
using (HttpWebResponse httpWebResponse = (HttpWebResponse)httpWebRequest.GetResponse())
{
    using (Stream responseStream = httpWebResponse.GetRepsonseStream())
    {
        using (StreamReader streamReader = new StreamReader(responseStream))
        {
            string xml = streamReader.ReadToEnd();
            XmlDocument xmlDocument = new XmlDocument();
            xmlDocument.LoadXml(xml);
            string innerXml = xmlDocument.SelectSingleNode("Response//IP").InnerXml;
            string innerXml2 = xmlDocument.SelectSingleNode("Response//CountryName").InnerXml;
            string innerXml3 = xmlDocument.SelectSingleNode("Response//CountryCode").InnerXml;
            string innerXml4 = xmlDocument.SelectSingleNode("Response//RegionName").InnerXml;
            string innerXml5 = xmlDocument.SelectSingleNode("Response//City").InnerXml;
            string innerXml6 = xmlDocument.SelectSingleNode("Response//TimeZone").InnerXml;
```

A. The file is redirecting users to a website that requests privilege escalations from the user.

B. The file is redirecting users to the website that is downloading ransomware to encrypt files.

C. The file is redirecting users to a website that harvests cookies and stored account information.

D. The file is redirecting users to a website that is determining users' geographic location.

Correct Answer: D

QUESTION 4

Refer to the exhibit. What is the connection status of the ICMP event?

Distribution Port/ICMP Code	Message	Classification	Application Protocol	Client	Application Risk	Business Relevance	Access Control Rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129:2:2)	Generic Protocol Command Decode	ICMP	ICMP client	Medium	Medium	rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129:2:2)	Generic Protocol Command Decode	DNS	DNS client	Very Low	Very High	Default Action
0 (No Code) / icmp	PROTOCOL-ICMP Echo Reply (1:408:8)	Misc Activity	DNS	DNS client	Very Low	Very High	Allow ICMP
54107 / udp	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt (3:19187:7)	Attempted User Privilege Gain	DNS	DNS client	Very Low	Very High	
49367 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
57477 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
54879 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
60999 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52240 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
54359 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52489 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
60169 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52250 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52485 / up	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
49940 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
57214 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
51608 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52652 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55528 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
61222 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55640 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55991 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	

A. blocked by a configured access policy rule

B. allowed by a configured access policy rule

C. blocked by an intrusion policy rule

D. allowed in the default action

Correct Answer: B

QUESTION 5

An engineer notices that every Sunday night, there is a two-hour period with a large load of network activity. Upon further investigation, the engineer finds that the activity is from locations around the globe outside the organization\\'s service area. What are the next steps the engineer must take?

A. Assign the issue to the incident handling provider because no suspicious activity has been observed during business hours.

B. Review the SIEM and FirePower logs, block all traffic, and document the results of calling the call center.

C. Define the access points using StealthWatch or SIEM logs, understand services being offered during the hours in question, and cross-correlate other source events.

D. Treat it as a false positive, and accept the SIEM issue as valid to avoid alerts from triggering on weekends.

Correct Answer: A