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.passapply.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

A SOC engineer discovers that the organization had three DDOS attacks overnight. Four servers are reported offline, even though the hardware seems to be working as expected. One of the offline servers is affecting the pay system reporting times. Three employees, including executive management, have reported ransomware on their laptops. Which steps help the engineer understand a comprehensive overview of the incident?

A. Run and evaluate a full packet capture on the workloads, review SIEM logs, and define a root cause.

B. Run and evaluate a full packet capture on the workloads, review SIEM logs, and plan mitigation steps.

C. Check SOAR to learn what the security systems are reporting about the overnight events, research the attacks, and plan mitigation step.

D. Check SOAR to know what the security systems are reporting about the overnight events, review the threat vectors, and define a root cause.

Correct Answer: D

QUESTION 2

Refer to the exhibit. Which indicator of compromise is represented by this STIX?

```
{
  "type": "bundle",
  "id": "bundle--56be2a39",
  "objects": [
        {
          "type": "indicator",
          "spec_version": "2.1",
          "id": "indicator--d81f86b9-9f",
          "created": "2020-08-10T13:49:37.079Z",
          "modified": "2020-08-10T13:49:37.079Z",
          "name": "Malicious site hosting downloader",
          "indicator_types":[
                "malicious-activity"
          ],
          "pattern": "[url:value = 'http://y2z7atc.cn/4823/']",
          "pattern_type": "stix",
          "valid_from": "2020-08-10T13:49:37.079Z"
        },
        {
          "type": "malware",
          "spec_version": "2.1",
          "id": "malware- -162d9 a",
          "created": "2020-08-13T09:15:17.182Z",
          "modified": "2020-08-13T09:15:17.182Z",
          "name": "y2z7atc backdoor",
          "malware_types": [
                "backdoor",
                "remote-access-trojan"
          ],
          "is_family": false,
          "kil_chain_phases": [
                {
                  "kill_chain_name": "mandant-attack-lifecycle-model",
                  "phase_name": "establish-foothold"
                }
          ]

        },
        {
          "type": "relationship",
          "spec_version": "2.1",
          "id": "relationship--864af2e5",
          "created": "2020-08-15T18:03:58.029Z",
          "modified": "2020-08-15T18:03:58.029Z",
          "relationship_type": "indicates",
          "source_ref": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4"
          "target_ref": "malware--162d917e07661-4611-b5d6-652791454fca"
        }
    ]
}
```

A. website redirecting traffic to ransomware server

B. website hosting malware to download files

C. web server vulnerability exploited by malware

D. cross-site scripting vulnerability to backdoor server

Correct Answer: C

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

What is the HTTP response code when the REST API information requested by the authenticated user cannot be found?

A. 401

B. 402

C. 403

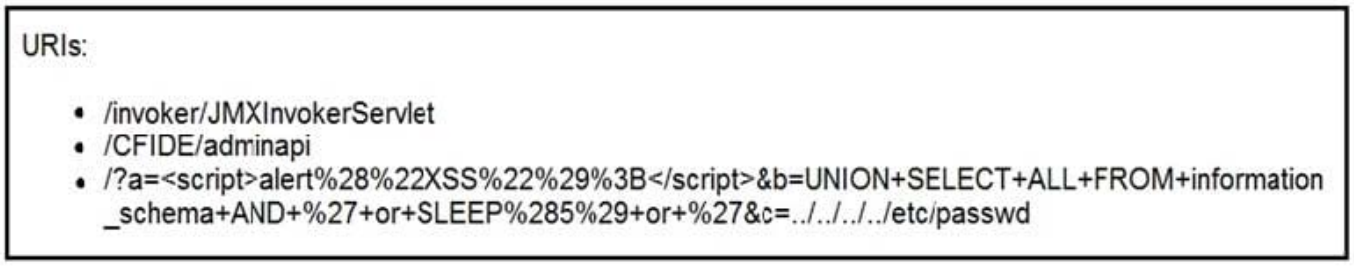
D. 404

E. 405

Correct Answer: A

Reference: https://airbrake.io/blog/http-errors/401-unauthorized-error#:~:text=The%20401%20Unauthorized%20Error%20is,client%20could%20not%20be%20authenticated.

QUESTION 5



Refer to the exhibit. At which stage of the threat kill chain is an attacker, based on these URIs of inbound web requests from known malicious Internet scanners?

A. exploitation

B. actions on objectives

C. delivery

D. reconnaissance

Correct Answer: C

Reference: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-101-july2017.pdf