CertsDeals

Free Questions for 200-201 by certsdeals

Shared by Brewer on 22-07-2024

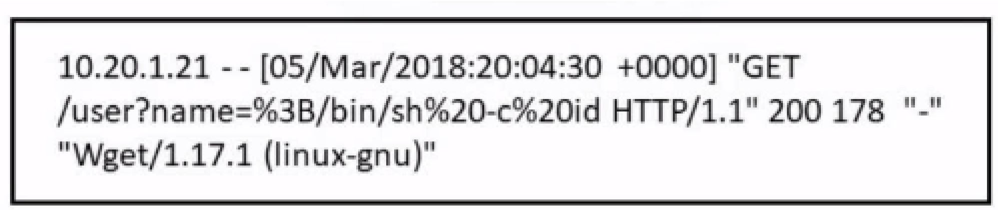
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Refer to the exhibit.



```
10.20.1.21 - - [05/Mar/2018:20:04:30 +0000] "GET
/user?name=%3B/bin/sh%20-c%20id HTTP/1.1" 200 178 "-"
"Wget/1.17.1 (linux-gnu)"
```

Which attack is being attempted against a web application?

Options:

A- SQL injection

B- man-in-the-middle

C- command injection

D- denial of service

Answer:

C

Explanation:

The exhibit shows an HTTP GET request with a parameter that includes ; /bin/sh -c id.

This indicates a command injection attempt, where the attacker is trying to execute shell commands on the server.

Command injection vulnerabilities allow an attacker to execute arbitrary commands on the host operating system via a vulnerable application.

The use of /bin/sh and the -c flag is typical in command injection exploits to run shell commands, such as id, which returns user identity information.

OWASP Command Injection

Analyzing HTTP Requests for Injection Attacks

Web Application Security Testing Guidelines

Question 2

Question Type: MultipleChoice

According to CVSS, what is attack complexity?

Options:

A- existing exploits available in the wild exploiting the vulnerability

B- existing circumstances beyond the attacker's control to exploit the vulnerability

C- number of actions an attacker should perform to exploit the vulnerability

D- number of patches available for certain attack mitigation and how complex the workarounds are

Answer:

B

Explanation:

In the Common Vulnerability Scoring System (CVSS), attack complexity refers to the conditions beyond the attacker's control that must exist for the vulnerability to be successfully exploited.

This includes factors such as the need for user interaction, the presence of specific configurations, or network conditions that are not easily controlled by the attacker.

A high attack complexity means that these external factors make exploitation more difficult, while a low attack complexity indicates that fewer such conditions are required.

CVSS v3.1 Specifications Document

Understanding Attack Complexity in Vulnerability Assessments

Cybersecurity Frameworks and Metrics

Question 3

Question Type: MultipleChoice

What is a comparison between rule-based and statistical detection?

Options:

A- Statistical is based on measured data while rule-based uses the evaluated probability approach.

B- Rule-based Is based on assumptions and statistical uses data Known beforehand.

C- Rule-based uses data known beforehand and statistical is based on assumptions.

D- Statistical uses the probability approach while rule-based Is based on measured data.

Answer:

C

Explanation:

Rule-based detection methods rely on predefined rules and patterns that are known beforehand. These rules are created based on prior knowledge of what constitutes normal and abnormal behavior.

Statistical detection, on the other hand, involves analyzing data to identify anomalies. It is based on assumptions about what normal behavior looks like and uses statistical methods to detect deviations from this norm.

Rule-based systems are typically straightforward but may miss novel attacks that do not match existing rules.

Statistical methods can detect previously unknown threats by recognizing patterns that deviate from established baselines but may produce more false positives.

Intrusion Detection Systems (IDS) Concepts

Comparative Studies on Rule-based and Statistical Anomaly Detection

Understanding Anomaly Detection in Network Security

Question 4

Question Type: **MultipleChoice**

An engineer configured regular expression "."\.(pd][Oo][Cc)|[Xx][Ll][Ss]|[Pp][Pp][Tt]) HTTP/1 .[01]" on Cisco ASA firewall. What does this regular expression do?

Options:

A- It captures documents in an HTTP network session.

B- It captures .doc, .xls, and .pdf files in HTTP v1.0 and v1.1.

C- It captures .doc, .xls, and .ppt files extensions in HTTP v1.0.

D- It captures Word, Excel, and PowerPoint files in HTTPv1.0 and v1.1.

Answer:

D

Explanation:

The regular expression provided is: .\.(pd][Oo][Cc)|[Xx][Ll][Ss]|[Pp][Pp][Tt]) HTTP/1 .[01]

This regular expression is designed to match file extensions for Word (.doc), Excel (.xls), and PowerPoint (.ppt) files in HTTP network sessions.

The regular expression uses character classes and alternatives to match different case variations of these file extensions.

The part .\.(pd][Oo][Cc)|[Xx][Ll][Ss]|[Pp][Pp][Tt]) matches the file extensions, and HTTP/1 .[01] ensures that the match is in the context of HTTP version 1.0 or 1.1.

Cisco ASA Regular Expressions Documentation

Understanding Regular Expressions in Network Security

Filtering and Capturing HTTP Traffic with Regex

Question 5

Question Type: MultipleChoice

A security engineer must protect the company from known issues that trigger adware. Recently new incident has been raised that could harm the system. Which security concepts are present in this scenario?

Options:

A- exploit and patching

B- risk and evidence

C- analysis and remediation

D- vulnerability and threat

Answer:

D

Explanation:

The security scenario involves protecting the company from known issues that trigger adware and addressing a recent incident that could harm the system.

This scenario involves identifying vulnerabilities (weaknesses in the system that can be exploited) and threats (potential harm that can exploit these vulnerabilities).

A vulnerability is an inherent flaw in the system, while a threat is an event or condition that has the potential to exploit the vulnerability.

The security engineer needs to assess both the vulnerabilities present and the threats that could exploit these vulnerabilities to implement effective protection measures.

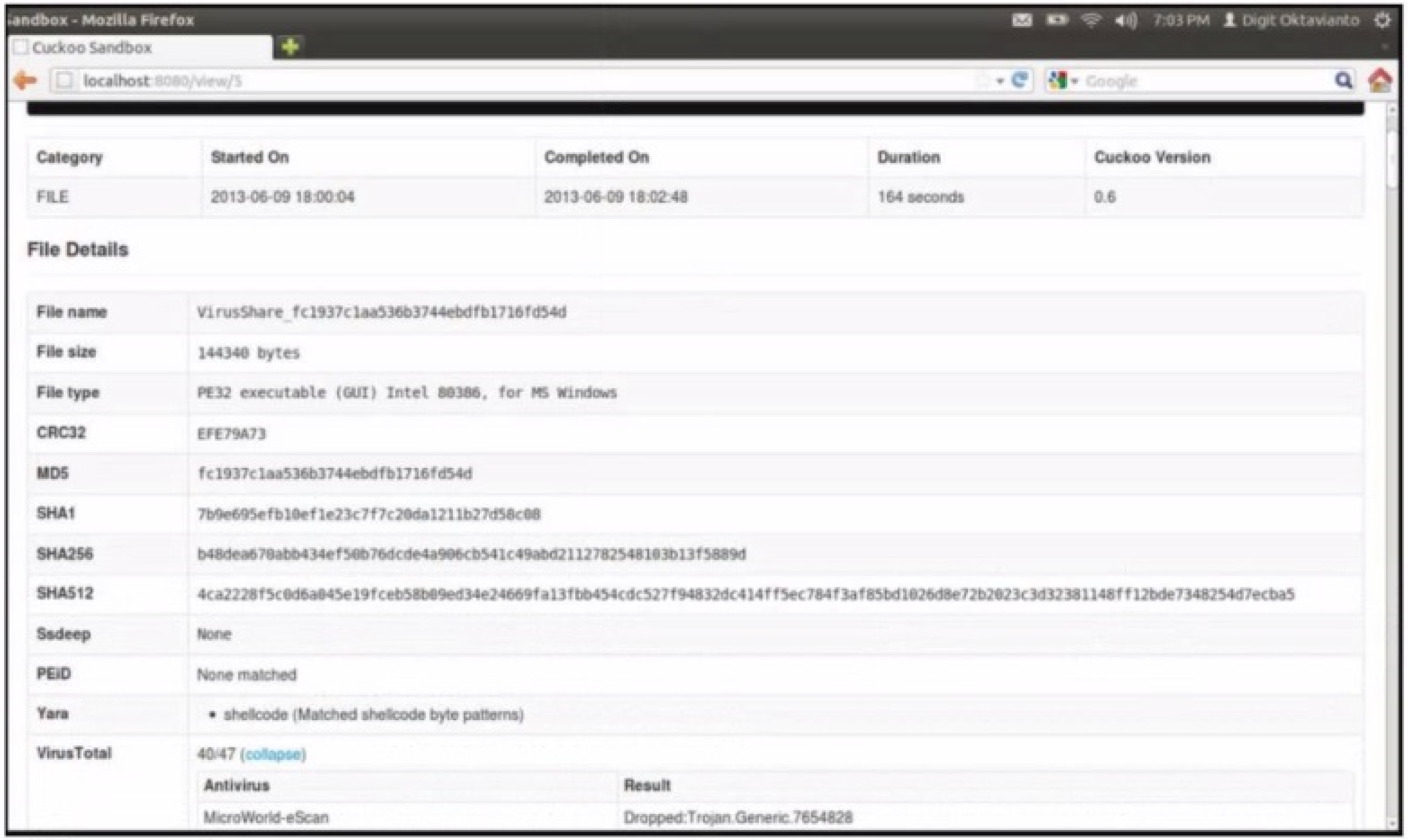
Cisco Cybersecurity Operations Fundamentals

Concepts of Vulnerability and Threat in Cybersecurity

Question 6

Question Type: MultipleChoice

Refer to the exhibit.



Category	Started On	Completed On	Duration	Cuckoo Version
FILE	2013-06-09 18:00:04	2013-06-09 18:02:48	164 seconds	0.6

File Details

File name	VirusShare_fc1937c1aa536b3744ebdfb1716fd54d
File size	144340 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	EFE79A73
MD5	fc1937c1aa536b3744ebdfb1716fd54d
SHA1	7b9e695efb10ef1e23c7f7c20da1211b27d58c08
SHA256	b48dea670abb434ef50b76dcde4a906cb541c49abd2112782548103b13f5889d
SHA512	4ca2228f5c0d6a045e19fceb58b09ed34e24669fa13fbb454cdc527f94832dc414ff5ec784f3af85bd1026d8e72b2023c3d32381148ff12bde7348254d7ecba5
Ssdeep	None
PEiD	None matched
Yara	• shellcode (Matched shellcode byte patterns)
VirusTotal	40/47 (collapse)

Antivirus	Result
MicroWorld-eScan	Dropped:Trojan.Generic.7654828

What does this Cuckoo sandbox report indicate?

Options:

A- The file is spyware.

B- The file will open unsecure ports when executed.

C- The file will open a command interpreter when executed.

D- The file is ransomware.

Answer:

C

Explanation:

The Cuckoo sandbox report shows the analysis results of a file named 'VirusShare_fc1937c1aa536b3744ebfb1716fd5f4d'.

The file type is identified as a PE32 executable for MS Windows.

The 'Yara' section indicates that the file contains shellcode, which matches specific shellcode byte patterns.

Shellcode typically indicates that the file will execute a payload, often used to open a command interpreter or execute commands directly.

Additionally, the antivirus result shows that the file was identified as containing a trojan (Trojan.Generic.7654828), which is consistent with behaviors such as opening a command interpreter for malicious purposes.

Cuckoo Sandbox Documentation

Analysis of Shellcode Behavior

Understanding Trojan Malware Functionality

Question 7

Question Type: **MultipleChoice**

An engineer must investigate suspicious connections. Data has been gathered using a tcpdump command on a Linux device and saved as sandboxmatware2022-12-22.pcaps file. The engineer is trying to open the tcpdump in the Wireshark tool. What is the expected result?

Options:

A- The tool does not support Linux.

B- The file is opened.

C- The file has an incorrect extension.

D- The file does not support the'-' character.

Answer:

B

Explanation:

Wireshark is a widely used network protocol analyzer that supports various capture file formats, including those generated by tcpdump.

The .pcap extension is a standard format for packet capture files and is fully supported by Wireshark.

The file extension or the inclusion of characters such as '-' in the file name does not impact Wireshark's ability to open and read the file.

When the engineer opens the sandboxmatware2022-12-22.pcaps file in Wireshark, the tool will read the packet capture data, allowing for detailed analysis of network traffic.

Cisco Cybersecurity Operations Fundamentals

Wireshark User Guide

tcpdump and libpcap Documentation

Question 8

Question Type: MultipleChoice

Which type of data is used to detect anomalies in the network?

Options:

A- statistical data

B- alert data

C- transaction data

D- metadata

Answer:

A

Explanation:

Statistical data is crucial for detecting anomalies within a network because it provides a baseline of normal behavior.

Anomaly detection involves comparing current network data against historical statistical data to identify deviations from expected patterns.

This method helps in identifying unusual activities that could signify a security threat, such as unusual login attempts, data transfers, or access patterns.

Statistical data analysis tools use metrics such as mean, variance, and standard deviation to flag anomalies, aiding in proactive threat detection.

Cisco Cybersecurity Operations Fundamentals

Network Anomaly Detection Techniques

Statistical Methods in Cybersecurity

Question 9

Question Type: MultipleChoice

Which items is an end-point application greylist used?

Options:

A- Items that have been established as malicious

B- Items that have been established as authorized

C- Items that have been installed with a baseline

D- Items before being established as harmful or malicious

Answer:

D

Explanation:

A greylist in endpoint applications refers to a list of items that are not yet classified as either good (whitelisted) or bad (blacklisted).

The primary function of a greylist is to hold applications, processes, or files that are under observation due to their unknown status.

These items are neither trusted nor immediately flagged as harmful, allowing security teams to monitor them closely for any suspicious behavior.

By placing items on a greylist, security operations can prevent potential threats without disrupting legitimate processes, awaiting further analysis to determine their true nature.

Cisco Cybersecurity Operations Fundamentals

Endpoint Security Best Practices

Greylisting Concepts in Cybersecurity

Question 10

Question Type: MultipleChoice

What matches the regular expression c(rgr)+e?

Options:

A- crgrrgre

B- np+e

C- c(rgr)e

D- ce

Answer:

A

Explanation:

The regular expressionc(rgr)+ematches strings where "rgr" occurs one or more times between "c" and "e". The string "crgrrgre" fits this pattern as it has the sequence "rgr" repeated twice between "c" and "e".The plus sign (+) in the regular expression indicates that the preceding element must appear one or more times for a match to occur