Lab - Analyze Exploit Code

Objectives

In this lab, you will research and analyze examples of exploit code.

- Conduct research and analyze code samples.

Background / Scenario

In this lab, you will interpret command line statements and code samples.

Required Resources

- PC or mobile device
- Internet access

Instructions

Part 1: Conduct research and analyze exploit code samples.

1. Refer to the following command.

```
nmap -sV --script vulners --script-args mincvss=4 10.6.6.23
```

What information will be displayed from the command?

Answer Area

Vulnerability scan. Checks for known vulnerabilities (CVEs) based on the detected software versions. Limited to vulnerabilities with a CVSS score of >=4

Show Answer

What Kali tool is being launched with the above script?

Answer Area

GVM scanner. (Greenbone Vulnerability Management) and it's an open-source framework used for vulnerability scanning and management.

Show Answer

What scripting language do you think was used?

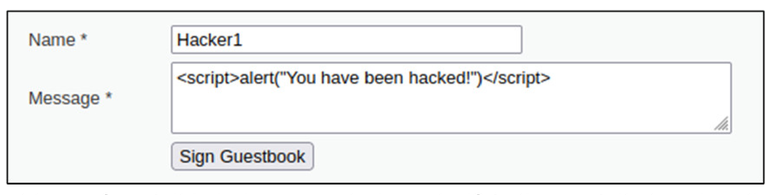
Answer Area

bash script

Show Answer

To learn more about the features and syntax of bash scripts. Search the web for “bash script examples.”

3. Refer to the line of code shown in the message box.



What type of exploit is being executed created? Is the exploit stored on the client side or the server side? What language is it?

Answer Area

Server side
Javascript

Show Answer

In an actual exploit, what could malicious this code do?

Answer Area

Trigger a false warning. Refer users to visit other sites

Show Answer

4. Refer to the following command.

```
nmap --script smb-enum-users.nse -p139,445 10.6.6.23
```

What information will be displayed from the command?

Answer Area

list user accounts via the SMB (Server Message Block) protocol on a target system

Show Answer

5. Refer to the following command.

```
1' OR 1=1 UNION SELECT user, password FROM users #
```

What type of exploit is shown? What is the purpose of the following line of code?

Answer Area

pick sensitive user account information from a db

Show Answer

6. Refer to the following commands.

```
smbclient //172.17.0.2/tmp
smb: >put malicious_file.txt malicious_file.txt
```

What is being attempted with the commands?

Answer Area

file transfer using smbclient

Show Answer

Reflection

Why is it important that an Ethical Hacker be familiar with exploit code in various scripting languages?

Answer Area

to know how to assess security of various systems

Show Answer

Show All Answers Clear My Responses