**MIS6130 LABS ASSIGNMENT**

**DAVID KIMANI 652263**

**Understanding the Basic Concepts of Scripting and Software Development**

**Brief about the Lab**

**Overview**

* To work successfully as a penetration tester, you need to be familiar with coding, most specifically scripting languages, although knowledge of common compiled languages is also a plus. There are two major reasons for this. First, malware is code. Some of it is compiled code, and much of it is scripts.

**Logic Constructs**

* Loops - repeatedly execute a section of code
* Conditionals - programming language commands that are used for handling decisions (if) statement
* Boolean operators - simple words (AND, OR, NOT, or AND NOT) that are used as conjunctions
* String operators - allow you to manipulate values of variables in various useful ways
* Arithmetic operators - perform mathematical operations

**Data Structures**

* JavaScript Object Notation (JSON): JSON is a lightweight format for storing and transporting data that is easy to understand
* ***Arrays***: An array is a special variable that holds more than one value at a time
* ***Lists***: A list is a data structure in programming languages that contains an ordered structure of elements.
* ***Trees***: A tree is a non-linear data structure represented using nodes in a hierarchical model.
* **Libraries** - collection of resources that can be reused by programs
* ***procedure*** - a section of code that is created to perform a specific task
* **Function** - a block of code that is very useful when you need to execute similar tasks over and over
* ***class*** - a code template that can be used to create different objects

**Popular Pentest Programming Languages**

* JavaScript
* Ruby
* PowerShell
* Python
* Bash

**Lab 10.1.19**

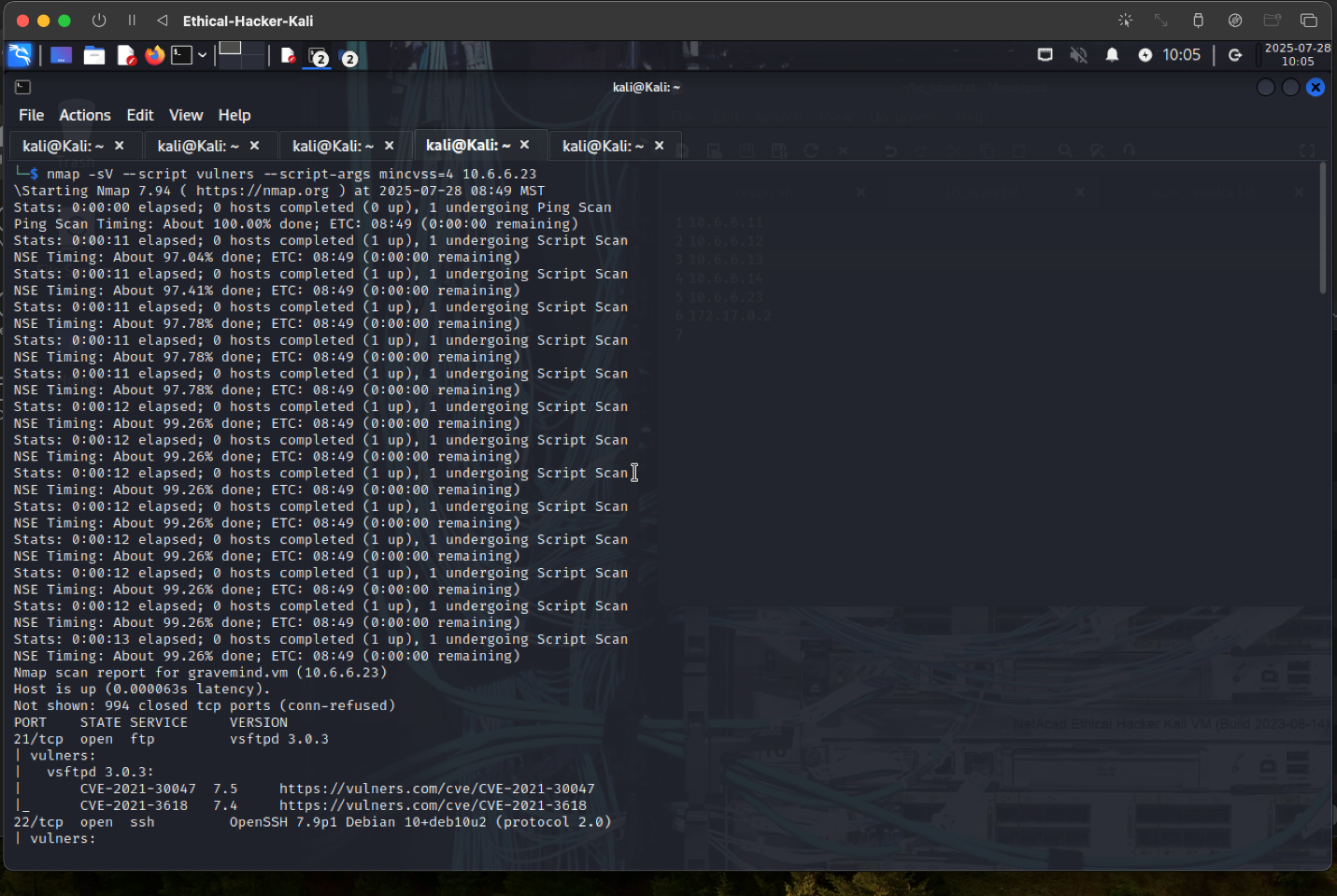
**Query 1:**

Running this command:

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

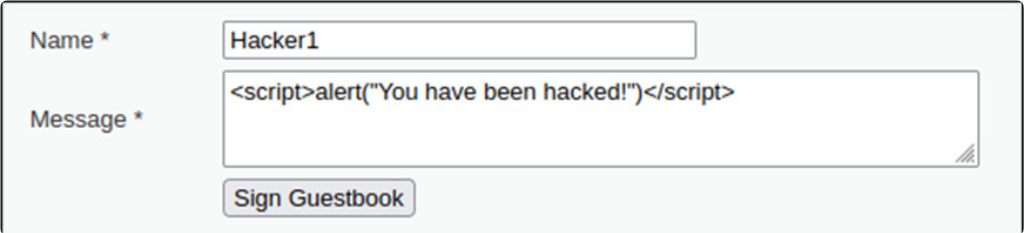
What do we see?

* Runs a vulnerability scan. Checks for known vulnerabilities (CVEs) based on the detected software versions. Limited to vulnerabilities with a CVSS score of >=4
* (CVSS) - Common Vulnerability Scoring System
* Uses GVM scanner (Greenbone Vulnerability Management) - an open-source framework used for vulnerability scanning and management.



**Query 2:**

Refer to the line of code shown



What type of exploit is being executed created?

* It is a stored XSS exploit. The exploit is stored on the server side. It is JavaScript.

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

* Trigger a false warning. Refer users to visit other sites

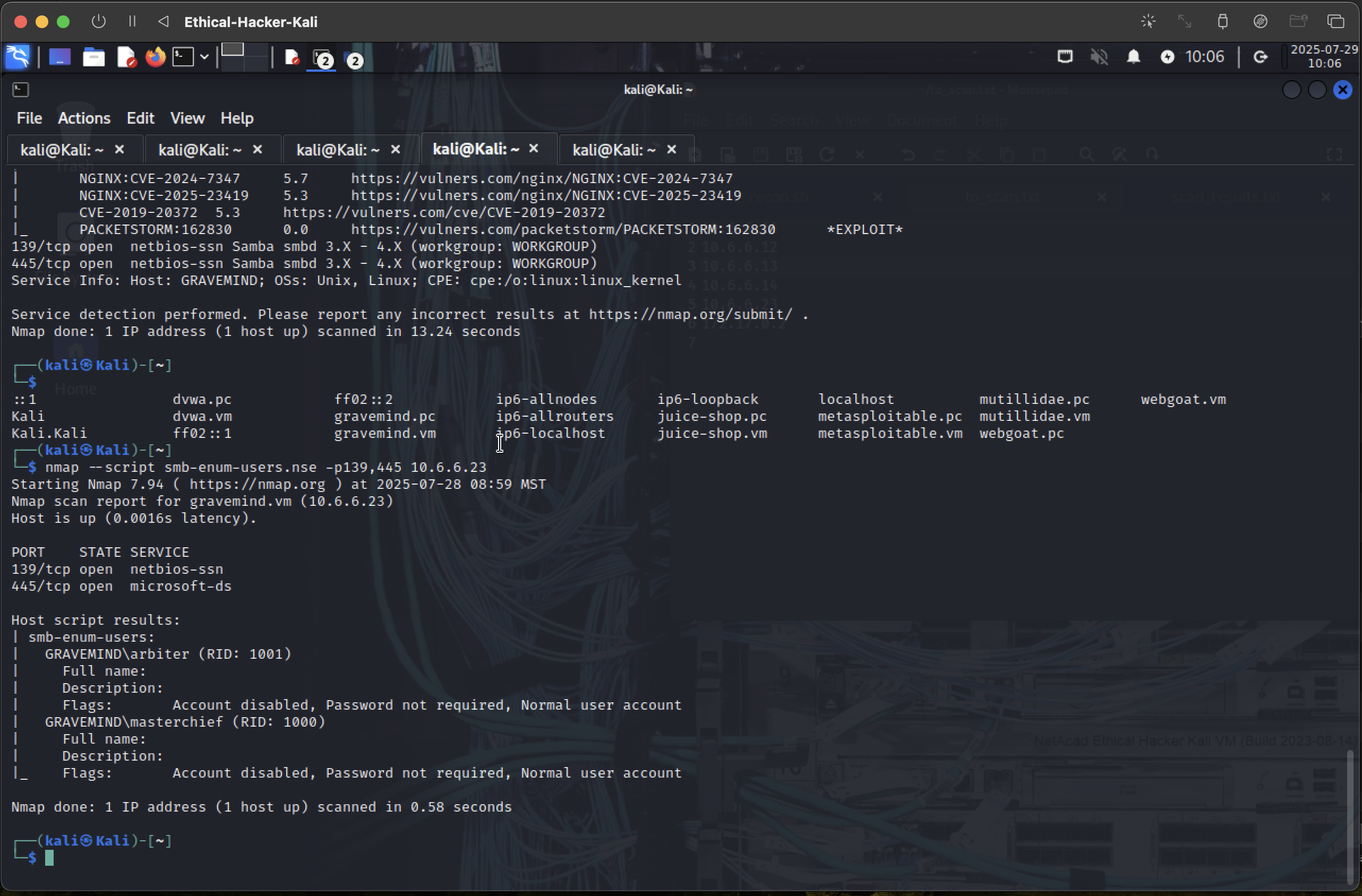
**Query 3:**

Run this command:

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

What do we see?

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



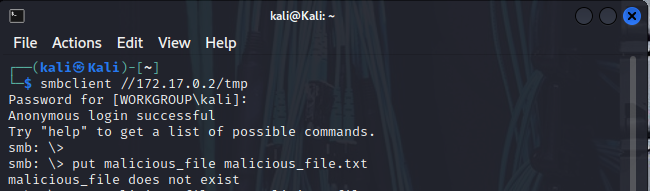
**Query 4:**

Run this command:

* smbclient //172.17.0.2/tmp  
  smb: >put malicious\_file.txt malicious\_file.txt

What do we see?

* We see a transfer of files between systems using the smbclient utility



**Query 5:**

Run this command:

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

What do we see?

* It’s an SQL injection exploit. The purpose is to retrieve usernames and passwords from a database table called “users”

**Conclusion**

What’s the importance of being familiar with exploit code in various scripting languages?

* Ethical Hackers may need to create or use exploit scripts in order to assess the security of various systems, including web applications.