Penetration testing and vulnerability assessment report

Aarya Dahal

BSc.Hons.Ethical Hacking and CyberSecurity, Softwarica College

ST5063CEM: Practical Pen-Testing

Nirmal Dahal

February 24, 2023

Abstract

This report is a sample report of penetration testing and vulnerability assessment report of machine sumo that was given to us.

PENETRATION TESTING AND VULNERABILITY REPORT

FOR HACKME.INC

AARYA DAHAL

2023

Confidentiality Statement

The contents of this document are exclusive property of HACKME Inc. and Aarya Dahal which are proprietary and confidential, it is not to be permitted duplication, redistribution or use without the consent of both HACKME Inc. and Aarya Dahal.

Disclaimer

The report is produced based on the allotted time. All conclusions and suggestions made will only be held accountable during the test itself, not later. Time-limited involvement prevents a thorough assessment of all security safeguards.

Document Details

Company	IAMSECURE Inc.
Document Title	Vulnerability Assessment and Penetration Testing
Duration	February 2023
Abstract	VAPT on HACKME Inc. to check for any security issues and breaches possible.
Classification	Confidential

Table of Contents

Table of Figures

Analytical Summary

A test was done where a simulated cyberattack was carried out on the network of HACKME Inc. to identify and examine its potential weaknesses. An immediate approach must be taken for security checks for any system breaches that could occur, starting off with gathering information about the system. List of vulnerabilities were found, and tested for any further privilege escalation that could occur due to it.

With further analysis I found out that the system could be completely breached to reach the highest privilege possible by some critical level vulnerabilities. A major shellshocks' vulnerability was found. It is highly recommended that HACKME Inc. address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Moreover, the results of the test were analyzed and reported, with recommendations for making the system more secure. CVSS 3.1 was used to check for CVS score.

Scope

Assessment	Details
External Penetration Test	HACKME INC. (192.168.150.87)

Objectives

By locating potential vulnerabilities and weakness in an organization's IT systems, network, or applications, an attacker's ability to gain unauthorized access, compromise data, or harm the system is tested during the penetration. This penetration test aims to do the following:

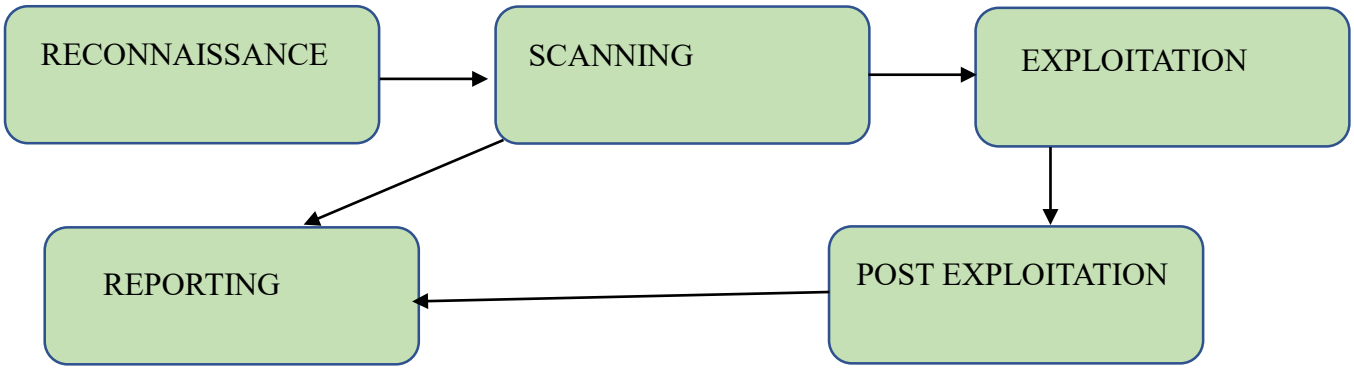
• Finding system and network flaws and vulnerabilities that could be used by attackers

• Evaluating the performance of current security measures, such as firewalls, intrusion detection systems, and encryption techniques

• Testing the effectiveness of previous security measures or improvements made based on previous penetration tests.

• Recommending ways to strengthen security policies, configure security controls, and fix vulnerabilities in order to improve the organization's security position

Methodology



Reconnaissance

A crucial step in a penetration test is reconnaissance, which entails collecting as much as possible about the HACKME Inc. Objective of reconnaissance is to discover potential weaknesses and attack routes that could be used to breach the target or acquire unauthorized access.

Scanning

Scanning is the process of utilizing automated tools to examine a target system or network for flaws and vulnerabilities during a penetration test. The main objective is to identify potential attack vectors. Both vulnerability scanning and port scanning were used. The scanning phase is essential because it offers a thorough overview of the HACKME Inc. and any vulnerabilities that might be exploited and are documented. Any new found vulnerabilities are also scanned and documented.

Exploitation

After thorough recon and scanning, this phase attempts to exploit any vulnerability that were found and to gain unauthorized access to the HACKME Inc. and demonstrate the impact of a potential attack.

Post-Exploitation

Post-exploitation is a critical phase of a penetration test that involves maintaining access and establishing a foothold within the target system or network after an initial exploitation has succeeded. The goal of post-exploitation is to expand the level of access and control over the target system or network and demonstrate the potential impact of a real-world attack. Attempts of privilege escalation, or the process of increasing one's level of access to a target system, are also done.

Reporting

After successfully exploiting the system, exposure of sensitive data is reported. All founded vulnerabilities, their exploits as well as company's strength and weaknesses are also thoroughly documented in this phase.

For reconnaissance gaining basic understanding of the company's network and system were important. Such information was gathered and a profile of the company was built.

For scanning, automated tools like nmap and nikto were used to find any open ports in the network, find about the operating system and vulnerabilities that could be found which were associated with them.

For exploitation, metasploit was used where the shellshock vulnerability that was found was searched. The exploitation of vulnerability was tested in order to find any plausible security breach that could occur due to it. Analysis and correlation of data were also performed during this stage.

A thorough report was created that documents all the findings in a standardized format, along with supporting evidence of the exploit's attack narrative and determine security levels while implementing industries' best practices. The risk categories assigned to each vulnerability are included in the report.

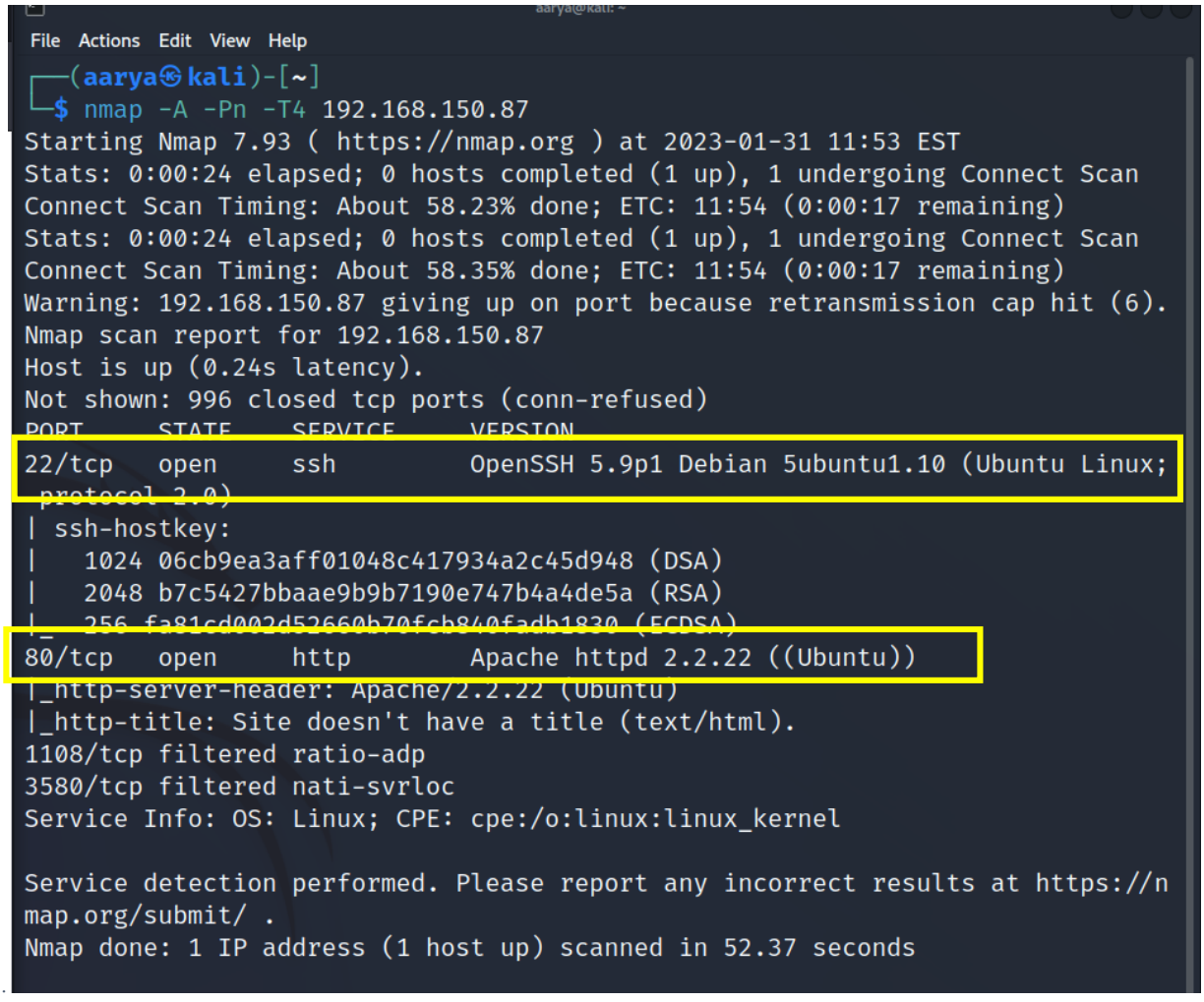
Attack Narrative

Network scan

Nmap, a powerful open-source network exploration and security auditing tool, was utilized to identify open ports of the company's network. The tool conducted scans of the operating system and examined both TCP and UDP ports, revealing that two critical ports, specifically port 22 and port 80 that were open.

Figure 1

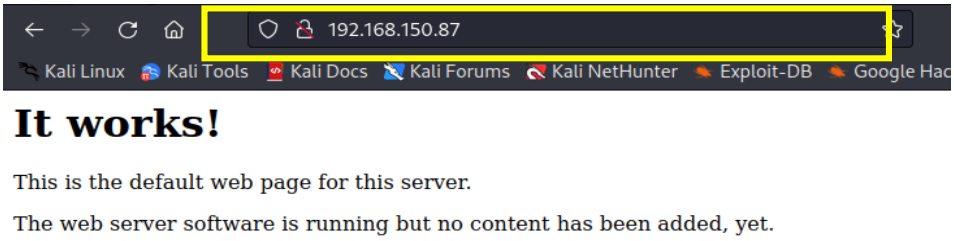
Scanning the IP address of network of the company



As the IP address was searched in the web browser a website was discovered which was found to be running on port 80. However, the website didn't contain much useful information.

Figure 2

The website hosted on the port 80 of the server

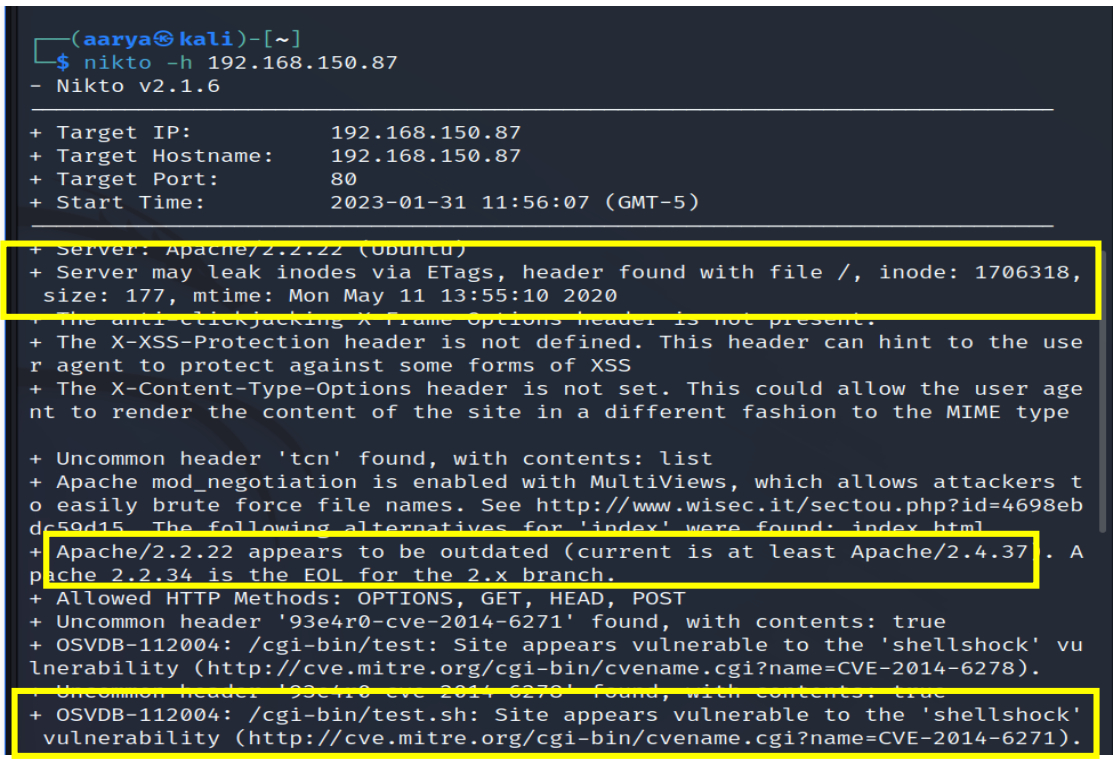


Vulnerability scan

Nikto is a tool used to search for security weaknesses in a system, including vulnerabilities related to the web server and its setup. A scan was done using Nikto on IP address of the company and it was discovered vulnerabilities such as Shellshock, outdated Apache, ETags and XSS were present.

Figure 3

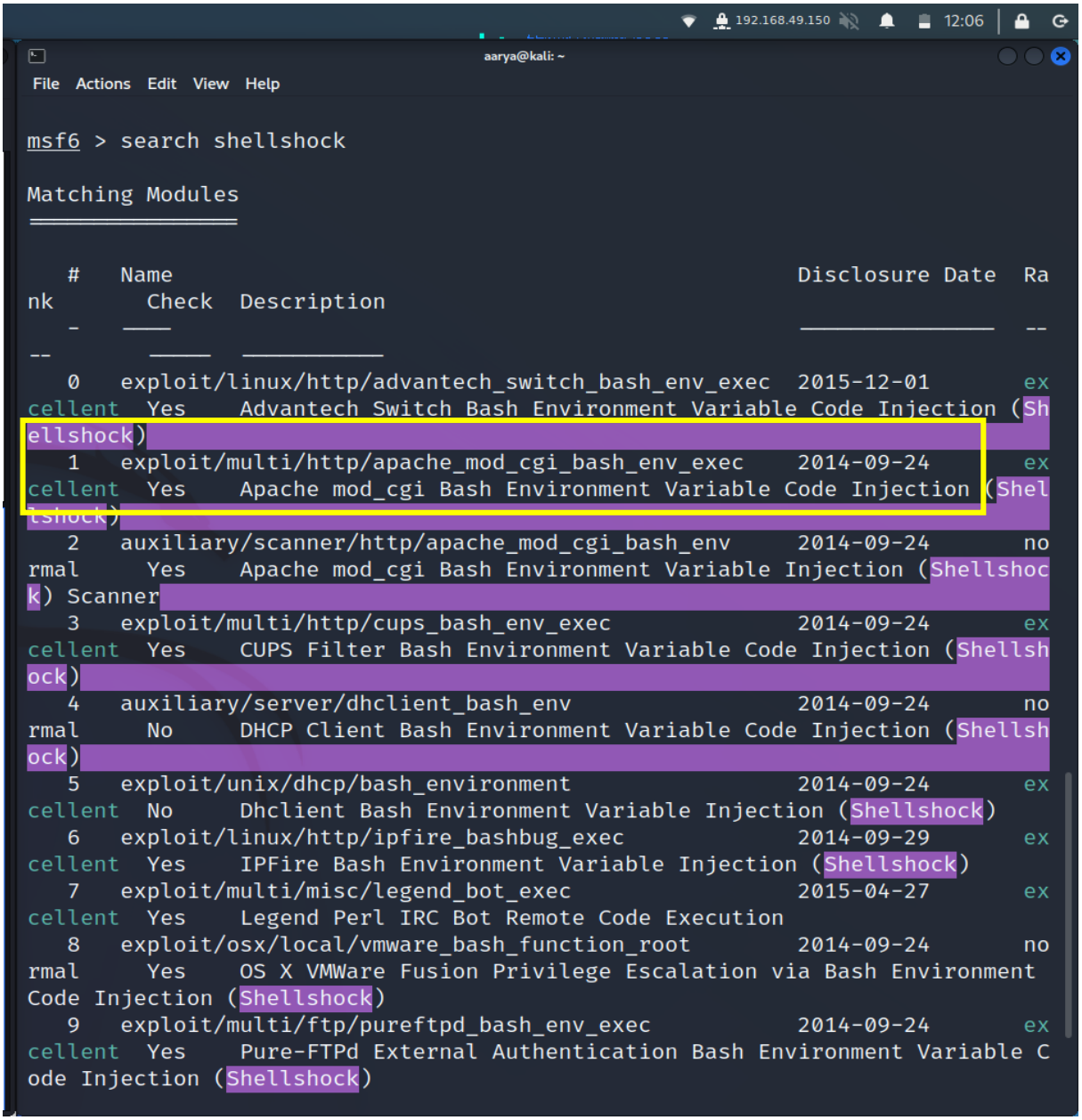
Scanning the target machine for vulnerabilities.



Since, CVE number of shellshock was also provided, it was exploited first. Metasploit was used to check for any exploits that could be found for this vulnerability *(see figure 4)*.

Figure 4

Exploit of shellshock through metasploit

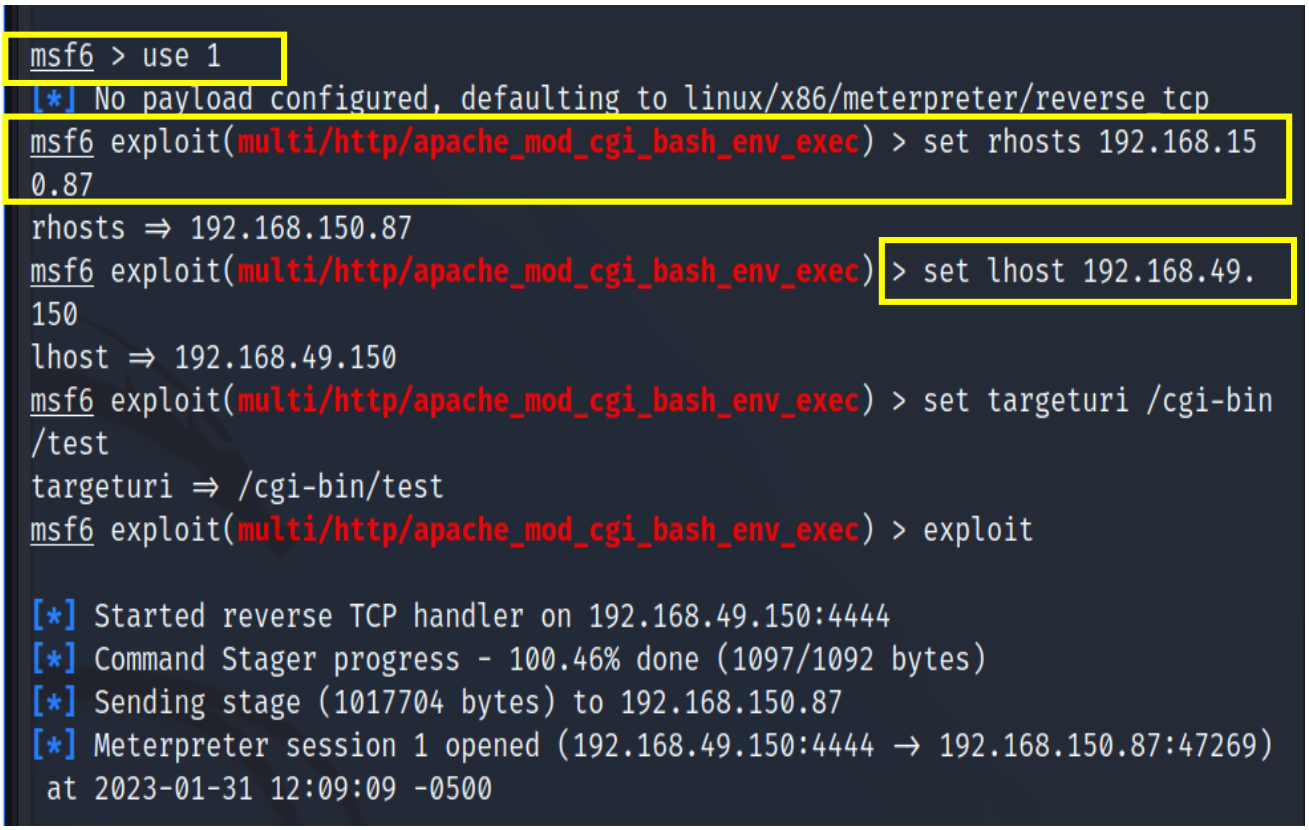


First, the metasploit was used to search for the best way to exploit the vulnerability. Then, the IP address of the company's network was set as the "rhosts" and the VPN's IP address as the "lhost." The "targeturi" was set to "/cgi-bin/test" where the exploit would be carried out, which opened up a Meterpreter session after successful exploitation *(see figure 5,6).*

Exploitation

Figure 5

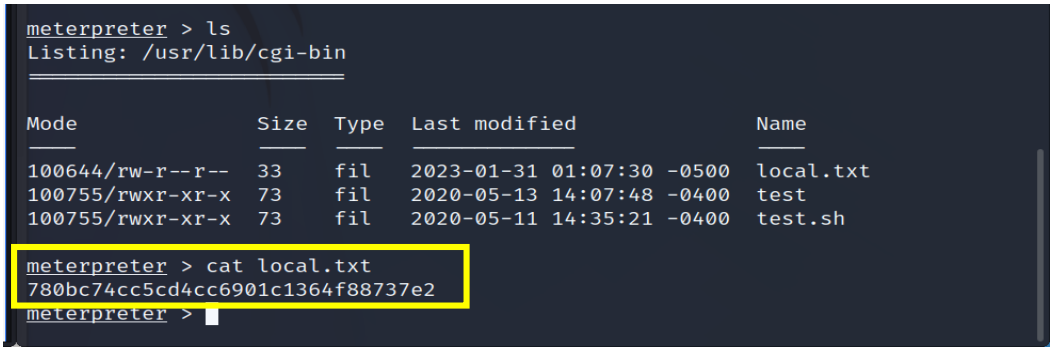
Using module 1



The directory where meterpreter was operating was identified by examining the files in that directory which was functioning in the /usr/lib/cgi-bin where different files were present whose contents were analyzed. This way a user privileged account's access was gained.

Figure 6

Listing files of meterpreter



Post-Exploitation

To further exploit the system, the shell was commandeered, and an examination was conducted to confirm the availability of Python on the system which was Python 2.7.3. Thus, python scripts could be executed.

Additionally, the details about the operating system and the version of GCC were also reviewed. It was determined that the Linux version running on the machine was outdated and was using Ubuntu 12.04.

Figure 7

Shell extraction

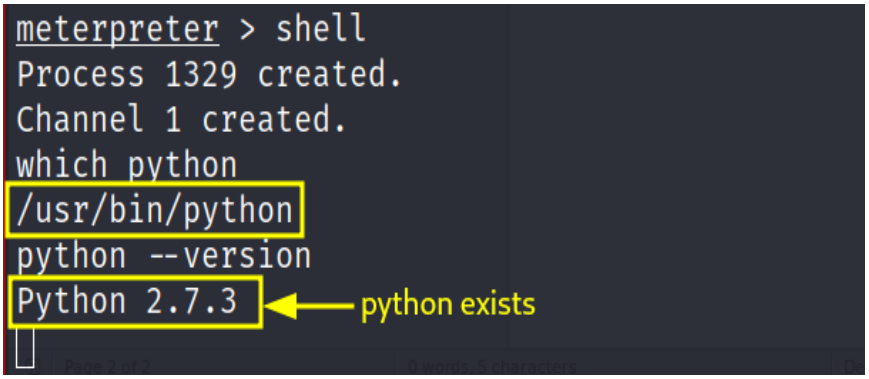
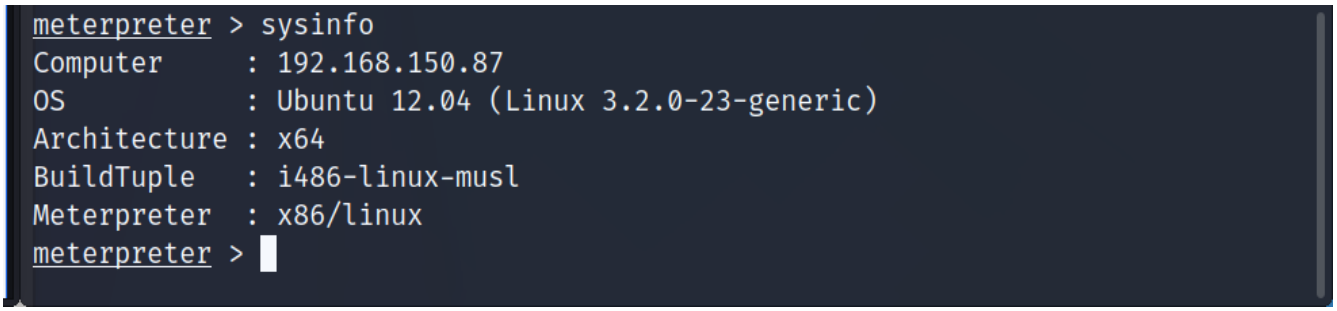


Figure 8

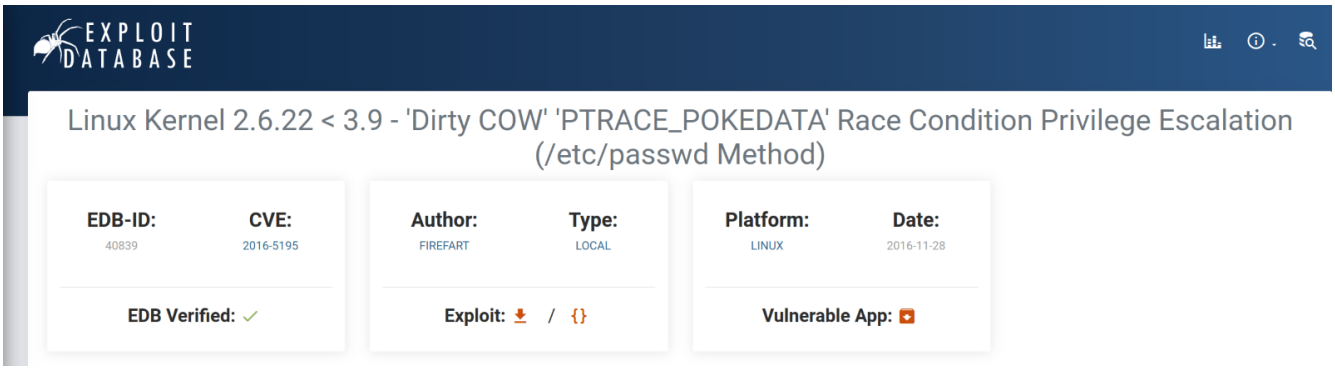
System information



Since the version of Ubuntu on the target system was outdated, the Exploit Database was consulted to locate potentially exploitable vulnerabilities for privilege escalation. A search resulted in the identification of an exploit known as "dirtycow," which appeared to be suitable for escalating privileges on the target system (Bonacini, 2016).

Figure 9

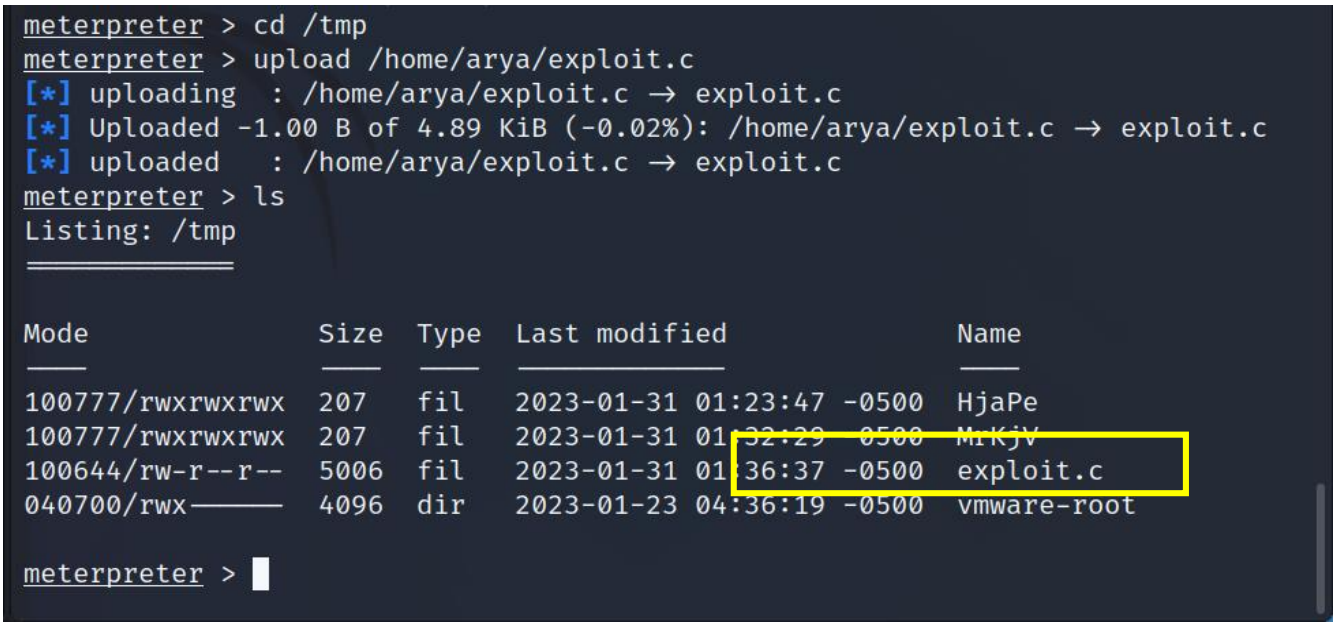
Exploit of outdated ubuntu in the ExploitDB.



The exploit was subsequently downloaded to the host machine as exploit.c. Exploitation could now be initiated from the existing meterpreter session. To enable execution of the exploit file, the current directory was changed to "/tmp," which had the requisite permissions.

Figure 10

Uploading the exploit to the target machine.

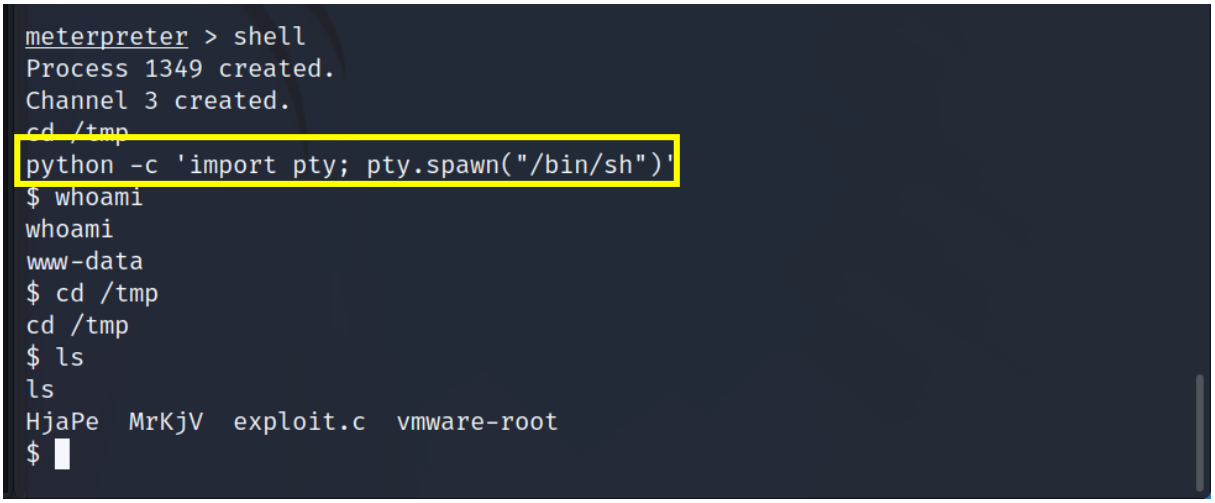


As the exploit was successfully inside, python shell was extracted.

Privilege Elevation

Figure 11

Extracting python shell



Since the shell was extracted, the directory was changed to /tmp since it had all the necessary executable permission. As the exploit had the extension '.c', it was compiled by gcc to exploit.

Figure 12

Compiling exploit.c

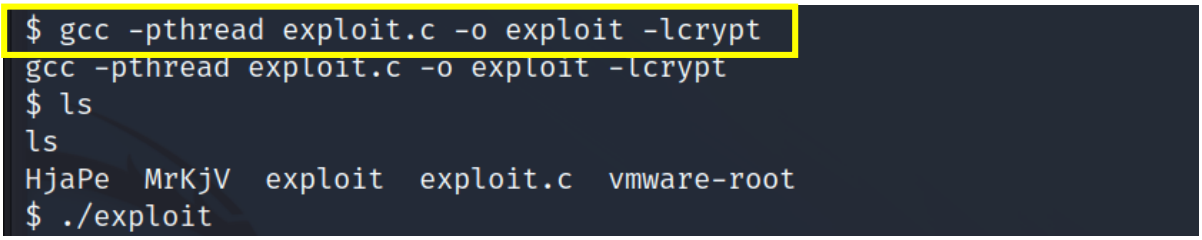
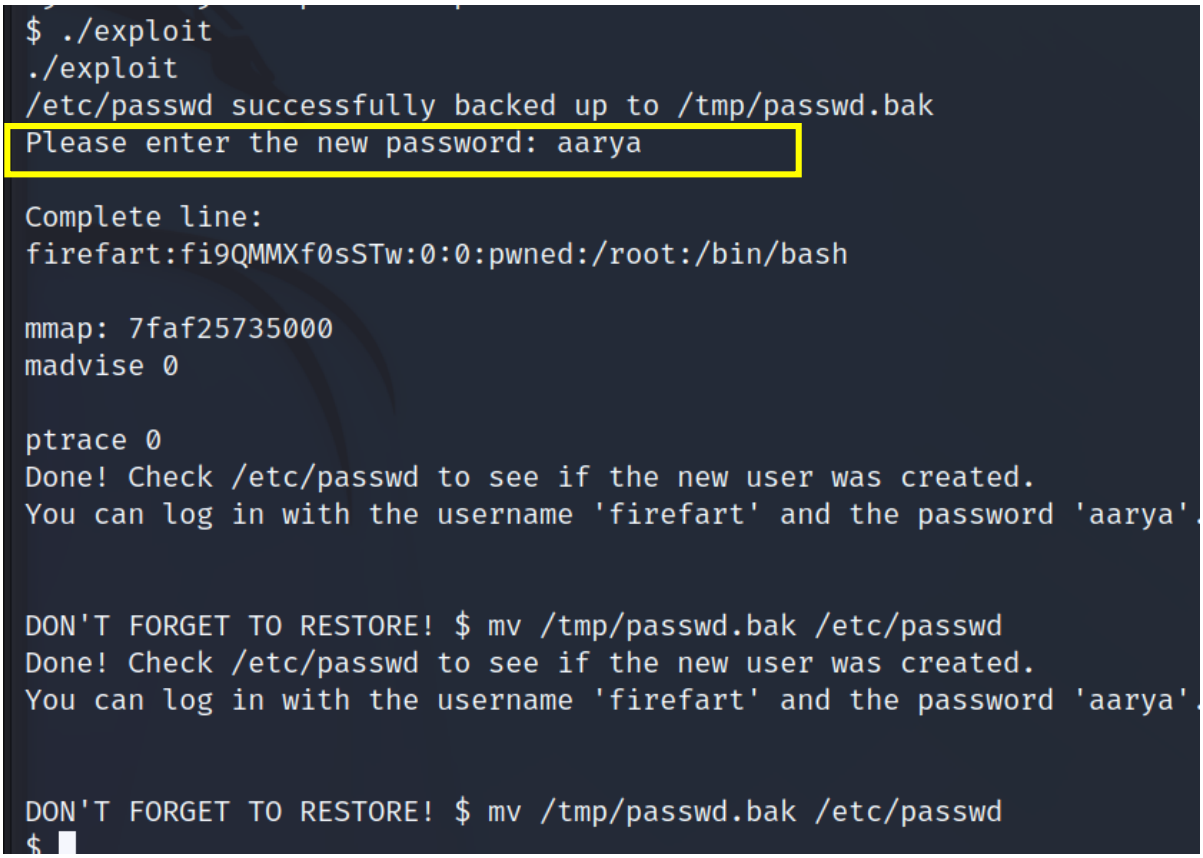


Figure 13

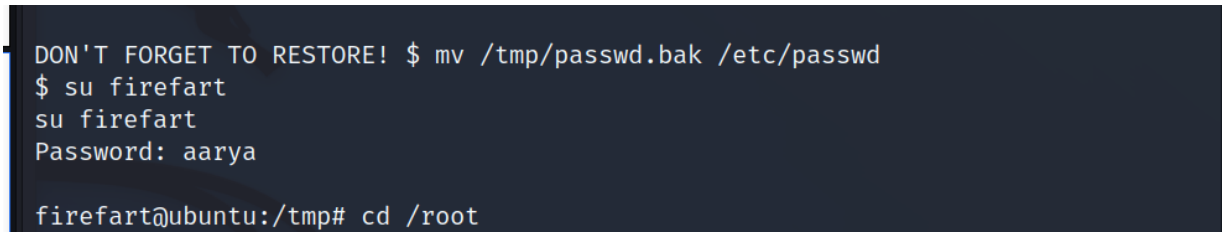
Execution of the dirty cow exploit.



After executing exploit, a new password for the user firefart was created and successfully logged in.

Figure 14

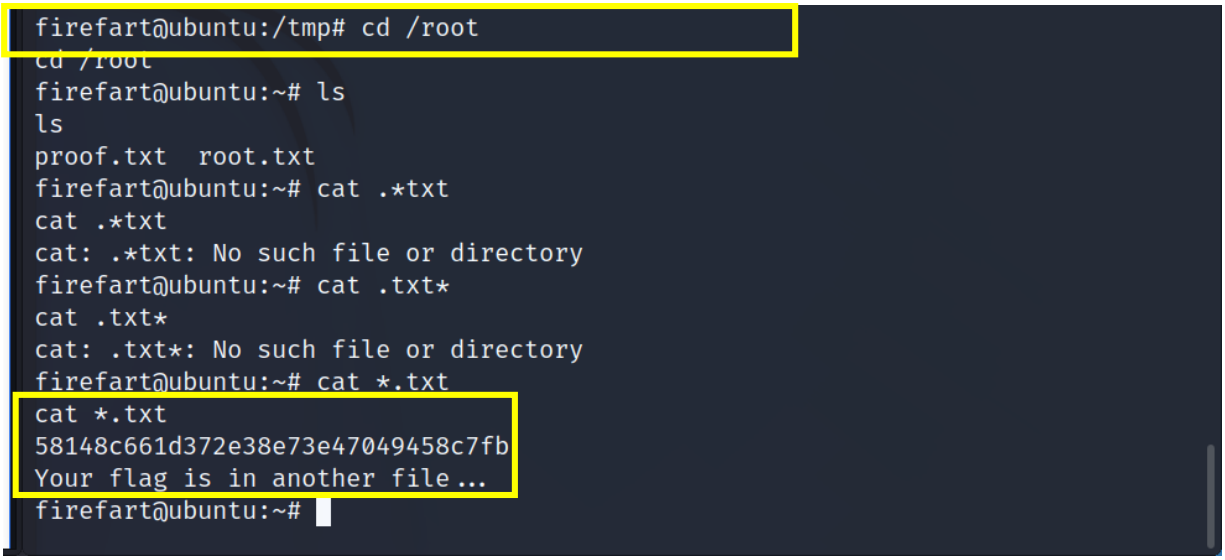
Su firefart.



Since most important files are in root directory, after the directory was changed to root some important documents were found.

Figure 15

Reading the contents inside the root.



This way highest privilege was also gained.

Technical Findings

Bash Remote Code Execution (Shellshock)

Description

A flaw in the Bash version executing on the remote host permits command injection by tampering with environment variables.

Impact

Upon exploitation attacker may remotely execute CGI scripts in /cgi-bin which will gain access to the system.

Remediation

It is critical to address this vulnerability by updating Bash to a secure version or implementing a workaround to mitigate the risk of exploitation.

Steps of Reproduction

1. 1. Submit a fraudulent Request to the server to CGI script that is open to attack.
2. 2. A specified collection of environment variables that can be utilized to insert arbitrary commands into the script should be included in the request.
3. 3. Check the response to determine if the server executed the injected commands.
4. 4. Do the procedure once more with other combinations of environment variables to determine if the vulnerability may be exploited in various ways.

Reference

(CVE-2014-6271)

CVSSv3.1

CVS score is 10 with low attack complexity *(see figure 16)*.

Figure 16

CVSS of Shellshock.

CVSS Base Metrics	***Value***
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Changed
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	High
CVSS v3.1 score	10.0 (Critical)

(tenable)

ETag Header Information Disclosure

Description

ETag is an HTTP header used by servers to validate cached resources.

Impact

If the ETag header exposes server-side implementation details, it can potentially enable attacks such as cache poisoning, session fixation, or bypassing access controls.

Remediation

To prevent ETag information disclosure, the server should either use weak ETags that only contain an opaque identifier or disable ETags altogether

CVSSv3.1

(informational)

Outdated Linux System

Description

Running an outdated Linux system can pose significant security risks as it may contain known vulnerabilities that can be exploited by attackers.

Impact

The vulnerabilities that arises with outdated linux system could allow attackers to gain unauthorized access, escalate privileges, or execute arbitrary code on the system.

Remediation

To mitigate the risks of an outdated Linux system, it's recommended to apply security updates and patches regularly. It's also important to use a supported version of the Linux distribution and to disable any unnecessary services or applications to reduce the attack surface.

CVSS

(Informational)

Conclusion

This concludes the vulnerability assessment and penetration testing report. The system of HACKME Inc. was successfully breached. Thus, is recommended to follow the above remediation to make the company more secure.

Conclusion

Above sample of VAPT is concluded. APA7 format is not followed for the sample report.

Video Link

https://youtu.be/Iw_YWWQMKVA

References

Bonacini, G. (2016, November 27). Linux kernel 2.6.22 < 3.9 - 'dirty COW /proc/self/mem' race condition privilege escalation (/etc/passwd method). Exploit Database. Retrieved February 20, 2023, from https://www.exploit-db.com/exploits/40847

CVE. (n.d.). You are viewing this page in an unauthorized frame window. NVD. Retrieved February 20, 2023, from https://nvd.nist.gov/vuln/detail/cve-2014-6271

tenable. (n.d.). Bash remote code execution (shellshock). Tenable. Retrieved February 20, 2023, from https://www.tenable.com/plugins/nessus/77823