VULNERABILITY ASSESSMENT AND PENETRATION TESTING

1. INTRODUCTION

In the modern digital era, organizations across all sectors increasingly depend on information systems, networked infrastructures, and web-based services to support daily operations, decision-making processes, and long-term strategic goals. While these technologies provide scalability, automation, and global connectivity, they simultaneously introduce a wide range of security risks. Cyber adversaries continuously exploit vulnerabilities arising from outdated software, misconfigurations, weak authentication mechanisms, and insufficient security monitoring.

Cyberattacks such as ransomware outbreaks, data breaches, and unauthorized system intrusions have demonstrated that even a single unpatched vulnerability can lead to catastrophic consequences. As a result, organizations must adopt proactive security measures rather than relying solely on reactive incident response mechanisms. One of the most effective proactive approaches is **Vulnerability Assessment and Penetration Testing** .

This report presents a comprehensive VAPT exercise conducted within a controlled laboratory environment using **Metasploitable2**, an intentionally vulnerable virtual machine designed for security testing and training purposes. The primary objective of this exercise is to replicate real-world security assessment workflows using open-source tools while adhering to recognized industry standards and methodologies.

The assessment not only focuses on identifying technical vulnerabilities but also emphasizes understanding the **risk implications** associated with these vulnerabilities. By correlating technical findings with potential business impact, this report demonstrates how security assessments contribute to informed decision-making, risk management, and overall organizational resilience.

2. OBJECTIVES OF THE ASSESSMENT

The objectives of this Vulnerability Assessment and Penetration Testing exercise extend beyond simple vulnerability discovery. The assessment is designed to provide both technical and conceptual understanding of cybersecurity evaluation processes.

The specific objectives include:

- To gain a clear understanding of how security assessments can be performed using freely available, open-source tools without reliance on commercial solutions
- To simulate a structured penetration testing lifecycle similar to real-world professional engagements
- To identify exposed network services, insecure configurations, and outdated software components that increase the system's attack surface
- To analyze identified vulnerabilities using standardized scoring systems such as CVSS to determine severity and exploitability
- To prioritize vulnerabilities based on realistic threat scenarios using likelihood and impact analysis
- To recommend actionable remediation and mitigation strategies aligned with industry best practices
- To develop professional-quality documentation that communicates findings effectively to both technical and non-technical stakeholders

Additionally, this exercise aims to enhance analytical thinking, technical documentation skills, and familiarity with industry terminology—skills that are essential for roles in cybersecurity operations, penetration testing, and risk management.

3. SCOPE OF THE ASSESSMENT

Defining the scope of a security assessment is a critical step that ensures clarity, legal compliance, and focused testing efforts. A clearly defined scope prevents unintended disruptions and ensures that testing activities remain ethical and authorized.

3.1 In-Scope Components (Expanded)

The following components were included in the scope of this assessment:

- **Target System:** Metasploitable2 virtual machine
- **IP Address:** 192.168.56.102
- **Network Environment:** Internal, isolated host-only network
- **Operating System:** Linux-based legacy operating system
- **Network Services:** All TCP services exposed by the target system
- **Assessment Techniques:** Network scanning, service enumeration, vulnerability identification, and risk analysis

All vulnerabilities identified through automated scanning and manual analysis were considered within scope for documentation and risk evaluation.

3.2 Out-of-Scope Components

The following activities were explicitly excluded from the assessment:

- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, as they can disrupt system availability
- Social engineering attacks such as phishing or pretexting
- Physical security testing
- Wireless network attacks
- Advanced exploitation or persistence techniques beyond proof-of-concept

Excluding these elements ensures that the assessment remains controlled, ethical, and aligned with academic objectives.

4. VAPT METHODOLOGY

The assessment follows a structured and repeatable VAPT methodology inspired by well-established industry frameworks, including the **OWASP Testing Guide**, **NIST SP 800-115**, and general penetration testing best practices. This methodology ensures consistency, reliability, and accuracy of findings.

4.1 Planning Phase

The planning phase establishes the foundation for the entire assessment. In professional environments, this phase includes obtaining legal authorization, defining engagement rules, and identifying constraints.

Key planning activities in this assessment included:

- Defining the assessment scope and objectives
- Selecting appropriate open-source tools for scanning and analysis
- Designing an isolated lab environment to prevent unintended network exposure
- Establishing documentation standards and report structure

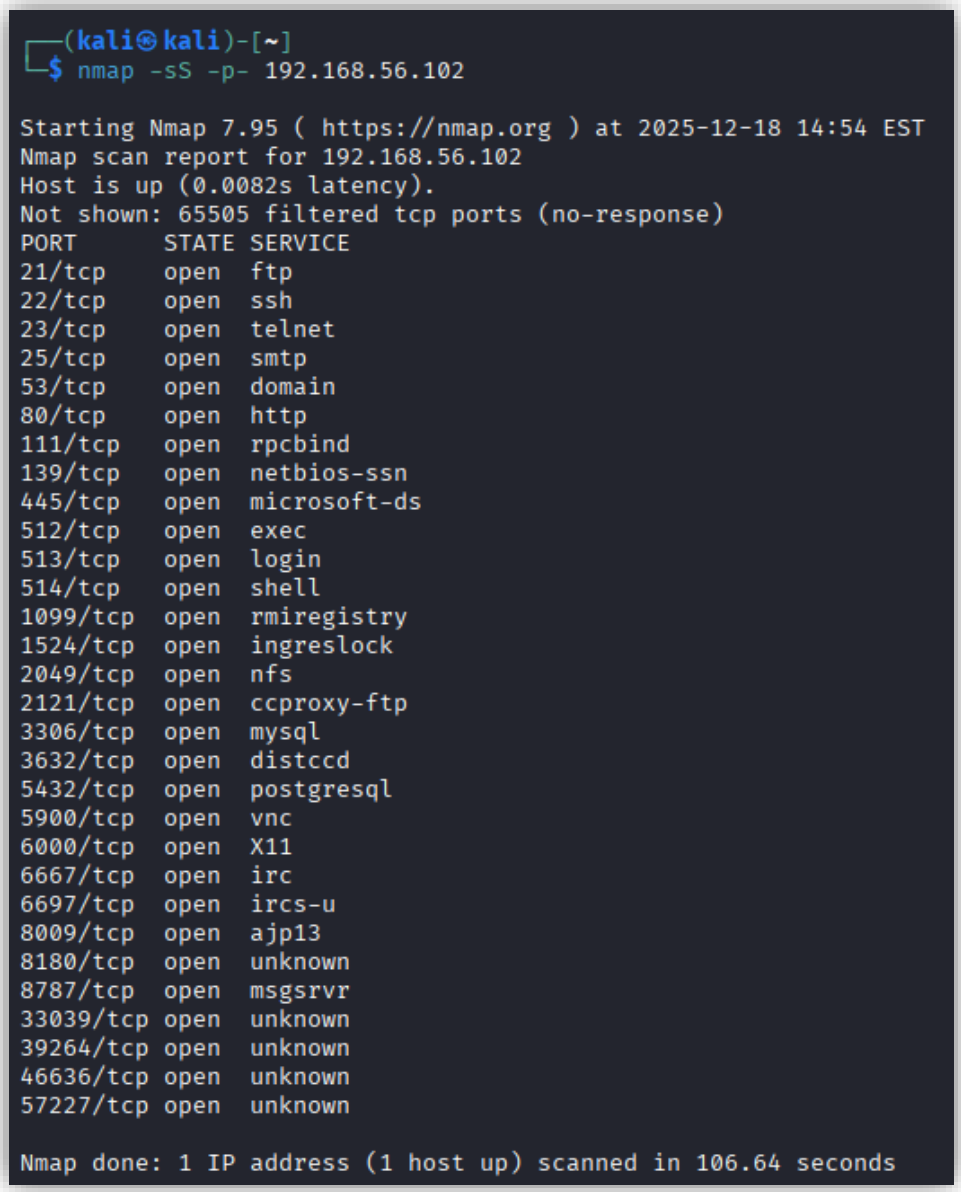
4.2 Discovery and Enumeration Phase

The discovery phase represents the reconnaissance stage of an attack lifecycle. During this phase, an attacker gathers information about the target system to identify potential entry points.

The following activities were performed:

- **Host discovery** to verify system availability
- **Port scanning** to identify open network ports
- **Service enumeration** to determine running services
- **Version detection** to identify outdated or vulnerable software

This phase is critical because the quality of discovery directly influences the effectiveness of vulnerability assessment and exploitation planning.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p- 192.168.56.102

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-18 14:54 EST
Nmap scan report for 192.168.56.102
Host is up (0.0082s latency).
Not shown: 65505 filtered tcp ports (no-response)
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
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33039/tcp open  unknown
39264/tcp open  unknown
46636/tcp open  unknown
57227/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 106.64 seconds
```

Nmap host discovery and port scanning output

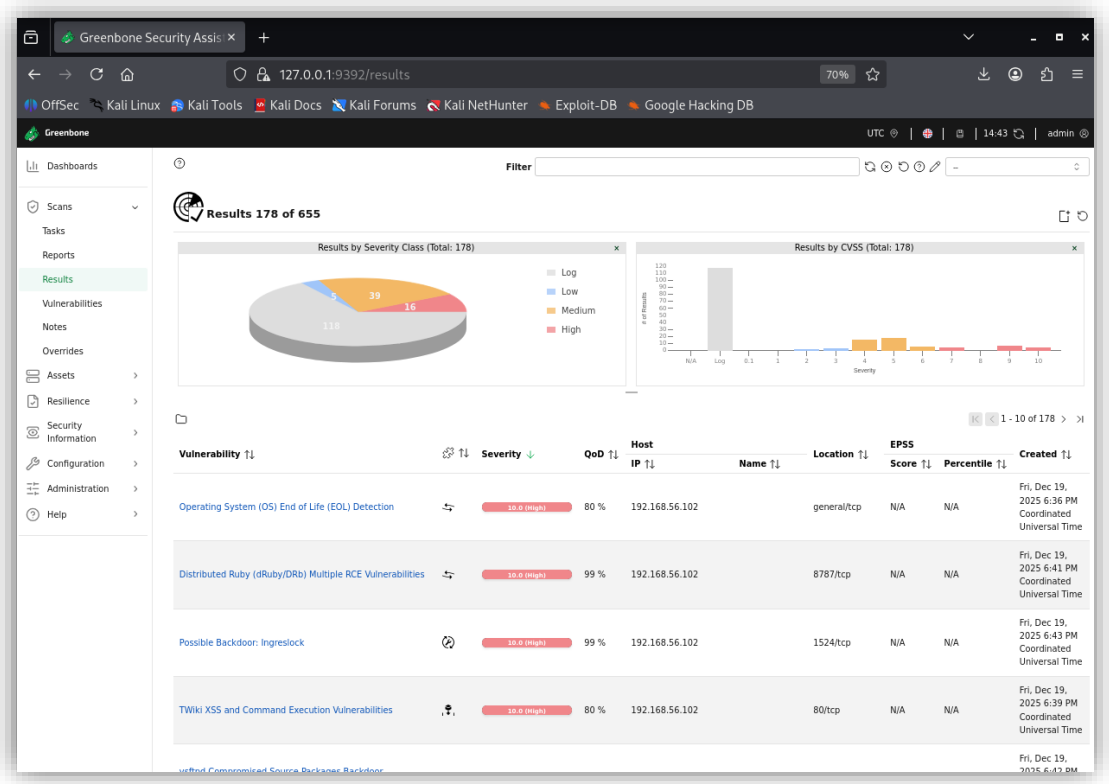
4.3 Vulnerability Assessment Phase

The vulnerability assessment phase focuses on identifying known security weaknesses using automated scanning tools. OpenVAS was used as the primary vulnerability scanner due to its extensive vulnerability database and CVSS integration.

OpenVAS enabled the identification of:

- Outdated operating systems
- Misconfigured services
- Known remote code execution vulnerabilities
- Backdoor and malicious service indicators

Each identified vulnerability was mapped to a CVE where applicable and assigned a severity score based on CVSS standards.



OpenVAS vulnerability scan dashboard and results

4.4 Risk Assessment Phase

Risk assessment transforms technical findings into actionable insights. Rather than treating all vulnerabilities equally, this phase evaluates:

- **Likelihood:** How easily a vulnerability can be exploited
- **Impact:** The potential damage caused by successful exploitation

A structured risk matrix was used to classify vulnerabilities into Low, Medium, High, or Critical categories. This prioritization supports effective remediation planning and resource allocation.

4.5 Reporting Phase

The reporting phase consolidates all findings into a structured document. Effective reporting is essential because even the most accurate technical findings lose value if they are not communicated clearly.

This report is designed to:

- Provide technical depth for security professionals
- Offer clarity for management and decision-makers
- Serve as a reference for remediation planning

5. LAB SETUP AND ENVIRONMENT

The assessment was conducted within a virtualized lab environment to ensure safety, repeatability, and isolation.

5.1 Environment Components

- **Kali Linux:** Served as the attacker system, providing a comprehensive suite of security testing tools
- **Metasploitable2:** Served as the intentionally vulnerable target system

- **Oracle VirtualBox:** Used to host and manage virtual machines
- **Network Configuration:** Host-only adapter ensuring isolated internal communication

This setup accurately reflects internal network penetration testing scenarios commonly encountered in enterprise environments.

6. DISCOVERY PHASE RESULTS

6.1 Host Discovery

Host discovery confirmed that the target system was reachable and active within the internal network. This step verifies basic connectivity and ensures that subsequent scans can be conducted effectively.

6.2 Port Enumeration

A full TCP port scan revealed multiple open ports, many of which correspond to legacy services. Each open port represents a potential attack vector that can be leveraged by malicious actors.

6.3 Service and Version Enumeration

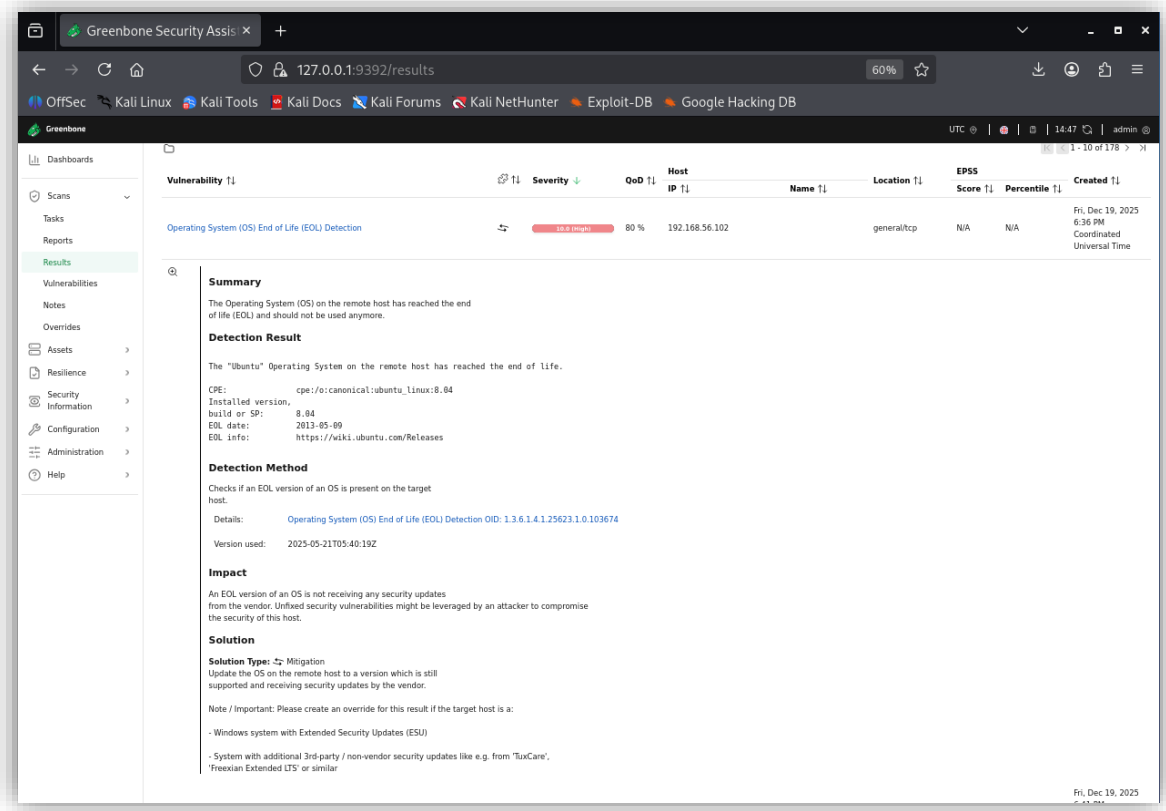
Service detection revealed several outdated and vulnerable services. Many of these services are known to contain publicly documented exploits, highlighting the risks associated with legacy system deployments.

7. VULNERABILITY ASSESSMENT FINDINGS

7.1 Operating System End of Life (EOL)

The target system operates on an end-of-life operating system that no longer receives security updates. This significantly increases exposure to known exploits and reduces the effectiveness of defensive controls.

Impact:
Attackers can exploit unpatched vulnerabilities to gain unauthorized access, escalate privileges, and maintain persistence.



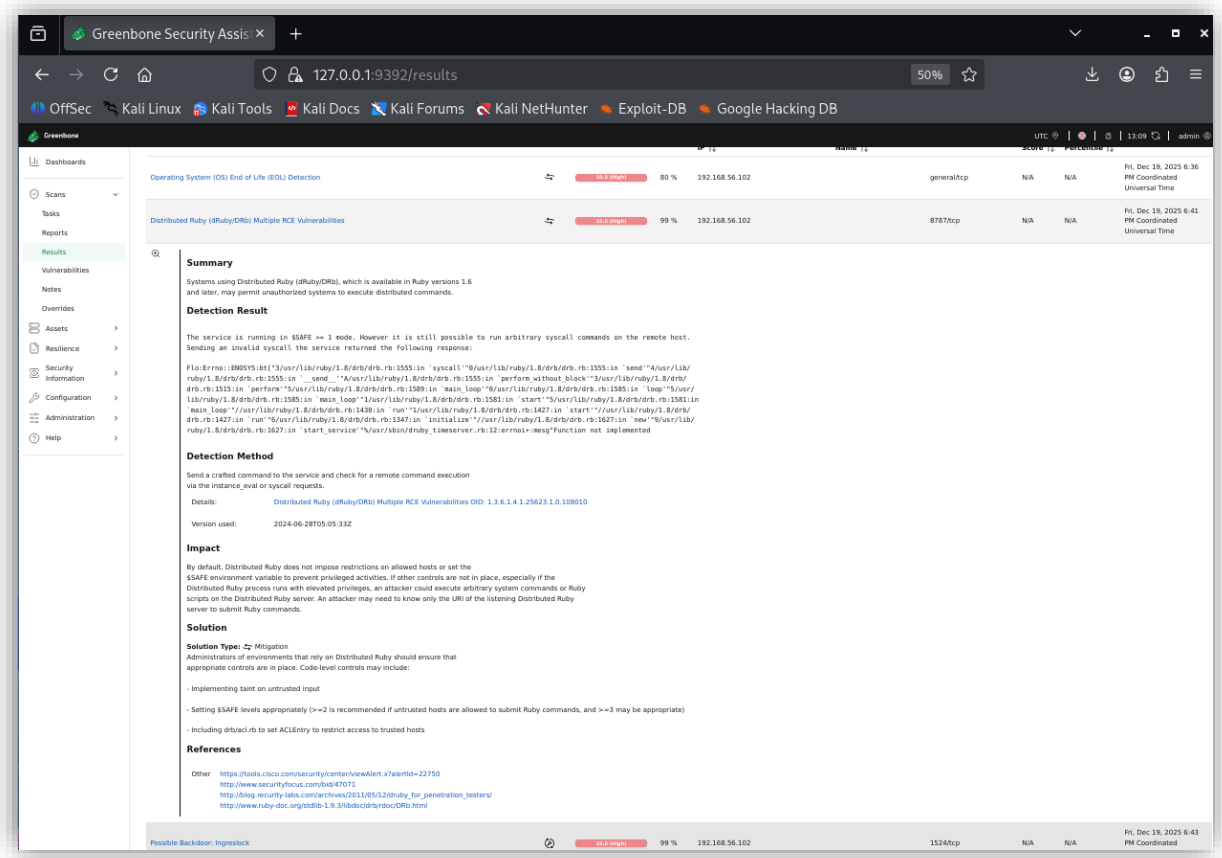
OpenVAS OS EOL vulnerability details

7.2 Distributed Ruby (DRb) Remote Code Execution

The Distributed Ruby service permits unauthenticated remote execution of system commands. This vulnerability demonstrates how exposed services can directly lead to complete system compromise.

Impact:

Successful exploitation allows attackers to execute arbitrary commands, install malware, and pivot to other systems.



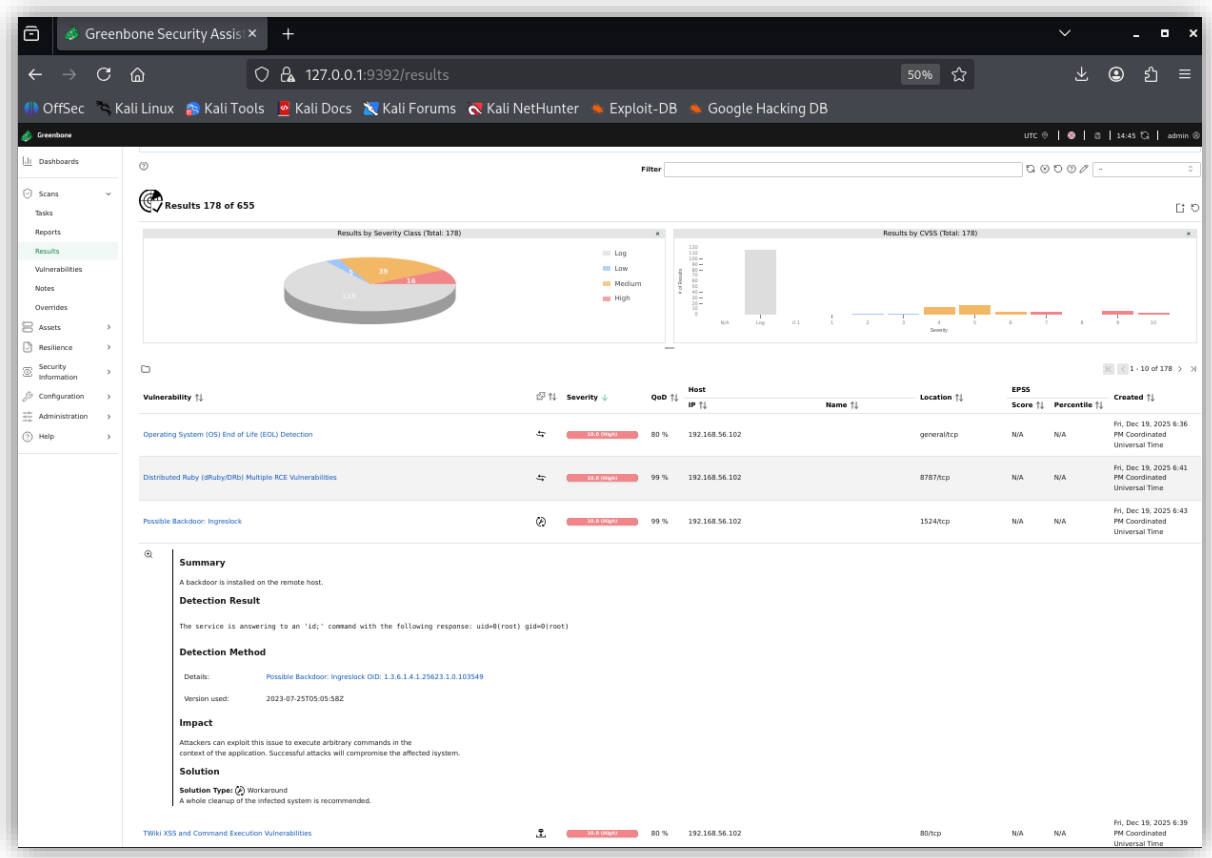
OpenVAS DRb RCE vulnerability evidence

7.3 Possible Backdoor: Ingreslock

The detection of a backdoor service responding with root-level command execution indicates a severe compromise. Backdoors pose significant risks because they provide persistent access even after partial remediation.

Impact:

Persistent unauthorized access and complete system takeover.



OpenVAS backdoor detection evidence

8. RISK ASSESSMENT AND PRIORITIZATION

The use of a structured risk matrix ensures that vulnerabilities are prioritized based on real-world threat scenarios rather than theoretical severity alone.

Vulnerability	Likelihood	Impact	Risk
OS EOL	Medium	High	High
DRb RCE	High	High	Critical
Ingreslock	High	High	Critical

9. REMEDIATION AND MITIGATION STRATEGIES

Remediation strategies focus on eliminating root causes rather than temporary fixes. Recommendations emphasize system upgrades, secure configuration, network segmentation, and continuous monitoring.

10. CHALLENGES ENCOUNTERED DURING ASSESSMENT

- OpenVAS scan interruption at 98% due to unstable legacy services
- Extended scan duration caused by outdated system components
- Complexity introduced by multiple exposed services

These challenges closely mirror real-world security assessments involving legacy infrastructure.

11. REAL-WORLD RELEVANCE

Many production environments still operate legacy systems due to operational constraints, cost considerations, or compatibility requirements. Such systems are commonly found in healthcare, manufacturing, education, and government sectors, making them high-value targets for attackers.

12. CONCLUSION

This VAPT exercise demonstrates the importance of proactive security assessments in identifying and mitigating vulnerabilities before they are exploited. The findings highlight the severe risks posed by outdated systems and insecure services and emphasize the need for continuous security improvement.

13. LEARNING OUTCOMES

This project enhanced understanding of:

- End-to-end VAPT methodology
- Vulnerability discovery and analysis
- Risk-based prioritization
- Professional cybersecurity documentation

14. REFERENCES

- OWASP Testing Guide
- NIST SP 800-115
- CVSS v3.1 Specification
- OpenVAS Documentation
- CIS Security Benchmarks