Comprehensive Security Assessment & VAPT Report

1.Introduction

This report documents a complete security assessment and Vulnerability Assessment and Penetration Testing (VAPT) exercise performed using only free and open-source tools. The engagement combines theoretical understanding with hands-on practical work in a controlled lab environment (Kali Linux attacking Metasploitable 3 target VM).
The goal is to understand how to evaluate systems without relying on paid tools, align the assessment with recognized standards and frameworks, and produce professional documentation suitable for corporate environments.

2.Objectives

1. Understand core concepts of security assessment and VAPT.
2. Apply a structured VAPT methodology (Planning → Discovery → Attack → Reporting).
3. Align testing activities with security standards and compliance requirements.
4. Perform basic risk assessment using CVSS and a risk matrix.
5. Identify and analyze common network and web application vulnerabilities.
6. Document and report findings in a clear, professional format, including executive summary, technical details, and remediation.

---

3. Scope

- **In-Scope Assets**
    - Metasploitable 3 virtual machine (intentionally vulnerable server).
    - Services and web applications hosted on Metasploitable 3.
- **Out-of-Scope**
    - Any systems other than lab VMs.
    - Production systems or live internet targets.

The assessment is strictly for educational purposes within an isolated lab environment.

---

4. Theoretical Knowledge

Understanding Security Assessment

Objective: Learn how to evaluate systems without paid tools.

Concept of Security Assessment

A *security assessment* is a structured process used to identify, analyze, and prioritize weaknesses in systems, networks, and applications. It helps organizations understand:

- What assets they have.
- What threats and vulnerabilities exist.
- What impact those vulnerabilities could cause.
- What controls are needed to reduce risk.

Security assessments are often aligned with frameworks such as NIST guidelines (e.g., NIST SP 800-115 for technical testing).

Types of Security Testing

1. **Vulnerability Assessment**
    - **Purpose:** Systematically identify known vulnerabilities.
    - **Tools (free/open-source):**
        - OpenVAS / GVM – network and system vulnerability scanner.
    - Outcome: List of vulnerabilities (with CVEs, CVSS scores, severity).
2. **Penetration Testing**
    - **Purpose:** Simulate real attacks to validate exploitability and impact.
    - **Tools:**
        - Kali Linux toolset: Nmap, Metasploit, Nikto, OWASP ZAP, etc.
    - Outcome: Validated attack paths, proof-of-concept exploits, and impact.
3. **Compliance Testing**
    - Purpose: Check alignment with policies, standards, and regulations.
    - Examples:
        - CIS Benchmarks checklists.
        - Internal security baseline checklists.
    - Outcome: Compliance status (Compliant/Non-compliant) per control requirement.

VAPT Methodology

Objective: Follow a structured approach using methodologies.

A typical VAPT engagement follows these phases:

Planning Phase

- Define scope: IP ranges, systems, and applications to be tested.

- Define rules of engagement: what is allowed (e.g., no DoS, no data destruction).
- Identify stakeholders: system owners, security team, etc.
- Prepare documentation: authorization letter, test plan.

Tool Example:

- **Dradis CE – used to:**
  - Maintain engagement notes.
  - Track hosts, findings, and evidence.
  - Prepare draft reports.

Discovery Phase

- **Information Gathering / Reconnaissance**
  - Identify live hosts, open ports, and running services.
  - Enumerate service versions and potential vulnerabilities.
- **Tools & Activities**
  - **Nmap:**
    - Host discovery:
    - nmap -sn <192.168.0.101>
    - Port scan and service detection:
    - nmap -sV -sC -O <192.168.0.101>
  - **OWASP ZAP (for web apps):**
    - Crawl target web application.
    - Run active/passive scans for common issues (XSS, SQLi, etc.).

Attack (Exploitation) Phase

- Use identified vulnerabilities to attempt exploitation.
- Tools:
  - **Metasploit Framework:**
    - Search for exploits based on service versions (e.g., Tomcat, SMB).
    - Launch modules against vulnerable services.
  - Manual exploitation for basic web vulnerabilities (e.g., SQLi, XSS).

Example high-level steps:

1. Import Nmap results into Metasploit.
2. Identify vulnerable services.

3. Use appropriate exploit modules.
4. Capture evidence (screenshots, command output).

Reporting Phase

- Aggregate findings in a structured format.
- Tools:
    - Dradis CE
    - CherryTree for detailed notes and screenshots.
    - Standard report templates (can be from GitHub or self-designed).

Sections typically include:

- Executive Summary
- Methodology
- Findings with technical detail
- Risk rating and CVSS scores
- Remediation recommendations

Security Standards & Compliance

Objective: Align with regulations using resources.

Key standards:

- ISO/IEC 27001 – Information Security Management System (ISMS).
- GDPR – Data protection and privacy for EU residents.
- HIPAA – Healthcare data security and privacy (US).
- CIS Benchmarks – Configuration baselines for systems (e.g., Windows, Linux).

How to Learn / Apply:

- Use OWASP Top 10 as a baseline for web application testing:
    - Focus on risks like Injection, Broken Authentication, XSS, Security Misconfiguration, etc.
- Map findings to relevant controls:
    - Example: Insecure HTTP methods → relates to configuration hardening and access control standards.

Risk Assessment Basics

Objective: Prioritize vulnerabilities with scoring systems.

CVSS (Common Vulnerability Scoring System)

- Used to quantify the severity of vulnerabilities (0.0–10.0).
- Parameters include:
    - Attack Vector, Complexity, Privileges Required, User Interaction.
    - Impact on Confidentiality, Integrity, Availability.

Procedure:

1. Take CVE from vulnerability scanner (e.g., OpenVAS).
2. Open the NVD CVSS calculator.
3. Input the metrics based on the vulnerability description.
4. Record the Base Score and Severity (Low/Medium/High/Critical).

Risk Matrix (3×3)

Combine:

- Likelihood (Low / Medium / High).
- Impact (Low / Medium / High).

This produces a 3×3 grid. Example:

- High Likelihood + High Impact → High Risk.
- Low Likelihood + Medium Impact → Low/Medium Risk.

This helps management focus on the most important issues first.

Common Vulnerabilities

Objective: Identify flaws in labs/tools.

1. **Network Vulnerabilities**
    - Open or unnecessary ports.
    - Default or weak credentials.
    - Outdated services with known CVEs.
    - Insecure protocols (e.g., Telnet, FTP).

Tool: Nmap for discovery and basic vulnerability hints.

2. **Web Application Vulnerabilities**
    - SQL Injection.
    - Cross-Site Scripting (XSS).

- Insecure Direct Object References (IDOR).
- Security Misconfiguration.

Practice Platforms:

- OWASP Juice Shop
- Metasploitable 3 web apps
- VulnHub VMs

Documentation Fundamentals

Objective: Create reports with tools.

- CherryTree – structure notes by:
  - Host.
  - Vulnerability.
  - Exploit attempt.
  - Evidence (screenshots, output).
- Dradis CE – collaborative reporting platform to:
  - Store findings in a central project.
  - Generate report drafts using templates.
- Spreadsheets – for vulnerability tracking and risk matrix.

5. Practical Application: Lab Setup & Execution

Setup Testing Environment

Objective: Build a safe lab where all testing is legal and controlled.

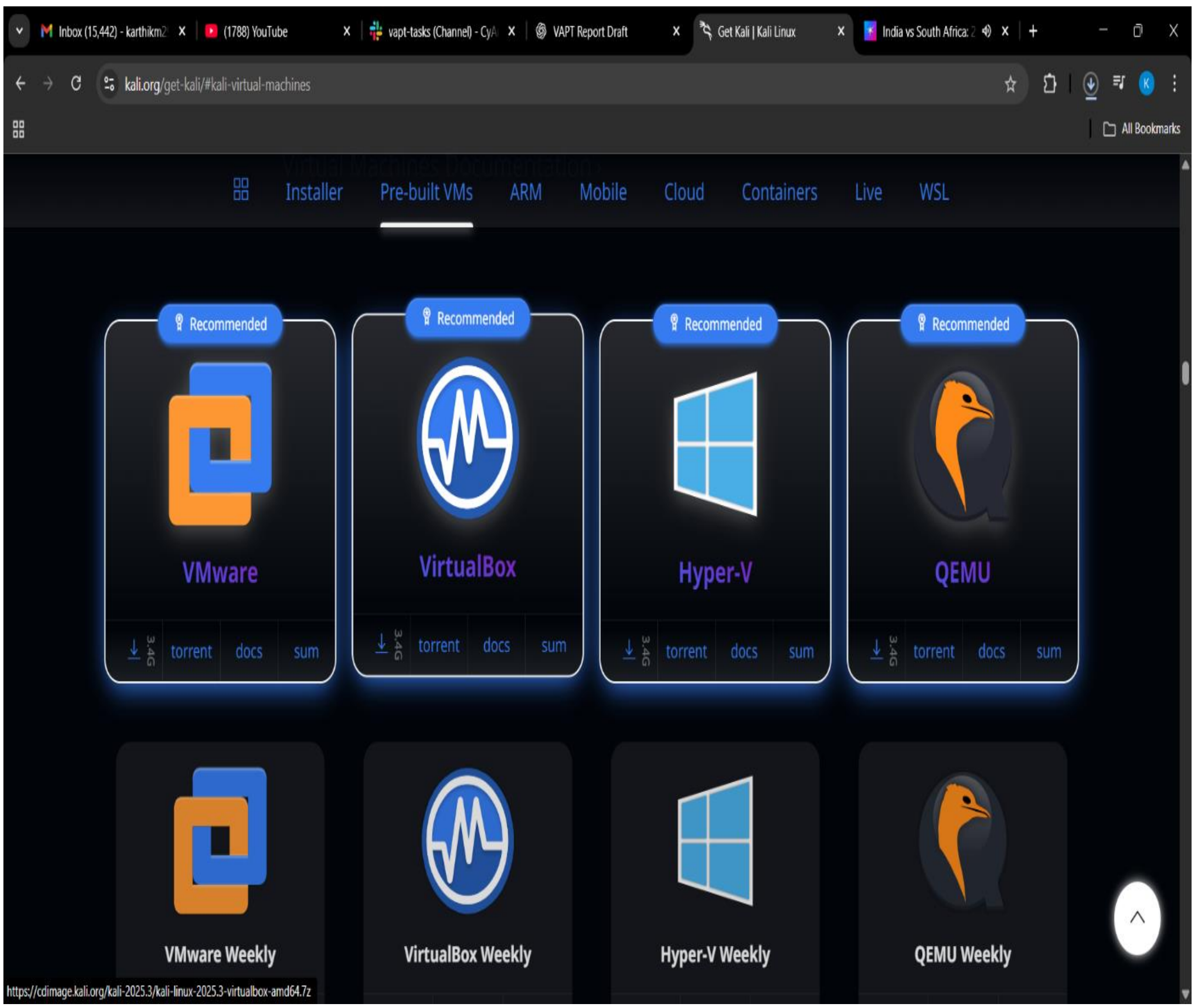
Install and Configure VirtualBox

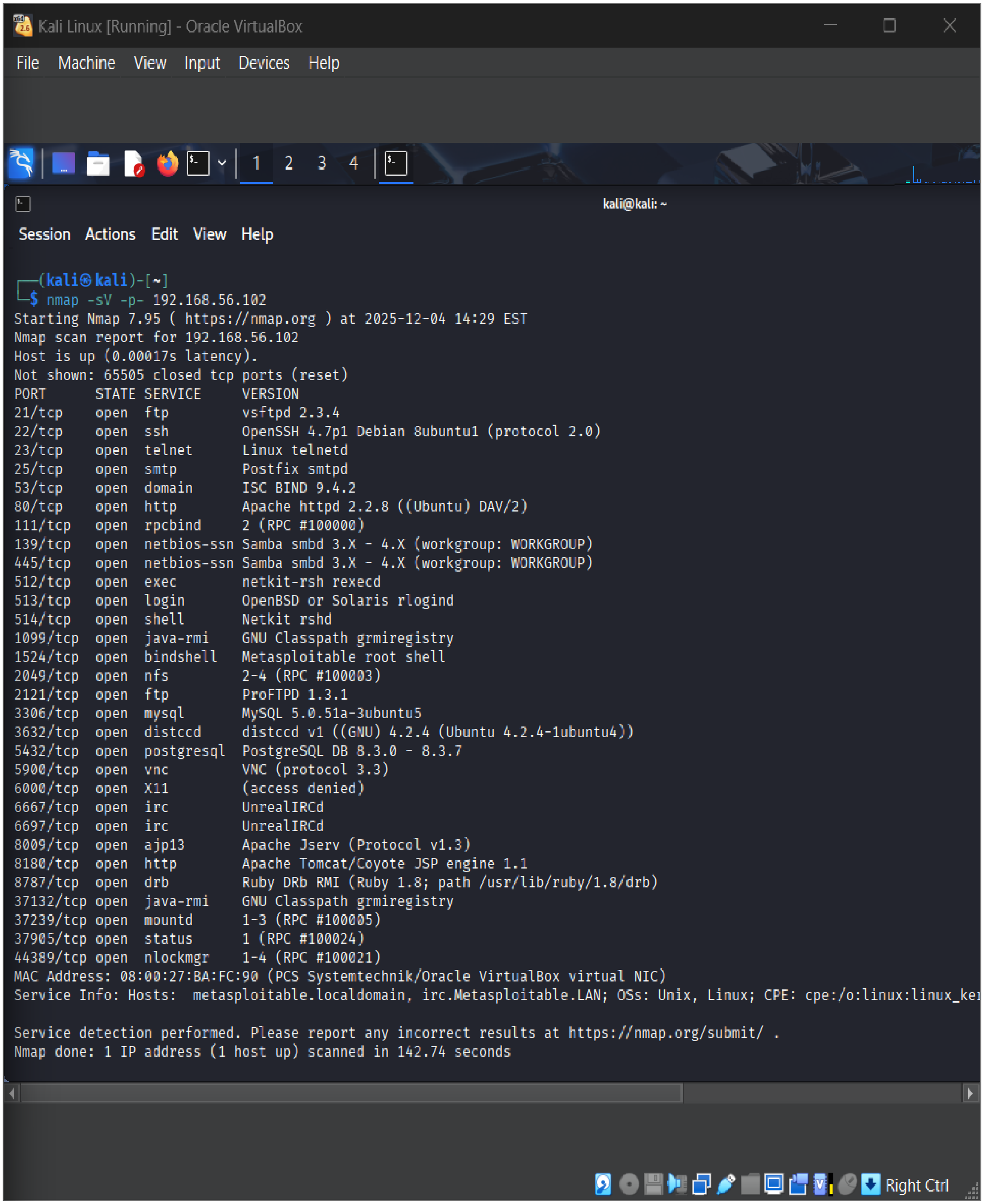
1. **Install VirtualBox on the host machine (Windows/Linux).**
2. **Create two VMs:**
   - Kali Linux (attacker).
   - Metasploitable 3 (target VM, downloaded from GitHub).
3. **Configure networking:**
   - Use Host-Only or Internal Network so the VMs can communicate but are isolated from the internet.

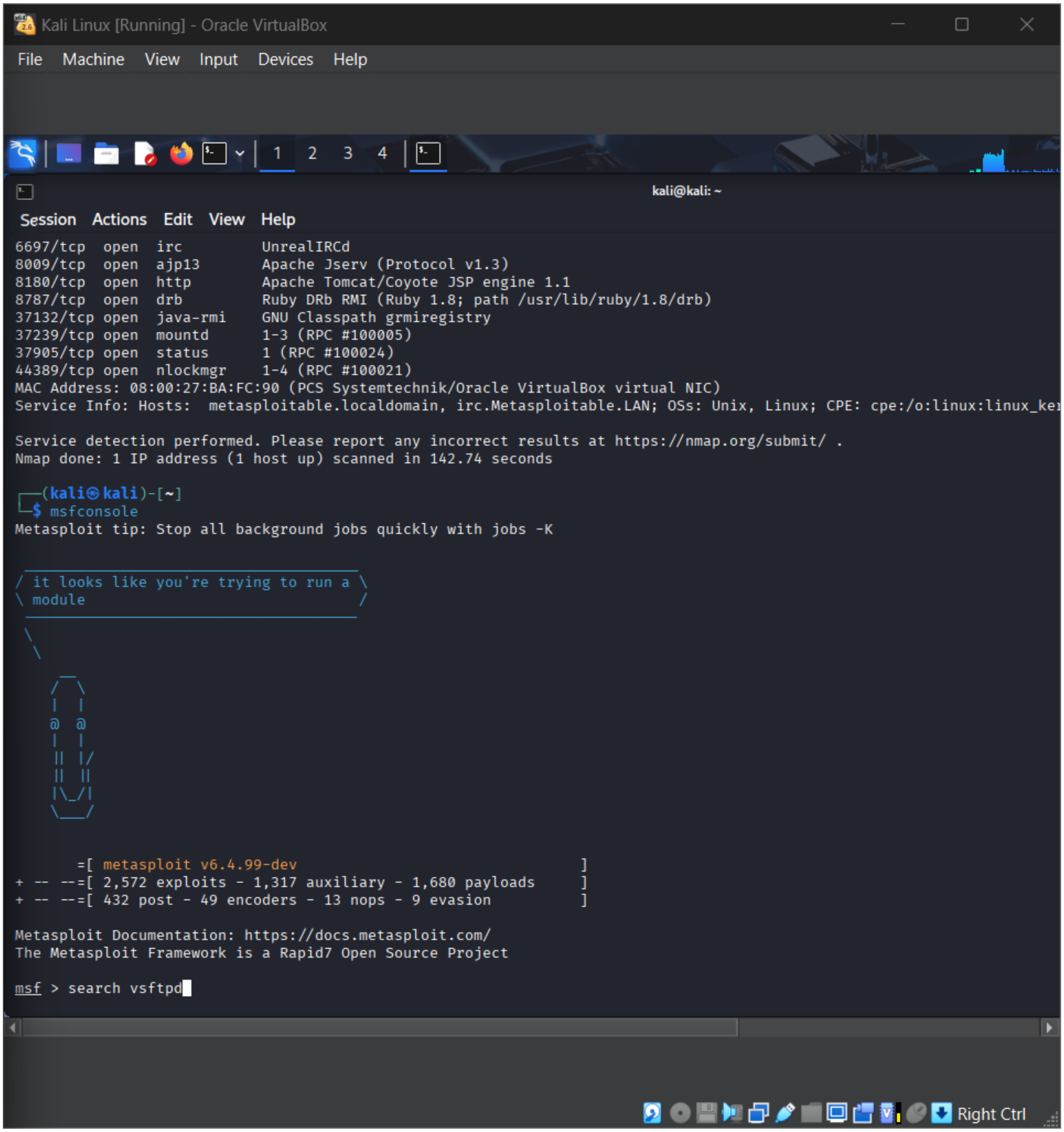
- Assign:
  - Kali: e.g., 192.168.56.101
  - Metasploitable 3: 192.168.56.102
- Ensure both are on the same subnet.

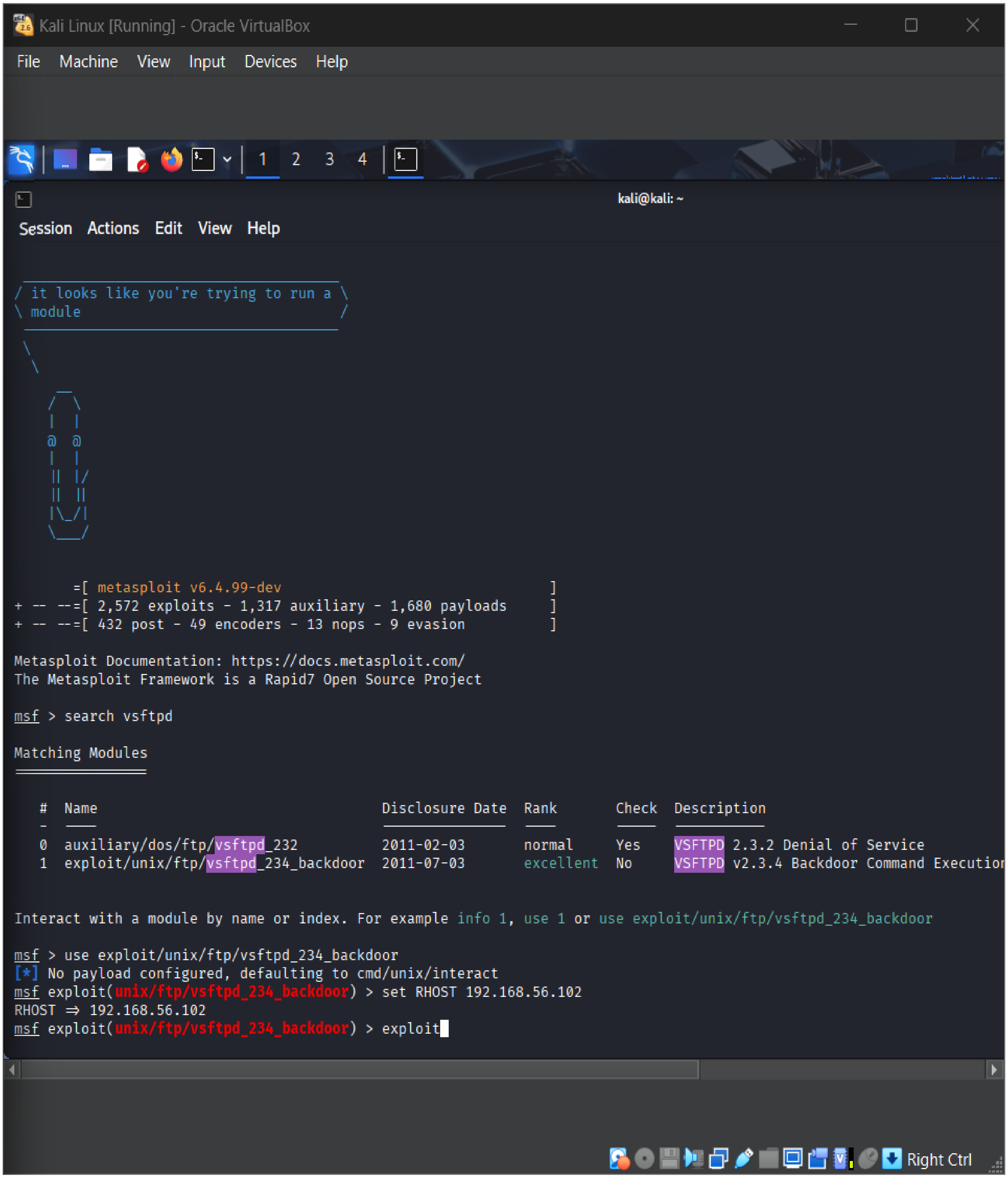
Install & Update Kali Linux

1. Boot Kali and update packages:
2. sudo apt update && sudo apt upgrade -y
3. Confirm essential tools:
   - Nmap, Metasploit, Nikto, and optionally OWASP ZAP and OpenVAS/GVM.




Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -sV -p- 192.168.56.102
Starting Nmap 7.95 (https://nmap.org) at 2025-12-04 14:29 EST
Nmap scan report for 192.168.56.102
Host is up (0.00017s latency).
Not shown: 65505 closed tcp ports (reset)
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 OpenBSD or Solaris rlogind
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
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
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
6697/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37132/tcp open java-rmi GNU Classpath grmiregistry
37239/tcp open mountd 1-3 (RPC #100005)
37905/tcp open status 1 (RPC #100024)
44389/tcp open nlockmgr 1-4 (RPC #100021)
MAC Address: 08:00:27:BA:FC:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ker
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.74 seconds
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help
6697/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
8787/tcp open drb Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
37132/tcp open java-rmi GNU Classpath grmiregistry
37239/tcp open mountd 1-3 (RPC #100005)
37905/tcp open status 1 (RPC #100024)
44389/tcp open nlockmgr 1-4 (RPC #100021)
MAC Address: 08:00:27:BA:FC:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_ker
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.74 seconds
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Stop all background jobs quickly with jobs -K
it looks like you're trying to run a module
=[metasploit v6.4.99-dev]
+ -- --=[2,572 exploits - 1,317 auxiliary - 1,680 payloads]
+ -- --=[432 post - 49 encoders - 13 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search vsftpd
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
Session Actions Edit View Help
it looks like you're trying to run a module
=[metasploit v6.4.99-dev]
+ -- --=[2,572 exploits - 1,317 auxiliary - 1,680 payloads]
+ -- --=[432 post - 49 encoders - 13 nops - 9 evasion]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
msf > search vsftpd
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Executio
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
Right Ctrl

Vulnerability Scanning

Tools:

- OpenVAS / GVM
- Nikto

Configure and Start OpenVAS / GVM

1. Install (if not already installed):
2. sudo apt install gvm -y
3. Initialize and set up:
4. sudo gvm-setup
5. Start the services:
6. sudo gvm-start
7. Access the Greenbone web interface:
    - Open browser in Kali: https://127.0.0.1:9392
    - Log in with the credentials generated during setup.

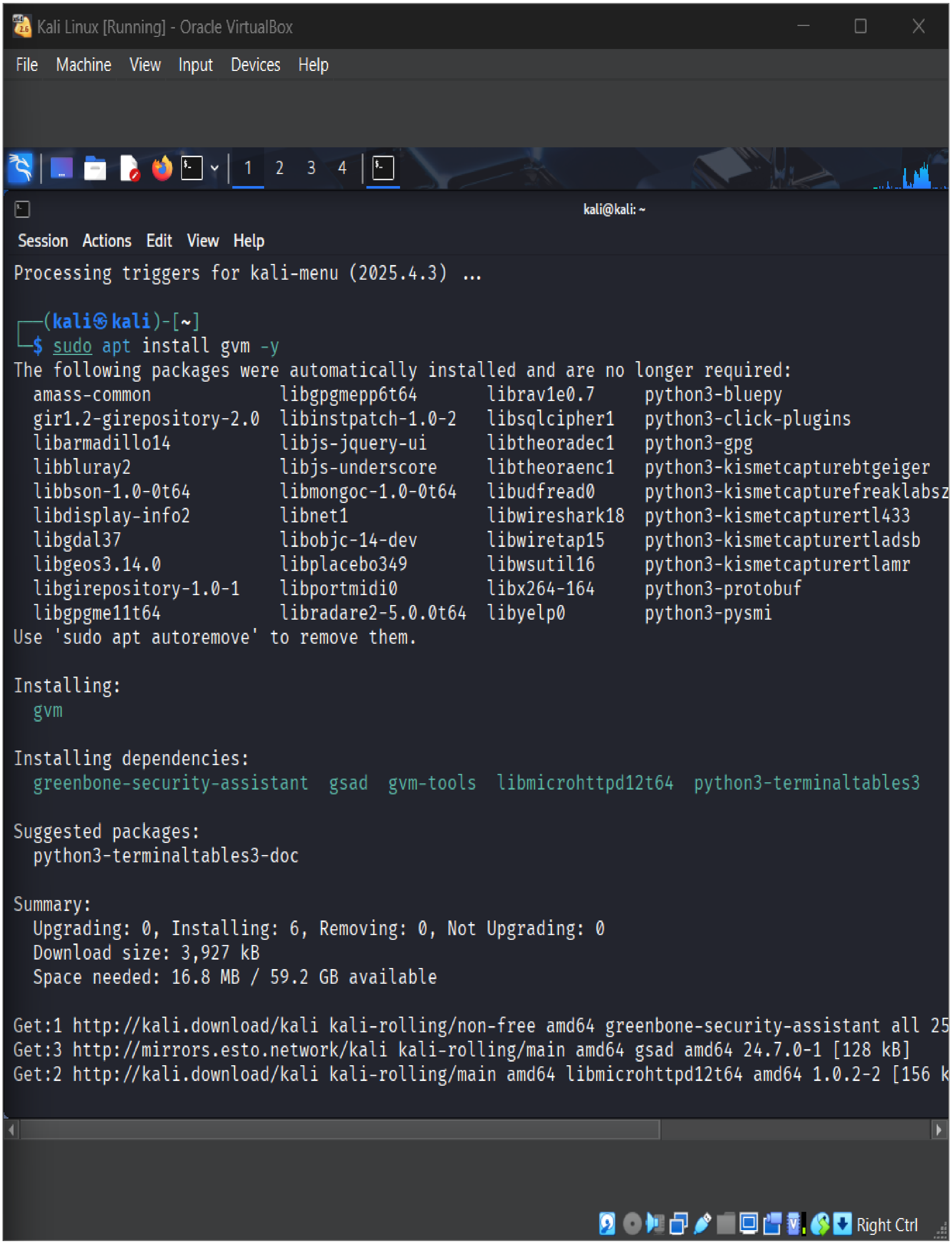
Create and Run a Scan against Metasploitable 3

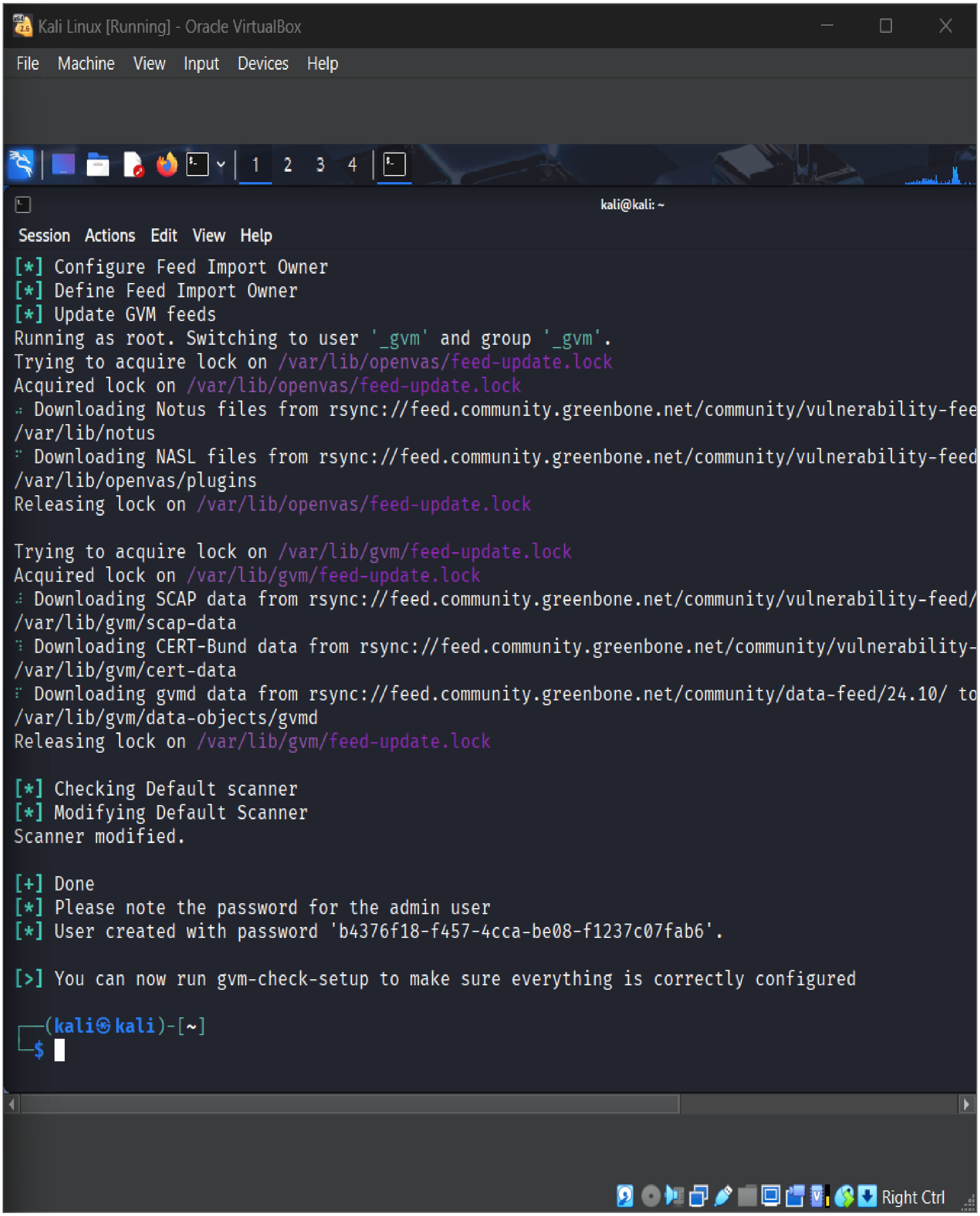
1. Add Target
    - In Greenbone, go to *Configuration* → *Targets*.
    - Create a new target with:
        - Name: Metasploitable3
        - IP Address: 192.168.56.101
2. Create a Task
    - Go to *Scans* → *Tasks*.
    - Create a new task:
        - Task Name: Full Scan – Metasploitable3
        - Target: Metasploitable3.
3. Run the Task
    - Start the task and wait for completion.
4. View Report
    - Open the report details.
    - Note:
        - Vulnerability name.

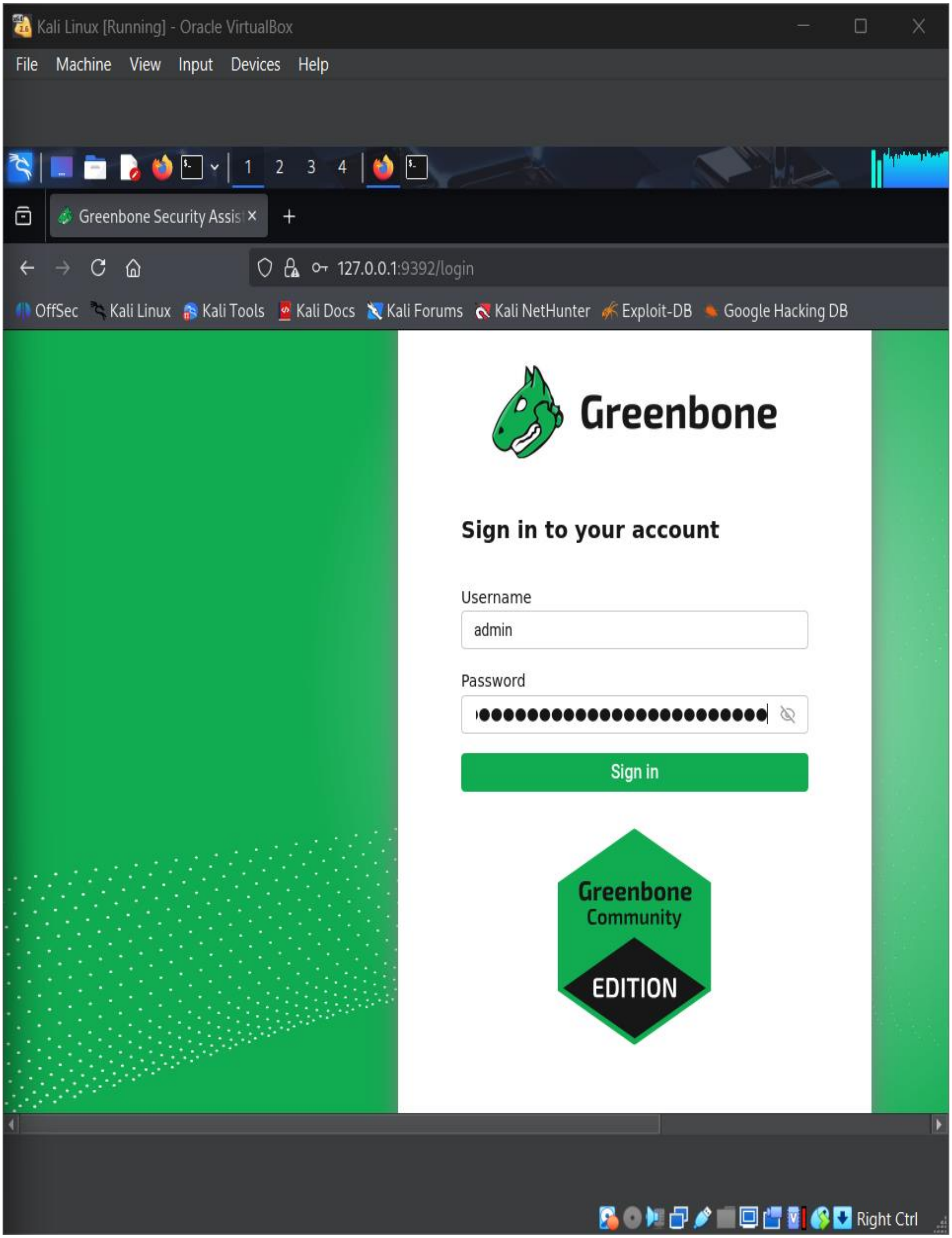
- CVSS score.
- CVE ID.
- Affected port/service.
- Short description and proposed solution.

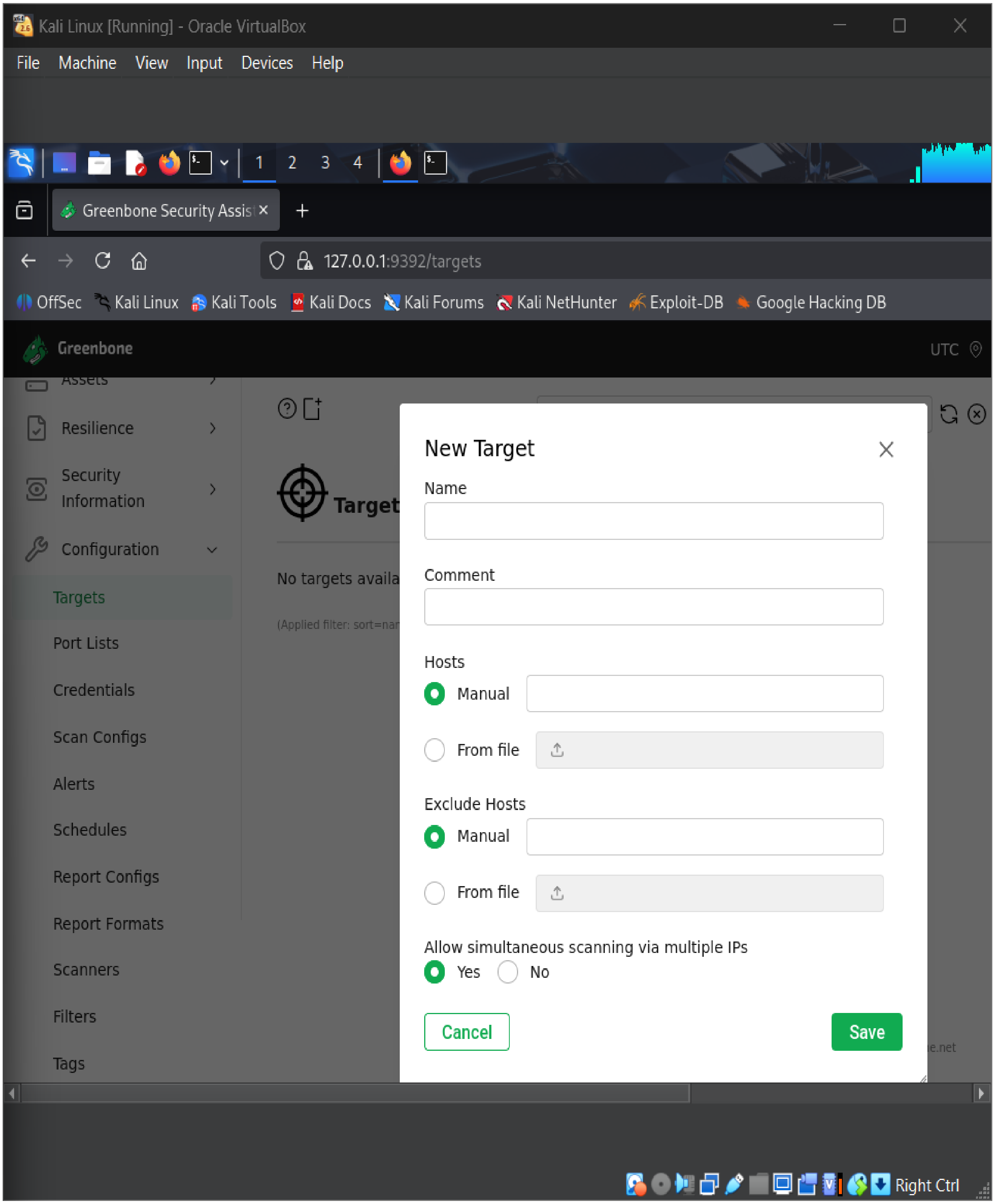
Web Server Scanning with Nikto

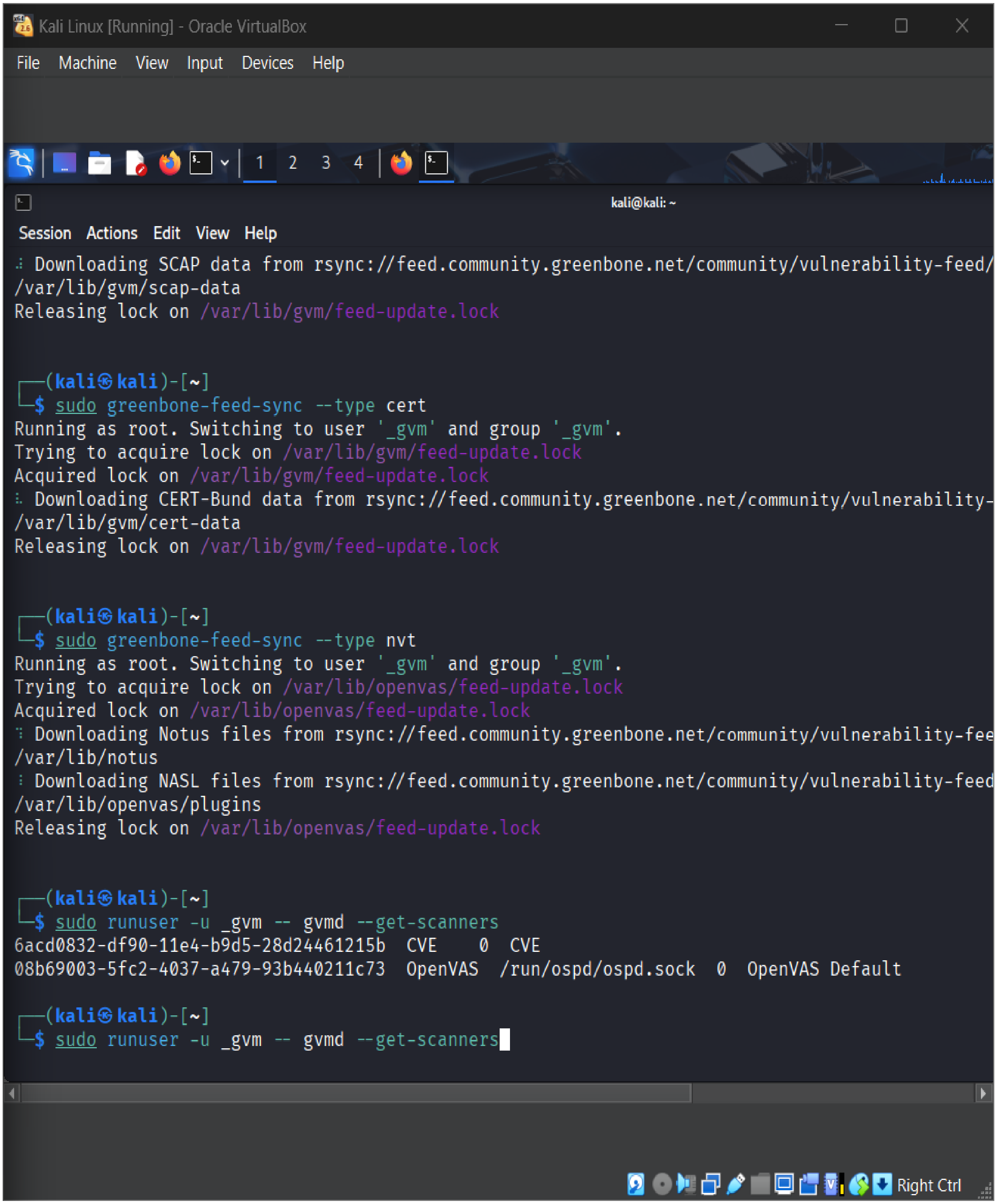
1. Identify web service ports on Metasploitable 3 using Nmap:
2. nmap -sV 192.168.56.101
   - Look for HTTP/HTTPS ports (e.g., 80, 8080).
3. Run Nikto against the web server:
4. nikto -h http://192.168.56.101
5. Record:
   - Outdated software versions.
   - Known vulnerabilities.
   - Dangerous HTTP methods.
   - Directory listing and configuration issues.

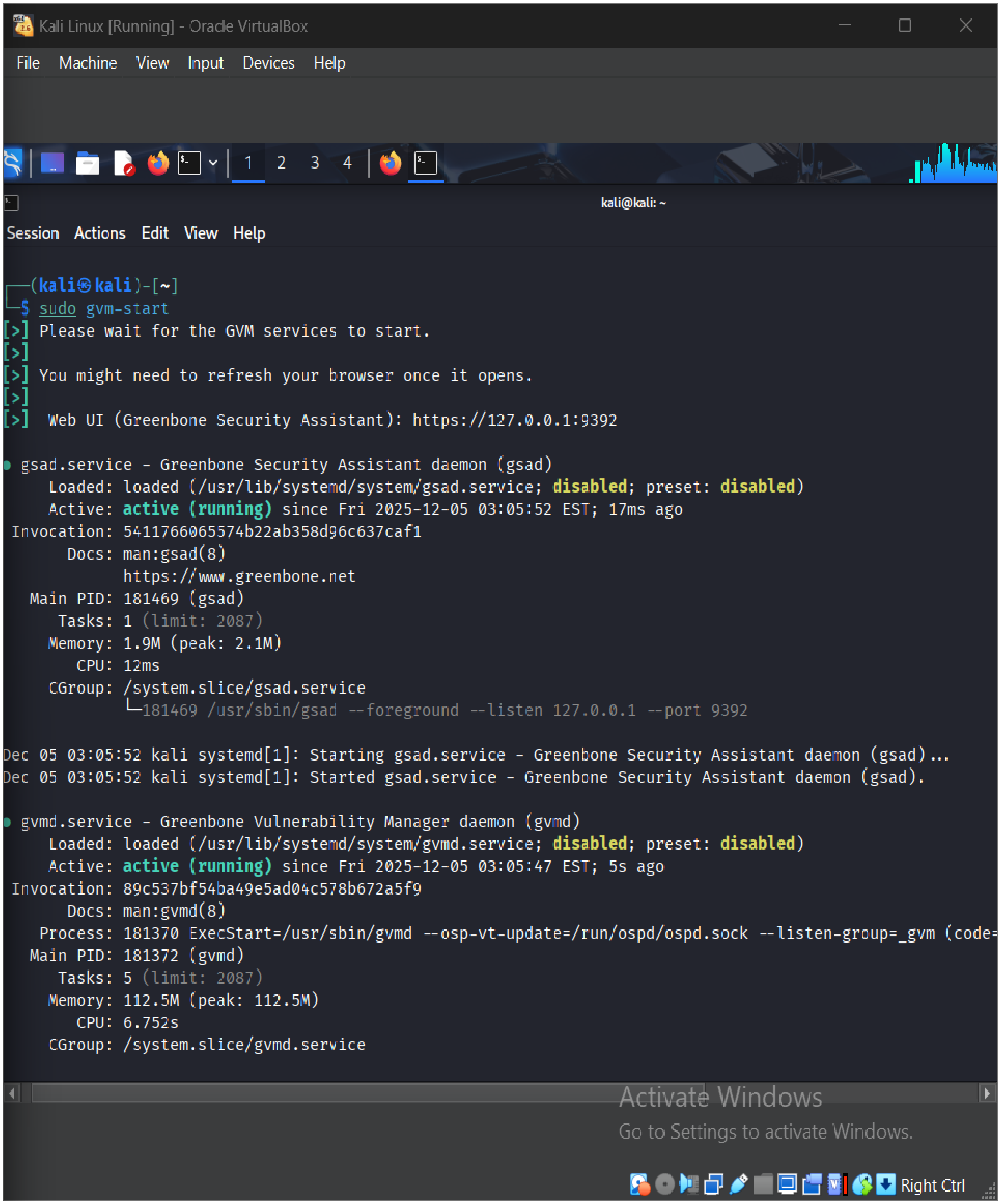

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help
Processing triggers for kali-menu (2025.4.3) ...
┌──(kali㉿kali)-[~]
└─$ sudo apt install gvm -y
The following packages were automatically installed and are no longer required:
amass-common libgpgmepp6t64 librav1e0.7 python3-bluepy
gir1.2-girepository-2.0 libinstpatch-1.0-2 libsqlcipher1 python3-click-plugins
libarmadillo14 libjs-jquery-ui libtheoradec1 python3-gpg
libbluray2 libjs-underscore libtheoraenc1 python3-kismetcapturebtgeiger
libbson-1.0-0t64 libmongoc-1.0-0t64 libudfread0 python3-kismetcapturefreaklabsz
libdisplay-info2 libnet1 libwireshark18 python3-kismetcapturertl433
libgdal37 libobjc-14-dev libwiretap15 python3-kismetcapturertladsb
libgeos3.14.0 libplacebo349 libwsutil16 python3-kismetcapturertlamr
libgirepository-1.0-1 libportmidi0 libx264-164 python3-protobuf
libgpgme11t64 libradare2-5.0.0t64 libyelp0 python3-pysmi
Use 'sudo apt autoremove' to remove them.
Installing:
gvm
Installing dependencies:
greenbone-security-assistant gsad gvm-tools libmicrohttpd12t64 python3-terminaltables3
Suggested packages:
python3-terminaltables3-doc
Summary:
Upgrading: 0, Installing: 6, Removing: 0, Not Upgrading: 0
Download size: 3,927 kB
Space needed: 16.8 MB / 59.2 GB available
Get:1 http://kali.download/kali kali-rolling/non-free amd64 greenbone-security-assistant all 25
Get:3 http://mirrors.esto.network/kali kali-rolling/main amd64 gsad amd64 24.7.0-1 [128 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 libmicrohttpd12t64 amd64 1.0.2-2 [156 k
Right Ctrl

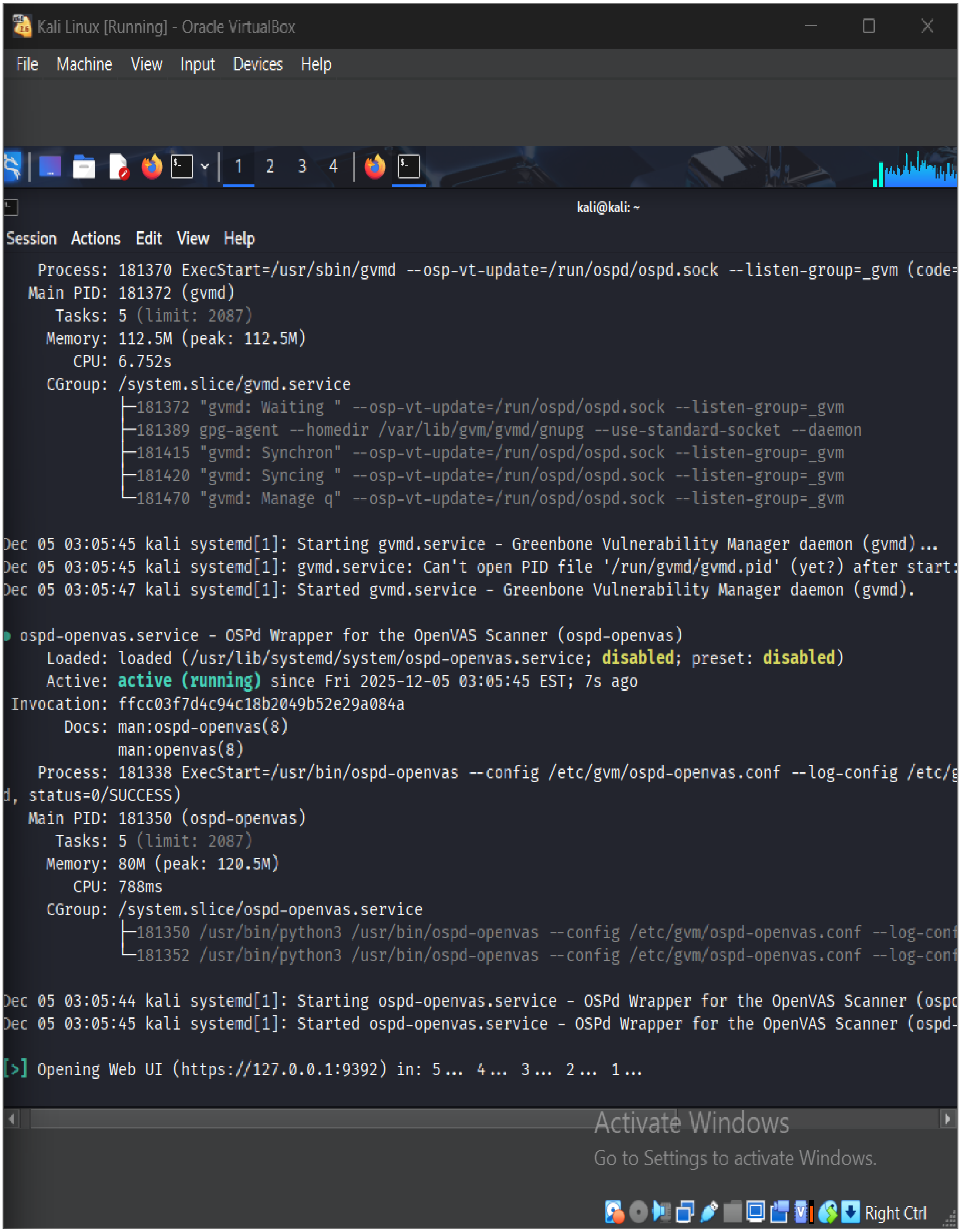

Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help
[*] Configure Feed Import Owner
[*] Define Feed Import Owner
[*] Update GVM feeds
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-fee
/var/lib/notus
Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed
/var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/
/var/lib/gvm/scap-data
Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-
/var/lib/gvm/cert-data
Downloading gvmd data from rsync://feed.community.greenbone.net/community/data-feed/24.10/ to
/var/lib/gvm/data-objects/gvmd
Releasing lock on /var/lib/gvm/feed-update.lock
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.
[+] Done
[*] Please note the password for the admin user
[*] User created with password 'b4376f18-f457-4cca-be08-f1237c07fab6'.
[>] You can now run gvm-check-setup to make sure everything is correctly configured
(kali㉿kali)-[~]
$
Right Ctrl

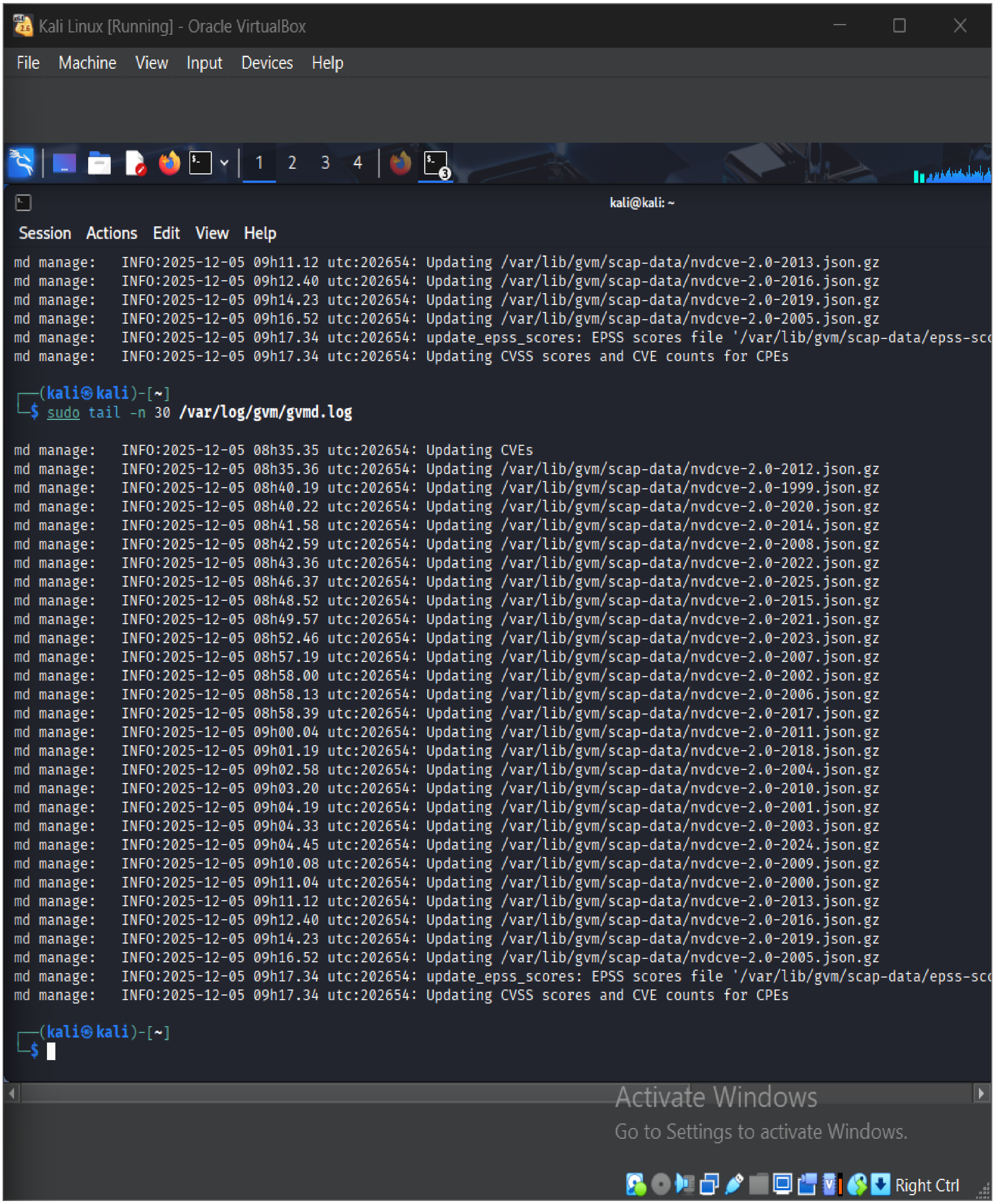

Kali Linux [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
Greenbone Security Assis
127.0.0.1:9392/login
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Greenbone
Sign in to your account
Username
admin
Password
Sign in
Greenbone
Community
EDITION
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File
Machine
View
Input
Devices
Help
Greenbone Security Assis
127.0.0.1:9392/targets
OffSec
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
Greenbone
UTC
Resilience
Security Information
Configuration
Targets
Port Lists
Credentials
Scan Configs
Alerts
Schedules
Report Configs
Report Formats
Scanners
Filters
Tags
No targets availa
New Target
Name
Comment
Hosts
Manual
From file
Exclude Hosts
Manual
From file
Allow simultaneous scanning via multiple IPs
Yes
No
Cancel
Save
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help
Downloading SCAP data from rsync://feed.community.greenbone.net/community/vulnerability-feed/
/var/lib/gvm/scap-data
Releasing lock on /var/lib/gvm/feed-update.lock
(kali㉿kali)-[~]
$ sudo greenbone-feed-sync --type cert
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/gvm/feed-update.lock
Acquired lock on /var/lib/gvm/feed-update.lock
Downloading CERT-Bund data from rsync://feed.community.greenbone.net/community/vulnerability-
/var/lib/gvm/cert-data
Releasing lock on /var/lib/gvm/feed-update.lock
(kali㉿kali)-[~]
$ sudo greenbone-feed-sync --type nvt
Running as root. Switching to user '_gvm' and group '_gvm'.
Trying to acquire lock on /var/lib/openvas/feed-update.lock
Acquired lock on /var/lib/openvas/feed-update.lock
Downloading Notus files from rsync://feed.community.greenbone.net/community/vulnerability-fee
/var/lib/notus
Downloading NASL files from rsync://feed.community.greenbone.net/community/vulnerability-feed
/var/lib/openvas/plugins
Releasing lock on /var/lib/openvas/feed-update.lock
(kali㉿kali)-[~]
$ sudo runuser -u _gvm -- gvmd --get-scanners
6acd0832-df90-11e4-b9d5-28d24461215b CVE 0 CVE
08b69003-5fc2-4037-a479-93b440211c73 OpenVAS /run/ospd/ospd.sock 0 OpenVAS Default
(kali㉿kali)-[~]
$ sudo runuser -u _gvm -- gvmd --get-scanners
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help
┌──(kali㉿kali)-[~]
└─$ sudo gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
● gsad.service - Greenbone Security Assistant daemon (gsad)
Loaded: loaded (/usr/lib/systemd/system/gsad.service; disabled; preset: disabled)
Active: active (running) since Fri 2025-12-05 03:05:52 EST; 17ms ago
Invocation: 5411766065574b22ab358d96c637caf1
Docs: man:gsad(8)
https://www.greenbone.net
Main PID: 181469 (gsad)
Tasks: 1 (limit: 2087)
Memory: 1.9M (peak: 2.1M)
CPU: 12ms
CGroup: /system.slice/gsad.service
└─181469 /usr/sbin/gsad --foreground --listen 127.0.0.1 --port 9392
Dec 05 03:05:52 kali systemd[1]: Starting gsad.service - Greenbone Security Assistant daemon (gsad)...
Dec 05 03:05:52 kali systemd[1]: Started gsad.service - Greenbone Security Assistant daemon (gsad).
● gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)
Loaded: loaded (/usr/lib/systemd/system/gvmd.service; disabled; preset: disabled)
Active: active (running) since Fri 2025-12-05 03:05:47 EST; 5s ago
Invocation: 89c537bf54ba49e5ad04c578b672a5f9
Docs: man:gvmd(8)
Process: 181370 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=
Main PID: 181372 (gvmd)
Tasks: 5 (limit: 2087)
Memory: 112.5M (peak: 112.5M)
CPU: 6.752s
CGroup: /system.slice/gvmd.service
Activate Windows
Go to Settings to activate Windows.
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
Session Actions Edit View Help
Process: 181370 ExecStart=/usr/sbin/gvmd --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm (code=
Main PID: 181372 (gvmd)
Tasks: 5 (limit: 2087)
Memory: 112.5M (peak: 112.5M)
CPU: 6.752s
CGroup: /system.slice/gvmd.service
├─181372 "gvmd: Waiting " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
├─181389 gpg-agent --homedir /var/lib/gvm/gvmd/gnupg --use-standard-socket --daemon
├─181415 "gvmd: Synchron" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
├─181420 "gvmd: Syncing " --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
└─181470 "gvmd: Manage q" --osp-vt-update=/run/ospd/ospd.sock --listen-group=_gvm
Dec 05 03:05:45 kali systemd[1]: Starting gvmd.service - Greenbone Vulnerability Manager daemon (gvmd)...
Dec 05 03:05:45 kali systemd[1]: gvmd.service: Can't open PID file '/run/gvmd/gvmd.pid' (yet?) after start:
Dec 05 03:05:47 kali systemd[1]: Started gvmd.service - Greenbone Vulnerability Manager daemon (gvmd).
● ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-openvas)
Loaded: loaded (/usr/lib/systemd/system/ospd-openvas.service; disabled; preset: disabled)
Active: active (running) since Fri 2025-12-05 03:05:45 EST; 7s ago
Invocation: ffcc03f7d4c94c18b2049b52e29a084a
Docs: man:ospd-openvas(8)
man:openvas(8)
Process: 181338 ExecStart=/usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-config /etc/g
d, status=0/SUCCESS)
Main PID: 181350 (ospd-openvas)
Tasks: 5 (limit: 2087)
Memory: 80M (peak: 120.5M)
CPU: 788ms
CGroup: /system.slice/ospd-openvas.service
├─181350 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-conf
└─181352 /usr/bin/python3 /usr/bin/ospd-openvas --config /etc/gvm/ospd-openvas.conf --log-conf
Dec 05 03:05:44 kali systemd[1]: Starting ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd
Dec 05 03:05:45 kali systemd[1]: Started ospd-openvas.service - OSPd Wrapper for the OpenVAS Scanner (ospd-
[>] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
Activate Windows
Go to Settings to activate Windows.
Right Ctrl


Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
Session Actions Edit View Help
md manage: INFO:2025-12-05 09h11.12 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2013.json.gz
md manage: INFO:2025-12-05 09h12.40 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2016.json.gz
md manage: INFO:2025-12-05 09h14.23 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2019.json.gz
md manage: INFO:2025-12-05 09h16.52 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2005.json.gz
md manage: INFO:2025-12-05 09h17.34 utc:202654: update_epss_scores: EPSS scores file '/var/lib/gvm/scap-data/epss-sc
md manage: INFO:2025-12-05 09h17.34 utc:202654: Updating CVSS scores and CVE counts for CPEs
(kali㉿kali)-[~]
$ sudo tail -n 30 /var/log/gvm/gvmd.log
md manage: INFO:2025-12-05 08h35.35 utc:202654: Updating CVEs
md manage: INFO:2025-12-05 08h35.36 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2012.json.gz
md manage: INFO:2025-12-05 08h40.19 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-1999.json.gz
md manage: INFO:2025-12-05 08h40.22 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2020.json.gz
md manage: INFO:2025-12-05 08h41.58 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2014.json.gz
md manage: INFO:2025-12-05 08h42.59 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2008.json.gz
md manage: INFO:2025-12-05 08h43.36 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2022.json.gz
md manage: INFO:2025-12-05 08h46.37 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2025.json.gz
md manage: INFO:2025-12-05 08h48.52 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2015.json.gz
md manage: INFO:2025-12-05 08h49.57 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2021.json.gz
md manage: INFO:2025-12-05 08h52.46 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2023.json.gz
md manage: INFO:2025-12-05 08h57.19 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2007.json.gz
md manage: INFO:2025-12-05 08h58.00 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2002.json.gz
md manage: INFO:2025-12-05 08h58.13 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2006.json.gz
md manage: INFO:2025-12-05 08h58.39 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2017.json.gz
md manage: INFO:2025-12-05 09h00.04 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2011.json.gz
md manage: INFO:2025-12-05 09h01.19 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2018.json.gz
md manage: INFO:2025-12-05 09h02.58 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2004.json.gz
md manage: INFO:2025-12-05 09h03.20 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2010.json.gz
md manage: INFO:2025-12-05 09h04.19 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2001.json.gz
md manage: INFO:2025-12-05 09h04.33 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2003.json.gz
md manage: INFO:2025-12-05 09h04.45 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2024.json.gz
md manage: INFO:2025-12-05 09h10.08 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2009.json.gz
md manage: INFO:2025-12-05 09h11.04 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2000.json.gz
md manage: INFO:2025-12-05 09h11.12 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2013.json.gz
md manage: INFO:2025-12-05 09h12.40 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2016.json.gz
md manage: INFO:2025-12-05 09h14.23 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2019.json.gz
md manage: INFO:2025-12-05 09h16.52 utc:202654: Updating /var/lib/gvm/scap-data/nvdcve-2.0-2005.json.gz
md manage: INFO:2025-12-05 09h17.34 utc:202654: update_epss_scores: EPSS scores file '/var/lib/gvm/scap-data/epss-sc
md manage: INFO:2025-12-05 09h17.34 utc:202654: Updating CVSS scores and CVE counts for CPEs
(kali㉿kali)-[~]
$
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

Document Findings

Create a Vulnerability Tracking Sheet

Recommended columns:

- Hostname / IP
- Port
- Protocol
- Service / Application
- Vulnerability Title
- CVE ID (if available)
- CVSS Score
- Risk Level (High/Medium/Low)
- Description
- Evidence (screenshot/file reference)
- Recommendation / Remediation
- Status (Open/Closed)

Asset & Service Inventory Sheet (Host: 192.168.56.102)

Table1

IP Address	Port	Protocol	Service	Version	Severity
192.168.56.102	22	TCP	SSH	OpenSSH (default creds)	High
192.168.56.102		TCP	FTP	vsftpd 2.3.4 (backdoored)	High
192.168.56.102	6200	TCP	vsftpd	2.3.4 (backdoor)	High
192.168.56.102	3306	TCP	MySQL	5.0.51a (empty root password)	High
192.168.56.102	5432	TCP	PostgreSQL	8.3.1 (weak creds)	High
192.168.56.102	5900	TCP	VNC	Unencrypted / weak passwd	High
192.168.56.102	1524	TCP	Ingreslock	Backdoor remote command	High
192.168.56.102	3632	TCP	DistCC Daemon	RCE vulnerable	High
192.168.56.102	1099	TCP	Java RMI	Remote class load → RCE	High
192.168.56.102	80	TCP	HTTP	TikiWiki, TWiki, PHP-CGI	High
192.168.56.102	25	TCP	SMTP	STARTTLS injection + VRFY	Medium
192.168.56.102	445	TCP	Samba 3.0.20	Remote command execution	Medium
192.168.56.102	23	TCP	Telnet	Clear-text login	Medium
192.168.56.102	6667	TCP	UnrealIRCd	Remote backdoor	High
192.168.56.102	8787	TCP	druby	Remote Ruby exec	High

Table2

Column 1	Column 2	Column 3	Column 4	Column 5
Critical Vulnerability Register (Top High Risks)				
Vulnerability	**Port**	**CVSS**	**Description**	**Impact**
TWiki RCE + XSS	80	10	Full code execution via eval() and unsanitized URLPARAM	Full server compromise
OS End of Life	general	10	Ubuntu 8.04 unsupported	No security patches; total compromise likel
dRuby Remote Command Execution	8787	10	Allows ruby syscall remote execution	Root takeover possible
Java RMI Remote Code Execution	1099	10	Remote class loading enables arbitrary exec	Full host compromise
vsftpd Backdoor	21 & 6200	7.5	Known malicious build triggers remote shell	Verified backdoor
Ingreslock backdoor	1524	10	Returns root id immediately	Remote root without auth
DistCC RCE	3632	9.3	Unrestricted compilation exec path	Attackers run shell commands

Table3

CVSS Scoring Tracker Sheet	Column 1	Column 2	Column 3	Column 4
Vuln ID	Name	CVSS	Vector Breakdown	Risk
VULN-001	TWiki RCE	10	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical
VULN-002	Ingreslock	10	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical
VULN-003	Java RMI RCE	10	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical
VULN-004	dRuby RCE	10	AV:N/AC:L/Au:N/C:C/I:C/A:C	Critical
VULN-005	OS EOL	10	NA (lifecycle scoring)	Critical
VULN-006	vsftpd Backdoor	7.5	AV:N/AC:L/Au:N/C:C/I:C/A:C	High
VULN-007	DistCC RCE	9.3	AV:N/AC:M/Au:N/C:C/I:C/A:C	High
VULN-009	MySQL weak root	9	AV:N/AC:L/Au:N/C:P/I:P/A:N	High
VULN-010	PostgreSQL weak	9	AV:N/AC:L/Au:N/C:P/I:P/A:N	High

Table4

Column 1	Column 2	Column 3	Column 4
Risk Matrix (Based on Likelihood × Impact)			
Likelihood ↓ / Impact →	Low	Medium	High
High	FTP anon login	SMTP STARTTLS MITM	Java RMI RCE, TWiki, dRuby, OS EOL, DistCC, vsftpd
Medium	Weak SSH MAC	SSL Expired	Samba RCE
Low	TCP timestamps	TRACE enabled	phpinfo exposure

Table5

Column 1	Column 2	Column 3	Column 4	Column 5
5. Remediation Action Plan Sheet				
Priority	Vulnerability	Fix Action	Owner	ETA
P1 (Critical)	OS unsupported	Replace OS (upgrade to supported Ubuntu)	Infra	Immediate
P1 (Critical)	TWiki RCE	Decommission or upgrade to ≥ 4.2.4	AppSec	Immediate
P1	Java RMI RCE	Disable remote class loading	DevOps	48 hrs
P1	dRuby RCE	Disable DRb or restrict ACL	DevOps	72 hrs
P1	vsftpd backdoor	Remove immediately	Admin	Immediate
P1	Ingreslock	Kill daemon, patch image	SOC/Blue	24 hrs
P2	Weak DB creds	Set strong creds & enforce MFA	DBA	3 days
P2	VNC weak/no auth	Harden + encryption	Infra	2 days
P2	Samba RCE	Patch Samba 3.x	Infra	5 days
P3	phpinfo exposed	Delete phpinfo scripts	Web	Done
P3	SSL Expired	Reissue certificates	SecOps	1 week

Remediation Plan

- **List recommended actions in priority order.**
    1. **Immediate (High Risk)**
        - Patch critical vulnerabilities (Tomcat, SMB, etc.).
        - Disable unnecessary services and close unused ports.
    2. **Short Term (Medium Risk)**
        - Harden configurations (e.g., disable directory listing, enforce strong passwords).
        - Enable logging and monitoring.
    3. **Long Term (Low Risk / Strategic)**
        - Implement patch management process.
        - Regularly perform vulnerability assessments and penetration tests.
        - Align with CIS Benchmarks and ISO 27001 controls.

Conclusion:

Summarize:

- The lab environment (Metasploitable 3) is intentionally vulnerable and thus contains multiple critical issues.
- **The assessment demonstrates:**
    - How to use free tools (OpenVAS, Nmap, Nikto, Metasploit, etc.) to identify and validate vulnerabilities.
    - How to align technical findings with risk and prioritization via CVSS and a risk matrix.
    - How to structure and present results in a corporate-style report.

Highlight key learnings:

- Importance of systematic methodology (Planning → Discovery → Attack → Reporting).
- Value of using standards like OWASP Top 10 and CVSS for prioritizing remediation.
- Necessity of continuous monitoring, patching, and secure configuration.

---

6. Summary:

- **Security Assessment & Methodologies**
    - NIST SP 800-115 (Technical Guide to Information Security Testing).
- **VAPT and Web Security**
    - OWASP Web Security Testing Guide (WSTG).
    - OWASP Top 10.
- **Vulnerability Scanning & Risk**
    - NVD (National Vulnerability Database) for CVEs and CVSS scores.
- **Configuration & Compliance**
    - CIS Benchmarks for system hardening.
- **Tools Documentation**
    - Official documentation pages for:
        - Nmap
        - OpenVAS / Greenbone
        - Metasploit Framework
        - Nikto
        - OWASP ZAP
        - Kali Linux