Vulnerability Assessment and Penetration Testing

ABSTRACT

1 Security Assessment

It is a systematic review of an organization's IT systems, networks and processes to find vulnerabilities, threats and weakness, ensuring that security controls work effectively and identifying areas needing improvement to protect data and maintain compliance.

1.1 NIST Framework & Guideliness

A voluntary, flexible approach for managing cyber risk across all size of organizations, focusing on five core functions as:

A.Identify: Understanding Assets, system and risks.

B.Protect: Implement safeguards as access control, encryption and backups.

C.Detect: Identify cybersecurity events.

D.Respond: Take actions on detected incident.

E.Recover: Restore capabilities after an event.

1.2 Types of Security Testing

1.2.1 Vulnerability Assessment

- The goal of vulnerability assessment is to systematically find, quantify and proritize security weakness in systems, networks and applications.
- Using the automated tools like OpenVAS to scan the systems for any vulnerabilities.
- After using OpenVAS, the result is to prioritize the list of vulnerabilities (High, Medium and low) with recommended remediation steps.

1.2.2 Penetration Testing

- The goal is to simulate a real-world cyberattack to exploit identified vulnerabilities and test defences.
- Using the tolls like Metasploit and Nmap and techniques like social engineering, SQL injection to gain unauthorised access and assess potential damage.
- Demonstrates that how vulnerabilities can be exploited, the extent of potential breach and provides actionable insights for strengthening defences.

1.2.3 Compliance Testing

- The goal is to verify systems, processes and control meet specific internal policies, industry regulations (PCI, DSS, HIPPA) or Government mandates (GDPR).

- Conducted formal audits and assessments against defined standards using documented evidence, producing a compliance report confirming adherence or non-adherence for legal and regulatory assurance.

2.VAPT Methodology

The methodology involves both vulnerability assessment and penetration testing and the goal of vulnerability assessment is to identify a weakness in a system (such as Outdated software's and misconfigurations.

The goal of penetration testing actively tries to exploit these flaws to see how far an attacker could get, revealing real-world impact. The Phases are

- Planning: Define goals, Scope (networks, apps), rules, timelines and compliance needs.
- Discovery: Collect data on the target using active and passive methods.
- Attack: Gaining access into the systems or applications through a identified vulnerabilities.
- Reporting: create a detailed reports with findings, evedence, risk level (High, Medium, Low)

3.Security Standards and compliance

Security standards & compliance are framework of rules, policies, and controls that guide organizations to protect data, manage risks and meet legal/industry requirements (like GDPR, HIPPA, PCI, DSS), ensuring data privacy security operations and customer trust through processes like risk assessment and access control and regular audits.

3.1 Key Standards & Framework

- ISO 27001/27002: International standard for information security management systems (ISMS)
- NIST Cybersecurity Framework: Guidelines from the U.S, national institute of standards and technology for managing cyber risk.
- GDPR (General Data Production Regulation): EU law for data protection and privacy.
- HIPPA (Health insurance portability and Accountability Act): U.S law for protecting sensitive health information.
- PCI DSS (Payment card industry and Data security Standard): Requirements for handling credit card data.

4.Risk Assessment

It is the process to identify hazards, analyze the likelihood and severity of potential harm, and determine control measures to eliminate or reduce risks.

4.1 Types of Risk Assessment

- Health & Safety: Focuses on physical hazards in the workplace.
- Cybersecurity: Identifies IT vulnerabilities and threats to digital systems.
- Finance/Investment: Analyzes potential losses in investments or loans, often using qualitative or quantitative methods.

4.2 CVSS and Risk Matrix

Risk matrix is a security tool which is used in the risk assessment to prioritize the risk based on the severity level (High, Medium and Low).

Common vulnerability scoring system is an open framework that provides a standardized way to rate the severity of computer security vulnerabilities, producing a numerical scale from 0.0 - 10.0.

5.Setup Testing Environment

5.1 Installing VMware workstation

Installing the VMware workstation from the official website and later setting up the configurations.

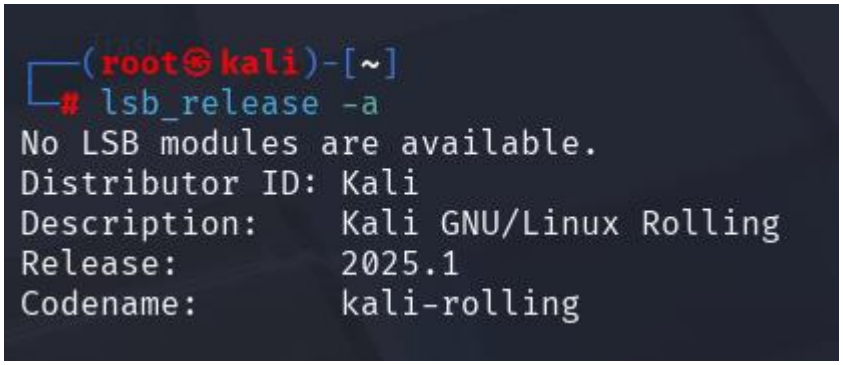
5.2 Installing Kali linux

Installed the kali linux from the official website as

https://kali.org/get-kali/

And then setting up in the VMware workstation.To verify that succesfully configured, check the version of the kali Linux as

lsb_release –a



5.3 Installing Metasploiable 3

Install the metasploitable 3 from the internet and configure it to the VMware workstation and verify that successfully installed or not. The default credentials are msfadmin/msfadmin.

6.Vulnerability Scanning

Use the open-source tool called Openvas to scan and identify the vulnerabilities and also you can use nikto for web application scanning.

Before setting up the openvas tool you have to start the services in your kali Linux

sudo systemctl start osap-openvas

suso systemctl start gvmd

sudo systemctl start gsad

sudo systemctl start redis-server

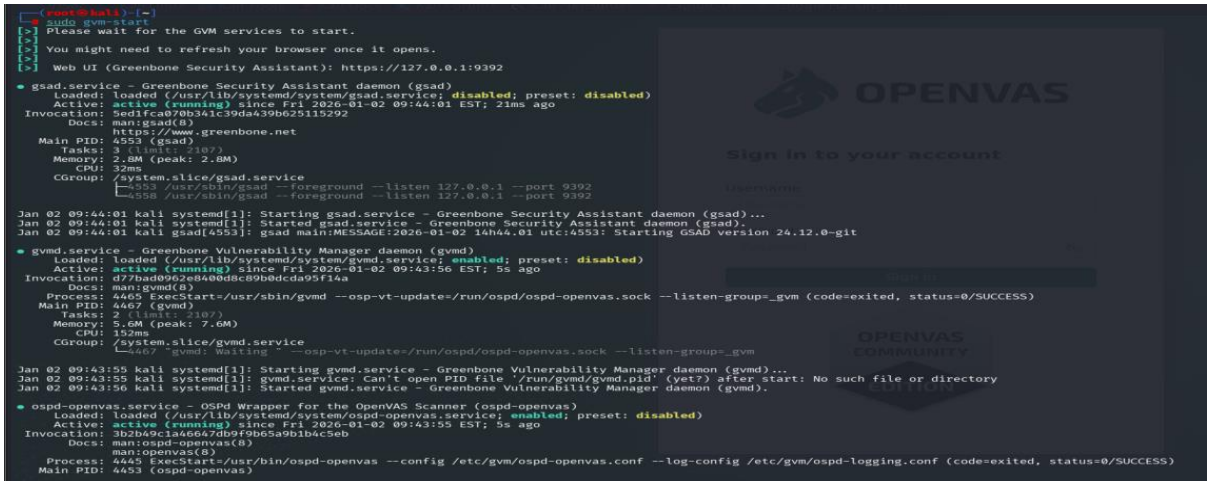
After starting those server, you must verify that there are running are not,

sudo systemctl status osap-openvas

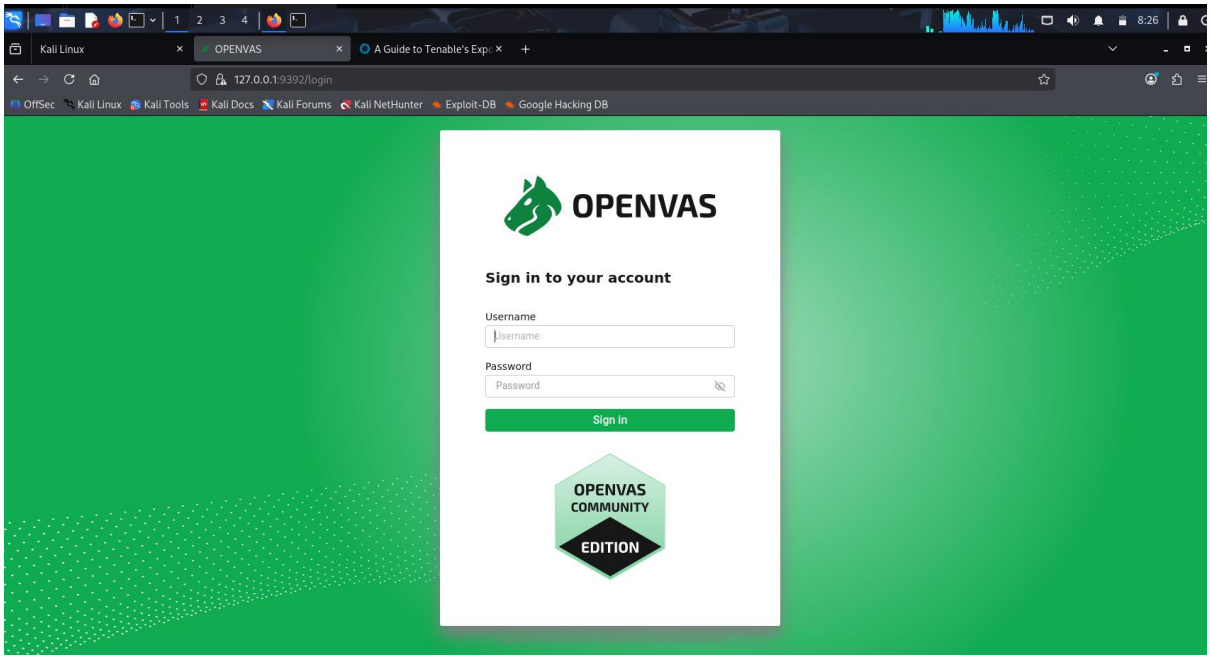
suso systemctl status gvmd

sudo systemctl status gsad

sudo systemctl status redis-server



After starting it will be directly open in the browser and it will be look as

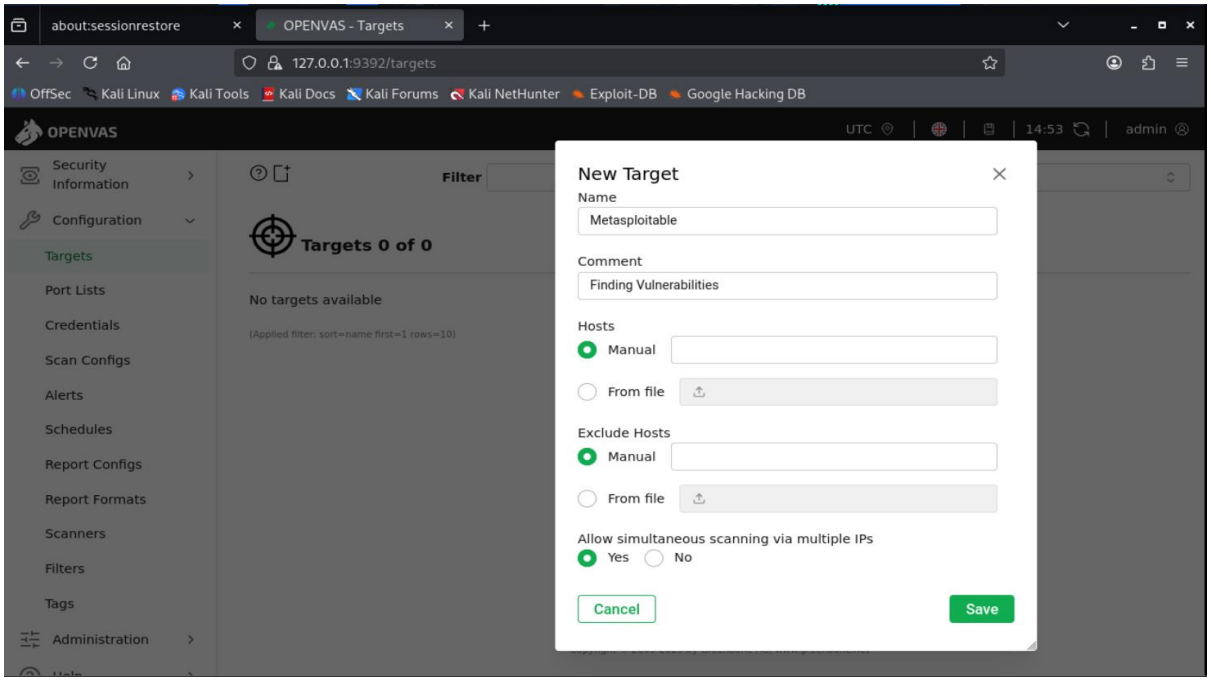


You can setup the login credentials by using the commands as

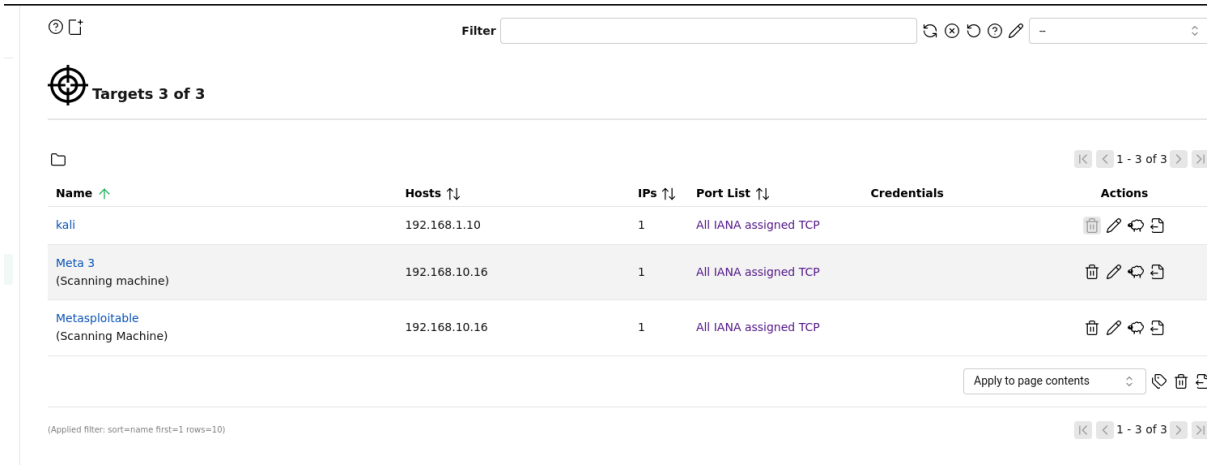
sudo runuser -u _gvm -- gvmd --user=admin --new-password=1234

After login into the openvas you have to create the target to scan the machine which was setup before called metasploitable 3

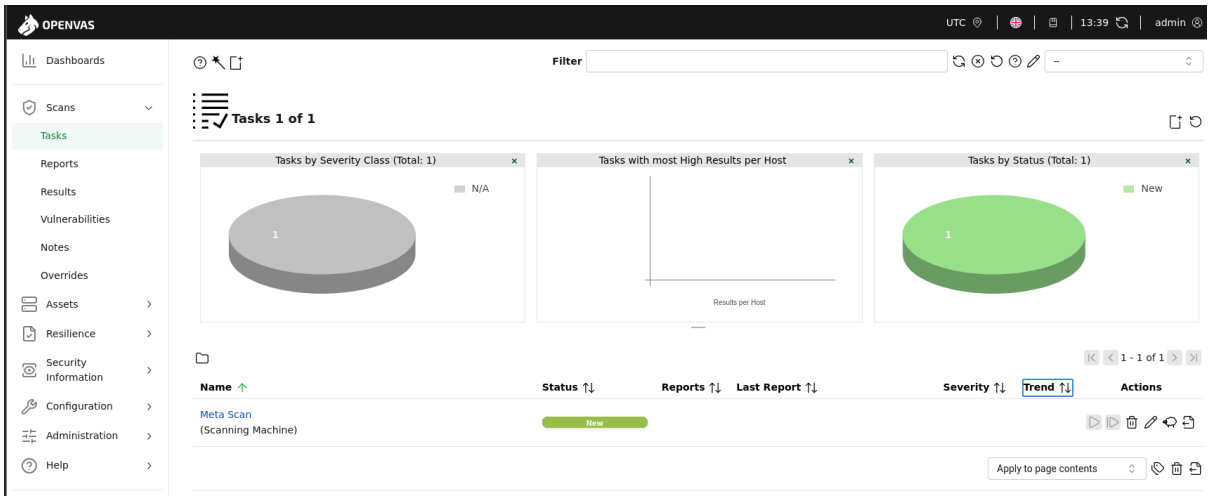
Go to configurations -> Target -> New target and provide the details of the machine like Ip address and any particular ports.



I have created the two targets under the configuration in which that will be scan the machines throught he ip address you provided.



After setting up the target navigate to Scans -> tasks -> new task and create the new task, in scan targets select the target before you created. I have created a task and that will added in the img below.



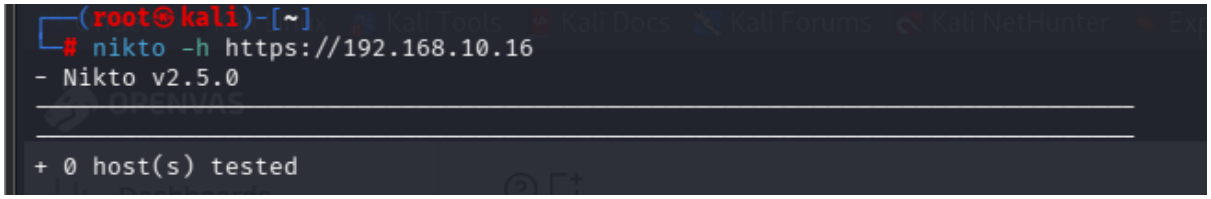
6.1 Using Nikto

First, i have installed the nikto in my kali Linux by using the command as

sudo apt install nikto

I have scanned the metasploitable 3 using the nikto in my kali Linux but i didn't get the results from that because the firewalls are fully protected to that machine.

nikto –h https://192.168.101.6



I have scanned the Metasploitable 3 using the OpenVAS but i didn’t get any results and i have tried a lot but i didn't get any results.

I got a lot of errors for the services which are in the kali Linux while setting up the OpenVAS. I tried a lot and i get the web UI working but the results didn’t get.

7.Conclusion

By setting up a controlled testing environment with Kali Linux and Metasploitable, performing vulnerability scans using tools like OpenVAS and Nikto, and carefully documenting and prioritizing identified weaknesses, you build practical, hands-on experience in real-world security assessment.

This structured approach not only strengthens understanding of vulnerability detection and risk evaluation but also reinforces the importance of ethical testing, proper documentation, and informed decision-making.

Ultimately, these practices help develop a strong foundation in VAPT, supporting safer system design and improved cybersecurity readiness.