



# **Amal Jyothi College of Engineering Kanjirappally, Kerala**

## **NESSUS**

### **MCA SEMINAR REPORT**

*Submitted in the partial fulfillment of the requirements for the  
Award of the Degree in*

Master of Computer Applications

By

**ANNU MARIYA JOMICHAN**

Reg No: LAJC18MCA012

*Under The Guidance Of*

**Ms. DILU MARIYA JOSEPH**

**January 2021**

**DEPARTMENT OF COMPUTER APPLICATIONS**

**AMAL JYOTHI COLLEGE OF ENGINEERING  
KANJIRAPPALLY**



**CERTIFICATE**

*This is to certify that the seminar report, "**NESSUS**" is the bonafide work of **ANNU MARIYA JOMICHAN (Reg.No:LAJC18MCA012)** in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications under APJ Abdul Kalam Technological University during the year 2020-21.*

**Ms. Dilu Mariya Joseph**  
**Internal Guide**

**Sr. Elsin Chakkalackal S.H**  
**Coordinator**

**Fr. Rubin Thottupuram**  
**Head of the Department**

## **ACKNOWLEDGEMENT**

First and foremost, I thank God almighty for his eternal love and protection throughout the seminar. I take this opportunity to express my gratitude to all who helped me in completing this seminar successfully. It has been said that gratitude is the memory of the heart. I wish to express my sincere gratitude to our manager **Rev. Fr. Dr. Mathew Paikatt** and Principal **Dr. Z V Lakaparampil** for providing good faculty for guidance.

I owe a great depth of gratitude towards our Head of the Department **Fr. Rubin Thottupuram** for helping us. I extend my whole hearted thanks to the seminar coordinators **Fr. Rubin Thottupuram** and **Sr.Elsin Chakkalackal S.H** for their valuable suggestions and for overwhelming concern and guidance from the beginning to the end of the seminar. I would also like to express sincere gratitude to my guide, **Ms. Dilu Mariya Joseph** for her inspiration and helping hand.

I thank our beloved teachers for their cooperation and suggestions that helped me throughout the seminar. I express my thanks to all my friends and classmates for their interest, dedication, and encouragement shown towards the seminar. I convey my hearty thanks to my family for the moral support, suggestions, and encouragement to make this venture a success.

**ANNU MARIYA JOMICHAN**

## **ABSTRACT**

Nessus is a great vulnerability scanning tool. It comes with an easy to use graphical user interface and is capable of scanning multiple networks for open ports and vulnerabilities. Nessus support Mac, linux and windows operating system. Nessus is a remote scanning tool that you can use to check computers for security vulnerabilities. It does not actively block any vulnerabilities that your computers have but it will be able to sniff them out by quickly running 1200+ vulnerability checks and throwing alerts when any security patches need to be made. If you are an administrator in charge of any computer (or group of computers) connected to the internet, Nessus is a great tool help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

Nessus holds a significant place among the penetration testing tool, which is branded susceptibility scanner and has been advanced by Tenable Network Security use it for free only if you use it for personal use amid a non-enterprise setting. However, it allows you to scan for numerous kinds of vulnerabilities. Nessus does not actively prevent attacks, it is only a tool that checks your computers to find vulnerabilities that hackers cloud exploit.

# **CONTENTS**

1. INTRODUCTION	1
1.1 KALI LINUX	
1.2 PENETRATION TESTING	
2. NESSUS	3
2.1 INTRODUCTION TO NESSUS	
2.2 FEATURES	
2.3 INSTALLING AND CONFIGURING NESSUS	
3. IMPLEMENTATION AND SCREENSHOTS	6
4. CONCLUSION	12
5. REFERENCES	13

# **1. INTRODUCTION**

## **1.1 KALI LINUX**

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. It was developed by Mati Aharoni and Devon Kearns of Offensive Security through the rewrite of Backtrack, their previous information security testing Linux distribution based on Knoppix. The third core developer Raphael Hertzog joined them as a Debian expert. Kali Linux was released on the 13th march, 2013 as a complete, top to bottom. Rebuild of Backtrack Linux, adhering completely to Debian development standards.

Features and other information of Kali Linux includes

- Over 600 penetration testing tools pre-installed
- Multi-language support
- Developed in a secure environment
- Free of cost
- OS Family - Unix like
- Working State - Active
- Platforms - x86, x86-64, armel, armhf
- Kernel Type - Monolithic kernel (Linux)
- Default UI - GNOME3

## **1.2 PENETRATION TESTING**

Penetration testing which is also called pen testing is refers to the process of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit and make use of it. Pen test can be done manually or it can be done automatically through software application. In either way, the process includes collecting information about the target before the test (reconnaissance), identify possible loop holes (entry points), attempting to break in (either virtually or for real) and reporting back the finding. The main objective of penetration testing is to determine security weakness.

**Different Strategies**

- Targeted testing - Testing team working together.
- External testing - Targets externally visible servers or devices.
- Internal testing - Attack behind the firewall.
- Blind testing - Simulates the actions of a real attacker

**Targeted testing:**

This testing is performed by the organization's IT testing team and the penetration testing team working together. It's sometimes referred to as a "lights-turned-on" approach because everyone can see and know the test being carried out.

**External testing:**

This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

**Internal testing:**

This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

**Blind testing:**

A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

**Benefits of Penetration Testing**

- Intelligently manage vulnerabilities.
- Avoid the cost of network downtime.
- Meet regulatory requirements and avoid fines.
- Preserve corporate image and customer loyalty.

## 2. NESSUS

### 2.1 INTRODUCTION TO NESSUS

Nessus is a great vulnerability scanning tool. It comes with an easy to use graphical user interface and is capable of scanning multiple networks for open ports and vulnerabilities. Nessus support Mac, linux and windows operating system. Nessus is a remote scanning tool that you can use to check computers for security vulnerabilities. It does not actively block any vulnerabilities that your computers have but it will be able to sniff them out by quickly running 1200+ vulnerability checks and throwing alerts when any security patches need to be made. If you are an administrator in charge of any computer (or group of computers) connected to the internet, Nessus is a great tool help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

Nessus holds a significant place among the penetration testing tool, which is branded susceptibility scanner and has been advanced by Tenable Network Security use it for free only if you use it for personal use amid a non-enterprise setting. However, it allows you to scan for numerous kinds of vulnerabilities. Nessus does not actively prevent attacks, it is only a tool that checks your computers to find vulnerabilities that hackers cloud exploit.

### 2.2 FEATURES

#### **Performance:**

- Issue tracking
- Detection rate
- False positives
- Automated scans

#### **Network**

- Compliance Testing
- Perimeter Scanning



## NESSUS

- Configuration Scanning

### Application

- Manual Application Testing
- Code Analysis
- Black-Box Scanning

## 2.3 INSTALLING AND CONFIGURING NESSUS

Nessus does not come pre-installed on Kali Linux, but can be installed and activated easily:

### Step 1: Purchase Nessus

You can purchase Nessus from Tenable's online store (including bundles containing training and additional products such as the Passive Vulnerability Scanner) or through one of our resellers.

### Step 2: Obtain Nessus and an Activation Code

Once you've purchased Nessus, you will receive an account on the Tenable Support Portal and an activation code to be used in the installation process.

### Step 3: Installing Nessus

Once you've transferred the appropriate Nessus Debian package to your Kali Linux installation, run the following commands to install and start Nessus (it is assumed that your Kali Linux is configured with access to the Internet):

```
annu@kali:~/Downloads$ sudo apt install ./Nessus-8.12.1-debian6_amd64_1.deb
[sudo] password for annu:
Reading package lists... Done
Building dependency tree
Reading state information... Done
Note, selecting 'nessus' instead of './Nessus-8.12.1-debian6_amd64_1.deb'
nessus is already the newest version (8.12.1).
0 upgraded, 0 newly installed, 0 to remove and 1058 not upgraded.
annu@kali:~/Downloads$ /etc/init.d/nessusd start
```

## NESSUS

### Start Nessus

```
annu@kali:~/Downloads$ sudo -i
root@kali:~# /bin/systemctl start nessusd.service
root@kali:~# systemctl enable nessusd
root@kali:~# systemctl start nessusd
root@kali:~# systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor prese>
   Active: active (running) since Sun 2020-11-08 12:27:54 EST; 12min ago
 Main PID: 4672 (nessus-service)
    Tasks: 13 (limit: 4396)
   Memory: 113.8M
    CGroup: /system.slice/nessusd.service
            └─4672 /opt/nessus/sbin/nessus-service -q
              └─4673 nessusd -q

Nov 08 12:27:54 kali systemd[1]: Started The Nessus Vulnerability Scanner.
lines 1-11/11 (END)...skipping...
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/lib/systemd/system/nessusd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2020-11-08 12:27:54 EST; 12min ago
 Main PID: 4672 (nessus-service)
    Tasks: 13 (limit: 4396)
   Memory: 113.8M
    CGroup: /system.slice/nessusd.service
            └─4672 /opt/nessus/sbin/nessus-service -q
              └─4673 nessusd -q
```

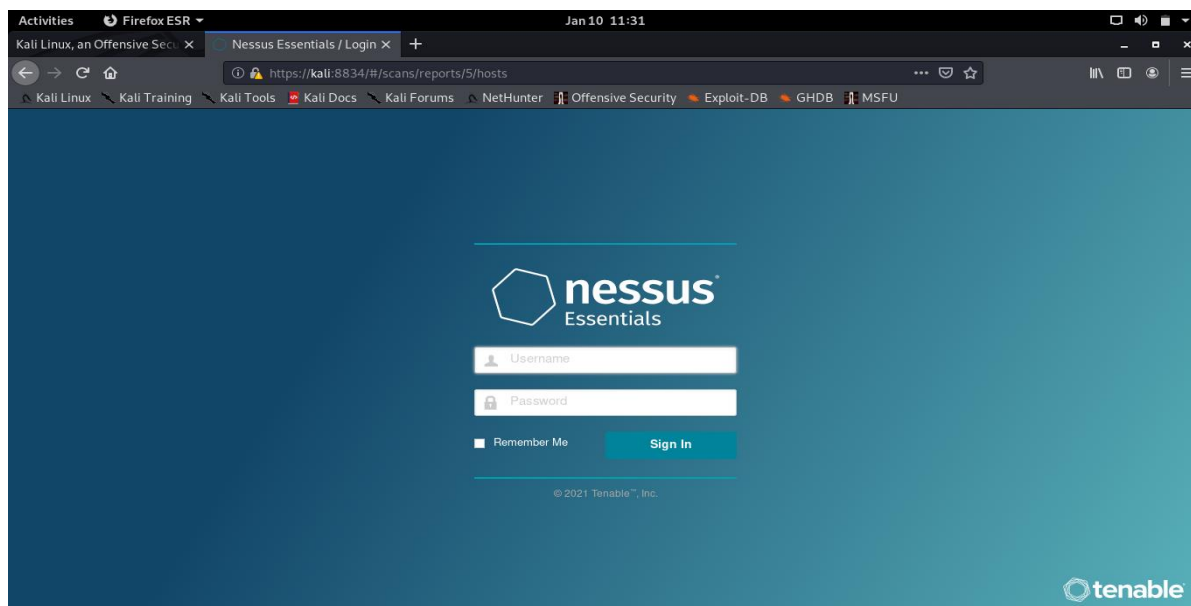
Installing Nessus on Kali Linux via the command line. The web interface can be accessed with your browser by making an HTTPS connection to TCP port 8834 (e.g. <https://localhost:8834/>). You can also access the Nessus Web Interface remotely by using the default IP address assigned to Kali Linux (e.g. <https://192.168.1.250:8834/>). Make certain that javascript is enabled in the browser you are using to manage the Nessus server.

### Step 4: Configure and use Nessus

To configure Nessus, follow the installation wizard. Create an administrator user account, activate with your activation code from the Tenable Support Portal and let Nessus fetch and process the plugins. This account is used to login to the Nessus.

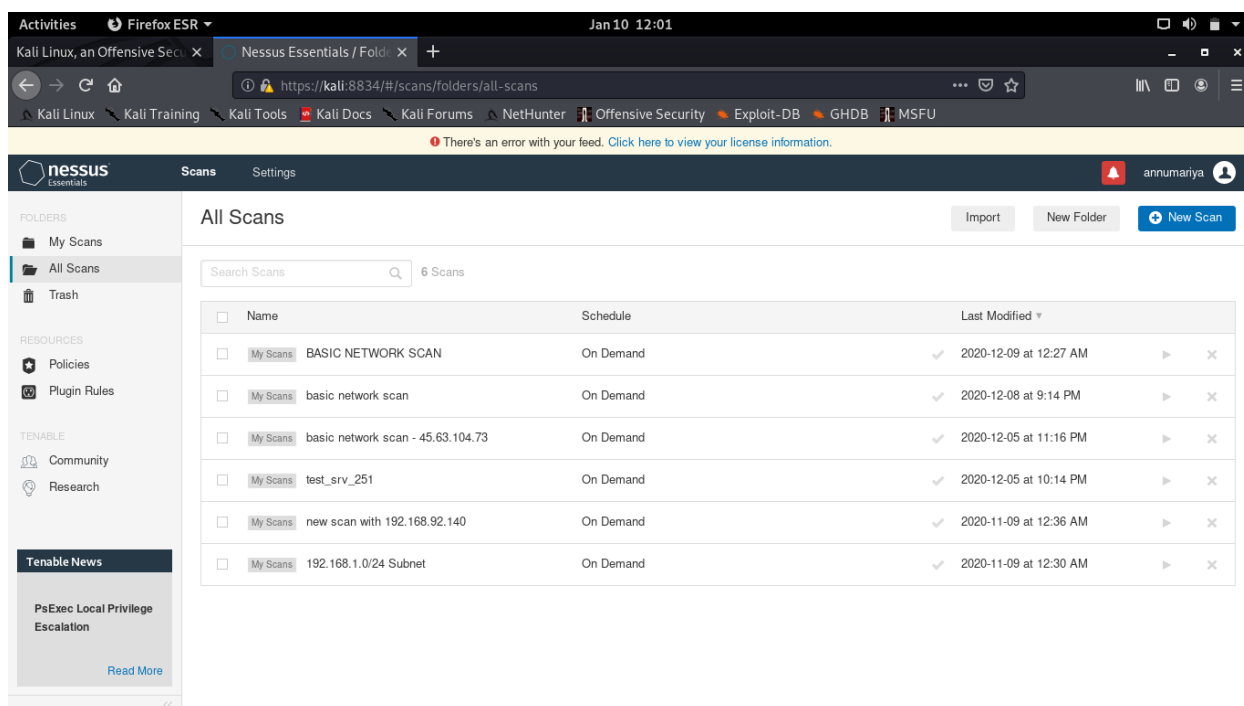
### 3. IMPLEMENTATION AND SCREENSHOTS

#### SIGN IN TO NESSUS



To sign in enter user name and password.

#### ALL SCAN



## MY SCAN

Activities Firefox ESR Jan 10 12:01

Kali Linux, an Offensive Security... Nessus Essentials / Folders / my-scans

https://kali:8834/#/scans/folders/my-scans

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

There's an error with your feed. [Click here to view your license information.](#)

nessus Essentials Scans Settings annumariya

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

TENABLE

- Community
- Research

Tenable News

Carbon Black Installer  
Multiple Vulnerabilities  
[Read More](#)

### My Scans

Import New Folder New Scan

Search Scans 6 Scans

<input type="checkbox"/>	Name	Schedule	Last Modified		
<input type="checkbox"/>	BASIC NETWORK SCAN	On Demand	✓ 2020-12-09 at 12:27 AM	▶	✕
<input type="checkbox"/>	basic network scan	On Demand	✓ 2020-12-08 at 9:14 PM	▶	✕
<input type="checkbox"/>	basic network scan - 45.63.104.73	On Demand	✓ 2020-12-05 at 11:16 PM	▶	✕
<input type="checkbox"/>	test_srv_251	On Demand	✓ 2020-12-05 at 10:14 PM	▶	✕
<input type="checkbox"/>	new scan with 192.168.92.140	On Demand	✓ 2020-11-09 at 12:36 AM	▶	✕
<input type="checkbox"/>	192.168.1.0/24 Subnet	On Demand	✓ 2020-11-09 at 12:30 AM	▶	✕

Take new scan - some scanning templates will appear from that take web application test.

## NESSUS

## SCAN TEMPLATE

Activities Firefox ESR Jan 10 12:00

Kali Linux, an Offensive Security... Nessus Essentials / Scan +

https://kali:8834/#/scans/reports/new 67%

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

There's an error with your feed. [Click here to view your license information.](#)

nessus essentials Scans Settings annumaraja

## Scan Templates

[Back to Scans](#)

Scanner

### DISCOVERY

- Host Discovery**  
A simple scan to discover live hosts and open ports.

### VULNERABILITIES

- Basic Network Scan**  
A full system scan suitable for any host.
- Advanced Scan**  
Configure a scan without using any recommendations.
- Advanced Dynamic Scan**  
Configure a dynamic plugin scan without recommendations.
- Malware Scan**  
Scan for malware on Windows and Unix systems.
- Mobile Device Scan**  
Assess mobile devices via Microsoft Exchange or an MDM.
- Web Application Tests**  
Scan for published and unknown web vulnerabilities.
- Credentialed Patch Audit**  
Authenticate to hosts and enumerate missing updates.
- Badlock Detection**  
Remote and local checks for CVE-2016-2118 and CVE-2016-4128.
- Bash Shellshock Detection**  
Remote and local checks for CVE-2014-7169 and CVE-2014-7169.
- UPOW Detection**  
Remote checks for CVE-2016-0800.
- Intel AMT Security Bypass**  
Remote and local checks for CVE-2017-5688.
- Shadow Brokers Scan**  
Scan for vulnerabilities disclosed in the Shadow Brokers leaks.
- Spectre and Meltdown**  
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.
- WannaCry Ransomware**  
Remote and local checks for MS17-010.
- Ripple2U Remote Scan**  
A remote scan to fingerprint hosts potentially running the Tack stack in the network.
- ZeroLogon Remote Scan**  
A remote scan to detect Microsoft Netlogon Elevation of Privilege (ZeroLogon).

### COMPLIANCE

- Audit Cloud Infrastructure**  
Audit the configuration of third-party cloud services.
- Internal PCI Network Scan**  
Perform an internal PCI DSS (11.2.1) vulnerability scan.
- MDM Config Audit**  
Audit the configuration of mobile device managers.
- Offline Config Audit**  
Audit the configuration of network devices.
- PCI Quarterly External Scan**  
Approved for quarterly external scanning as required by PCI.
- Policy Compliance Auditing**  
Audit system configurations against a known baseline.
- SCAP and OVAL Auditing**  
Audit systems using SCAP and OVAL definitions.

Tenable News

Secometa GateManager Multiple Vulnerabilities

[Read More](#)

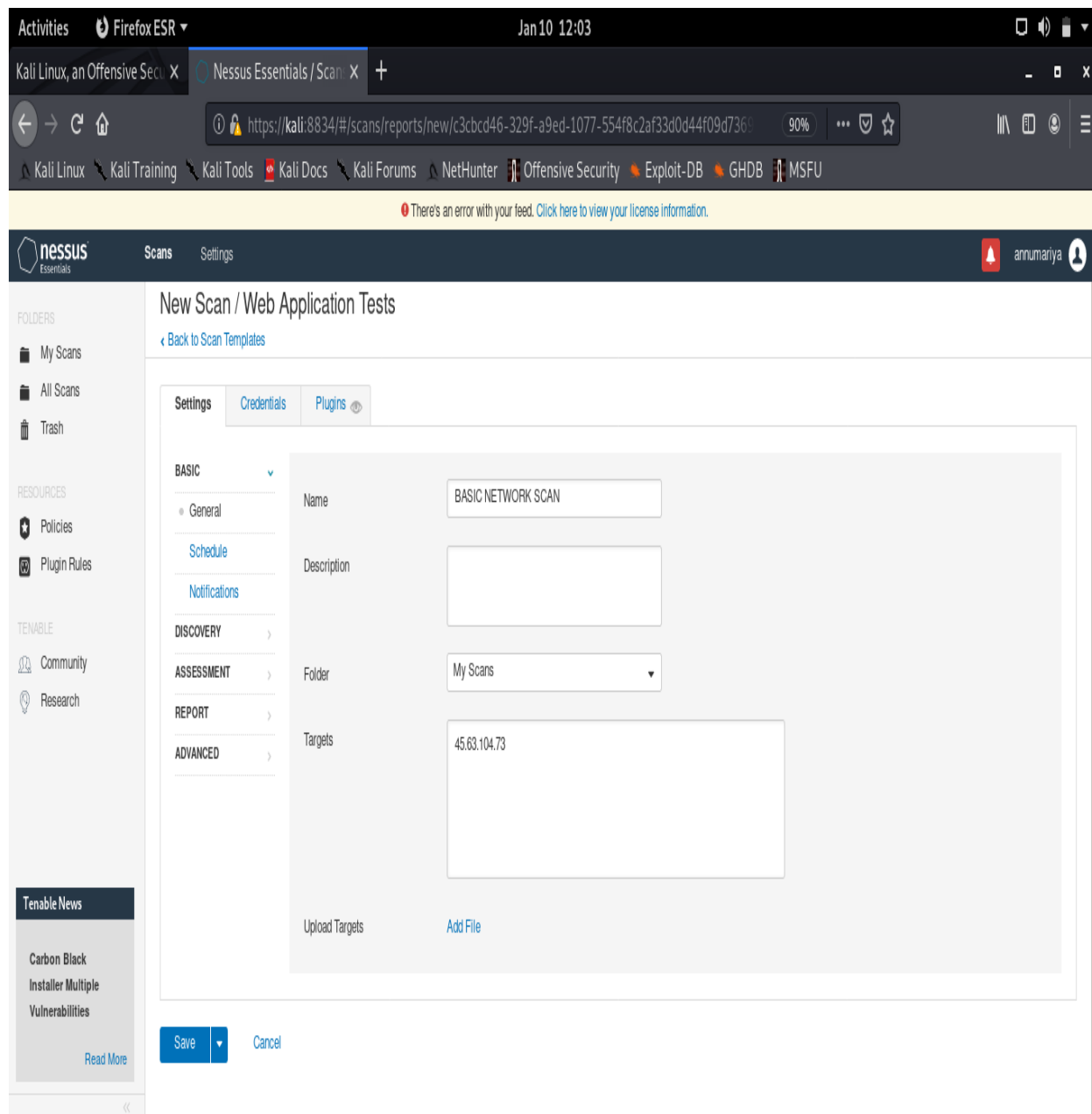
## NESSUS

## NEW SCAN

## BASIC NETWORK SCAN

TARGET: 45.63.104.73

Then enter name and target then save.



Activities

Firefox ESR

Jan 10 12:04

Kali Linux, an Offensive Security

Nessus Essentials / Folders

+

← → ↻ 🏠

🔒 <https://kali.8834/#/scans/reports/24/hosts> 90% 📄 📌 ⚙

🔍 Kali Linux 📖 Kali Training 🛠️ Kali Tools 🇸🇰 Kali Docs 🗣️ Kali Forums 🏠 NetHunter 🛡️ Offensive Security 🔥 Exploit-DB 🏠 GHDB 🏠 MSFU

There's an error with your feed. [Click here to view your license information.](#)

nessus

Essentials

Scans Settings

🔔

annumariya

👤

FOLDERS

📁 My Scans

📁 All Scans

🗑️ Trash

RESOURCES

🛡️ Policies

🔧 Plugin Rules

TENABLE

👤 Community

🔍 Research

Tenable News

Marvell

QConvergeConsole

GUI Multiple

Vulnerabil...

Read More

BASIC NETWORK SCAN

⏏

Configure

Audit Trail

Launch

Report

Export

⏏ Back to All Scans

Hosts 1

Vulnerabilities 13

Notes 1

History 1

Filter

Search Hosts

🔍

1 Host

☐

Host

Vulnerabilities ▼

☐

45.63.104.73

4

✕

Scan Details

Policy:

Web Application Tests

Status:

Completed

Scanner:

Local Scanner

Start:

2020-12-09 at 12:01 AM

End:

2020-12-09 at 12:27 AM

Elapsed:

26 minutes

Vulnerabilities

Critical

High

Medium

Low

Info

## NESSUS

Activities Jan 10 12:05

Kali Linux, an Offensive Security... +

<https://kali:8834/#/scans/reports/24/vulnerabilities> 67%

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

There's an error with your feed. [Click here to view your license information.](#)

nessus Essentials Scans Settings annumariya

### BASIC NETWORK SCAN

[Back to All Scans](#)

Configure Audit Trail Launch Report Export

Hosts Vulnerabilities 13 Notes History

Filter Search Vulnerabilities 13 Vulnerabilities

Sev	Name	Family	Count	
MAJOR	HTTP (Multiple Issues)	Web Servers	4	
MAJOR	PHP (Multiple Issues)	Web Servers	3	
MEDIUM	Browsable Web Directories	CGI abuses	1	
MEDIUM	Web Server info.php / phpinfo.php Detection	CGI abuses	1	
INFO	Apache HTTP Server (Multiple Issues)	Web Servers	2	
INFO	HTTP (Multiple Issues)	CGI abuses	2	
INFO	Nessus SYN scanner	Port scanners	2	
INFO	Nessus Scan Information	Settings	1	
INFO	Web Application Cookies Not Marked HttpOnly	Web Servers	1	
INFO	Web Application Cookies Not Marked Secure	Web Servers	1	
INFO	Web Application Sitemap	Web Servers	1	
INFO	Web mirroring	Web Servers	1	
INFO	Web Server Directory Enumeration	Web Servers	1	

**Scan Details**

Policy: Web Application Tests  
 Status: Completed  
 Scanner: Local Scanner  
 Start: 2020-12-09 at 12:01 AM  
 End: 2020-12-09 at 12:27 AM  
 Elapsed: 26 minutes

**Vulnerabilities**

Legend: Critical, High, Medium, Low, Info

**Tenable News**

Rockwell Automation  
 FactoryTalk Multiple  
 Vulnerabil...

[Read More](#)

After the operation is performed vulnerabilities will be displayed.



## **4. CONCLUSION**

Nessus is the world's most widely-deployed vulnerability assessment solution. Nessus quickly and accurately identifies vulnerabilities, configuration issues and malware in physical, virtual and cloud environments to help you prioritize what to fix first. Combine Nessus with Kali Linux to build a superior pen testing toolkit that provides deep insight into your network systems. Nessus holds a significant place among the penetration testing tool, which is branded susceptibility scanner and has been advanced by Tenable Network Security use it for free only if you use it for personal use amid a non-enterprise setting. However, it allows you to scan for numerous kinds of vulnerabilities. Nessus does not actively prevent attacks, it is only a tool that checks your computers to find vulnerabilities that hackers could exploit.

## 5. REFERENCE

<https://www.tenable.com/blog/installing-and-using-nessus-on-kali-linux>

<https://www.tenable.com/blog/getting-started-with-nessus-on-kali-linux>

[https://linuxhint.com/nessus\\_installation\\_kali\\_linux/](https://linuxhint.com/nessus_installation_kali_linux/)

<https://youtu.be/Fu7MiHcyd44>