Leonard M. Estos
Cybersecurity Researcher & Technical Author
Edmonton, Alberta, Canada

Project Name: Scanning Vulnerabilities INSTANTLY with Nessus!

What is Nessus?
Nessus is a widely used vulnerability scanning tool developed by Tenable. It is designed to identify security **vulnerabilities in devices, applications, operating systems, cloud services, and other network resources**. Nessus performs remote security scans and alerts users about potential weaknesses that attackers could exploit. It achieves this by running thousands of checks on a target system to detect outdated software, misconfigurations, malware, and other vulnerabilities. Initially launched as an open-source project in 1998, Nessus transitioned to a commercial product in 2005.vOpen Nessus Essential in Edge

- Discovery Scan
- Basic Network Scan
- Malware Scan
- Compliance Scan
- Vulnerability Report – PDF

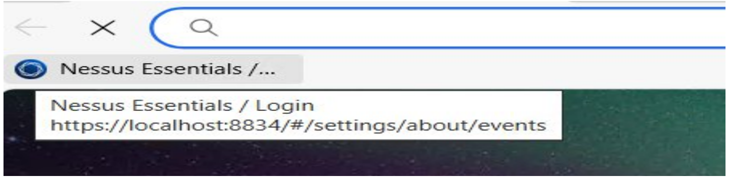
Nessus Installation:

1. **Download the Nessus installer**
Navigate to the Tenable Nessus download page.
Find the Nessus Essentials or Pro version and select the correct package for your operating system (Windows, macOS, Kali Linux, etc.).
If prompted, provide your contact information to receive an activation code via email.

2. **Run the installer**
Locate the downloaded file and run it. This will start the installation wizard.
Follow the wizard's prompts to install the software.

3. **Activate Nessus**
After installation, the web interface should automatically open. If not, manually navigate to **https://localhost:8834** in your web browser.
Accept any security warnings to proceed to the activation page.
Enter the activation code you received from Tenable.

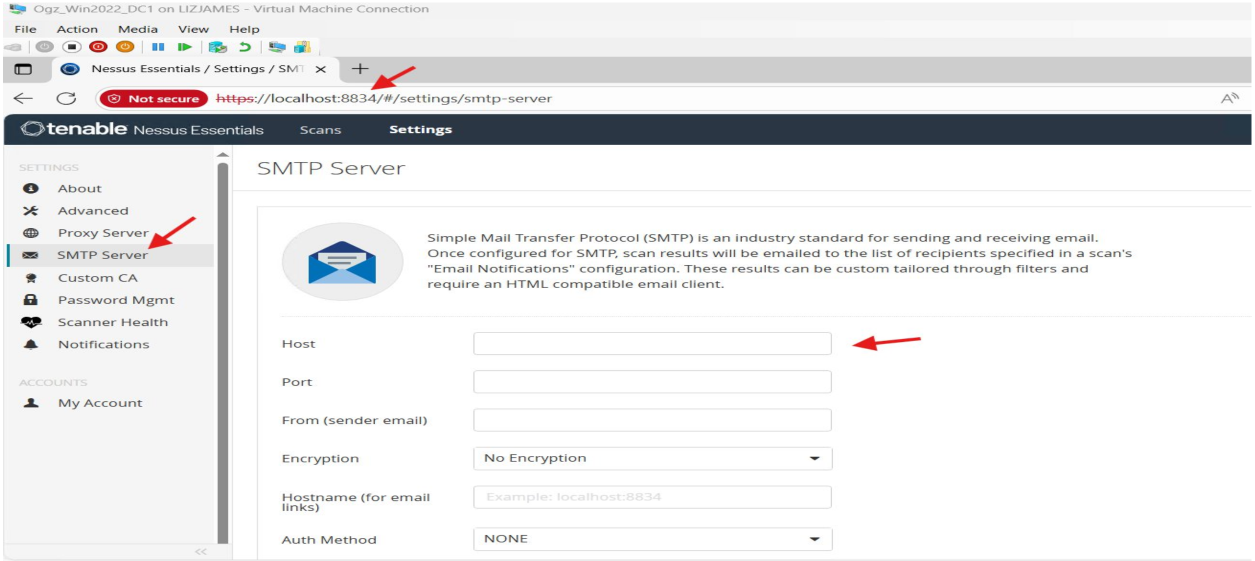
4. **Complete the setup and start scanning**
The Nessus initialization process will begin, which involves downloading and installing necessary plugins. This may take some time, depending on your internet speed.
Once the plugins are fully installed, you can create your user account and begin configuring your first scan.



Nessus Essentials / Login
https://localhost:8834/#/settings/about/events

Nessus Settings: Nessus Administration Settings Overview. These settings are crucial for the scanner's operation and integration:

1. Accessing Settings: In the Tenable Nessus web interface, you generally navigate to the Settings option in the top or side navigation bar.
2. SMTP Server Configuration:
   - This setting allows you to configure a Simple Mail Transfer Protocol (SMTP) server.
   - Once configured, Nessus can send email notifications (e.g., scan results or alerts) to specified recipients.
   - It's usually found under a dedicated SMTP Server link within the Settings area.
3. Scanner Health:
   - The Scanner Health page provides vital information about the performance of your Nessus scanner.
   - It helps in troubleshooting by monitoring real-time data like CPU load, memory usage, disk space, and network activity.


Ogz_Win2022_DC1 on LIZJAMES - Virtual Machine Connection
File
Action
Media
View
Help
Nessus Essentials / Settings / SMT
Not secure
https://localhost:8834/#/settings/smtp-server
tenable Nessus Essentials
Scans
Settings
SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
Password Mgmt
Scanner Health
Notifications
ACCOUNTS
My Account

SMTP Server

Simple Mail Transfer Protocol (SMTP) is an industry standard for sending and receiving email. Once configured for SMTP, scan results will be emailed to the list of recipients specified in a scan's "Email Notifications" configuration. These results can be custom tailored through filters and require an HTML compatible email client.

Host

Port

From (sender email)

Encryption: No Encryption

Hostname (for email links): Example: localhost:8834

Auth Method: NONE

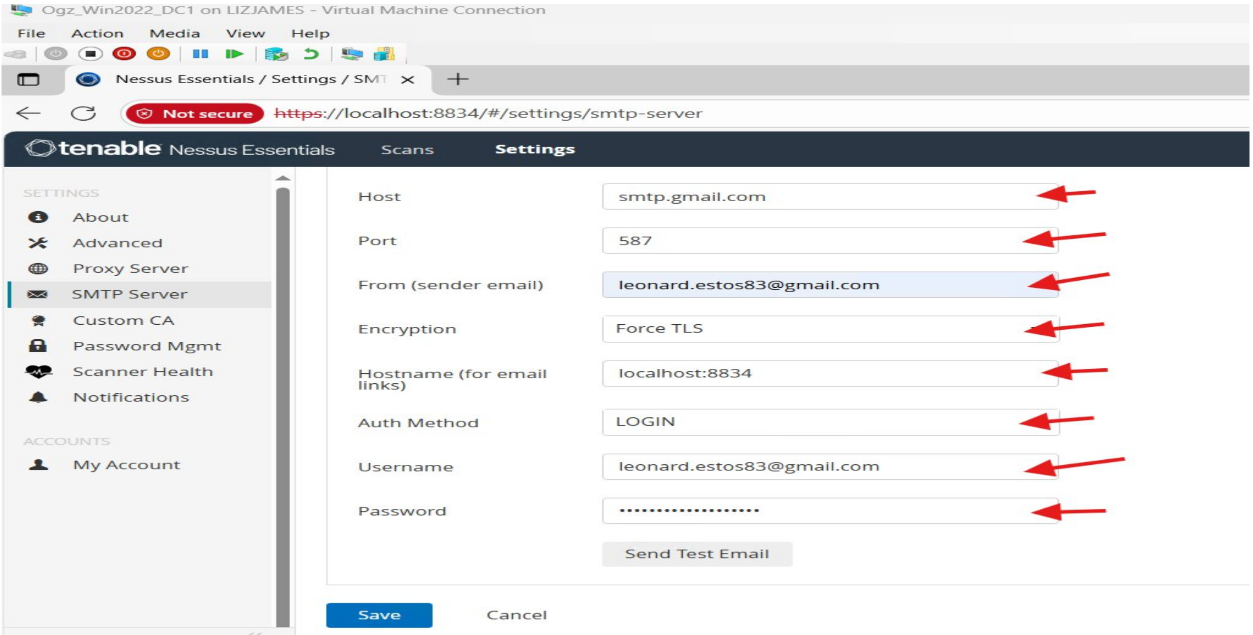
Enable SMTP Settings:

Due to Google's security policies, external applications like Nessus must use a dedicated, 16-character **App Password** for authentication, not your regular account password. This is only possible if you have **2-Step Verification (2SV)** enabled on your Google account.

1. **Enable 2-Step Verification:** If you haven't already, go to your **Google Account Security** settings and enable 2-Step Verification.

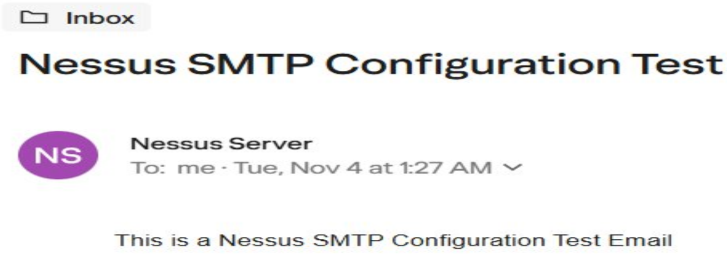
2. **Access App Passwords:** In the same **Security** section of your Google Account, **find/search** and click on **App passwords** (under "Signing in to Google"). You may need to sign in again.
3. **Generate Password:**
   - For the **Select app** dropdown, choose **Mail**.
   - For the **Select device** dropdown, choose **Other (Custom name)** and type a name like Nessus or Nessus SMTP.
   - Click the **Generate** button.

4. **Copy the Password:** Google will display a **16-character App Password**. **Copy this password immediately**, as it will disappear once you close the window, and you'll need to generate a new one if you lose it.



Host: smtp.gmail.com
Port: 587
From (sender email): leonard.estos83@gmail.com
Encryption: Force TLS
Hostname (for email links): localhost:8834
Auth Method: LOGIN
Username: leonard.estos83@gmail.com
Password: ••••••••••••••••••••

Result of test mail:



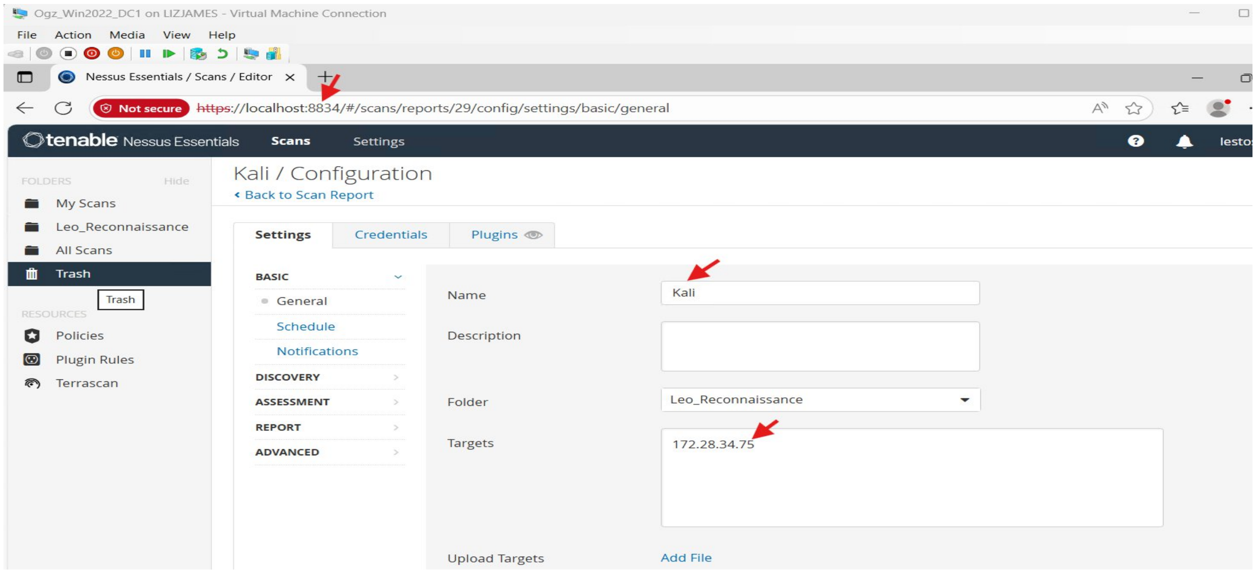
Nessus SMTP Configuration Test

Nessus Server
To: me · Tue, Nov 4 at 1:27 AM

This is a Nessus SMTP Configuration Test Email

First Scan: Host Discovery

1. **Initiate a new scan**: From the dashboard, click on the "New Scan" button.
2. **Select scan type**: Choose the appropriate scan category from the options provided. The available types are Discover, Vulnerabilities, and Compliance.
3. **Configure scan parameters**:
    - **Name**: Enter a descriptive name for the scan.
    - **Folder**: Select or create a folder to categorize the scan.
    - **Targets**: Enter the specific IP address of the endpoint you wish to scan.
4. **Execute the scan**: After filling in the required fields, initiate the scan.



https://localhost:8834/#/scans/reports/29/config/settings/basic/general

Kali / Configuration

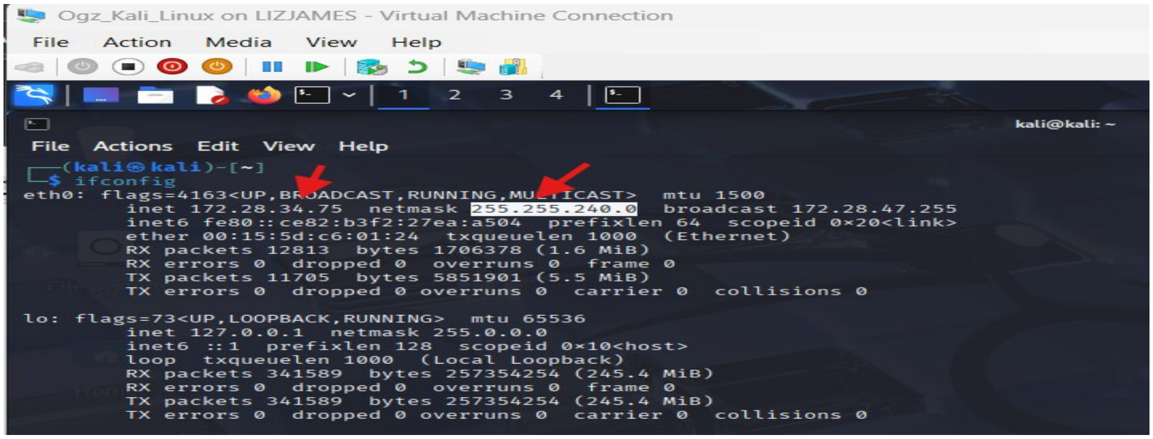
Name: Kali

Description:

Folder: Leo_Reconnaissance

Targets: 172.28.34.75

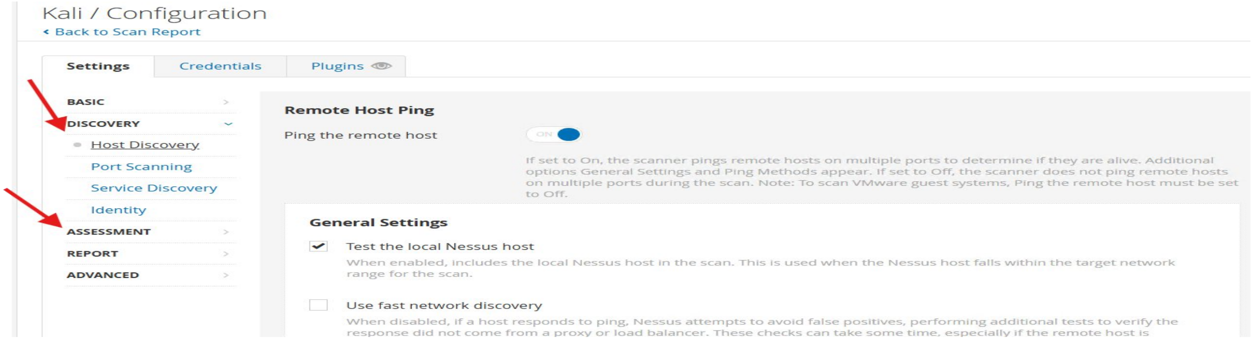
5. In the targets section, use **172.28.32.0/20** as well. We used the dicer /20 because the subnet mask is **255.255.240.0**. **Host Discovery Scan** will search for the IP address from **172.28.32.1 - 172.28.47.254** or discover any endpoint devices on that range of IP’s.


Ogz_Kali_Linux on LIZJAMES - Virtual Machine Connection
File Action Media View Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.28.34.75  netmask 255.255.240.0  broadcast 172.28.47.255
        inet6 fe80::ce82:b3f2:27ea:a504  prefixlen 64  scopeid 0x20<link>
        ether 00:15:5d:c6:01:24  txqueuelen 1000  (Ethernet)
        RX packets 12813  bytes 1706378 (1.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11705  bytes 5851901 (5.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 341589  bytes 257354254 (245.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 341589  bytes 257354254 (245.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

6. The **Custom Scan feature** allows you to configure specific settings for **Discovery, Assessment, Reporting, and Advanced functions**.



Remote Host Ping

Ping the remote host

If set to On, the scanner pings remote hosts on multiple ports to determine if they are alive. Additional options General Settings and Ping Methods appear. If set to Off, the scanner does not ping remote hosts on multiple ports during the scan. Note: To scan VMware guest systems, Ping the remote host must be set to Off.

General Settings

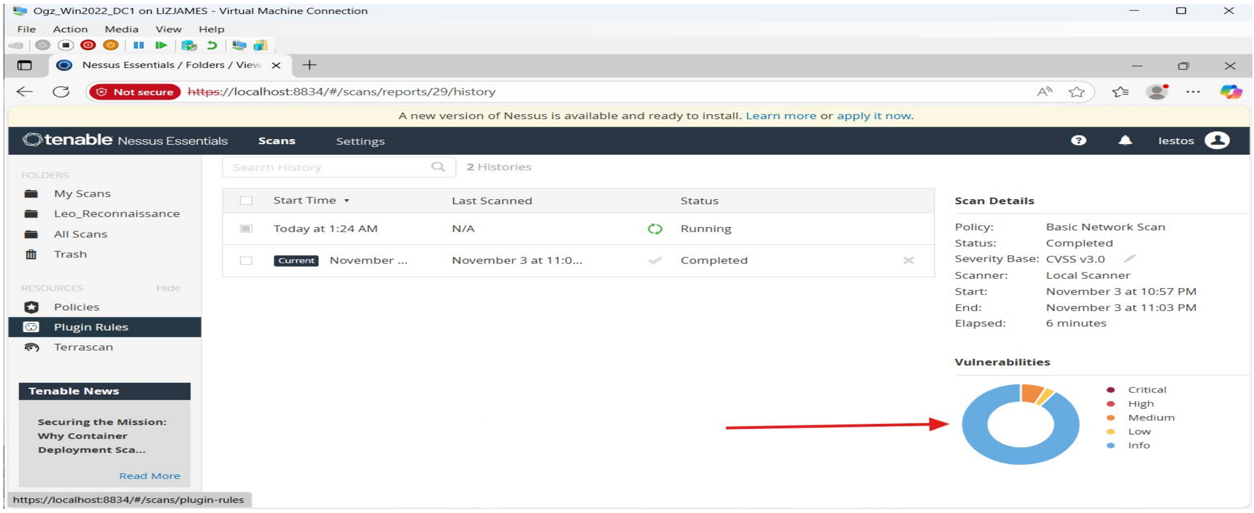
☑ Test the local Nessus host

When enabled, includes the local Nessus host in the scan. This is used when the Nessus host falls within the target network range for the scan.

☐ Use fast network discovery

When disabled, if a host responds to ping, Nessus attempts to avoid false positives, performing additional tests to verify the response did not come from a proxy or load balancer. These checks can take some time, especially if the remote host is

7. **Click Scan** > Scan details/result where we can see the results of **Vulnerabilities including the assessments**.


Ogz_Win2022_DC1 on LIZJAMES - Virtual Machine Connection
File
Action
Media
View
Help
Nessus Essentials / Folders / View
Not secure
https://localhost:8834/#/scans/reports/29/history
tenable Nessus Essentials
Scans
Settings
lestos
FOLDERS
My Scans
Leo_Reconnaissance
All Scans
Trash
RESOURCES
Hide
Policies
Plugin Rules
Terrascan
Tenable News
Securing the Mission: Why Container Deployment Sca...
Read More
Search History
Vulnerabilities
Critical
High
Medium
Low
Info
https://localhost:8834/#/scans/plugin-rules

A new version of Nessus is available and ready to install. Learn more or apply it now.

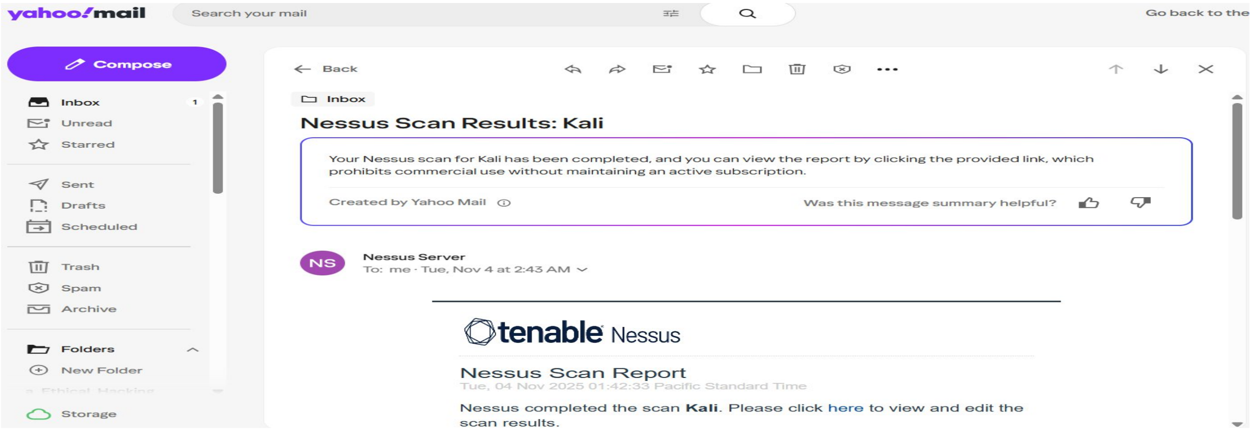
2 Histories

	Start Time ▾	Last Scanned		Status	
☐	Today at 1:24 AM	N/A		Running	
☐	Current November ...	November 3 at 11:0...	✓	Completed	×

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	November 3 at 10:57 PM
End:	November 3 at 11:03 PM
Elapsed:	6 minutes

8. The following section provides a sample of the email alert and report generated upon completion of all scans.



Nessus Scan Results: Kali

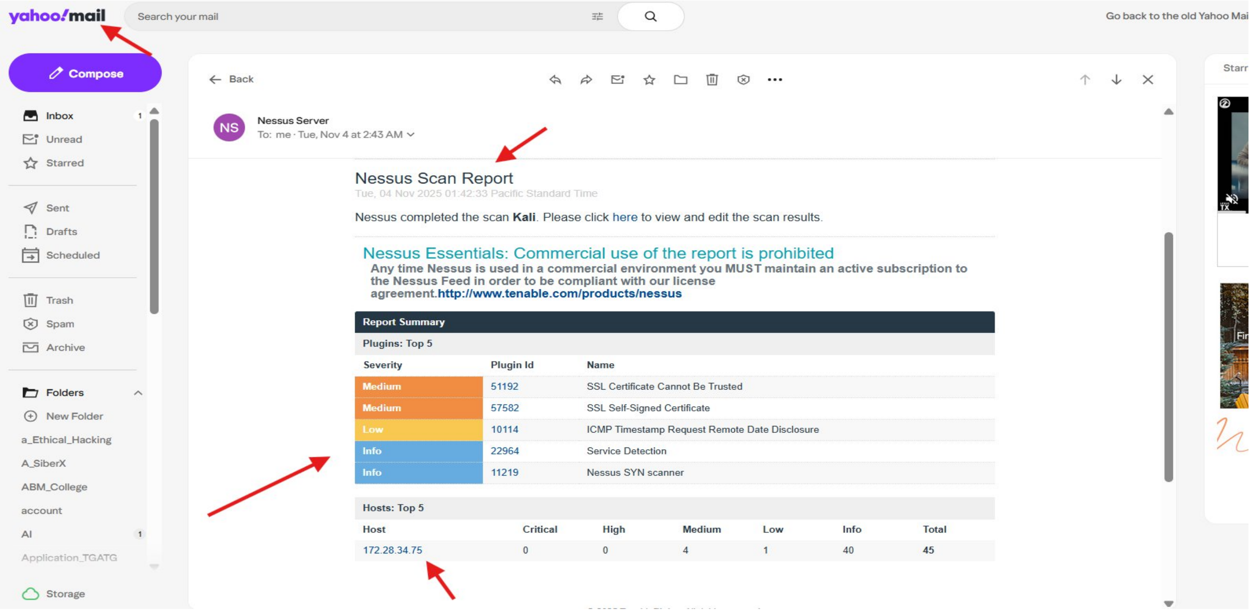
Your Nessus scan for Kali has been completed, and you can view the report by clicking the provided link, which prohibits commercial use without maintaining an active subscription.

Created by Yahoo Mail ⓘ Was this message summary helpful?

Nessus Server
To: me · Tue, Nov 4 at 2:43 AM

Nessus Scan Report
Tue, 04 Nov 2025 01:42:33 Pacific Standard Time

Nessus completed the scan **Kali**. Please click here to view and edit the scan results.



Nessus Server
To: me · Tue, Nov 4 at 2:43 AM

Nessus Scan Report
Tue, 04 Nov 2025 01:42:33 Pacific Standard Time

Nessus completed the scan **Kali**. Please click here to view and edit the scan results.

Nessus Essentials: Commercial use of the report is prohibited
Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the Nessus Feed in order to be compliant with our license agreement.http://www.tenable.com/products/nessus

Report Summary

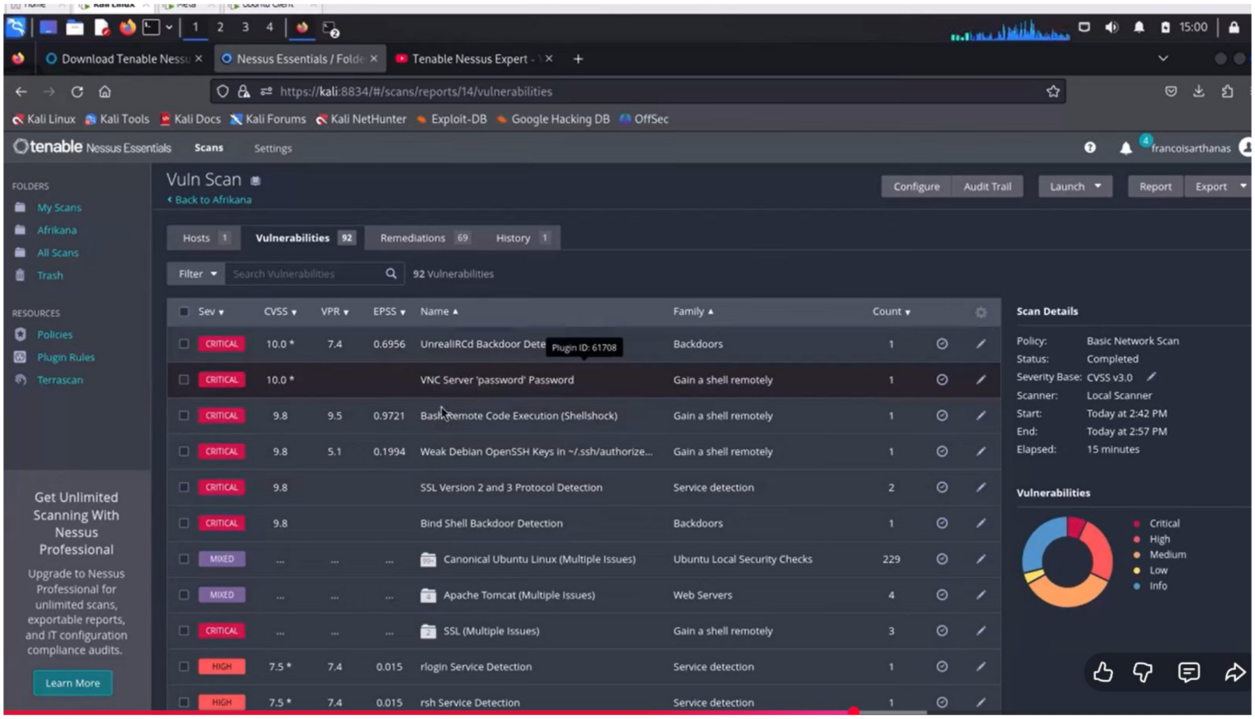
Plugins: Top 5

Severity	Plugin Id	Name
Medium	51192	SSL Certificate Cannot Be Trusted
Medium	57582	SSL Self-Signed Certificate
Low	10114	ICMP Timestamp Request Remote Date Disclosure
Info	22964	Service Detection
Info	11219	Nessus SYN scanner

Hosts: Top 5

Host	Critical	High	Medium	Low	Info	Total
172.28.34.75	0	0	4	1	40	45

9. **Network Scanning Results and Remediation**. The data below summarizes the findings from the Network Scan and provides actionable steps for **Remediation and Solution.**



https://kali:8834/#/scans/reports/14/vulnerabilities

Vuln Scan
‹ Back to Afrikana

Hosts 1 | Vulnerabilities 92 | Remediations 69 | History 1

92 Vulnerabilities

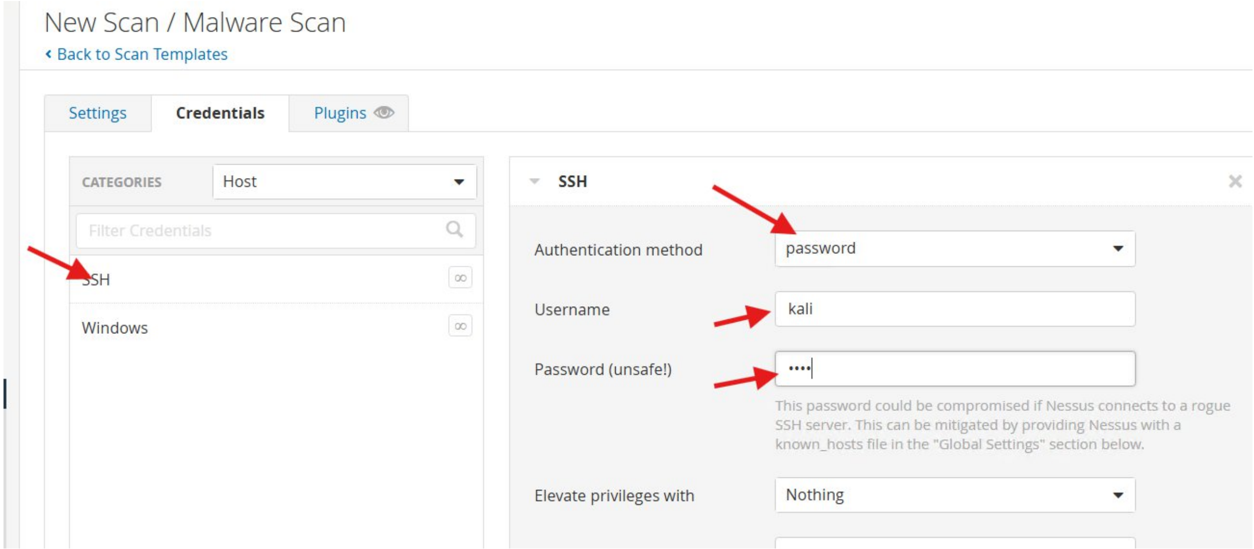
Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6956	UnrealIRCd Backdoor Dete Plugin ID: 61708	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	9.5	0.9721	Bash Remote Code Execution (Shellshock)	Gain a shell remotely	1
CRITICAL	9.8	5.1	0.1994	Weak Debian OpenSSH Keys in ~/.ssh/authorize...	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	Canonical Ubuntu Linux (Multiple Issues)	Ubuntu Local Security Checks	229
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	7.4	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5 *	7.4	0.015	rsh Service Detection	Service detection	1

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 2:42 PM
End: Today at 2:57 PM
Elapsed: 15 minutes

Vulnerabilities

10. **Malware Scanning Vulnerabilities**. The data below summarizes the findings from the Malware Scan and provides actionable steps for **Remediation and Solution.** On this we need to provide the **Authentication method.** Now, click **Credentials** and follow below.



New Scan / Malware Scan

‹ Back to Scan Templates

CATEGORIES: Host

SSH

Authentication method: password

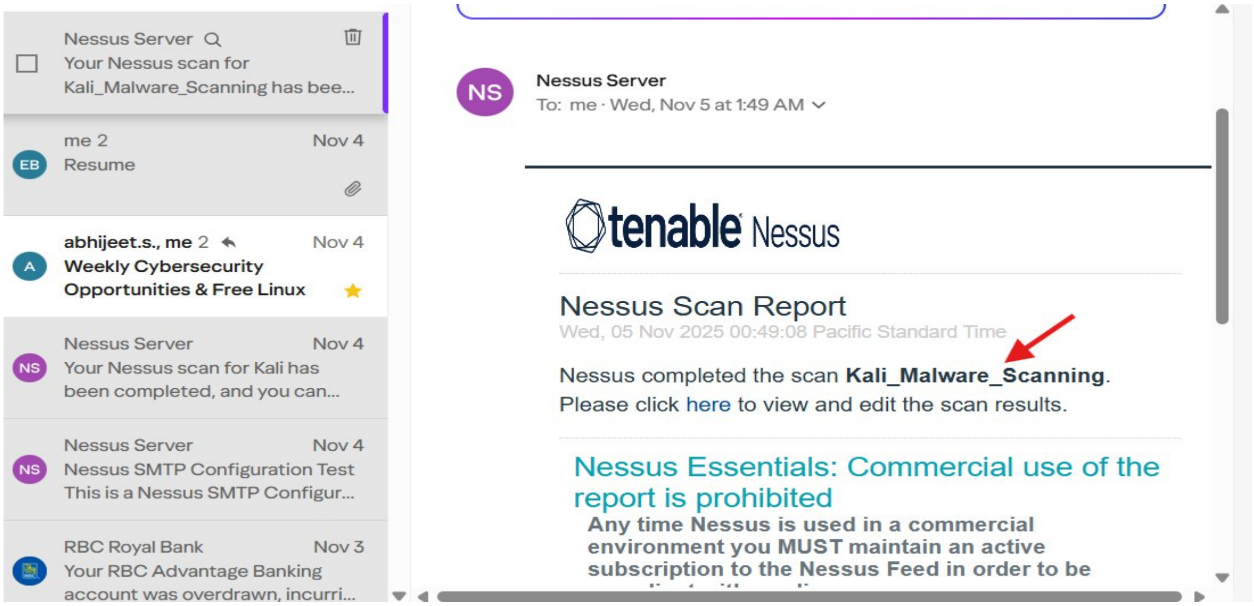
Username: kali

Password (unsafe!): ••••

This password could be compromised if Nessus connects to a rogue SSH server. This can be mitigated by providing Nessus with a known_hosts file in the "Global Settings" section below.

Elevate privileges with: Nothing

11. The following section provides a sample of the email alert and report generated upon completion of all scans.



Nessus Server
Your Nessus scan for Kali_Malware_Scanning has bee...

me 2 — Nov 4
Resume

abhijeet.s., me 2 — Nov 4
Weekly Cybersecurity Opportunities & Free Linux

Nessus Server — Nov 4
Your Nessus scan for Kali has been completed, and you can...

Nessus Server — Nov 4
Nessus SMTP Configuration Test
This is a Nessus SMTP Configur...

RBC Royal Bank — Nov 3
Your RBC Advantage Banking account was overdrawn, incurri...

Nessus Server
To: me · Wed, Nov 5 at 1:49 AM

tenable Nessus

Nessus Scan Report
Wed, 05 Nov 2025 00:49:08 Pacific Standard Time

Nessus completed the scan **Kali_Malware_Scanning**.
Please click here to view and edit the scan results.

Nessus Essentials: Commercial use of the report is prohibited

Any time Nessus is used in a commercial environment you MUST maintain an active subscription to the Nessus Feed in order to be

” When you train Smarter, you defend Stronger”
Leonard Estos