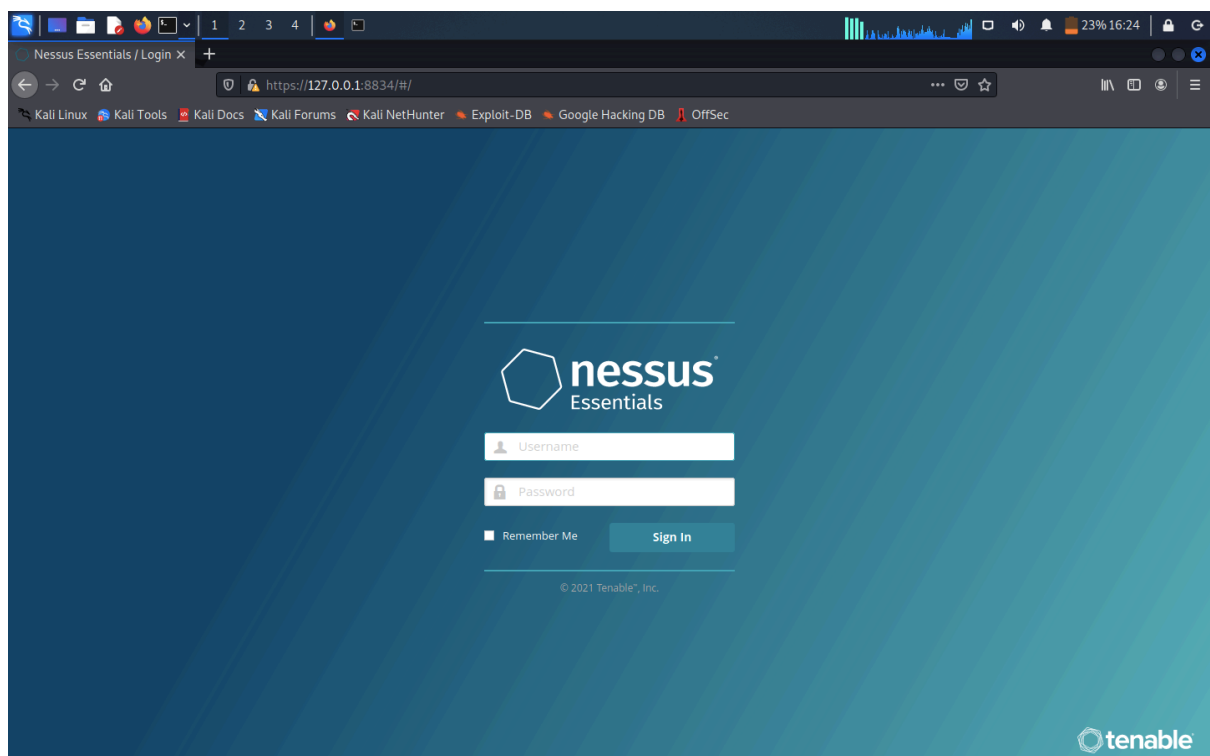


# Nessus Essentials

In this lab, we will cover vulnerability scanning using Nessus Essentials. We will go through some of the main steps of vulnerability management lifecycle. We will use Nessus Essentials to scan local VMs(Windows 10 pro and Metasploitable) hosted on VMware Fusion, to discover vulnerabilities and their remedies. It categorizes the vulnerabilities based on the severity. For example, if the scanner determines the vulnerability as Critical, it requires an immediate action.

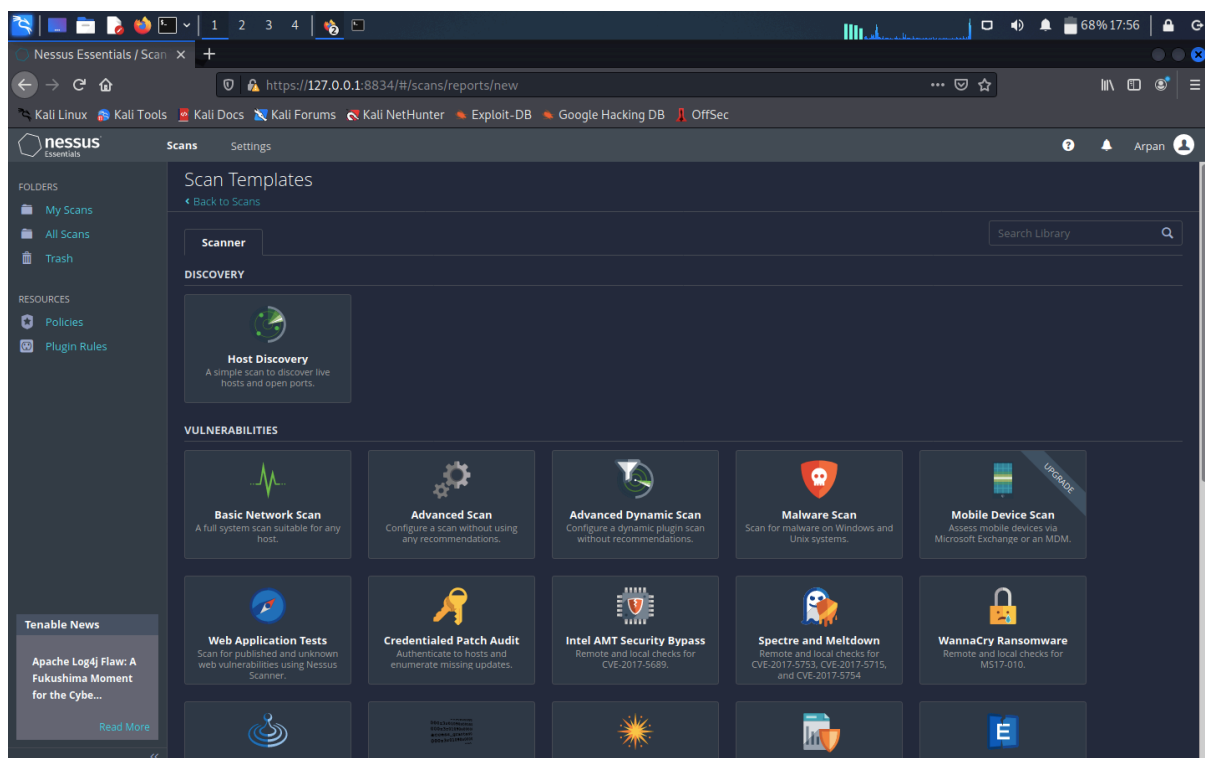
## Installing the VM's -

We will be installing Kali linux, Windows 10 and Metasploitable VMs on VMware Fusion. We will install and configure Nessus Essentials in kali and run scans on Windows 10 and Metasploitable VMs and compare the results. Windows 10 VM is up to date so it is likely to show less or no vulnerabilities whereas Metasploitable is intentionally made vulnerable hence, it can show a lot of vulnerabilities.



## Installing Nessus Essentials -

Visit the tenable website, get the activation key by creating an account and download the suitable debian file for kali. Open kali terminal and use the command `dpkg -i` followed by the debian package to install Nessus essentials. Use command `“sudo systemctl start nessusd.service”` to start Nessus. We can view the status using `“sudo systemctl status nessusd.service”`. Access the web interface by navigating to the local host on port 8834 (save the url for future reference), click on advanced and accept the risk. Fill in the credentials and the activation key from the mail. It will take some time to finish initialising. Finally, we will be able to see the Nessus interface and the templates. Provide the IP addresses of the target machines and begin scanning.



## Running Scans on VMs -

First we will run a basic network scan on Windows 10 VM. It will list all the vulnerabilities that exist.

The screenshot shows the Nessus Essentials interface. The main panel displays a scan report for 'Windows 10'. The 'Vulnerabilities' tab is active, showing a list of 17 vulnerabilities. The first vulnerability is 'SMB Signing not required' with a severity of 'MEDIUM'. The right sidebar shows 'Scan Details' and a 'Vulnerabilities' pie chart.

Sev	Score	Name	Family	Count
MEDIUM	5.3	SMB Signing not required	Misc.	1
INFO	...	SMB (Multiple Issues)	Windows	6
INFO		DCE Services Enumeration	Windows	9
INFO		Nessus SYN scanner	Port scanners	3
INFO		Common Platform Enumeration (CPE)	General	1
INFO		Device Type	General	1
INFO		Ethernet Card Manufacturer Detection	Misc.	1
INFO		Ethernet MAC Addresses	General	1
INFO		ICMP Timestamp Request Remote Da...	General	1
INFO		Link-Local Multicast Name Resolution...	Service detection	1
INFO		Nessus Scan Information	Settings	1

**Scan Details**

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 5:59 PM
- End: Today at 6:02 PM
- Elapsed: 3 minutes

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info

The scan lists the vulnerabilities and clicking on them describes the details of the vulnerabilities. For example - the screenshots below mentions the trace route information and target credential status by authentication protocol. This further helps in remediation of the vulnerabilities.

The screenshot shows the Nessus Essentials interface with the details of a specific vulnerability, 'Traceroute Information' (Plugin #10287). The 'Description' section explains that it makes a traceroute to the remote host. The 'Output' section shows the results of a tracert command. The 'Plugin Details' section on the right provides metadata about the plugin.

**Traceroute Information**

**Description**  
Makes a traceroute to the remote host.

**Output**

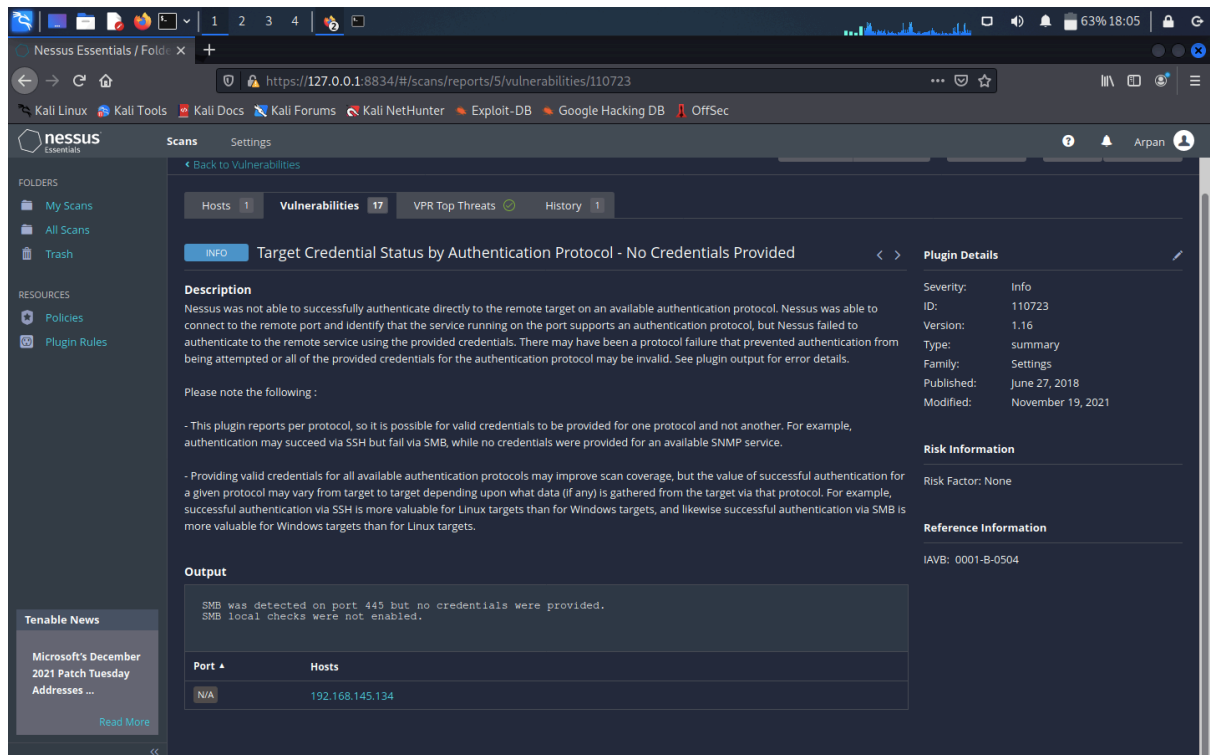
```
For your information, here is the traceroute from 192.168.145.135 to 192.168.145.134 :
192.168.145.135
192.168.145.134
Hop Count: 1
```

**Plugin Details**

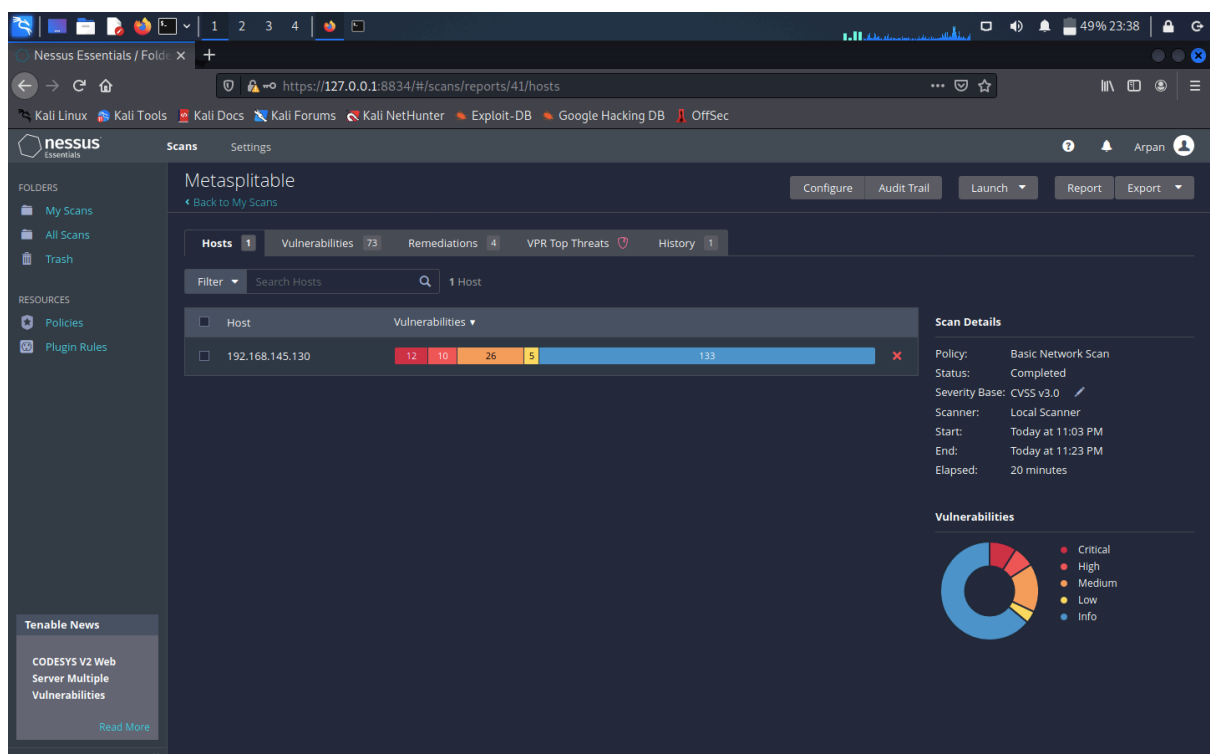
- Severity: Info
- ID: 10287
- Version: 1.67
- Type: remote
- Family: General
- Published: November 27, 1999
- Modified: August 20, 2020

**Risk Information**

- Risk Factor: None



Now we will run scan on Metasploitable VM. We can see all the vulnerabilities and the severity levels. Looking at the report, we can find out how many critical vulnerabilities are present and how to remediate them. Usually the critical vulnerabilities are the ones which require immediate action.



Nessus Essentials / Folder: X +

https://127.0.0.1:8834/#/scans/reports/41/vulnerabilities

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

nessus Essentials Scans Settings ? Arpan

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

Tenable News

CVE-2021-44228, CVE-2021-45046, CVE-2021-4104: Fre...  
[Read More](#)

Hosts 1 Vulnerabilities 73 Remediations 4 VPR Top Threats History 1

Filter Search Vulnerabilities 73 Vulnerabilities

Sev	Score	Name	Family	Count	
CRITICAL	10.0 *	NFS Exported Share Information Discl...	RPC	1	
CRITICAL	10.0 *	rexecd Service Detection	Service detection	1	
CRITICAL	10.0	Unix Operating System Unsupported ...	General	1	
CRITICAL	10.0 *	UnrealIRCd Backdoor Detection	Backdoors	1	
CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1	
CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1	
MIXED	...	DNS (Multiple Issues)	DNS	6	
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3	
MIXED	...	Apache Tomcat (Multiple Issues)	Web Servers	3	
MIXED	...	Web Server (Multiple Issues)	Web Servers	3	
HIGH	7.5	NFS Shares World Readable	RPC	1	
HIGH	7.5 *	rlogin Service Detection	Service detection	1	

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 11:03 PM  
End: Today at 11:23 PM  
Elapsed: 20 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).

Nessus Essentials / Folder: X +

https://127.0.0.1:8834/#/scans/reports/41/remediations

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

nessus Essentials Scans Settings ? Arpan

FOLDERS

- My Scans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

Tenable News

Log4Shell: 5 Steps The OT Community Should Take Ri...  
[Read More](#)

Metaspiltable

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 73 Remediations 4 VPR Top Threats History 1

Search Actions 4 Actions

Action	Vulns	Hosts
ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS: Upgrade to BIND 9.11.22, 9.16.6, 9.17.4 or later.	3	1
Apache Tomcat AJP Connector Request Injection (Ghostcat): Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.	2	1
Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.	1	1
UnrealIRCd Backdoor Detection: Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.	0	1

Scan Details

Policy: Basic Network Scan  
Status: Completed  
Severity Base: CVSS v3.0  
Scanner: Local Scanner  
Start: Today at 11:03 PM  
End: Today at 11:23 PM  
Elapsed: 20 minutes

We can compare the scans between these VMs and figure out ways to keep our machines secure. Running out of date softwares can result in the compromise of our machine whereas keeping it updated is usually the best way to remediate the vulnerabilities and make the machine more secure.