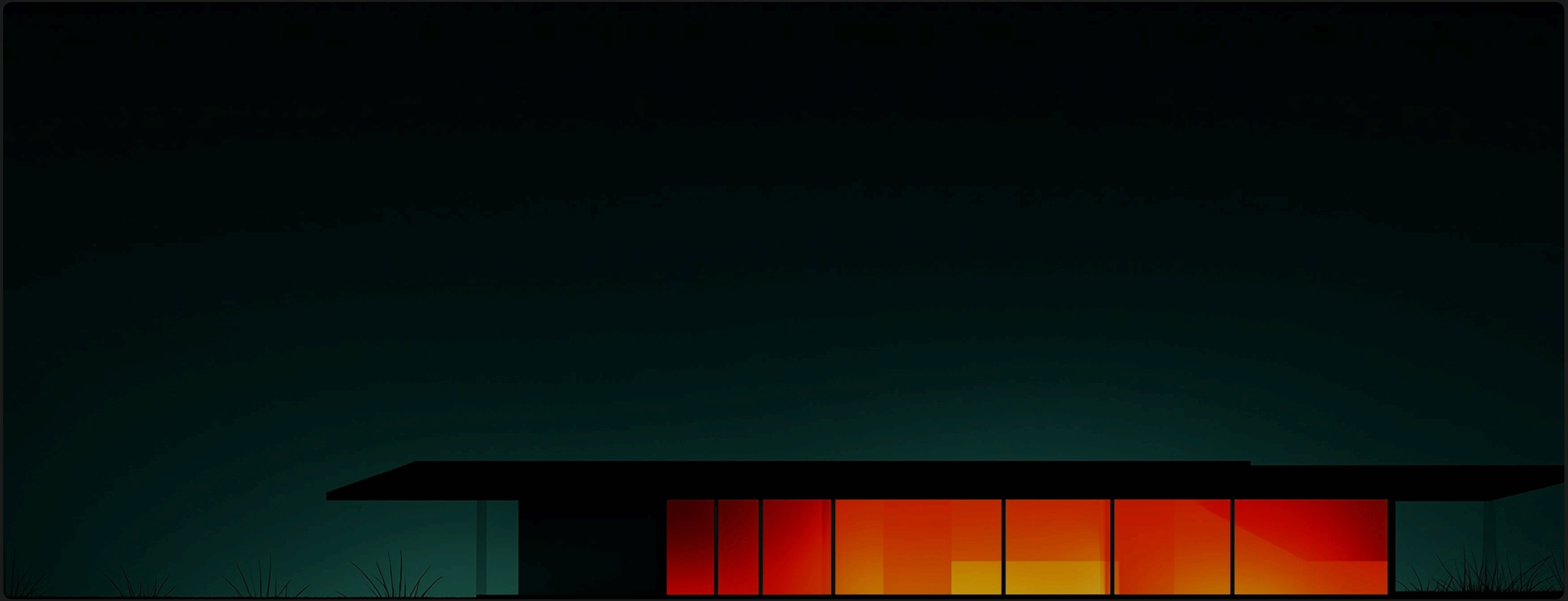
Vulnerability scan comparison using Nessus

Firewall Impact Study

Jash Vaidya



Vulnerability scan comparison using Nessus

This project was completed under the guidance and mentorship of Professor Dimple Chauhan.
I sincerely appreciate her support and valuable guidance throughout this work.

Author	Professor	Scope
Jash Vaidya	Dimple Chauhan	Kali local scan against Windows VM IP 10.0.2.15

Legal & Scope

Important legal and scope note.

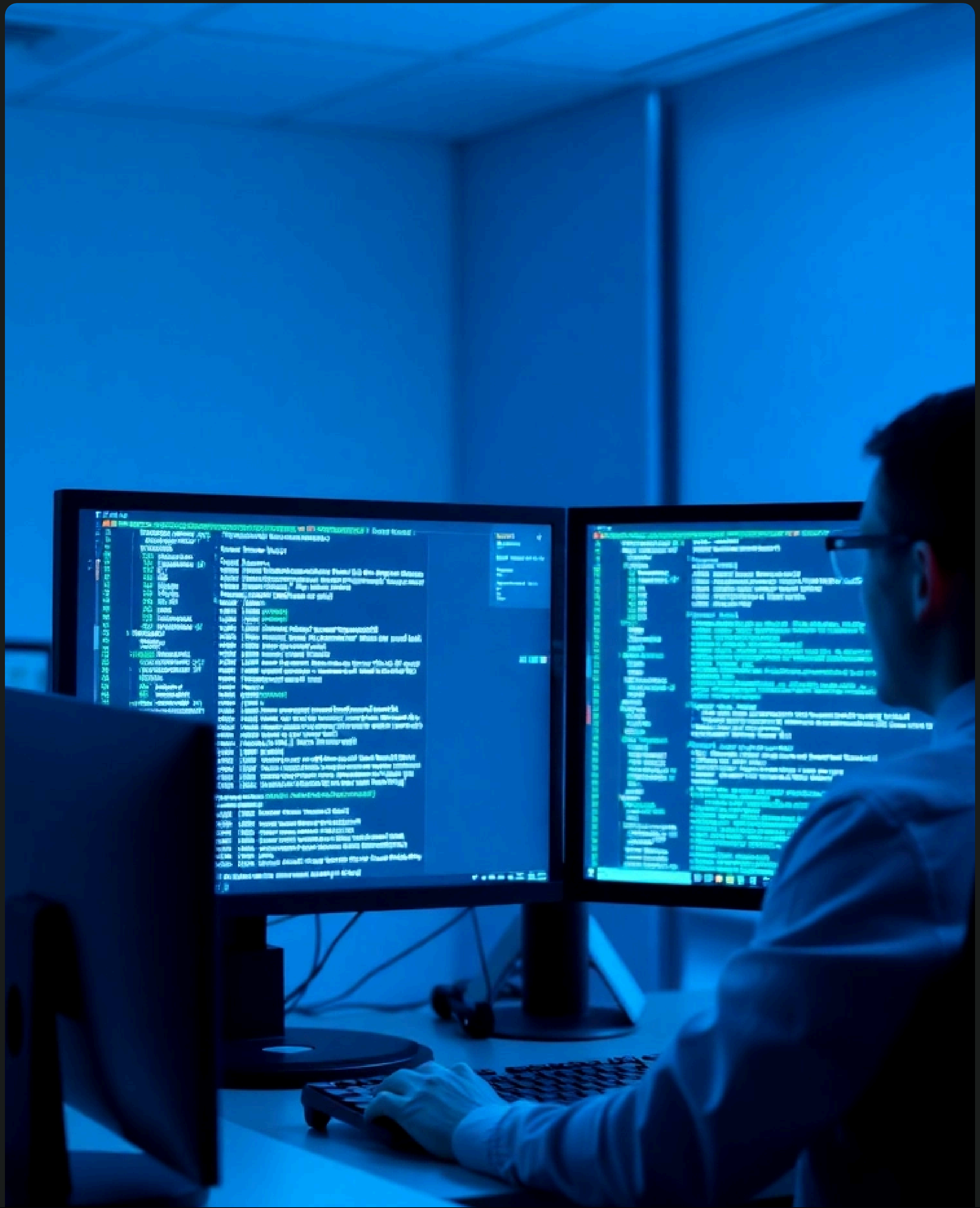
- All scans ran only on local lab VMs with explicit permission
- Do not run vulnerability scans against networks or hosts you do not own
- This demo is unauthenticated — showing external attack surface only

Objective

What we're testing — and why

- Compare Nessus findings with the **Windows firewall on** vs. **firewall off**
- Explain why scan results are **identical in this lab** environment
- Provide **remediation steps** and a path to deeper, more realistic testing

Even a small, controlled test reveals how firewall placement and scan credentials shape what defenders actually see.



Test Environment & Scan Settings

Unauthenticated basic network scan from Kali Linux targeting a Windows VM over VirtualBox NAT.

Kali Linux

Running Nessus Essentials locally on the attack machine

Windows VM

IP 10.0.2.15, hosted in VirtualBox under NAT network mode

Basic Network Scan

Unauthenticated, default timing, no credentials provided to scanner

Updated Before Scans

All Nessus plugins refreshed prior to each scan run for accuracy

⚠ Unauthenticated scans have limited depth · NAT network mode may affect external host visibility

Methodology

1

Enable Firewall & Scan

Run Nessus with the Windows firewall enabled. Save a screenshot of the results as Windows with Firewall ON.

2

Disable Firewall & Rescan

Turn off the Windows firewall and run the identical scan again. Save the results screenshot as Windows with Firewall OFF.png.

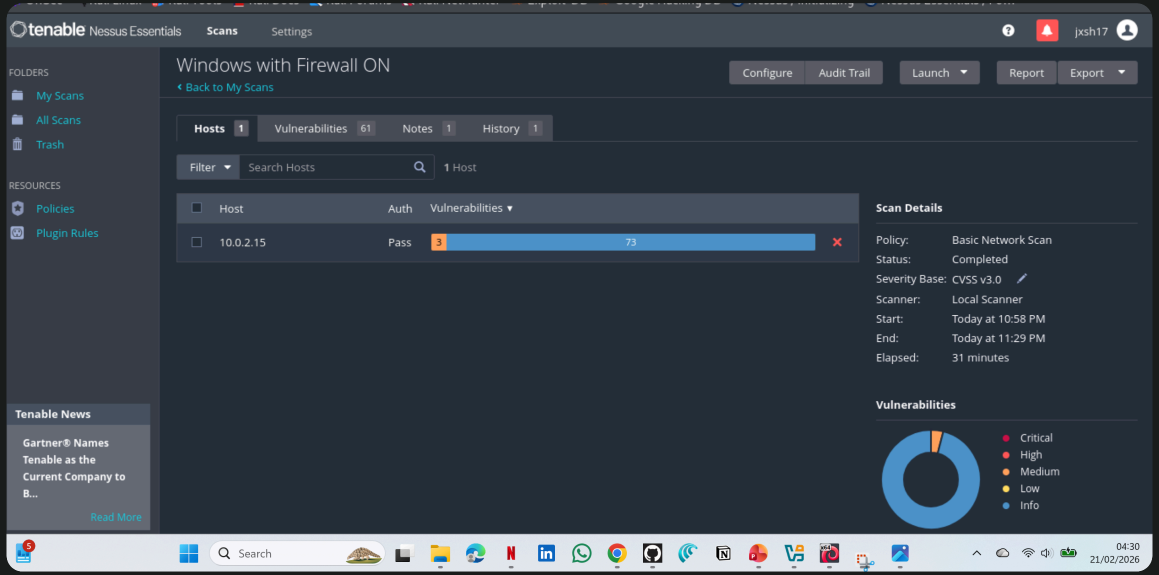
3

Compare & Analyse

Use the same scan profile for both runs, then compare totals and top findings to ensure a fair, controlled comparison.

Results snapshot

Key observation: Both scans returned **identical findings and counts** — firewall state had no impact on Nessus results.



Windows with Firewall ON

‹ Back to My Scans

Hosts 1 | Vulnerabilities 61 | Notes 1 | History 1

Filter ▾ Search Hosts — 1 Host

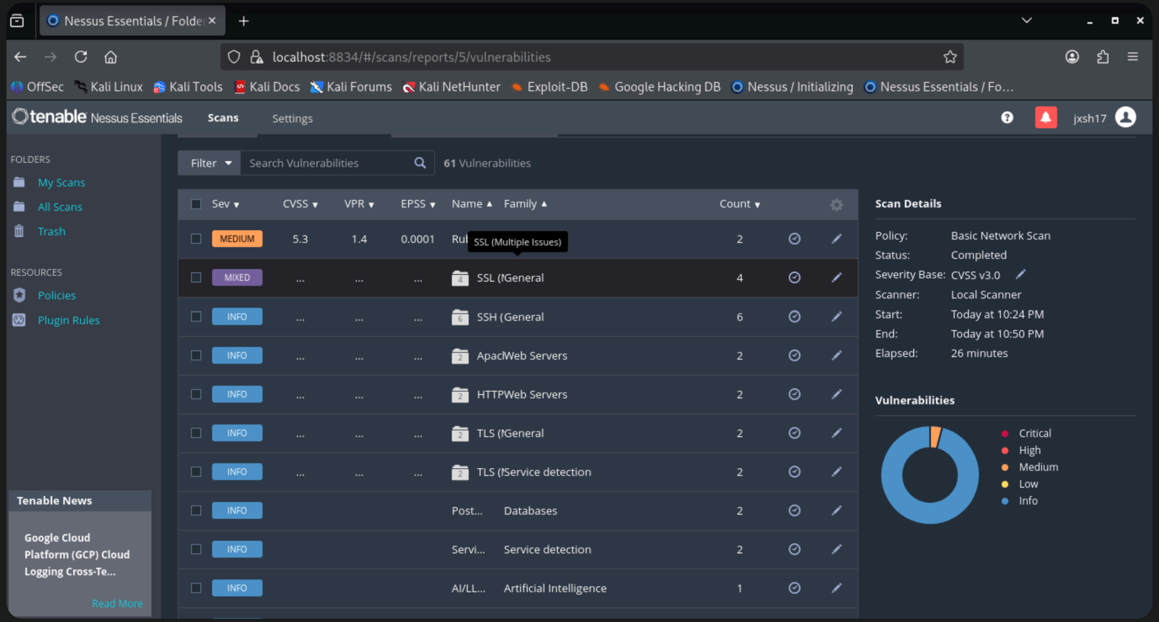
Host	Auth	Vulnerabilities ▾
10.0.2.15	Pass	3 73

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:58 PM
End:	Today at 11:29 PM
Elapsed:	31 minutes

Vulnerabilities

● Critical ● High ● Medium ● Low ● Info



Filter ▾ Search Vulnerabilities — 61 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
MEDIUM	5.3	1.4	0.0001	Rul		2
MIXED	...	...	...	SSL (!	General	4
INFO	...	...	...	SSH (	General	6
INFO	...	...	...	Apac	Web Servers	2
INFO	...	...	...	HTTP	Web Servers	2
INFO	...	...	...	TLS (!	General	2
INFO	...	...	...	TLS (!	Service detection	2
INFO				Post...	Databases	2
INFO				Servi...	Service detection	2
INFO				AI/LL...	Artificial Intelligence	1

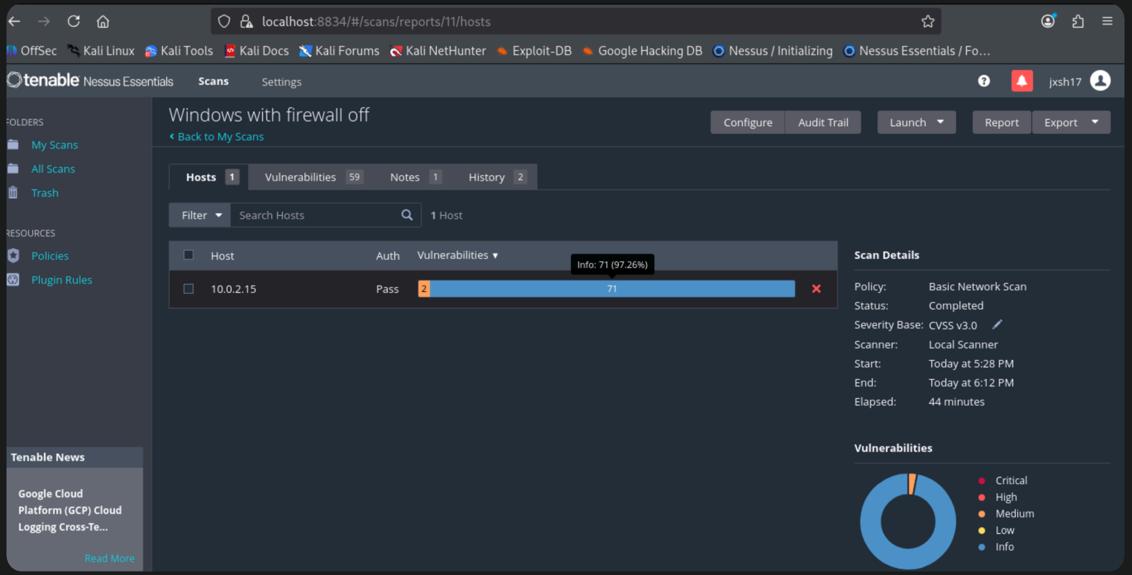
Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:24 PM
End:	Today at 10:50 PM
Elapsed:	26 minutes

Vulnerabilities

● Critical ● High ● Medium ● Low ● Info

Nessus results with **firewall enabled**



Windows with firewall off

‹ Back to My Scans

Hosts 1 | Vulnerabilities 59 | Notes 1 | History 2

Filter ▾ Search Hosts — 1 Host

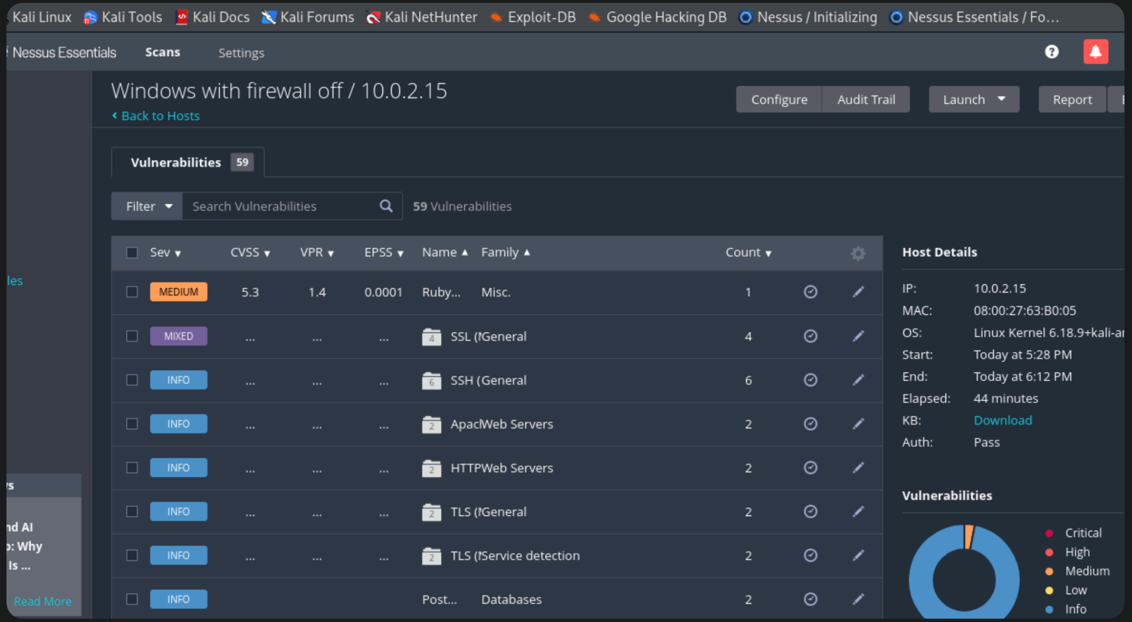
Host	Auth	Vulnerabilities ▾
10.0.2.15	Pass	2 71

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 5:28 PM
End:	Today at 6:12 PM
Elapsed:	44 minutes

Vulnerabilities

● Critical ● High ● Medium ● Low ● Info



Windows with firewall off / 10.0.2.15

‹ Back to Hosts

Vulnerabilities 59

Filter ▾ Search Vulnerabilities — 59 Vulnerabilities

Sev ▾	CVSS ▾	VPR ▾	EPSS ▾	Name ▴	Family ▴	Count ▾
MEDIUM	5.3	1.4	0.0001	Ruby...	Misc.	1
MIXED	...	...	...	SSL (!	General	4
INFO	...	...	...	SSH (	General	6
INFO	...	...	...	Apac	Web Servers	2
INFO	...	...	...	HTTP	Web Servers	2
INFO	...	...	...	TLS (!	General	2
INFO	...	...	...	TLS (!	Service detection	2
INFO				Post...	Databases	2

Host Details

IP:	10.0.2.15
MAC:	08:00:27:63:B0:05
OS:	Linux Kernel 6.18.9+kali-ar
Start:	Today at 5:28 PM
End:	Today at 6:12 PM
Elapsed:	44 minutes
KB:	Download
Auth:	Pass

Vulnerabilities

● Critical ● High ● Medium ● Low ● Info

Nessus results with **firewall disabled**

Key numbers at a glance

🔒 Firewall ON

76

Total vulnerabilities

3

Medium severity findings

🔓 Firewall OFF

73

Total vulnerabilities

2

Medium severity findings

These numbers reflect a point-in-time snapshot of Nessus scan results under two network conditions.

If totals are identical, this is expected — see the following slide for explanation.

insert difference, or "Identical — firewall had no measurable impact on visible vulnerabilities"

Analysis

Why the scans can be identical

NAT hides the host

VirtualBox NAT limits external exposure, disabling the host firewall did not open new ports to the scanner, so the attack surface remained unchanged.

Minimal exposed services

The target had very few running services at scan time, leaving Nessus nothing new to detect between the two scans.

Unauthenticated scan

Without credentials, Nessus cannot see deeper host-level issues — many vulnerabilities remain hidden until an authenticated scan is run.

Conclusion & next steps

Both scans returned identical results, confirming a low external attack surface under the current setup.
Maintain firewall rules, apply critical updates, and disable unused services.

01 — Run authenticated scans

Use Nessus authenticated scans to perform deeper host-level checks and uncover vulnerabilities not visible externally.

02 — Switch to bridged networking

Switch to host-only or bridged network mode to expose the target more realistically and validate scan coverage.

03 — Schedule scans & integrate with SIEM

Establish recurring scan cadence and feed results into your SIEM for continuous monitoring and faster incident response.

Thank you.

Presented by: Jash Vaidya
Professor: Dimple Chauhan

Questions? Feel free to ask.