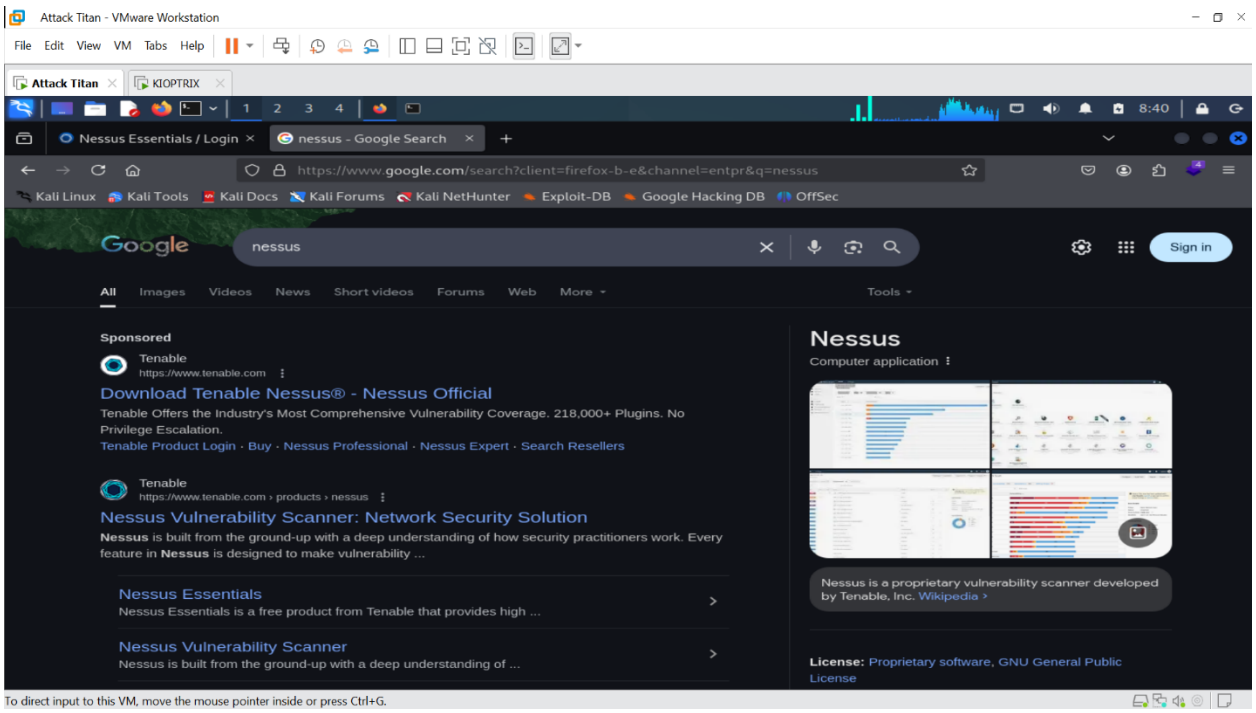
Vulnerability Scanning Using Nessus – Lab Report

By: Lloyd Ensor Azumah

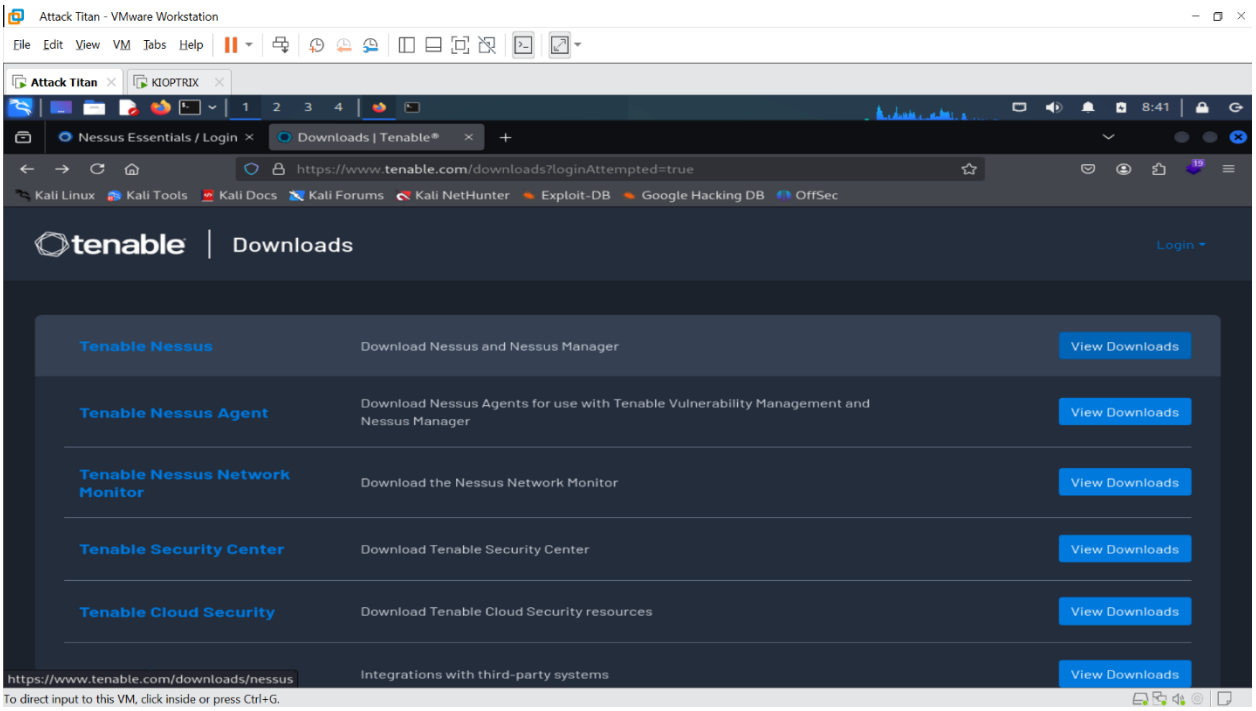
Date: Insert Date

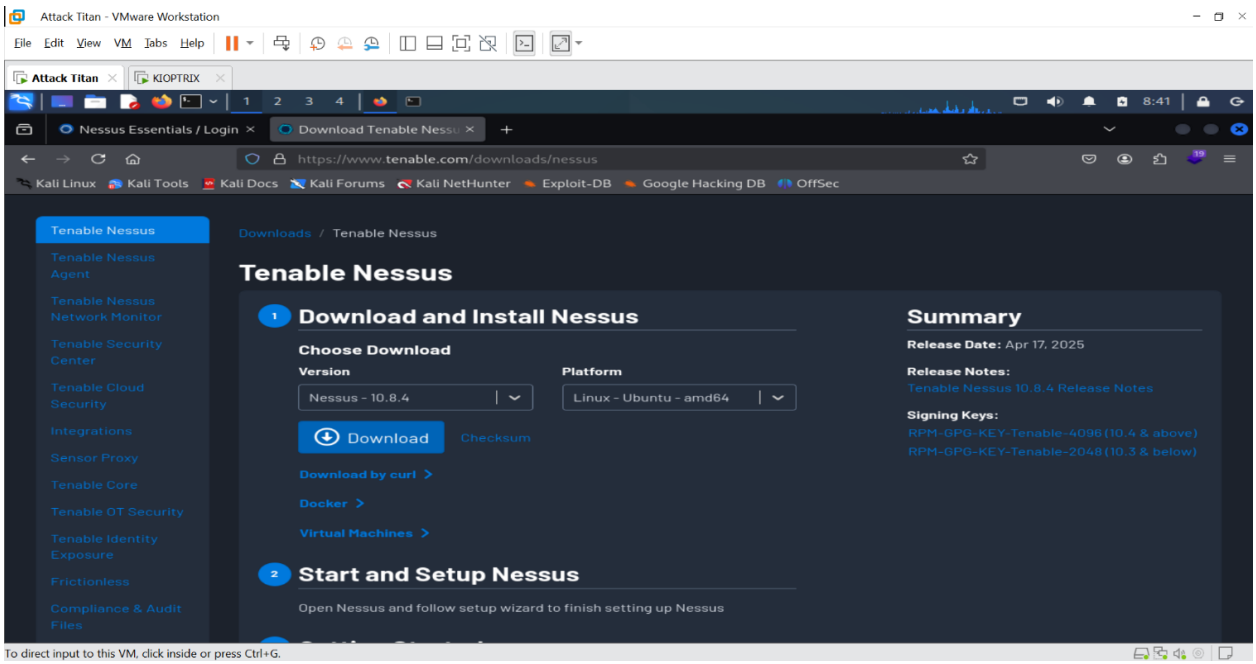
Overview

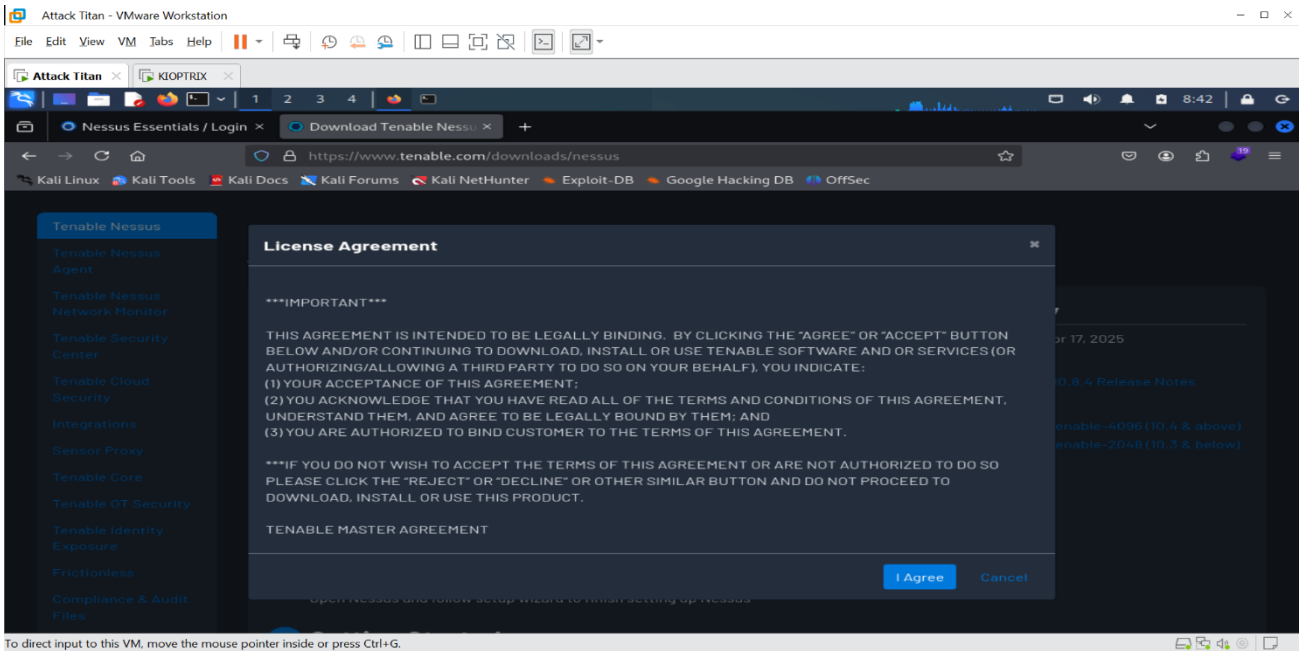
1. Installation of Nessus



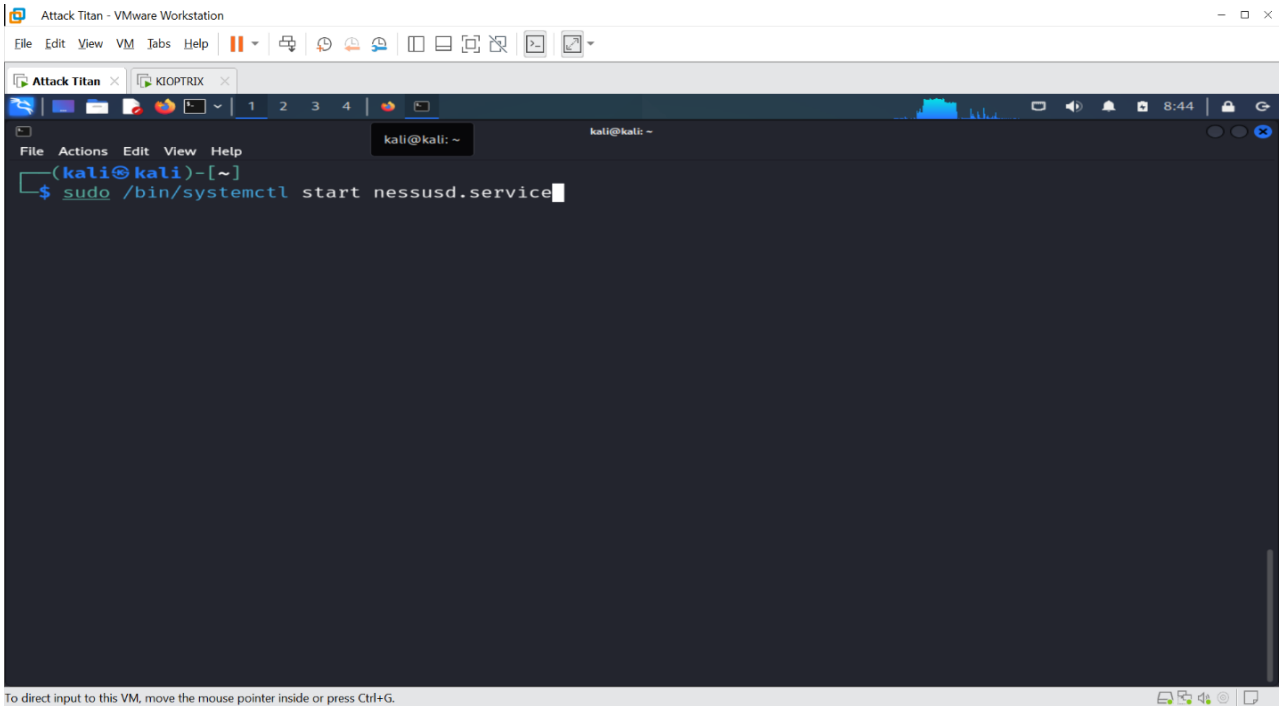
- Downloaded Tenable Nessus Essentials for Linux (Ubuntu - amd64) from the official Tenable website.


Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Login
Downloads | Tenable®
https://www.tenable.com/downloads?loginAttempted=true
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
tenable | Downloads
Login
Tenable Nessus
Download Nessus and Nessus Manager
View Downloads
Tenable Nessus Agent
Download Nessus Agents for use with Tenable Vulnerability Management and Nessus Manager
View Downloads
Tenable Nessus Network Monitor
Download the Nessus Network Monitor
View Downloads
Tenable Security Center
Download Tenable Security Center
View Downloads
Tenable Cloud Security
Download Tenable Cloud Security resources
View Downloads
Integrations with third-party systems
View Downloads
https://www.tenable.com/downloads/nessus
To direct input to this VM, click inside or press Ctrl+G.

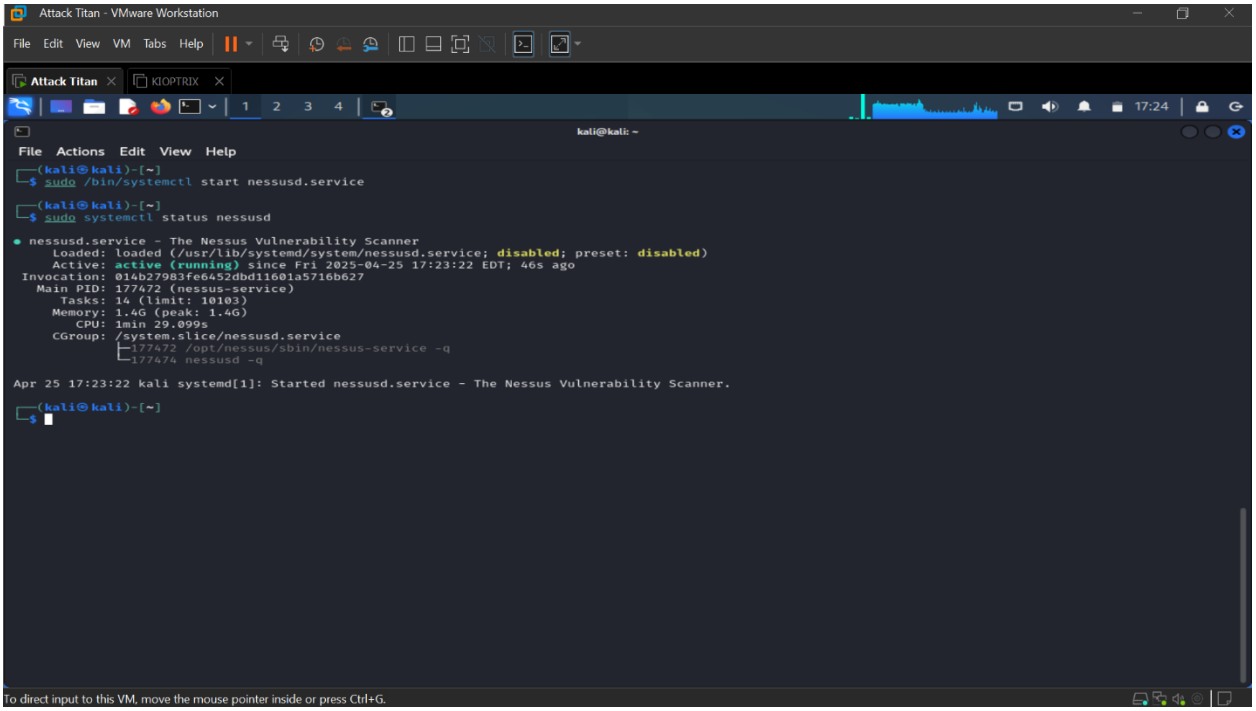

Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Login
Download Tenable Nessu
https://www.tenable.com/downloads/nessus
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Tenable Nessus
Tenable Nessus Agent
Tenable Nessus Network Monitor
Tenable Security Center
Tenable Cloud Security
Integrations
Sensor Proxy
Tenable Core
Tenable OT Security
Tenable Identity Exposure
Frictionless
Compliance & Audit Files
Downloads / Tenable Nessus
Tenable Nessus
1 Download and Install Nessus
Choose Download
Version
Nessus - 10.8.4
Platform
Linux - Ubuntu - amd64
Download
Checksum
Download by curl >
Docker >
Virtual Machines >
Summary
Release Date: Apr 17, 2025
Release Notes:
Tenable Nessus 10.8.4 Release Notes
Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)
2 Start and Setup Nessus
Open Nessus and follow setup wizard to finish setting up Nessus
To direct input to this VM, click inside or press Ctrl+G.

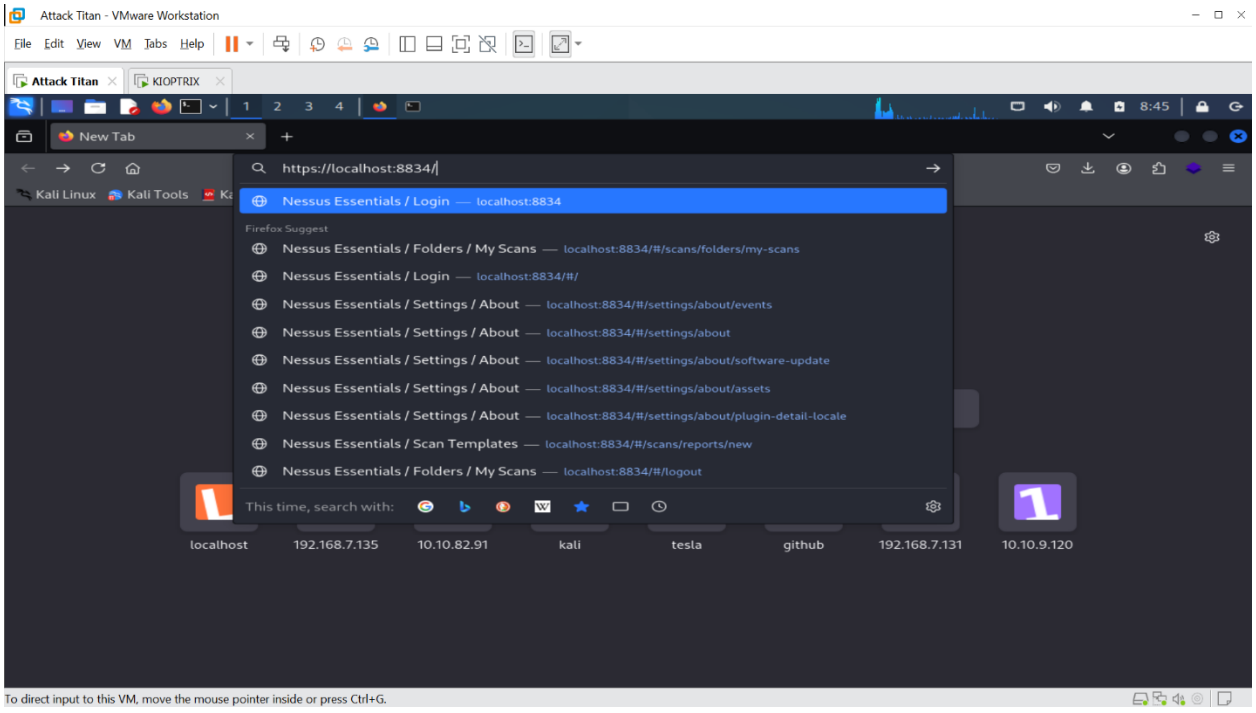


- Agreed to terms and initiated the download.

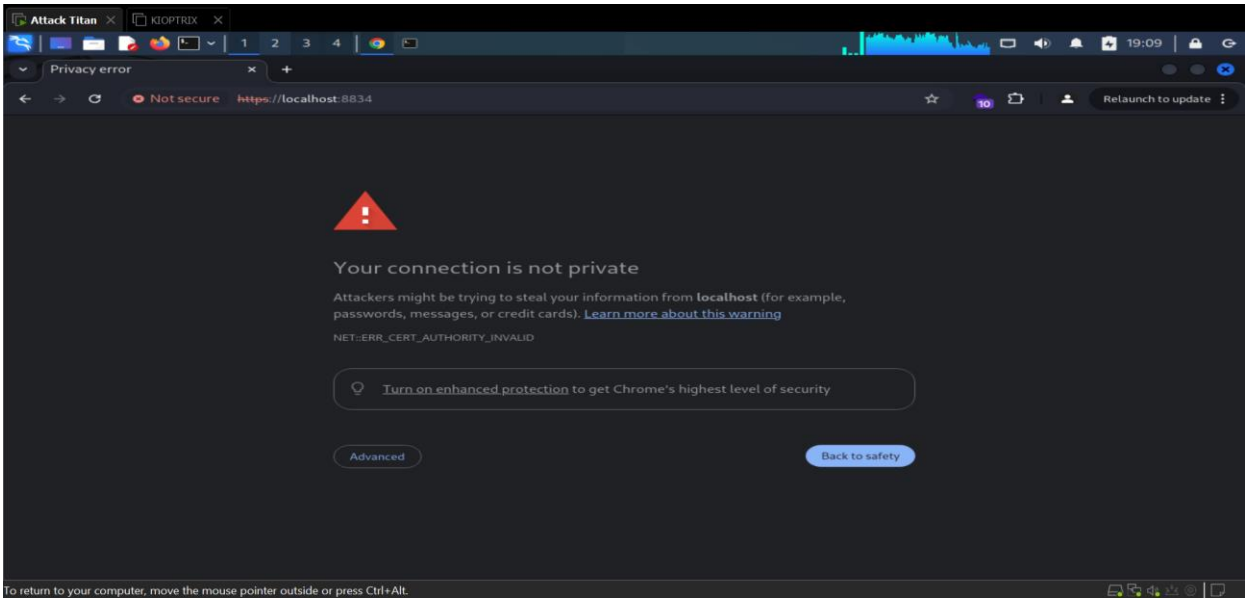


- Installed the package and manually started the Nessus service.

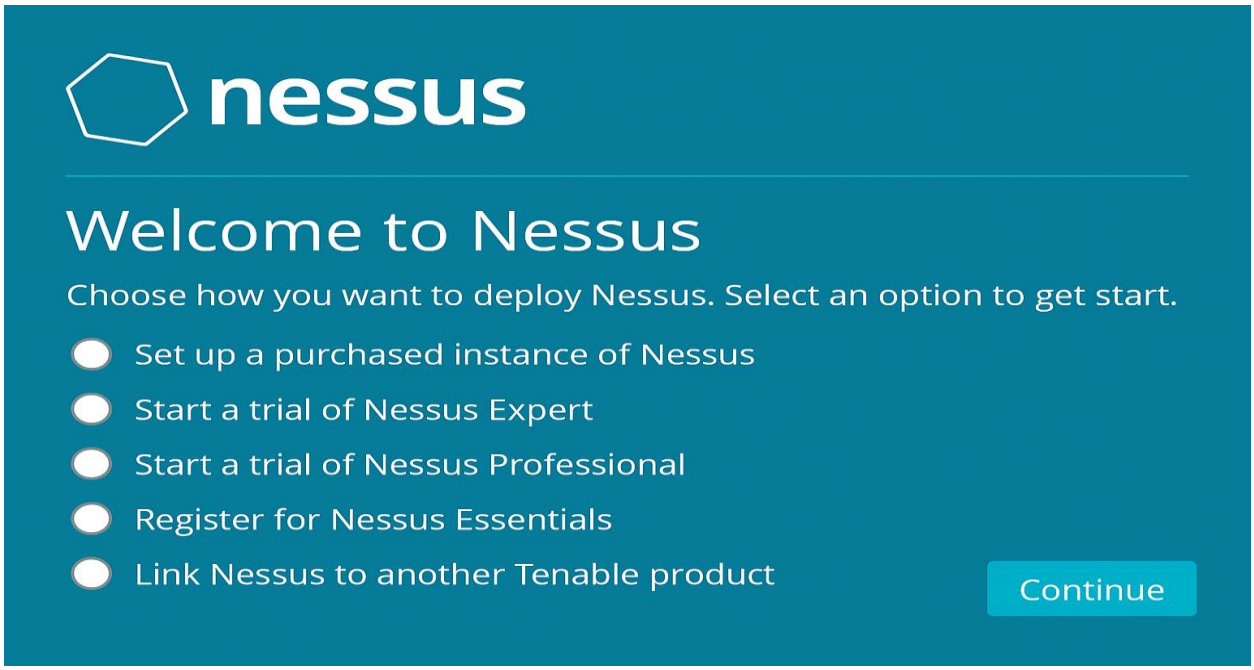




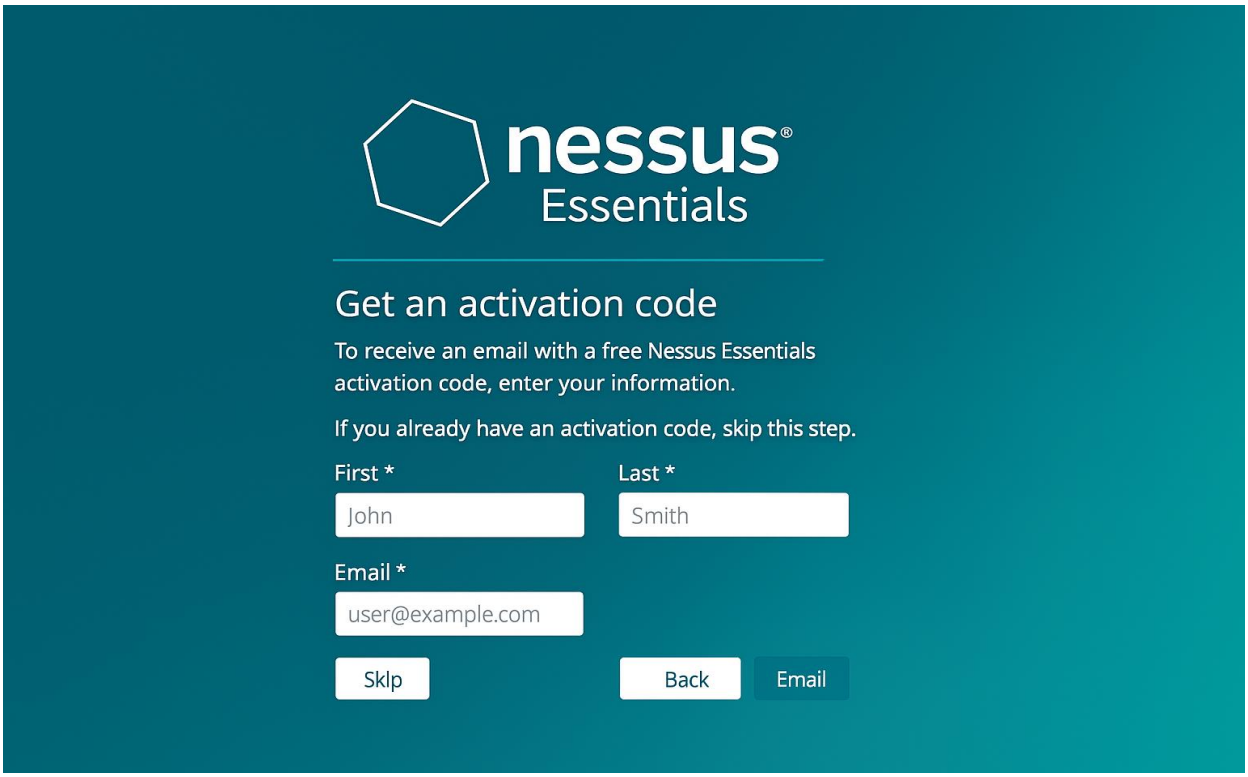
- Accessed the web interface via https://localhost:8834 (browser may display a security warning due to self-signed certificate).



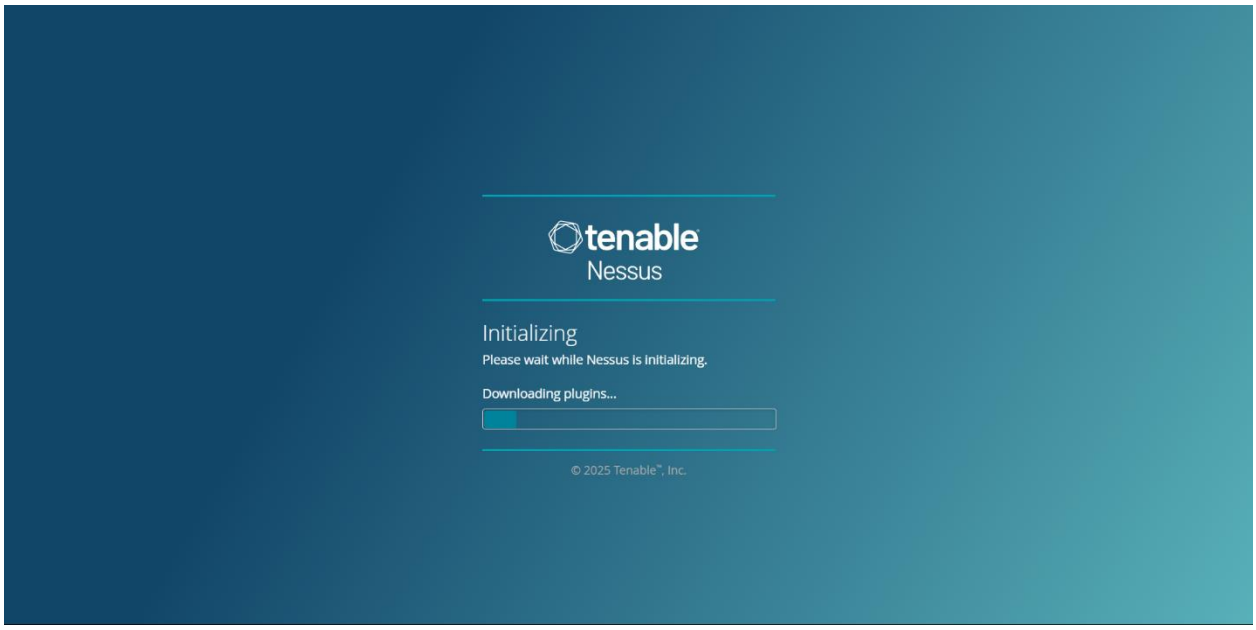
2. Configuration and Setup



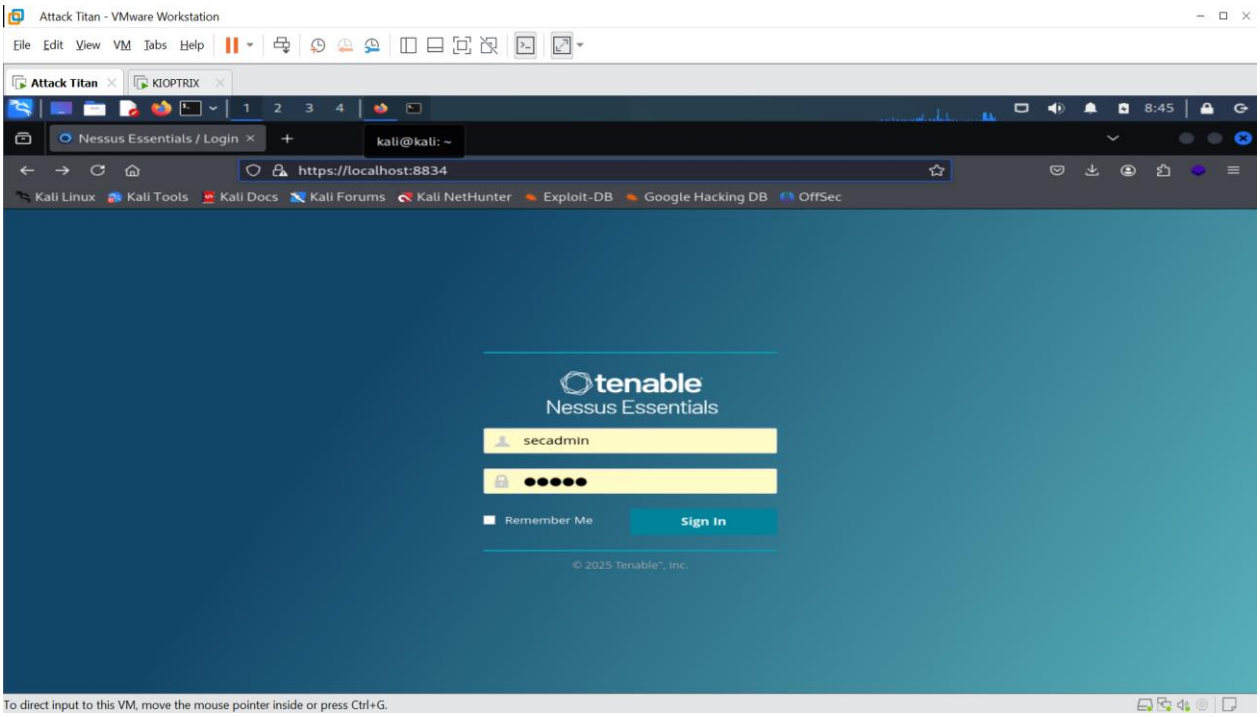
- Selected “Register for Nessus Essentials” to receive an activation code.



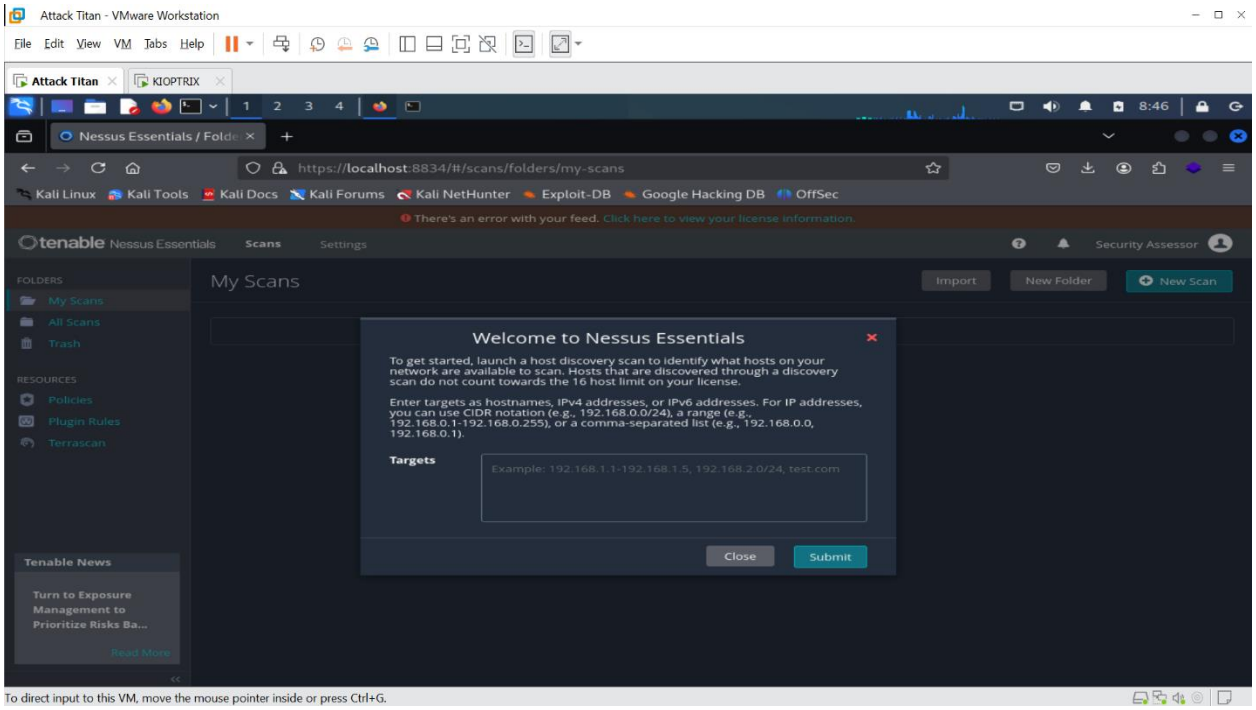
- Registered using name and email address.



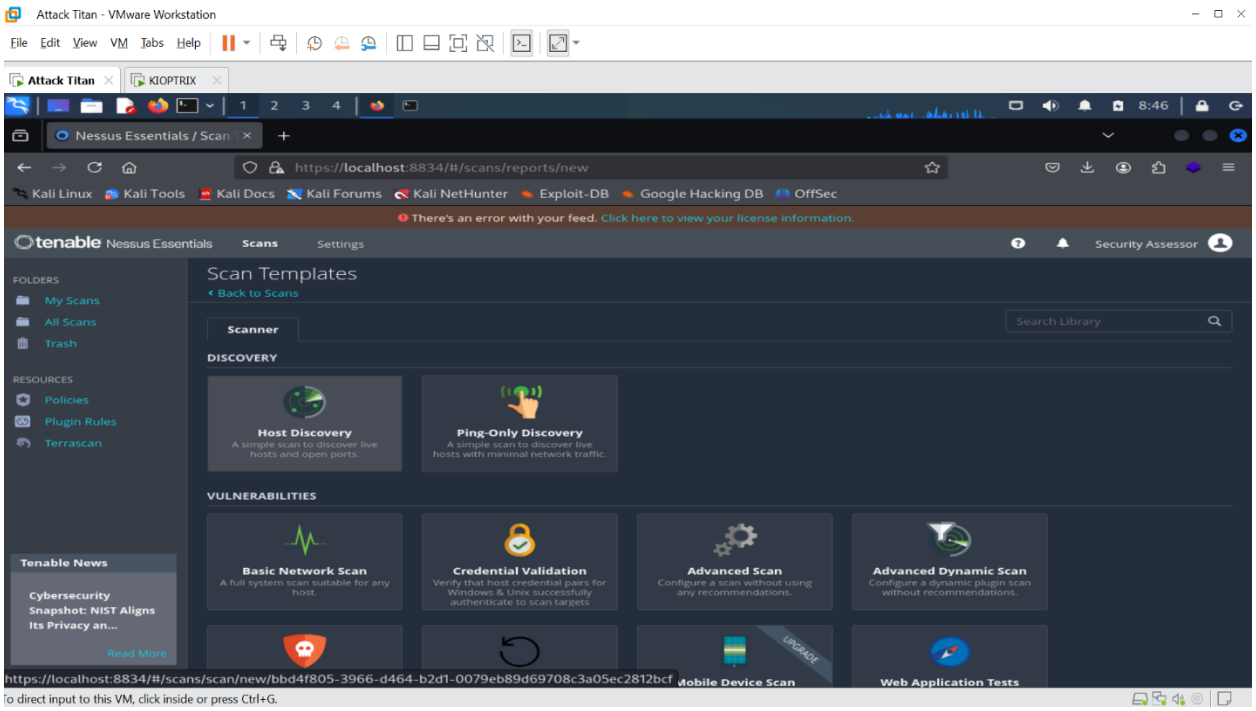
- Nessus automatically downloads required plugins and core components upon activation.
(NB: This is important as this enables Nessus function properly)



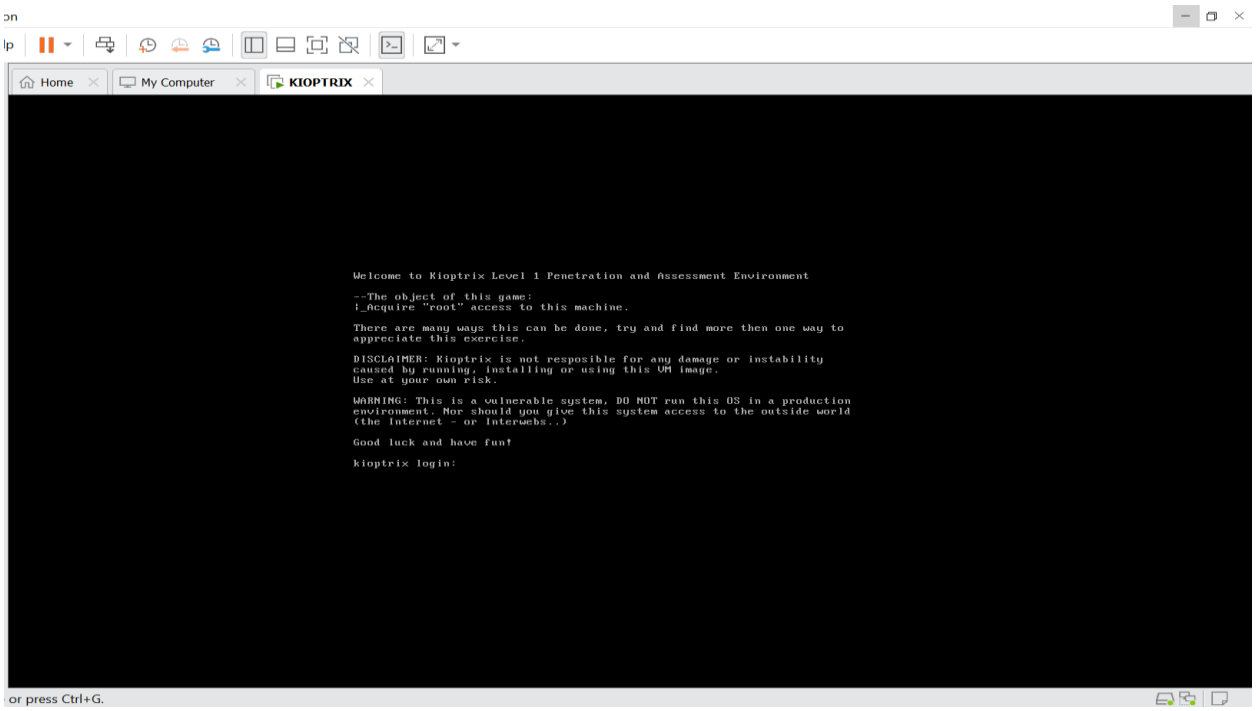
- Logged into the Nessus dashboard to begin scanning activities.



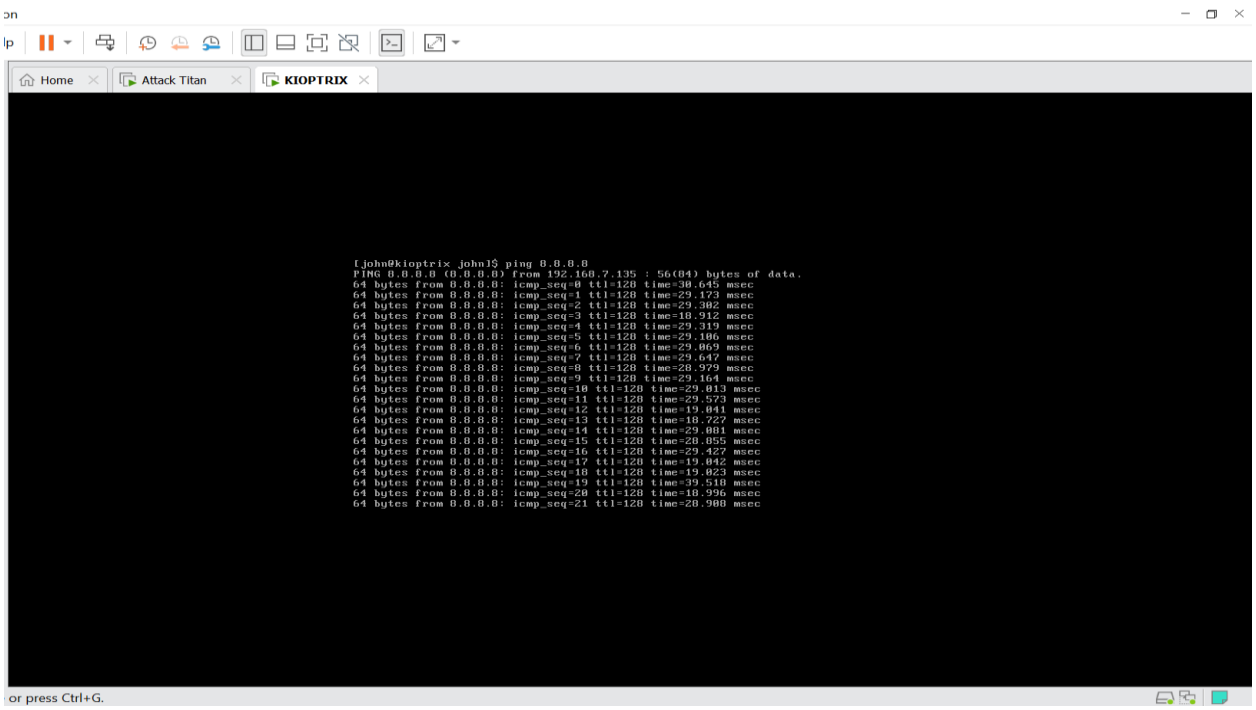
3. Performing a Vulnerability Scan



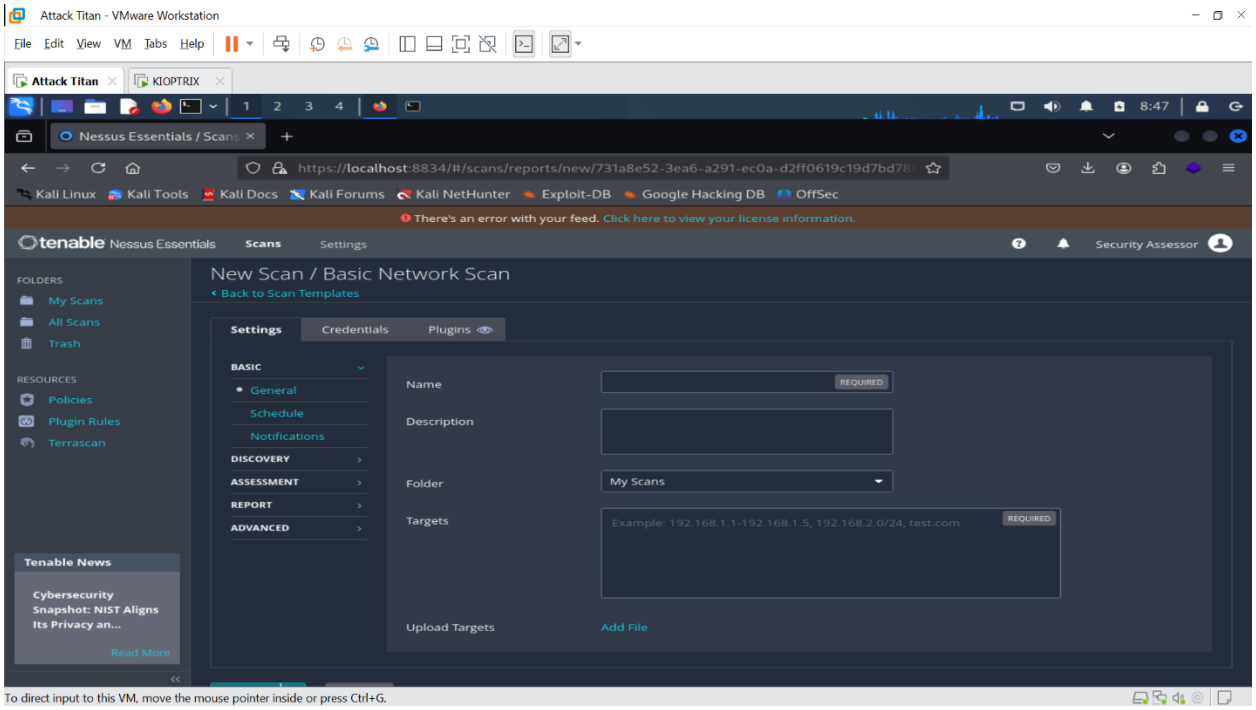
- Created a new Basic Network Scan.



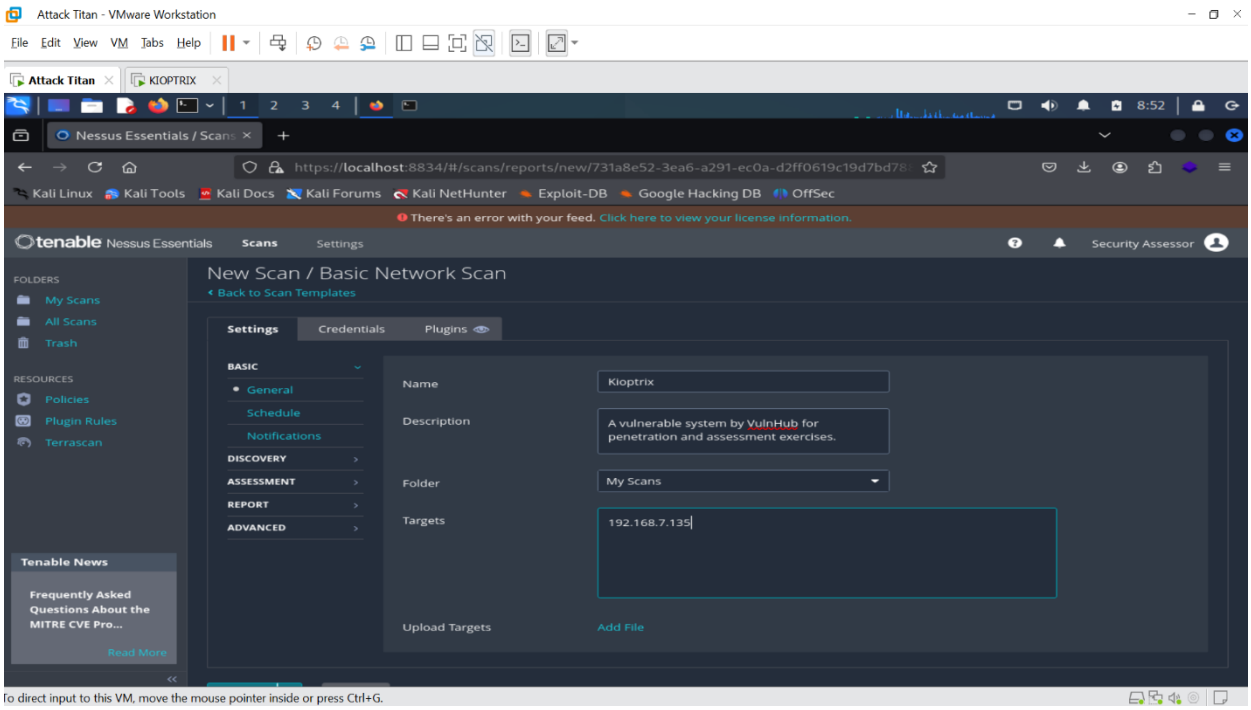
- Target machine: Kioptrix with IP address 192.168.7.135.

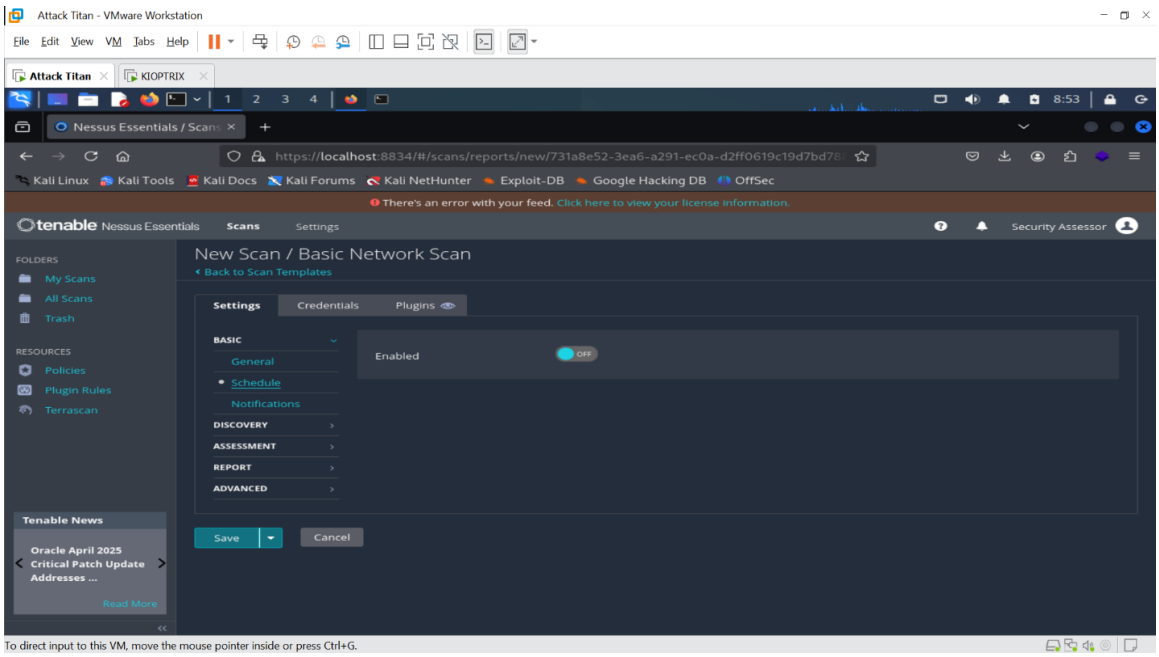


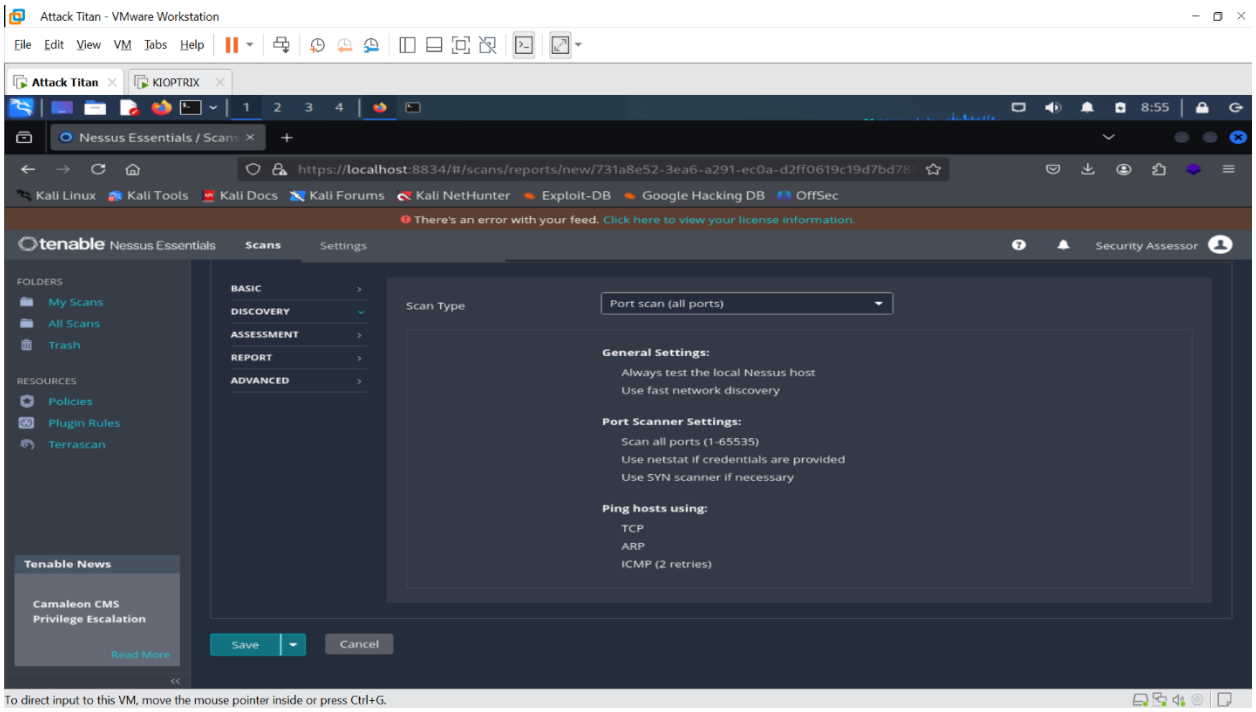
- Ensured both the attack and target machines were on the same virtual NAT network. Verified using ping.



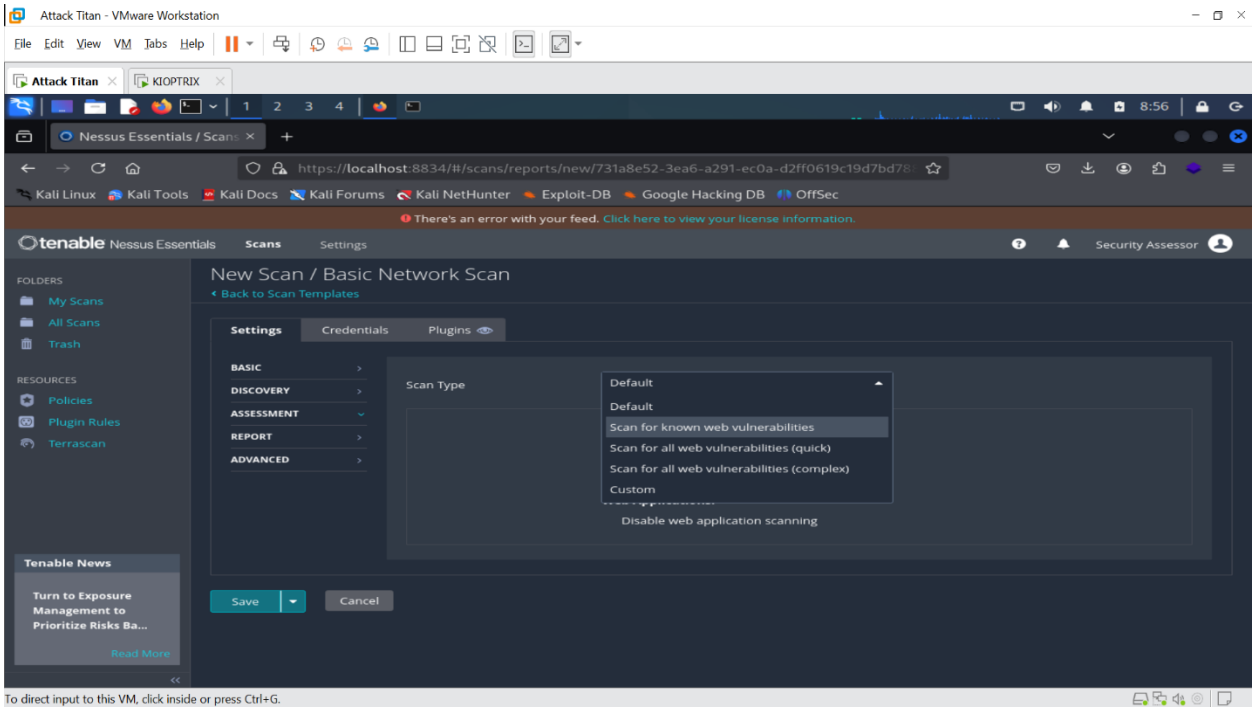
- Configured scan settings to include target name, IP address, all ports and optionally enhance web application tests.

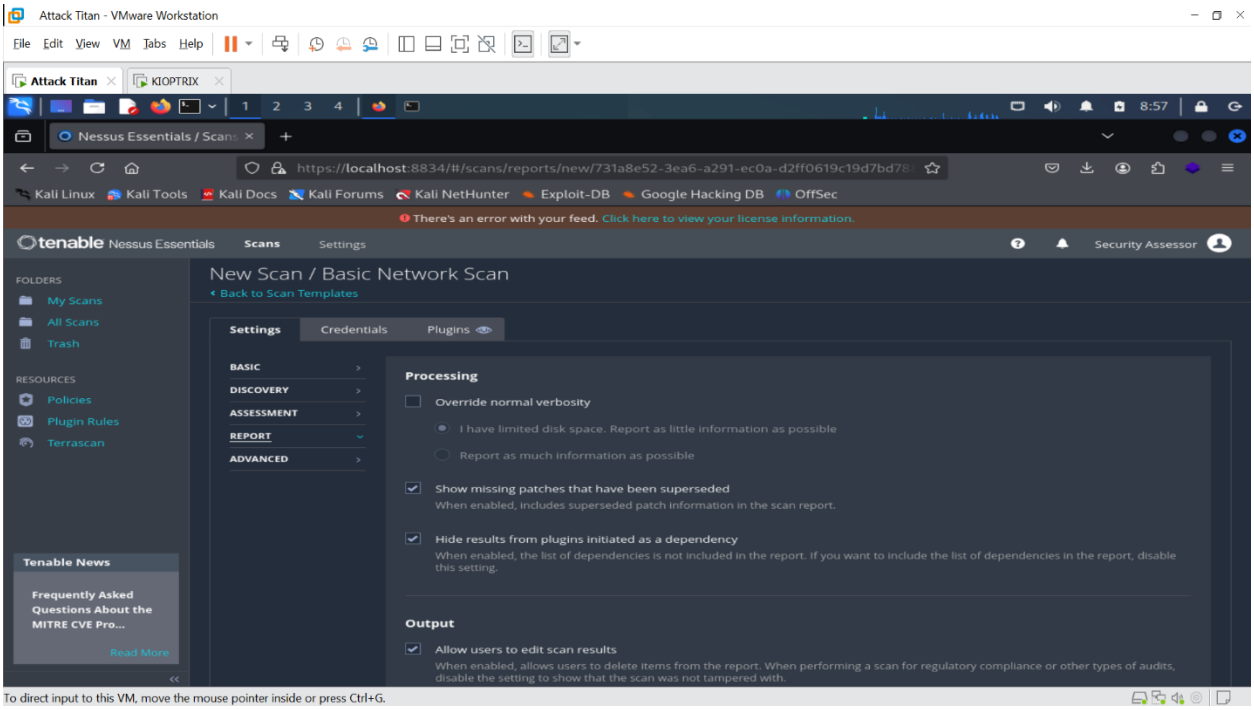


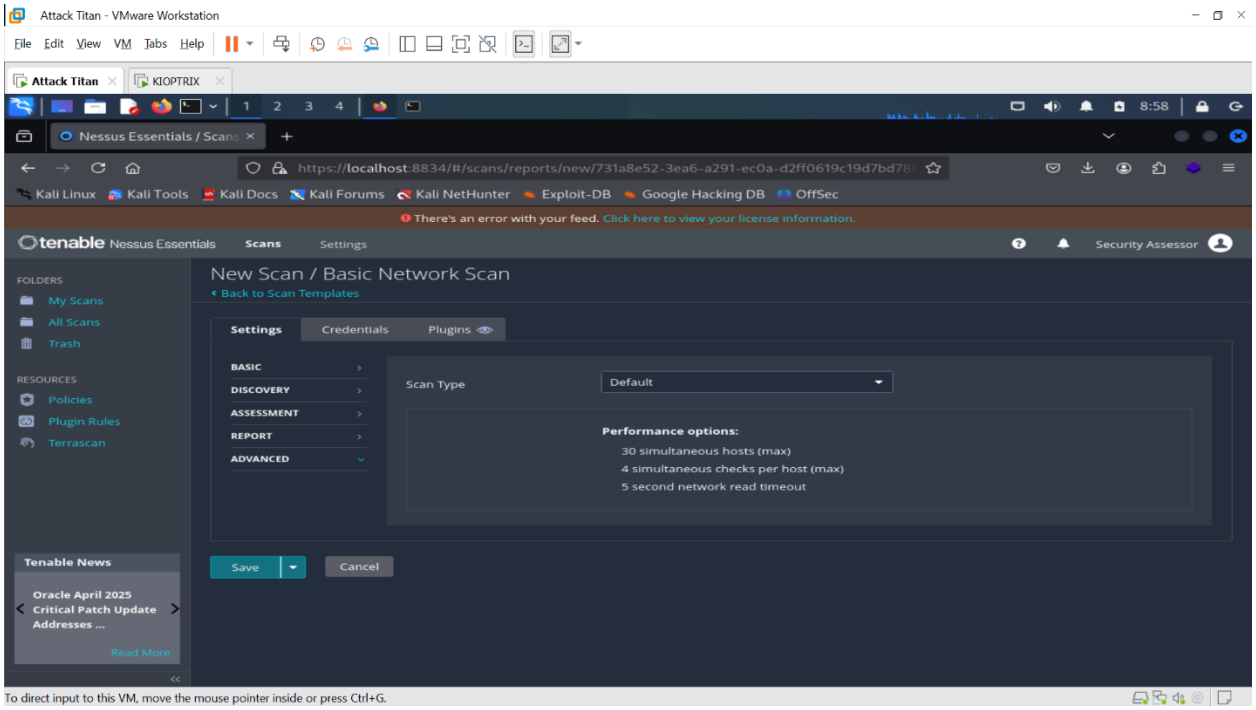




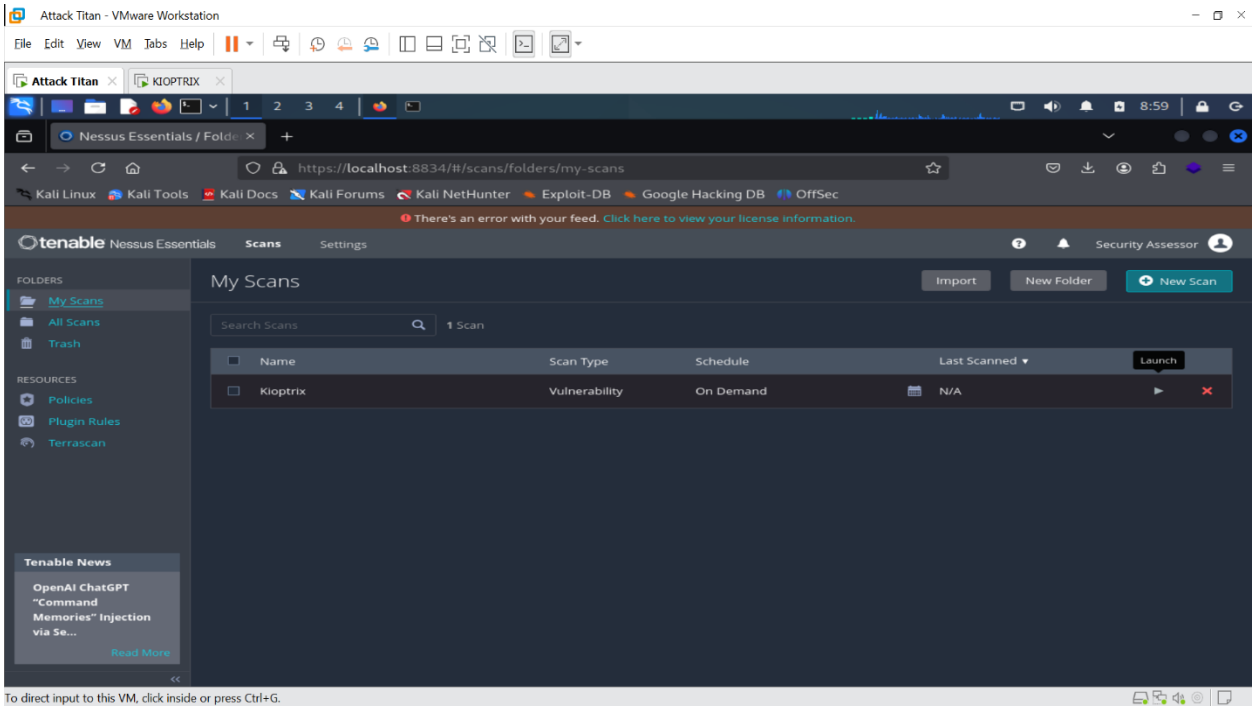
- Configured scan settings to include all ports and optionally enhance web application tests.

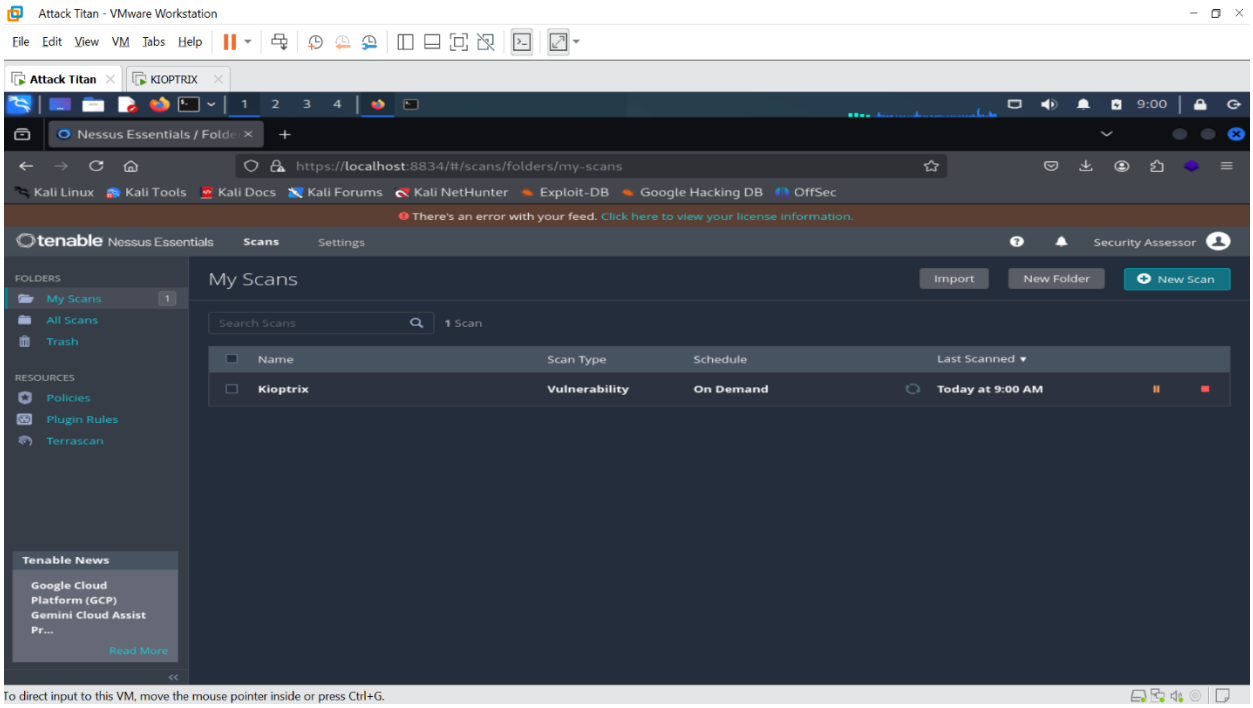

Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Scans
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd78
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
Security Assessor
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Turn to Exposure Management to Prioritize Risks Ba...
Read More
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Default
Default
Scan for known web vulnerabilities
Scan for all web vulnerabilities (quick)
Scan for all web vulnerabilities (complex)
Custom
Disable web application scanning
Save
Cancel
To direct input to this VM, click inside or press Ctrl+G.


Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Scans
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd78
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
Security Assessor
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Frequently Asked Questions About the MITRE CVE Pro...
Read More
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Processing
Override normal verbosity
I have limited disk space. Report as little information as possible
Report as much information as possible
Show missing patches that have been superseded
When enabled, includes superseded patch information in the scan report.
Hide results from plugins initiated as a dependency
When enabled, the list of dependencies is not included in the report. If you want to include the list of dependencies in the report, disable this setting.
Output
Allow users to edit scan results
When enabled, allows users to delete items from the report. When performing a scan for regulatory compliance or other types of audits, disable the setting to show that the scan was not tampered with.
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

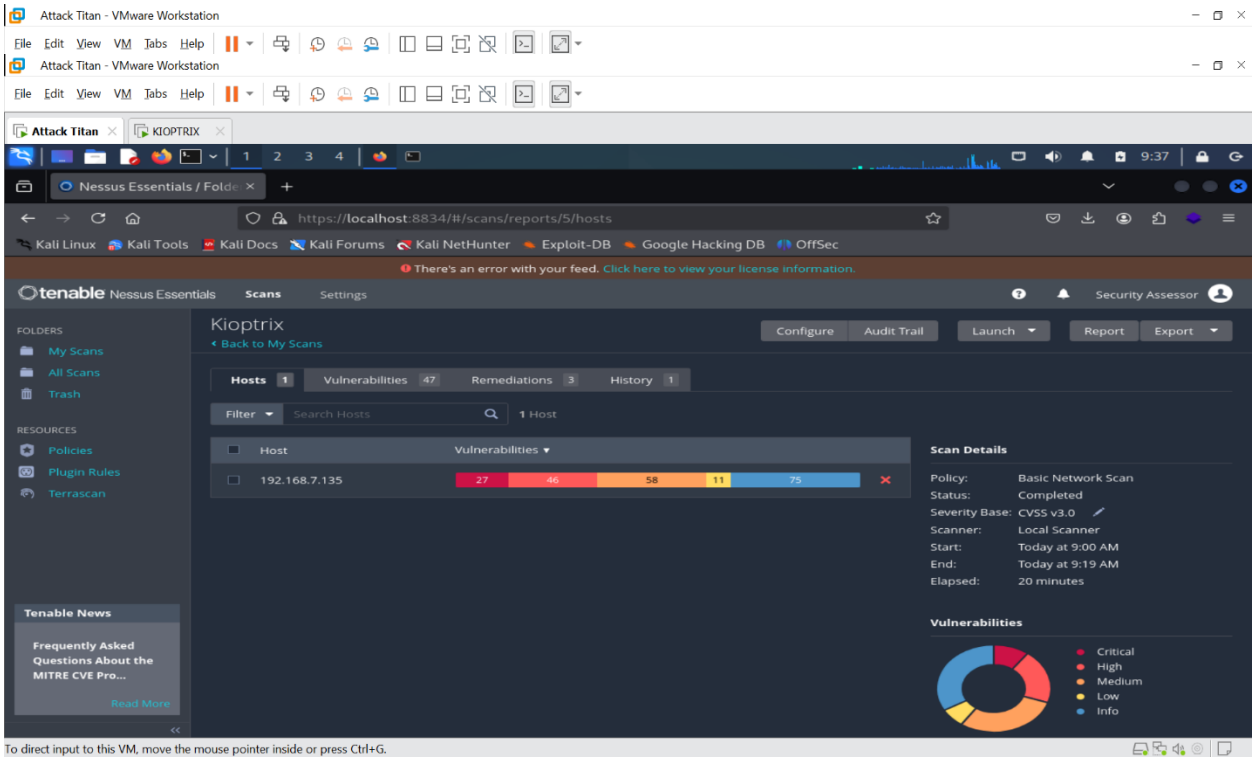


- Saved and launched the scan.



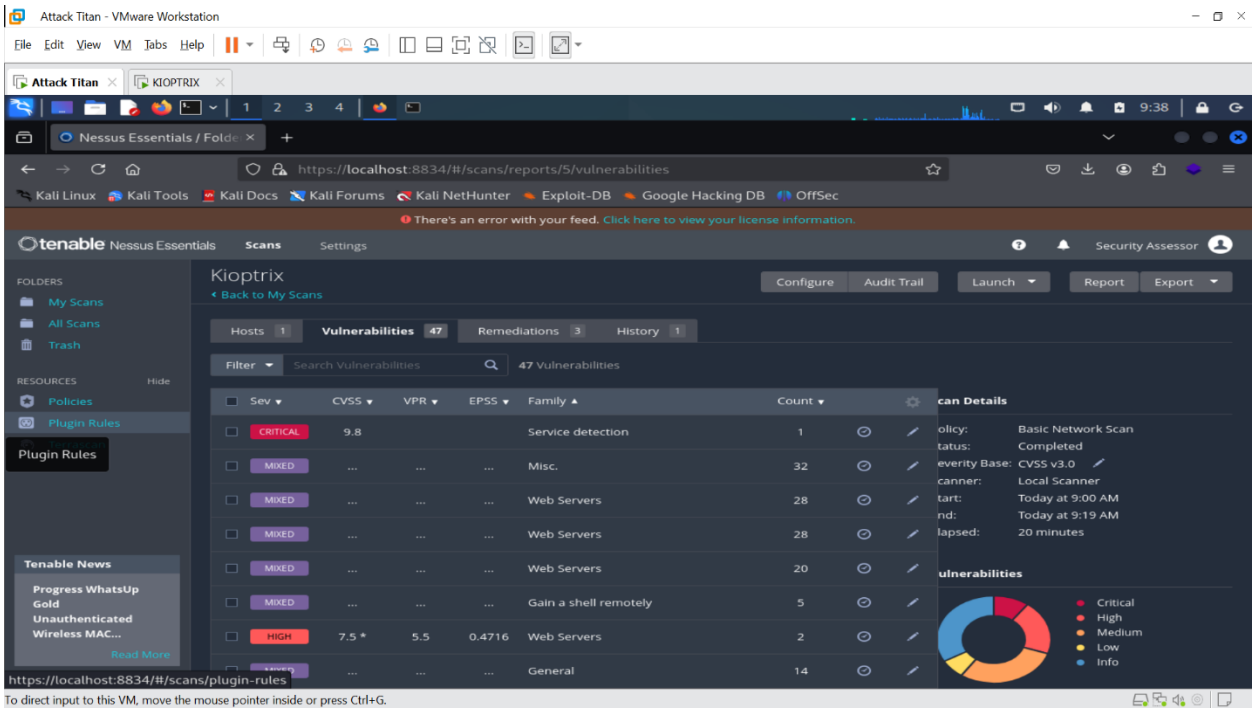

Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Folde
https://localhost:8834/#/scans/folders/my-scans
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
Security Assessor
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Scan Type
Schedule
Last Scanned
Kioptrix
Vulnerability
On Demand
Today at 9:00 AM
Tenable News
Google Cloud Platform (GCP) Gemini Cloud Assist Pr...
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Scan Execution and Results

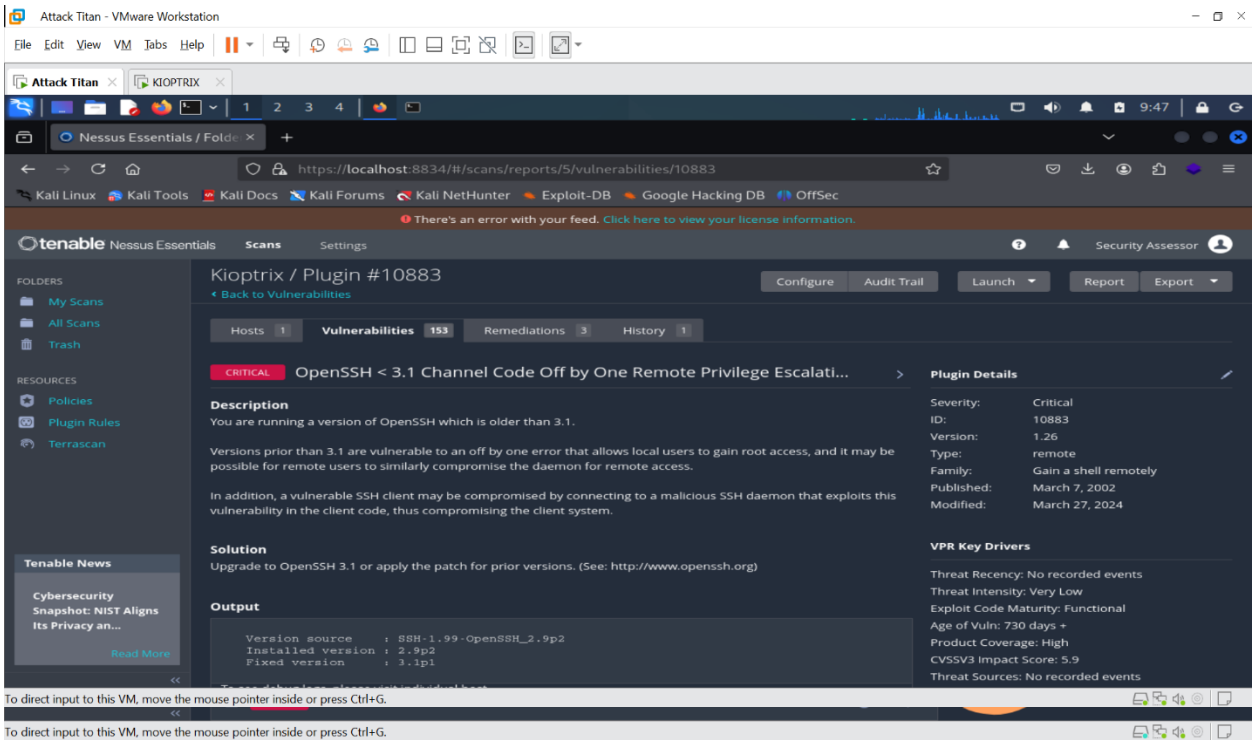


- Scan ran successfully and completed after a few minutes.

- The results highlighted:



- A categorized list of discovered vulnerabilities (Critical, High, Medium, Low, Info).

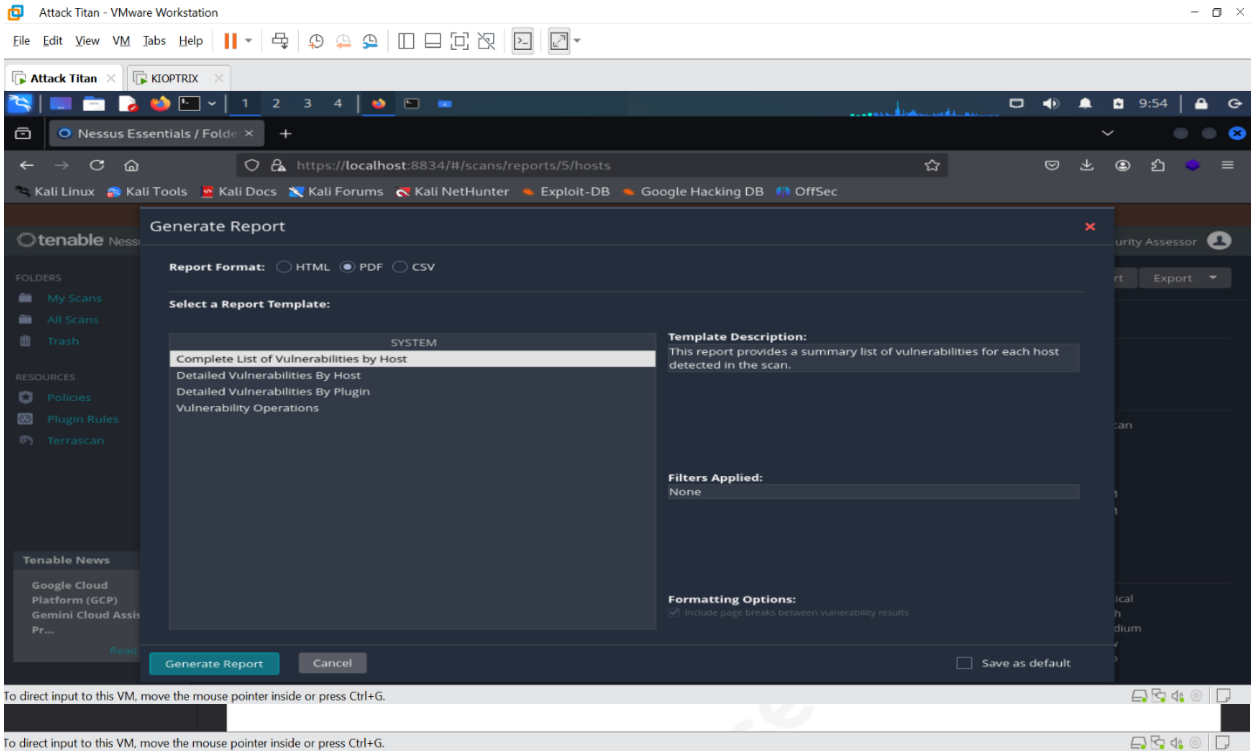


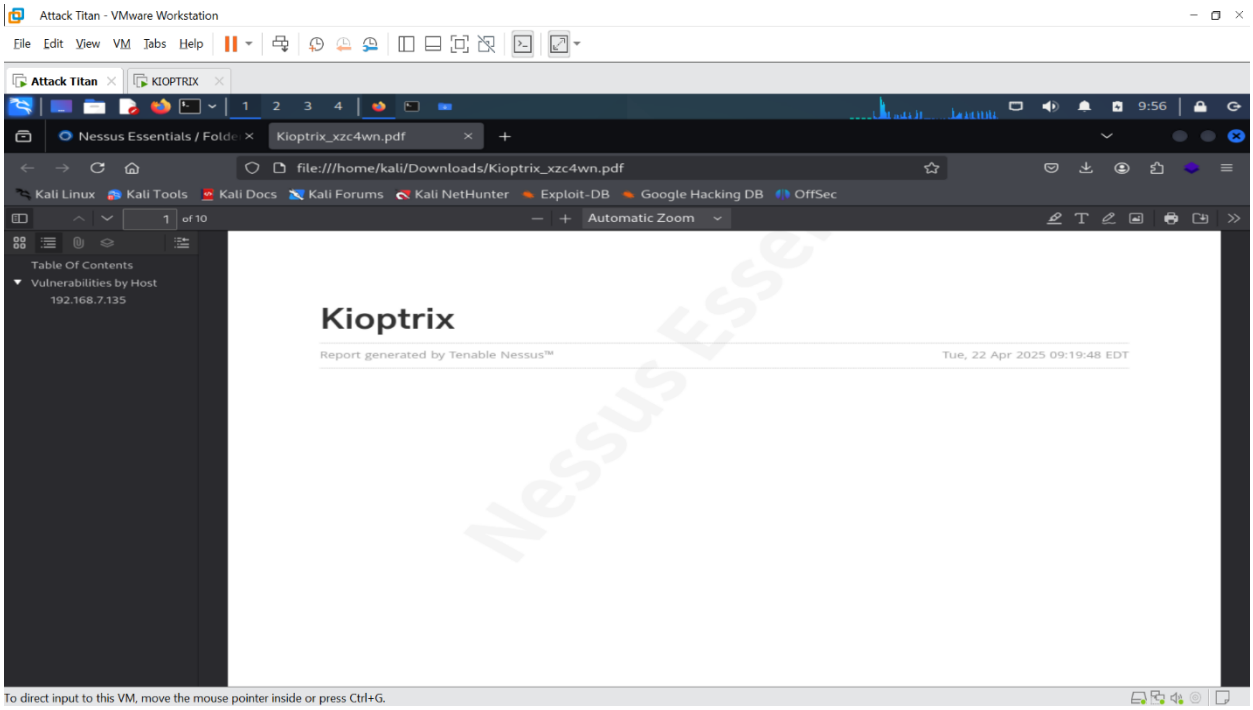
- Description and recommended remediation steps for each vulnerability.

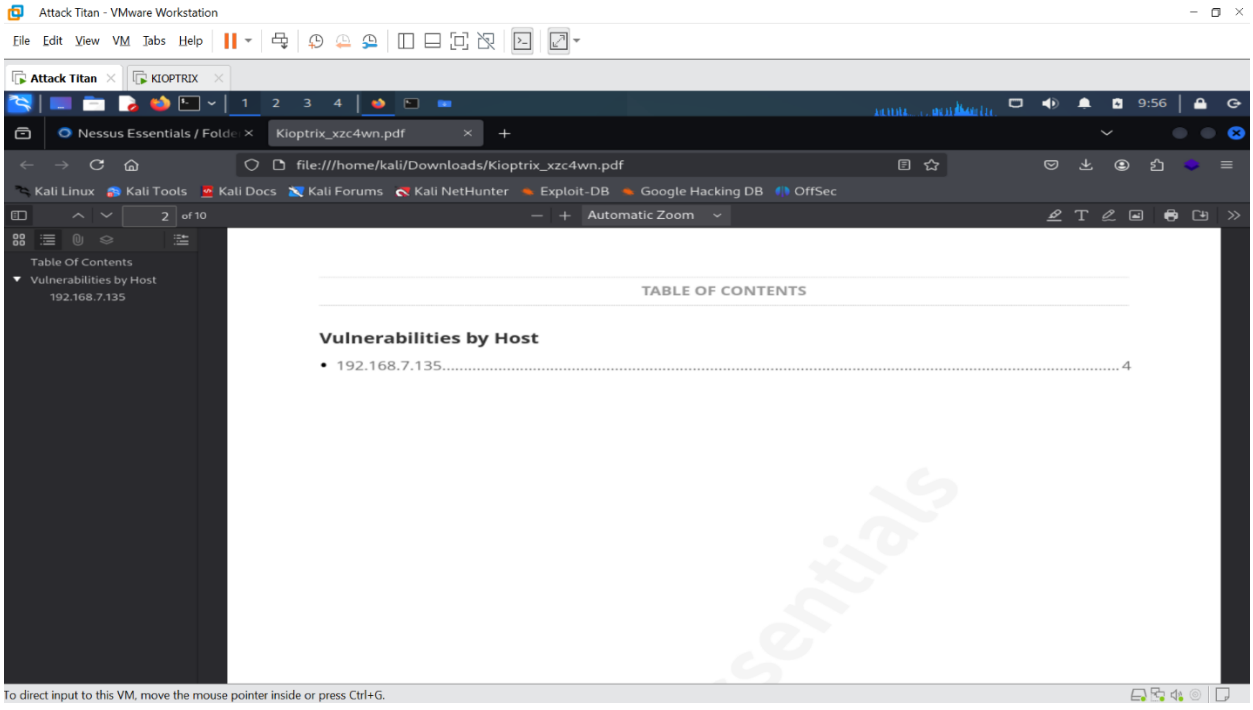
4. Reporting

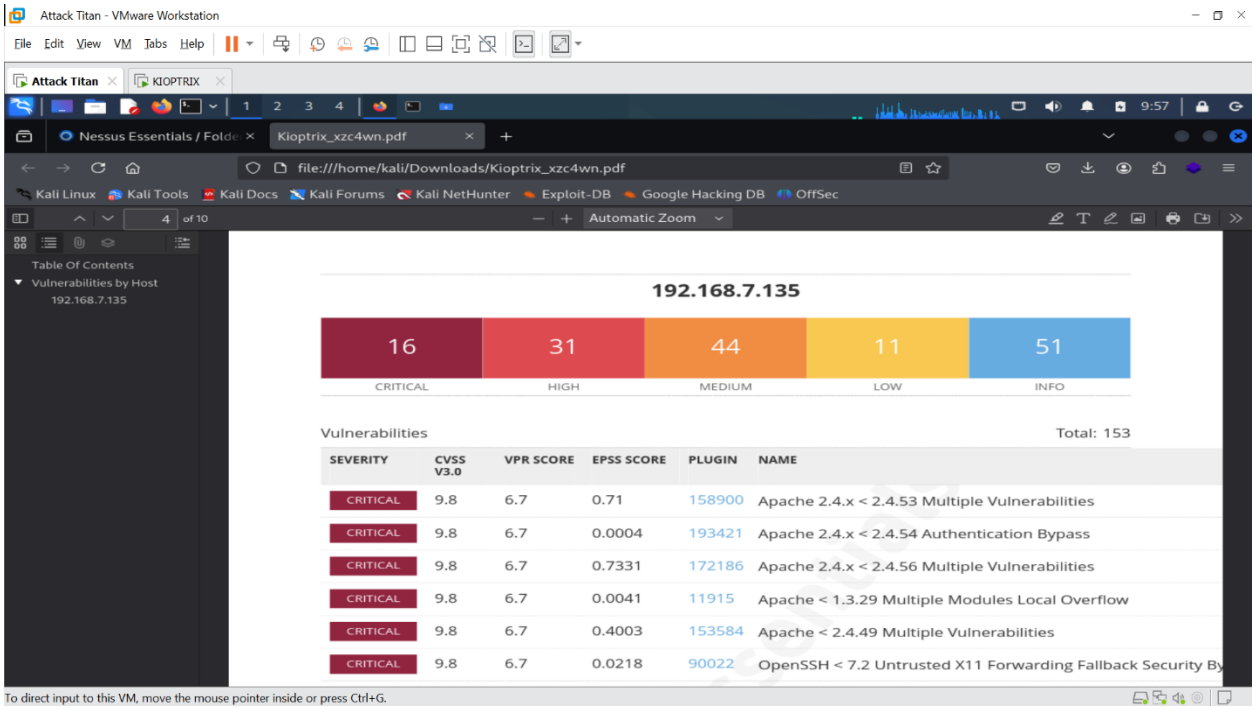
- Generated two types of reports:

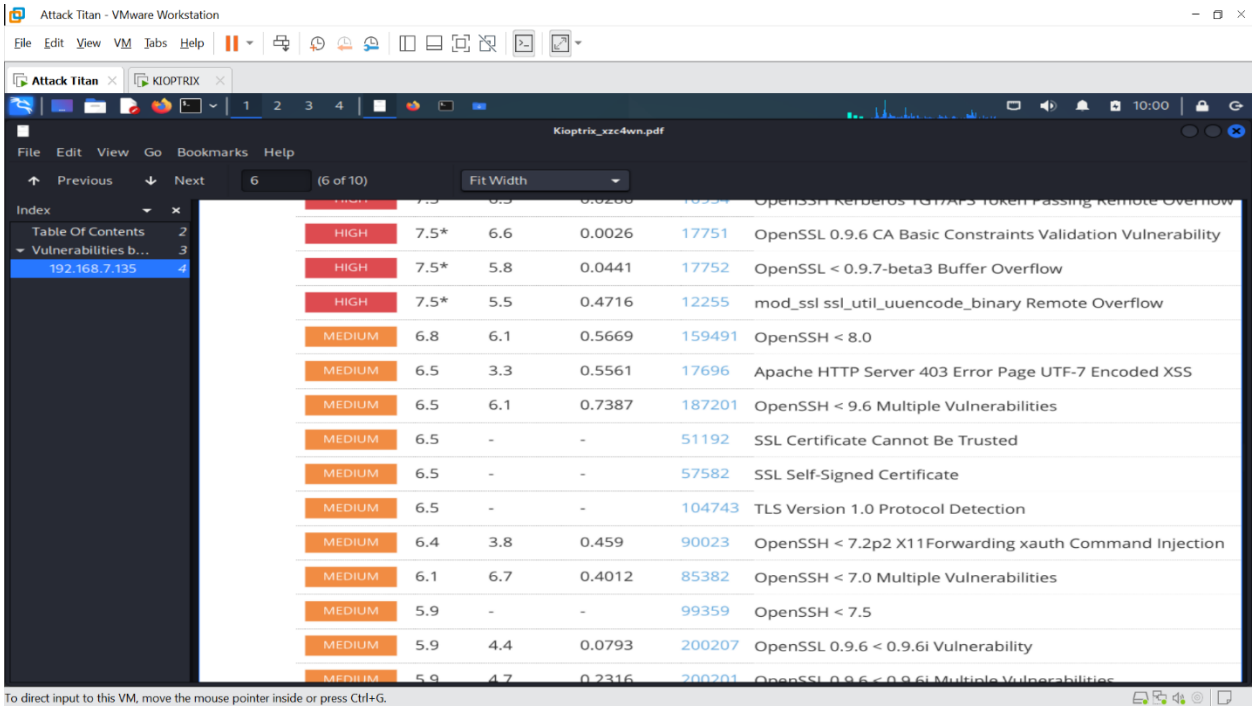
1. Summary Report – A brief overview of discovered vulnerabilities.



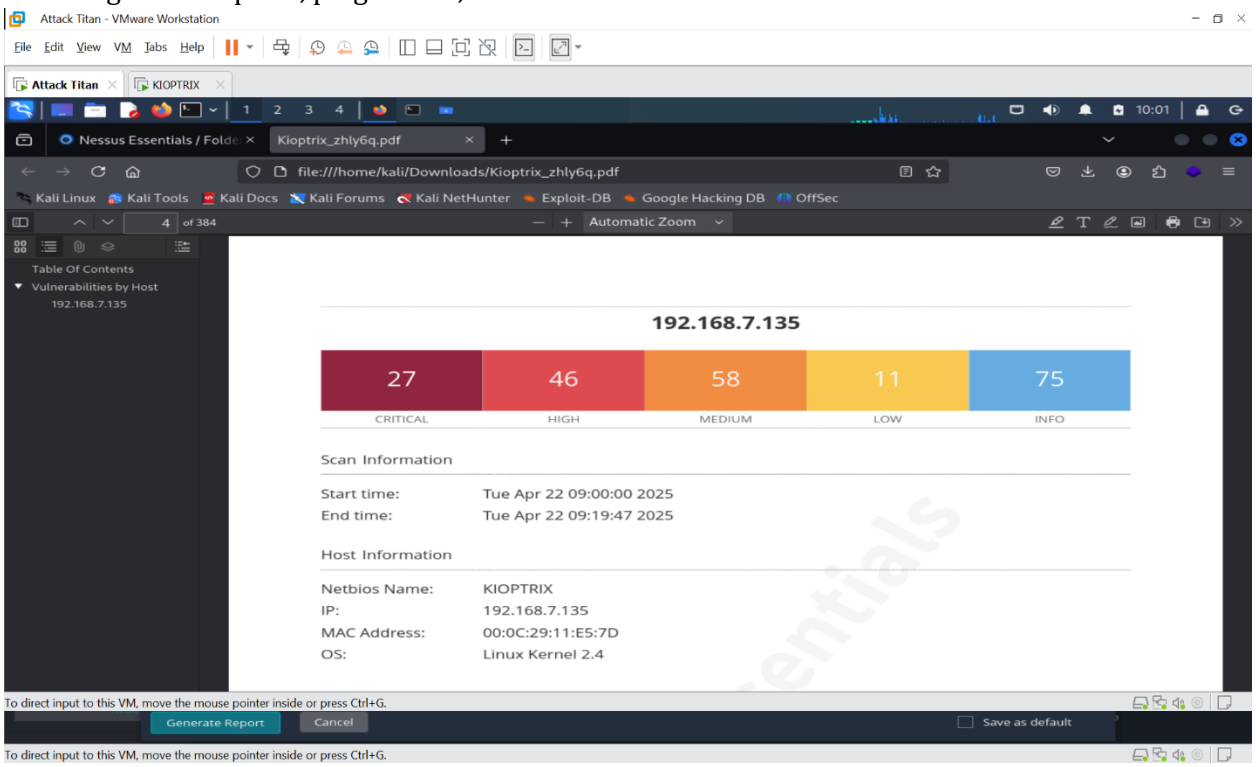

Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Folde
Kioptrix_xzc4wn.pdf
file:///home/kali/Downloads/Kioptrix_xzc4wn.pdf
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
1 of 10
Automatic Zoom
Table Of Contents
Vulnerabilities by Host
192.168.7.135
Kioptrix
Report generated by Tenable Nessus™
Tue, 22 Apr 2025 09:19:48 EDT
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

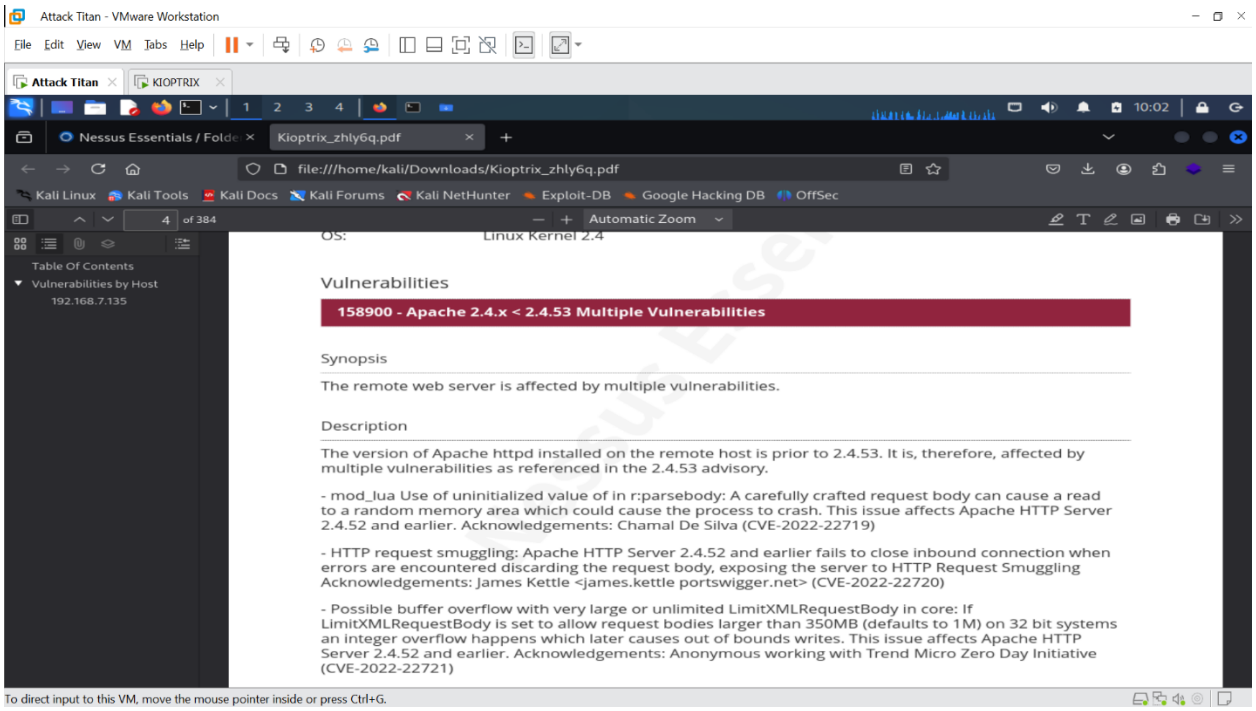

Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Folde
Kioptrix_xzc4wn.pdf
file:///home/kali/Downloads/Kioptrix_xzc4wn.pdf
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
2 of 10
Automatic Zoom
Table Of Contents
Vulnerabilities by Host
192.168.7.135
TABLE OF CONTENTS
Vulnerabilities by Host
192.168.7.135 4
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

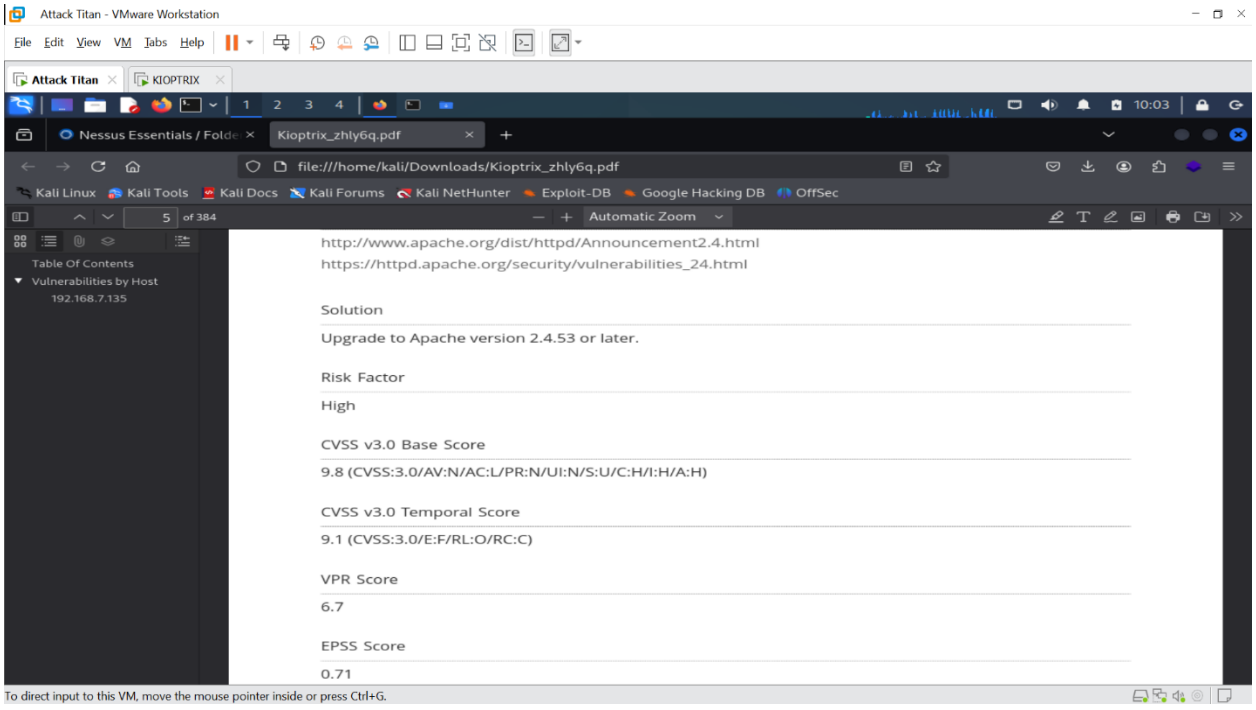

Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Folde
Kioptrix_xzc4wn.pdf
file:///home/kali/Downloads/Kioptrix_xzc4wn.pdf
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
4 of 10
Automatic Zoom
Table Of Contents
Vulnerabilities by Host
192.168.7.135
192.168.7.135
16 CRITICAL
31 HIGH
44 MEDIUM
11 LOW
51 INFO
Vulnerabilities
Total: 153
SEVERITY CVSS V3.0 VPR SCORE EPSS SCORE PLUGIN NAME
CRITICAL 9.8 6.7 0.71 158900 Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
CRITICAL 9.8 6.7 0.0004 193421 Apache 2.4.x < 2.4.54 Authentication Bypass
CRITICAL 9.8 6.7 0.7331 172186 Apache 2.4.x < 2.4.56 Multiple Vulnerabilities
CRITICAL 9.8 6.7 0.0041 11915 Apache < 1.3.29 Multiple Modules Local Overflow
CRITICAL 9.8 6.7 0.4003 153584 Apache < 2.4.49 Multiple Vulnerabilities
CRITICAL 9.8 6.7 0.0218 90022 OpenSSH < 7.2 Untrusted X11 Forwarding Fallback Security By
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Kioptrix_xzc4wn.pdf
File Edit View Go Bookmarks Help
Previous Next 6 (6 of 10) Fit Width
Index
Table Of Contents 2
Vulnerabilities b... 3
192.168.7.135 4
HIGH 7.5* 6.6 0.0026 17751 OpenSSL 0.9.6 CA Basic Constraints Validation Vulnerability
HIGH 7.5* 5.8 0.0441 17752 OpenSSL < 0.9.7-beta3 Buffer Overflow
HIGH 7.5* 5.5 0.4716 12255 mod_ssl ssl_util_uuencode_binary Remote Overflow
MEDIUM 6.8 6.1 0.5669 159491 OpenSSH < 8.0
MEDIUM 6.5 3.3 0.5561 17696 Apache HTTP Server 403 Error Page UTF-7 Encoded XSS
MEDIUM 6.5 6.1 0.7387 187201 OpenSSH < 9.6 Multiple Vulnerabilities
MEDIUM 6.5 - - 51192 SSL Certificate Cannot Be Trusted
MEDIUM 6.5 - - 57582 SSL Self-Signed Certificate
MEDIUM 6.5 - - 104743 TLS Version 1.0 Protocol Detection
MEDIUM 6.4 3.8 0.459 90023 OpenSSH < 7.2p2 X11Forwarding xauth Command Injection
MEDIUM 6.1 6.7 0.4012 85382 OpenSSH < 7.0 Multiple Vulnerabilities
MEDIUM 5.9 - - 99359 OpenSSH < 7.5
MEDIUM 5.9 4.4 0.0793 200207 OpenSSL 0.9.6 < 0.9.6i Vulnerability
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

2. Detailed Vulnerability Report by Host – In-depth information for each vulnerability, including affected ports, plugin used, and CVSS score.




Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Folde
Kioptrix_zhly6q.pdf
file:///home/kali/Downloads/Kioptrix_zhly6q.pdf
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
4 of 384
Automatic Zoom
Table Of Contents
Vulnerabilities by Host
192.168.7.135
OS: Linux Kernel 2.4
Vulnerabilities
158900 - Apache 2.4.x < 2.4.53 Multiple Vulnerabilities
Synopsis
The remote web server is affected by multiple vulnerabilities.
Description
The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.
- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)
- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)
- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Attack Titan - VMware Workstation
File Edit View VM Tabs Help
Attack Titan
KIOPTRIX
Nessus Essentials / Folde
Kioptrix_zhly6q.pdf
file:///home/kali/Downloads/Kioptrix_zhly6q.pdf
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
5 of 384
Automatic Zoom
Table Of Contents
Vulnerabilities by Host
192.168.7.135
http://www.apache.org/dist/httpd/Announcement2.4.html
https://httpd.apache.org/security/vulnerabilities_24.html
Solution
Upgrade to Apache version 2.4.53 or later.
Risk Factor
High
CVSS v3.0 Base Score
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVSS v3.0 Temporal Score
9.1 (CVSS:3.0/E:F/RL:O/RC:C)
VPR Score
6.7
EPSS Score
0.71
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Key Takeaways

- Nessus is a powerful and user-friendly tool for identifying vulnerabilities in a network.
- Proper scan configuration and understanding report details are essential for effective vulnerability management.
- This lab provided valuable hands-on experience in real-world vulnerability assessment techniques.