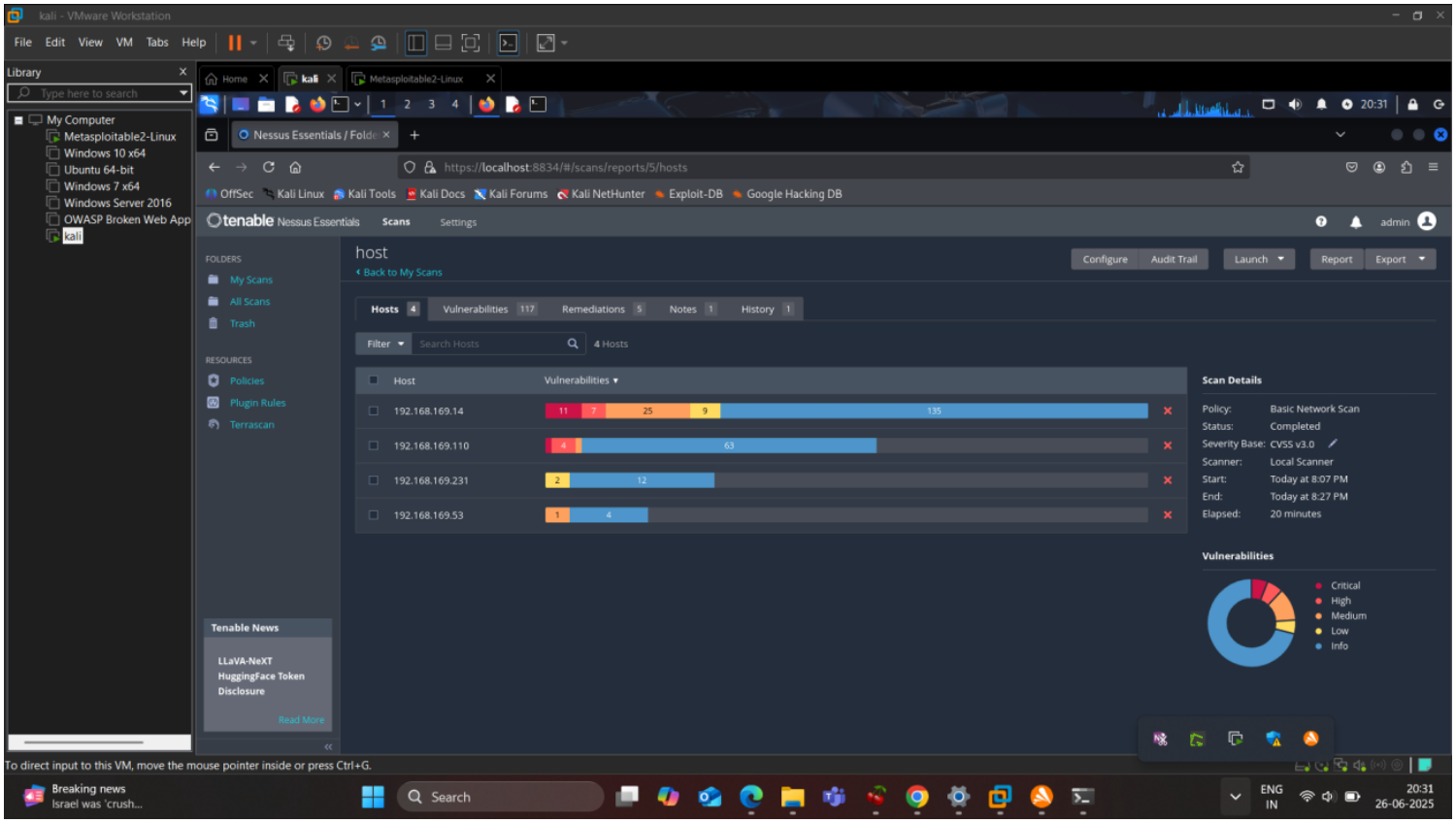
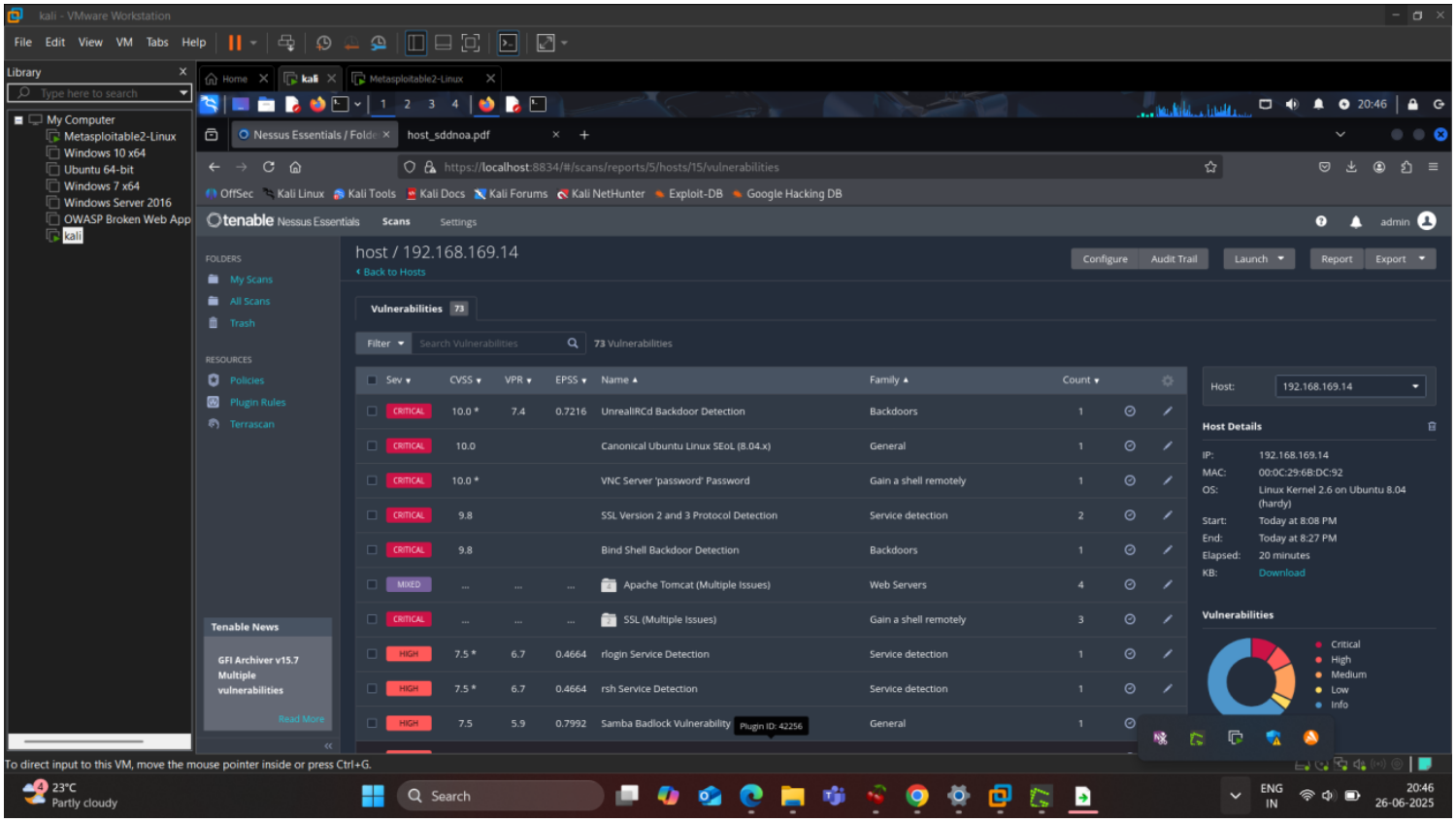
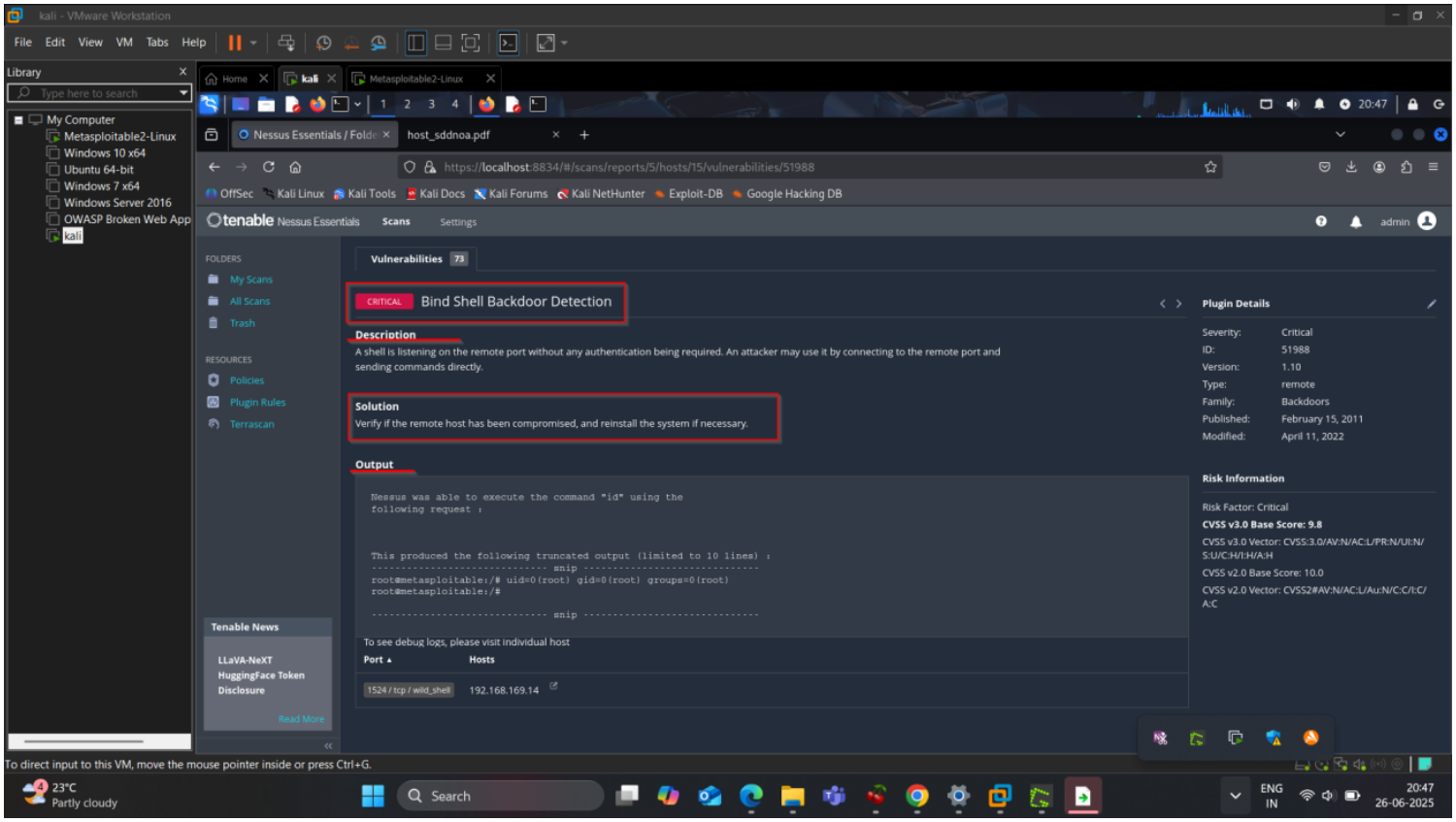
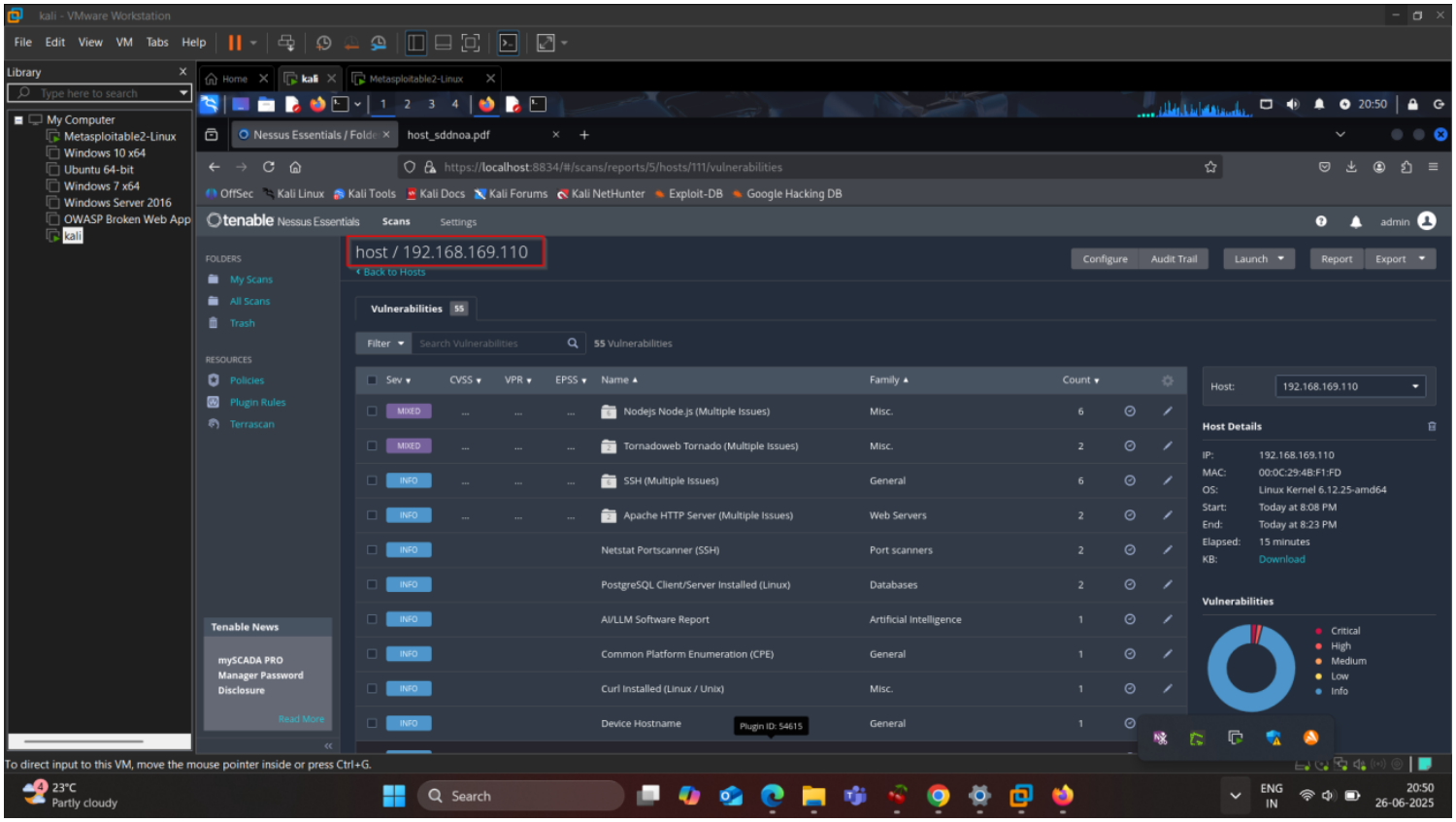
task3

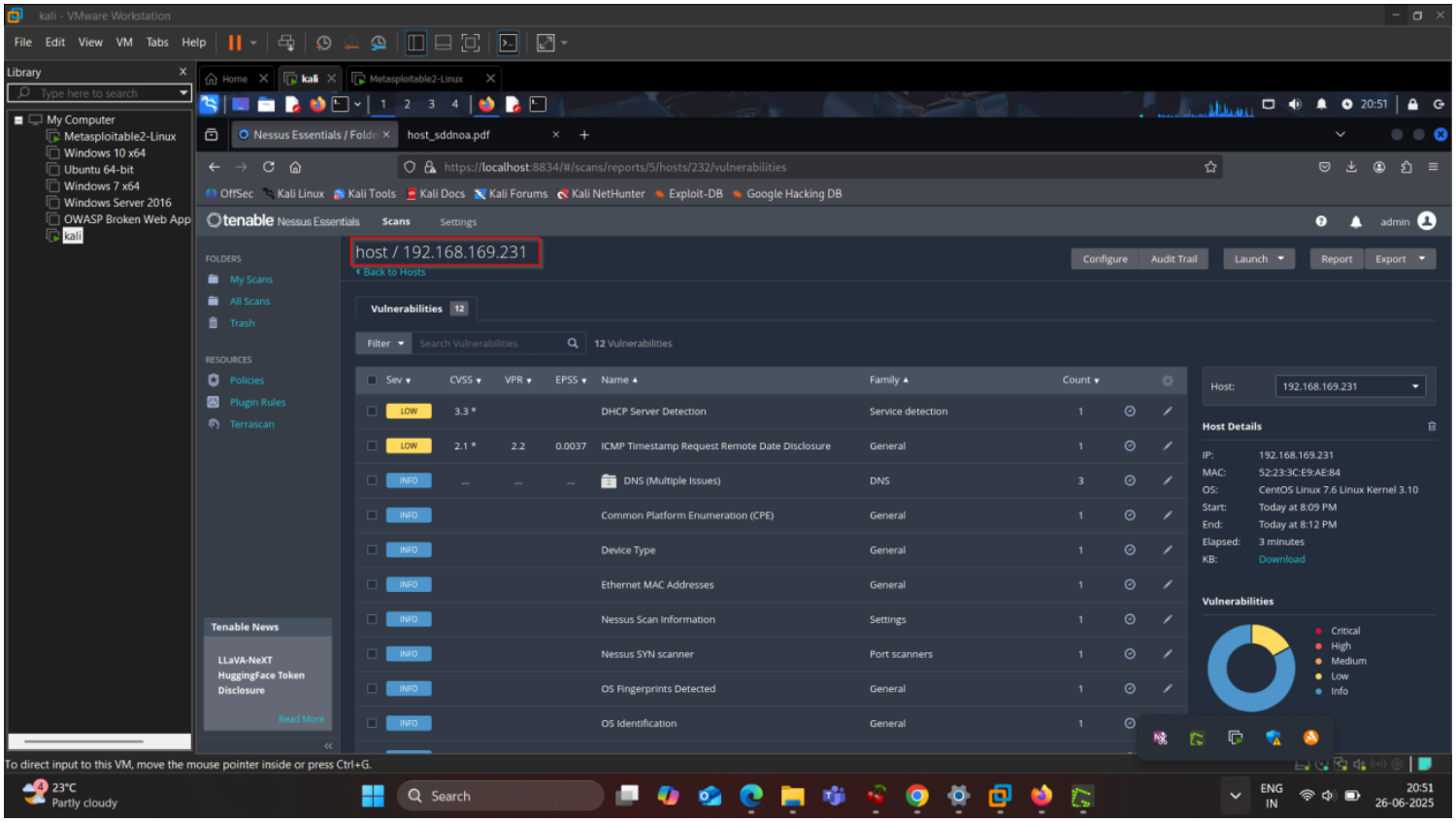
instaklled nessus and scanned sub net of own system

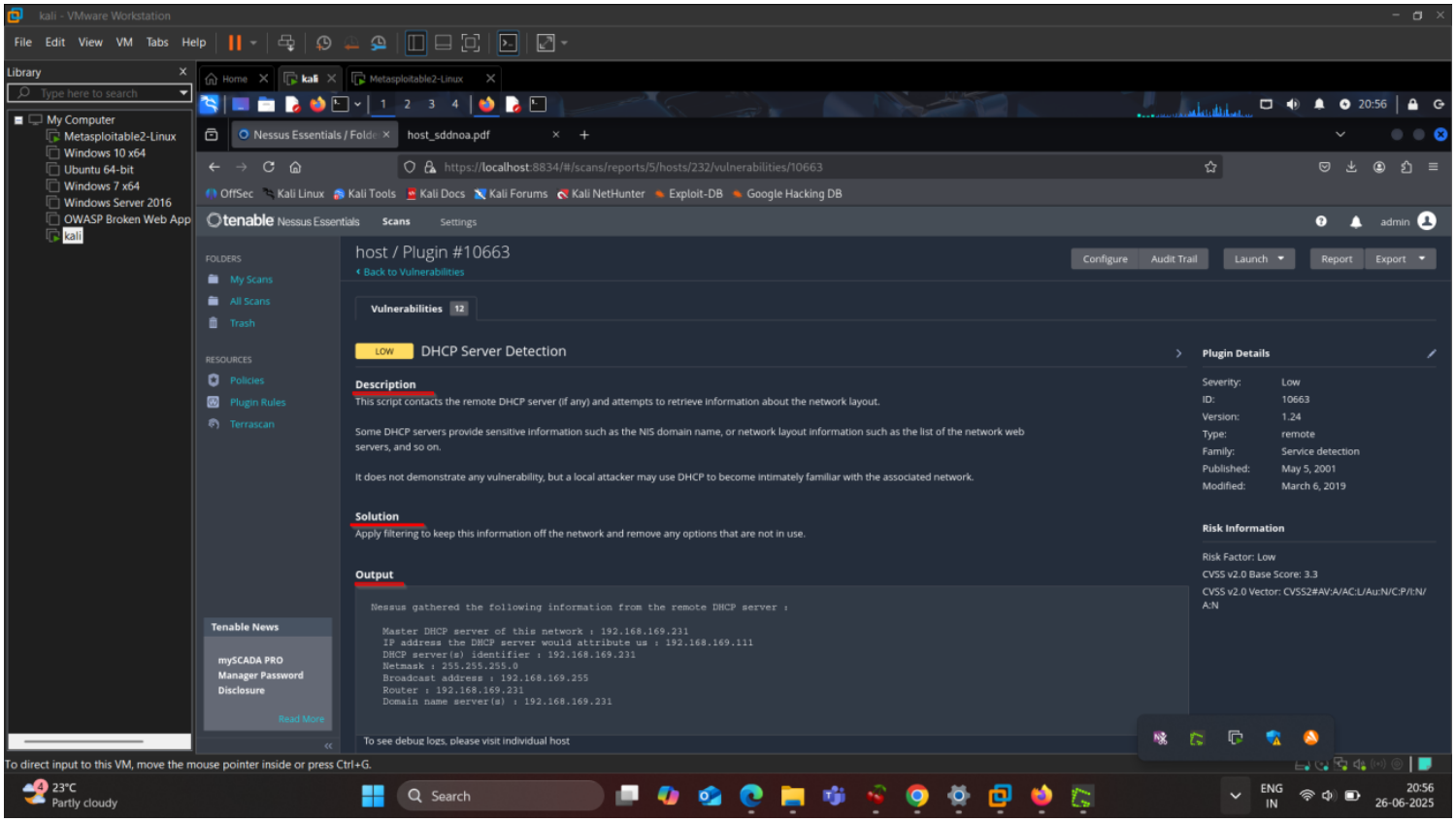


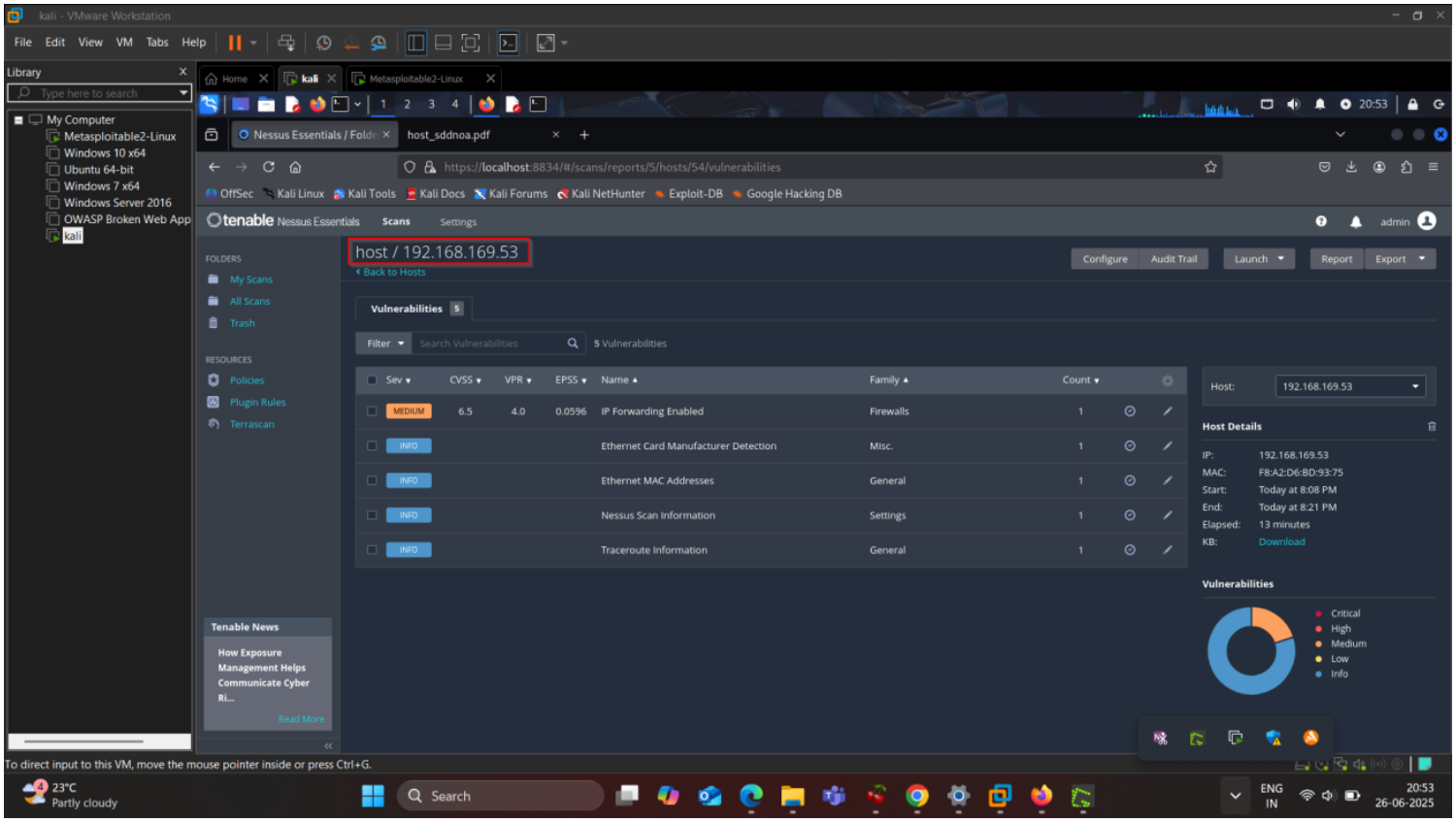

kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
Nessus Essentials / Folde
host_sddnoa.pdf
https://localhost:8834/#/scans/reports/5/hosts/15/vulnerabilities
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials Scans Settings admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
host / 192.168.169.14
Back to Hosts
Configure Audit Trail Launch Report Export
Vulnerabilities 73
Filter Search Vulnerabilities 73 Vulnerabilities
Sev CVSS VPR EPSS Name Family Count
CRITICAL 10.0 * 7.4 0.7216 UnrealIRCd Backdoor Detection Backdoors 1
CRITICAL 10.0 Canonical Ubuntu Linux SEoL (8.04.x) General 1
CRITICAL 10.0 * VNC Server 'password' Password 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 Apache Tomcat (Multiple Issues) Web Servers 4
CRITICAL SSL (Multiple Issues) Gain a shell remotely 3
HIGH 7.5 * 6.7 0.4664 rlogin Service Detection Service detection 1
HIGH 7.5 * 6.7 0.4664 rsh Service Detection Service detection 1
HIGH 7.5 5.9 0.7992 Samba Badlock Vulnerability Plugin ID: 42256 General 1
Host: 192.168.169.14
Host Details
IP: 192.168.169.14
MAC: 00:0C:29:6B:DC:92
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 8:08 PM
End: Today at 8:27 PM
Elapsed: 20 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
GFI Archiver v15.7 Multiple vulnerabilities
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C Partly cloudy
Search
ENG IN
20:46 26-06-2025

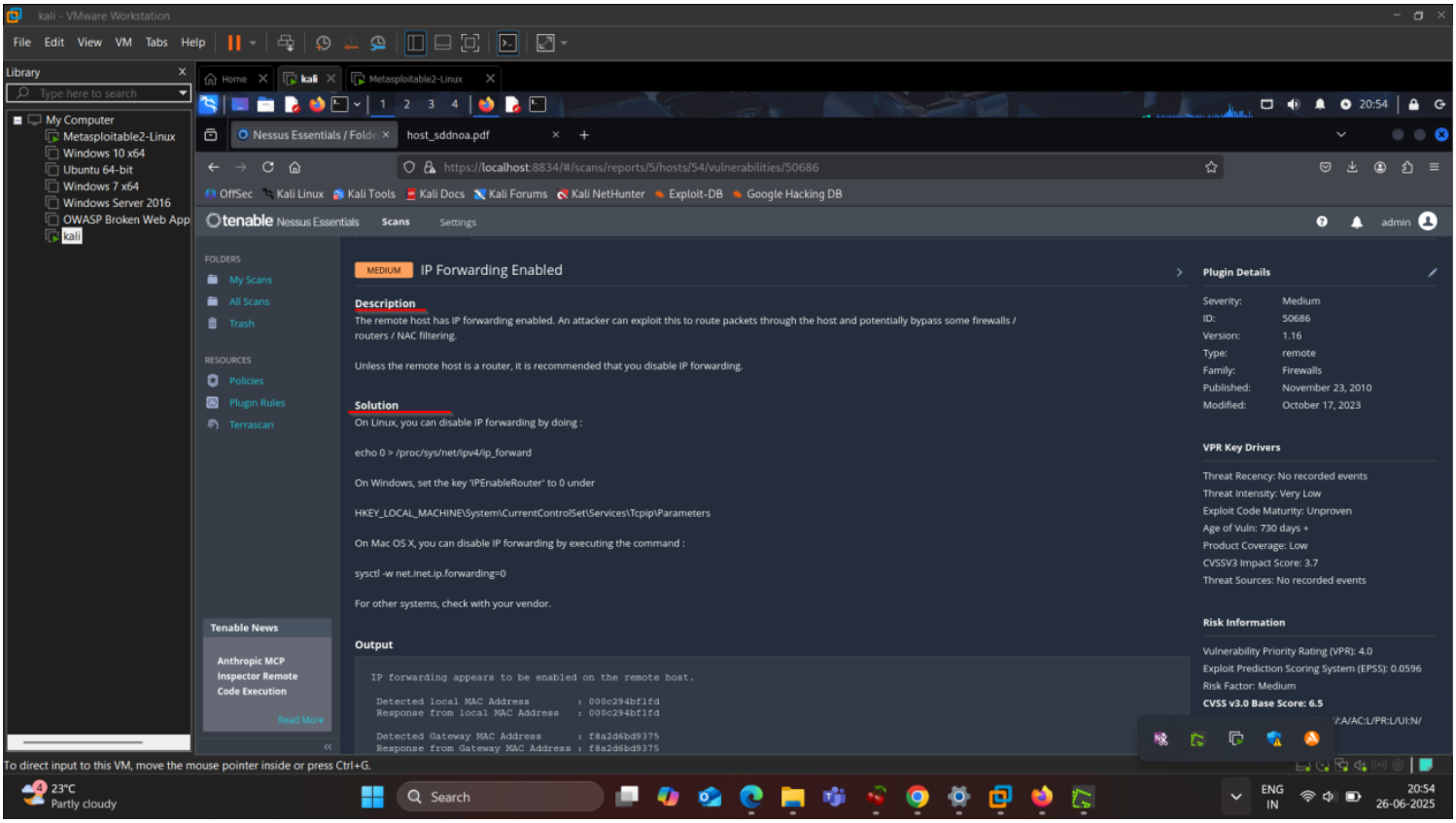

kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
Nessus Essentials / Folde
host_sddnoa.pdf
https://localhost:8834/#/scans/reports/5/hosts/15/vulnerabilities/51988
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials Scans Settings admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Vulnerabilities 73
CRITICAL Bind Shell Backdoor Detection
Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.
Output
Nessus was able to execute the command "id" using the following request :
This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
------------------------------ snip ------------------------------
To see debug logs, please visit individual host
Port Hosts
1524 / tcp / wild_shell 192.168.169.14
Plugin Details
Severity: Critical
ID: 51988
Version: 1.10
Type: remote
Family: Backdoors
Published: February 15, 2011
Modified: April 11, 2022
Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Tenable News
LLaVA-NeXT HuggingFace Token Disclosure
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C Partly cloudy
Search
ENG IN
20:47 26-06-2025


kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
Nessus Essentials / Folde
host_sddnoa.pdf
https://localhost:8834/#/scans/reports/5/hosts/111/vulnerabilities
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
admin
host / 192.168.169.110
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Vulnerabilities 55
Filter
Search Vulnerabilities
55 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MIXED Nodejs Node.js (Multiple Issues) Misc. 6
MIXED Tornadoweb Tornado (Multiple Issues) Misc. 2
INFO SSH (Multiple Issues) General 6
INFO Apache HTTP Server (Multiple Issues) Web Servers 2
INFO Netstat Portscanner (SSH) Port scanners 2
INFO PostgreSQL Client/Server Installed (Linux) Databases 2
INFO AI/LLM Software Report Artificial Intelligence 1
INFO Common Platform Enumeration (CPE) General 1
INFO Curl Installed (Linux / Unix) Misc. 1
INFO Device Hostname General 1
Plugin ID: 54615
Host: 192.168.169.110
Host Details
IP: 192.168.169.110
MAC: 00:0C:29:4B:F1:FD
OS: Linux Kernel 6.12.25-amd64
Start: Today at 8:08 PM
End: Today at 8:23 PM
Elapsed: 15 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
mySCADA PRO Manager Password Disclosure
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C Partly cloudy
Search
ENG IN
20:50 26-06-2025


kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
Nessus Essentials / Folde
host_sddnoa.pdf
https://localhost:8834/#/scans/reports/5/hosts/232/vulnerabilities
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
admin
host / 192.168.169.231
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Vulnerabilities 12
Filter
Search Vulnerabilities
12 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
LOW 3.3 * DHCP Server Detection Service detection 1
LOW 2.1 * 2.2 0.0037 ICMP Timestamp Request Remote Date Disclosure General 1
INFO DNS (Multiple Issues) DNS 3
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Ethernet MAC Addresses General 1
INFO Nessus Scan Information Settings 1
INFO Nessus SYN scanner Port scanners 1
INFO OS Fingerprints Detected General 1
INFO OS Identification General 1
Host: 192.168.169.231
Host Details
IP: 192.168.169.231
MAC: 52:23:3C:E9:AE:84
OS: CentOS Linux 7.6 Linux Kernel 3.10
Start: Today at 8:09 PM
End: Today at 8:12 PM
Elapsed: 3 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
LLaVA-NeXT HuggingFace Token Disclosure
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C Partly cloudy
Search
ENG IN
20:51 26-06-2025


kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
host_sddnoa.pdf
https://localhost:8834/#/scans/reports/5/hosts/232/vulnerabilities/10663
tenable Nessus Essentials
Scans
Settings
admin
host / Plugin #10663
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 12
LOW
DHCP Server Detection
Description
This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout.
Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on.
It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.
Solution
Apply filtering to keep this information off the network and remove any options that are not in use.
Output
Nessus gathered the following information from the remote DHCP server :
Master DHCP server of this network : 192.168.169.231
IP address the DHCP server would attribute us : 192.168.169.111
DHCP server(s) identifier : 192.168.169.231
Netmask : 255.255.255.0
Broadcast address : 192.168.169.255
Router : 192.168.169.231
Domain name server(s) : 192.168.169.231
To see debug logs, please visit individual host
Plugin Details
Severity: Low
ID: 10663
Version: 1.24
Type: remote
Family: Service detection
Published: May 5, 2001
Modified: March 6, 2019
Risk Information
Risk Factor: Low
CVSS v2.0 Base Score: 3.3
CVSS v2.0 Vector: CVSS2#AV:A/AC:L/Au:N/C:P/I:N/A:N
Tenable News
mySCADA PRO Manager Password Disclosure
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C
Partly cloudy
Search
ENG
IN
20:56
26-06-2025


kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
host_sddnoa.pdf
https://localhost:8834/#/scans/reports/5/hosts/54/vulnerabilities
tenable Nessus Essentials
Scans
Settings
admin
host / 192.168.169.53
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 5
Filter
Search Vulnerabilities
5 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
MEDIUM 6.5 4.0 0.0596 IP Forwarding Enabled Firewalls 1
INFO Ethernet Card Manufacturer Detection Misc. 1
INFO Ethernet MAC Addresses General 1
INFO Nessus Scan Information Settings 1
INFO Traceroute Information General 1
Host: 192.168.169.53
Host Details
IP: 192.168.169.53
MAC: F8:A2:D6:BD:93:75
Start: Today at 8:08 PM
End: Today at 8:21 PM
Elapsed: 13 minutes
KB: Download
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
How Exposure Management Helps Communicate Cyber Ri...
Read More
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C
Partly cloudy
Search
ENG
IN
20:53
26-06-2025


kali - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Metasploitable2-Linux
Windows 10 x64
Ubuntu 64-bit
Windows 7 x64
Windows Server 2016
OWASP Broken Web App
kali
Nessus Essentials / Folde
host_sddnoa.pdf
https://localhost:8834/#/scans/reports/5/hosts/54/vulnerabilities/50686
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Anthropic MCP Inspector Remote Code Execution
Read More
MEDIUM
IP Forwarding Enabled
Description
The remote host has IP forwarding enabled. An attacker can exploit this to route packets through the host and potentially bypass some firewalls / routers / NAC filtering.
Unless the remote host is a router, it is recommended that you disable IP forwarding.
Solution
On Linux, you can disable IP forwarding by doing :
echo 0 > /proc/sys/net/ipv4/ip_forward
On Windows, set the key 'IPEnableRouter' to 0 under
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters
On Mac OS X, you can disable IP forwarding by executing the command :
sysctl -w net.inet.ip.forwarding=0
For other systems, check with your vendor.
Output
IP forwarding appears to be enabled on the remote host.
Detected local MAC Address : 000c294bf1fd
Response from local MAC Address : 000c294bf1fd
Detected Gateway MAC Address : f8a2d6bd9375
Response from Gateway MAC Address : f8a2d6bd9375
Plugin Details
Severity: Medium
ID: 50686
Version: 1.16
Type: remote
Family: Firewalls
Published: November 23, 2010
Modified: October 17, 2023
VPR Key Drivers
Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Low
CVSSV3 Impact Score: 3.7
Threat Sources: No recorded events
Risk Information
Vulnerability Priority Rating (VPR): 4.0
Exploit Prediction Scoring System (EPSS): 0.0596
Risk Factor: Medium
CVSS v3.0 Base Score: 6.5
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C Partly cloudy
Search
ENG IN
20:54 26-06-2025