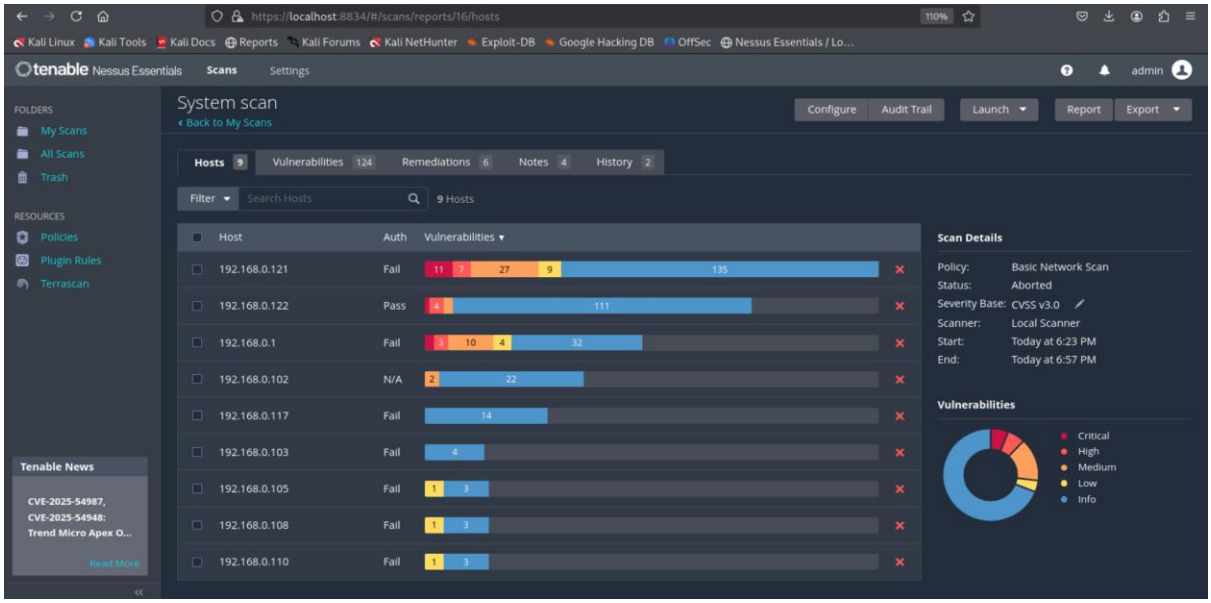
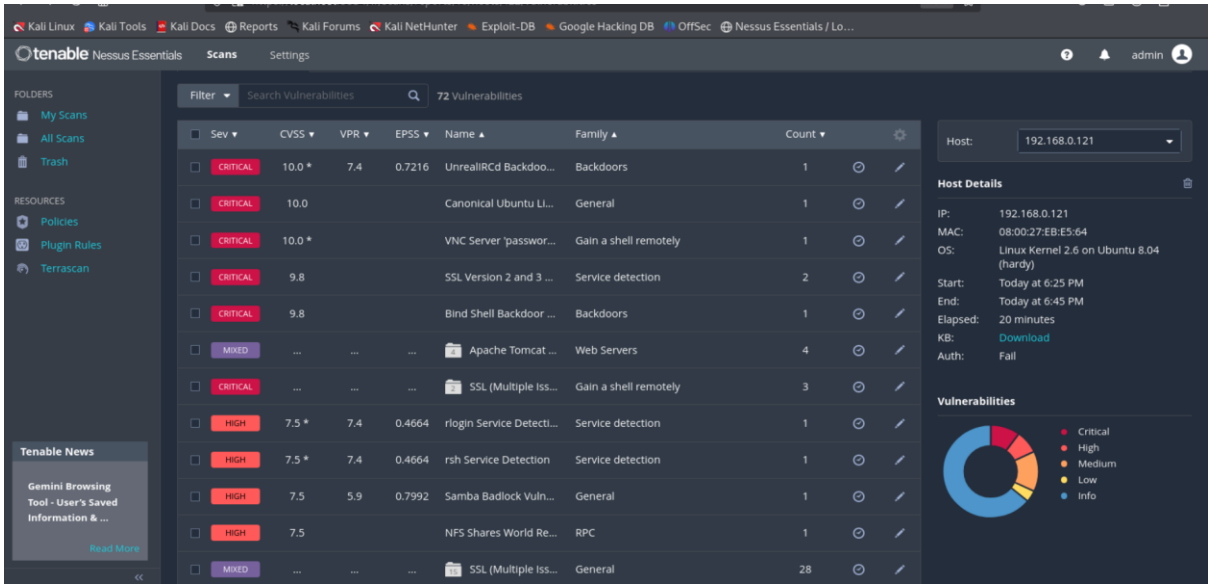
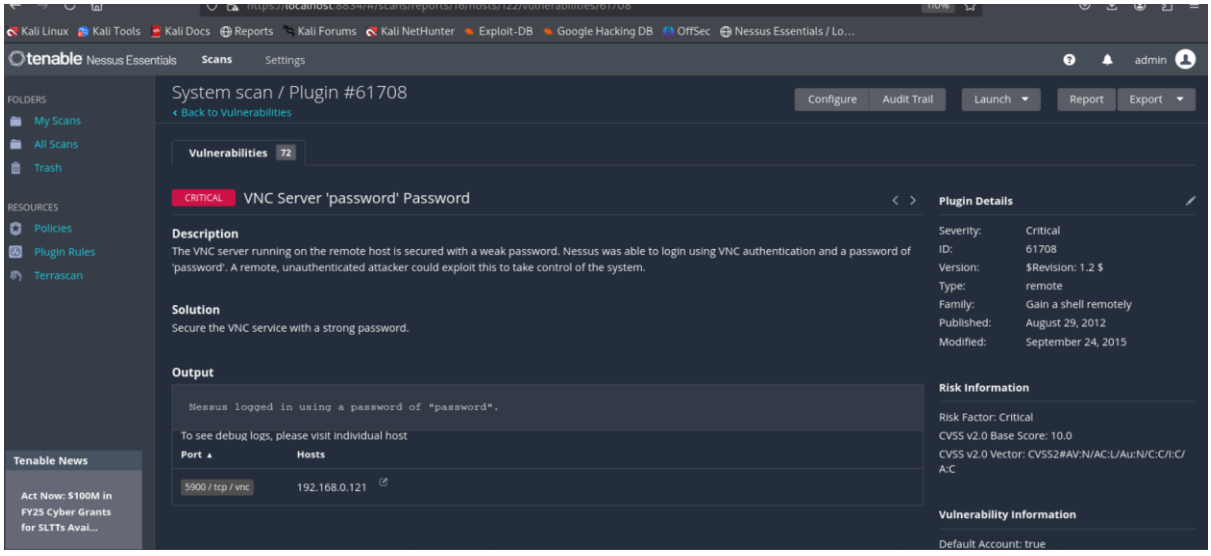

https://localhost:8834/#/scans/reports/16/hosts
Kali Linux Kali Tools Kali Docs Reports Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Lo...
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
CVE-2025-54987, CVE-2025-54948: Trend Micro Apex O...
Read More
System scan
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 9
Vulnerabilities 124
Remediations 6
Notes 4
History 2
Filter
Search Hosts
9 Hosts
Host
Auth
Vulnerabilities
192.168.0.121 Fail 11 7 27 9 135
192.168.0.122 Pass 4 111
192.168.0.1 Fail 3 10 4 32
192.168.0.102 N/A 2 22
192.168.0.117 Fail 14
192.168.0.103 Fail 4
192.168.0.105 Fail 1 3
192.168.0.108 Fail 1 3
192.168.0.110 Fail 1 3
Scan Details
Policy: Basic Network Scan
Status: Aborted
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:23 PM
End: Today at 6:57 PM
Vulnerabilities
Critical
High
Medium
Low
Info


Kali Linux Kali Tools Kali Docs Reports Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Lo...
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Gemini Browsing Tool - User's Saved Information & ...
Read More
Filter
Search Vulnerabilities
72 Vulnerabilities
Sev
CVSS
VPR
EPSS
Name
Family
Count
CRITICAL 10.0 * 7.4 0.7216 UnrealIRCd Backdoo... Backdoors 1
CRITICAL 10.0 Canonical Ubuntu Li... General 1
CRITICAL 10.0 * VNC Server 'passwor... Gain a shell remotely 1
CRITICAL 9.8 SSL Version 2 and 3 ... Service detection 2
CRITICAL 9.8 Bind Shell Backdoor ... Backdoors 1
MIXED Apache Tomcat ... Web Servers 4
CRITICAL SSL (Multiple Iss... Gain a shell remotely 3
HIGH 7.5 * 7.4 0.4664 rlogin Service Detecti... Service detection 1
HIGH 7.5 * 7.4 0.4664 rsh Service Detection Service detection 1
HIGH 7.5 5.9 0.7992 Samba Badlock Vuln... General 1
HIGH 7.5 NFS Shares World Re... RPC 1
MIXED SSL (Multiple Iss... General 28
Host: 192.168.0.121
Host Details
IP: 192.168.0.121
MAC: 08:00:27:EB:E5:64
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 6:25 PM
End: Today at 6:45 PM
Elapsed: 20 minutes
KB: Download
Auth: Fail
Vulnerabilities
Critical
High
Medium
Low
Info


Kali Linux Kali Tools Kali Docs Reports Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Lo...
tenable Nessus Essentials
Scans
Settings
admin
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Act Now: $100M in FY25 Cyber Grants for SLTTs Avai...
System scan / Plugin #61708
Back to Vulnerabilities
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 72
CRITICAL VNC Server 'password' Password
Description
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.
Solution
Secure the VNC service with a strong password.
Output
Nessus logged in using a password of "password".
To see debug logs, please visit individual host
Port
Hosts
5900 / tcp / vnc 192.168.0.121
Plugin Details
Severity: Critical
ID: 61708
Version: $Revision: 1.2 $
Type: remote
Family: Gain a shell remotely
Published: August 29, 2012
Modified: September 24, 2015
Risk Information
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
Vulnerability Information
Default Account: true


UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:145 errors:0 dropped:0 overruns:0 frame:0
TX packets:67 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:14805 (14.4 KB) TX bytes:7498 (7.3 KB)
Base address:0xd020 Memory:f0200000-f0220000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:105 errors:0 dropped:0 overruns:0 frame:0
TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:25617 (25.0 KB) TX bytes:25617 (25.0 KB)
msfadmin@metasploitable:~$ vncpassswd
-bash: vncpassswd: command not found
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
msfadmin@metasploitable:~$