Lab Report

CSE451, Computer and Networks Security

Name: Ahmed Khaled Saad Ali Mekheimer ID: 1809799

Lab No: (5) Experiment Title: Vulnerability Scanning Using OpenVAS

Date: 8 / 12 /2022

1. Screenshots

Machine	IP
Linux Kali	192.168.11.134
Windows Server 2016	192.168.11.135
Linux Metasploit	192.168.11.136

- Introduction

Install and setup of gvm (OpenVAS)

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/home/kali]
└─# sudo gvm-setup
[>] Starting PostgreSQL service

[>] Creating GVM's certificate files

[>] Creating PostgreSQL database
could not change directory to "/home/kali": Permission denied
[i] User _gvm already exists in PostgreSQL
could not change directory to "/home/kali": Permission denied
[i] Database gvmd already exists in PostgreSQL
could not change directory to "/home/kali": Permission denied
[i] Role DBA already exists in PostgreSQL

[*] Applying permissions
could not change directory to "/home/kali": Permission denied
NOTICE:  role "_gvm" is already a member of role "dba"
GRANT ROLE
could not change directory to "/home/kali": Permission denied
[i] Extension uuid-ossp already exists for gvmd database
could not change directory to "/home/kali": Permission denied
[i] Extension pgcrypto already exists for gvmd database
could not change directory to "/home/kali": Permission denied
[i] Extension pg-gvm already exists for gvmd database
[>] Migrating database

(gvmd:24839): md manage-WARNING **: 14:55:09.254: sql_exec_internal: PQexec failed
ted
 (7)

(gvmd:24839): md manage-WARNING **: 14:55:09.254: sql_exec_internal: SQL: CREATE O
on_str () RETURNS text AS $$ WITH pref_str AS (   SELECT name,          substring(
 substring (name, '^.*?:([^:]+):') AS pref_id,          (substring (name, '^.*?:([
name,                        '^[^:]*:[^:]*:[^:]*:(.*)')           || value) AS pr
```

```
File  Actions  Edit  View  Help
sent 71 bytes  received 111 bytes  121.33 bytes/sec
total size is 13  speedup is 0.07
[*] Updating Cert Data
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.

receiving incremental file list
timestamp
             13 100%    6.35kB/s    0:00:00 (xfr#1, to-chk=0/1)

sent 71 bytes  received 111 bytes  121.33 bytes/sec
total size is 13  speedup is 0.07

[+] GVM feeds updated
[*] Checking Default scanner
08b69003-5fc2-4037-a479-93b440211c73  OpenVAS  /run/ospd/ospd.sock  0  OpenVAS Def
[i] No need to alter default scanner

[+] Done
[i] Admin user already exists for GVM
[i] If you have forgotten it, you can change it. See gvmd manpage for more informa

[>] You can now run gvm-check-setup to make sure everything is correctly configure
```

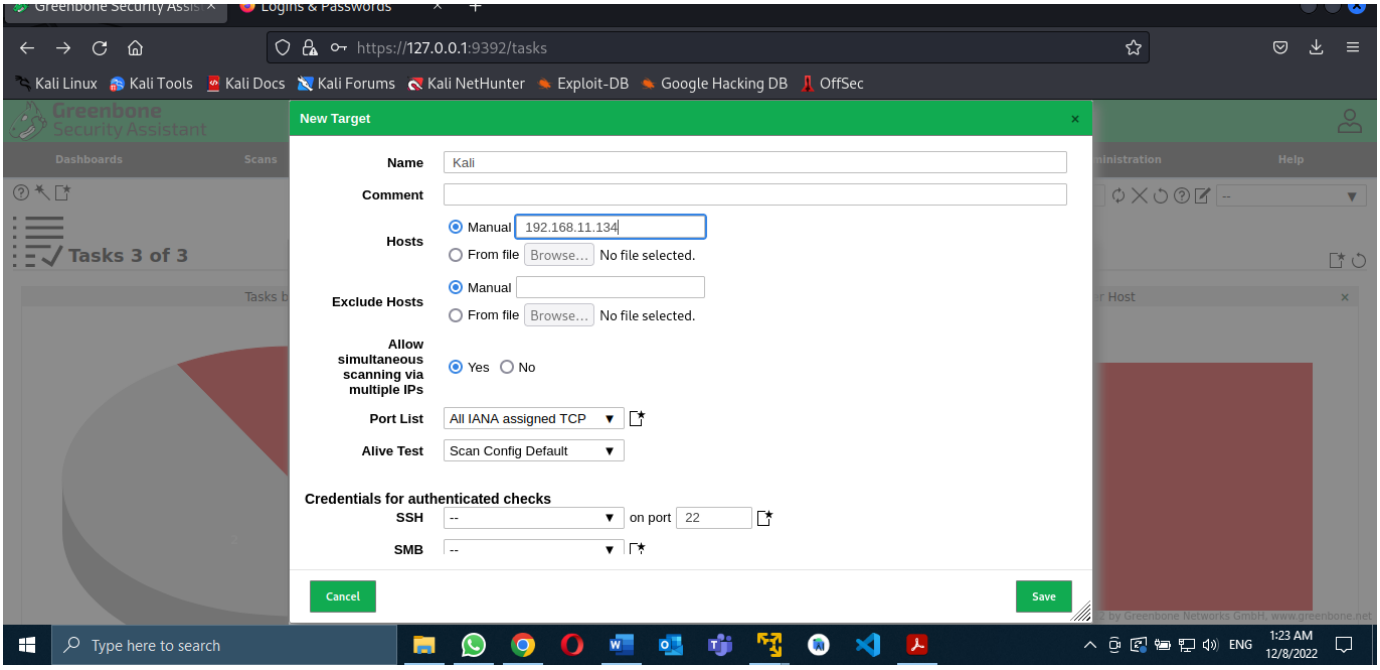
```
kali@kali: ~
File  Actions  Edit  View  Help

[+] GVM feeds updated
[*] Checking Default scanner
[*] Modifying Default Scanner
Scanner modified.

[+] Done
[*] Please note the password for the admin user
[*] User created with password '5e614e37-5d8b-4549-aafb-27bf745ac635'.

[>] You can now run gvm-check-setup to make sure everything is correctly configured

┌──(kali㉿kali)-[~]
└─$ sudo apt install gvm -y
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
gvm is already the newest version (22.4.0+kali4).
gvm set to manually installed.
The following package was automatically installed and is no longer required:
  python-pastedeploy-tpl
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

┌──(kali㉿kali)-[~]
└─$ sudo gvm-check-setup
gvm-check-setup 22.4.0
  Test completeness and readiness of GVM-22.4.0
Step 1: Checking OpenVAS (Scanner) ...
        OK: OpenVAS Scanner is present in version 22.4.0.
```

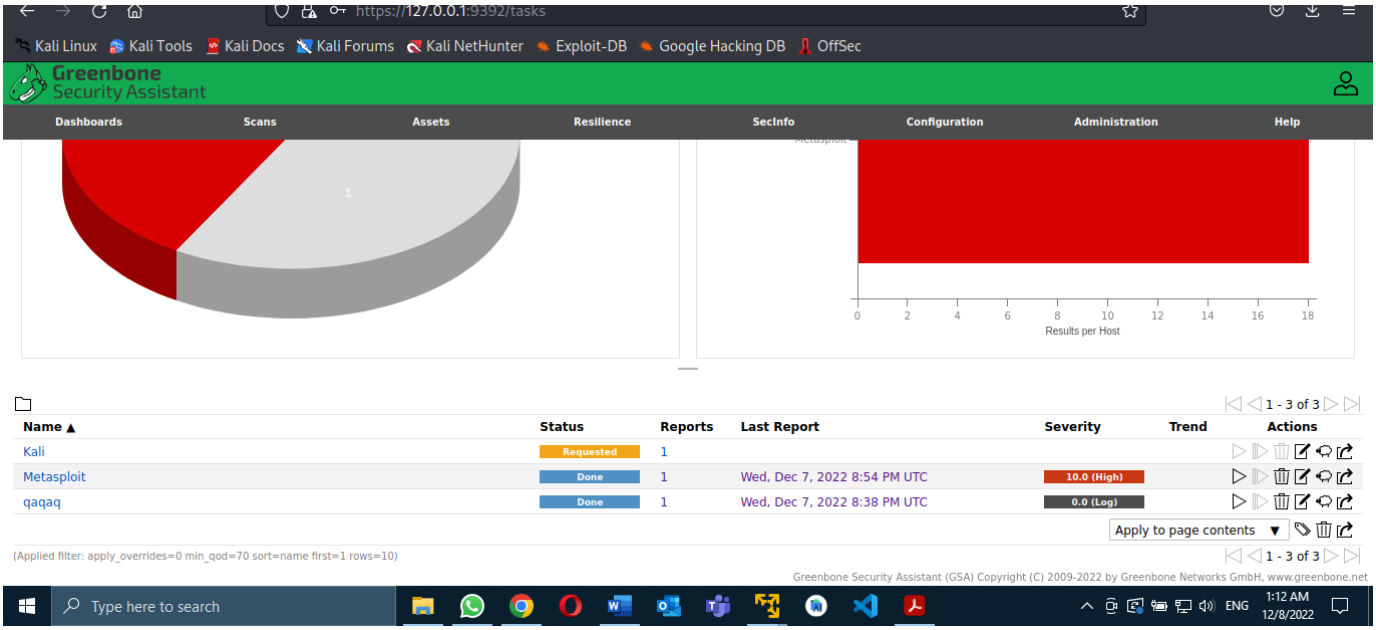
```
kali@kali: ~
File  Actions  Edit  View  Help
 Microsoft Windows targets will not work.
        SUGGEST: Install nsis.
        OK: xsltproc found.
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/gvm/pwpolicy.conf file to set a password policy.

It seems like your GVM-22.4.0 installation is OK.


┌──(kali㉿kali)-[~]
└─$ sudo runuser -u _gvm - gvmd - create-user=<Ahmed> - password=<11Ahmed5599>
zsh: parse error near `\n'

┌──(kali㉿kali)-[~]
└─$ sudo runuser -u _gvm -- gvmd --create-user=Ahmed --password=11Ahmed5599
User created.

┌──(kali㉿kali)-[~]
└─$ sudo gvm-check-setup
gvm-check-setup 22.4.0
  Test completeness and readiness of GVM-22.4.0
Step 1: Checking OpenVAS (Scanner)...
        OK: OpenVAS Scanner is present in version 22.4.0.
        OK: Notus Scanner is present in version 22.4.1.
        OK: Server CA Certificate is present as /var/lib/gvm/CA/servercert.pem.
Checking permissions of /var/lib/openvas/gnupg/*
        OK: _gvm owns all files in /var/lib/openvas/gnupg
        OK: redis-server is present.
        OK: scanner (db_address setting) is configured properly using the redis-server
 socket: /var/run/redis-openvas/redis-server.sock
        OK: redis-server is running and listening on socket: /var/run/redis-openvas/re
```

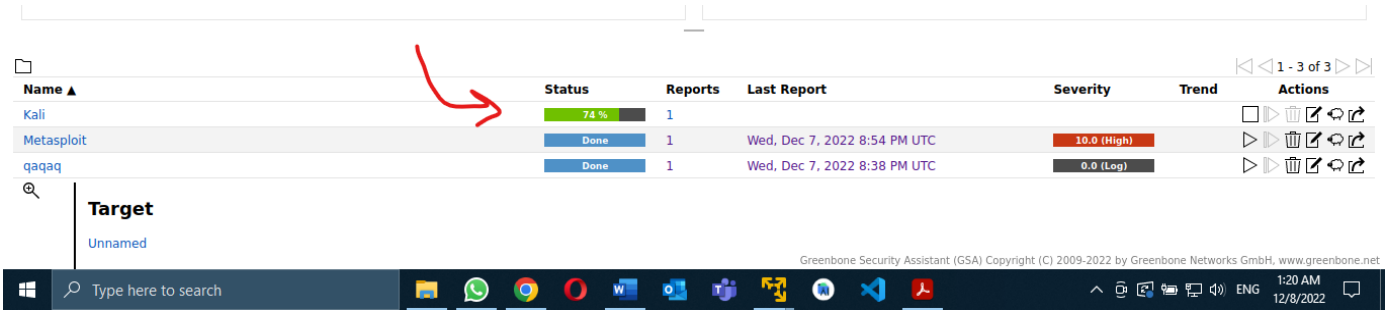
ENG 5:57 PM 12/7/2022

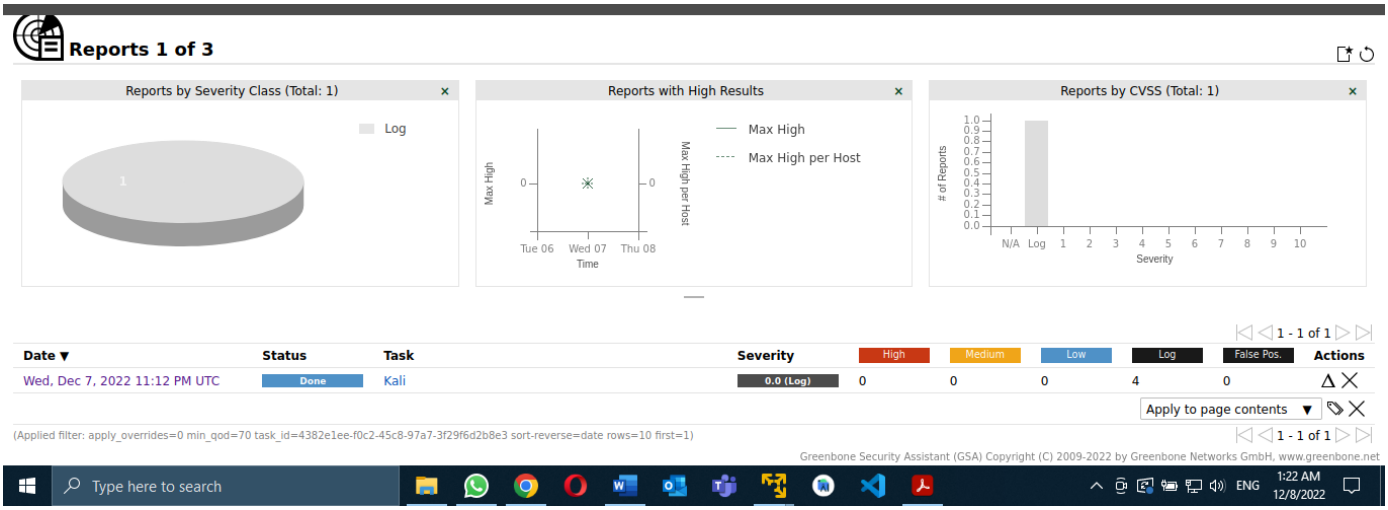
- Scanning Target for vulnerabilities

Task Scanning Kali Machine (192.168.11.134)

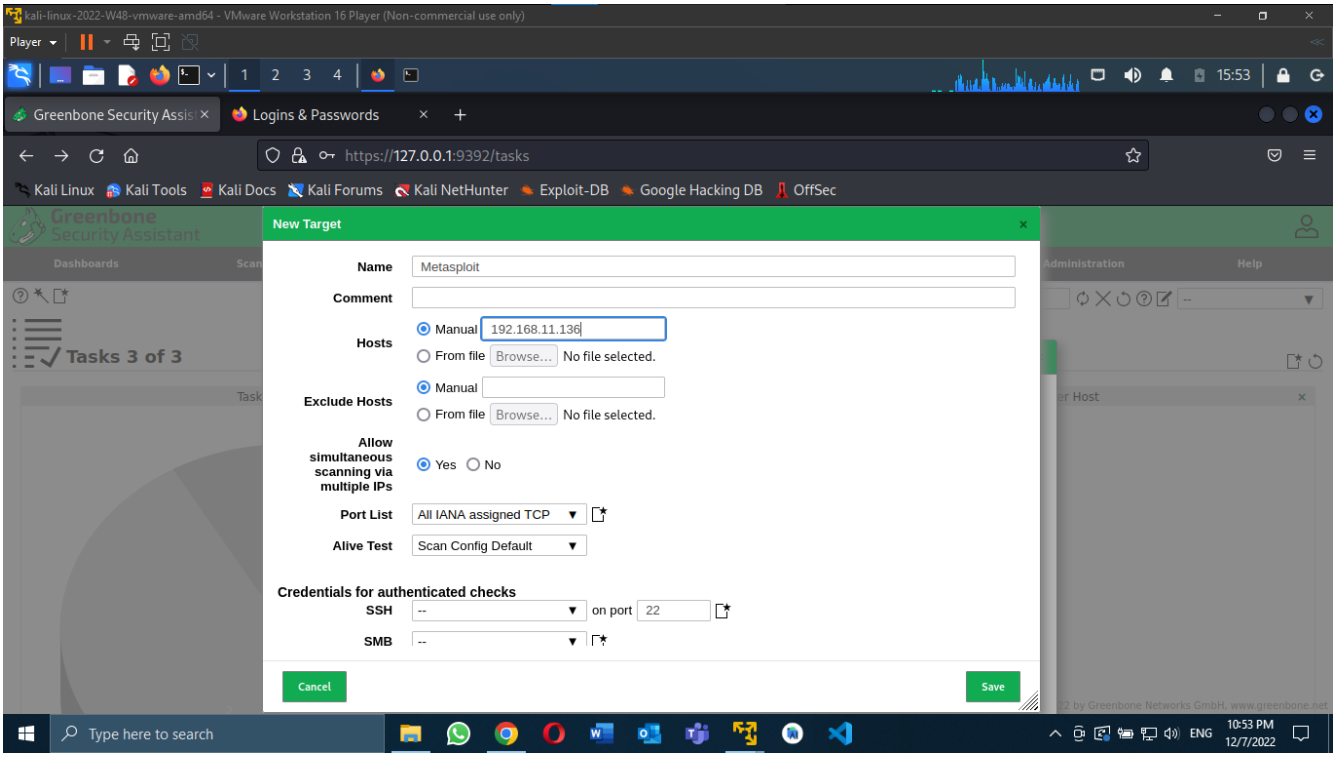


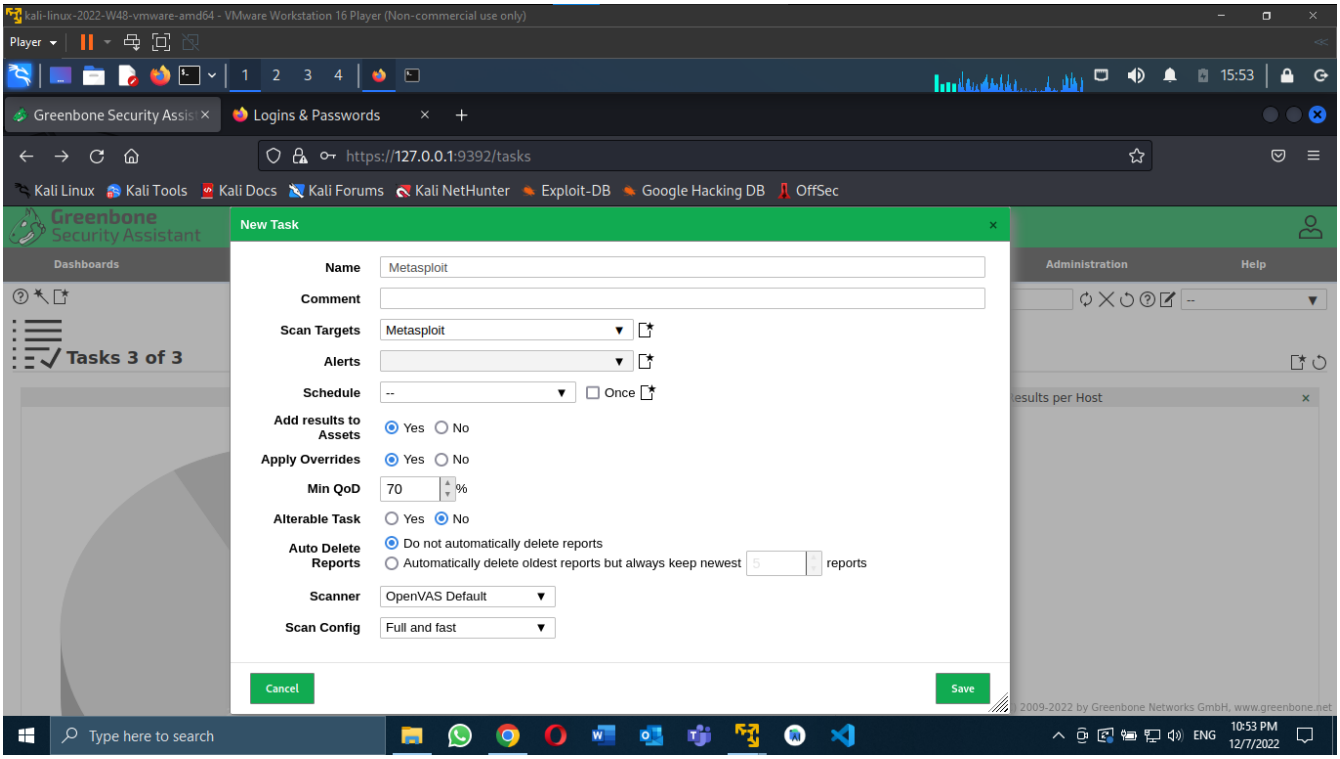


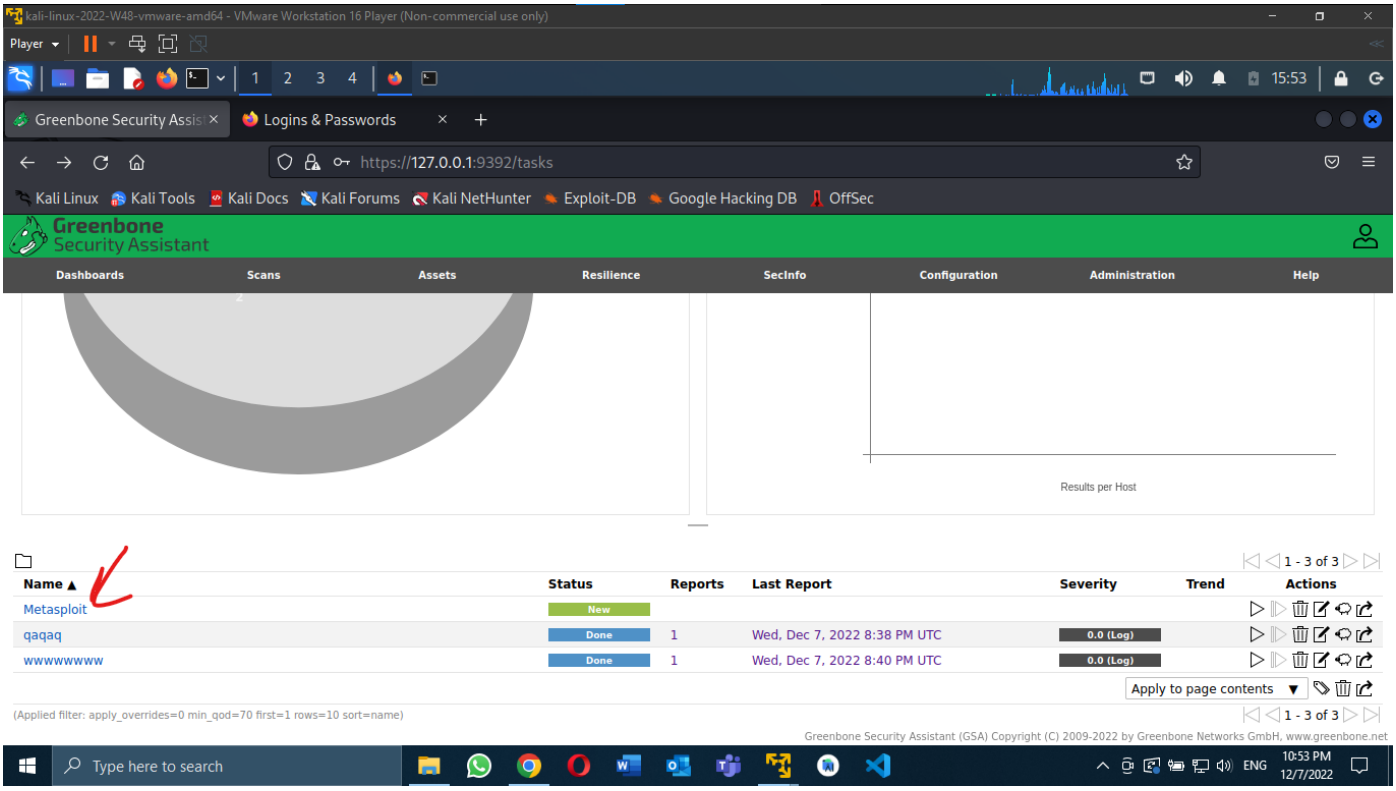

1 - 3 of 3
Name
Status
Reports
Last Report
Severity
Trend
Actions
Kali
74 %
1
Metasploit
Done
1
Wed, Dec 7, 2022 8:54 PM UTC
10.0 (High)
qaqaq
Done
1
Wed, Dec 7, 2022 8:38 PM UTC
0.0 (Log)
Target
Unnamed
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net
Type here to search
ENG
1:20 AM
12/8/2022

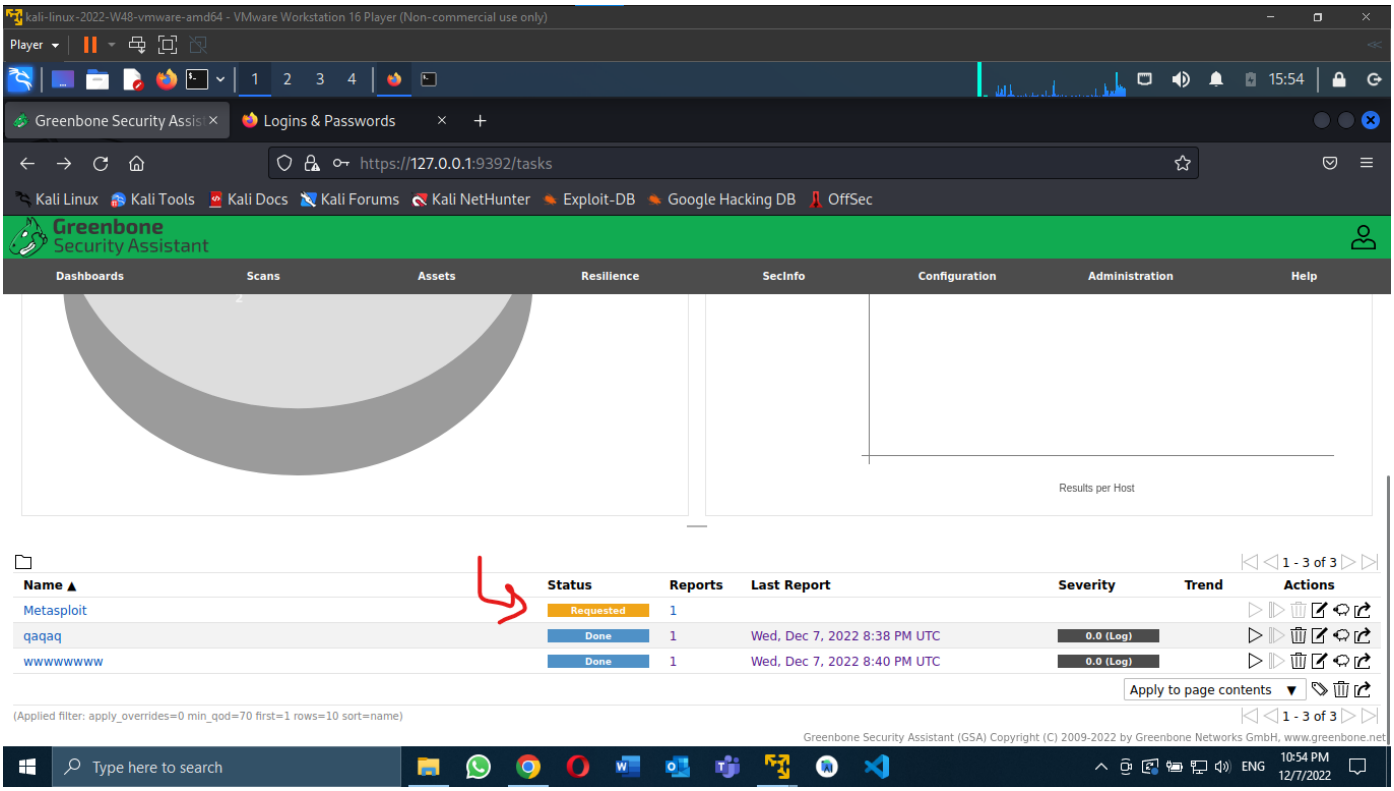

Reports 1 of 3
Reports by Severity Class (Total: 1)
Log
1
Reports with High Results
Max High
Max High per Host
Tue 06
Wed 07
Thu 08
Time
Reports by CVSS (Total: 1)
# of Reports
N/A
Log
Severity
1 - 1 of 1
Date
Status
Task
Severity
High
Medium
Low
Log
False Pos.
Actions
Wed, Dec 7, 2022 11:12 PM UTC
Done
Kali
0.0 (Log)
0
0
0
4
0
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 task_id=4382e1ee-f0c2-45c8-97a7-3f29f6d2b8e3 sort-reverse=date rows=10 first=1)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net
Type here to search
ENG
1:22 AM
12/8/2022

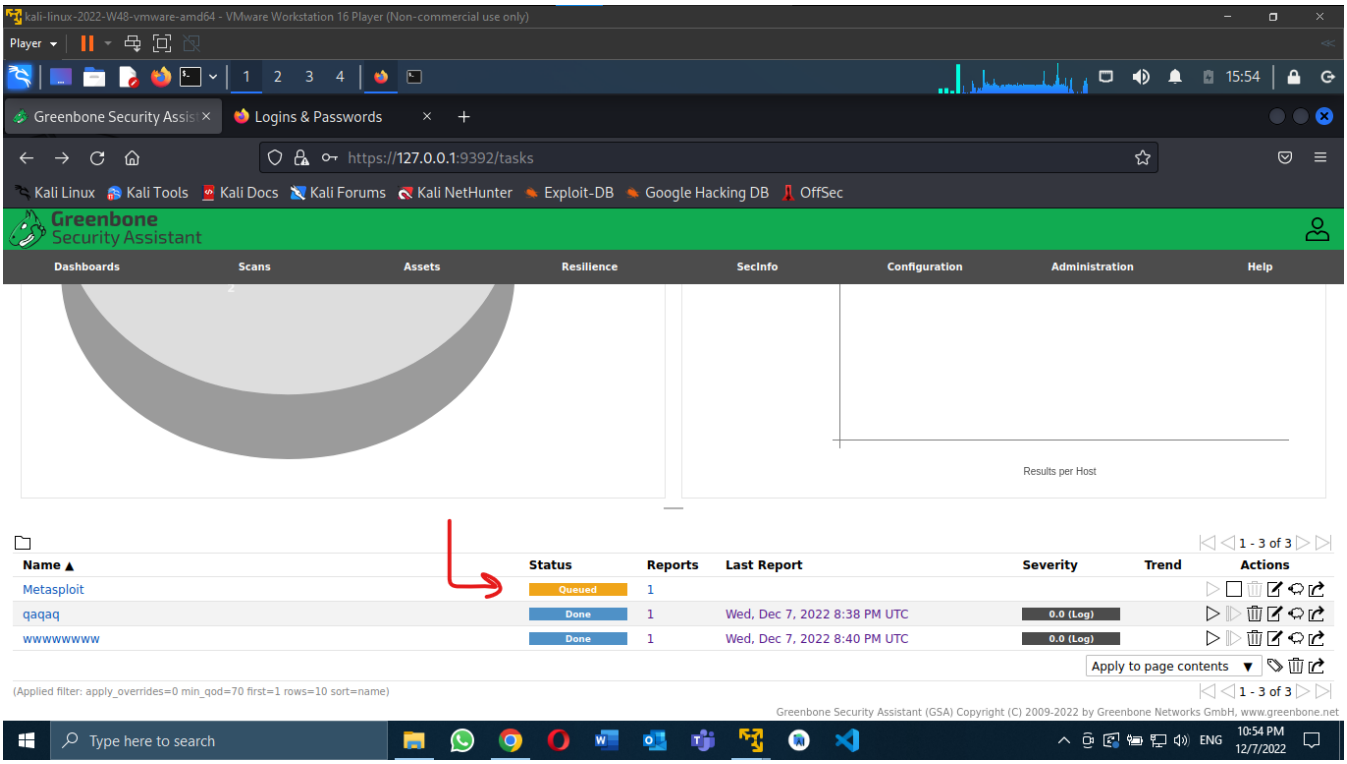
- Task scanning Metasploit Machine (192.168.11.136)

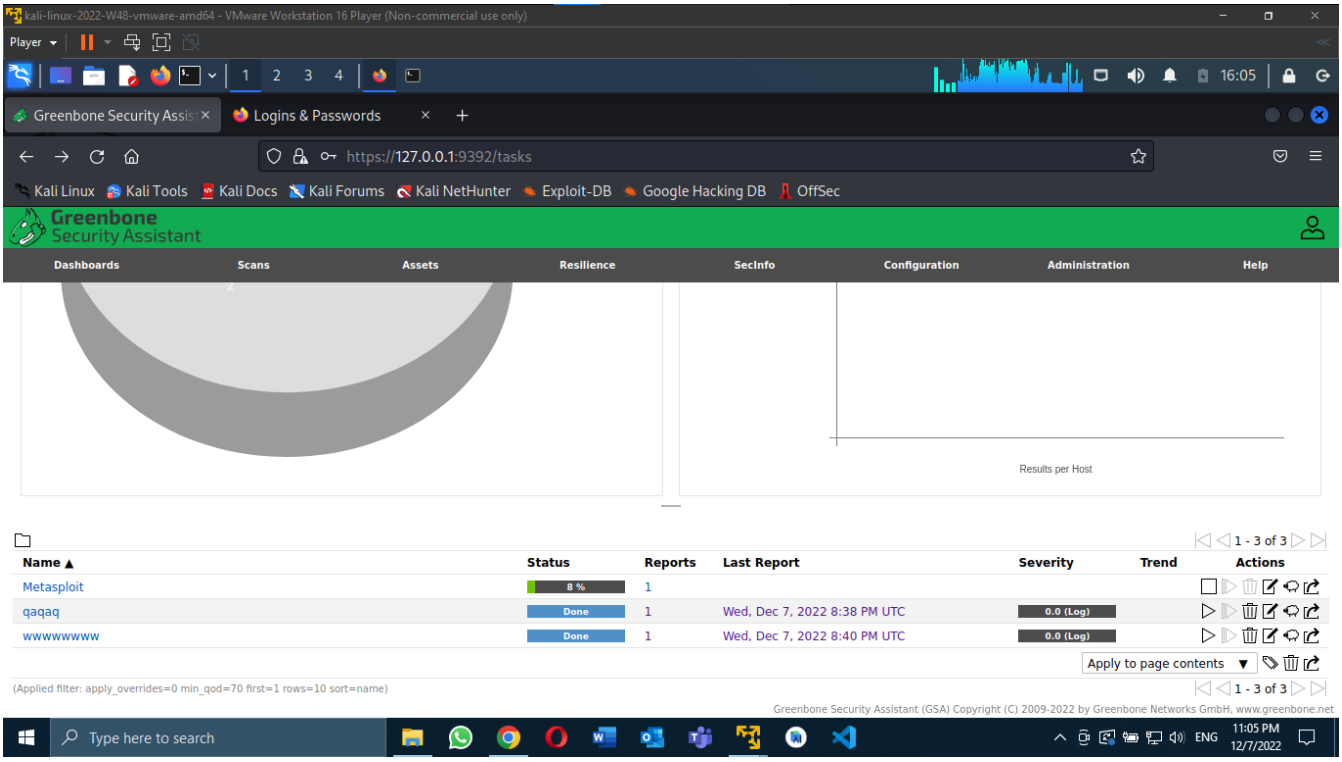


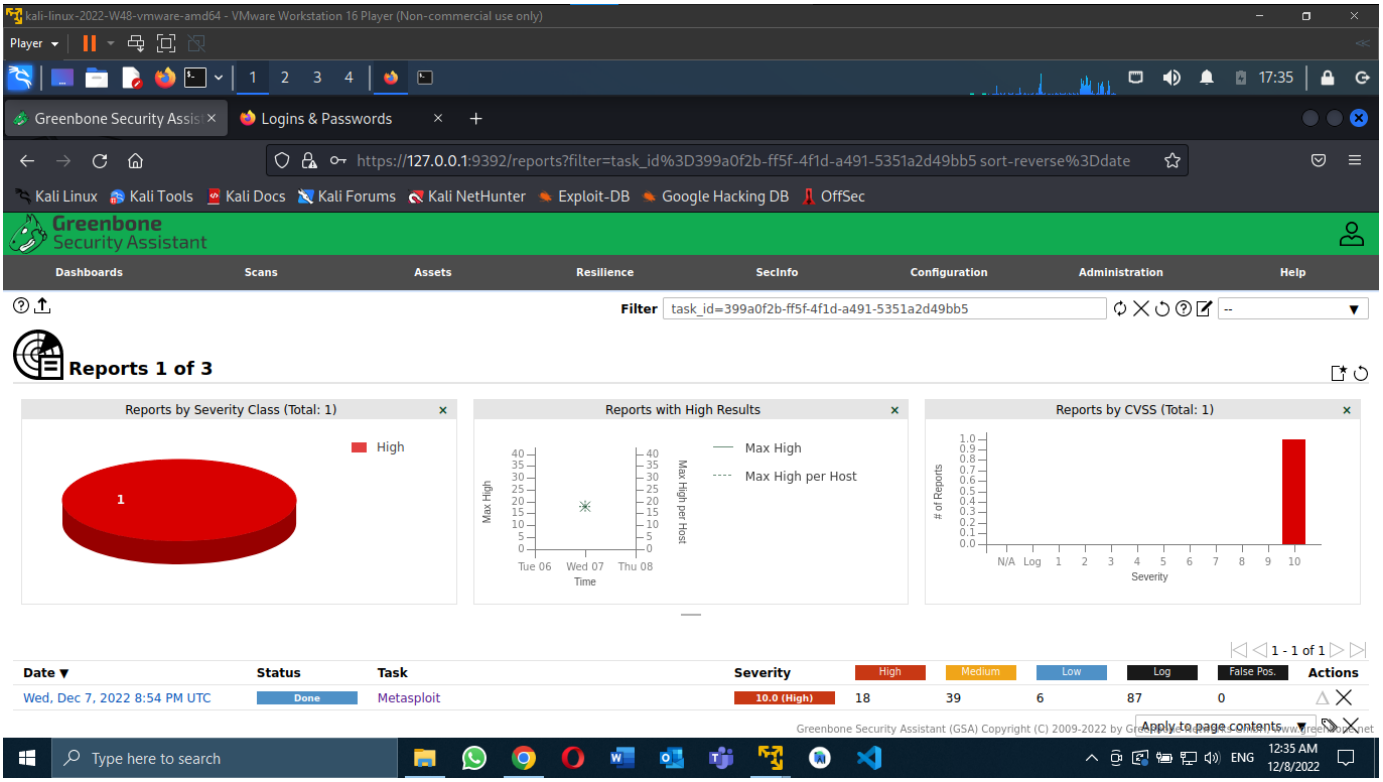


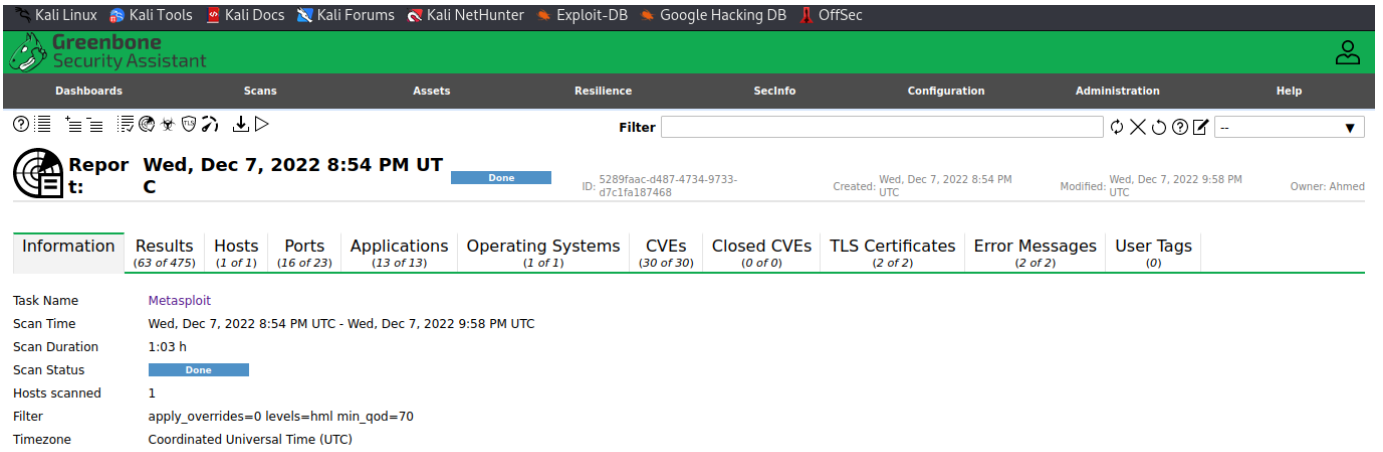

kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Greenbone Security Assis
Logins & Passwords
https://127.0.0.1:9392/tasks
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Results per Host
1 - 3 of 3
Name Status Reports Last Report Severity Trend Actions
Metasploit New
qaqaq Done 1 Wed, Dec 7, 2022 8:38 PM UTC 0.0 (Log)
wwwwwwww Done 1 Wed, Dec 7, 2022 8:40 PM UTC 0.0 (Log)
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 sort=name)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net
Type here to search
ENG 10:53 PM 12/7/2022


kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Greenbone Security Assis
Logins & Passwords
https://127.0.0.1:9392/tasks
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Results per Host
1 - 3 of 3
Name Status Reports Last Report Severity Trend Actions
Metasploit Requested 1
qaqaq Done 1 Wed, Dec 7, 2022 8:38 PM UTC 0.0 (Log)
wwwwwwww Done 1 Wed, Dec 7, 2022 8:40 PM UTC 0.0 (Log)
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 sort=name)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net
Type here to search
ENG 10:54 PM 12/7/2022


kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Greenbone Security Assis
Logins & Passwords
https://127.0.0.1:9392/tasks
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Results per Host
1 - 3 of 3
Name Status Reports Last Report Severity Trend Actions
Metasploit Queued 1
qaqaq Done 1 Wed, Dec 7, 2022 8:38 PM UTC 0.0 (Log)
wwwwwwww Done 1 Wed, Dec 7, 2022 8:40 PM UTC 0.0 (Log)
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 sort=name)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net
Type here to search
ENG 10:54 PM 12/7/2022


kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Greenbone Security Assis
Logins & Passwords
https://127.0.0.1:9392/tasks
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Results per Host
1 - 3 of 3
Name Status Reports Last Report Severity Trend Actions
Metasploit 8 % 1
qaqaq Done 1 Wed, Dec 7, 2022 8:38 PM UTC 0.0 (Log)
wwwwwwww Done 1 Wed, Dec 7, 2022 8:40 PM UTC 0.0 (Log)
Apply to page contents
(Applied filter: apply_overrides=0 min_qod=70 first=1 rows=10 sort=name)
Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH, www.greenbone.net
Type here to search
ENG 11:05 PM 12/7/2022


kali-linux-2022-W48-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Greenbone Security Assis
Logins & Passwords
https://127.0.0.1:9392/reports?filter=task_id%3D399a0f2b-ff5f-4f1d-a491-5351a2d49bb5 sort-reverse%3Ddate
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter task_id=399a0f2b-ff5f-4f1d-a491-5351a2d49bb5
Reports 1 of 3
Reports by Severity Class (Total: 1)
High
1
Reports with High Results
Max High
Max High per Host
Tue 06 Wed 07 Thu 08
Time
Reports by CVSS (Total: 1)
# of Reports
N/A Log 1 2 3 4 5 6 7 8 9 10
Severity
1 - 1 of 1
Date Status Task Severity High Medium Low Log False Pos. Actions
Wed, Dec 7, 2022 8:54 PM UTC Done Metasploit 10.0 (High) 18 39 6 87 0
Apply to page contents
Type here to search
ENG 12:35 AM 12/8/2022


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
Greenbone Security Assistant
Dashboards Scans Assets Resilience SecInfo Configuration Administration Help
Filter
Report: Wed, Dec 7, 2022 8:54 PM UTC
Done
ID: 5289faac-d487-4734-9733-d7c1fa187468
Created: Wed, Dec 7, 2022 8:54 PM UTC
Modified: Wed, Dec 7, 2022 9:58 PM UTC
Owner: Ahmed
Information Results (63 of 475) Hosts (1 of 1) Ports (16 of 23) Applications (13 of 13) Operating Systems (1 of 1) CVEs (30 of 30) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (2 of 2) User Tags (0)
Task Name Metasploit
Scan Time Wed, Dec 7, 2022 8:54 PM UTC - Wed, Dec 7, 2022 9:58 PM UTC
Scan Duration 1:03 h
Scan Status Done
Hosts scanned 1
Filter apply_overrides=0 levels=hml min_qod=70
Timezone Coordinated Universal Time (UTC)

- Vulnerabilities

Report:Wed, Dec 7, 2022 8:54 PM UTC Done

ID: 5289faac-d487-4734-9733-d7c1fa187468 Created: Wed, Dec 7, 2022 8:54 PM UTC Modified: Wed, Dec 7, 2022 9:58 PM UTC Owner: Ahmed

Information | Results (63 of 475) | Hosts (1 of 1) | Ports (16 of 23) | Applications (13 of 13) | Operating Systems (1 of 1) | CVEs (30 of 30) | Closed CVEs (0 of 0) | TLS Certificates (2 of 2) | Error Messages (2 of 2) | User Tags (0)

1 - 63 of 63

Vulnerability	Severity ▼	QoD	Host IP	Name	Location	Created
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.11.136		1524/tcp	Wed, Dec 7, 2022 9:32 PM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.11.136		1099/tcp	Wed, Dec 7, 2022 9:33 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:29 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.11.136		8787/tcp	Wed, Dec 7, 2022 9:29 PM UTC
The rexec service is running	10.0 (High)	80 %	192.168.11.136		512/tcp	Wed, Dec 7, 2022 9:28 PM UTC
Operating System (OS) End of Life (EOL) Detection	10.0 (High)	80 %	192.168.11.136		general/tcp	Wed, Dec 7, 2022 9:25 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	192.168.11.136		8009/tcp	Wed, Dec 7, 2022 9:37 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	9.3 (High)	99 %	192.168.11.136		3632/tcp	Wed, Dec 7, 2022 9:29 PM UTC
VNC Brute Force Login	9.0 (High)	95 %	192.168.11.136		5900/tcp	Wed, Dec 7, 2022 9:29 PM UTC
PostgreSQL weak password	9.0 (High)	99 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:29 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	192.168.11.136		6697/tcp	Wed, Dec 7, 2022 9:22 PM UTC
FTP Brute Force Logins Reporting	7.5 (High)	95 %	192.168.11.136		2121/tcp	Wed, Dec 7, 2022 9:58 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:40 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.11.136		6200/tcp	Wed, Dec 7, 2022 9:30 PM UTC

vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.11.136		21/tcp	Wed, Dec 7, 2022 9:30 PM UTC
phpinfo() output Reporting	7.5 (High)	80 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:29 PM UTC
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:38 PM UTC
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability	7.4 (High)	70 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:35 PM UTC
TWiki Cross-Site Request Forgery Vulnerability - Sep10	6.8 (Medium)	80 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:29 PM UTC
Yap Blog 'index.php' Remote File Include Vulnerability	6.8 (Medium)	99 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:40 PM UTC
Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection Vulnerability	6.8 (Medium)	99 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:34 PM UTC
Anonymous FTP Login Reporting	6.4 (Medium)	80 %	192.168.11.136		21/tcp	Wed, Dec 7, 2022 9:21 PM UTC
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:28 PM UTC
TWiki < 6.1.0 XSS Vulnerability	6.1 (Medium)	80 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:29 PM UTC
TWiki Cross-Site Request Forgery Vulnerability	6.0 (Medium)	80 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:29 PM UTC
Samba MS-RPC Remote Shell Command Execution Vulnerability - Active Check	6.0 (Medium)	99 %	192.168.11.136		445/tcp	Wed, Dec 7, 2022 9:30 PM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:27 PM UTC
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection	5.9 (Medium)	98 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:27 PM UTC
HTTP Debugging Methods (TRACE/TRACK) Enabled	5.8 (Medium)	99 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:29 PM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3 (Medium)	80 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:27 PM UTC
Weak Host Key Algorithm(s) (SSH)	5.3 (Medium)	80 %	192.168.11.136		22/tcp	Wed, Dec 7, 2022 9:22 PM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	192.168.11.136		22/tcp	Wed, Dec 7, 2022 9:22 PM UTC
SSL/TLS: Server Certificate / Certificate in Chain with RSA keys less than 2048 bits	5.3 (Medium)	80 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:27 PM UTC
awiki <= 20100125 Multiple LFI Vulnerabilities - Active Check	5.0 (Medium)	99 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:37 PM UTC
Check if Mailserver answer to VRFY and EXPN requests	5.0 (Medium)	99 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:27 PM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:26 PM UTC
QWikiwiki directory traversal vulnerability	5.0 (Medium)	99 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:38 PM UTC
SSL/TLS: Certificate Expired	5.0 (Medium)	99 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:26 PM UTC

Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability	4.3 (Medium)	99 %	192.168.11.136		80/tcp	Wed, Dec 7, 2022 9:40 PM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:26 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:27 PM UTC
SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability	4.0 (Medium)	80 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:27 PM UTC
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm	4.0 (Medium)	80 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:26 PM UTC
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)	3.7 (Low)	80 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:27 PM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4 (Low)	80 %	192.168.11.136		5432/tcp	Wed, Dec 7, 2022 9:28 PM UTC
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)	3.4 (Low)	80 %	192.168.11.136		25/tcp	Wed, Dec 7, 2022 9:28 PM UTC
Weak MAC Algorithm(s) Supported (SSH)	2.6 (Low)	95 %	192.168.11.136		22/tcp	Wed, Dec 7, 2022 9:22 PM UTC
TCP timestamps	2.6 (Low)	80 %	192.168.11.136		general/tcp	Wed, Dec 7, 2022 9:22 PM UTC
ICMP Timestamp Reply Information Disclosure	2.1 (Low)	80 %	192.168.11.136		general/icmp	Wed, Dec 7, 2022 9:25 PM UTC

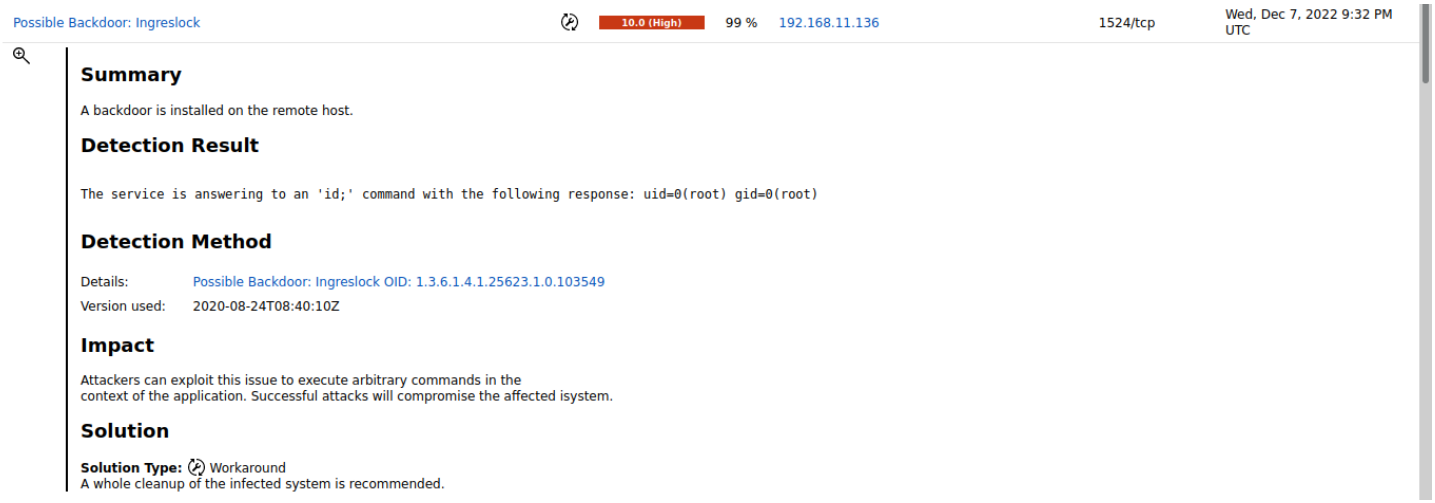
2. Five Vulnerabilities of Metasploitable target:

1) Possible Backdoor: Ingreslock

This is an old vulnerability that was first reported in 2004. Backdoor.Ingreslock is a backdoor exploit that gives third parties access to the computer affected by the vulnerability. Backdoor.Ingreslock gained some attention due to the known browser goggle chrome notfications showing the presence of Backdoor.Ingreslock in its memory processes. Although original versions of Backdoor.Ingreslock are inactive, some Trojans can use alike vulnerabilities to target computers.

Solution

The Backdoor.Ingreslock vulnerability can be countered easily, although Backdoor.Ingreslock may be an indicator for a bigger problem. On the other hand, security practices and scans for vulnerabilities can root out problems like Backdoor.Ingreslock. It is better to look for the source of the possible attack, which may include an attack website or a third-part showing signs of injecting and targeting the computer.



Possible Backdoor: Ingreslock | 10.0 (High) | 99 % | 192.168.11.136 | 1524/tcp | Wed, Dec 7, 2022 9:32 PM UTC

Summary

A backdoor is installed on the remote host.

Detection Result

The service is answering to an 'id;' command with the following response: uid=0(root) gid=0(root)

Detection Method

Details: Possible Backdoor: Ingreslock OID: 1.3.6.1.4.1.25623.1.0.103549

Version used: 2020-08-24T08:40:10Z

Impact

Attackers can exploit this issue to execute arbitrary commands in the context of the application. Successful attacks will compromise the affected isystem.

Solution

Solution Type: Workaround

A whole cleanup of the infected system is recommended.

2)The rexec service is running

The RSH remote execution service (rexec) is a legacy service, most of the time is used to -without checking- and blindly have trusted Ips and host. Major problem is that no encryption is applied or any form of authentication in the protocol.

Solution

Disable the rexec service and use better protocols like SSH (Secure Shell Protocol).

The rexec service is running	10.0 (High)	80 %	192.168.11.136	512/tcp	Wed, Dec 7, 2022 9:28 PM UTC

Summary

This remote host is running a rexec service.

Detection Result

```
The rexec service was detected on the target system.
```

Insight

rexec (remote execution client for an exec server) has the same kind of functionality that rsh has: you can execute shell commands on a remote computer.

The main difference is that rexec authenticate by reading the username and password *unencrypted* from the socket.

Detection Method

Checks if a vulnerable version is present on the target host.

Details: The rexec service is running OID: 1.3.6.1.4.1.25623.1.0.100111

Version used: 2020-10-01T11:33:30Z

Solution

Solution Type: Mitigation

Disable the rexec service and use alternatives like SSH instead.

3) OS End of Life Detection.

The Operating System on the remote host has reached the end of life and is advised to not use it further.

Solution:

Upgrade the Operating System on the remote host to have a version that gets security patches from the OS vendor.

Operating System (OS) End of Life (EOL) Detection | 10.0 (High) | 80 % | 192.168.11.136 | general/tcp | Wed, Dec 7, 2022 9:25 PM UTC

Summary

The Operating System (OS) on the remote host has reached the End of Life (EOL) and should not be used anymore.

Detection Result

```
The "Ubuntu" Operating System on the remote host has reached the end of life.

CPE:                cpe:/o:canonical:ubuntu_linux:8.04
Installed version,
build or SP:        8.04
EOL date:           2013-05-09
EOL info:           https://wiki.ubuntu.com/Releases
```

Product Detection Result

Product cpe:/o:canonical:ubuntu_linux:8.04

Method OS Detection Consolidation and Reporting (OID: 1.3.6.1.4.1.25623.1.0.105937)

Log View details of product detection

Detection Method

Checks if an EOL version of an OS is present on the target host.

Details: Operating System (OS) End of Life (EOL) Detection OID: 1.3.6.1.4.1.25623.1.0.103674

Version used: 2022-04-05T13:00:52Z

Impact

An EOL version of an OS is not receiving any security updates from the vendor. Unfixed security vulnerabilities might be leveraged by an attacker to compromise the security of this host.

Solution

Solution Type: Mitigation

Upgrade the OS on the remote host to a version which is still supported and receiving security updates by the vendor.

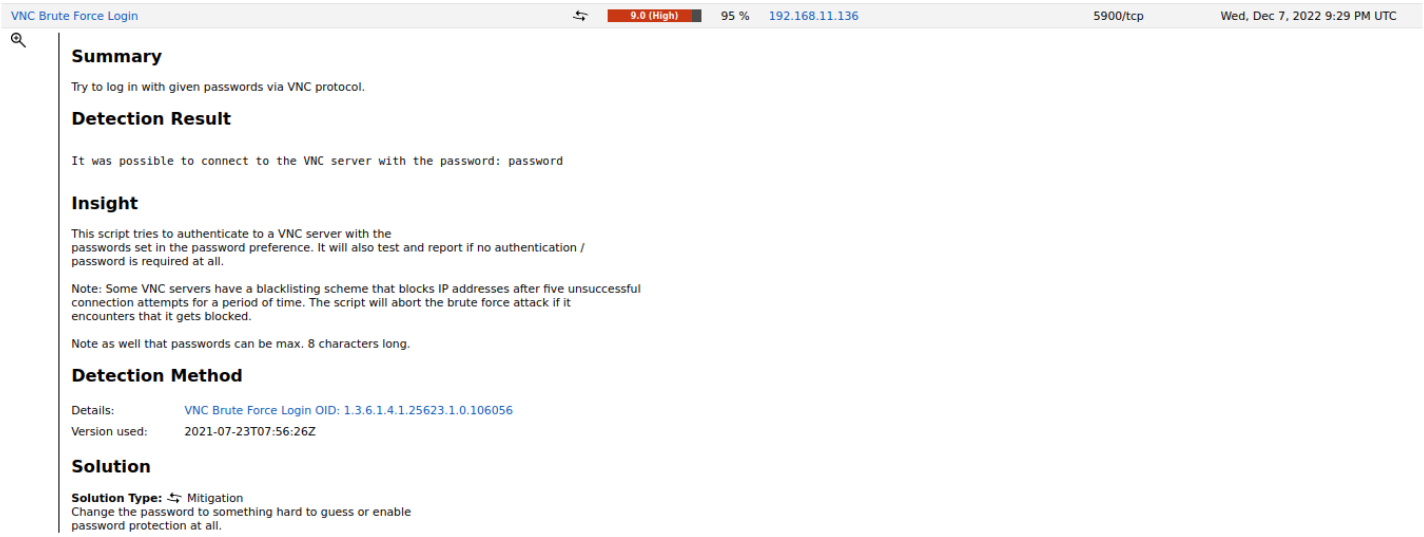
4)VNC Brute force login

When trying to log in with given and saved passwords using VNC protocol, the script tries to authenticate the written password to a VNC server with the passwords saved in a password preference list. It tests and replies if no authentication/password is needed.

Some VNC servers can blacklist IP addresses after five unsuccessful connection requests for some time. The script will abandon the brute force attack if it receives a block and be aware that passwords can be maximum 8 characters long.

Solution:

Make your password difficult to be thought of or use a password protection policy.



VNC Brute Force Login | 9.0 (High) | 95 % | 192.168.11.136 | 5900/tcp | Wed, Dec 7, 2022 9:29 PM UTC

Summary

Try to log in with given passwords via VNC protocol.

Detection Result

```
It was possible to connect to the VNC server with the password: password
```

Insight

This script tries to authenticate to a VNC server with the passwords set in the password preference. It will also test and report if no authentication / password is required at all.

Note: Some VNC servers have a blacklisting scheme that blocks IP addresses after five unsuccessful connection attempts for a period of time. The script will abort the brute force attack if it encounters that it gets blocked.

Note as well that passwords can be max. 8 characters long.

Detection Method

Details: VNC Brute Force Login OID: 1.3.6.1.4.1.25623.1.0.106056

Version used: 2021-07-23T07:56:26Z

Solution

Solution Type: Mitigation

Change the password to something hard to guess or enable password protection at all.

5) PostgreSQL weak password

It used to be ok to login into the remote PostgreSQL as a postgres user with the aid of weak credentials.

Solution:

Change the password as soon as possible.

PostgreSQL weak password	9.0 (High)	99 %	192.168.11.136	5432/tcp	Wed, Dec 7, 2022 9:29 PM UTC

Summary

It was possible to login into the remote PostgreSQL as user postgres using weak credentials.

Detection Result

```
It was possible to login as user postgres with password "postgres".
```

Product Detection Result

Product cpe:/a:postgresql:postgresql:8.3.1

Method PostgreSQL Detection (OID: 1.3.6.1.4.1.25623.1.0.100151)

Log View details of product detection

Detection Method

Details: PostgreSQL weak password OID: 1.3.6.1.4.1.25623.1.0.103552

Version used: 2022-05-31T14:35:19Z

Solution

Solution Type: Mitigation
Change the password as soon as possible.