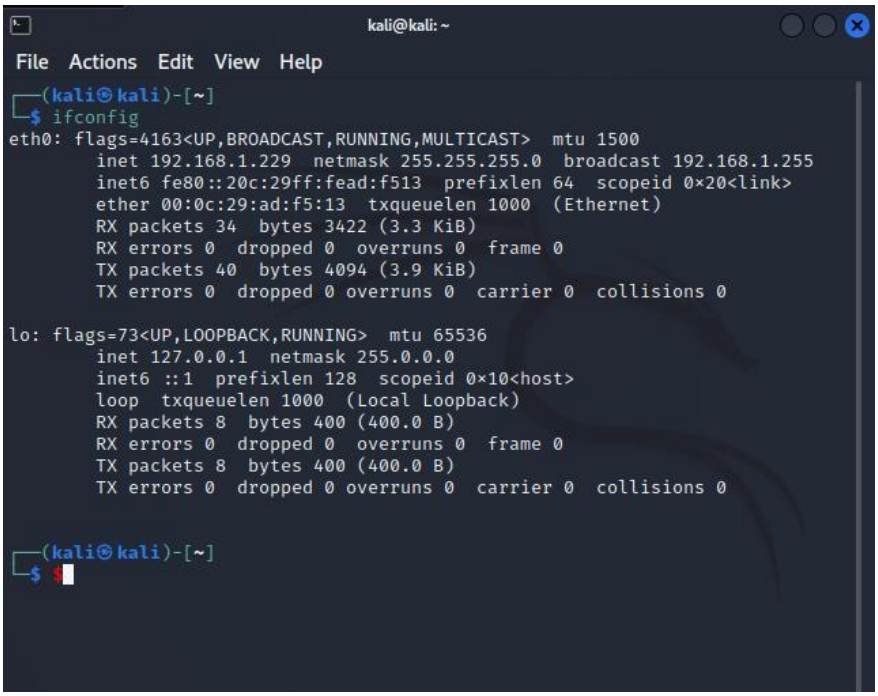
Lab 5 -Vulnerability Scanning Using OpenVAS

Name: Hamza Abdellah Ahmed

ID :18P7231

VMs IPs Table

Kali Linux:



Pinging google:

```
root@kali: /home/kali
File  Actions  Edit  View  Help
time=45.5 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=3 ttl=117
time=46.5 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=4 ttl=117
time=48.0 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=5 ttl=117
time=46.7 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=6 ttl=117
time=46.0 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=7 ttl=117
time=46.3 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=8 ttl=117
time=47.1 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=9 ttl=117
time=45.5 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=10 ttl=117
 time=45.9 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=11 ttl=117
 time=45.2 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=12 ttl=117
 time=46.0 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=13 ttl=117
 time=46.2 ms
64 bytes from mrs09s10-in-f14.1e100.net (172.217.21.14): icmp_seq=14 ttl=117
 time=45.2 ms
^C
--- google.com ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13033ms
rtt min/avg/max/mdev = 44.942/46.077/48.019/0.805 ms

┌──(root💀 kali)-[/home/kali]
└─#
```

Metasploitable:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:87:d2:f3
          inet addr:192.168.1.115  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe87:d2f3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5377 (5.2 KB)  TX bytes:7862 (7.6 KB)
          Interrupt:17 Base address:0x2000

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:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25525 (24.9 KB)  TX bytes:25525 (24.9 KB)

msfadmin@metasploitable:~$
```

Kali Linux	**192.168.1.229**
Metasploitable	**192.168.1.115**

Installing openvas

```
root@kali: /home/kali
File  Actions  Edit  View  Help
java all 1.2-2 [62.2 kB]
Get:39 http://kali.download/kali kali-rolling/main amd64 libfontbox-java all
 1:1.8.16-2 [211 kB]
Get:40 http://kali.download/kali kali-rolling/main amd64 libpdfbox-java all
1:1.8.16-2 [5,205 kB]
Get:41 http://kali.download/kali kali-rolling/main amd64 libptexenc1 amd64 2
021.20210626.59705-1 [65.1 kB]
Get:42 http://http.kali.org/kali kali-rolling/main amd64 libteckit0 amd64 2.
5.11+ds1-1 [336 kB]
Get:43 http://kali.download/kali kali-rolling/main amd64 libtexlua53 amd64 2
021.20210626.59705-1 [132 kB]
Get:44 http://kali.download/kali kali-rolling/main amd64 libtexluajit2 amd64
 2021.20210626.59705-1 [267 kB]
Get:45 http://http.kali.org/kali kali-rolling/main amd64 libzzip-0-13 amd64
0.13.72+dfsg.1-1.1 [58.3 kB]
Get:46 http://kali.download/kali kali-rolling/main amd64 lmodern all 2.004.5
-6.1 [9,489 kB]
Get:47 http://http.kali.org/kali kali-rolling/main amd64 openvas all 21.4.3~
0kali1 [5,128 B]
Get:48 http://kali.download/kali kali-rolling/main amd64 preview-latex-style
 all 12.2-1 [201 kB]
Get:49 http://kali.download/kali kali-rolling/main amd64 t1utils amd64 1.41-
4 [62.1 kB]
Get:50 http://http.kali.org/kali kali-rolling/main amd64 tcl amd64 8.6.11+1
[5,788 B]
Get:51 http://kali.download/kali kali-rolling/main amd64 tex-gyre all 201806
21-3.1 [6,210 kB]
Get:52 http://kali.download/kali kali-rolling/main amd64 texlive-binaries am
d64 2021.20210626.59705-1 [10.1 MB]
Get:53 http://kali.download/kali kali-rolling/main amd64 texlive-base all 20
21.20210921-1 [21.1 MB]
58% [Working]                                          3,389 kB/s 21s
```

Netstat ant

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ openvas --help                                                    1 ✗
Usage:
  openvas [OPTION?] - Open Vulnerability Assessment Scanner

Help Options:
  -h, --help                        Show help options

Application Options:
  -V, --version                     Display version information
  -c, --config-file=<filename>      Configuration file
  -s, --cfg-specs                   Print configuration settings
  -y, --sysconfdir                  Print system configuration directory (set
 at compile time)
  -u, --update-vt-info              Updates VT info into redis store from VT
files
  --scan-start=<string>             ID of scan to start. ID and related data
must be stored into redis before.
  --scan-stop=<string>              ID of scan to stop


┌──(kali㉿kali)-[~]
└─$ netstat -antp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
    PID/Program name

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ openvas-start
openvas-start: command not found
```

Instructions given in the lab is no longer working. Had to do this to make it work:

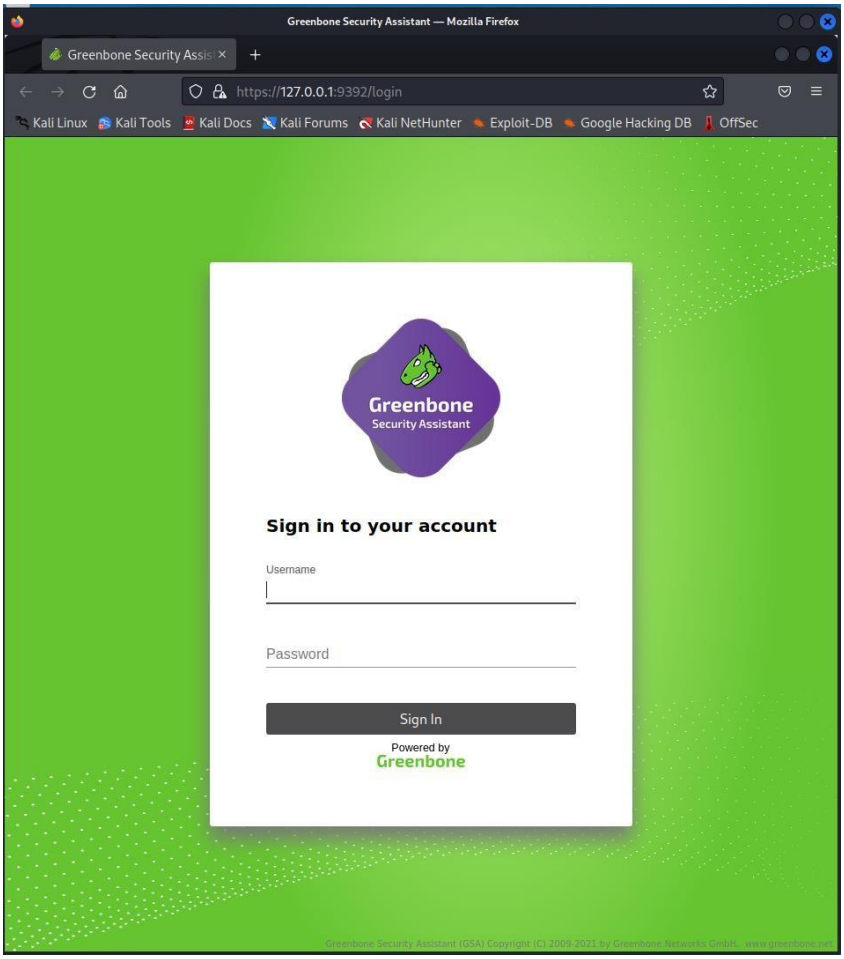
sudo apt install gvm to install Greenbone Vulnerability Management(gvm)

sudo gvm-setup to set up the tool for the first time use

sudo gvm-feed-update to update the feed only

sudo gvm-start/stop to start or stop the service

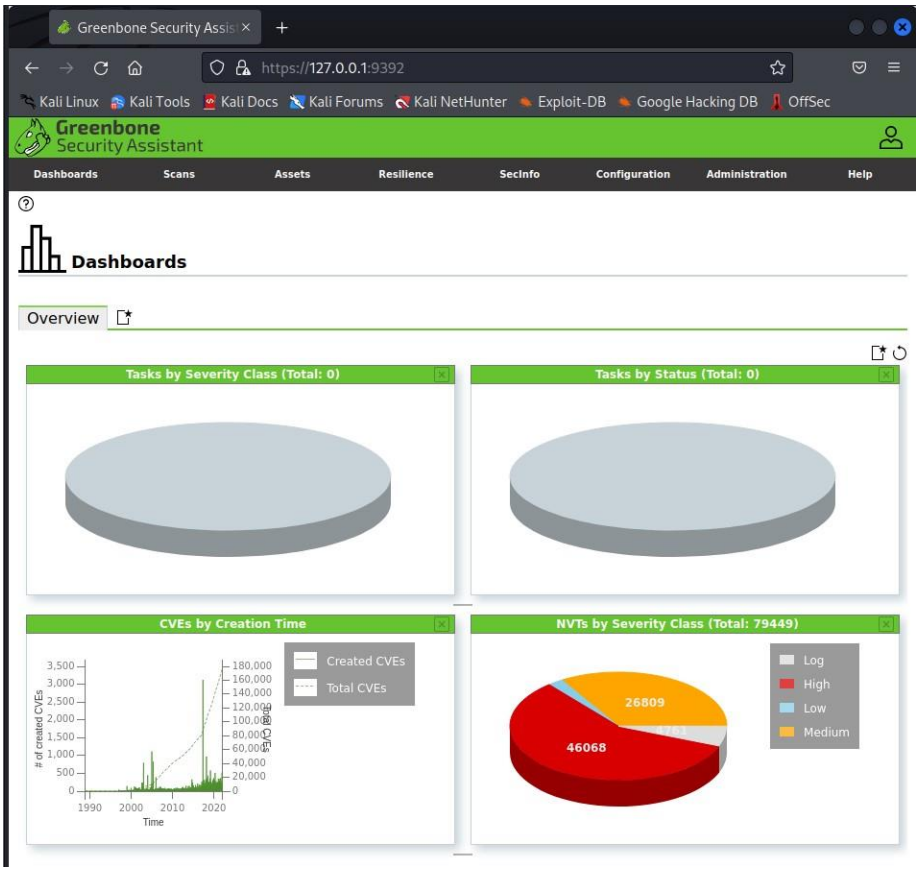
After applying the previous commands and running sudo gvm-start we get to this page:



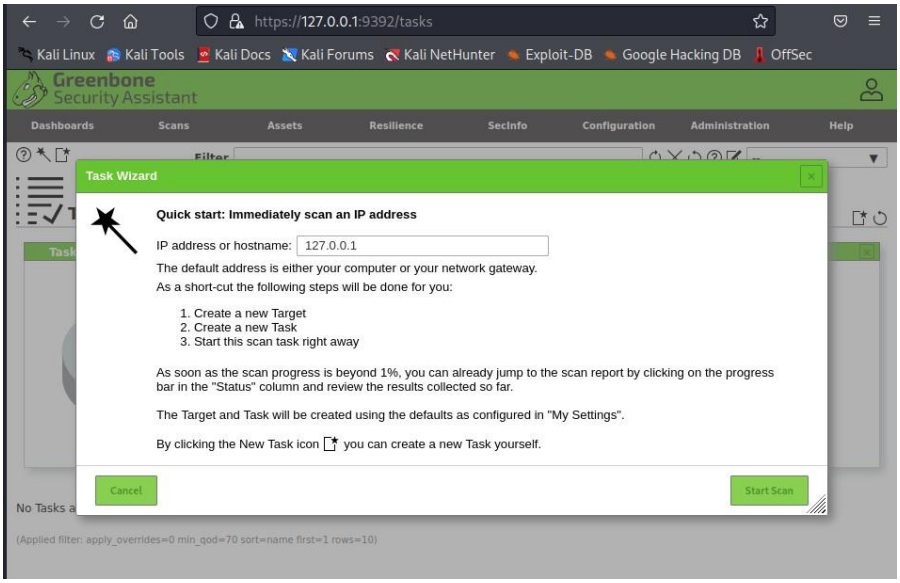
Again, instructions are outdated in the lab report. Username “admin” and password “admin” doesn’t log me in. Did the following command to create a new user:

```
┌──(root💀 kali)-[/]
└─sudo runuser -u _gvm -- gvmd --create-user=admin2 --new-password=12345
User created with password '753161df-ed65-4173-98e5-be277f8fc651'.
```

Now we are inside.



Task Wizard:



After the test is scan, we can see the severity is 0 which is OK.

1 - 1 of 1

Name	Status	Reports	Last Report	Severity ▲	Trend	Actions
Immediate scan of IP 127.0.0.1	Done	1	Sun, Jan 2, 2022 1:05 PM UTC	0.0 (Log)		

Apply to page contents

(Applied filter: apply_overrides=0 min_qod=70 sort=severity first=1 rows=10)

1 - 1 of 1

Report:

Dashboards | Scans | Assets | Resilience | SecInfo | Configuratio

Name	Immediate scan of IP 127.0.0.1
Comment	
Alterable	No
Status	0 %

Target

Target for immediate scan of IP 127.0.0.1 - 2022-01-02 13:05:50

Scanner

Name	OpenVAS Default
Type	OpenVAS Scanner
Scan Config	Full and fast
Order for target hosts	
Network Source Interface	
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

Assets

Add to Assets	Yes
Apply Overrides	Yes
Min QoD	70 %

Scan

Duration of last Scan	4 minutes
Average Scan duration	4 minutes
Auto delete Reports	Do not automatically delete reports

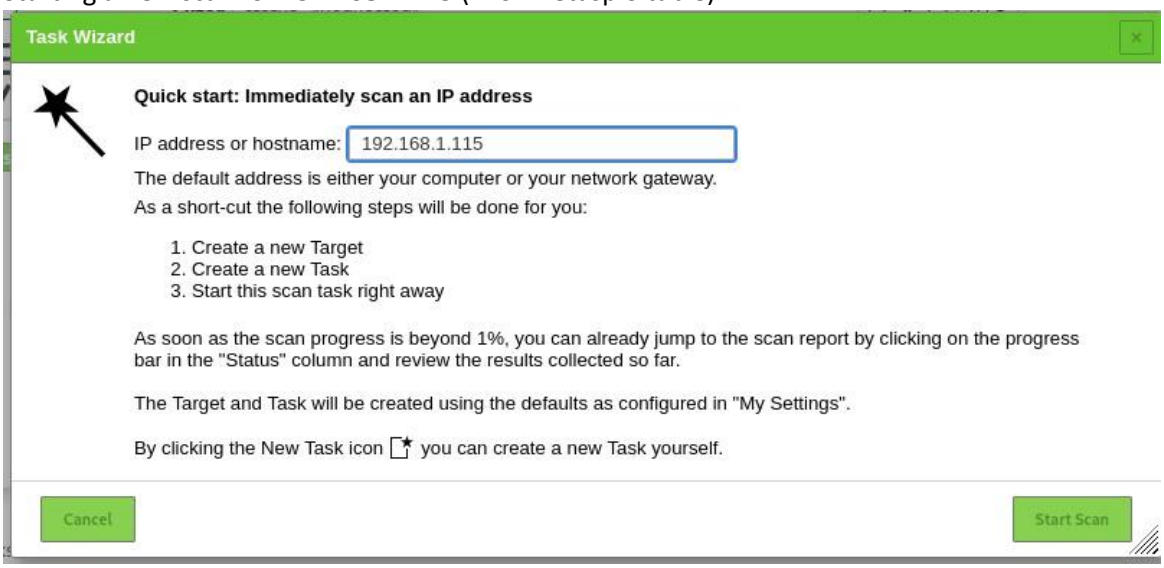
Questions and Discussion

1. **Take a screen shot of your own work for all of the above steps and put them all together in your report, you must order them as the flow of the experiments go, label each screen shot with a suitable title.**

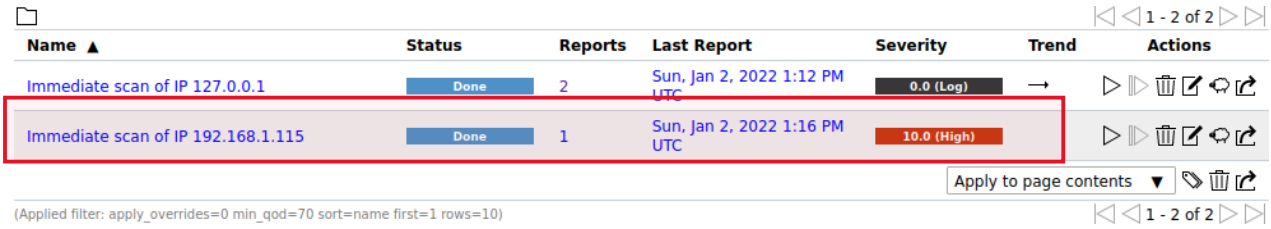
   Completed in previous pages

2. **Use OpenVAS to find Five vulnerabilities of the Metasploitable target, and briefly describe them.**

   Starting a new scan for **192.168.1.115** (IP of metasploitable)

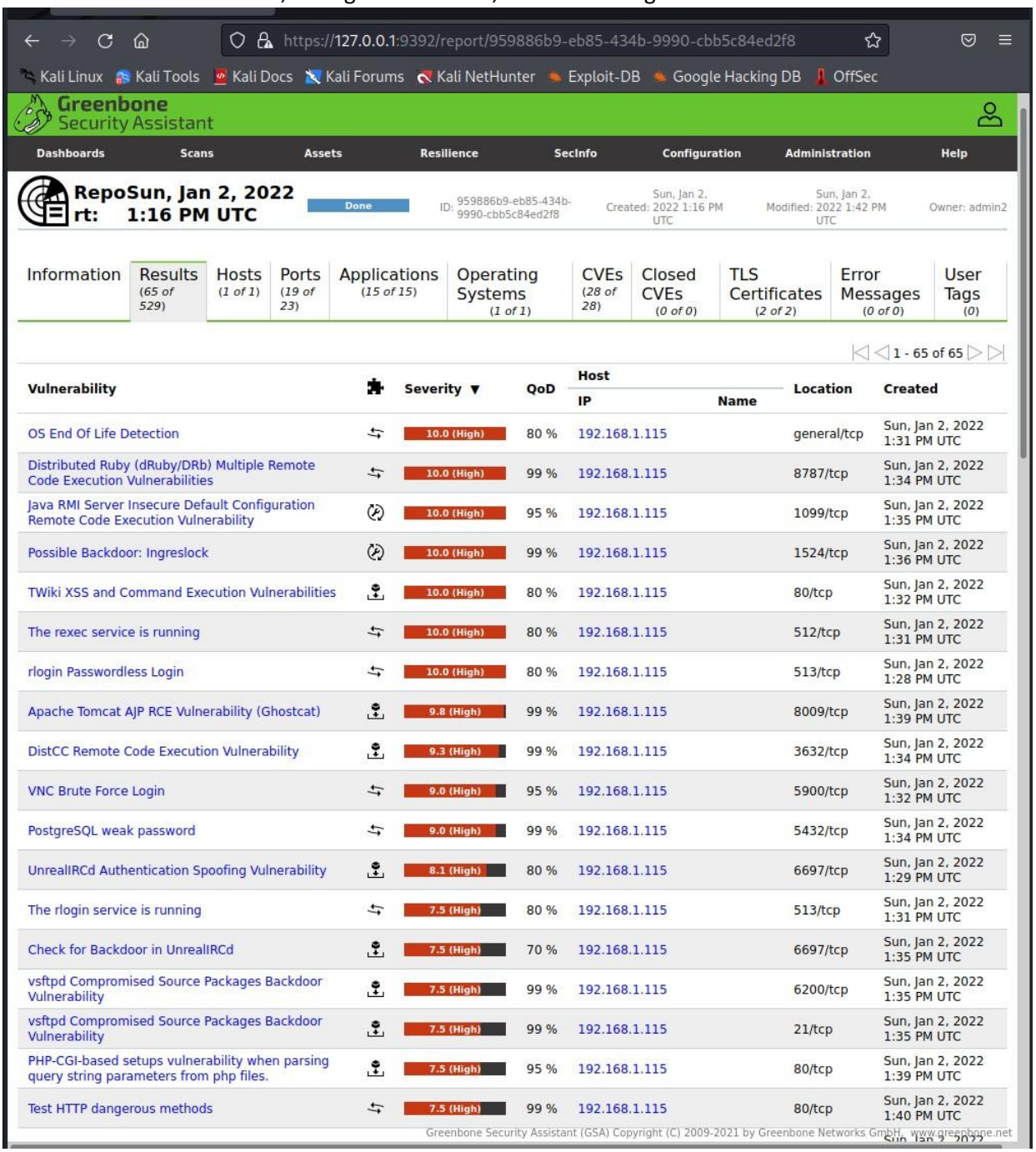


   Scan results after the scan is complete:



   Severity is **HIGH** (10)

If we click on the scan name, then go to “Results”, we can investigate the vulnerabilities:



Vulnerability	Severity ▼	QoD	Host IP	Host Name	Location	Created
OS End Of Life Detection	10.0 (High)	80 %	192.168.1.115		general/tcp	Sun, Jan 2, 2022 1:31 PM UTC
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	192.168.1.115		8787/tcp	Sun, Jan 2, 2022 1:34 PM UTC
Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability	10.0 (High)	95 %	192.168.1.115		1099/tcp	Sun, Jan 2, 2022 1:35 PM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	192.168.1.115		1524/tcp	Sun, Jan 2, 2022 1:36 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	80 %	192.168.1.115		80/tcp	Sun, Jan 2, 2022 1:32 PM UTC
The rexec service is running	10.0 (High)	80 %	192.168.1.115		512/tcp	Sun, Jan 2, 2022 1:31 PM UTC
rlogin Passwordless Login	10.0 (High)	80 %	192.168.1.115		513/tcp	Sun, Jan 2, 2022 1:28 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	192.168.1.115		8009/tcp	Sun, Jan 2, 2022 1:39 PM UTC
DistCC Remote Code Execution Vulnerability	9.3 (High)	99 %	192.168.1.115		3632/tcp	Sun, Jan 2, 2022 1:34 PM UTC
VNC Brute Force Login	9.0 (High)	95 %	192.168.1.115		5900/tcp	Sun, Jan 2, 2022 1:32 PM UTC
PostgreSQL weak password	9.0 (High)	99 %	192.168.1.115		5432/tcp	Sun, Jan 2, 2022 1:34 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	192.168.1.115		6697/tcp	Sun, Jan 2, 2022 1:29 PM UTC
The rlogin service is running	7.5 (High)	80 %	192.168.1.115		513/tcp	Sun, Jan 2, 2022 1:31 PM UTC
Check for Backdoor in UnrealIRCd	7.5 (High)	70 %	192.168.1.115		6697/tcp	Sun, Jan 2, 2022 1:35 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.1.115		6200/tcp	Sun, Jan 2, 2022 1:35 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.5 (High)	99 %	192.168.1.115		21/tcp	Sun, Jan 2, 2022 1:35 PM UTC
PHP-CGI-based setups vulnerability when parsing query string parameters from php files.	7.5 (High)	95 %	192.168.1.115		80/tcp	Sun, Jan 2, 2022 1:39 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	192.168.1.115		80/tcp	Sun, Jan 2, 2022 1:40 PM UTC

Here's 5 of these vulnerabilities:

1. **OS End Of Life Detection:** The Operating System on the remote host has reached the end of life and should not be used anymore.

2. **Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability:** Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

3. **Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities:** Systems using Distributed Ruby (dRuby/DRb), which is available in Ruby versions 1.6 and later, may permit unauthorized systems to execute distributed commands.

4. **Possible Backdoor: Ingreslock:** A backdoor is installed on the remote host. A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware.

5. **TWiki XSS and Command Execution Vulnerabilities:** The host is running TWiki and is prone to Cross-Site Scripting (XSS) and Command Execution Vulnerabilities.