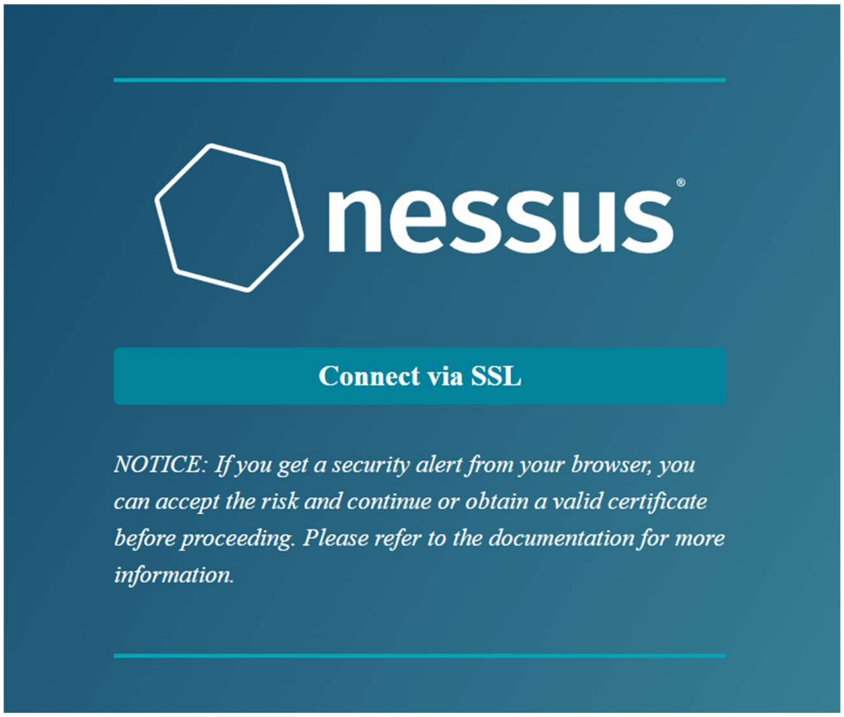
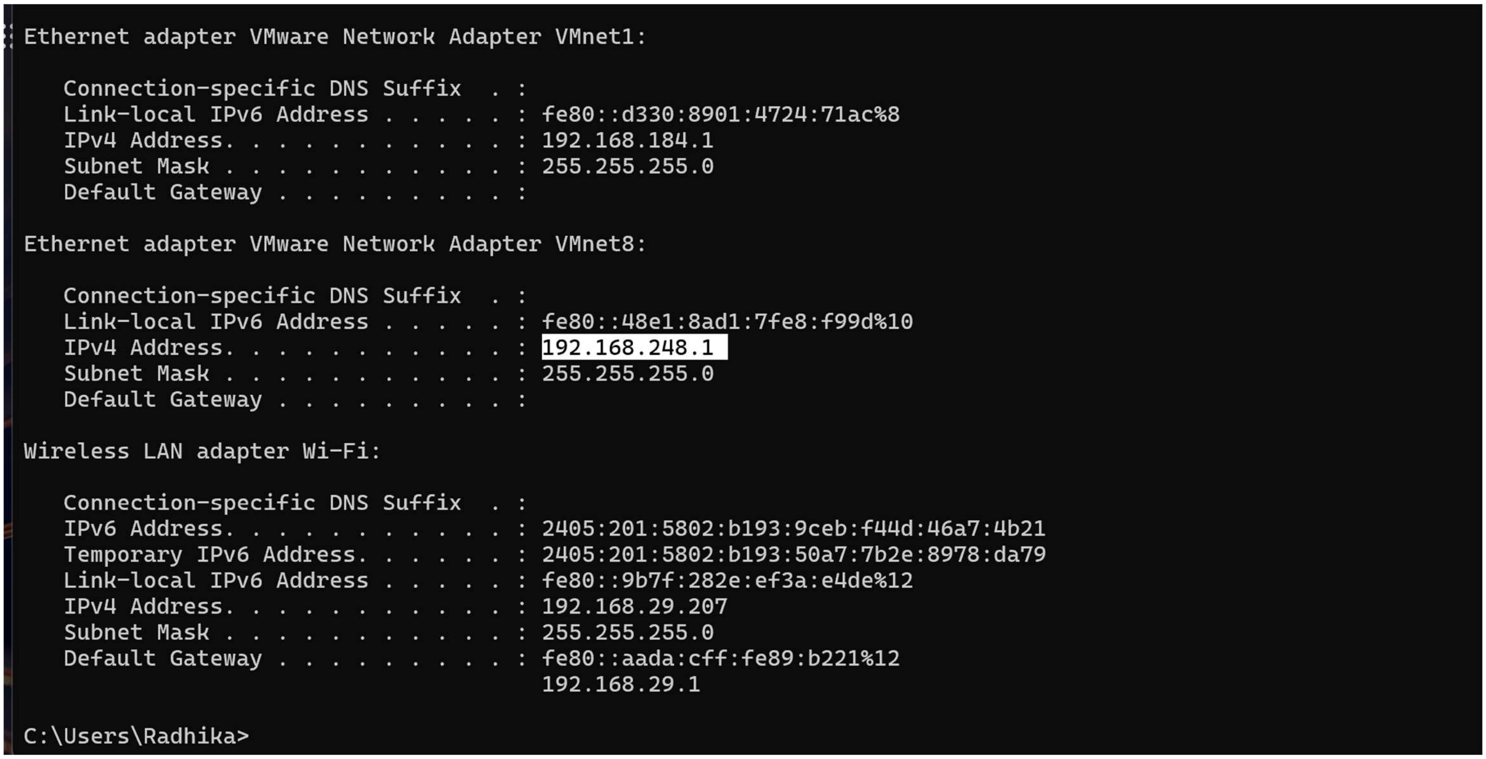
Nessus



NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.

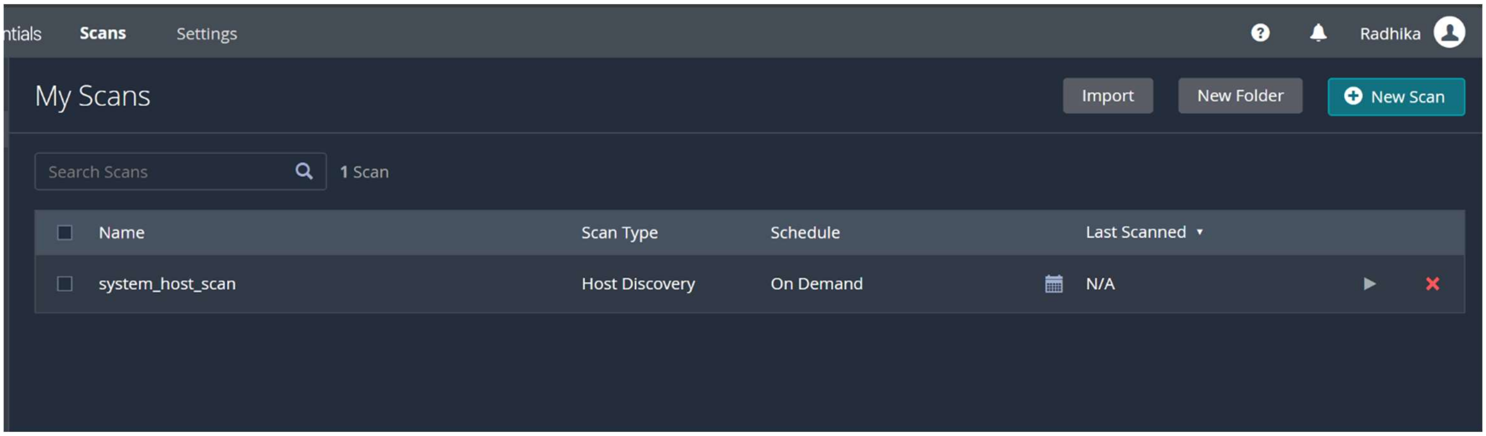
System's IP Address



```
Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d330:8901:4724:71ac%8
   IPv4 Address. . . . . . . . . . . : 192.168.184.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::48e1:8ad1:7fe8:f99d%10
   IPv4 Address. . . . . . . . . . . : 192.168.248.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2405:201:5802:b193:9ceb:f44d:46a7:4b21
   Temporary IPv6 Address. . . . . . : 2405:201:5802:b193:50a7:7b2e:8978:da79
   Link-local IPv6 Address . . . . . : fe80::9b7f:282e:ef3a:e4de%12
   IPv4 Address. . . . . . . . . . . : 192.168.29.207
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::aada:cff:fe89:b221%12
                                       192.168.29.1

C:\Users\Radhika>
```

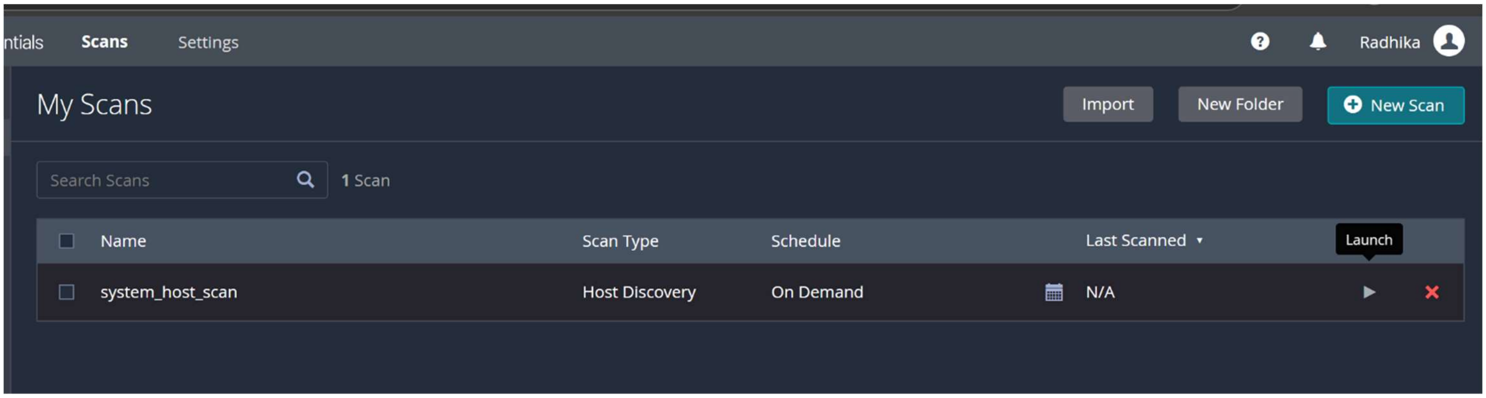
New Scan Started:

Host Scan



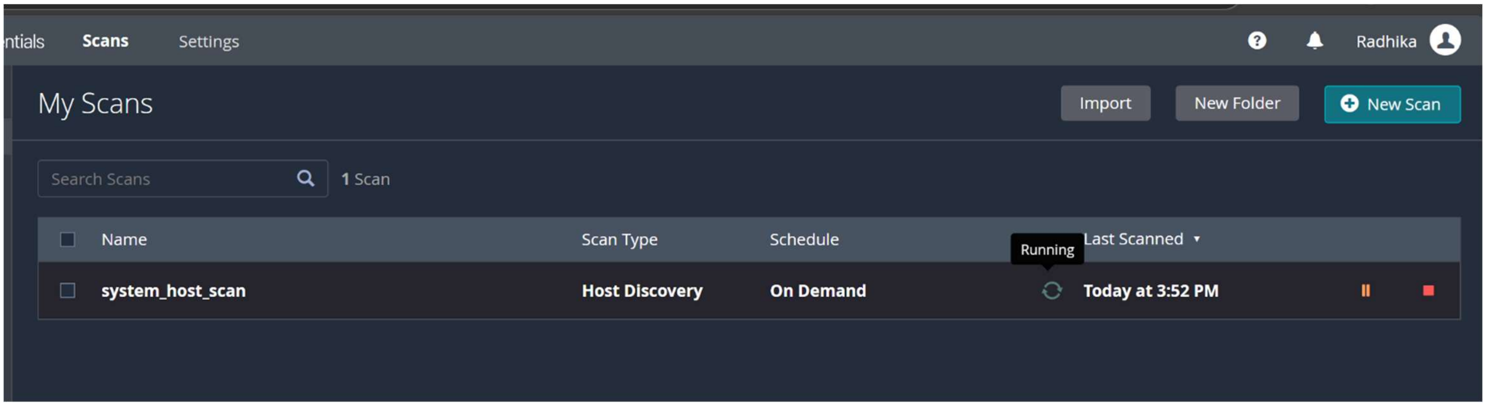
☐	Name	Scan Type	Schedule		Last Scanned ▾		
☐	system_host_scan	Host Discovery	On Demand	📅	N/A	▶	✕

Scan Launched



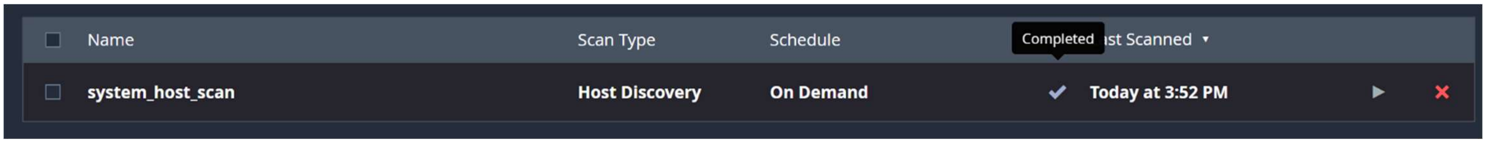
☐	Name	Scan Type	Schedule		Last Scanned ▾		
☐	system_host_scan	Host Discovery	On Demand	📅	N/A	▶	✕

Scan is running



☐	Name	Scan Type	Schedule		Last Scanned ▾		
☐	**system_host_scan**	**Host Discovery**	**On Demand**	⟳	**Today at 3:52 PM**	⏸	■

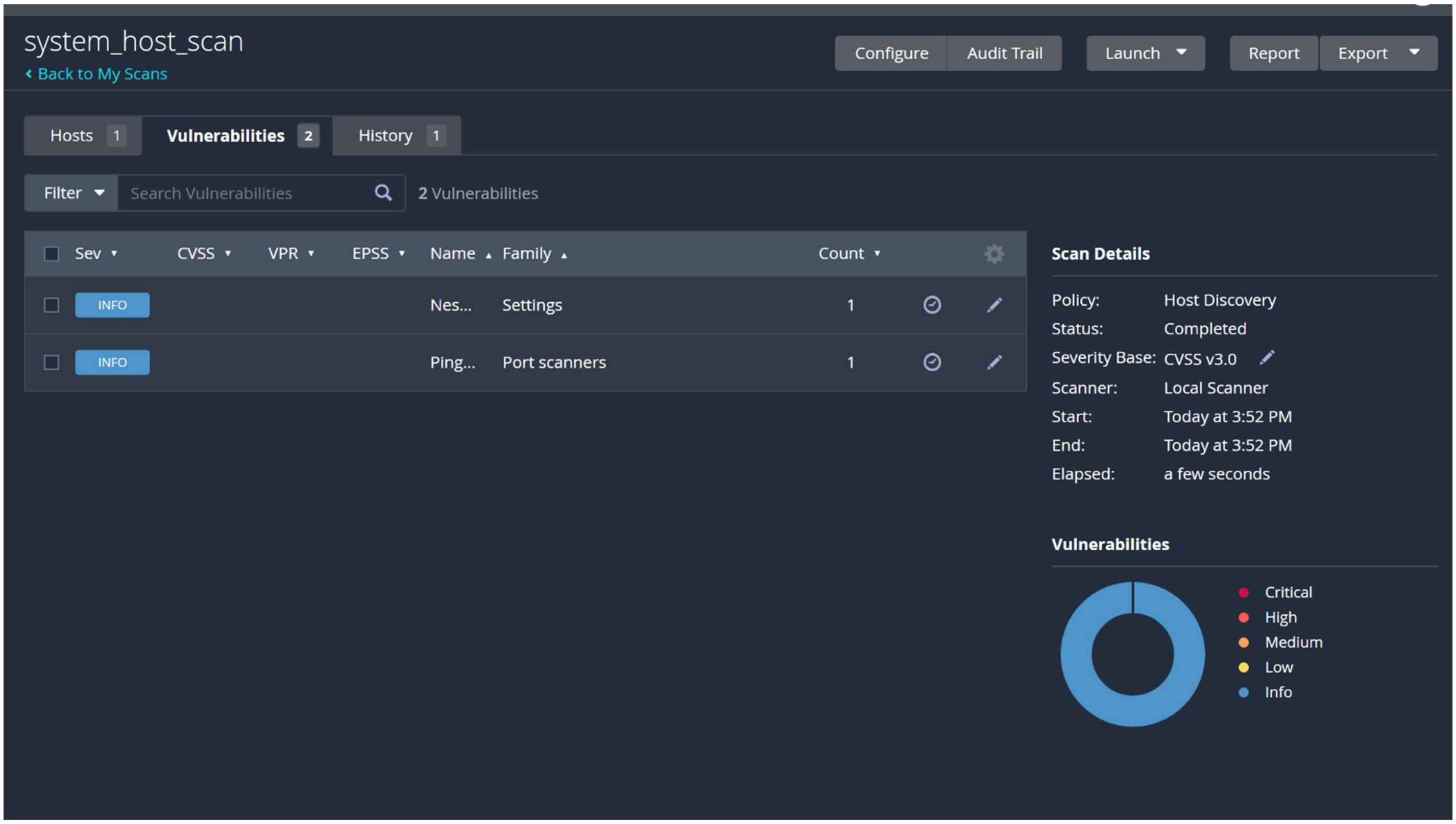
Scan is complete



☐	Name	Scan Type	Schedule		ıst Scanned ▾		
☐	**system_host_scan**	**Host Discovery**	**On Demand**	✓	**Today at 3:52 PM**	▶	✕

Here is the report

It shows that there are no vulnerabilities in the system host.



2 Vulnerabilities

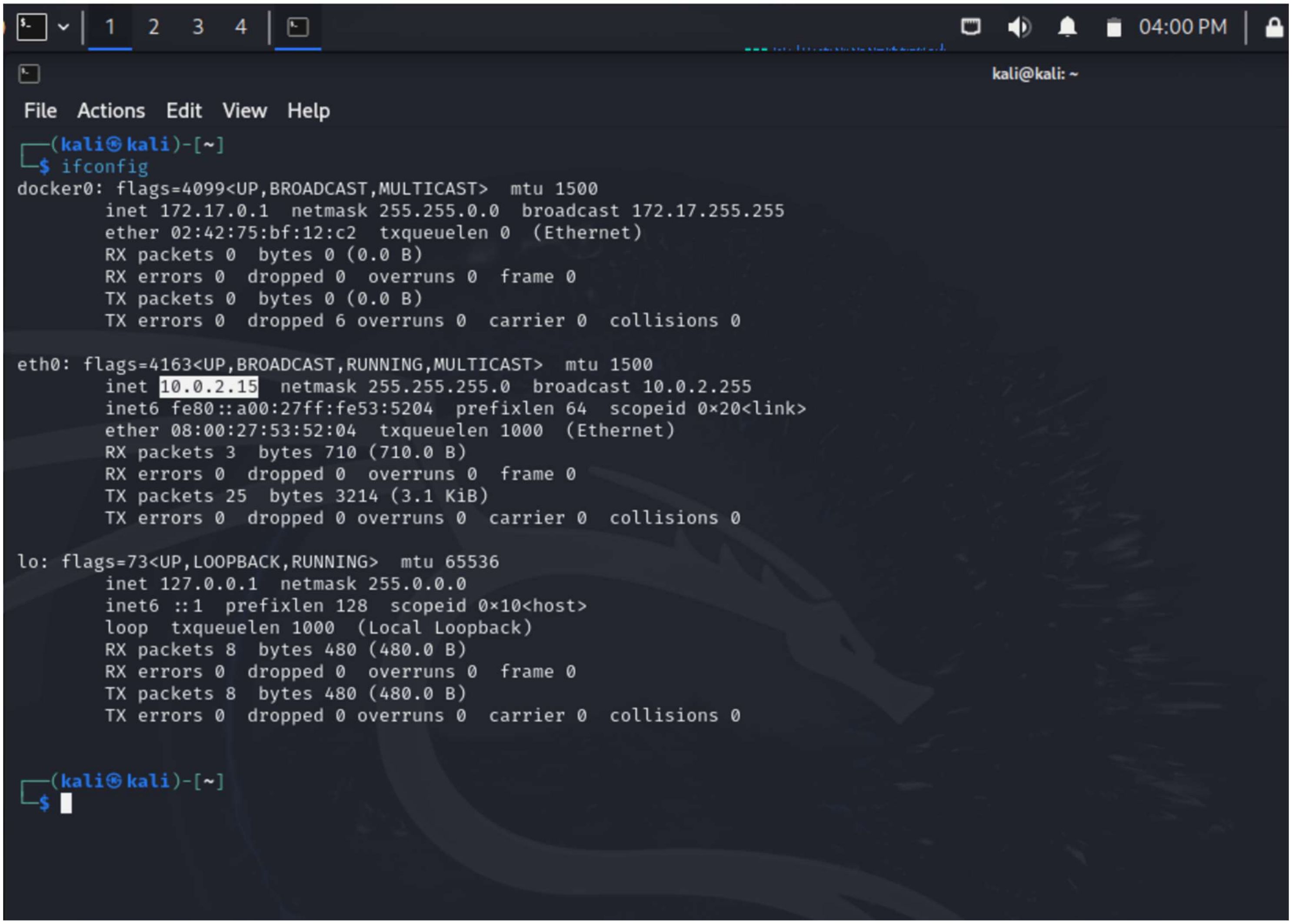
Sev	CVSS	VPR	EPSS	Name	Family	Count
INFO				Nes...	Settings	1
INFO				Ping...	Port scanners	1

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:52 PM
End: Today at 3:52 PM
Elapsed: a few seconds

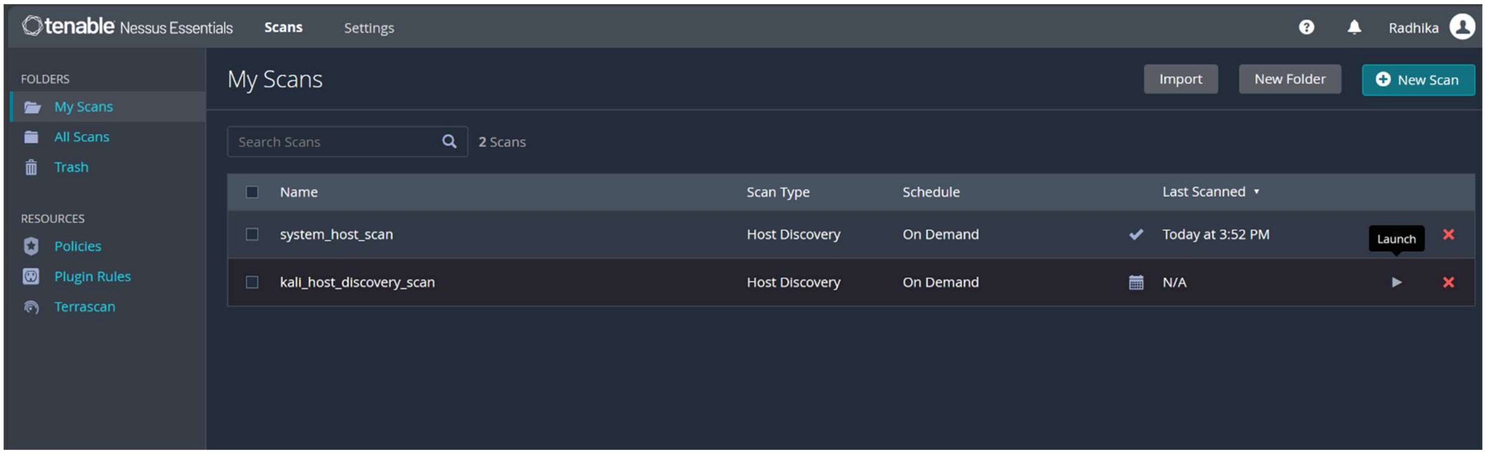
Vulnerabilities

Kali Linux IP Address



```
┌──(kali㉿kali)-[~]
└─$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:75:bf:12:c2  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 6 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe53:5204  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:53:52:04  txqueuelen 1000  (Ethernet)
        RX packets 3  bytes 710 (710.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3214 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ █
```

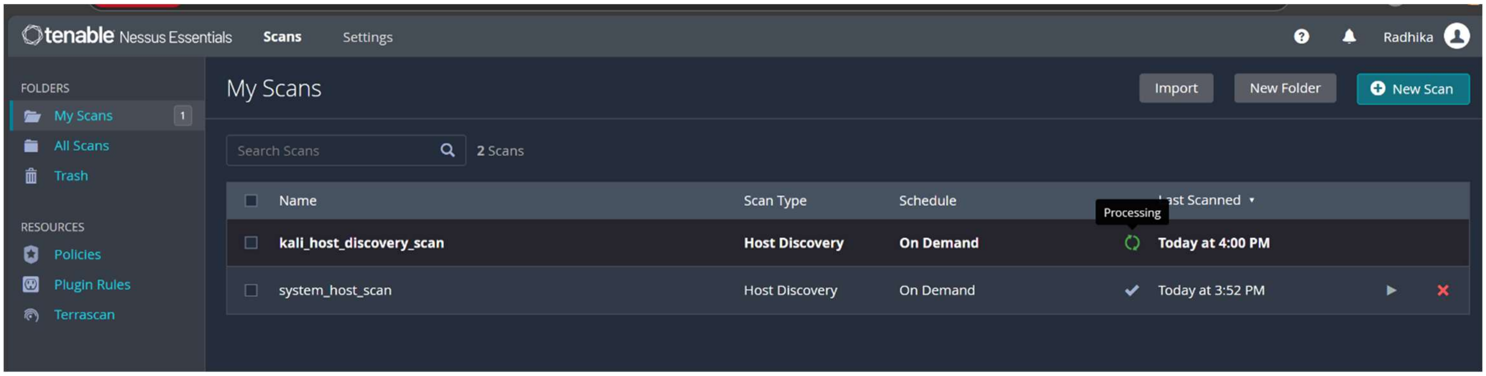
Launching Host Discovery scan on Kali Linux IP



My Scans

Search Scans 2 Scans

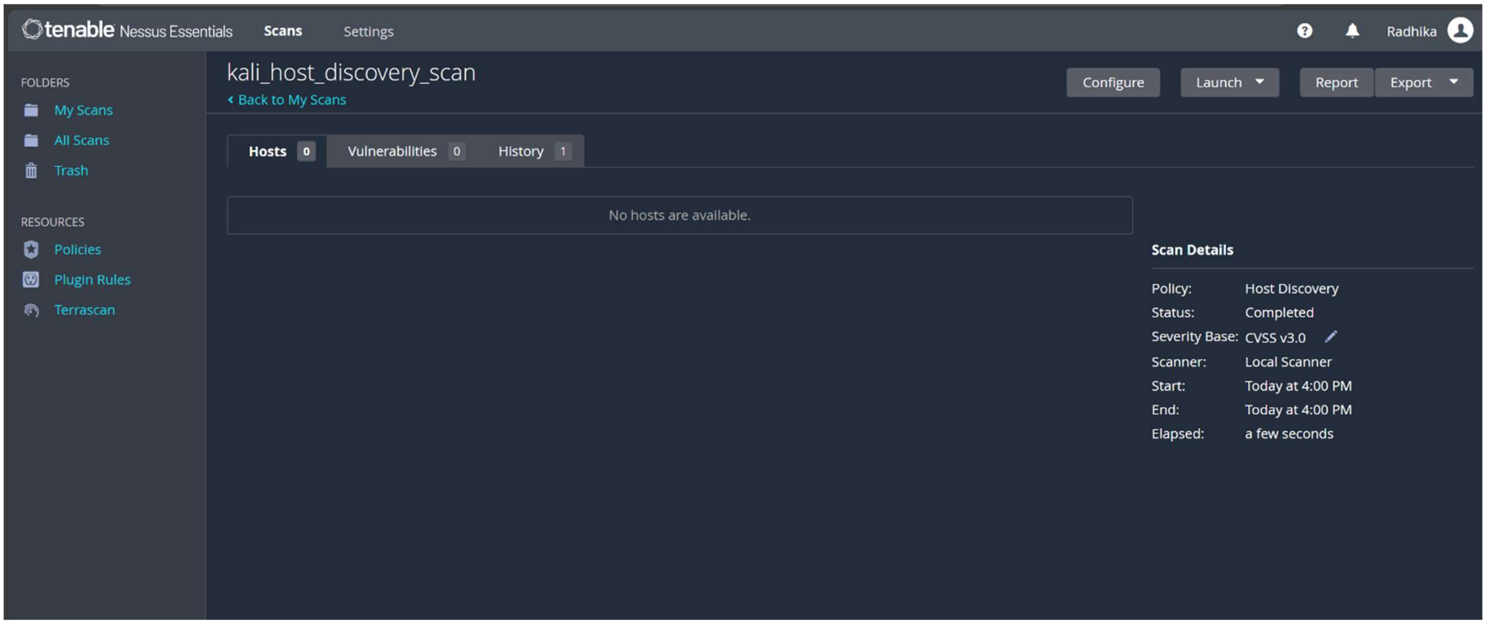
□	Name	Scan Type	Schedule		Last Scanned ▾		
□	system_host_scan	Host Discovery	On Demand	✓	Today at 3:52 PM		✕
□	kali_host_discovery_scan	Host Discovery	On Demand		N/A	▶	✕



My Scans

2 Scans

Name	Scan Type	Schedule	Last Scanned
kali_host_discovery_scan	Host Discovery	On Demand	Today at 4:00 PM
system_host_scan	Host Discovery	On Demand	✓ Today at 3:52 PM



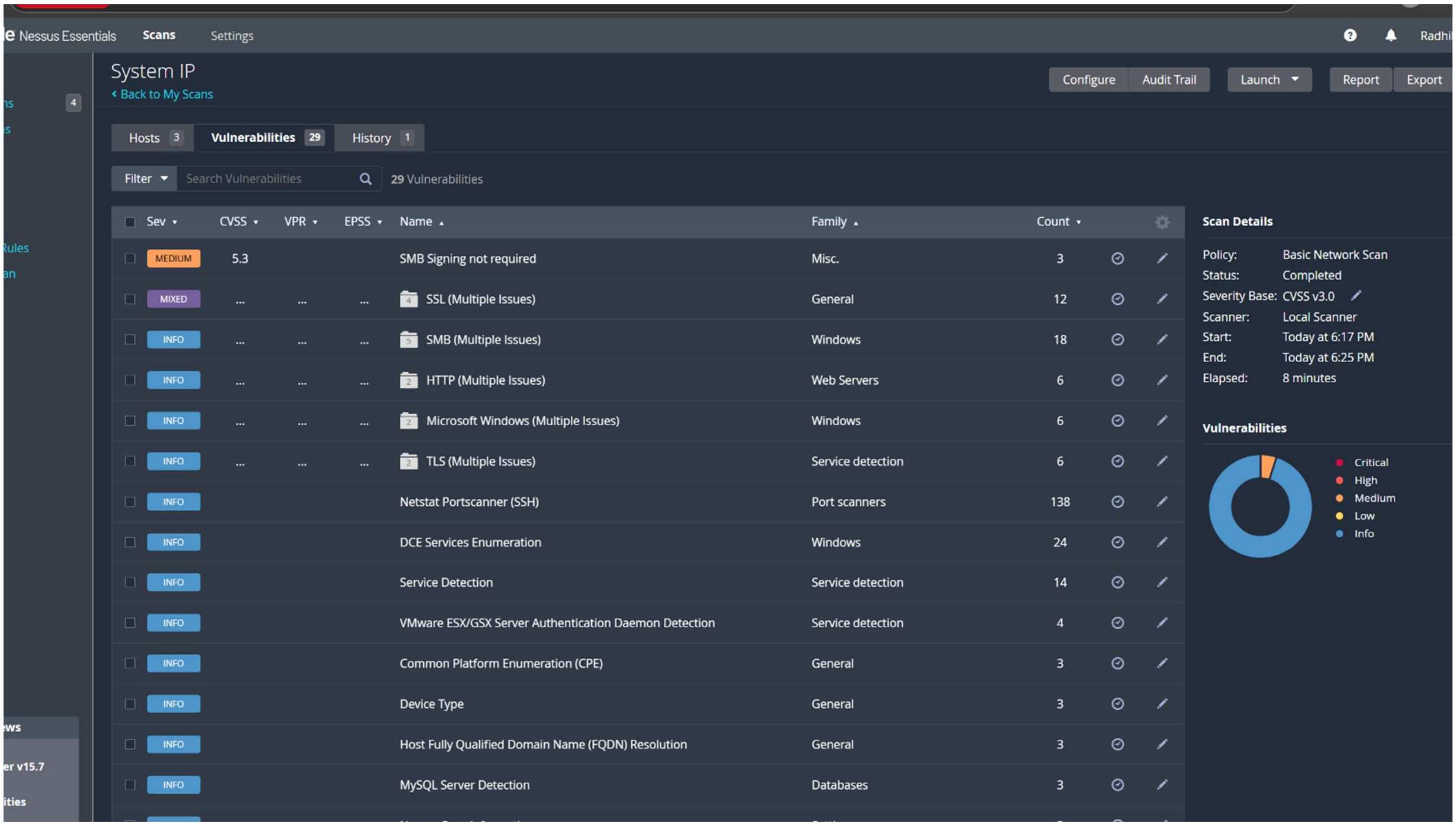
kali_host_discovery_scan

No hosts are available.

Scan Details

Policy: Host Discovery
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:00 PM
End: Today at 4:00 PM
Elapsed: a few seconds

SIMILARLY, ALL SCANS ARE PERFORMED, AND IT IS CONCLUDED THAT THE SYSTEM HAS SOME VULNERABILITIES, AS SHOWN IN THE ATTACHED SCREENSHOT BELOW.



System IP

‹ Back to My Scans

Hosts 3 | Vulnerabilities 29 | History 1

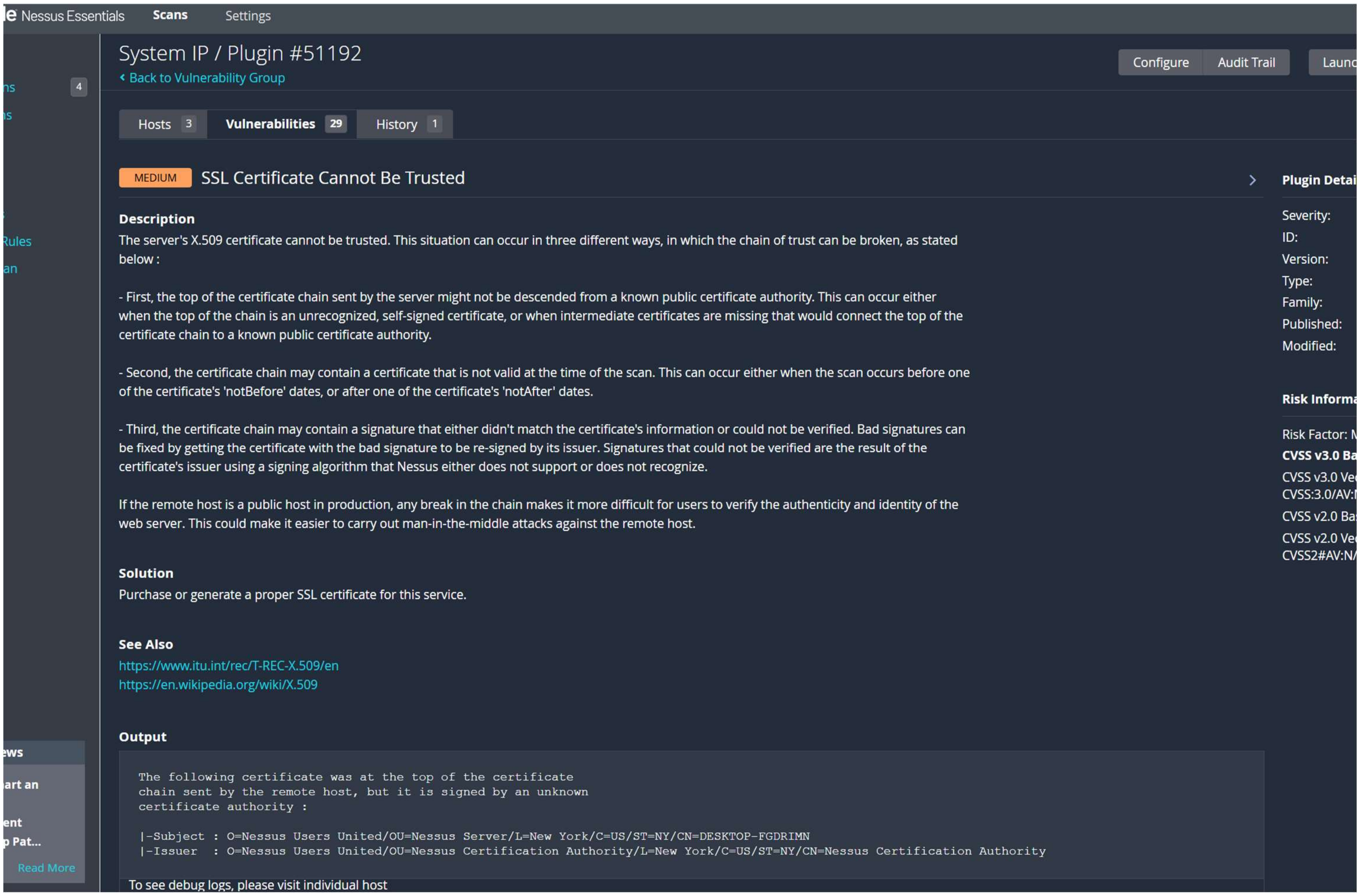
Filter | Search Vulnerabilities | 29 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
MEDIUM	5.3			SMB Signing not required	Misc.	3
MIXED	...	...	...	4 SSL (Multiple Issues)	General	12
INFO	...	...	...	5 SMB (Multiple Issues)	Windows	18
INFO	...	...	...	2 HTTP (Multiple Issues)	Web Servers	6
INFO	...	...	...	2 Microsoft Windows (Multiple Issues)	Windows	6
INFO	...	...	...	2 TLS (Multiple Issues)	Service detection	6
INFO				Netstat Portscanner (SSH)	Port scanners	138
INFO				DCE Services Enumeration	Windows	24
INFO				Service Detection	Service detection	14
INFO				VMware ESX/GSX Server Authentication Daemon Detection	Service detection	4
INFO				Common Platform Enumeration (CPE)	General	3
INFO				Device Type	General	3
INFO				Host Fully Qualified Domain Name (FQDN) Resolution	General	3
INFO				MySQL Server Detection	Databases	3

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 6:17 PM
End: Today at 6:25 PM
Elapsed: 8 minutes

Vulnerabilities



System IP / Plugin #51192

‹ Back to Vulnerability Group

Hosts 3 | Vulnerabilities 29 | History 1

MEDIUM SSL Certificate Cannot Be Trusted

Description

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.

If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

Solution

Purchase or generate a proper SSL certificate for this service.

See Also

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

Output

```
The following certificate was at the top of the certificate
chain sent by the remote host, but it is signed by an unknown
certificate authority :

|-Subject : O=Nessus Users United/OU=Nessus Server/L=New York/C=US/ST=NY/CN=DESKTOP-FGDRIMN
|-Issuer  : O=Nessus Users United/OU=Nessus Certification Authority/L=New York/C=US/ST=NY/CN=Nessus Certification Authority
```

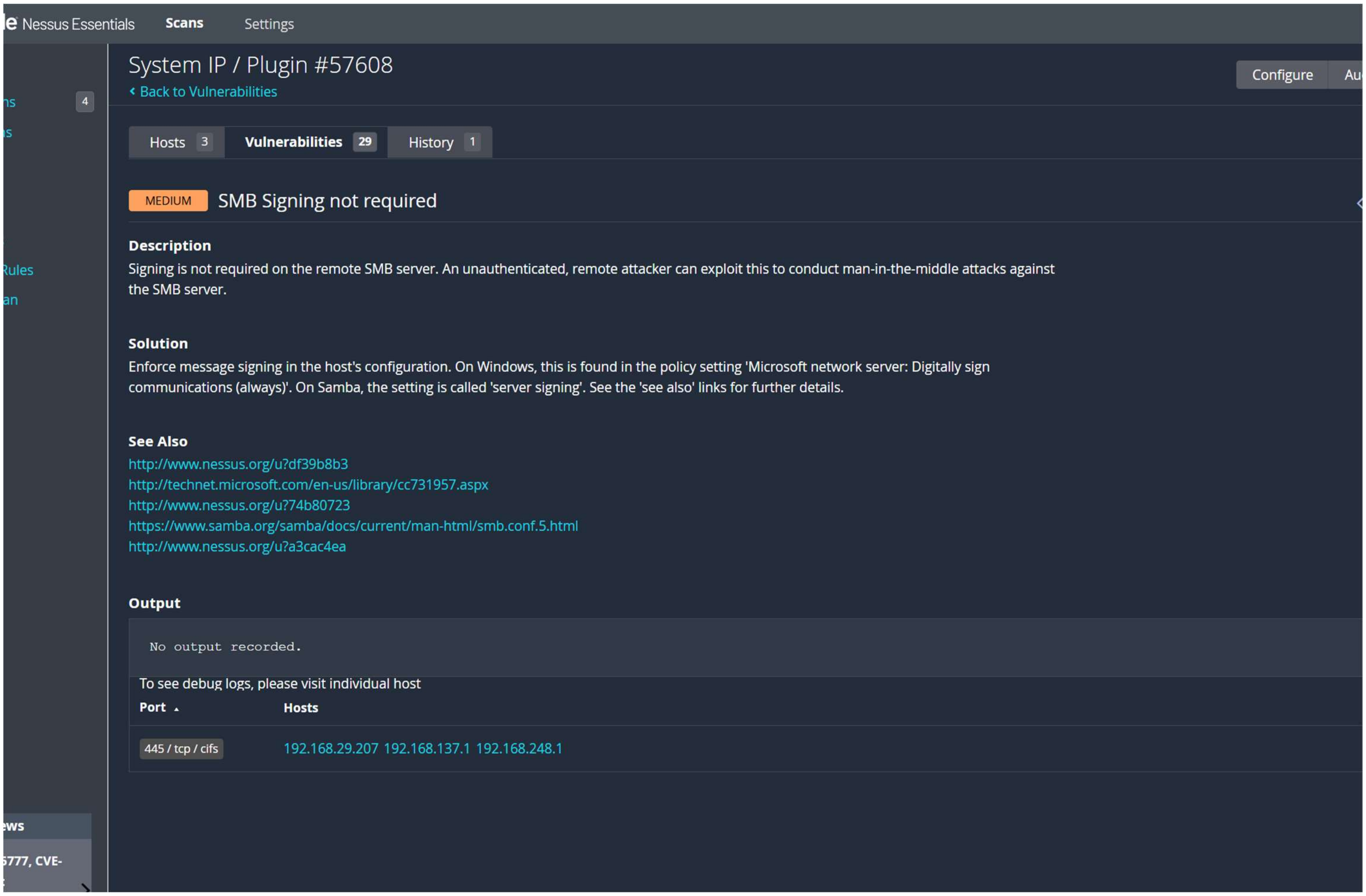
To see debug logs, please visit individual host

Plugin Detai

Severity:
ID:
Version:
Type:
Family:
Published:
Modified:

Risk Informa

Risk Factor: M
CVSS v3.0 Ba
CVSS v3.0 Ve
CVSS:3.0/AV:N
CVSS v2.0 Ba
CVSS v2.0 Ve
CVSS2#AV:N/



System IP / Plugin #57608

‹ Back to Vulnerabilities

MEDIUM SMB Signing not required

Description

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Solution

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

See Also

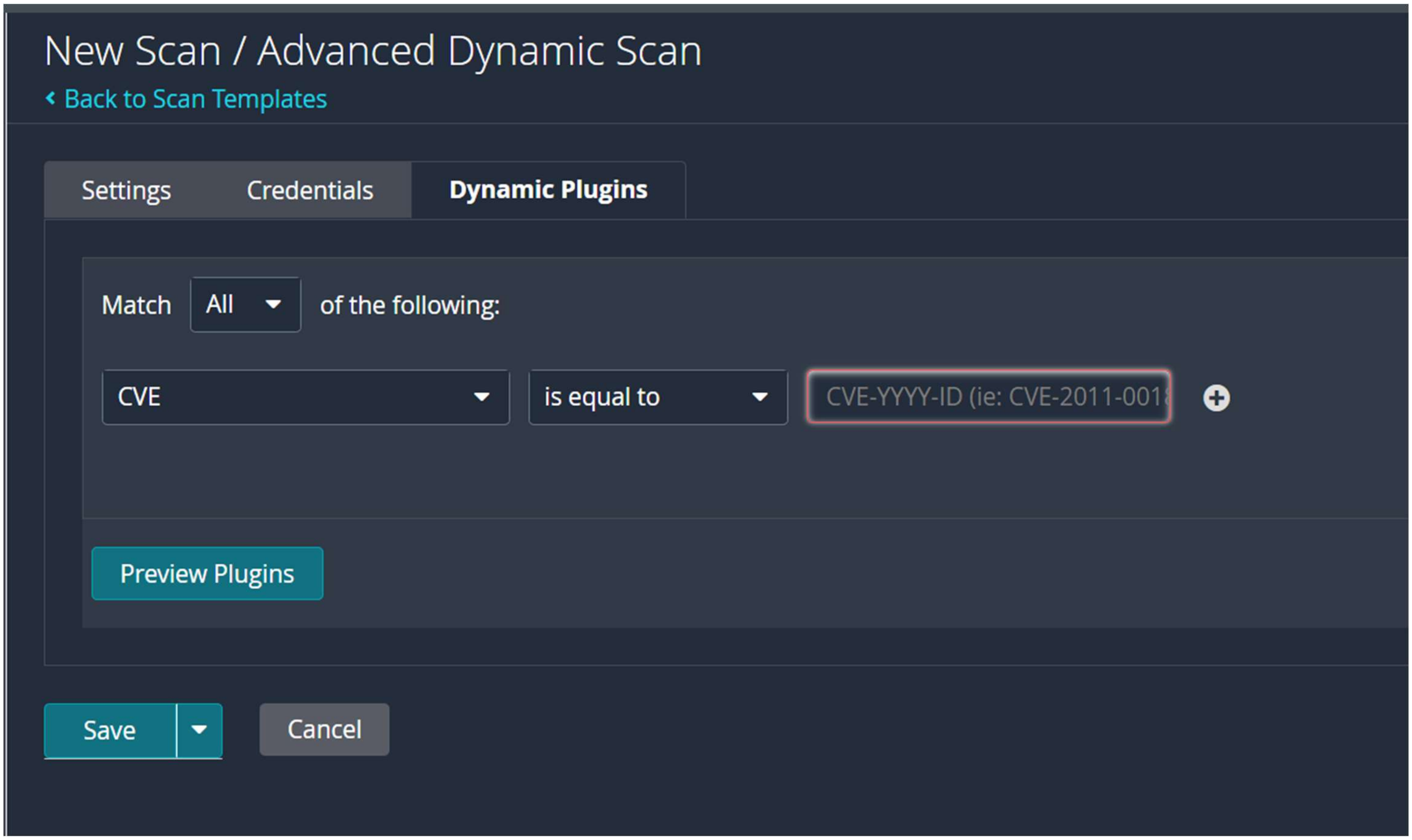
http://www.nessus.org/u?df39b8b3
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▴	Hosts
445 / tcp / cifs	192.168.29.207 192.168.137.1 192.168.248.1

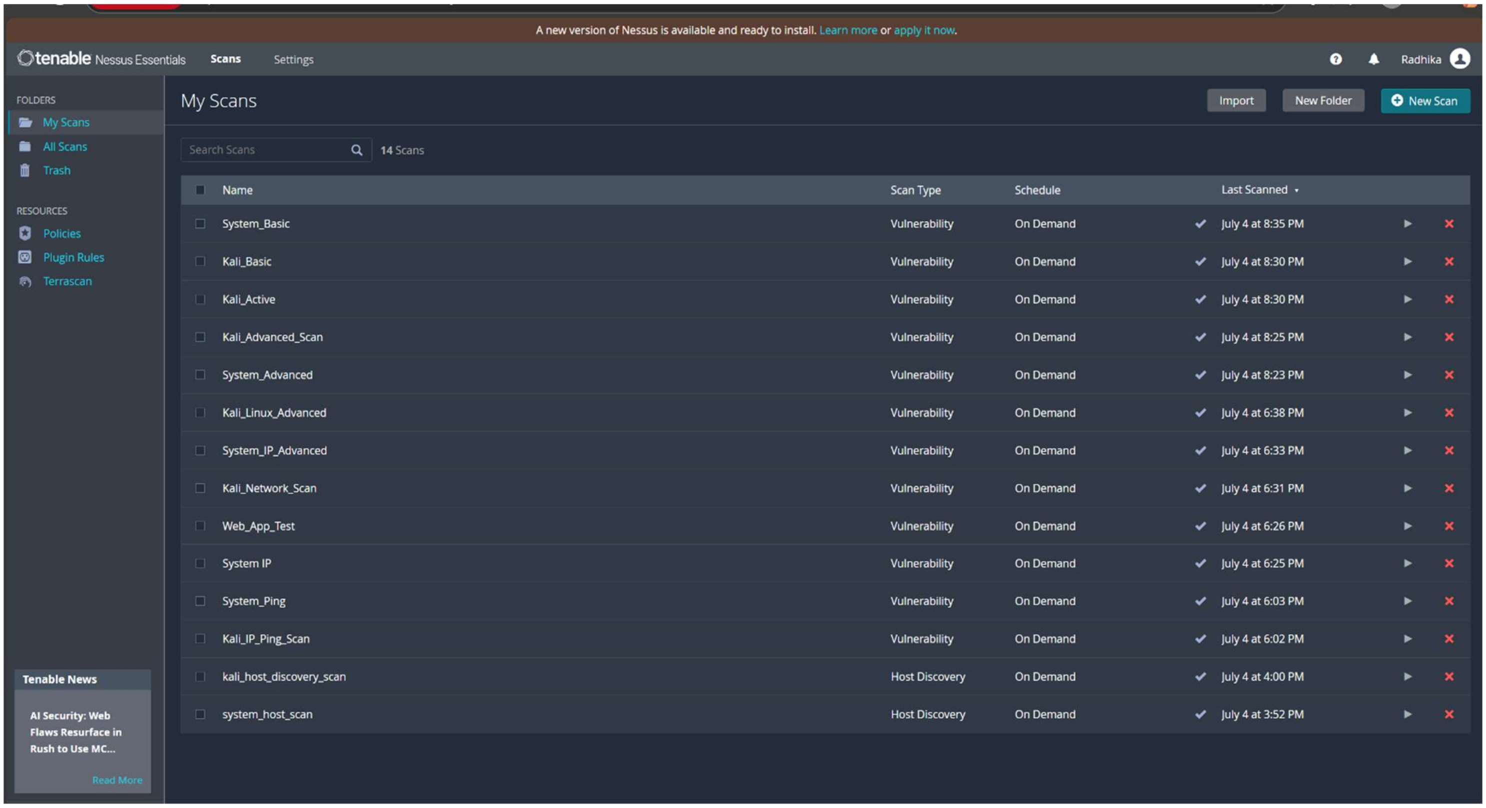


New Scan / Advanced Dynamic Scan

‹ Back to Scan Templates

Match All ▾ of the following:

CVE ▾ is equal to ▾ CVE-YYYY-ID (ie: CVE-2011-001



A new version of Nessus is available and ready to install. Learn more or apply it now.

Tenable News

AI Security: Web Flaws Resurface in Rush to Use MC...

Read More

My Scans

14 Scans

Name	Scan Type	Schedule	Last Scanned
System_Basic	Vulnerability	On Demand	✓ July 4 at 8:35 PM
Kali_Basic	Vulnerability	On Demand	✓ July 4 at 8:30 PM
Kali_Active	Vulnerability	On Demand	✓ July 4 at 8:30 PM
Kali_Advanced_Scan	Vulnerability	On Demand	✓ July 4 at 8:25 PM
System_Advanced	Vulnerability	On Demand	✓ July 4 at 8:23 PM
Kali_Linux_Advanced	Vulnerability	On Demand	✓ July 4 at 6:38 PM
System_IP_Advanced	Vulnerability	On Demand	✓ July 4 at 6:33 PM
Kali_Network_Scan	Vulnerability	On Demand	✓ July 4 at 6:31 PM
Web_App_Test	Vulnerability	On Demand	✓ July 4 at 6:26 PM
System IP	Vulnerability	On Demand	✓ July 4 at 6:25 PM
System_Ping	Vulnerability	On Demand	✓ July 4 at 6:03 PM
Kali_IP_Ping_Scan	Vulnerability	On Demand	✓ July 4 at 6:02 PM
kali_host_discovery_scan	Host Discovery	On Demand	✓ July 4 at 4:00 PM
system_host_scan	Host Discovery	On Demand	✓ July 4 at 3:52 PM