VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

School of Information Technology and Engineering

Lab Assessment-V, SEPTEMBER 2020

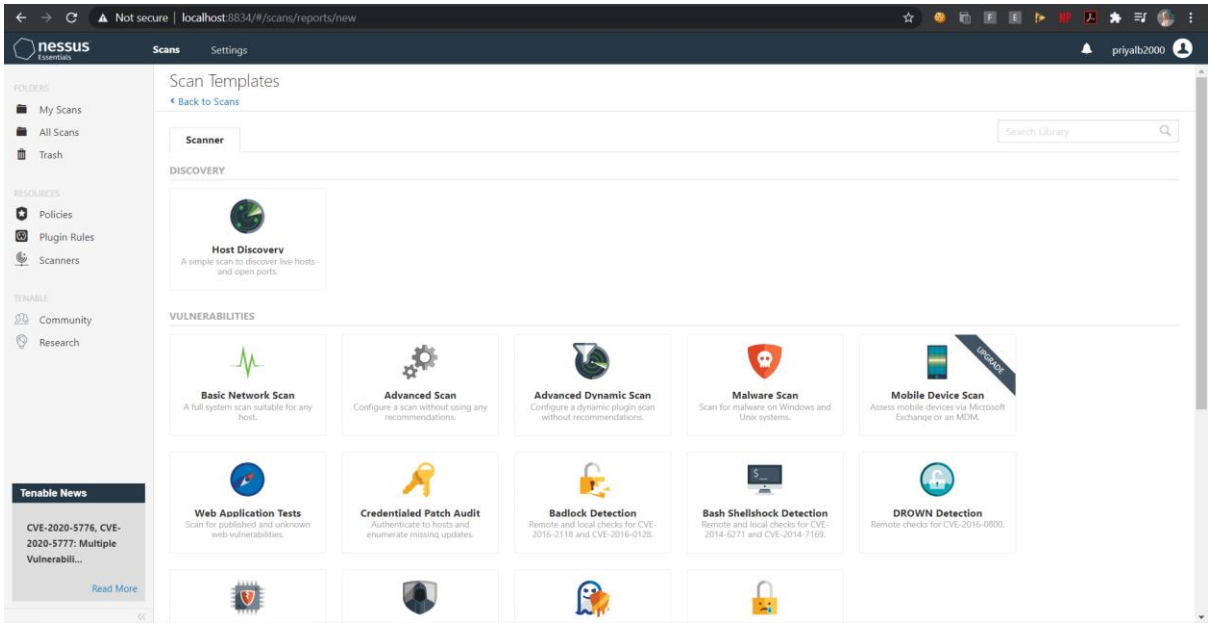
B.Tech., Fall-2020-2021

NAME	PRIYAL BHARDWAJ
REG. NO.	18BIT0272
COURSE CODE	CSE3501
COURSE NAME	INFORMATION SECURITY ANALYSIS & AUDIT
SLOT	L19+L20
FACULTY	Prof. THANDEESWARAN R.

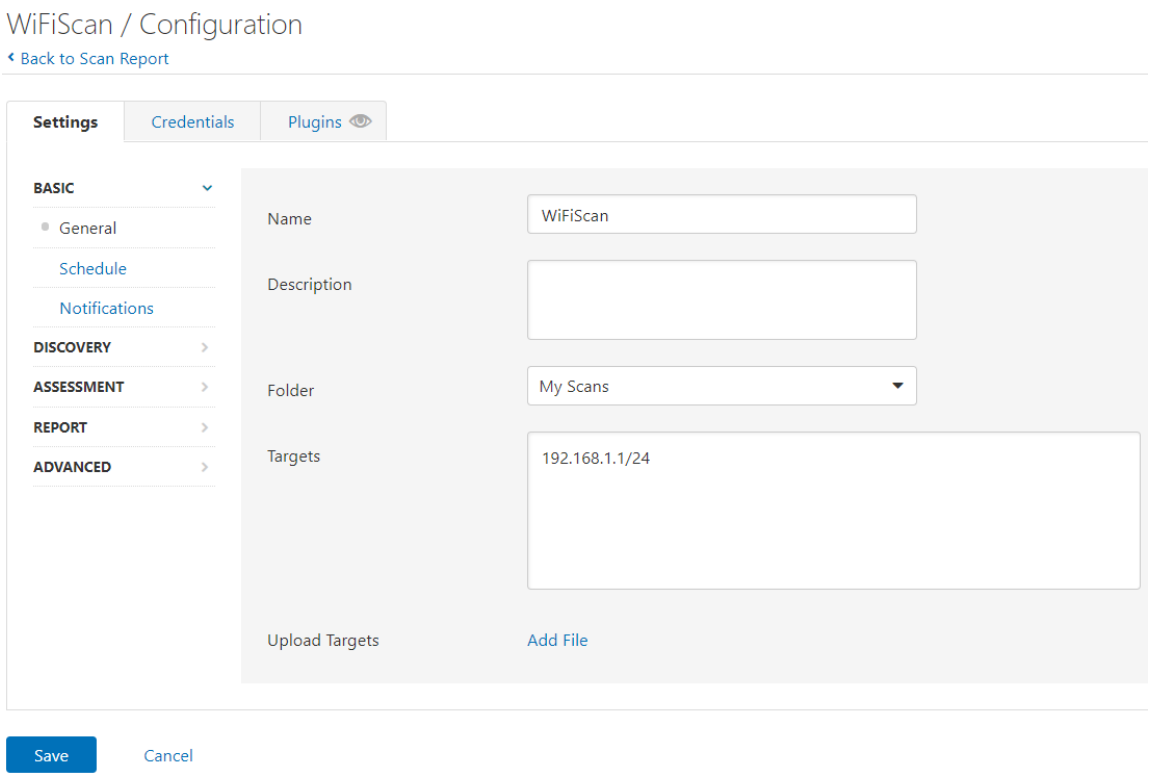
Install Nessus (https://www.tenable.com/downloads/nessus) and prepare a
report that includes

- Descriptive Report on the Identified Vulnerabilities
- Graphical Report
- Basic Network Scan
- Advanced Scan
- Dynamic Scan
- Malware Scan
- Web Application Vulnerability scan / plugin #49704 – External ULs
- Web Application Vulnerability scan / plugin #85582 – Clickjacking
- Badlock detection / SYN scanner
- Scanner health

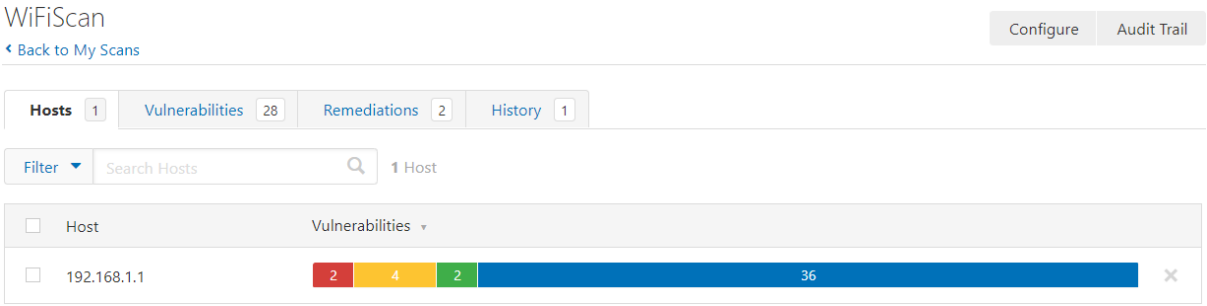
Installed Nessus and created a Login:



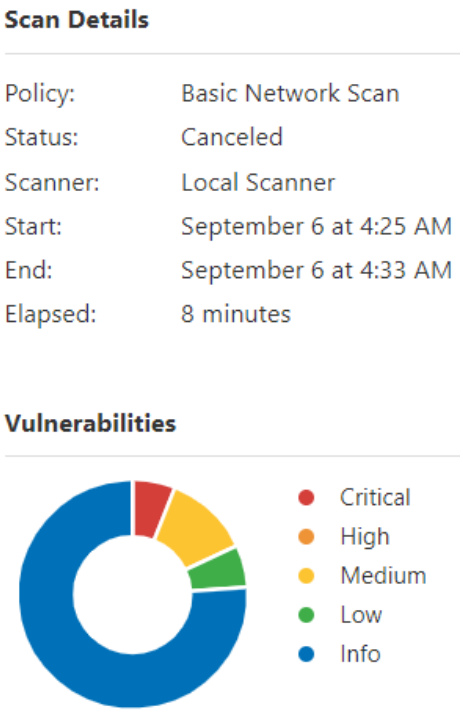
Selected **Basic Network Scan**:
Name: WiFiScan
Folder: My Scans
Targets: 192.168.1.1/24 (IP Address of my home WiFi router)



Scan details – Hosts:



Graphical Report



Scan details – Vulnerabilities (sorted by Count): (Report on identified vulnerabilities)

WiFiScan

Configure | Audit Trail

‹ Back to My Scans

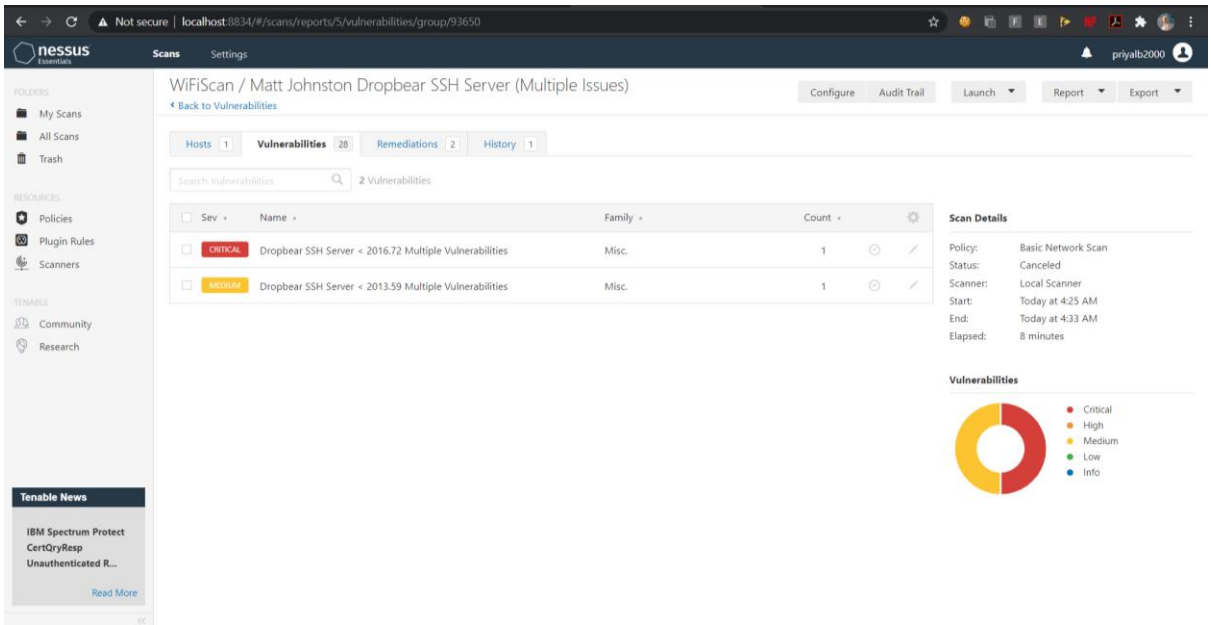
Hosts 1 | **Vulnerabilities 28** | Remediations 2 | History 1

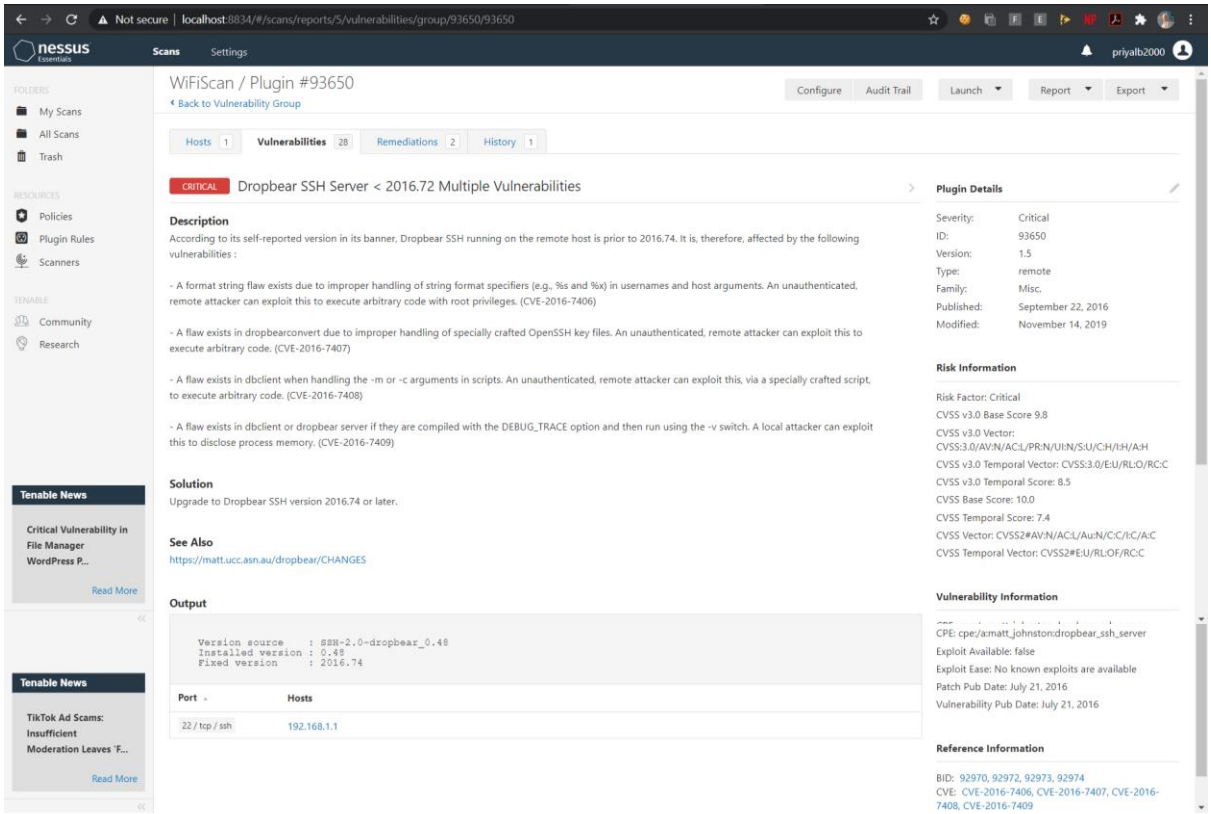
Filter | Search Vulnerabilities | **28** Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Treck TCP/IP stack multiple vulnerabilities. (Ripple20)	Misc.	1
MEDIUM	IP Forwarding Enabled	Firewalls	1
MEDIUM	Unencrypted Telnet Server	Misc.	1
LOW	DHCP Server Detection	Service detection	1
INFO	Device Type	General	1
INFO	DNS Server Detection	DNS	1
INFO	Ethernet Card Manufacturer Detection	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	ICMP Netmask Request Information Disclosure	General	1
INFO	Nessus Scan Information	Settings	1
INFO	No Credentials Provided	Settings	1
INFO	OS Identification	General	1
INFO	Patch Report	General	1
INFO	SSH Protocol Versions Supported	General	1
INFO	SSH Server Type and Version Information	Service detection	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	Telnet Server Detection	Service detection	1
INFO	Traceroute Information	General	1
INFO	Treck/Kasago Network Stack Detection With IP Option.	Service detection	1
INFO	Universal Plug and Play (UPnP) Protocol Detection	Service detection	1
INFO	Web Server No 404 Error Code Check	Web Servers	1
MIXED	2 Matt Johnston Dropbear SSH Server (Multiple Issues)	Misc.	2
INFO	2 FTP (Multiple Issues)	Service detection	2
INFO	Web Server UPnP Detection	Service detection	2
MIXED	3 SSH (Multiple Issues)	Misc.	3
INFO	2 HTTP (Multiple Issues)	Web Servers	3
INFO	Service Detection	Service detection	5
INFO	Nessus SYN scanner	Port scanners	6

Vulnerability details for “Matt Johnston Dropbear SSH Server (Multiple Issues) → Dropbear SSH Server < 2016.72 Multiple Vulnerabilities”

(Since 33 vulnerabilities were identified, the report would be too long if each one’s rdetails are included.)





Note: The downloaded Vulnerabilty Report has been merged with this document. Scroll down to view.

WiFiScan

Report generated by Nessus™

Sun, 06 Sep 2020 04:33:10 India Standard Time

Nessus Essentials

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.1.1.....4

Nessus Essentials

Hosts Executive Summary

Nessus Essentials

192.168.1.1

2	0	4	2	25
CRITICAL	HIGH	MEDIUM	LOW	INFO

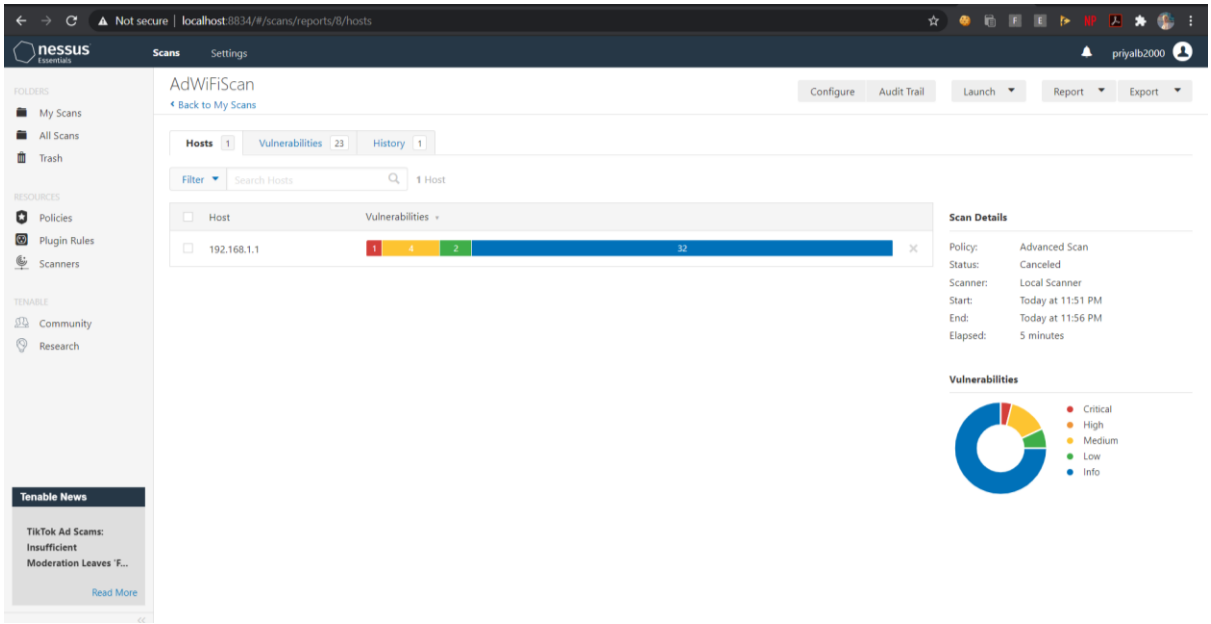
Vulnerabilities Total: 33

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
CRITICAL	10.0	137702	Treck TCP/IP stack multiple vulnerabilities. (Ripple20)
MEDIUM	5.8	50686	IP Forwarding Enabled
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
MEDIUM	5.0	121007	SSH Known Hard Coded Private Keys
LOW	3.3	10663	DHCP Server Detection
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
INFO	N/A	10113	ICMP Netmask Request Information Disclosure
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	110723	No Credentials Provided

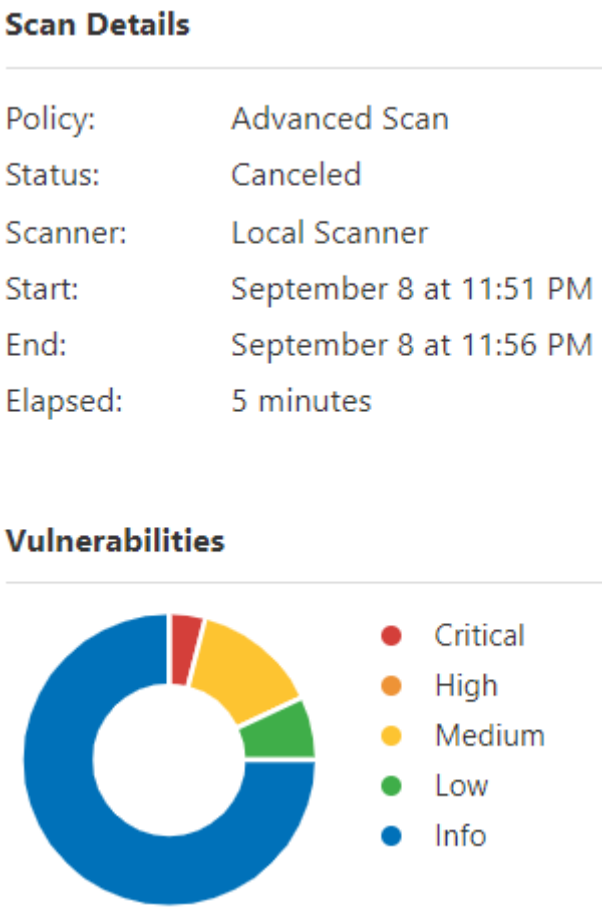
Nessus Essentials

INFO	N/A	11936	OS Identification
INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	138615	Treck/Kasago Network Stack Detection With IP Option.
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	35712	Web Server UPnP Detection

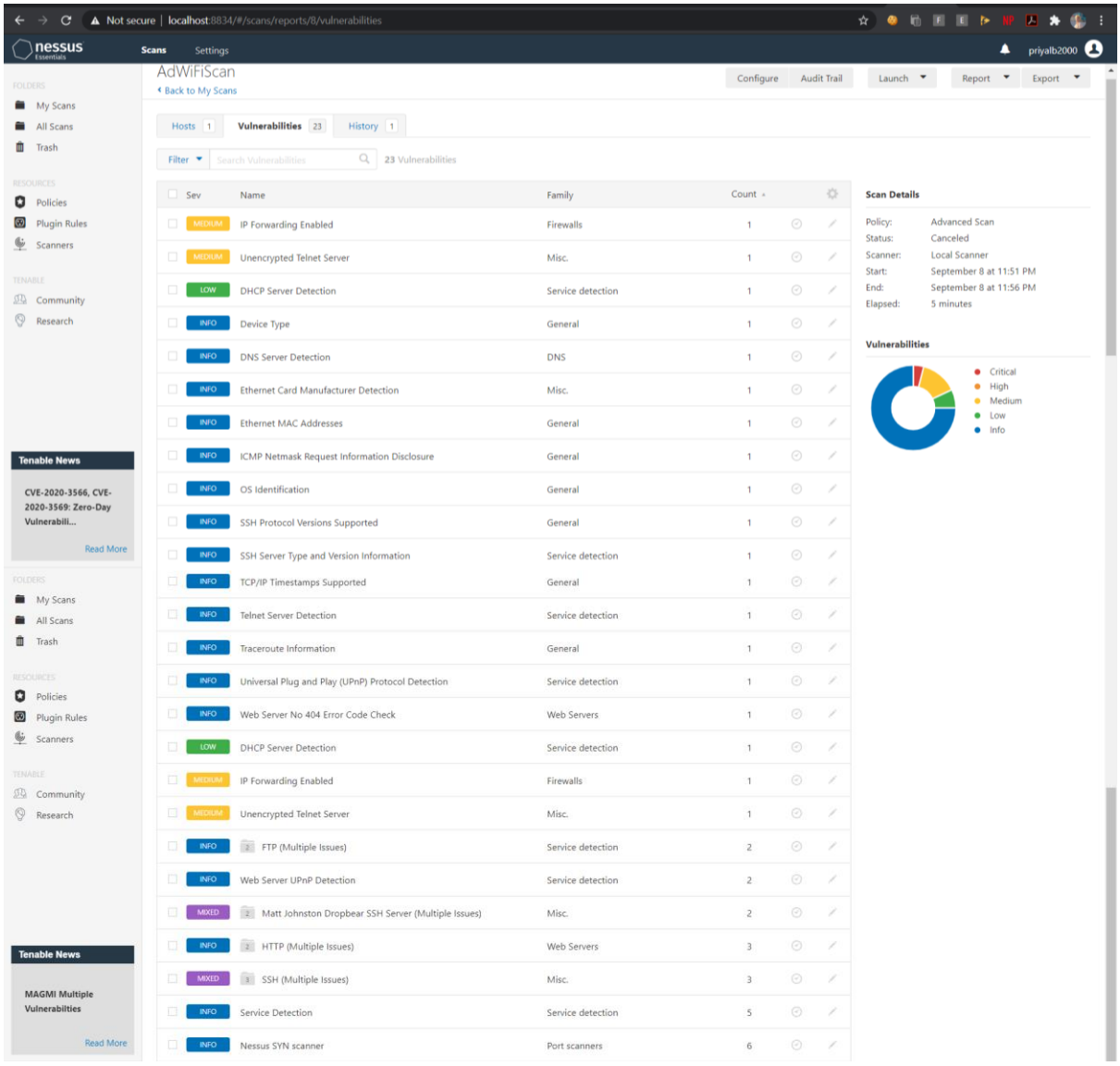
Selected **Advanced Scan**:
Name: AdWiFiScan
Folder: My Scans
Targets: 192.168.1.1/24 (IP Address of my home WiFi router)



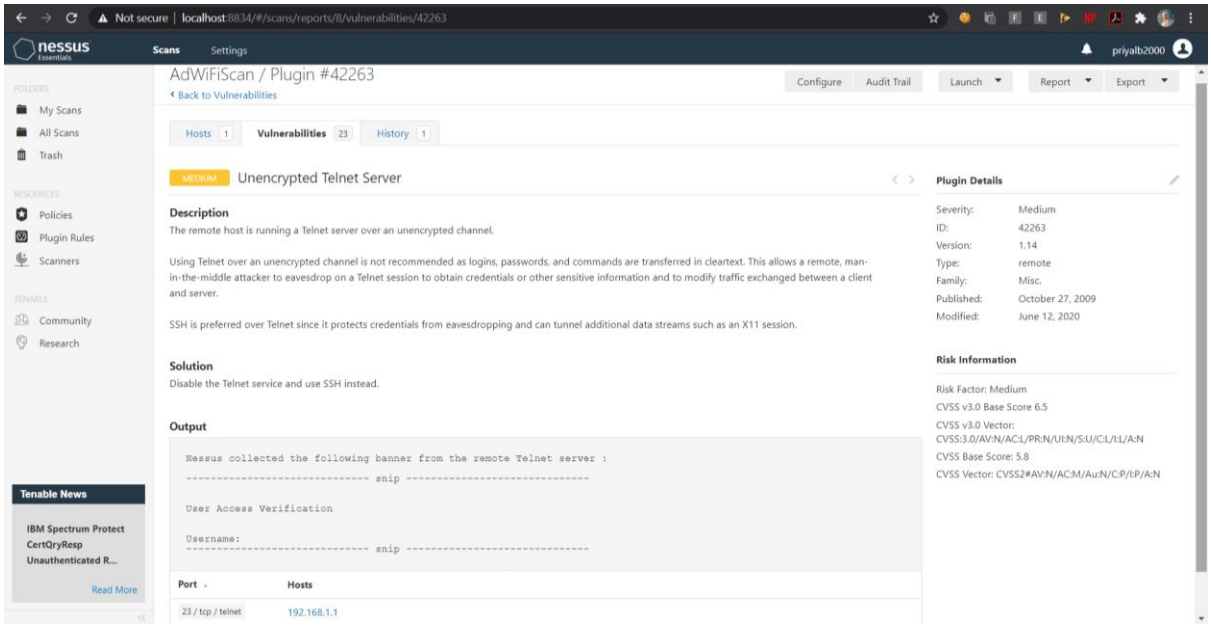
Graphical Report:



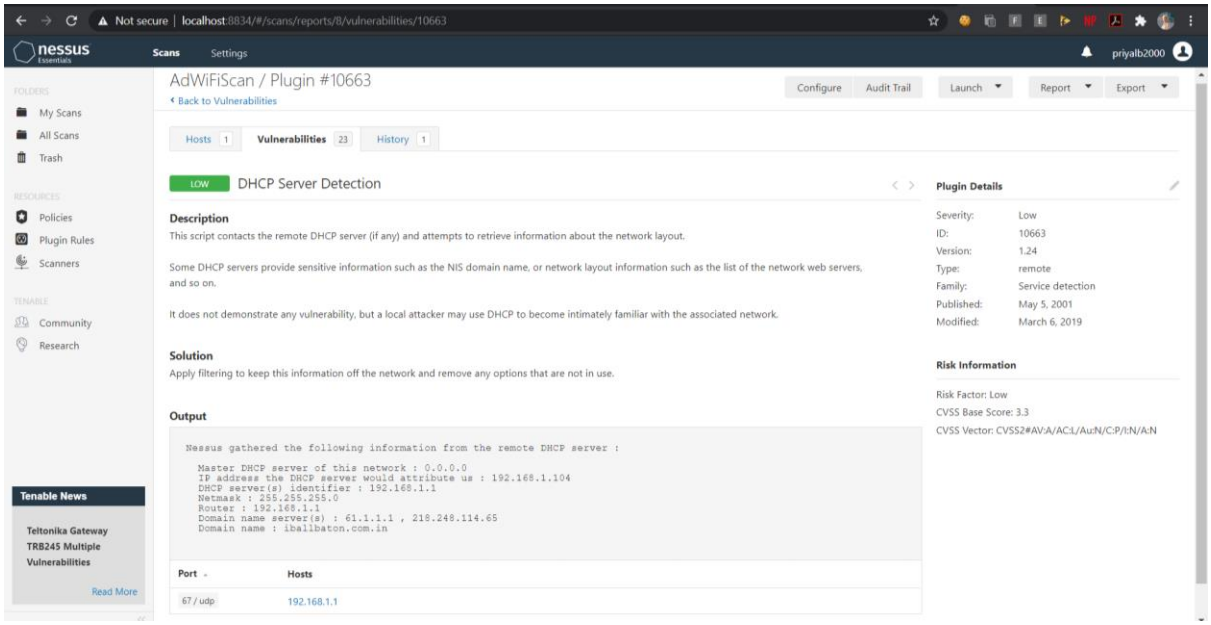
Scan details – Vulnerabilities (sorted by Count):
(Report on identified vulnerabilities)



Vulnerability details for “Unencrypted Telnet Server”



Vulnerability details for “DHCP Server Detection”



(Since 23 vulnerabilities were identified, the report would be too long if each one’s rdetails are included.)

Note: The downloaded Vulnerabilty Report has been merged with this document. Scroll down to view.

AdWiFiScan

Report generated by Nessus™

Tue, 08 Sep 2020 23:56:21 India Standard Time

Nessus Essentials

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.1.1.....4

Nessus Essentials

Hosts Executive Summary

Nessus Essentials

192.168.1.1

1	0	4	2	21
CRITICAL	HIGH	MEDIUM	LOW	INFO

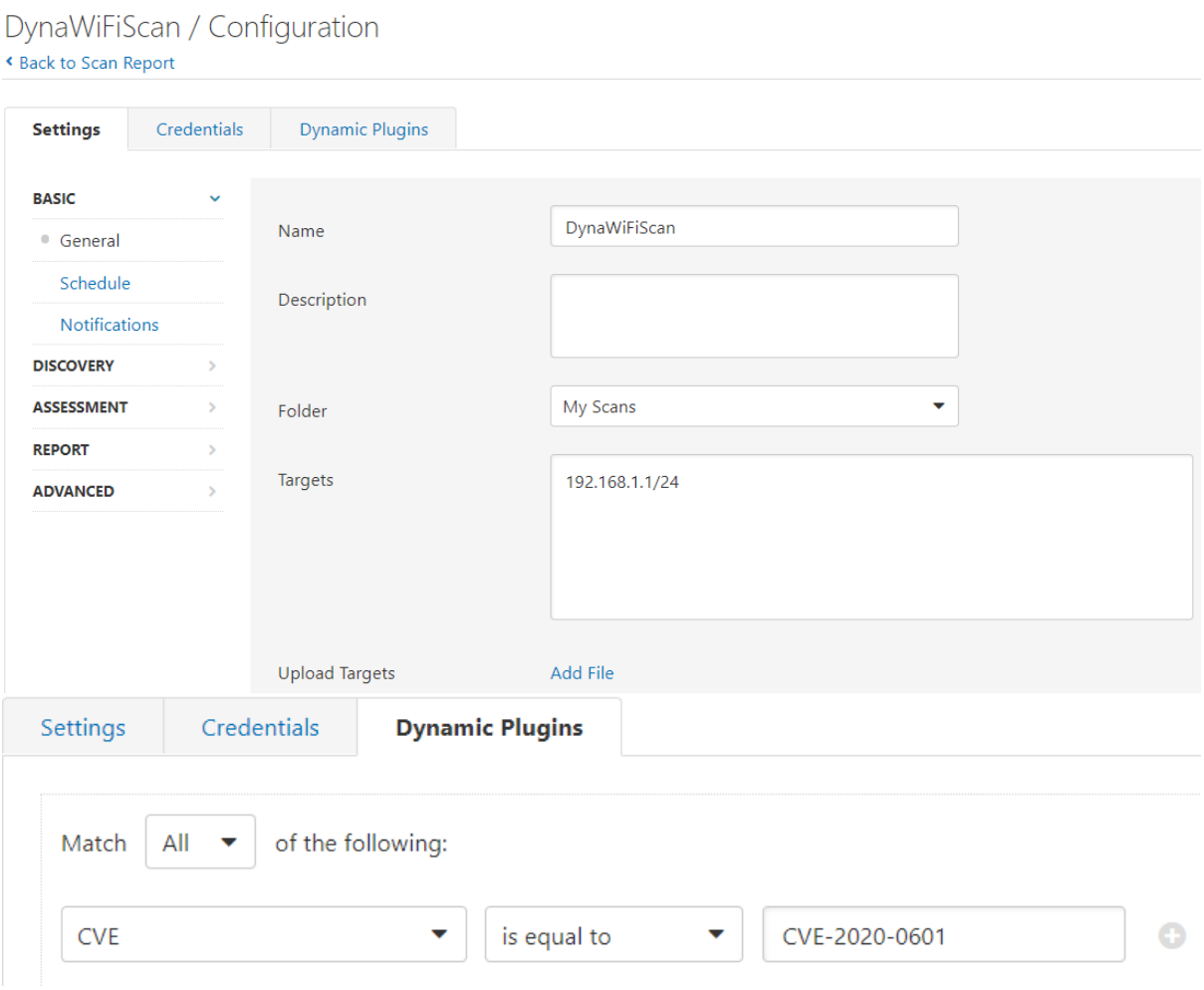
Vulnerabilities Total: 28

SEVERITY	CVSS	PLUGIN	NAME
CRITICAL	10.0	93650	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
MEDIUM	5.8	50686	IP Forwarding Enabled
MEDIUM	5.8	42263	Unencrypted Telnet Server
MEDIUM	5.0	70545	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities
MEDIUM	5.0	121007	SSH Known Hard Coded Private Keys
LOW	3.3	10663	DHCP Server Detection
LOW	2.6	70658	SSH Server CBC Mode Ciphers Enabled
INFO	N/A	10113	ICMP Netmask Request Information Disclosure
INFO	N/A	11002	DNS Server Detection
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	11936	OS Identification
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported

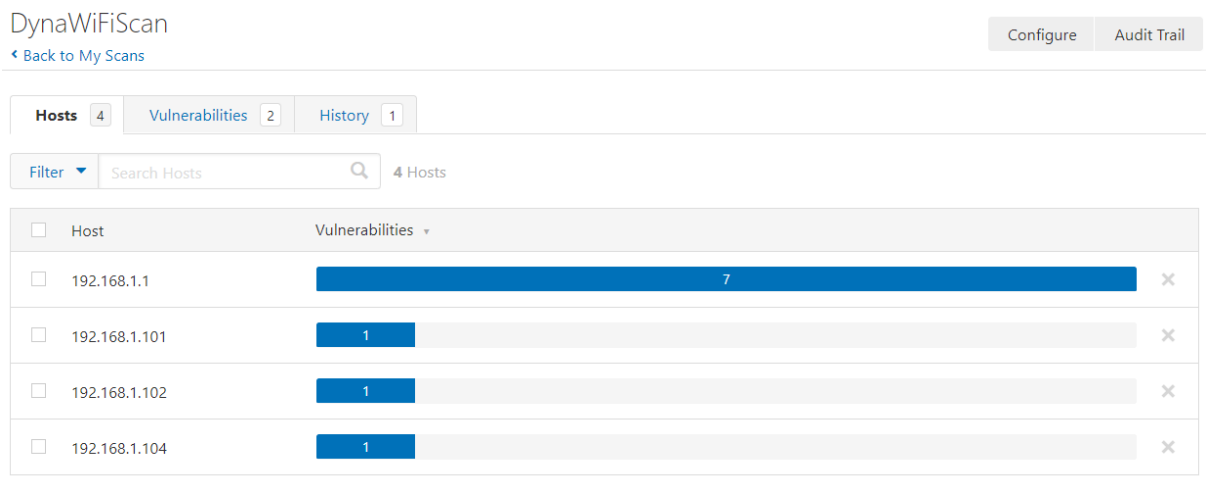
Nessus Essentials

INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	11819	TFTP Daemon Detection
INFO	N/A	10281	Telnet Server Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	35711	Universal Plug and Play (UPnP) Protocol Detection
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	35712	Web Server UPnP Detection

Selected **Advanced Dynamic Scan**:
Name: DynaWiFiScan
Folder: My Scans
Targets: 192.168.1.1/24 (IP Address of my home WiFi router)
Dynamic Plugins: CVE-2020-0601



Scan details – Hosts:



Graphical Report:

Scan Details

Policy:	Advanced Dynamic Scan
Status:	Canceled
Scanner:	Local Scanner
Start:	September 9 at 12:38 AM
End:	September 9 at 12:48 AM
Elapsed:	10 minutes

Vulnerabilities

Scan details – Vulnerabilities:
(Report on identified vulnerabilities)

DynaWiFiScan

Back to My Scans

Configure | Audit Trail

Hosts 4 | **Vulnerabilities** 2 | History 1

Filter | Search Vulnerabilities | 2 Vulnerabilities

Sev	Name	Family	Count
INFO	Nessus SYN scanner	Port scanners	6
INFO	Nessus Scan Information	Settings	4

Vulnerability details for “Nessus Syn Scanner”

Not secure | localhost:8834/#/scans/reports/15/vulnerabilities/11219

nessus Essentials | Scans | Settings | priyalb2000

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Scanners

TENABLE
Community
Research

Tenable News
TikTok Ad Scams: Insufficient Moderation Leaves 'F...
Read More

DynaWiFiScan / Plugin #11219

Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Hosts 4 | Vulnerabilities 2 | History 1

INFO Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 21/tcp was found to be open
```

Port	Hosts
21 / tcp / ftp	192.168.1.1

```
Port 22/tcp was found to be open
```

Port	Hosts
22 / tcp / ssh	192.168.1.1

```
Port 23/tcp was found to be open
```

Port	Hosts
23 / tcp / telnet	192.168.1.1

```
Port 53/tcp was found to be open
```

Port	Hosts
53 / tcp	192.168.1.1

```
Port 80/tcp was found to be open
```

Port	Hosts
80 / tcp / www	192.168.1.1

```
Port 5431/tcp was found to be open
```

Port	Hosts
5431 / tcp / www	192.168.1.1

Plugin Details

Severity:	Info
ID:	11219
Version:	$Revision: 1.33 $
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	August 20, 2020

Risk Information

Risk Factor: None

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Scanners

TENABLE
Community
Research

Tenable News
Trading Technologies Messaging Multiple Unauthenti...
Read More

Note: The downloaded Vulnerabilty Report has been merged with this document. Scroll down to view.

DynaWiFiScan

Report generated by Nessus™

Wed, 09 Sep 2020 00:48:00 India Standard Time

Nessus Essentials

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.1.1....4
- 192.168.1.101....5
- 192.168.1.102....6
- 192.168.1.104....7

Nessus Essentials

Hosts Executive Summary

Nessus Essentials

192.168.1.1

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 2

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

Nessus Essentials

192.168.1.101

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	19506	Nessus Scan Information

Nessus Essentials

192.168.1.102

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	19506	Nessus Scan Information

Nessus Essentials

192.168.1.104

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

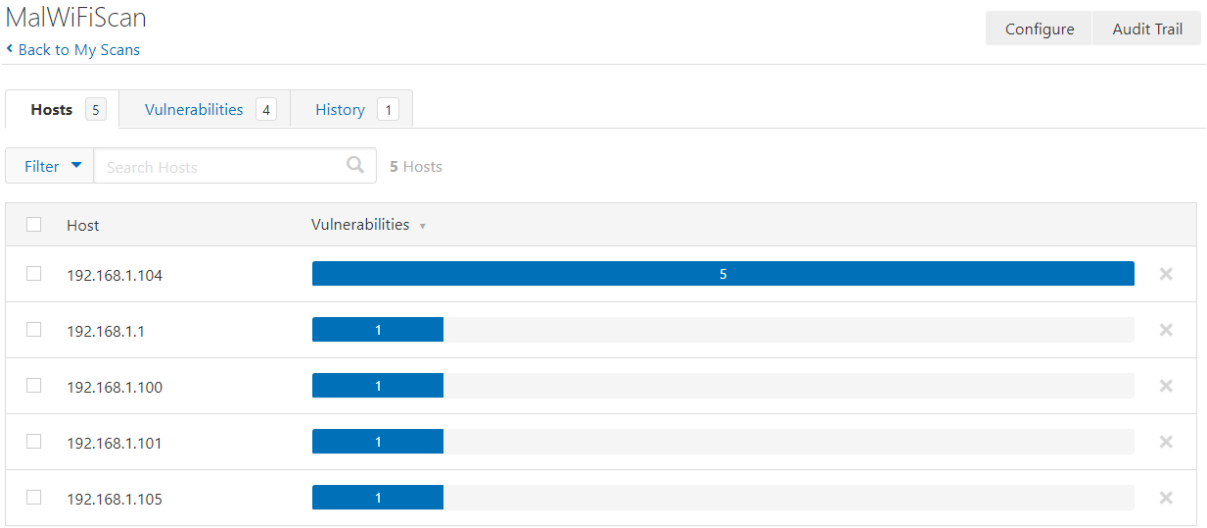
Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	19506	Nessus Scan Information

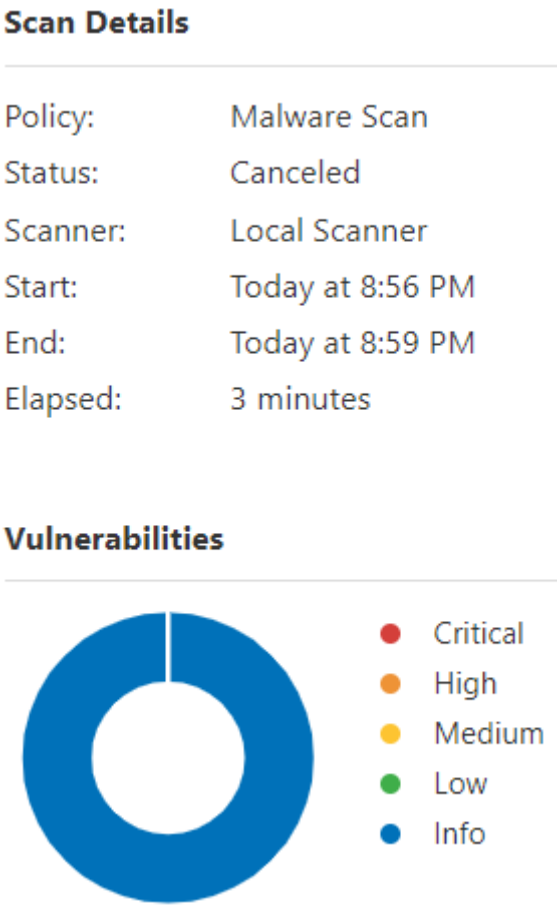
Nessus Essentials

Selected **Malware Scan**:
Name: MalWiFiScan
Folder: My Scans
Targets: 192.168.1.1/24 (IP Address of my home WiFi router)
Windows Credentials

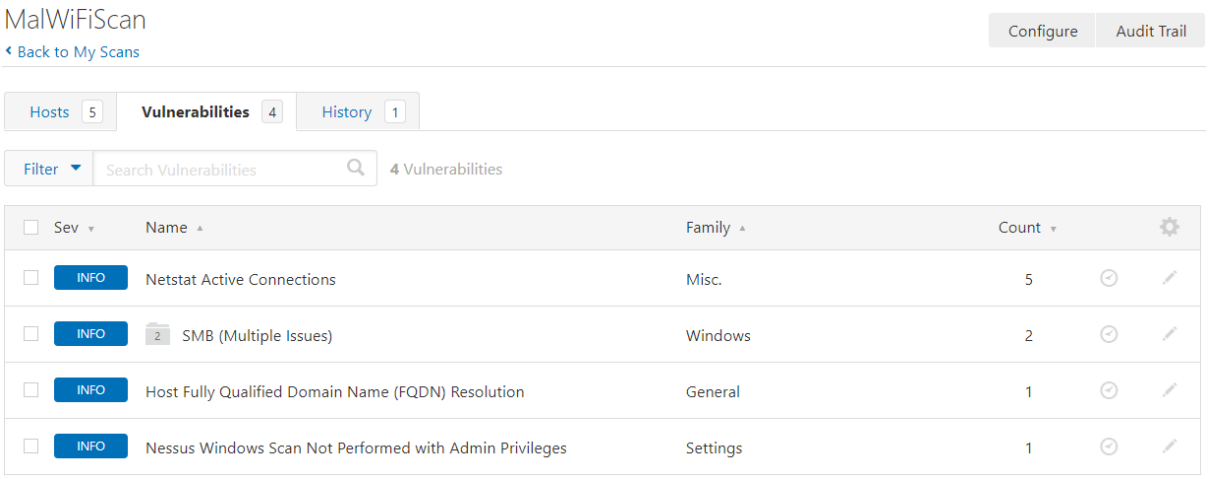
Scan details – Hosts:



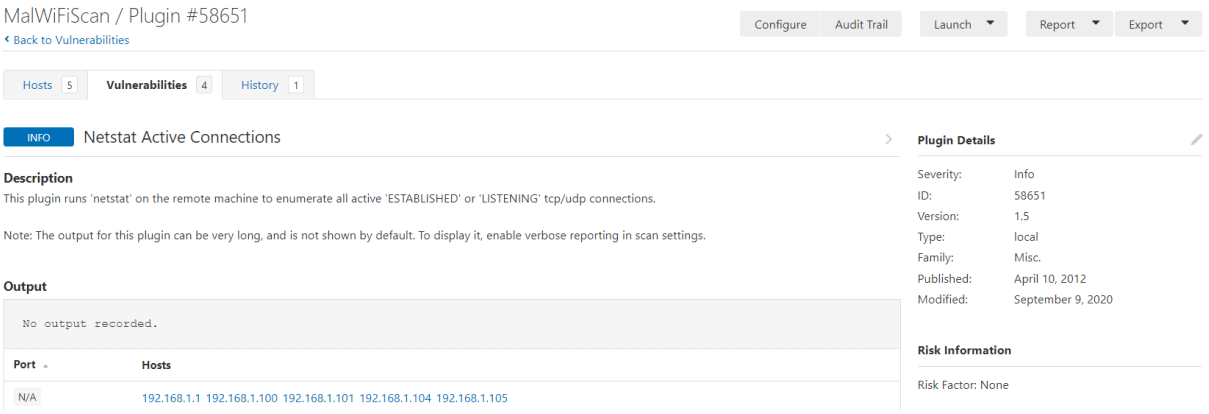
Graphical Report:



Scan details – Vulnerabilities:
(Report on identified vulnerabilities)



Vulnerability details for “Nessus Syn Scanner”



Note: The downloaded Vulnerabilty Report has been merged with this document. Scroll down to view.

MalWiFiScan

Report generated by Nessus™

Fri, 11 Sep 2020 20:59:53 India Standard Time

Nessus Essentials

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.1.1....4
- 192.168.1.100....5
- 192.168.1.101....6
- 192.168.1.104....7
- 192.168.1.105....8

Nessus Essentials

Hosts Executive Summary

Nessus Essentials

192.168.1.1

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	58651	Netstat Active Connections

Nessus Essentials

192.168.1.100

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	58651	Netstat Active Connections

Nessus Essentials

192.168.1.101

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	58651	Netstat Active Connections

Nessus Essentials

192.168.1.104

0	0	0	0	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 5

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	10394	Microsoft Windows SMB Log In Possible
INFO	N/A	10395	Microsoft Windows SMB Shares Enumeration
INFO	N/A	24786	Nessus Windows Scan Not Performed with Admin Privileges
INFO	N/A	58651	Netstat Active Connections

Nessus Essentials

192.168.1.105

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

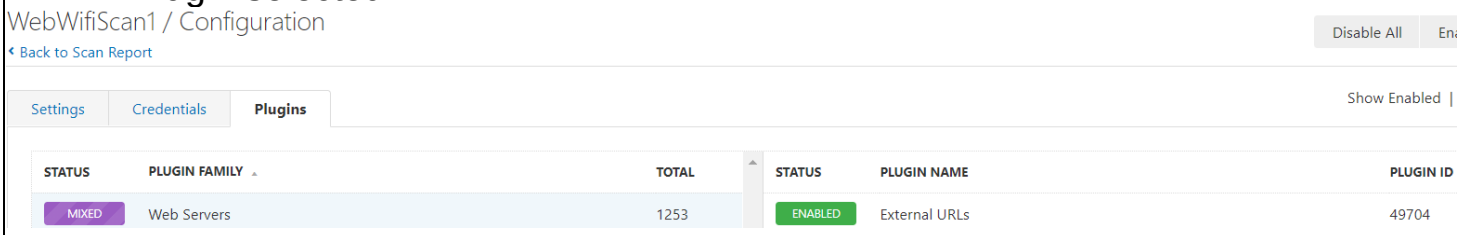
Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	58651	Netstat Active Connections

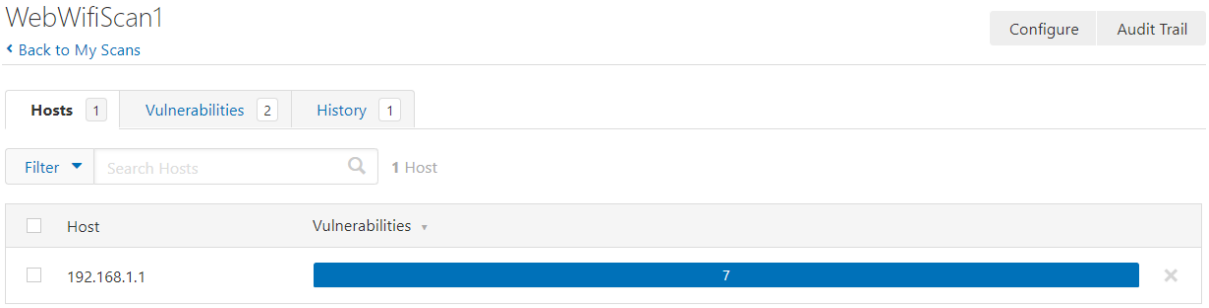
Nessus Essentials

Selected **Web Application Vulnerability Scan / plugin #49704 – External ULs**:
Name: WebWiFiScan1
Folder: My Scans
Targets: 192.168.1.1/24 (IP Address of my home WiFi router)

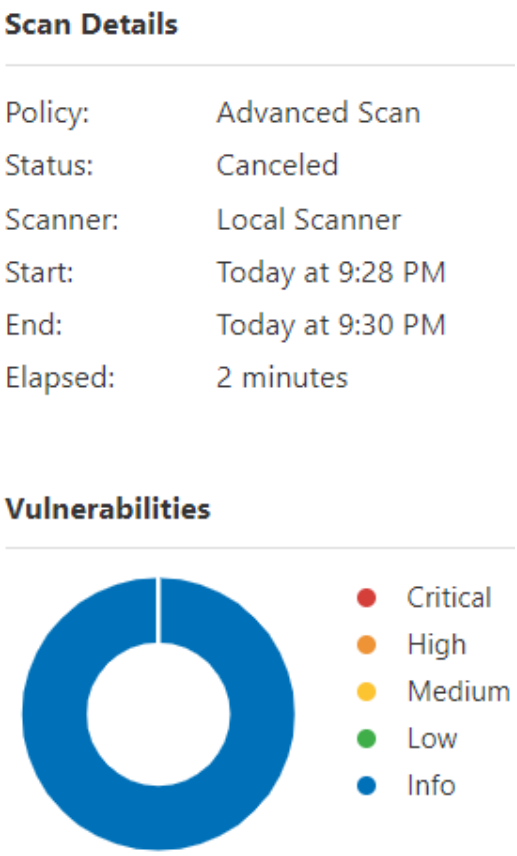
Plugin selected:



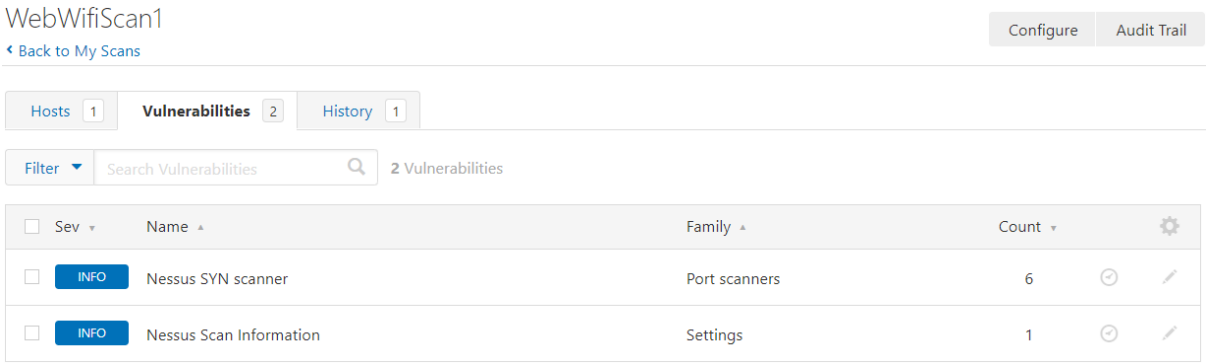
Scan details – Hosts:



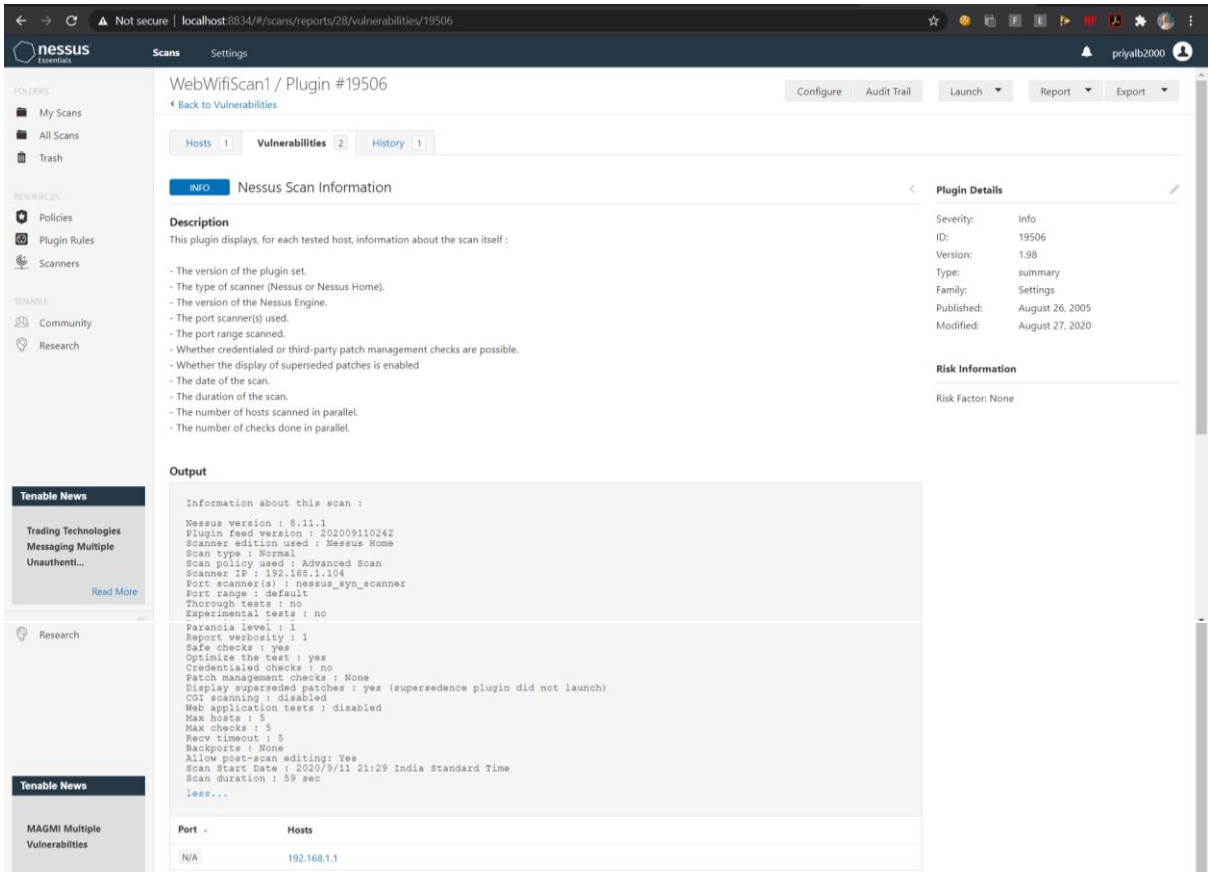
Graphical Report:



Scan details – Vulnerabilities:
(Report on identified vulnerabilities)



Vulnerability details for “Nessus Scan Information”



Note: The downloaded Vulnerabilty Report has been merged with this document. Scroll down to view.

WebWifiScan1

Report generated by Nessus™

Fri, 11 Sep 2020 21:30:17 India Standard Time

Nessus Essentials

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.1.1.....4

Nessus Essentials

Hosts Executive Summary

Nessus Essentials

192.168.1.1

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

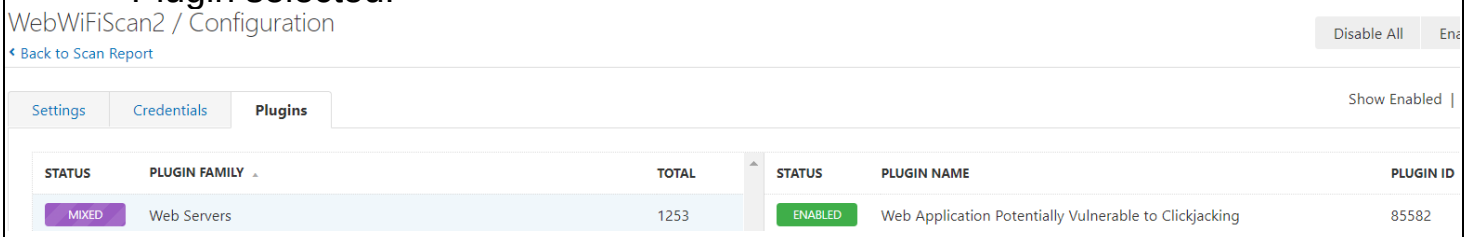
Vulnerabilities Total: 2

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

Nessus Essentials

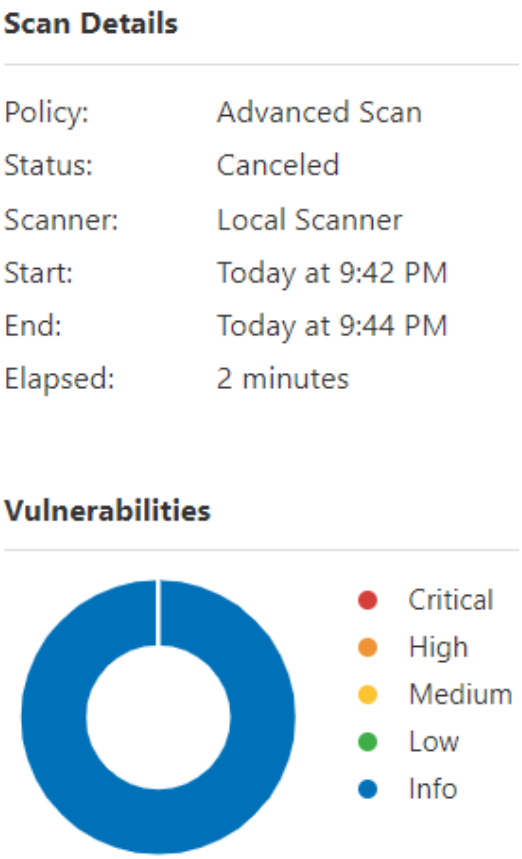
Selected **Web Application Vulnerability Scan / plugin #85582 – Clickjacking**:
Name: WebWiFiScan1
Folder: My Scans
Targets: 192.168.1.1/24 (IP Address of my home WiFi router)

Plugin selected:

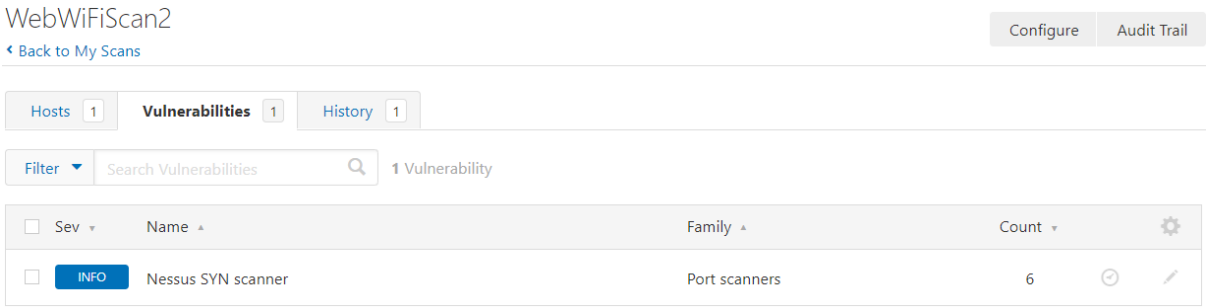


Scan details – Hosts:

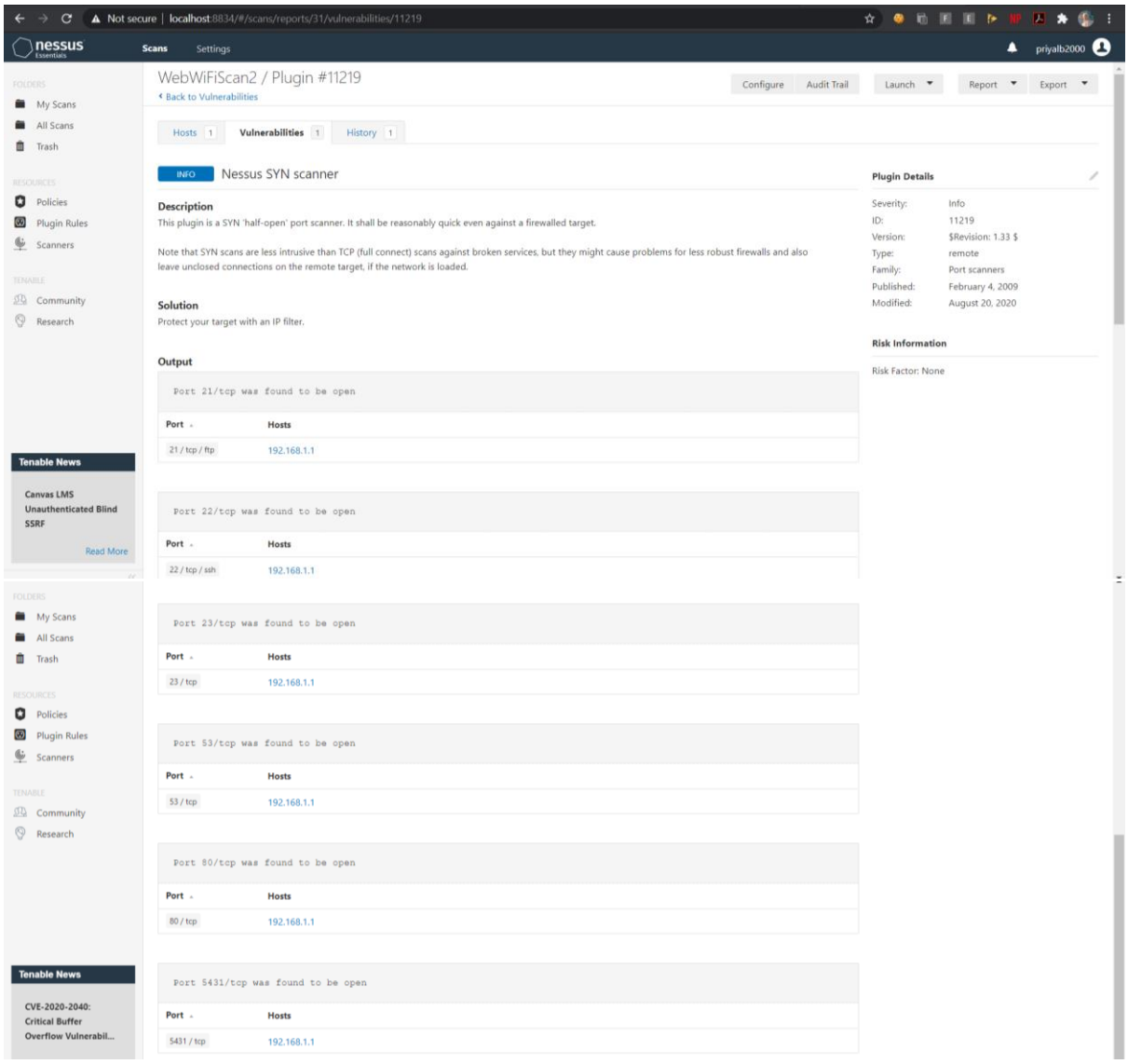
Graphical Report:



Scan details – Vulnerabilities:
(Report on identified vulnerabilities)



Vulnerability details for “Nessus Syn Scanner”



Note: The downloaded Vulnerabilty Report has been merged with this document. Scroll down to view.

WebWiFiScan2

Report generated by Nessus™ Fri, 11 Sep 2020 21:44:32 India Standard Time

Nessus Essentials

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.1.1.....4

Nessus Essentials

Hosts Executive Summary

Nessus Essentials

192.168.1.1

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

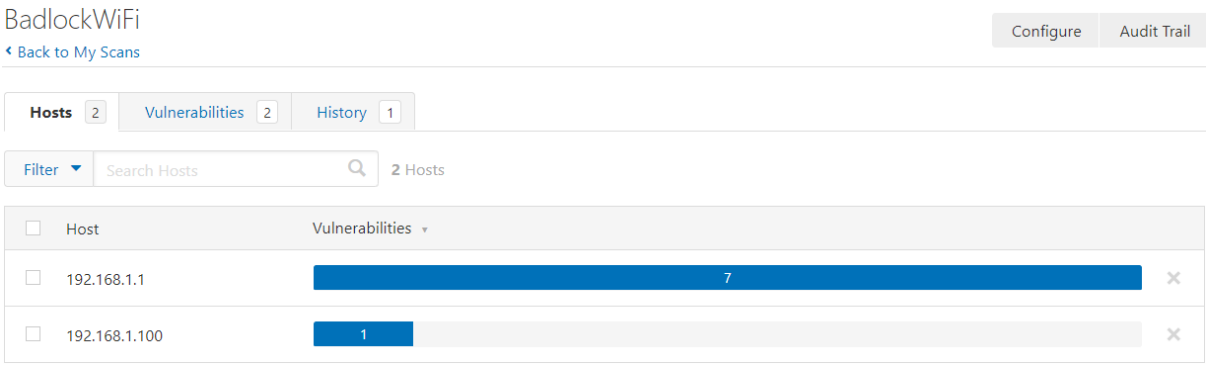
Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	11219	Nessus SYN scanner

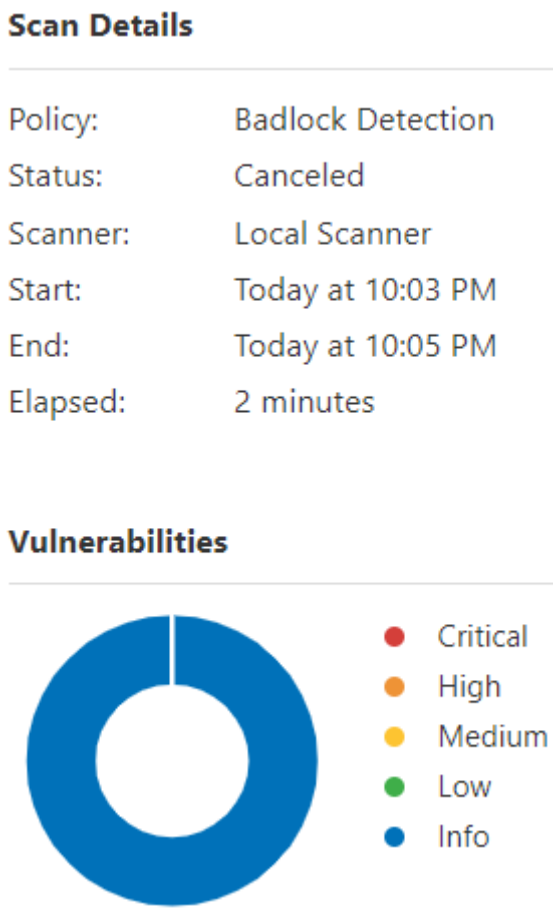
Nessus Essentials

Selected **Badlock Detection**:
Name: BadlockWiFi
Folder: My Scans
Targets: 192.168.1.1/24 (IP Address of my home WiFi router)

Scan details – Hosts:



Graphical Report:



Scan details – Vulnerabilities:
(Report on identified vulnerabilities)

BadlockWiFi

‹ Back to My Scans

Configure | Audit Trail

Hosts 2 | **Vulnerabilities** 2 | History 1

Filter | Search Vulnerabilities | 2 Vulnerabilities

Sev	Name	Family	Count
INFO	Nessus SYN scanner	Port scanners	6
INFO	Nessus Scan Information	Settings	2

Vulnerability details for “Nessus Scan Information”

Not secure | localhost:8834/#/scans/reports/34/vulnerabilities/19506

nessus Essentials | Scans | Settings | priyalb2000

FOLDERS: My Scans, All Scans, Trash

RESOURCES: Policies, Plugin Rules, Scanners

TENABLE: Community, Research

Tenable News

What COVID-19 Response Strategies Tell Us About th...

Read More

BadlockWiFi / Plugin #19506

‹ Back to Vulnerabilities

Configure | Audit Trail | Launch | Report | Export

Hosts 2 | **Vulnerabilities** 2 | History 1

INFO Nessus Scan Information

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Plugin Details

Severity:	Info
ID:	19506
Version:	1.98
Type:	summary
Family:	Settings
Published:	August 26, 2005
Modified:	August 27, 2020

Risk Information

Risk Factor: None

Output

```
Information about this scan :

Nessus version : 8.11.1
Plugin feed version : 202009110242
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Badlock Detection
Scanner IP : 192.168.1.104
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 120
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2020/9/11 22:04 India Standard Time
Scan duration : 26 sec
less...
```

Port	Hosts
N/A	192.168.1.100

```
Information about this scan :

Nessus version : 8.11.1
Plugin feed version : 202009110242
Scanner edition used : Nessus Home
Scan type : Normal
Scan policy used : Badlock Detection
Scanner IP : 192.168.1.104
Port scanner(s) : nessus_syn_scanner
Port range : default
more...
```

Port	Hosts
N/A	192.168.1.1

Tenable News

Unauthenticated email forgery/spoofing in WordPres...

Note: The downloaded Vulnerabilty Report has been merged with this document. Scroll down to view.

BadlockWiFi

Report generated by Nessus™

Fri, 11 Sep 2020 22:05:23 India Standard Time

Nessus Essentials

TABLE OF CONTENTS

Hosts Executive Summary

- 192.168.1.1.....4
- 192.168.1.100.....5

Nessus Essentials

Hosts Executive Summary

Nessus Essentials

192.168.1.1

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 2

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information

Nessus Essentials

192.168.1.100

0	0	0	0	1
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 1

SEVERITY	CVSS	PLUGIN	NAME
INFO	N/A	19506	Nessus Scan Information

Nessus Essentials

Scanner Health:

****