



VIT[®]

Vellore Institute of Technology

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

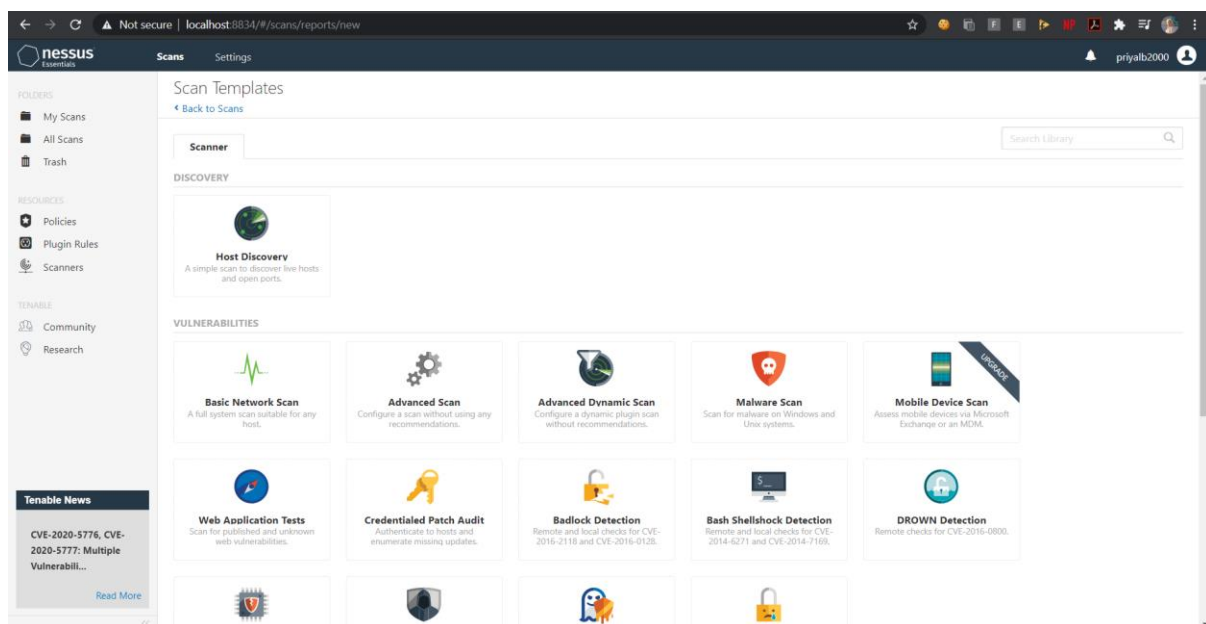
School of Information Technology and Engineering
Lab Assessment-V, SEPTEMBER 2020
B.Tech., Fall-2020-2021

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

WiFiScan

[Back to My Scans](#)

Configure

Audit Trail

Hosts1

Vulnerabilities28

Remediations2

History1

Filter

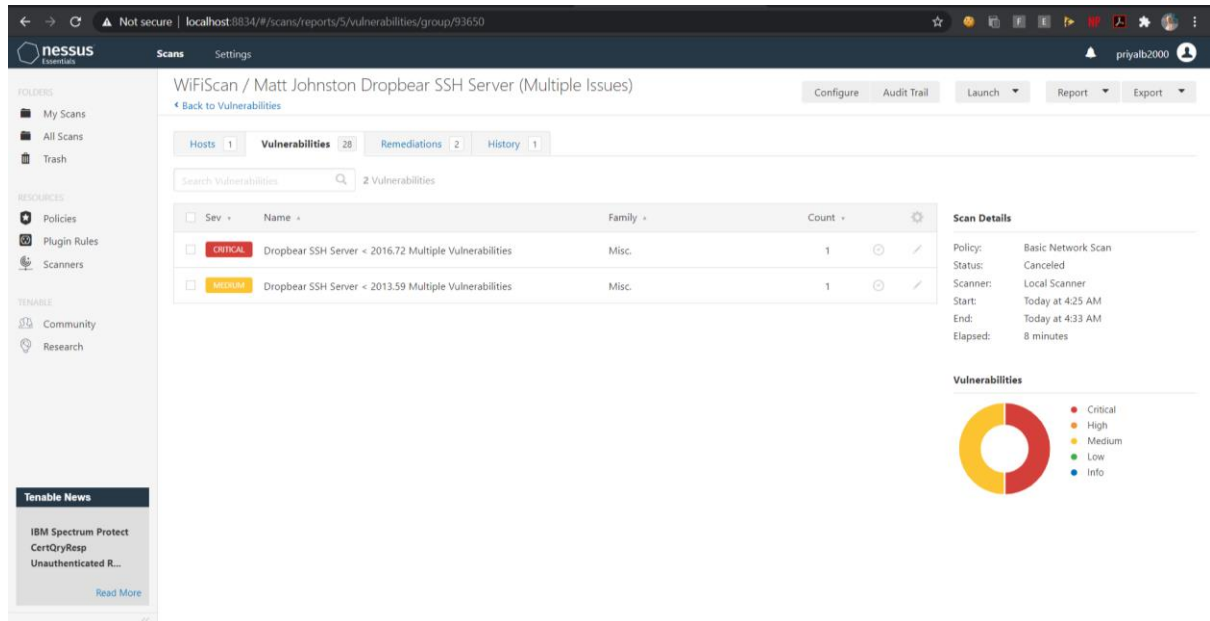
Search Vulnerabilities

28 Vulnerabilities

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



WiFiScan / Matt Johnston Dropbear SSH Server (Multiple Issues)

Back to Vulnerabilities

Hosts 1 Vulnerabilities 28 Remediations 2 History 1

Search Vulnerabilities

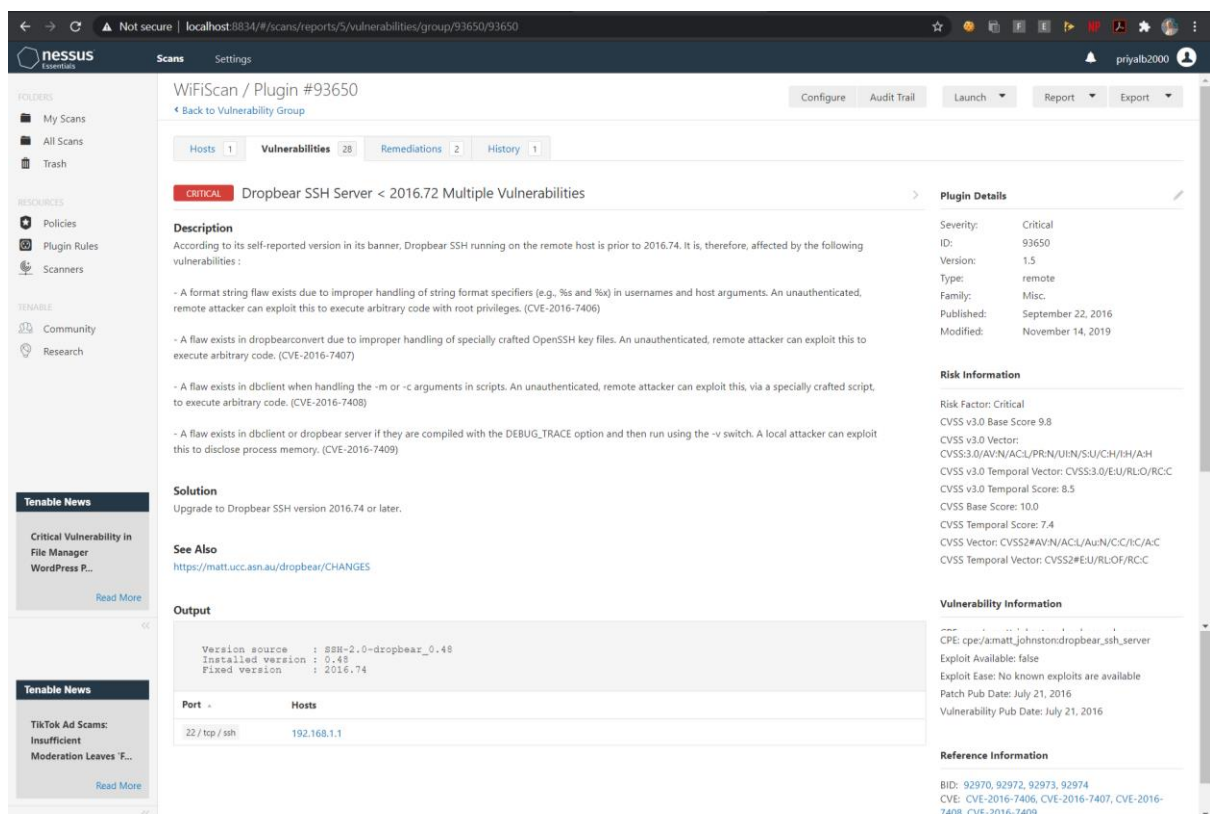
Sev	Name	Family	Count
CRITICAL	Dropbear SSH Server < 2016.72 Multiple Vulnerabilities	Misc.	1
MEDIUM	Dropbear SSH Server < 2013.59 Multiple Vulnerabilities	Misc.	1

Scan Details

Policy: Basic Network Scan
Status: Canceled
Scanner: Local Scanner
Start: Today at 4:25 AM
End: Today at 4:33 AM
Elapsed: 8 minutes

Vulnerabilities

Donut chart showing severity distribution: Critical (red), High (orange), Medium (yellow), Low (green), Info (blue).



WiFiScan / Plugin #93650

Back to Vulnerability Group

Hosts 1 Vulnerabilities 28 Remediations 2 History 1

CRITICAL Dropbear SSH Server < 2016.72 Multiple Vulnerabilities

Description

According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities:

- A format string flaw exists due to improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges. (CVE-2016-7406)
- A flaw exists in dropbearconvert due to improper handling of specially crafted OpenSSH key files. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-7407)
- A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code. (CVE-2016-7408)
- A flaw exists in dbclient or dropbear server if they are compiled with the DEBUG_TRACE option and then run using the -v switch. A local attacker can exploit this to disclose process memory. (CVE-2016-7409)

Solution

Upgrade to Dropbear SSH version 2016.74 or later.

See Also

<https://matt.ucc.asn.au/dropbear/CHANGES>

Output

```
Version source : SSH-2.0-dropbear_0.48
Installed version : 0.48
Fixed version : 2016.74
```

Port	Hosts
22 / tcp / ssh	192.168.1.1

Plugin Details

Severity: Critical
ID: 93650
Version: 1.5
Type: remote
Family: Misc.
Published: September 22, 2016
Modified: November 14, 2019

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/CH/I/H/A/H
CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C
CVSS v3.0 Temporal Score: 8.5
CVSS Base Score: 10.0
CVSS Temporal Score: 7.4
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/CC:R/IC:AC
CVSS Temporal Vector: CVSS2#E:U/RL:O/RC:C

Vulnerability Information

CPE: cpe:/a:matt_johnston:dropbear_ssh_server
Exploit Available: false
Exploit Ease: No known exploits are available
Patch Pub Date: July 21, 2016
Vulnerability Pub Date: July 21, 2016

Reference Information

BID: 92970, 92972, 92973, 92974
CVE: CVE-2016-7406, CVE-2016-7407, CVE-2016-7408, CVE-2016-7409

Note: The downloaded Vulnerability 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

TABLE OF CONTENTS

Hosts Executive Summary

• 192.168.1.1.....	4
--------------------	---

Nessus Essentials

Hosts Executive Summary

192.168.1.1



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

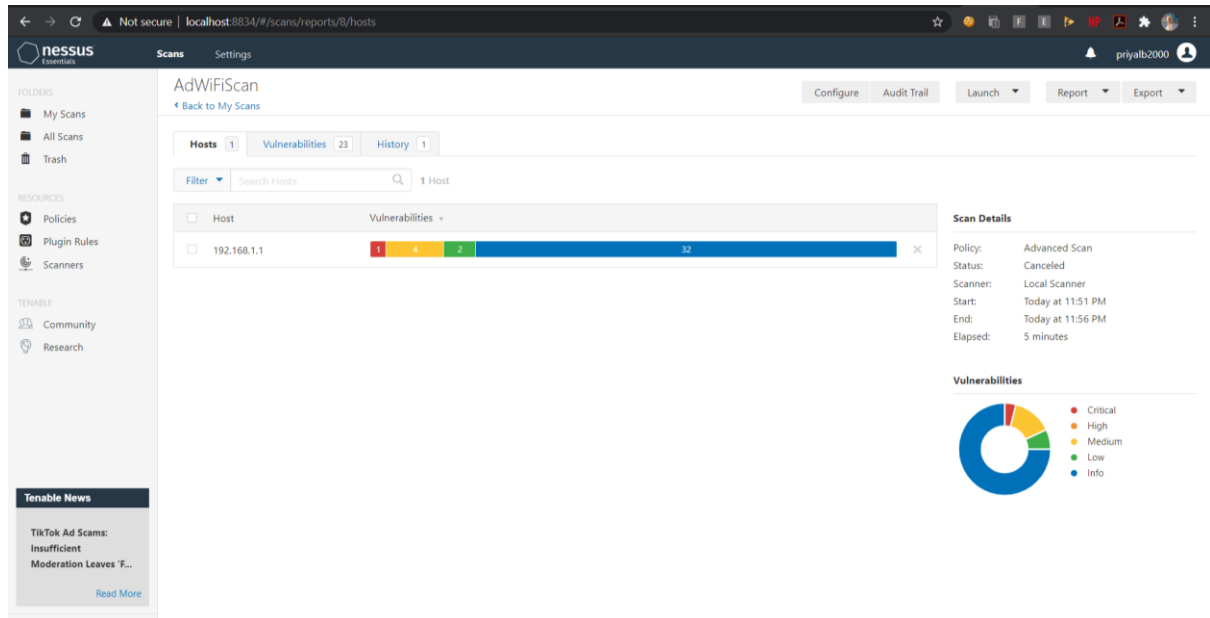
INFO	N/A	11936	OS Identification
INFO	N/A	66334	Patch Report
INFO	N/A	70657	SSH Algorithms and Languages Supported
INFO	N/A	10881	SSH Protocol Versions Supported
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	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:

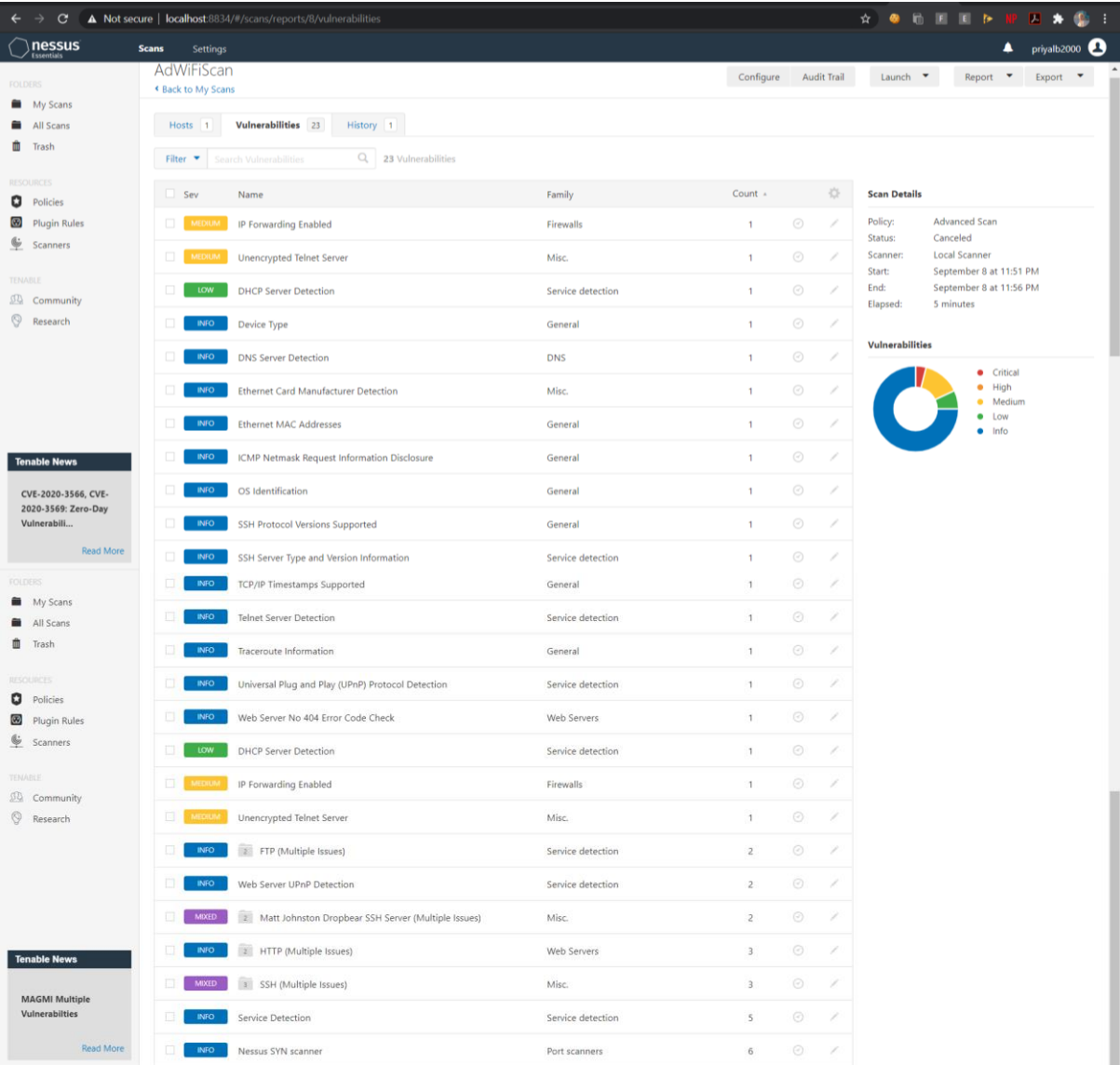
Scan Details

Policy:	Advanced Scan
Status:	Canceled
Scanner:	Local Scanner
Start:	September 8 at 11:51 PM
End:	September 8 at 11:56 PM
Elapsed:	5 minutes

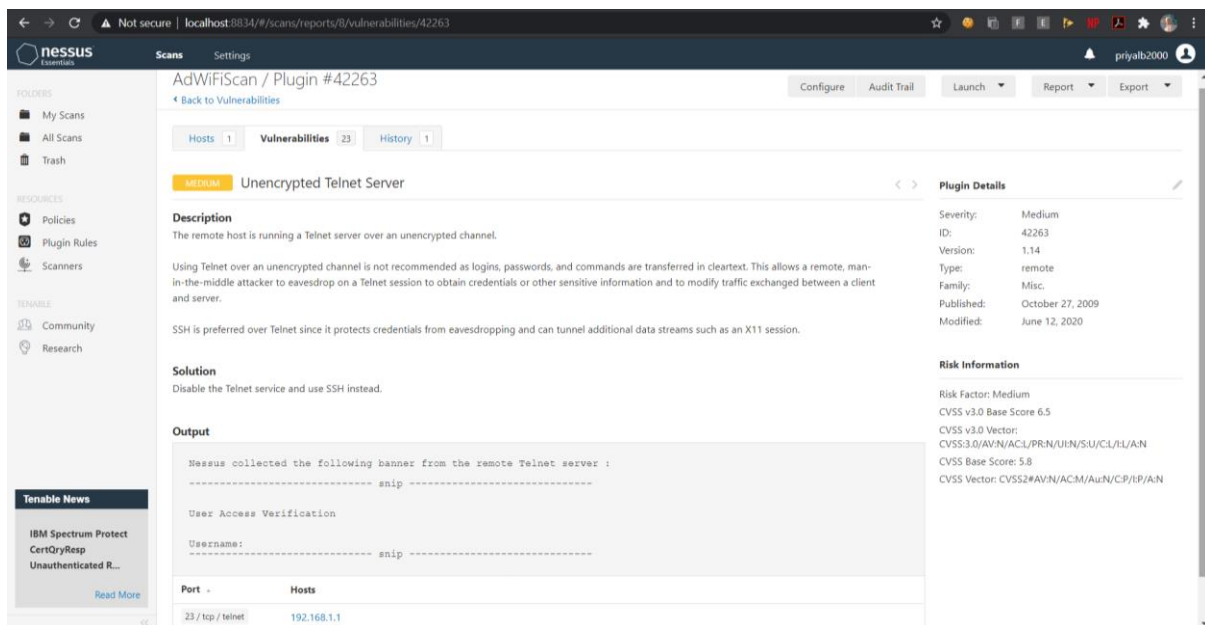
Vulnerabilities



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

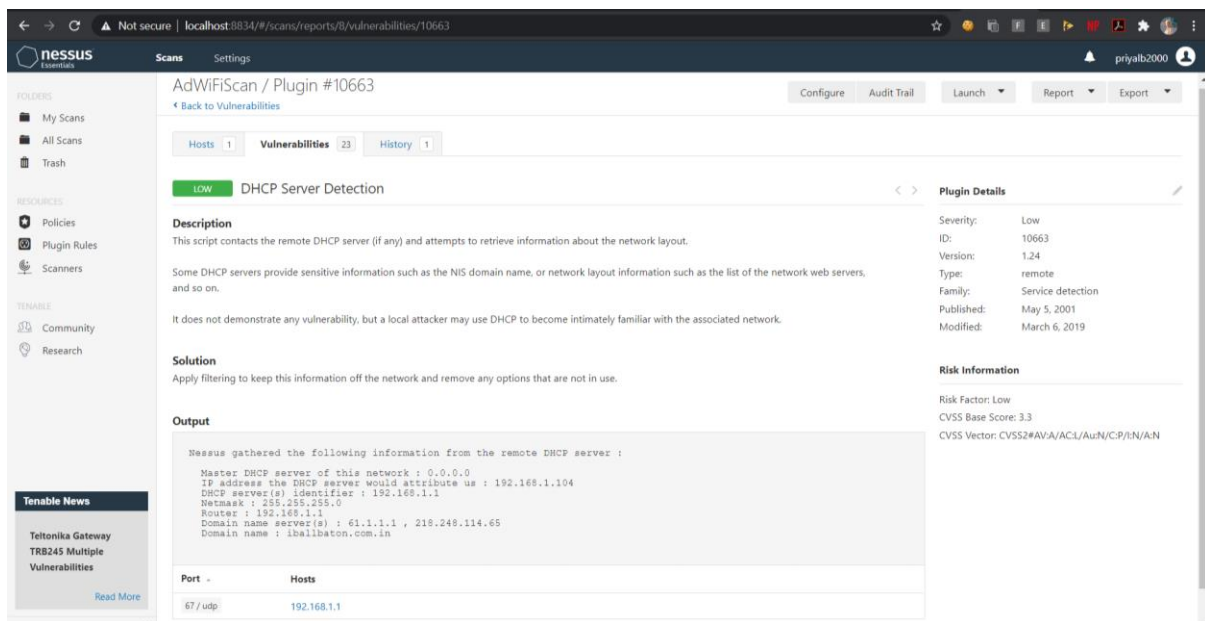


Vulnerability details for “Unencrypted Telnet Server”



The screenshot displays the Nessus Essentials interface for a vulnerability report. The browser address bar shows 'localhost:8834/#scans/reports/8/vulnerabilities/42263'. The page title is 'AdWiFiScan / Plugin #42263'. The left sidebar contains navigation links for Folders (My Scans, All Scans, Trash), Resources (Policies, Plugin Rules, Scanners), and Tenable (Community, Research). The main content area shows the vulnerability details for 'Unencrypted Telnet Server' (Plugin #42263), which is categorized as 'MEDIUM'. The description states: 'The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in plaintext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server. SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.' The solution is to 'Disable the Telnet service and use SSH instead.' The output shows a banner from the remote Telnet server: 'Nessus collected the following banner from the remote Telnet server : ----- snip ----- User Access Verification Username: ----- snip -----'. The risk information includes: Risk Factor: Medium, CVSS v3.0 Base Score: 6.5, CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N, CVSS Base Score: 5.8, CVSS Vector: CVSS2#AV:N/AC:M/Au:N/CP:R/PA:N. A table at the bottom shows the port and host details: Port 23 / tcp / telnet on Host 192.168.1.1.

Vulnerability details for “DHCP Server Detection”



The screenshot displays the Nessus Essentials interface for a vulnerability report. The browser address bar shows 'localhost:8834/#scans/reports/8/vulnerabilities/10663'. The page title is 'AdWiFiScan / Plugin #10663'. The left sidebar contains navigation links for Folders (My Scans, All Scans, Trash), Resources (Policies, Plugin Rules, Scanners), and Tenable (Community, Research). The main content area shows the vulnerability details for 'DHCP Server Detection' (Plugin #10663), which is categorized as 'LOW'. The description states: 'This script contacts the remote DHCP server (if any) and attempts to retrieve information about the network layout. Some DHCP servers provide sensitive information such as the NIS domain name, or network layout information such as the list of the network web servers, and so on. It does not demonstrate any vulnerability, but a local attacker may use DHCP to become intimately familiar with the associated network.' The solution is to 'Apply filtering to keep this information off the network and remove any options that are not in use.' The output shows information gathered from the remote DHCP server: 'Nessus gathered the following information from the remote DHCP server : Master DHCP server of this network : 0.0.0.0 IP address the DHCP server would attribute us : 192.168.1.104 DHCP server(s) identifier : 192.168.1.1 Netmask : 255.255.255.0 Router : 192.168.1.1 Domain name server(s) : 61.1.1.1 , 218.248.114.65 Domain name : iballbaton.com.in'. The risk information includes: Risk Factor: Low, CVSS Base Score: 3.3, CVSS Vector: CVSS2#AV:A/AC:L/Au:N/CP:R/PA:N. A table at the bottom shows the port and host details: Port 67 / udp on Host 192.168.1.1.

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

Note: The downloaded Vulnerability 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

TABLE OF CONTENTS

Hosts Executive Summary

• 192.168.1.1.....	4
--------------------	---

Nessus Essentials

Hosts Executive Summary

192.168.1.1



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

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

DynaWiFiScan / Configuration

[Back to Scan Report](#)

Settings

Credentials

Dynamic Plugins

BASIC

General

Schedule

Notifications

DISCOVERY

ASSESSMENT

REPORT

ADVANCED

Name

DynaWiFiScan

Description

Folder

My Scans

Targets

192.168.1.1/24

Upload Targets

Add File

Settings

Credentials

Dynamic Plugins

Match

All

of the following:

CVE

is equal to

CVE-2020-0601

Scan details – Hosts:

DynaWiFiScan

[Configure](#) [Audit Trail](#)

[Back to My Scans](#)

Hosts	4	Vulnerabilities	2	History	1
Filter	Search Hosts	4 Hosts			
<input type="checkbox"/>	Host	Vulnerabilities			
<input type="checkbox"/>	192.168.1.1	7			
<input type="checkbox"/>	192.168.1.101	1			
<input type="checkbox"/>	192.168.1.102	1			
<input type="checkbox"/>	192.168.1.104	1			

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

Configure Audit Trail

Back to My Scans

Hosts 4 Vulnerabilities 2 History 1

Filter Search Vulnerabilities 2 Vulnerabilities

<input type="checkbox"/> Sev ▾	Name ▲	Family ▲	Count ▾	⚙
<input type="checkbox"/> INFO	Nessus SYN scanner	Port scanners	6	🕒 ✎
<input type="checkbox"/> INFO	Nessus Scan Information	Settings	4	🕒 ✎

Vulnerability details for “Nessus Syn Scanner”

The screenshot displays the Nessus Essentials web interface for the 'DynaWiFiScan / Plugin #11219'. The interface is divided into a left sidebar, a main content area, and a right sidebar.

Left Sidebar:

- 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

Main Content Area:

DynaWiFiScan / Plugin #11219

[Back to Vulnerabilities](#)

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/top was found to be open

Port	Hosts
21 / tcp / ftp	192.168.1.1

Port 22/top was found to be open

Port	Hosts
22 / tcp / ssh	192.168.1.1

Port 23/top was found to be open

Port	Hosts
23 / tcp / telnet	192.168.1.1

Port 53/top was found to be open

Port	Hosts
53 / tcp	192.168.1.1

Port 80/top was found to be open

Port	Hosts
80 / tcp / www	192.168.1.1

Port 5431/top was found to be open

Port	Hosts
5431 / tcp / www	192.168.1.1

Right Sidebar:

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

Note: The downloaded Vulnerability 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

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

192.168.1.1



Vulnerabilities

Total: 2

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

192.168.1.101



Vulnerabilities

Total: 1

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

192.168.1.102



Vulnerabilities

Total: 1

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

192.168.1.104



Vulnerabilities

Total: 1

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

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:

MalWiFiScan

[Configure](#) [Audit Trail](#)

[Back to My Scans](#)

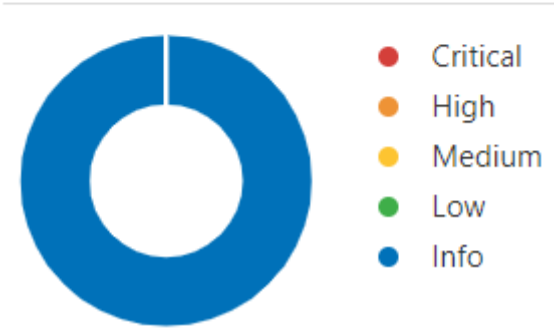
Hosts	5	Vulnerabilities	4	History	1
Filter	Search Hosts		5 Hosts		
<input type="checkbox"/>	Host	Vulnerabilities			
<input type="checkbox"/>	192.168.1.104	5			
<input type="checkbox"/>	192.168.1.1	1			
<input type="checkbox"/>	192.168.1.100	1			
<input type="checkbox"/>	192.168.1.101	1			
<input type="checkbox"/>	192.168.1.105	1			

Graphical Report:

Scan Details

Policy: Malware Scan
Status: Canceled
Scanner: Local Scanner
Start: Today at 8:56 PM
End: Today at 8:59 PM
Elapsed: 3 minutes

Vulnerabilities



Scan details – Vulnerabilities: (Report on identified vulnerabilities)

MalWiFiScan

[Back to My Scans](#)

Configure

Audit Trail

Hosts 5

Vulnerabilities 4

History 1

Filter

Search Vulnerabilities

4 Vulnerabilities

<input type="checkbox"/>	Sev	Name	Family	Count	
<input type="checkbox"/>	INFO	Netstat Active Connections	Misc.	5	
<input type="checkbox"/>	INFO	SMB (Multiple Issues)	Windows	2	
<input type="checkbox"/>	INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1	
<input type="checkbox"/>	INFO	Nessus Windows Scan Not Performed with Admin Privileges	Settings	1	

Vulnerability details for “Nessus Syn Scanner”

MalWiFiScan / Plugin #58651

[Back to Vulnerabilities](#)

Configure

Audit Trail

Launch

Report

Export

Hosts 5

Vulnerabilities 4

History 1

INFO

Netstat Active Connections

Description

This plugin runs 'netstat' on the remote machine to enumerate all active 'ESTABLISHED' or 'LISTENING' tcp/udp connections.

Note: The output for this plugin can be very long, and is not shown by default. To display it, enable verbose reporting in scan settings.

Output

No output recorded.

Port	Hosts
N/A	192.168.1.1 192.168.1.100 192.168.1.101 192.168.1.104 192.168.1.105

Plugin Details

Severity: Info

ID: 58651

Version: 1.5

Type: local

Family: Misc.

Published: April 10, 2012

Modified: September 9, 2020

Risk Information

Risk Factor: None

Note: The downloaded Vulnerability 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

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

192.168.1.1



Vulnerabilities

Total: 1

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

192.168.1.100



Vulnerabilities

Total: 1

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

192.168.1.101



Vulnerabilities

Total: 1

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

192.168.1.104



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

192.168.1.105



Vulnerabilities

Total: 1

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

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:

WebWifiScan1 / Configuration

[Back to Scan Report](#)

Disable All Enable All

Settings

Credentials

Plugins

Show Enabled |

STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
MIXED	Web Servers	1253	ENABLED	External URLs	49704

Scan details – Hosts:

WebWifiScan1

Configure Audit Trail

[Back to My Scans](#)

Hosts 1	Vulnerabilities 2	History 1
Filter	Search Hosts	1 Host
<input type="checkbox"/> Host	Vulnerabilities	
<input type="checkbox"/> 192.168.1.1		7

Graphical Report:

Scan Details

Policy:	Advanced Scan
Status:	Canceled
Scanner:	Local Scanner
Start:	Today at 9:28 PM
End:	Today at 9:30 PM
Elapsed:	2 minutes

Vulnerabilities



Scan details – Vulnerabilities: (Report on identified vulnerabilities)

WebWifiScan1

[Back to My Scans](#)

Configure

Audit Trail

Hosts	1	Vulnerabilities	2	History	1
Filter	Search Vulnerabilities		2 Vulnerabilities		
Sev	Name	Family	Count		
<input type="checkbox"/>	INFO Nessus SYN scanner	Port scanners	6		
<input type="checkbox"/>	INFO Nessus Scan Information	Settings	1		

Vulnerability details for “Nessus Scan Information”

The screenshot shows the Nessus web interface for a specific vulnerability. The browser address bar indicates the URL: `localhost:8834/#/scans/reports/28/vulnerabilities/19506`. The page title is "WebWifiScan1 / Plugin #19506". The left sidebar contains navigation options like "My Scans", "All Scans", "Trash", "Policies", "Plugin Rules", "Scanners", "Community", and "Research". The main content area displays the "Nessus Scan Information" vulnerability details. It includes a "Description" section with a list of scan parameters, an "Output" section with a detailed log of the scan process, and a "Risk Information" section showing the risk factor as "None". The "Output" section contains a large block of text detailing the scan configuration and results.

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.

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 : Advanced Scan
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 (supersession plugin did not launch)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 5
Max checks : 5
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Scan Start Date : 2020/9/11 21:29 India Standard Time
Scan duration : 59 sec
less...
```

Risk Information

Risk Factor: None

Port	Hosts
N/A	192.168.1.1

Note: The downloaded Vulnerability 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

TABLE OF CONTENTS

Hosts Executive Summary

• 192.168.1.1.....	4
--------------------	---

Nessus Essentials

Hosts Executive Summary

192.168.1.1



Vulnerabilities

Total: 2

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

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:

WebWiFiScan2 / Configuration

[Back to Scan Report](#)

Disable All Enable All

Settings

Credentials

Plugins

Show Enabled |

STATUS	PLUGIN FAMILY	TOTAL	STATUS	PLUGIN NAME	PLUGIN ID
MIXED	Web Servers	1253	ENABLED	Web Application Potentially Vulnerable to Clickjacking	85582

Scan details – Hosts:

WebWiFiScan2

Configure Audit Trail

[Back to My Scans](#)

Hosts	Vulnerabilities	History
Filter	Search Hosts	1 Host
<input type="checkbox"/> Host	Vulnerabilities	
<input type="checkbox"/> 192.168.1.1	6	

Graphical Report:

Scan Details

Policy:	Advanced Scan
Status:	Canceled
Scanner:	Local Scanner
Start:	Today at 9:42 PM
End:	Today at 9:44 PM
Elapsed:	2 minutes

Vulnerabilities



Scan details – Vulnerabilities: (Report on identified vulnerabilities)

WebWiFiScan2

[Back to My Scans](#)

[Configure](#)

[Audit Trail](#)

Hosts1

Vulnerabilities1

History1

Filter

Search Vulnerabilities

1 Vulnerability

<input type="checkbox"/>	Sev	Name	Family	Count	
<input type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	6	<div><div></div><div></div></div>

Vulnerability details for “Nessus Syn Scanner”

←

→

↺

Not secure | localhost:8834/#scans/reports/31/vulnerabilities/11219

Scans Settings

My Scans

All Scans

Trash

Policies

Plugin Rules

Scanners

Community

Research

Tenable News

Canvas LMS Unauthenticated Blind SSRF

[Read More](#)

My Scans

All Scans

Trash

Policies

Plugin Rules

Scanners

Community

Research

Tenable News

CVE-2020-2040: Critical Buffer Overflow Vulnerabil...

WebWiFiScan2 / Plugin #11219

[Back to Vulnerabilities](#)

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

[Hosts](#) 1 [Vulnerabilities](#) 1 [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 / hp	192.168.1.1

Port 22/tcp was found to be open

Port	Hosts
22 / tcp / sh	192.168.1.1

Port 23/tcp was found to be open

Port	Hosts
23 / tcp	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	192.168.1.1

Port 5431/tcp was found to be open

Port	Hosts
5431 / tcp	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

Note: The downloaded Vulnerability 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

TABLE OF CONTENTS

Hosts Executive Summary

• 192.168.1.1.....	4
--------------------	---

Nessus Essentials

Hosts Executive Summary

192.168.1.1



Vulnerabilities

Total: 1

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

Selected **Badlock Detection**:

Name: BadlockWiFi

Folder: My Scans

Targets: 192.168.1.1/24 (IP Address of my home WiFi router)

Scan details – Hosts:

BadlockWiFi

[Back to My Scans](#)

Configure

Audit Trail

Hosts2Vulnerabilities2History1

FilterSearch Hosts2 Hosts

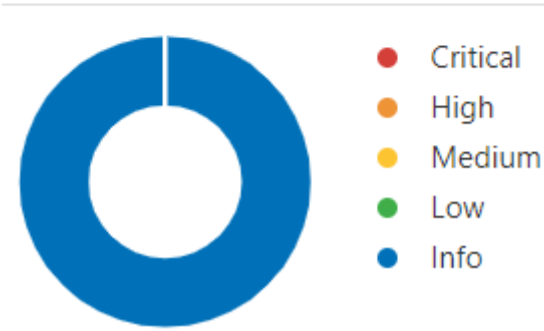
<input type="checkbox"/>	Host	Vulnerabilities	
<input type="checkbox"/>	192.168.1.1	7	×
<input type="checkbox"/>	192.168.1.100	1	×

Graphical Report:

Scan Details

Policy:	Badlock Detection
Status:	Canceled
Scanner:	Local Scanner
Start:	Today at 10:03 PM
End:	Today at 10:05 PM
Elapsed:	2 minutes

Vulnerabilities



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	
<input type="checkbox"/>	Sev	Name	Family	Count	
<input type="checkbox"/>	INFO	Nessus SYN scanner	Port scanners	6	
<input type="checkbox"/>	INFO	Nessus Scan Information	Settings	2	

Vulnerability details for “Nessus Scan Information”

nessus

Essentials

Scans Settings

Back to Vulnerabilities

Configure Audit Trail Launch Report Export

My Scans

All Scans

Trash

Policies

Plugin Rules

Scanners

Community

Research

Tenable News

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

Read More

My Scans

All Scans

Trash

Policies

Plugin Rules

Scanners

Community

Research

Tenable News

Unauthenticated email forgery/spoofing in WordPress...

BadlockWiFi / Plugin #19506

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.

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
Credential checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CPI 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

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

Note: The downloaded Vulnerability 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

TABLE OF CONTENTS

Hosts Executive Summary

• 192.168.1.1.....	4
• 192.168.1.100.....	5

Nessus Essentials

Hosts Executive Summary

192.168.1.1



Vulnerabilities

Total: 2

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

192.168.1.100



Vulnerabilities

Total: 1

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

Scanner Health:

Scanner Health

