



Nessus

A Vulnerability Scanner Tool in Network Forensic

- Chapter 10 -

서울과학기술대학교 컴퓨터공학과 진호천

Depart. Computer Science, Seoul National University of Science and Technology

CONTENTS



10.1	Introduction	205	10.7	Process of Nessus	209
10.2	History of Nessus.....	206	10.7.1	Step One: Download and Install Nessus.....	209
10.3	Related Study	206	10.7.2	Step Two: Set Up Your Nessus Account and Activation Code.....	209
10.4	Basics	206	10.7.3	Step Three: Start a Vulnerability Scan.....	210
10.4.1	Nessus Essential.....	207	10.7.4	Step Four: Make Sense of the Results	213
10.4.2	Nessus Professional	207	10.8	Pros and Cons of Nessus.....	216
10.4.3	Tenable.io	208	10.8.1	Pros of Nessus.....	216
10.5	Features of Nessus	208	10.8.2	Cons of Nessus.....	217
10.6	Block Diagrams of Nessus Scan Process	208	10.9	Conclusion	217
			References.....		217



- ✓ This chapter mainly introduces Nessie network vulnerability scanning software, which is a network vulnerability scanning tool that can simulate real data.
- ✓ This chapter explains Nessie in great detail, from installation to running steps. Nessie's scanning of network vulnerability risks is helpful to realize the update and evaluation of security protocols in DT security evaluation.
- ✓ This chapter mainly introduces Nessie network vulnerability scanning software, which is a network vulnerability scanning tool that can simulate real data.
- ✓ This chapter explains Nessie in great detail, from installation to running steps.
- ✓ Nessie's scanning of network vulnerability risks is helpful to realize the update and evaluation of security protocols in DT security evaluation.



- ✓ **Renaud Deraison** introduced Nessus project in 1998 when he was only 17 years old for the internet community to provide free remote security scanning. He introduced Nessus as an open-source project, led by the community while he was pursuing his career in IT field. So, the copyright of Nessus belongs to the Renaud Deraison.
- ✓ The availability of the source code to all has led to the creation of forks, which are the rivals to the Nessus system. Soon it became the leading vulnerability scanner in the world. Tenable network security company co-founder Renaud Deraison changed the Nessus 3 to a licensed version. The minority of the plugins and the Nessus 2 version are still GPL, which leads to the open-source project, based on Nessus like porz-wahn and openvas. Tenable began working in 2002. It had 2 million downloads of the free version at that time and 27000 businesses were already using it, while the paid version of Nessus came in 2005.



- ✓ Nessus is a network vulnerability scanner.
- ✓ It uses plug-ins, which are generally separate files, and the vulnerability checks are handled by them.
 - Plug-ins are the individual pieces of codes which are to be used by Nessus for conducting individual scan on target plug-ins that are wide in their capabilities and number.
- ✓ DT is a computer program operation.
- ✓ DT helps us in creating simulation of real-world data and predicts the network software performance or other software performances, along with internet of things analytical software and artificial intelligence to enhance the performance.



- ✓ It basically makes a virtual computer that receives feedback from the servers.
- ✓ Its configuration is simple or complex, according to the requirements. So, the plug-ins are launched in the manner given below and target the host.
 - ❖ Firstly, the parameters of scan are defined and then click on the new scan to create a new scan.
 - ❖ After that, add the necessary details and then launch the scan. A report gets generated which shows that how many vulnerabilities are present in the network.

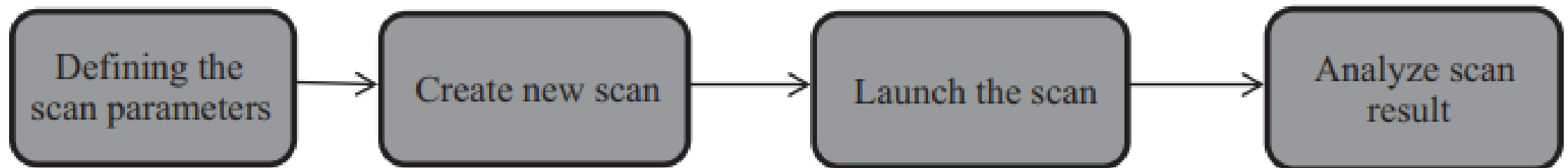
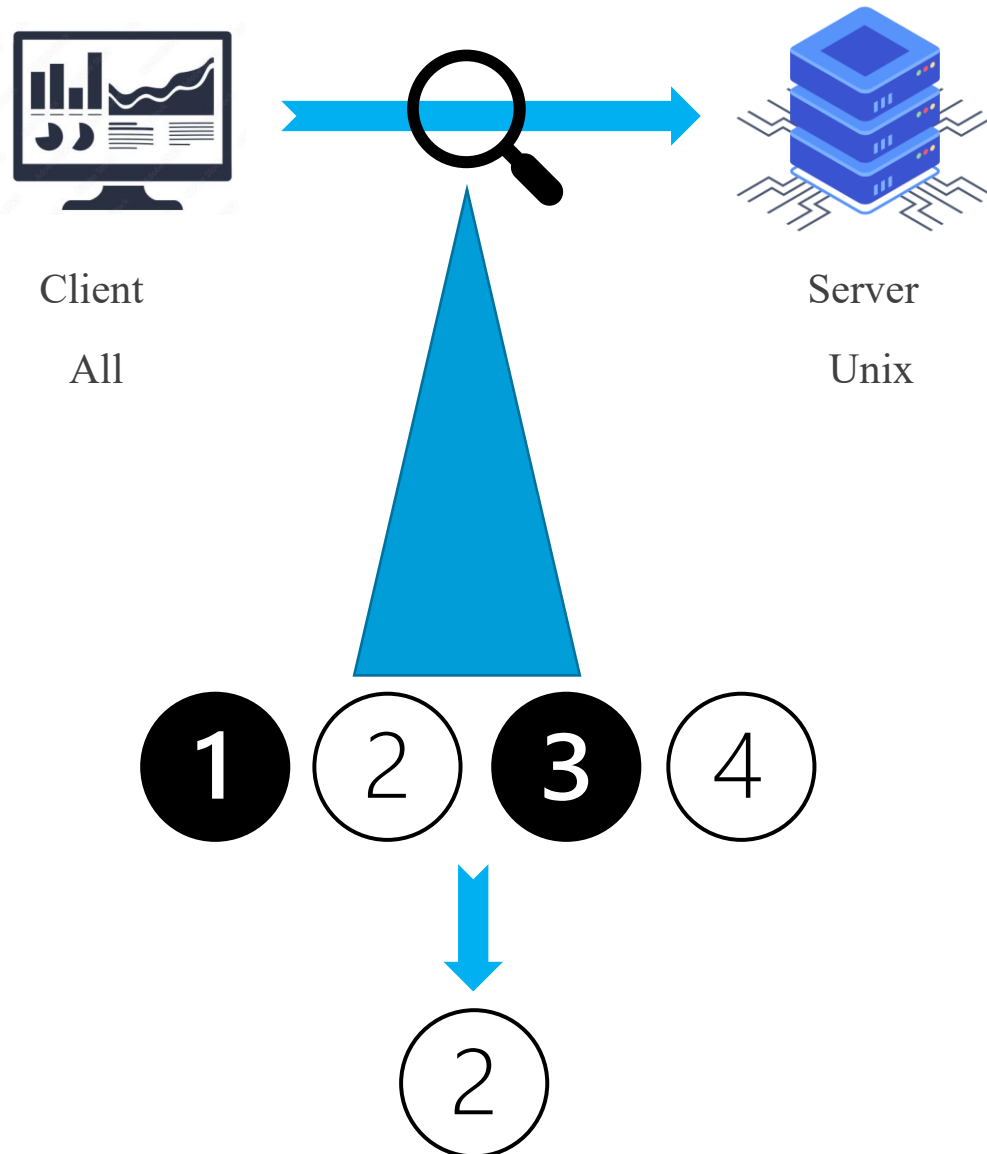


FIGURE 10.1 Scan functions of Nessus.



1. One of the most attractive and effective features of Nessus is that it is freely available. Anyone may download it and then use Nessus essential software. But there are some paid versions also available.
2. It is an open-source software and many people contribute to Nessus every day that helps it to stay up-to-date and freely available at all the times for the user.
3. Plug-ins can be updated once the features of plug-ins with new vulnerabilities are released.
4. Nessus scans for vulnerabilities on Linux, Windows and UNIX systems. This will help Nessus to become a good, all-round tool so that you can scan in a mixed environment in single session.
5. Nessus also utilizes N-map for port scanning.
6. The server-client architecture is a plus point of Nessus if there are multiple persons using the system. So, the user rights can be defined to lock down the types of scans they can do and unlock the ones they don't want to do.
7. The plug-in architecture of Nessus ensures that it checks each vulnerability as an individual plug-in. This means that it gives you the right to your own plug-ins.
8. It doesn't do the penetration testing because its main focus is to scan the system or the applications.
9. Nessus allows multiple profiles/policies to do different types of scans such as malware scan, bad shell shock detection and web applications scan.
10. It classifies the vulnerabilities into a prioritized risk-based-categories, from critical to normal.



✓ **Nessus essential**

- ❖ It is the free version of the vulnerability scanner. Its scans are limited to 16 IP addresses and this tool is basically aimed for students of the network technology and information security. It is also used by the businesses for understanding the requirements and see how it works for their purpose and then the organization buys the paid version. So, it is not only for the students but it is also used by the organizations and home users. You can pick up the free plug-ins that are provided by the community on the internet.

✓ **Nessus professional**

- ❖ It is one of the paid versions of the vulnerability scanner. It gives you full support features. It is the same software as Nessus essential but here there is no restriction limit of 16 IP addresses. It gives you live results and the system also sweeps periodically. Nessus professional is charged by the subscription method. This means that it is an yearly service and there is no monthly payment method. If you want discount, then you have an option for multiyear subscription which is generally 3 years long. It provides seven days' free trial version.

✓ **Tenable.io**

- ❖ It is a cloud version of Nessus pro. It is more costly than Nessus professional and it comes with advance support packages. It starts with the base price of 65 nodes and the price is increased in accordance with the node increment.



- ✓ The block diagram of Nessus shows how the user interacts with Nessus software and performs the vulnerability scanning onto that. Figure 10.2 shows how Nessus scan works and describes how the Nessus scan process works in which the user can check the vulnerability of network IP address locally and remotely. With the help of the above figure, the user can select which type of scan he wants to do and then add the necessary details to the new scan. Once the scan is executed, a report is generated, which illustrates the vulnerabilities present in the network.

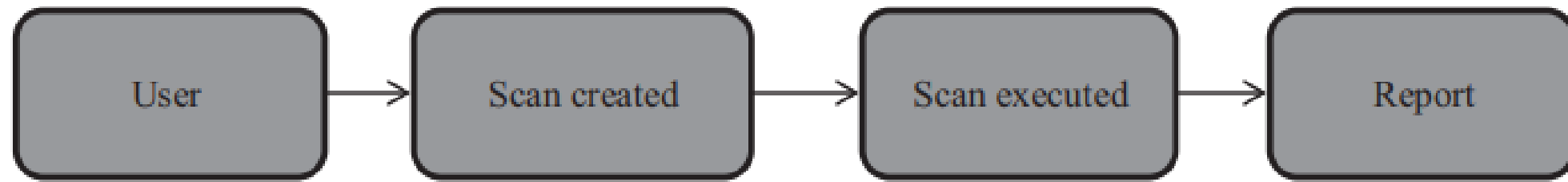


FIGURE 10.2 Block diagram of Nessus scan.



- ✓ For downloading Nessus, the users first need to sign up for an online account and then they can download the software and get an activation code on the email-id filled at the time of registration. The steps involved are:
 1. First, go to Nessus homepage, then enter the name and email address, and then click on the Register button. Users have to enter a real email address here because Nessus sends an activation code on that email id to be entered in the registration form.
 2. Now, click the Download button, to download Nessus on your operating system, according to the system bits. It's available for Mac, UNIX, windows and Linux.
 3. When the downloading is complete, then run the installer package and follow instructions on the screen and finish the installation.
 4. Now, Nessus creates a local server on your computer or laptop and runs from there.
- ✓ When Nessus is installed on your computer then point the web browser to the following address: [https:// localhost:8834/](https://localhost:8834/). This is the address where users have to complete the signup process and activate his/her copy of Nessus.



- A. Click "New Scan" : After the user logs in, click "New Scan", and the newly scanned dashboard will appear, as shown in Figure 10.3.
- B. Click "Basic Network Scan" : After clicking a new scan, the user must select the type of scan to be performed, as shown in Figure 10.4. Typically, basic network scanning is done in Nessus.
- C. Name the scan, add description, and set the target IP address: After selecting the basic network scan, you must enter necessary details, such as scan name, description, and target. See Figure 10.5.
- D. In the Target field, the user must enter IP scan details about the home network or local network. For example, if our router is at 192.168.0.1, after setting the target and starting the scan, a network vulnerability report will be generated, assessing the impact of the vulnerability based on the color code in Figures 10.6 and 10.7.
- E. In the Targets field, you must enter detailed IP scan information about the remote network. For example, if our router is at 192.168.1.52, after setting the target field, a report is generated showing the vulnerability of the network and its validity based on the color code. This is shown in Figure 10.8-10.10.
- F. Click "Save" : Now, depending on the number and type of devices connected to your network, it will take some time.

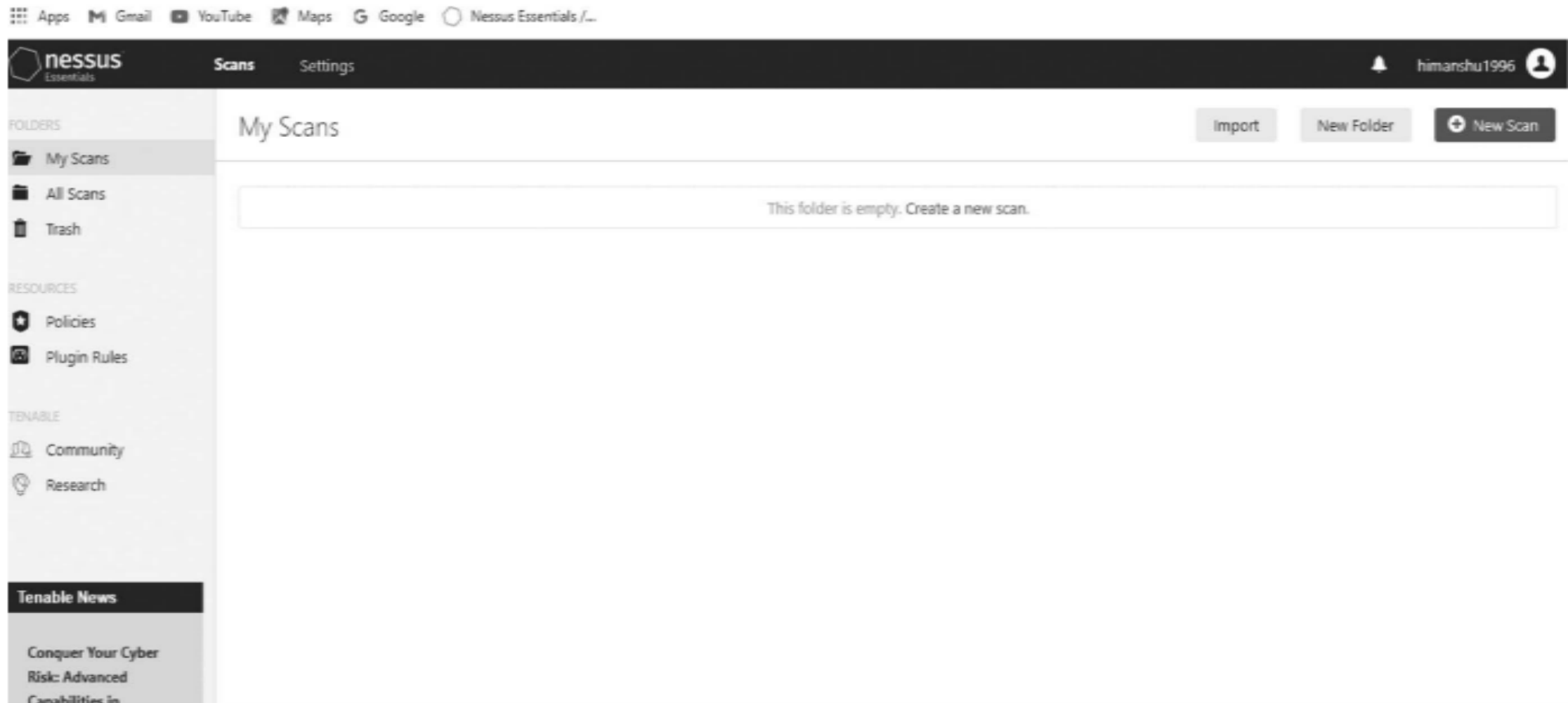


FIGURE 10.3 New scan dashboard.

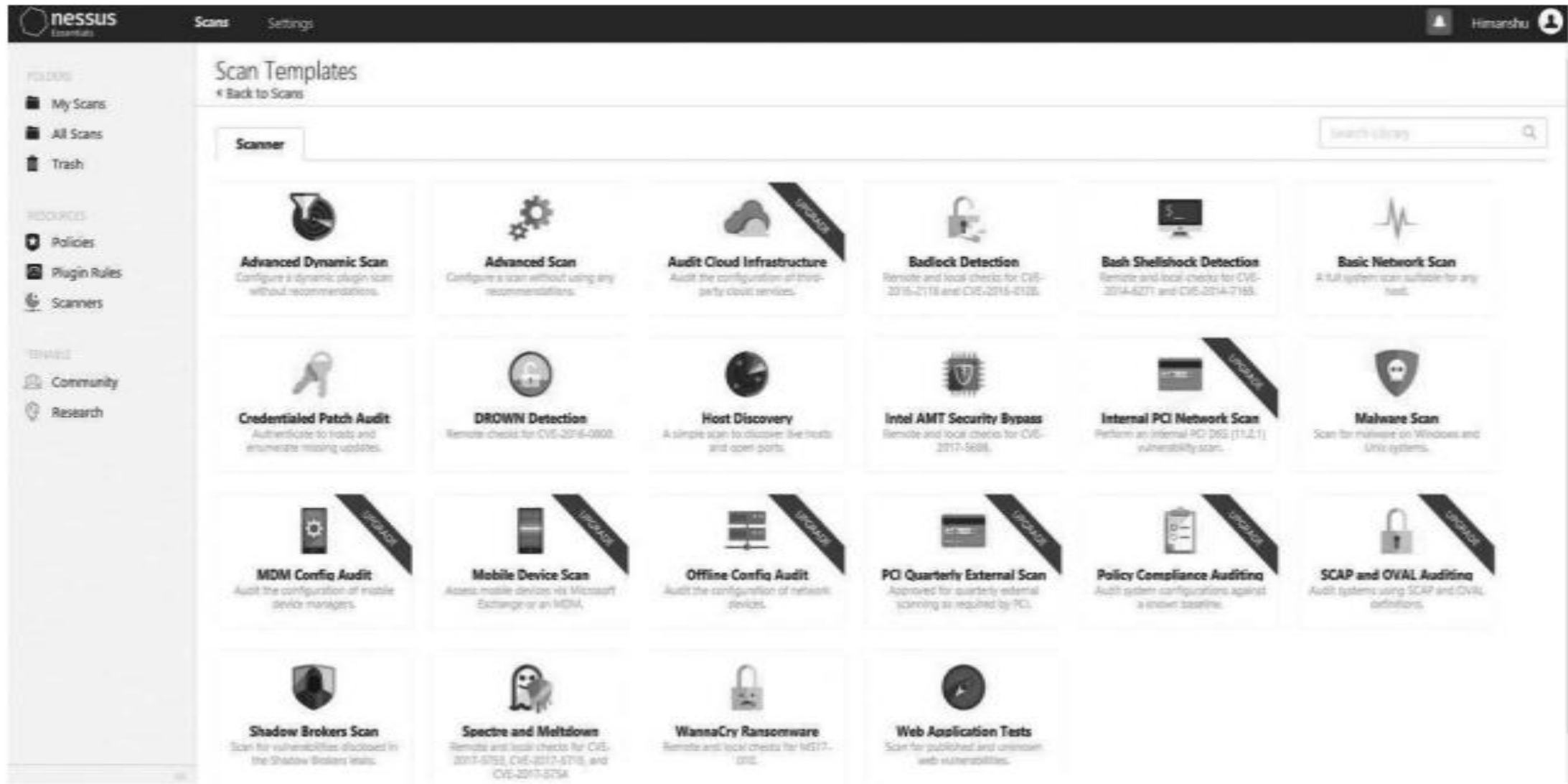


FIGURE 10.4 Basic network scan.



The screenshot shows the Nessus Essentials web interface for configuring a new scan. The top navigation bar includes the 'nessus Essentials' logo, 'Scans', and 'Settings' tabs. A user profile for 'Hinsamshu' is visible in the top right. The left sidebar contains navigation links for 'FOLDERS' (My Scans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules, Scanners). The main content area is titled 'New Scan / Basic Network Scan' with a back link to 'Scan Templates'. It features three tabs: 'Settings' (active), 'Credentials', and 'Plugins'. Under the 'Settings' tab, a left-hand menu lists categories: 'BASIC' (with sub-items 'General', 'Schedule', and 'Notifications'), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. The 'General' sub-item is selected, showing fields for 'Name' (required), 'Description', 'Folder' (set to 'My Scans'), and 'Targets' (with an example: '192.168.1.1-192.168.1.5, 192.168.2.0/24, test.com' and a required field indicator). At the bottom of the form are 'Upload Targets' and 'Add File' buttons. A 'Save' button with a dropdown arrow and a 'Cancel' button are at the very bottom.

FIGURE 10.5 Add the necessary details.



FIGURE 10.6 Local network vulnerabilities.



nessus Essentials

Scans Settings

example1 / 192.168.0.1

Configure Audit Trail Launch Report Export

Vulnerabilities 14

Filter Search Vulnerabilities 14 Vulnerabilities

Sev	Name	Family	Count		
MEDIUM	IP Forwarding Enabled	Firewalls	1		
MEDIUM	Unencrypted Telnet Server	Misc.	1		
MIXED	SSH (Multiple Issues)	Misc.	2		
LOW	DHCP Server Detection	Service detection	1		
INFO	Nessus SYN scanner	Port scanners	3		
INFO	Service Detection	Service detection	3		
INFO	HTTP (Multiple Issues)	Web Servers	2		
INFO	Embedded Web Server Detection	Web Servers	1		
INFO	Ethernet Card Manufacturer Detection	Misc.	1		
INFO	Ethernet MAC Addresses	General	1		
INFO	Nessus Scan Information	Settings	1		

Host Details

IP: 192.168.0.1
MAC: 60:9C:9F:35:5B:20
Start: August 22 at 11:14 AM
End: August 22 at 11:21 AM
Elapsed: 7 minutes
KB: Download

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

FIGURE 10.7 Local network vulnerabilities continued.

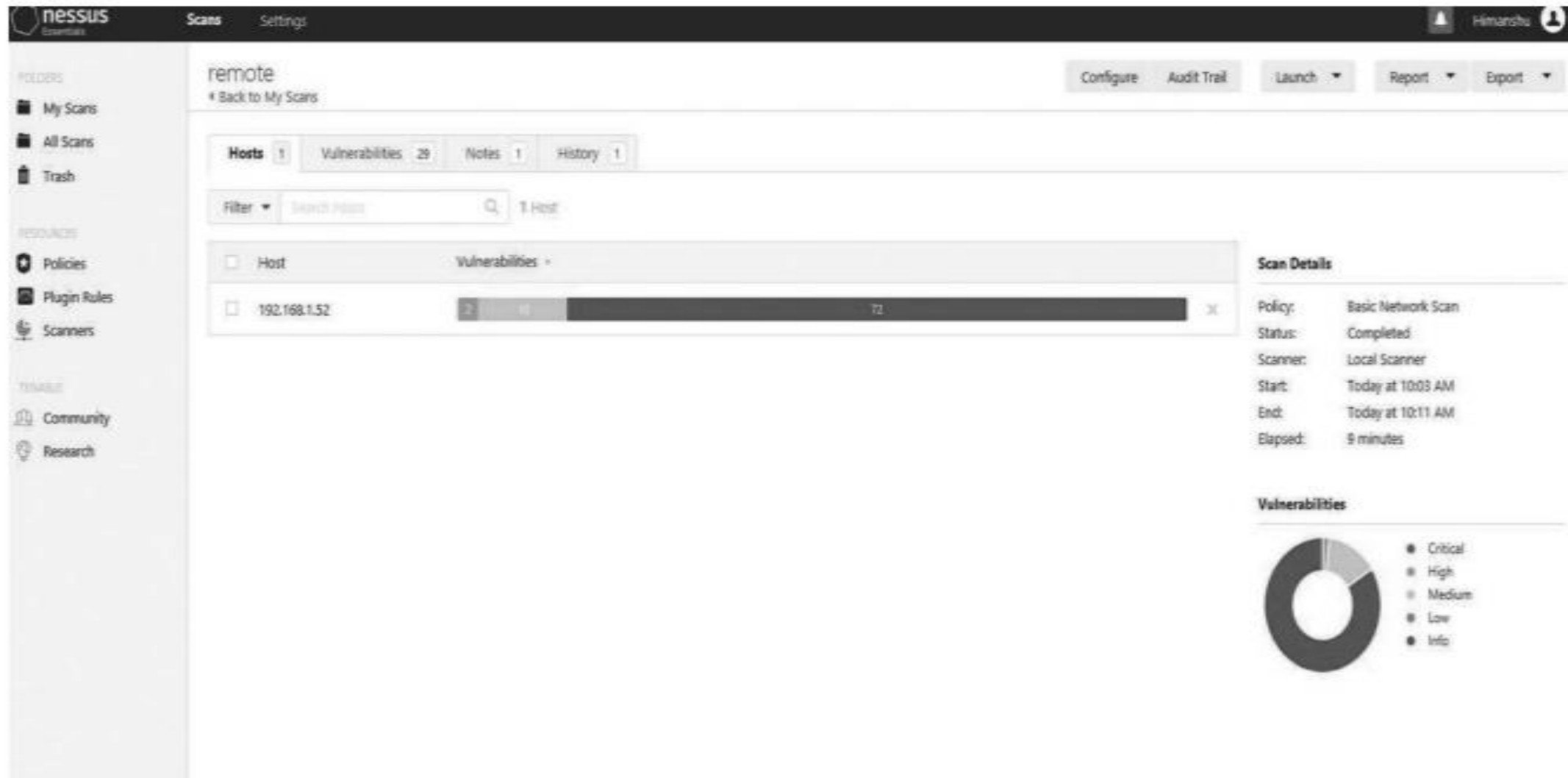


FIGURE 10.8 Remote network.

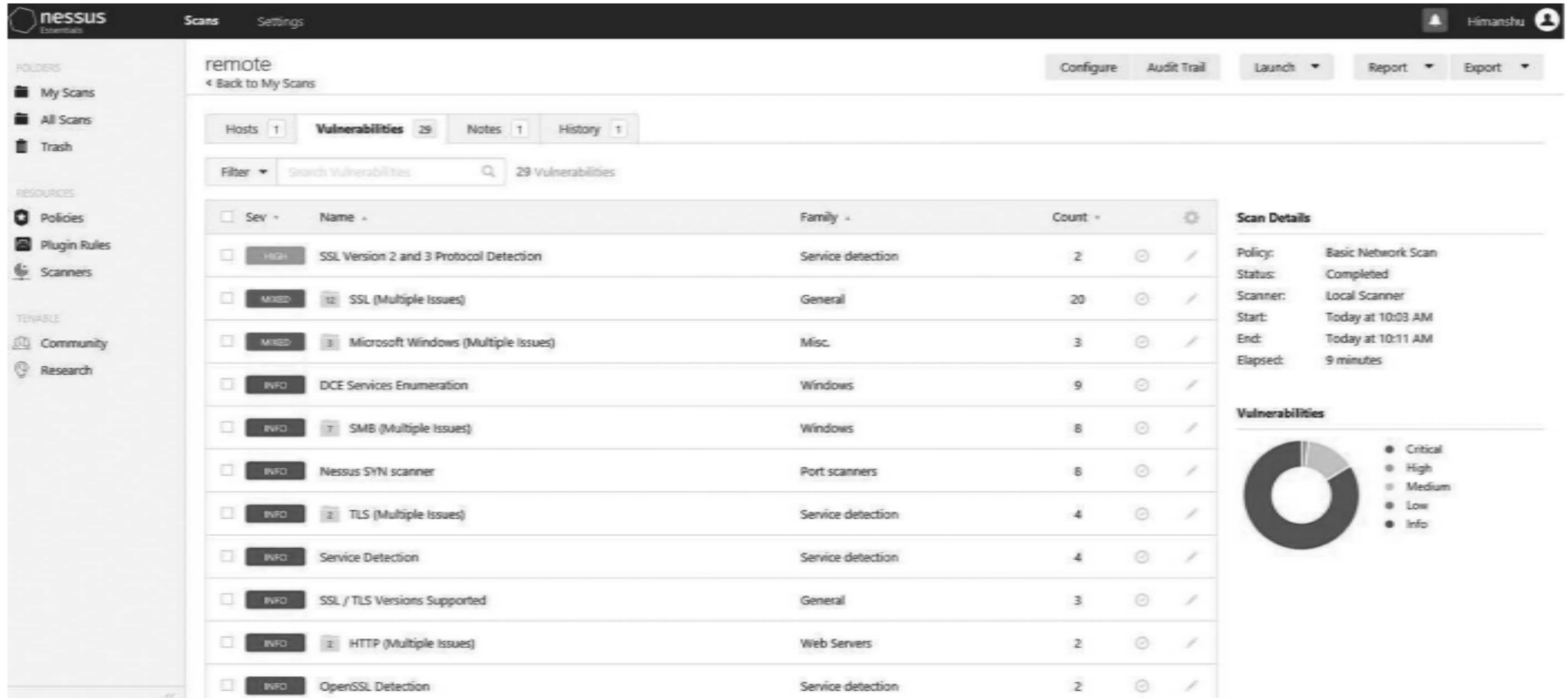


FIGURE 10.9 Remote network vulnerabilities.



The screenshot displays the Nessus Essentials web interface. On the left is a sidebar with navigation options: FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Scanners), and TOOLS (Community, Research). The main area shows a table of vulnerabilities under the 'Settings' tab. Each row includes a checkbox, a severity level (all are 'INFO'), a title, a category, a count (all are '1'), and icons for details and edit.

Severity	Title	Category	Count	Details	Edit
<input type="checkbox"/> INFO	Ethernet Card Manufacturer Detection	Misc.	1		
<input type="checkbox"/> INFO	Ethernet MAC Addresses	General	1		
<input type="checkbox"/> INFO	Host Fully Qualified Domain Name (FQDN) Resolution	General	1		
<input type="checkbox"/> INFO	Inconsistent Hostname and IP Address	Settings	1		
<input type="checkbox"/> INFO	Local Checks Not Enabled (info)	Settings	1		
<input type="checkbox"/> INFO	Nessus Scan Information	Settings	1		
<input type="checkbox"/> INFO	NetBIOS Multiple IP Address Enumeration	Windows	1		
<input type="checkbox"/> INFO	No Credentials Provided	Settings	1		
<input type="checkbox"/> INFO	OS Identification	General	1		
<input type="checkbox"/> INFO	Server Message Block (SMB) Protocol Version 1 Enabled (unauthenticated check)	Misc.	1		
<input type="checkbox"/> INFO	SSL Certificate Chain Contains Certificates Expiring Soon	Misc.	1		
<input type="checkbox"/> INFO	SSL Root Certification Authority Certificate Information	General	1		
<input type="checkbox"/> INFO	Traceroute Information	General	1		
<input type="checkbox"/> INFO	VMWare STARTTLS Support	Misc.	1		
<input type="checkbox"/> INFO	Windows Terminal Services Enabled	Windows	1		

FIGURE 10.10 Remote network vulnerabilities continued.

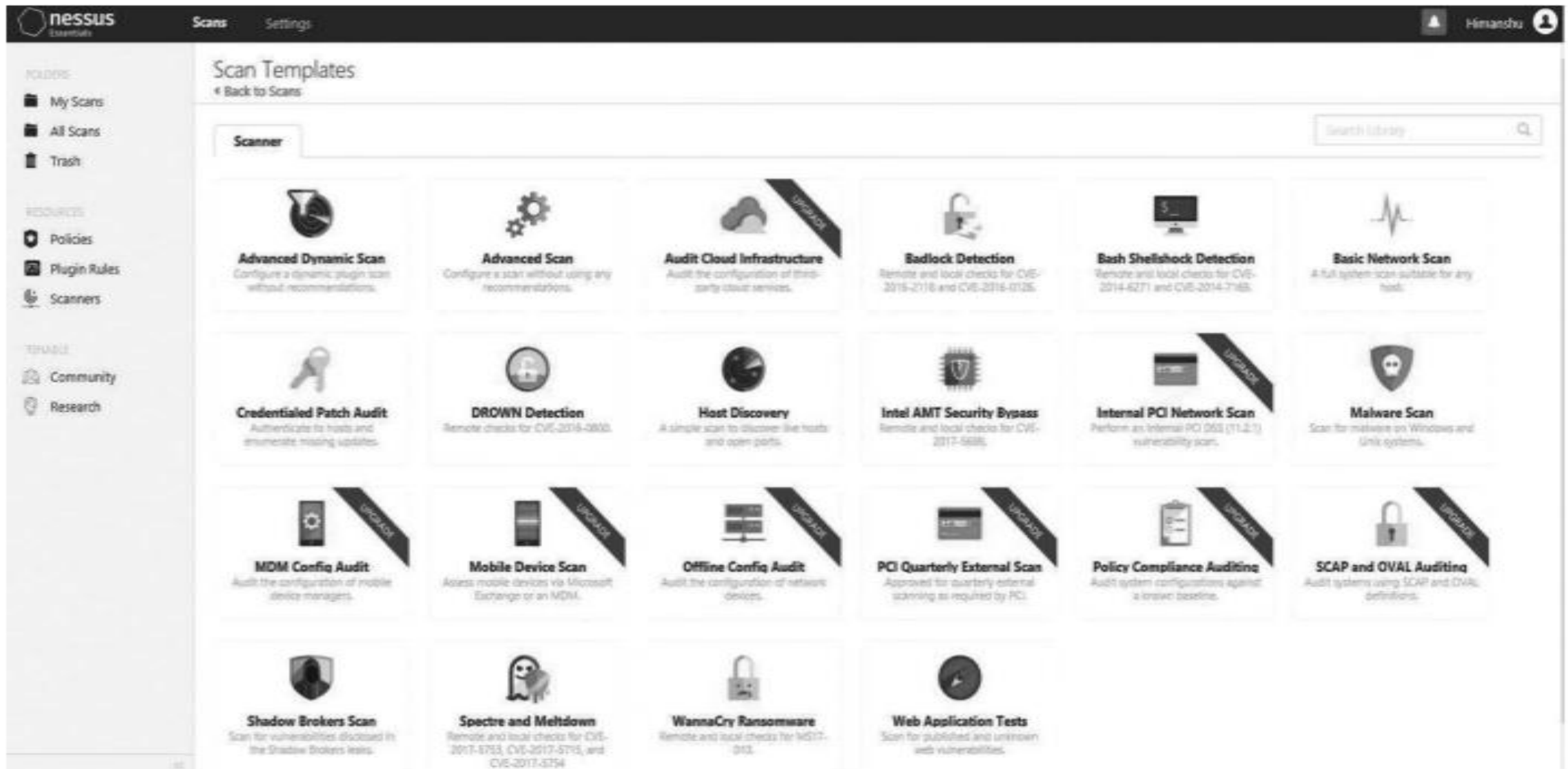


FIGURE 10.11 More features of Nessus.



The screenshot displays the Nessus web interface. On the left is a sidebar with navigation links: My Scans, All Scans, Trash, Policies, Plugin Rules, Scanners, Community, and Research. The main content area is titled 'remote / Plugin #20007' with a link to 'Back to Vulnerabilities'. Below this are tabs for Hosts (1), Vulnerabilities (29), Notes (1), and History (1). The selected tab shows the details for 'SSL Version 2 and 3 Protocol Detection'. The description explains that the remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0, which are affected by several cryptographic flaws, including insecure padding schemes and session renegotiation. It notes that an attacker can exploit these flaws for man-in-the-middle attacks or decryption. The solution recommends disabling SSL 2.0 and 3.0 and using TLS 1.1 or higher. The 'See Also' section provides links to academic papers and Nessus documentation. On the right, the 'Plugin Details' section lists attributes like Severity (High), ID (20007), Version (1.32), Type (remote), Family (Service detection), Published date (October 12, 2005), and Modified date (March 27, 2019). Below this is the 'Risk Information' section, which includes Risk Factor (High), CVSS v3.0 Base Score (7.5), CVSS v3.0 Vector, CVSS Base Score (7.1), and CVSS Vector. The 'Vulnerability Information' section at the bottom indicates 'In the news: true'.

remote / Plugin #20007
Back to Vulnerabilities

Hosts: 1 Vulnerabilities: 29 Notes: 1 History: 1

SSL Version 2 and 3 Protocol Detection

Description
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.1 (with approved cipher suites) or higher instead.

See Also
<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>
<http://www.nessus.org/u7b06c7e95>
<http://www.nessus.org/u7247c4540>

Plugin Details

Severity:	High
ID:	20007
Version:	1.32
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	March 27, 2019

Risk Information

Risk Factor: High
CVSS v3.0 Base Score: 7.5
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVSS Base Score: 7.1
CVSS Vector: CVSS2#AV:N/AC:M/Au:N/CC:R/N/A:N

Vulnerability Information

In the news: true

FIGURE 10.12 Plugins.

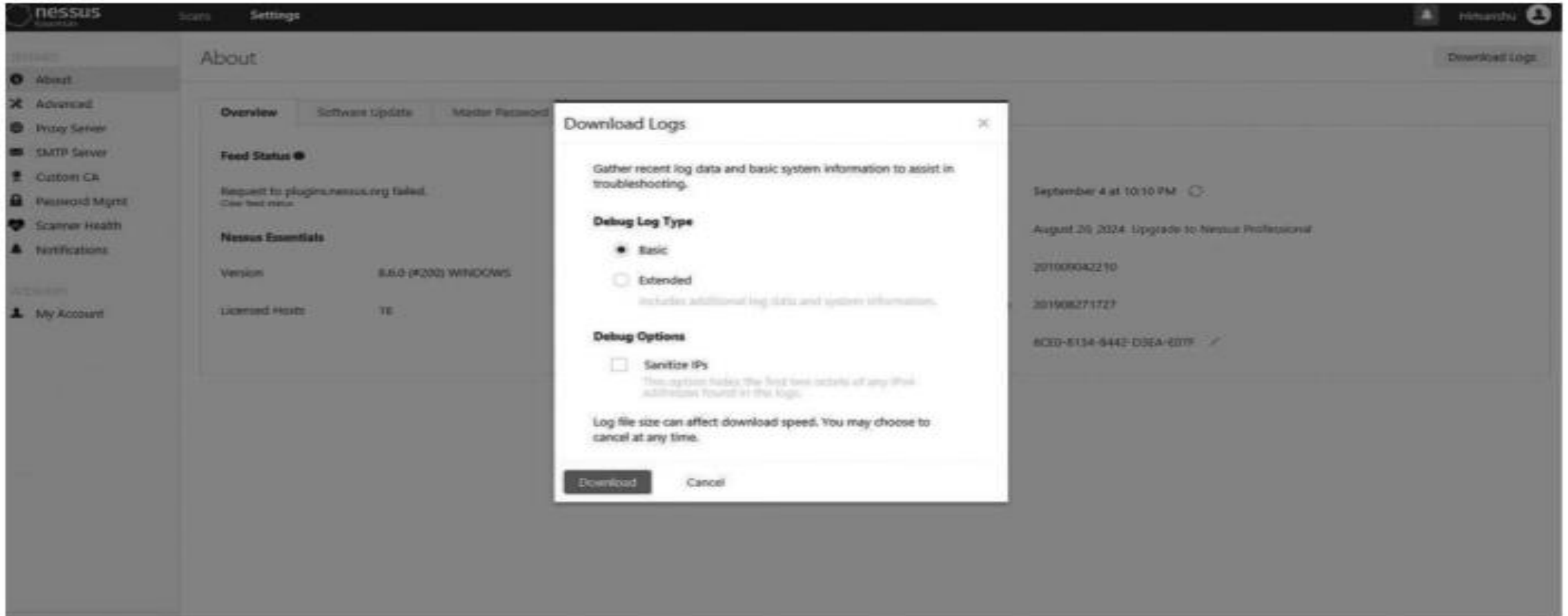


FIGURE 10.13 Download logs.



PROS

1. With Nessus, servers or workstations that lack critical patches can be identified.
2. It not only lists vulnerabilities, but also provides detailed descriptions of them.
3. Nessus Professional Edition also performs PCI scanning.
4. Nessus has the ability to use multiple configuration profiles/policies to perform different types of scans, such as malware scans, bad Shell Shock detection, and web application scans.
5. It also has the ability to classify vulnerabilities into risk-based priority categories, ranging from critical to normal.
6. Nessus' plugin architecture ensures that each vulnerability is checked as a separate plugin. This means that you have your own plugins.

CONS

1. It has the ability to use the upgrade function within records.
2. Sometimes, scans may take a long time to complete. Therefore, we need to divide them into smaller parts.
3. Advanced users are not allowed to disable plugins within plugin groups.
4. The status of the scan may improve as it only displays 0% or 100%, meaning that the progress bar does not show the percentage of the scan completed.
5. Scanning can be further simplified by default settings configuration.



This chapter presents study of the history of Nessus, what it is and how does it work with the plugins. It also studies features of Nessus which makes Nessus a highly recommended network vulnerability scanning tool in the network forensic. A block diagram also describes the flow of Nessus vulnerability scanner. This chapter also presents that the Nessus helps in digital twin evaluation for the network vulnerability scanning purpose, to make the simulation of the real-world data, to predict the network vulnerability assessment performance. This chapter also presents how Nessus is to be downloaded and the steps involved in taking a local IP address (1 92.168.0.1) and checking for the vulnerability. We found 2 vulnerabilities in medium state, 2 vulnerabilities in low and the rest 16 lie under info category. Then we performed the same with a remote IP address (1 92.168.1.52) and we found 2 vulnerabilities in high, 10 in medium state and the rest 72 lie under info category.



1. A. Sowmyashree and H. S. Guruprasad. "Evaluation and analysis of vulnerability scanners: Nessus and OpenVAS." *International Research Journal of Engineering and Technology (IRJET)*, Bangalore, India, Vol. 7, No. 5, pp. 2068–2073, 2020.
2. Sandeep Kumar Yadav, Daya Shankar Pandey and Shrikant Lade, "A comparative analysis of detecting vulnerability in network systems." *IJARCSSE*, Vol. 7, No. 5, pp. 336–340, May 2017.
3. Sheetal Bairwa, Bhawna Mewara and Jyoti Gajrani. "Vulnerability scanners: A proactive approach to assess web application security." *International Journal on Computational Sciences & Applications (IJCSA)*, Vol. 4, No. 1, pp. 113–124, Ajmer, India, February 2014.
4. Peng Li and Baojiang Cui, "A comparative study on software vulnerability static analysis techniques and tools." In *Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS)*, pp. 521–524, 2010.
5. Kushe R. "Comparative study of vulnerability scanning tools: Nessus vs Retina." *International Scientific Journal "Security & Future"*, Albania, Vol. 1, No. 2, pp. 69–71, 2017.
6. Harry Anderson. *Introduction to Nessus*. INFOCUS, 2003. http://apachepersonal.miun.se/~janjon/oldcourse/dtab80/lab/lab2/nessus_1.pdf
7. Harrison, Lane, Riley Spahn, Mike Iannacone, Evan Downing, and John R. Goodall. "Nv: Nessus Vulnerability Visualization for the Web." In *Proceedings of the ninth international symposium on visualization for cyber security*, pp. 25–32. 2012.
8. Paul Schmelzel. *Nessus: Vulnerability Scanning and beyond*. SANS, United States, 2002.



Welcome to Nessus

Choose how you want to deploy Nessus. Select a product to get started.

- ☐ Nessus Expert Trial
- ☐ Nessus Professional Trial
- ☐ Nessus Expert
- ☐ Nessus Professional
- ☐ Nessus Manager
- ☒ Nessus Essentials
- ☐ Managed Scanner

Continue

© 2023 Tenable™, Inc.



Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Chahot

Password *



Back

Submitting...

© 2023 Tenable™, Inc.



Initializing

Please wait while Nessus is initializing.

Downloading plugins...



Try to start

Scanner

DISCOVERY

Host Discovery
A simple scan to discover live hosts and open ports.

Basic Network Scan
A full system scan suitable for any host.

Advanced Scan
Configure a scan without using any recommendations.

Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.

Malware Scan
Scan for malware on Windows and Unix systems.

Mobile Device Scan
Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests
Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.

Spectre and Meltdown
Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754.

WannaCry Ransomware
Remote and local checks for MS17-010.

Ripple20 Remote Scan
A remote scan to fingerprint hosts potentially running the Treck stack in the network.

ZeroLogon Remote Scan
A remote scan to detect Microsoft Netlogon Elevation of Privilege (ZeroLogon).

Solorigate
Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exchange
Remote and local checks to detect Exchange vulnerabilities targeted by HAFNIUM.

PrintNightmare
Local checks to detect the PrintNightmare Vulnerability in Windows Print Spooler.

Active Directory Starter Scan
Look for misconfigurations in Active Directory.

Log4Shell
Detection of Apache Log4j CVE-2021-44228

Log4Shell Remote Checks
Detection of Apache Log4j CVE-2021-44228 via Remote Direct Checks

Log4Shell Vulnerability Ecosystem
Detection of Log4Shell Vulnerabilities

CISA Alerts AA22-011A and AA22-047A
Detection of vulnerabilities from recent CISA alerts.

ContiLeaks
Detection of vulnerabilities revealed in the ContiLeaks chats.

Ransomware Ecosystem
Vulnerabilities used by ransomware groups and affiliates.

2022 Threat Landscape Report (TLR)
A scan to detect vulnerabilities featured in our End of Year

UPGRADE



Haotian Chen / Configuration

[← Back to Scan Report](#)

Settings

CredentialsPlugins

BASIC ▾

- General
- Schedule
- Notifications

DISCOVERY >

ASSESSMENT >

REPORT >

ADVANCED >

Name

Test

Description

Folder

My Scans ▾

Targets

192.168.1.1-192.168.1.255

Upload Targets

Add File

Save

Cancel



Try to start

SeoulTech UCS Lab

[Back to My Scans](#)

[Settings](#) [Assets from](#) [Scanners](#) [Reports](#) [Export](#)

Hosts 10 **Vulnerabilities** 33 **Remediations** 1 **Notes** 1 **VPR Top Threats** 1 **History** 1

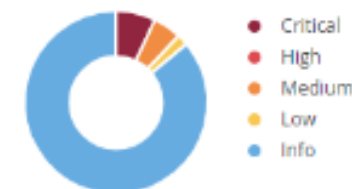
Filter Search Hosts 10 Hosts

<input type="checkbox"/>	Host	Vulnerabilities	
<input type="checkbox"/>	192.168.0.16	1 33	×
<input type="checkbox"/>	192.168.0.1	1 1 24	×
<input type="checkbox"/>	192.168.0.10	1 25	×
<input type="checkbox"/>	192.168.0.23	3 20	×
<input type="checkbox"/>	192.168.0.42	10	×
<input type="checkbox"/>	192.168.0.35	6	×
<input type="checkbox"/>	192.168.0.11	4	×
<input type="checkbox"/>	192.168.0.14	4	×
<input type="checkbox"/>	192.168.0.18	4	×
<input type="checkbox"/>	192.168.0.36	4	×

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:15 AM
End: Today at 11:02 AM
Elapsed: an hour

Vulnerabilities





Try to start

SeoulTech UCS Lab

Settings Hosts Main Dashboard Reports Export

[Back to Hosts](#)

Vulnerabilities 18

Filter Search Vulnerabilities 18 Vulnerabilities

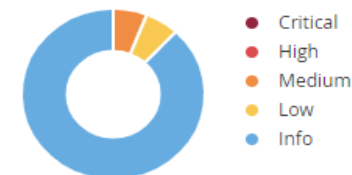
<input type="checkbox"/>	Sev	Score	Name	Family	Count		
<input type="checkbox"/>	MIXED	...	3 DNS (Multiple Issues)	DNS	3		
<input type="checkbox"/>	LOW	3.3 *	DHCP Server Detection	Service detection	1		
<input type="checkbox"/>	INFO	...	3 HTTP (Multiple Issues)	Web Servers	5		
<input type="checkbox"/>	INFO		Nessus SYN scanner	Port scanners	2		
<input type="checkbox"/>	INFO		Service Detection	Service detection	2		
<input type="checkbox"/>	INFO		Common Platform Enumeration (CPE)	General	1		
<input type="checkbox"/>	INFO		Device Type	General	1		
<input type="checkbox"/>	INFO		DNS Server hostname.bind Map Hostname Disclosure	DNS	1		
<input type="checkbox"/>	INFO		Embedded Web Server Detection	Web Servers	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 Timestamp Request Remote Date Disclosure	General	1		
<input type="checkbox"/>	INFO		Nessus Scan Information	Settings	1		
<input type="checkbox"/>	INFO		OS Identification	General	1		
<input type="checkbox"/>	INFO		TCP/IP Timestamps Supported	General	1		

Host: 192.168.0.1

Host Details

IP: 192.168.0.1
MAC: 88:36:6C:AC:14:04
OS: Linux Kernel 2.6
Start: Today at 10:15 AM
End: Today at 10:35 AM
Elapsed: 20 minutes
KB: [Download](#)

Vulnerabilities





Vulnerabilities 18

MEDIUM DNS Server Cache Snooping Remote Information Disclosure

Description

The remote DNS server responds to queries for third-party domains that do not have the recursion bit set.

This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited.

For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more.

Note: If this is an internal DNS server not accessible to outside networks, attacks would be limited to the internal network. This may include employees, consultants and potentially users on a guest network or WiFi connection if supported.

Solution

Contact the vendor of the DNS software for a fix.

See Also

http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf

Output

```
Nessus sent a non-recursive query for example.edu
and received 1 answer :
```

```
93.184.216.34
```

To see debug logs, please visit individual host

Port	Hosts
------	-------

53 / udp / dns	192.168.0.1
----------------	-------------

Plugin Details

Severity: Medium
ID: 12217
Version: 1.26
Type: remote
Family: DNS
Published: April 27, 2004
Modified: April 7, 2020

Risk Information

Risk Factor: Medium

CVSS v3.0 Base Score 5.3

CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N



Try to start

SeoulTech UCS Lab

朗读此页内容



语音选项

nessus Essentials

Scans Settings

Chahot

FOLDERS

My Scans
All Scans
Trash

SOURCES

Policies
Plugin Rules
Terrascan

Buhagyashree / Plugin #158900

[Back to Vulnerability Group](#)

Configure Audit Trail Launch Report Export

Vulnerabilities 17

CRITICAL Apache 2.4.x < 2.4.53 Multiple Vulnerabilities

Description

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)
- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)
- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)
- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (Zippenhop LLC) (CVE-2022-23943)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.53 or later.

See Also

<http://www.apache.org/dist/httpd/Announcement2.4.html>
https://httpd.apache.org/security/vulnerabilities_24.html

Output

```
URL          : http://192.168.0.23/  
Installed version : 2.4.52  
Fixed version  : 2.4.53
```

To see debug logs, please visit individual host

Port Hosts

Plugin Details

Severity: Critical
ID: 158900
Version: 1.6
Type: combined
Family: Web Servers
Published: March 14, 2022
Modified: June 15, 2022

Risk Information

Risk Factor: High
CVSS v3.0 Base Score 9.8
CVSS v3.0 Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/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 v2.0 Base Score: 7.5
CVSS v2.0 Temporal Score: 5.5
CVSS v2.0 Vector:
CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P
CVSS v2.0 Temporal Vector:
CVSS2#E:U/RL:O/RC:C
IAVM Severity: I

Vulnerability Information

CPE: cpe:/a:apache:httpd
cpe:/a:apache:http_server
Exploit Available: false
Exploit Ease: No known exploits are available
Patch Pub Date: March 14, 2022
Vulnerability Pub Date: December 16, 2021

Tenable News

Trend Micro Apex One
fcgiOfcDDA.exe File
Upload Vu...

[Read More](#)



THANKS

서울과학기술대학교 컴퓨터공학과 진호천