

# **Fundamentals of Information Security: Cybersecurity (88252)**

**Ana Herrera Flores'**

## **Security Lab 4 - Nessus Scanning**

### **Scan Types in Nessus and what they do:**

Basic Network Scan: provides additional information about the network before carrying out deeper scans.

Advanced Scan: it provides the user with the ability to customize the settings of the scan as well as a detailed scan.

Advanced Dynamic Scan: it includes new filters that match certain criteria, and it does this automatically.

Malware Scan: it identifies vulnerabilities that can be exploited by malware.

Mobile device scan: identify vulnerabilities for a mobile device but requires a Mobile Device Management (MDM) system.

Credentialed Path Audit scan: uses credentials that were provided to log in to the target system.

Intel AMT security bypass scan: it ensures accurate detection of the Intel AMT ports.

Spectre and Meltdown scan: it identifies hardware vulnerabilities.

WannaCry Ransomware scan: offer templates to detect vulnerabilities related to WannaCry, SMBv1, MS17-010 patch and others.

Ripple20 Remote scan: it scans vulnerabilities related to the Treck TCP/IP software library.

Solorigate: it identifies vulnerabilities, especially those related to SolarWinds Solorigate.

2020 Threat Landscape Retrospective (TLR) scan: report that identifies trends in vulnerabilities, ransomware, and others during COVID-19 pandemic.

ProxyLogon: MS Exchange scan: analyzes if an exchange server is vulnerable to the ProxyLogon exploit.

Host Discovery scan: it identifies active hosts on a network and provides information about these hosts.

Audit Cloud Infrastructure scan: it analyzes cloud environments.

Internal PCI Network scan: it identifies and helps organizations to organize vulnerabilities related to PCI DSS compliance requirements.

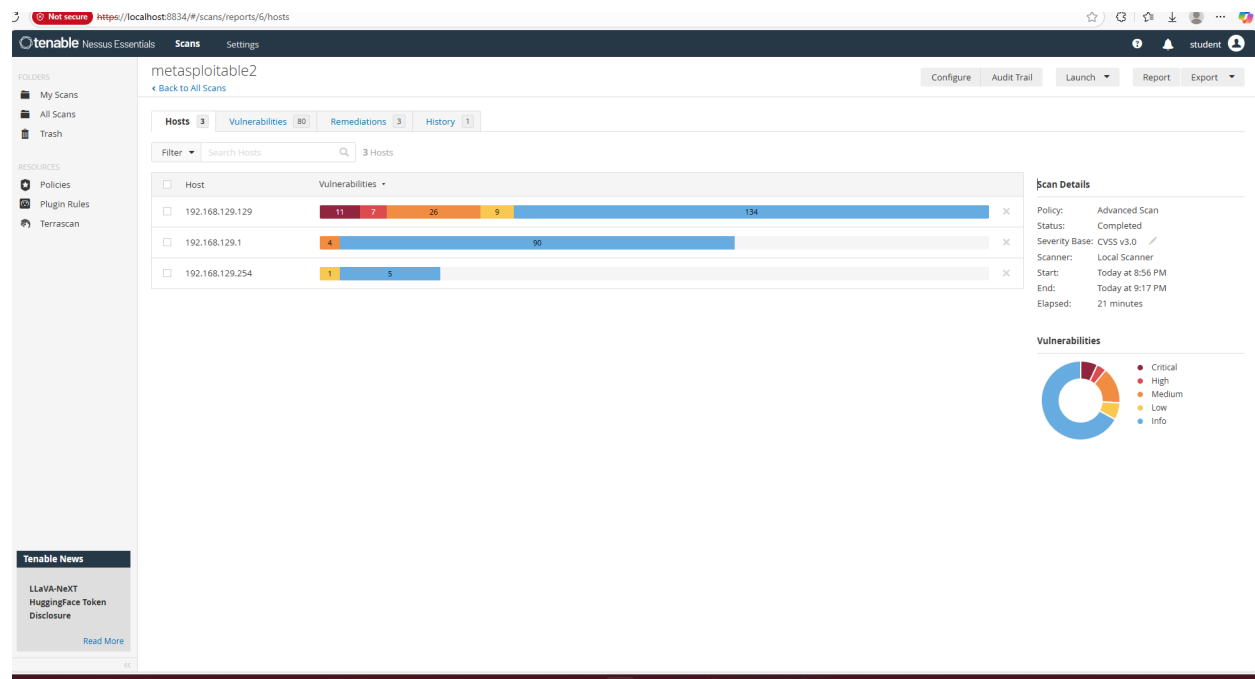
MDM Config Audit scan: detection and resolution of security configurations of MDM.

Offline Config Audit scan: it helps with the configuration of a system without internet connection.

PCI Quarterly External scan: it is designed to assess and fulfil the requirements of the Payment Card Industry Data Security Standard (PCI DSS).

SCAP and OVAL Auditing scan: SCAP automates security policies and vulnerability management. OVAL is a language used in SCAP to know system states and vulnerabilities.

## Scan MetaSploitable2:



As we can see in this screenshot, this is how the main dashboard looks with the scanning of MetaSploitable2. IP: 192.168.129.129

tenable Nessus Essentials Scans Settings

metasploitable2 / 192.168.129.129

Configure Audit Trail Launch Report Export

Vulnerabilities 72

Filter Search Vulnerabilities 72 Vulnerabilities

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.7216	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			Canonical Ubuntu Linux SEOL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5 *	6.7	0.4664	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	0.4664	rsh Service Detection	Service detection	1
HIGH	7.5	5.9	0.7992	Samba Badlock Vulnerability	General	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5			Unencrypted Telnet Server	Misc.	1

Host: 192.168.129.129

Host Details

IP: 192.168.129.129  
MAC: 00:0C:29:63:3E:2E  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 8:57 PM  
End: Today at 9:17 PM  
Elapsed: 20 minutes  
KB: [Download](#)

Vulnerabilities

● Critical  
● High  
● Medium  
● Low  
● Info

This second picture shows us in a little bit of detail the vulnerability scan.

tenable Nessus Essentials Scans Settings

metasploitable2 / Plugin #46882

Configure Audit Trail Launch Report Export

Vulnerabilities 72

CRITICAL UnrealIRCd Backdoor Detection

Description

The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also

<https://seclists.org/fulldisclosure/2010/jun/277>  
<https://seclists.org/fulldisclosure/2010/jun/284>  
[http://www.unrealircd.com/text/unrealsecadvisory\\_20100612.txt](http://www.unrealircd.com/text/unrealsecadvisory_20100612.txt)

Output

```
The remote IRC server is running as :
uid=0 (root) gid=0 (root)

To see debug logs, please visit individual host
```

Port	Hosts
6667 / tcp / irc	192.168.129.129

Plugin Details

Severity: Critical  
ID: 46882  
Version: 1.16  
Type: remote  
Family: Backdoors  
Published: June 14, 2010  
Modified: April 11, 2022

VPR Key Drivers

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Functional  
Age of Vuln: 730 days +  
Product Coverage: Low  
CVSSv3 Impact Score: 5.9  
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 7.4  
Exploit Prediction Scoring System (EPSS): 0.7216  
Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Temporal Score: 8.3  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C  
CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

As we can see it is telling us that there is software that has an open backdoor that can allow a hacker to execute arbitrary code. The solution would be to re-download and re-install the software.

**metasploitable2 / Plugin #201352**

**Vulnerabilities 72**

**CRITICAL Canonical Ubuntu Linux SEoL (8.04.x)**

**Description**  
According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.  
  
Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

**Solution**  
Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

**See Also**  
<http://www.nessus.org/u73bcb2d2e>

**Output**

```
OS : Ubuntu Linux 8.04
Security End of Life : May 8, 2013
Time since Security End of Life (Est.) : >= 12 years
```

To see debug logs, please visit individual host

Port	Hosts
80 / tcp / www	192.168.129.129

**Plugin Details**

Severity: Critical  
ID: 201352  
Version: 1.2  
Type: combined  
Family: General  
Published: July 3, 2024  
Modified: March 26, 2025

**Risk Information**

Risk Factor: Critical  
**CVSS v3.0 Base Score: 10.0**  
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

CPE: cpe:/o:canonical:ubuntu\_linux  
Unsupported by vendor: true

As we can see, the Canonical Ubuntu Linux version is not upgraded, so we no longer have the new security patches because this version is not maintained by the vendor. The solution will be to upgrade to a version that is currently supported.

**metasploitable2 / Plugin #61708**

**Vulnerabilities 72**

**CRITICAL VNC Server 'password' Password**

**Description**  
The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

**Solution**  
Secure the VNC service with a strong password.

**Output**

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port	Hosts
5900 / tcp / vnc	192.168.129.129

**Plugin Details**

Severity: Critical  
ID: 61708  
Version: \$Revision: 1.2 \$  
Type: remote  
Family: Gain a shell remotely  
Published: August 29, 2012  
Modified: September 24, 2015

**Risk Information**

Risk Factor: Critical  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

Default Account: true  
Exploited by Nessus: true

The VNC Server has a password of password which is weak, a hacker could exploit this vulnerability and take over the system. The solution is to set a stronger password.

**metasploit2 / Plugin #20007**

[Back to Vulnerabilities](#)

**Vulnerabilities 72**

**CRITICAL 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 1.2 (with approved cipher suites) or higher instead.

**See Also**  
<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>  
<http://www.nessus.org/u7b08c7e95>  
<http://www.nessus.org/u247c4540>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.nessus.org/u75d15ba70>  
<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://tools.ietf.org/html/rfc7507>  
<https://tools.ietf.org/html/rfc7568>

**Output**

**Plugin Details**

Severity: Critical  
ID: 20007  
Version: 1.34  
Type: remote  
Family: Service detection  
Published: October 12, 2005  
Modified: April 4, 2022

**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/C:H/I:H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Vulnerability Information**

In the news: true

**Tenable News**

Gerriscary: Hacking the Supply Chain of Popular Go...

Use of SSL Version 2 and 3 Protocol which is no longer considered secure. The solution is to disable these versions and use TLS 1.2.

**metasploit2 / Plugin #51988**

[Back to Vulnerabilities](#)

**Vulnerabilities 72**

**CRITICAL Bind Shell Backdoor Detection**

**Description**  
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

**Solution**  
Verify if the remote host has been compromised, and reinstall the system if necessary.

**Output**

Nessus was able to execute the command "id" using the following request :

```
----- snip -----
This produced the following truncated output (limited to 10 lines) :
root@metasploit2:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploit2:/#
----- snip -----
```

To see debug logs, please visit individual host

Port	Hosts
1524 / tcp / wild_shell	192.168.129.129

**Plugin Details**

Severity: Critical  
ID: 51988  
Version: 1.10  
Type: remote  
Family: Backdoors  
Published: February 15, 2011  
Modified: April 11, 2022

**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/C:H/I:H/A:H  
CVSS v2.0 Base Score: 10.0  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

**Tenable News**

Anthropic MCP Inspector Remote Code Execution

A shell is open on a remote port without authentication; an attacker can use this and send commands. Verify if the host hasn't been compromised and reinstall the system.

**metasploit2 / Plugin #10205**

**Vulnerabilities 72**

**HIGH rlogin Service Detection**

**Description**  
The rlogin service is running on the remote host. This service is vulnerable since data is passed between the rlogin client and server in cleartext. A man-in-the-middle attacker can exploit this to sniff logins and passwords. Also, it may allow poorly authenticated logins without passwords. If the host is vulnerable to TCP sequence number guessing (from any network) or IP spoofing (including ARP hijacking on a local network) then it may be possible to bypass authentication. Finally, rlogin is an easy way to turn file-write access into full logins through the .rhosts or rhosts.equiv files.

**Solution**  
Comment out the 'login' line in /etc/inetd.conf and restart the inetd process. Alternatively, disable this service and use SSH instead.

**Output**  
No output recorded.  
To see debug logs, please visit individual host

Port	Hosts
513/tcp/rlogin	192.168.129.129

**Plugin Details**

Severity: High  
ID: 10205  
Version: 1.36  
Type: remote  
Family: Service detection  
Published: August 30, 1999  
Modified: April 11, 2022

**VPR Key Drivers**

Threat Recency: No recorded events  
Threat Intensity: Very Low  
Exploit Code Maturity: Unproven  
Age of Vuln: 730 days  
Product Coverage: Low  
CVSSV3 Impact Score: 5.9  
Threat Sources: No recorded events

**Risk Information**

Vulnerability Priority Rating (VPR): 6.7  
Exploit Prediction Scoring System (EPSS): 0.4664  
Risk Factor: High  
CVSS v2.0 Base Score: 7.5  
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/AU:N/C:P/I:P/A:P

**Vulnerability Information**

Exploit Available: true  
Exploit Ease: Exploits are available

We can see that the rlogin service is functioning in a remote host and data running between client and server can be exploited by a hacker. It also might be possible to login to the system without a password. The solution is to run the command "login" and restart the process .