

Week 5 Lab Guide: Vulnerability Assessment and Validation

Zaitsev Igor

CS 2303

1. Unauthenticated Scan

First step – launching kali linux, and selecting a target to test

Since this is a lab image from Cisco, several vulnerable machines are pre-installed in the container:

```
(kali@kali) ~$ docker ps
```

CONTAINER ID	IMAGE	COMMAND	NAMES	CREATED	STATUS	PORTS
66861c2d6d80	cyberacademylabs/metasploitable2	"/bin/bash -c 'service-"	metasploitable2	2 years ago	Up 3 hours	
c36546e4c1a	santosomar/dwaa	"/main.sh"	dwaa.pc	2 years ago	Up 3 hours	
159b75f834a4	santosomar/mutillidae_2	"/run.sh"	mutillidae.pc	2 years ago	Up 3 hours	
dc1e5ab5f1f3	santosomar/webgoat	"/bin/sh -c 'bin/ba-"	webgoat.pc	2 years ago	Up 3 hours	
29f28a8c96b	santosomar/gravemind	"/bin/sh -c /root/st-"	gravemind.pc	2 years ago	Up 3 hours (healthy)	
2959d31388c3	santosomar/juice-shop	"docker-entrypoint.s-"	juice-shop.pc	2 years ago	Up 3 hours	
76adf3986998	santosomar/dwaa	"/main.sh"	dwaa.pc	2 years ago	Up 3 hours	
f268ea787b32	santosomar/dwaa	"/main.sh"	dwaa.pc	2 years ago	Up 3 hours	
ecda332b4b1	cyberacademylabs/metasploitable2	"/bin/bash -c 'service-"	metasploitable2	2 years ago	Up 3 hours	21-23/tcp, 25/tcp, 80/tcp, 111/tcp, 139/tcp, 443/tcp, 512-514/tcp, 1099/tcp, 1524/tcp, 2121/tcp, 3386/tcp, 3632/tcp, 5432/tcp
p. 5900/tcp, 6000/tcp, 6667/tcp, 8080/tcp, 8180/tcp						
8b701e0e6bda	santosomar/webgoat	"/bin/sh -c 'bin/ba-"	webgoat.pc	2 years ago	Up 3 hours	
7681d5f090af	santosomar/mutillidae_2	"/run.sh"	mutillidae.pc	2 years ago	Up 3 hours	
189d2d3898ff	santosomar/juice-shop	"docker-entrypoint.s-"	juice-shop.pc	2 years ago	Up 3 hours	
cf8a0cfcd32c	santosomar/gravemind	"/bin/sh -c /root/st-"	gravemind.pc	2 years ago	Up 3 hours (healthy)	

I chose the container that is most suitable for our purposes – Metasploitable.

Let's check the connection with the container:

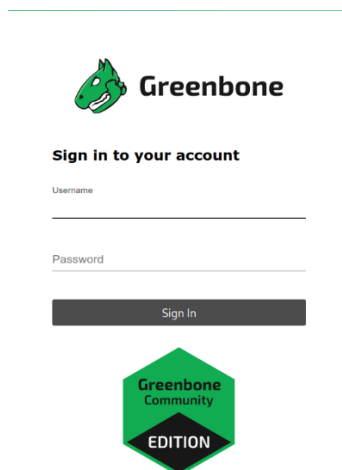
```
(kali@kali) ~$ ping -c 4 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.056 ms
64 bytes from 172.17.0.2: icmp_seq=2 ttl=64 time=0.221 ms
64 bytes from 172.17.0.2: icmp_seq=3 ttl=64 time=0.721 ms
64 bytes from 172.17.0.2: icmp_seq=4 ttl=64 time=0.043 ms

— 172.17.0.2 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3159ms
rtt min/avg/max/mdev = 0.043/0.260/0.721/0.275 ms

(kali@kali) ~$
```

2. Unauthenticated Scan

After launching GreenBone, we log in to the default account and begin scanning our vulnerable machine.



We add the IP address of our target in the appropriate field, and select Full and Fast in Scan Config:

New Target

Name

metasploitable

Comment

Hosts

☒ Manual

172.17.0.2

☐ From file

Browse...

No file selected.

Exclude Hosts

☒ Manual

☐ From file

Browse...

No file selected.

Allow simultaneous scanning via multiple IPs

☒ Yes

☐ No

Port List

All IANA assigned TCP

Alive Test

Scan Config Default

New Task

Name

meta scan

Comment

Scan Targets

metasploitable

Alerts

Schedule

--

☐ Once

Add results to Assets

☒ Yes

☐ No

Apply Overrides

☒ Yes

☐ No

Min QoD

70

%

Alterable Task

☐ Yes

☒ No

Auto Delete Reports

☒ Do not automatically delete reports

☐ Automatically delete oldest reports but always keep newest

5

reports

Scanner

OpenVAS Default

Scan Config

Full and fast

Cancel

Save

Greenbone Security Assistant

Dashboards

Scans

Assets

Resilience

SecInfo

Configuration

Administration

Help

Name

meta scan

Status

Requested

Reports

1

Last Report

Severity

Trend

Actions

Target

metasploitable

Scanner

Name

OpenVAS Default

Type

OpenVAS Scanner

Scan Config

Full and fast

Order for target hosts

sequential

Maximum concurrently executed NVTs per host

4

Maximum concurrently scanned hosts

20

The screenshot displays the Greenbone Security Assistant interface. At the top, there is a navigation bar with tabs for Dashboards, Scans, Assets, Resilience, SecInfo, Configuration, Administration, and Help. Below the navigation bar, there is a search bar and a filter dropdown. The main content area shows three charts:

- Tasks by Severity Class (Total: 1):** A 3D pie chart showing a single red slice representing 'High' severity. The value '1' is displayed on the slice.
- Tasks with most High Results per Host:** A horizontal bar chart showing a single red bar for 'meta scan' with a value of 20 on the 'Results per Host' axis.
- Tasks by Status (Total: 1):** A 3D pie chart showing a single blue slice representing 'Done'. The value '1' is displayed on the slice.

Vulnerability	Severity	QoD	Host IP	Name	Location	Created
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	<div><div></div><div>10.0 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	8787/tcp	Sat, Oct 11, 2025 12:25 PM UTC
Twiki XSS and Command Execution Vulnerabilities	<div><div></div><div>10.0 (High)</div></div>	80 %	172.17.0.2	metasploitable-vm	80/tcp	Sat, Oct 11, 2025 12:57 PM UTC
Operating System (OS) End of Life (EOL) Detection	<div><div></div><div>10.0 (High)</div></div>	80 %	172.17.0.2	metasploitable-vm	general/tcp	Sat, Oct 11, 2025 12:55 PM UTC
Possible Backdoor: Ingreslock	<div><div></div><div>10.0 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	1524/tcp	Sat, Oct 11, 2025 1:01 PM UTC
The resxw service is running	<div><div></div><div>10.0 (High)</div></div>	80 %	172.17.0.2	metasploitable-vm	512/tcp	Sat, Oct 11, 2025 12:56 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	<div><div></div><div>9.8 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	8009/tcp	Sat, Oct 11, 2025 1:03 PM UTC
DirCC RCE Vulnerability (CVE-2004-2687)	<div><div></div><div>9.8 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	3632/tcp	Sat, Oct 11, 2025 12:59 PM UTC
PostgreSQL Default Credentials (PostgreSQL Protocol)	<div><div></div><div>9.0 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	5432/tcp	Sat, Oct 11, 2025 12:59 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	<div><div></div><div>8.1 (High)</div></div>	80 %	172.17.0.2	metasploitable-vm	6697/tcp	Sat, Oct 11, 2025 12:51 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	<div><div></div><div>7.8 (High)</div></div>	95 %	172.17.0.2	metasploitable-vm	3306/tcp	Sat, Oct 11, 2025 12:59 PM UTC
FTP Brute Force Logins Reporting	<div><div></div><div>7.5 (High)</div></div>	95 %	172.17.0.2	metasploitable-vm	2121/tcp	Sat, Oct 11, 2025 12:59 PM UTC
PHP-CGI-based setups Vulnerability when parsing query string parameters from php files.	<div><div></div><div>7.5 (High)</div></div>	95 %	172.17.0.2	metasploitable-vm	80/tcp	Sat, Oct 11, 2025 1:06 PM UTC
phpinfo() output Reporting	<div><div></div><div>7.5 (High)</div></div>	80 %	172.17.0.2	metasploitable-vm	80/tcp	Sat, Oct 11, 2025 12:57 PM UTC
FTP Brute Force Logins Reporting	<div><div></div><div>7.5 (High)</div></div>	95 %	172.17.0.2	metasploitable-vm	21/tcp	Sat, Oct 11, 2025 12:59 PM UTC
Test HTTP dangerous methods	<div><div></div><div>7.5 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	80/tcp	Sat, Oct 11, 2025 1:09 PM UTC
The rlogin service is running	<div><div></div><div>7.8 (High)</div></div>	80 %	172.17.0.2	metasploitable-vm	513/tcp	Sat, Oct 11, 2025 12:56 PM UTC
rsync Unencrypted Cleartext Login	<div><div></div><div>7.8 (High)</div></div>	80 %	172.17.0.2	metasploitable-vm	514/tcp	Sat, Oct 11, 2025 12:56 PM UTC
UnrealIRCd Backdoor	<div><div></div><div>7.8 (High)</div></div>	70 %	172.17.0.2	metasploitable-vm	6697/tcp	Sat, Oct 11, 2025 12:59 PM UTC
vstpd Compromised Source Packages Backdoor Vulnerability	<div><div></div><div>7.8 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	6200/tcp	Sat, Oct 11, 2025 12:59 PM UTC
vstpd Compromised Source Packages Backdoor Vulnerability	<div><div></div><div>7.5 (High)</div></div>	99 %	172.17.0.2	metasploitable-vm	21/tcp	Sat, Oct 11, 2025 12:59 PM UTC

	ReportSat, Oct 11, 2025 12:35 PM UTC	Date	ID: 379df080-4f70-4400-8526-e6b4203261a6	Created: Sat, Oct 11, 2025 12:35 PM UTC	Modified: Sat, Oct 11, 2025 1:10 PM UTC	Owner: admin					
Information	Results (65 of 545)	Hosts (1 of 1)	Ports (18 of 21)	Applications (14 of 14)	Operating Systems (1 of 1)	CVEs (33 of 33)	Closed CVEs (0 of 0)	TLS Certificates (2 of 2)	Error Messages (0 of 0)	User Tags (0)	
CVE						NVT				Hosts Occurrences Severity ▼	
CVE-2008-5304 CVE-2008-5305						TWiki XSS and Command Execution Vulnerabilities				1	1 10.0 (High)
CVE-1999-0618						The rexec service is running				1	1 10.0 (High)
CVE-2020-1938						Apache Tomcat AJP RCE Vulnerability (Gh0stcat)				1	1 9.8 (High)
CVE-2004-2687						DistCC RCE Vulnerability (CVE-2004-2687)				1	1 9.3 (High)
CVE-2016-7144						UnrealIRCd Authentication Spoofing Vulnerability				1	1 8.3 (High)
CVE-2001-0645 CVE-2004-2357 CVE-2006-1451 CVE-2007-2554 CVE-2007-6081 CVE-2009-0919 CVE-2014-3419 CVE-2015-4669						MySQL / MariaDB Default Credentials (MySQL Protocol)				1	1 7.8 (High)
CVE-2016-6531 CVE-2018-15719											
CVE-1999-0501 CVE-1999-0502 CVE-1999-0507 CVE-1999-0508 CVE-2001-1594 CVE-2013-7404 CVE-2018-19063 CVE-2018-19064						FTP Brute Force Logins Reporting				1	2 7.5 (High)
CVE-2012-1823 CVE-2012-2311 CVE-2012-2336 CVE-2012-2335						PHP-CGI-based setups vulnerability when parsing query string parameters from php...				1	1 7.5 (High)
CVE-1999-0651						The rlogin service is running				1	1 7.5 (High)
CVE-1999-0651						rsh Unencrypted Cleartext Login				1	1 7.5 (High)
CVE-2010-2075						UnrealIRCd Backdoor				1	1 7.5 (High)
CVE-2014-0224						SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability				1	1 7.4 (High)
CVE-2011-0411 CVE-2011-1430 CVE-2011-1431 CVE-2011-1432 CVE-2011-1506 CVE-2011-1575 CVE-2011-1926 CVE-2011-2165											

Scan Report

October 11, 2025

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "meta scan". The scan started at Sat Oct 11 12:35:44 2025 UTC and ended at Sat Oct 11 13:10:25 2025 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

Contents

1	Result Overview	2
1.1	Host Authentications	2
2	Results per Host	2
2.1	172.17.0.2	2
2.1.1	High 6697/tcp	3
2.1.2	High 2121/tcp	5
2.1.3	High 80/tcp	6
2.1.4	High 8787/tcp	10
2.1.5	High 6200/tcp	12
2.1.6	High general/tcp	12
2.1.7	High 512/tcp	13
2.1.8	High 8009/tcp	14
2.1.9	High 5432/tcp	20
2.1.10	High 514/tcp	23

3. Authenticated Scan

To perform an authorized scan, you must enter the default credentials for ssh from metasploitable:

The screenshot shows a 'New Credential' dialog box. The 'Name' field is filled with 'msfcred'. The 'Comment' field is empty. The 'Type' dropdown is set to 'Username + Password'. The 'Allow insecure use' section has 'No' selected. The 'Auto-generate' section has 'No' selected. The 'Username' field is filled with 'msfadmin'. The 'Password' field is masked with dots. The 'Cancel' button is on the bottom left and the 'Save' button is on the bottom right.

We do the same as in the previous steps, only we include the added credentials in the target indication

New Target



Name MetasploitableAuth

Comment

Hosts ☒ Manual 172.17.0.2
☐ From file Browse... No file selected.

Exclude Hosts ☒ Manual
☐ From file Browse... No file selected.

Allow simultaneous scanning via multiple IPs ☒ Yes ☐ No

Port List All IANA assigned TCP ▼ *

Alive Test Scan Config Default ▼

Credentials for authenticated checks

SSH msfcred ▼ on port 22 *

Cancel

Save

New Task



Name AuthMetasplTask

Comment

Scan Targets MetasploitableAuth ▼ *

Alerts ▼ *

Schedule -- ▼ ☐ Once *Add results to Assets ☒ Yes ☐ NoApply Overrides ☒ Yes ☐ No

Min QoD 70 %

Alterable Task ☐ Yes ☒ No

Auto Delete Reports ☒ Do not automatically delete reports
☐ Automatically delete oldest reports but always keep newest 5 reports

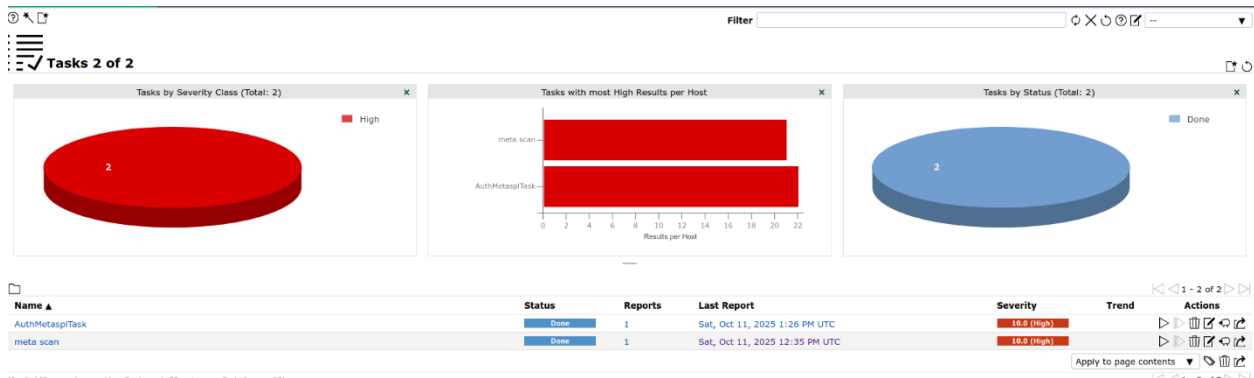
Scanner OpenVAS Default ▼

Scan Config Full and fast ▲

Cancel

Save

Results after authorized scan:



And some report details:

2.1.1 High 6697/tcp

High (CVSS: 8.1) NVT: UnrealIRCd Authentication Spoofing Vulnerability
<p>Product detection result</p> <p>cpe:/a:unrealircd:unrealircd:3.2.8.1 Detected by UnrealIRCd Detection (OID: 1.3.6.1.4.1.25623.1.0.809884)</p>
<p>Summary</p> <p>UnrealIRCd is prone to authentication spoofing vulnerability.</p>
<p>Vulnerability Detection Result</p> <p>Installed version: 3.2.8.1 Fixed version: 3.2.10.7</p>
<p>Impact</p> <p>Successful exploitation of this vulnerability will allows remote attackers to spoof certificate fingerprints and consequently log in as another user.</p>
<p>Solution:</p> <p>Solution type: VendorFix Upgrade to UnrealIRCd 3.2.10.7, or 4.0.6, or later.</p>
...continues on next page ...

... continued from previous page ...
Affected Software/OS UnrealIRCd before 3.2.10.7 and 4.x before 4.0.6.
Vulnerability Insight The flaw exists due to an error in the 'm_authenticate' function in 'modules/m_sasl.c' script.
Vulnerability Detection Method Checks if a vulnerable version is present on the target host. Details: UnrealIRCd Authentication Spoofing Vulnerability OID:1.3.6.1.4.1.25623.1.0.809883 Version used: 2023-07-14T16:09:27Z
Product Detection Result Product: cpe:/a:unrealircd:unrealircd:3.2.8.1 Method: UnrealIRCd Detection OID: 1.3.6.1.4.1.25623.1.0.809884)
References cve: CVE-2016-7144 url: http://seclists.org/oss-sec/2016/q3/420 url: http://www.securityfocus.com/bid/92763 url: http://www.openwall.com/lists/oss-security/2016/09/05/8 url: https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b5c50ba1a34a766 url: https://bugs.unrealircd.org/main_page.php

The short list of findings:

Vulnerabilities have been discovered that require access to the system - Backdoor Ingreslock (port 1524), which responds to id commands and returns uid=0(root) gid=0(root)

Weak/standard credentials of internal services have been identified - successful login to PostgreSQL with a postgres/postgres login and to MySQL with an empty password for root

Insecure system services have been detected - rsh, rlogin, and rexec services running with or without insecure authentication.

Problems with the SSL/TLS configuration have been identified - outdated protocols (SSLv2/SSLv3), weak ciphers and expired certificates on ports 25 and 5432

Vulnerabilities of web applications requiring access have been discovered - problems in TWiki (XSS, CSRF, command execution) and phpMyAdmin (XSS)

Insecure authentication methods have been identified - FTP, which allows anonymous login and transmission of credentials in clear text

Problems with SSH settings have been detected - weak encryption, key exchange, and authentication algorithms.

4. Validate One HighSeverity Finding

Now, let's try to validate Backdoor Ingreslock (port 1524) vulnerability with Nmap:

```
(root@Kali)-[~]
# nmap --script vuln -p1524 172.17.0.2
Starting Nmap 7.94 ( https://nmap.org ) at 2025-10-11 14:42 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000042s latency).

PORT      STATE SERVICE
1524/tcp  open  ingreslock
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 10.40 seconds
```

1524/tcp open bindshell Metasploitable root shell - This is the Ingreslock backdoor, which provides a root shell without authentication.

An authenticated scan reveals more vulnerabilities because it has direct access to the system through credentials, which allows you to analyze configurations, installed patches, registry settings, and local services that are unavailable during external scanning. It provides a more accurate assessment by checking the actual security settings rather than making assumptions based on network responses.

To minimize false positives, it is necessary to apply multi-level verification: reproduce vulnerabilities using tools like Metasploit, perform cross-validation with different scanners, analyze system logs and take into account the context of the environment. Manual confirmation of critical findings and maintaining a database of false positives make it possible to continuously improve the accuracy of scans.

To eliminate a high-criticality vulnerability, first of all, it is necessary to isolate vulnerable systems at the network level and install patches immediately. Then you should disable insecure services, change all standard credentials, and implement monitoring to promptly detect similar incidents in the future.

Finding ID / Name	Tool Used	Command / Method	Observation / Evidence	Result / Output Summary	Verdict
Backdoor: Ingreslock	OpenVAS (GB)	Authenticated service interrogation	Service responds to id; command with root privileges	Remote command execution confirmed on port 1524	Confirmed
PostgreSQL Default Credentials	OpenVAS (GB)	Database login testing	Successful login as postgres/postgres	Unauthorized database access via weak credentials	Confirmed
MySQL Empty Root Password	OpenVAS (GB)	Database authentication test	Root login with empty password	Complete database compromise possible	Confirmed