

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:

CONTAINER ID	IMAGE	COMMAND	NAMES	CREATED	STATUS	PORTS
66861c1c2d0d80	cyberacademylabs/metasploitable2	"bin/bash ./service."	metasploitable2	2 years ago	Up 3 hours	
c30546ee4c1a	santosomar/dwva	"main.sh"	dwva.pc	2 years ago	Up 3 hours	
159b7f034a4	santosomar/mutillidae_2	"run.sh"	mutillidae.pc	2 years ago	Up 3 hours	
dc1e65abf1f3	santosomar/webgoat	"bin/sh -c '/bin/ba..."	webgoat.pc	2 years ago	Up 3 hours	
29f20ae8c96b	santosomar/gravemind	"bin/sh -c '/root/st..."	gravemind.pc	2 years ago	Up 3 hours (healthy)	
2959d3128c3	santosomar/juice-shop	"docker-entrypoint.s..."	juice-shop.pc	2 years ago	Up 3 hours	
76adf3986998	santosomar/dwva	"main.sh"	dwva.vm	2 years ago	Up 3 hours	
f260ea787b32	santosomar/dwva	"main.sh"	dwva.vm	2 years ago	Up 3 hours	
ecdd3a32bb4b	cyberacademylabs/metasploitable2	"bin/bash ./service."	metasploitable.vm	2 years ago	Up 3 hours	21-23/tcp, 25/tcp, 80/tcp, 111/tcp, 139/tcp, 445/tcp, 512-514/tcp, 1099/tcp, 1521/tcp, 2121/tcp, 3306/tcp, 3632/tcp, 5432/tcp
db701e66bd3	santosomar/webgoat	"bin/sh -c '/bin/ba..."	webgoat.vm	2 years ago	Up 3 hours	
7601df090af	santosomar/mutillidae_2	"run.sh"	mutillidae.vm	2 years ago	Up 3 hours	
18902d23898ff	santosomar/juice-shop	"docker-entrypoint.s..."	juice-shop.vm	2 years ago	Up 3 hours	
cfbfa0cf032c	santosomar/gravemind	"bin/sh -c '/root/st..."	gravemind.vm	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.



[Sign in to your account](#)

Username

Password

Sign In



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

New Target

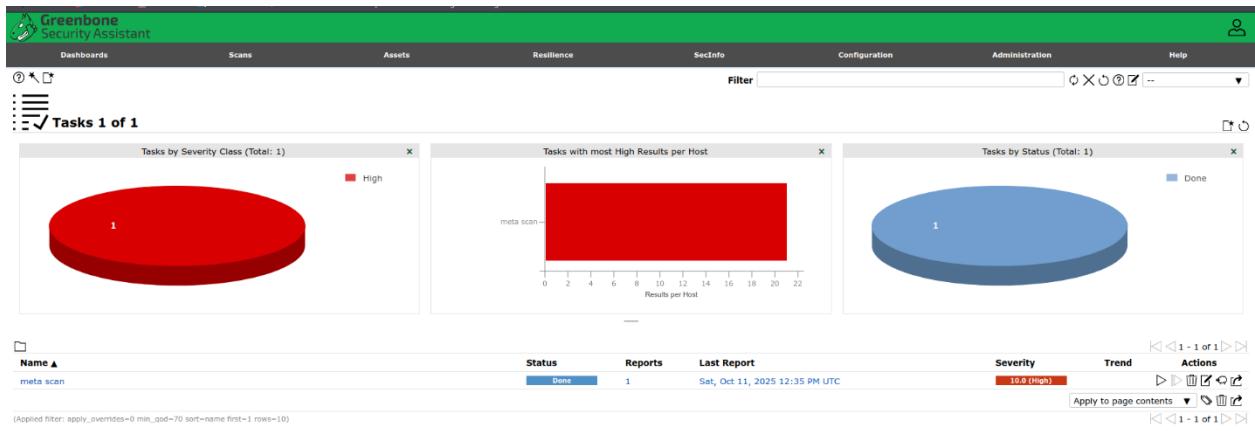
Name	metasploitable
Comment	
Hosts	<input checked="" type="radio"/> Manual <input type="text" value="172.17.0.2"/> <input type="radio"/> From file <input type="button" value="Browse..."/> No file selected.
Exclude Hosts	<input checked="" type="radio"/> Manual <input type="text"/> <input type="radio"/> From file <input type="button" value="Browse..."/> No file selected.
Allow simultaneous scanning via multiple IPs	<input checked="" type="radio"/> Yes <input type="radio"/> No
Port List	<input style="border: none; padding: 0; margin-right: 10px;" type="button" value="All IANA assigned TCP"/> <input style="border: none; padding: 0;" type="button" value="Scan Config Default"/>
Alive Test	<input style="border: none; padding: 0;" type="button" value="Scan Config Default"/>

New Task

Name	meta scan
Comment	
Scan Targets	<input style="border: none; padding: 0; margin-right: 10px;" type="button" value="metasploitable"/> <input style="border: none; padding: 0;" type="button" value="Scan Targets"/>
Alerts	<input style="border: none; padding: 0; margin-right: 10px;" type="button" value="Scan Targets"/> <input style="border: none; padding: 0;" type="button" value="Alerts"/>
Schedule	<input style="border: none; padding: 0; margin-right: 10px;" type="button" value="--"/> <input type="checkbox"/> Once <input style="border: none; padding: 0;" type="button" value="Scan Targets"/>
Add results to Assets	<input checked="" type="radio"/> Yes <input type="radio"/> No
Apply Overrides	<input checked="" type="radio"/> Yes <input type="radio"/> No
Min QoD	<input type="text" value="70"/> <input style="border: none; padding: 0; margin-left: 10px;" type="button" value="Min QoD"/>
Alterable Task	<input type="radio"/> Yes <input checked="" type="radio"/> No
Auto Delete Reports	<input checked="" type="radio"/> Do not automatically delete reports
	<input type="radio"/> Automatically delete oldest reports but always keep newest <input type="text" value="5"/> <input style="border: none; padding: 0; margin-left: 10px;" type="button" value="Scan Targets"/>
Scanner	<input style="border: none; padding: 0; margin-right: 10px;" type="button" value="OpenVAS Default"/> <input style="border: none; padding: 0;" type="button" value="Scanner"/>
Scan Config	<input style="border: none; padding: 0; margin-right: 10px;" type="button" value="Full and fast"/> <input style="border: none; padding: 0;" type="button" value="Scan Config"/>
<input style="border: 1px solid green; background-color: #2e6b2e; color: white; padding: 5px; margin-right: 20px;" type="button" value="Cancel"/> <input style="border: 1px solid green; background-color: #2e6b2e; color: white; padding: 5px;" type="button" value="Save"/>	

Greenbone Security Assistant		Dashboard	Scans	Assets	Resilience	SecInfo	Configuration	Administration	Help
<input type="checkbox"/>	Name	meta scan			Status	Requested	Reports	Last Report	Severity
<input type="checkbox"/>	Target	metasploitable				1			Trend
<input type="checkbox"/>	Scanner								Actions
	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							

After the scan is complete, we view the results and export the report in various formats.



Vulnerability	Severity	QoD	Host	Name	Location	Created
Distributed Ruby (dRuby/DRb) Multiple Remote Code Execution Vulnerabilities	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	8787/tcp	Sat, Oct 11, 2025 12:59 PM UTC
TWiki XSS and Command Execution Vulnerabilities	10.0 (High)	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	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	general/tcp	Sat, Oct 11, 2025 12:55 PM UTC
Possible Backdoor: Ingreslock	10.0 (High)	99 %	172.17.0.2	metasploitable.vm	1524/tcp	Sat, Oct 11, 2025 1:01 PM UTC
The rexec service is running	10.0 (High)	80 %	172.17.0.2	metasploitable.vm	512/tcp	Sat, Oct 11, 2025 12:56 PM UTC
Apache Tomcat AJP RCE Vulnerability (Ghostcat)	9.8 (High)	99 %	172.17.0.2	metasploitable.vm	8009/tcp	Sat, Oct 11, 2025 1:03 PM UTC
DistCC RCE Vulnerability (CVE-2004-2687)	9.3 (High)	99 %	172.17.0.2	metasploitable.vm	3632/tcp	Sat, Oct 11, 2025 12:59 PM UTC
PostgreSQL Default Credentials (PostgreSQL, Protocol)	9.0 (High)	99 %	172.17.0.2	metasploitable.vm	5432/tcp	Sat, Oct 11, 2025 12:59 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	9.1 (High)	80 %	172.17.0.2	metasploitable.vm	6697/tcp	Sat, Oct 11, 2025 12:51 PM UTC
MySQL / MariaDB Default Credentials (MySQL Protocol)	7.8 (High)	95 %	172.17.0.2	metasploitable.vm	3306/tcp	Sat, Oct 11, 2025 12:50 PM UTC
FTP Brut Force Logins Reporting	7.5 (High)	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.	7.5 (High)	95 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Oct 11, 2025 1:06 PM UTC
phpinfo() output Reporting	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Oct 11, 2025 12:57 PM UTC
FTP Brut Force Logins Reporting	7.5 (High)	95 %	172.17.0.2	metasploitable.vm	21/tcp	Sat, Oct 11, 2025 12:59 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	172.17.0.2	metasploitable.vm	80/tcp	Sat, Oct 11, 2025 1:09 PM UTC
The rlogin service is running	7.3 (High)	80 %	172.17.0.2	metasploitable.vm	513/tcp	Sat, Oct 11, 2025 12:56 PM UTC
rsh Unencrypted Cleartext Login	7.5 (High)	80 %	172.17.0.2	metasploitable.vm	514/tcp	Sat, Oct 11, 2025 12:56 PM UTC
UnrealIRCd Backdoor	7.5 (High)	70 %	172.17.0.2	metasploitable.vm	6697/tcp	Sat, Oct 11, 2025 12:59 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.3 (High)	99 %	172.17.0.2	metasploitable.vm	6200/tcp	Sat, Oct 11, 2025 12:59 PM UTC
vsftpd Compromised Source Packages Backdoor Vulnerability	7.3 (High)	99 %	172.17.0.2	metasploitable.vm	21/tcp	Sat, Oct 11, 2025 12:59 PM UTC

Report: Sat, Oct 11, 2025 12:35 PM UTC										Done			
										ID: 379fd80-4ff0-44b0-8526-e6a42b3261a6	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													
CVE-2008-5304	CVE-2008-5305					NVT							
CVE-1999-0618						TWiki XSS and Command Execution Vulnerabilities					Hosts		
CVE-2020-1938						The rexec service is running					Occurrences		
CVE-2004-2687						Apache Tomcat AJP RCE Vulnerability (Ghostcat)					Severity ▾		
CVE-2016-7144						DistCC RCE Vulnerability (CVE-2004-2687)					10.0 (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				1		
CVE-2016-6531	CVE-2018-15719					UnrealIRCd Authentication Spoofing Vulnerability					10.0 (High)		
CVE-1999-0501	CVE-1999-0502	CVE-1999-0507	CVE-1999-0508	CVE-2001-1594	CVE-2013-7404	CVE-2018-19063	CVE-2018-19064				1		
CVE-2012-1823	CVE-2012-2311	CVE-2012-2336	CVE-2012-2335			MySQL / MariaDB Default Credentials (MySQL Protocol)					9.8 (High)		
CVE-1999-0651						FTP Brute Force Logins Reporting					8.5 (High)		
CVE-1999-0651						PHP-CGI-based script vulnerability when parsing query string parameters from php...					7.8 (High)		
CVE-2010-2075						The rlogin service is running					7.5 (High)		
CVE-2014-0224						rsh Unencrypted Cleartext Login					7.5 (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				7.5 (High)		
CVE-2009-4898						UnrealIRCd Backdoor					7.5 (High)		
CVE-2000-0007						SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability					7.4 (High)		
CVE-2011-0411						Multiple Vendors STARTTLS Implementation Plaintext Arbitrary Command Injection ...					7.0 (Medium)		
CVE-2011-0411						TWiki Cross-Site Request Forgery Vulnerability - Sep10					6.8 (Medium)		
CVE-2000-0007						Apache mod_ftp Local Disclosure					6.2 (Medium)		

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:

Name	msfcrcd
Comment	
Type	Username + Password ▼
Allow insecure use	<input type="radio"/> Yes <input checked="" type="radio"/> No
Auto-generate	<input type="radio"/> Yes <input checked="" type="radio"/> No
Username	msfadmin
Password	*****

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

New Task

Name: AuthMetasploitTask

Comment:

Scan Targets: MetasploitableAuth

Alerts:

Schedule: -- Once

Add results to Assets: Yes No

Apply Overrides: Yes No

Min QoD: 70

Alterable Task: Yes No

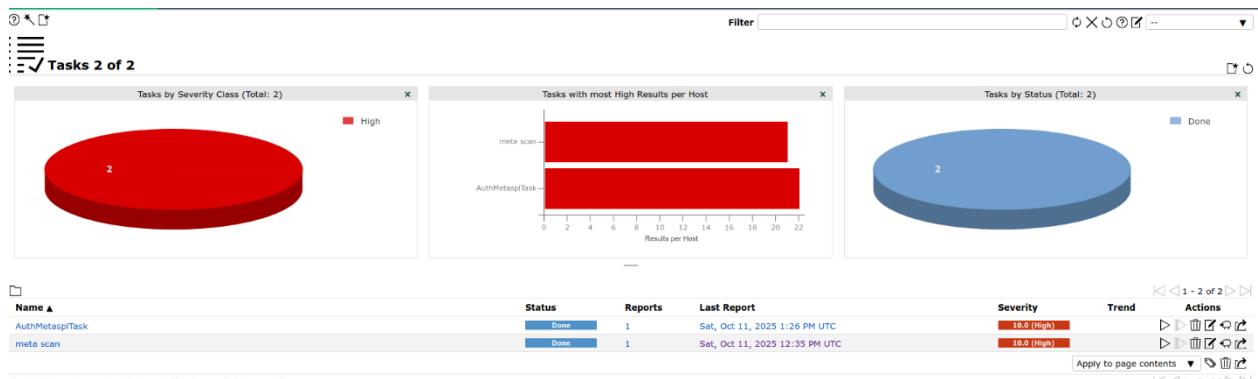
Auto Delete Reports:

- Do not automatically delete reports
- Automatically delete oldest reports but always keep newest: 5 reports

Scanner: OpenVAS Default

Scan Config: Full and fast
Base
Discovery

Results after authorized scan:



And some report details:

2.1.1 High 6697/tcp

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

... 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/f473e355e1dc422c4f019dbf86b
→c50ba1a34a766](https://github.com/unrealircd/unrealircd/commit/f473e355e1dc422c4f019dbf86b)

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	Confirmed on port 1524
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