Pentest Report – Metasploitable Corp

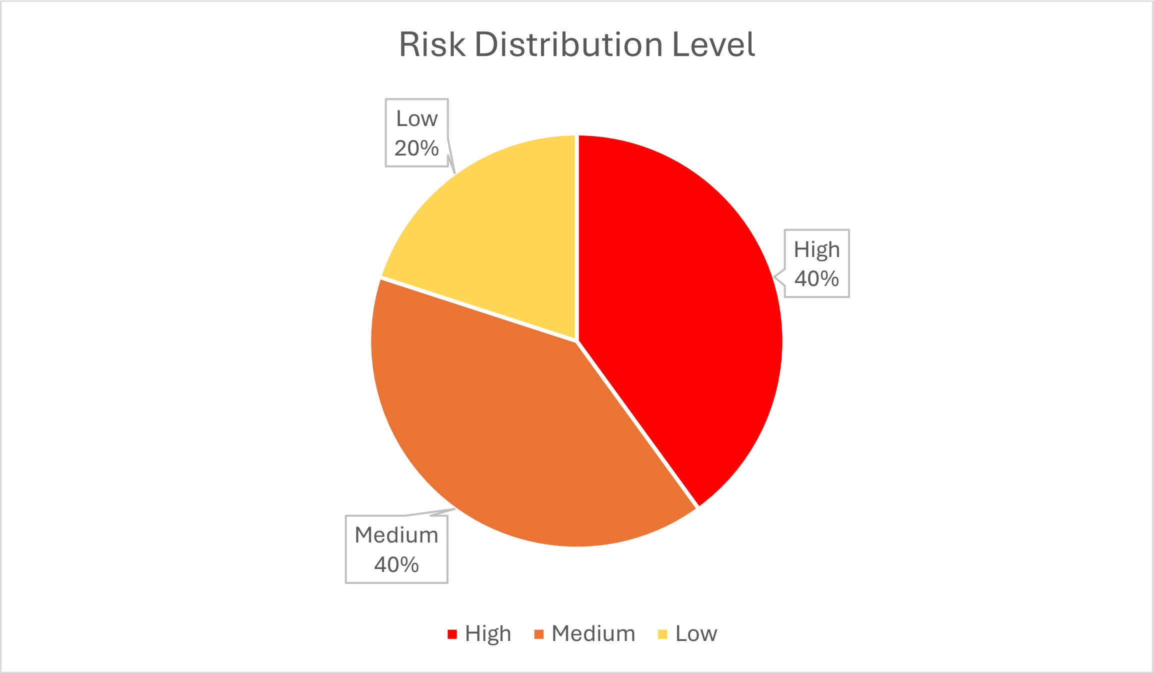
CONTENTS

1.0 EXECUTIVE SUMMARY

Infrastructure in Scope	Metasploitable
IP Address	192.168.1.46 (Self-hosted)

1.1 VULNERABILITIES

There was a total of 5 vulnerabilities, distributed as levels of risk: **2 vulnerabilities with High level risk, 2 vulnerabilities with medium level risk, and 1 vulnerability with Low level risk.** The risk level was estimated based on the impact level imposed by their likelihood of occurrence. The calculation methodology will be based on "Risk Calculation" formula shared later in this report.



ID	Level	Vulnerability	Components
1	HIGH	Operating System (OS) End of Life (EOL) Detection	Operating System
2	HIGH	rlogin Passwordless Login	
3	Medium	TWiki Cross-Site Forgery Vulnerability	TWiki Version Prior to 4.3.2
4	Medium	Anonymous FTP Login Reporting	FTP Server
5	Low	SSL/TLS: Man in the Middle Bypass Vulnerability.	OpenSSL Version

2.0 USED METHODOLOGIES

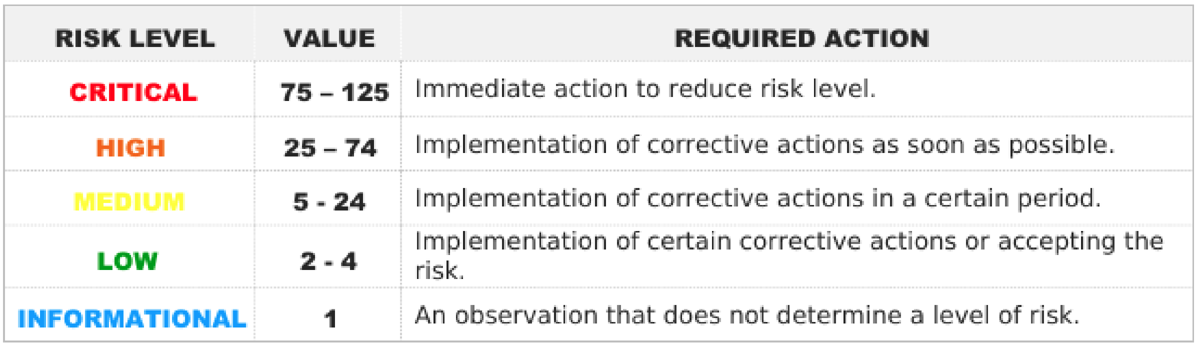
2.1 METHODOLOGY OF IDENTIFYING VULNERABILITIES

The techniques used in identifying and evaluating vulnerabilities are based on best industry practices on international level:

1. National Institute of Standards and Technology – NIST;
2. Open-Source Security Testing Methodology – OSSTM;
3. Open Information Systems Security Group - OISSG;
4. Open Web Application Security Project - OWASP.

2.2 RISK LEVEL ASSESSMENT METHODOLOGIES

Risk Represents the probability that a particular threat source can exploit that can have a certain level of impact on the organization or business.



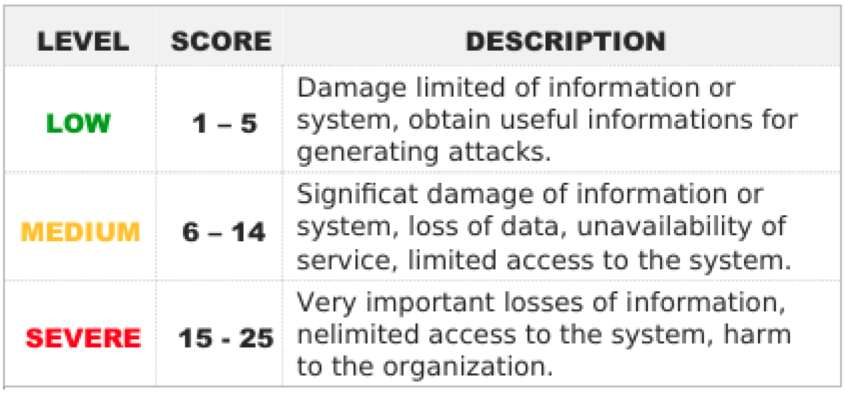
RISK LEVEL	VALUE	REQUIRED ACTION
CRITICAL	75 – 125	Immediate action to reduce risk level.
HIGH	25 – 74	Implementation of corrective actions as soon as possible.
MEDIUM	5 - 24	Implementation of corrective actions in a certain period.
LOW	2 - 4	Implementation of certain corrective actions or accepting the risk.
INFORMATIONAL	1	An observation that does not determine a level of risk.

The Risk Level calculation for vulnerabilities is done using the following formula:

Risk Level = Severity (Impact) x Probability (Likelihood)

2.2.1 Severity Value

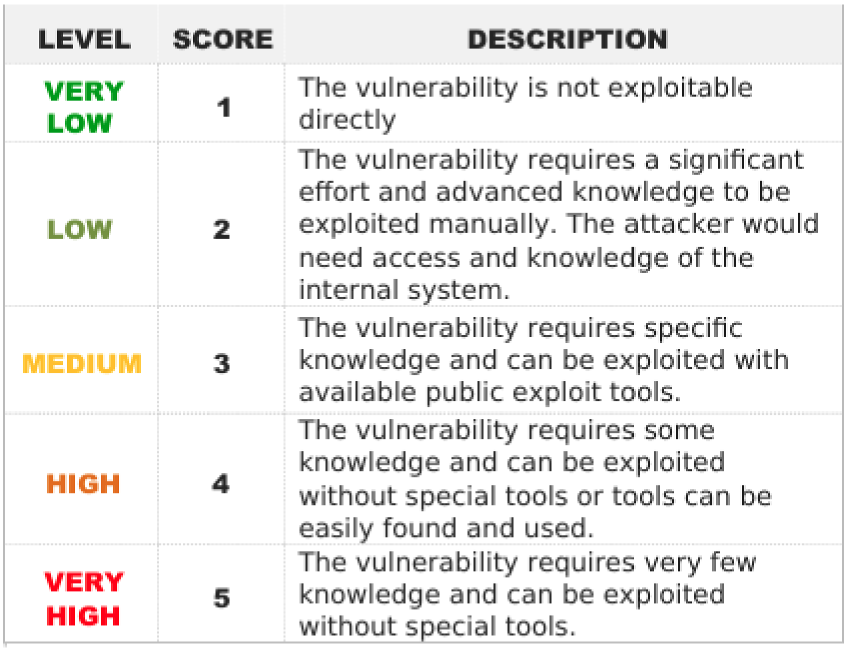
The negative impact on managed application and system information, loss or degradation or a combination theirs of the next security objectives: integrity, availability, confidentiality.



LEVEL	SCORE	DESCRIPTION
LOW	1 – 5	Damage limited of information or system, obtain useful informations for generating attacks.
MEDIUM	6 – 14	Significat damage of information or system, loss of data, unavailability of service, limited access to the system.
SEVERE	15 - 25	Very important losses of information, nelimited access to the system, harm to the organization.

2.2.2 Probability Value

The probability that a particular vulnerability to be exploited by an attacker. The calculation of the probability it has carefully: the motivation of the attacker, the level at knowledge required, ease of detection and exploitation of the vulnerability, the level of access required and existence of detection measures and prevention.



LEVEL	SCORE	DESCRIPTION
VERY LOW	1	The vulnerability is not exploitable directly
LOW	2	The vulnerability requires a significant effort and advanced knowledge to be exploited manually. The attacker would need access and knowledge of the internal system.
MEDIUM	3	The vulnerability requires specific knowledge and can be exploited with available public exploit tools.
HIGH	4	The vulnerability requires some knowledge and can be exploited without special tools or tools can be easily found and used.
VERY HIGH	5	The vulnerability requires very few knowledge and can be exploited without special tools.

3.0 TESTS PERFORMED

Around 5 specific tests were performed based on the best practices in the field. Multiple vulnerabilities have been identified and verified to be exploitable.

Code	Test	Vulnerability	Result
Configuration Management			
VLN-CM-1	(End Of Life) Testing for Infrastructure Configuration management	Security Misconfiguration	**FAIL**
Authentication			
VLN-AU-1	(rlogin) Testing for Default Guessable User Account	Guessable Account Details	**FAIL**
VLN-AU-2	(FTP) Testing for Default Guessable User Account	Guessable Account Details	**FAIL**
Client Side			
VLN-CL-1	Testing for Cross Origin Resource Sharing (CORS)	Cross-Site Request Forgery (CSRF)	**FAIL**
Cryptography			
VLN-CR-1	Testing for Weak SSL-TLS Configuration	Weak SSL/TLS Configuration	**FAIL**

Legend:

PASS: Unconfirmed Vulnerability

FAIL: Confirmed Vulnerability

N/A: Untested Vulnerability (Not Applicable)

4.0 IDENTIFIED WEAKNESS

4.1 LIST OF IDENTIFIED WEAKNESSES

ID	Vulnerability
1	VLN-CM-1 – Security Misconfiguration
2	VLN-AU-1 – (rlogin) Guess-able Account Details
3	VLN-CL-1 – Cross-Site Forgery Vulnerability
4	VLN-AU-2 – (FTP) Guess-able Account Details
5	VLN-CR-1 – Weak SSL Configuration

4.2 VULNERABILITY DISTRIBUTION BY CATEGORY

	Configuration Management	Authentication	Client Side	Cryptography
VLN-CM-1	X			
VLN-AU-1		X		
VLN-AU-2		X		
VLN-CL-1			X	
VLN-CR-1				x

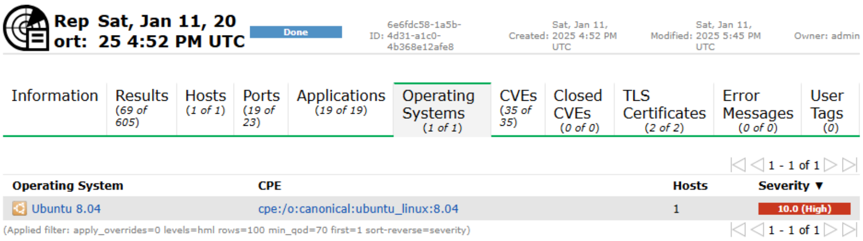
4.3 RISK LEVEL PER VULNERABILITY

The level risk was estimated by point of view of the technical impact of the system. The calculation methodology is presented in Chapter 4.2 Level risk assessment methodologies. Detailed values for the vulnerabilities are found in Chapter 6.4 -Detailed vulnerability report.

ID	Risk	Level	Vulnerability
1	70	**HIGH**	VLN-CM-1 – Security Misconfiguration
2	50	**HIGH**	VLN-AU-1 – (rlogin) Guess-able Account Details
3	20	**MEDIUM**	VLN-CL-1 – Cross-Site Forgery Vulnerability
4	16	**MEDIUM**	VLN-AU-2 – (FTP) Guess-able Account Details
5	5	LOW	VLN-CR-1 – Weak SSL Configuration

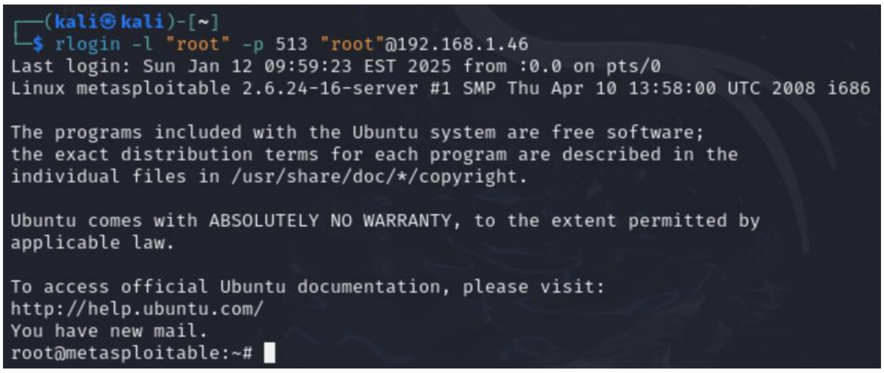
4.4 DETAILED VULNERABILITY REPORT

4.4.1 VLN-CM-1 – Security Misconfiguration

Summary	All operating systems and programs must be updated to the latest version, and all patches must be applied.
Risk	**70 (Probablity: 5 | Severity: 14)**
Risk Description	A hacker would gain Admin access to the insure server. If the server has sensitive information on it, the hacker can misuse them.
Technical Description	The Operating system no longer supports and lacks critical security patches.  Report: Sat, Jan 11, 2025 4:52 PM UTC Done ID: 6e6fdc58-1a5b-4d31-a1c0-4b368e12afe8 Created: Sat, Jan 11, 2025 4:52 PM UTC Modified: Sat, Jan 11, 2025 5:45 PM UTC Owner: admin Information Results (69 of 605) Hosts (1 of 1) Ports (19 of 23) Applications (19 of 19) Operating Systems (1 of 1) CVEs (35 of 35) Closed CVEs (0 of 0) TLS Certificates (2 of 2) Error Messages (0 of 0) User Tags (0) 1 - 1 of 1 Operating System | CPE | Hosts | Severity ▼ Ubuntu 8.04 | cpe:/o:canonical:ubuntu_linux:8.04 | 1 | 10.0 (High) (Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity) 1 - 1 of 1
Countermeasures	Upgrade OS to latest version Apply all available security patches

	Perform regular audits.

4.4.2 VLN-AU-I: (rlogin) Guessable Account Details

Summary	The rlogin service allows unauthenticated access due to weak passwords
Risk	**50 (Probablity: 5 | Severity: 10)**
Risk Description	Attacker can gain access to the system and exploit weak credentials to rlogin service.
Technical Description	The rlogin service allows passwordless login with guessable credentials. 
Countermeasures	Disable the rlogin service Use SSH instead of legacy rlogin

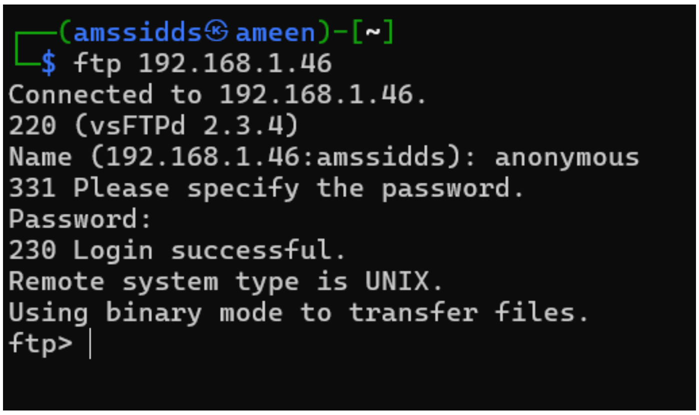
```
┌──(kali㉿kali)-[~]
└─$ rlogin -l "root" -p 513 "root"@192.168.1.46
Last login: Sun Jan 12 09:59:23 EST 2025 from :0.0 on pts/0
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# █
```

4.4.3 VLN-CL-1: Cross-Site Forgery Vulnerability

Summary	The application is vulnerable to CSRF allowing unauthorized actions to be performed on behalf of rightful user.
Risk	**20 (Probablity: 4 | Severity: 5)**
Risk Description	Attacker can trick a user into executing wrong actions on application
Technical Description	The vulnerability allows attackers to execute forged requests
Countermeasures	Implement CSRF tokens in forms

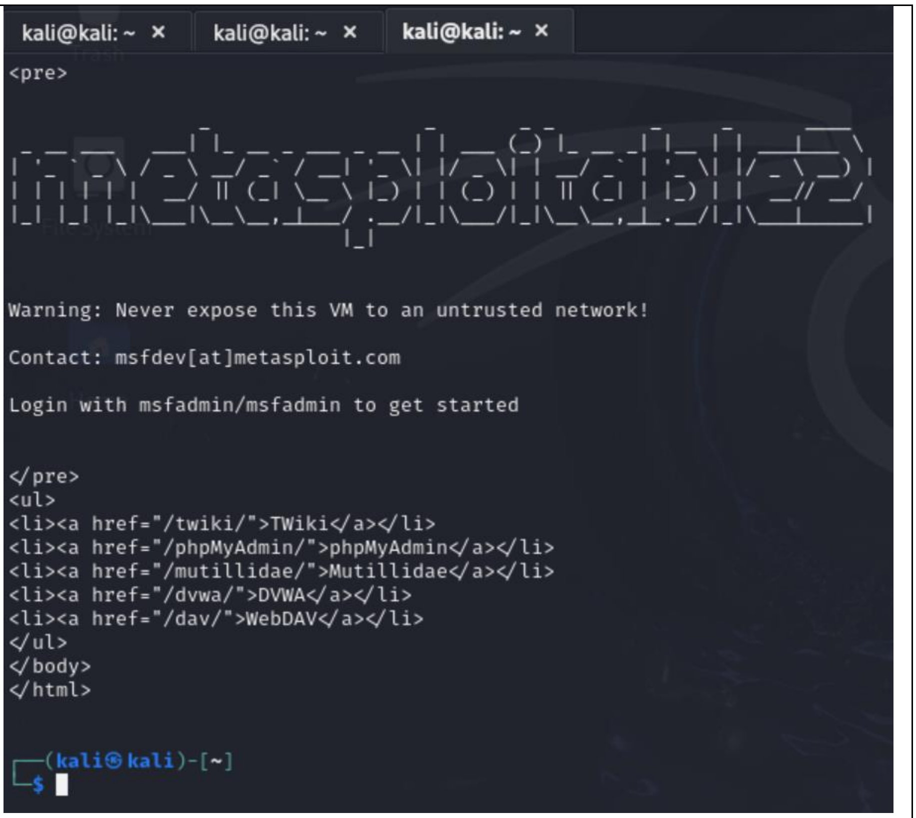
	Educate employee about not clicking on suspicious links

4.4.4 VLN-AU-2: (FTP) Guessable Account Details

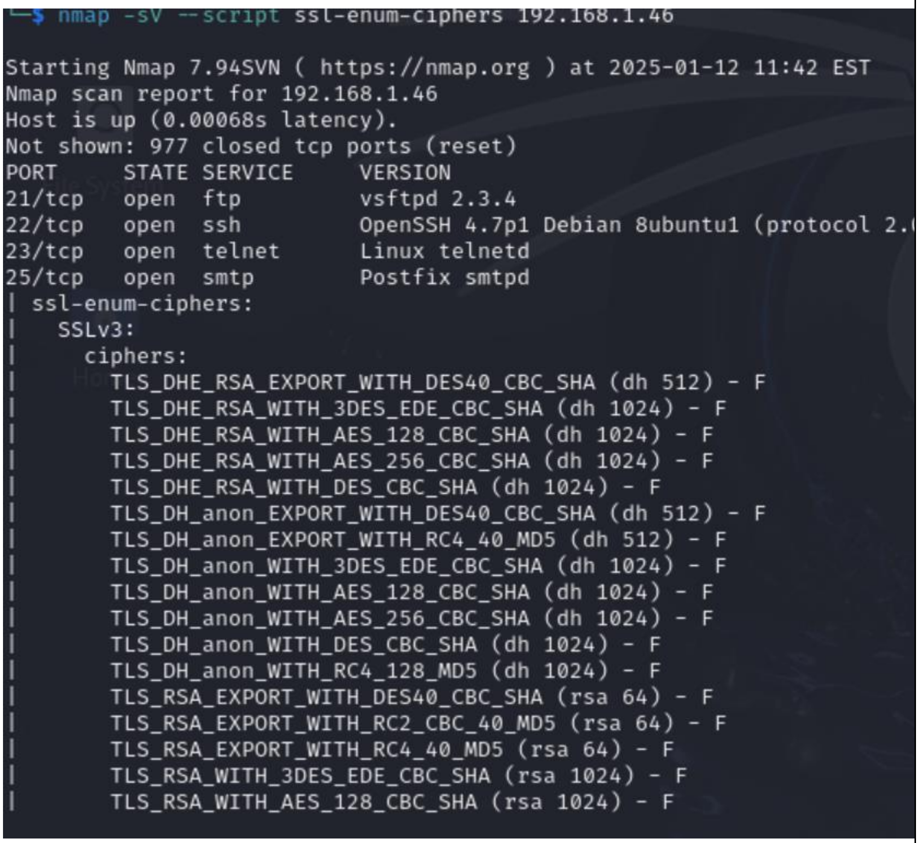
Summary	The FTP server allows anonymous login with weak credentials exposing sensitive data.
Risk	**16 (Probablity: 4 | Severity: 4)**
Risk Description	Attackers can exploit weak password and gain access to confidential information.
Technical Description	The FTP Server is configured to allow weak credentials, providing full access to confidential information without proper authentication  ┌──(amssidds㉿ameen)-[~] └─$ ftp 192.168.1.46 Connected to 192.168.1.46. 220 (vsFTPd 2.3.4) Name (192.168.1.46:amssidds): anonymous 331 Please specify the password. Password: 230 Login successful. Remote system type is UNIX. Using binary mode to transfer files. ftp>
Countermeasures	Disable FTO login Implement access controls to sensitive folders

4.4.5 VLN-CR-1: Weak SSL Configuration

Summary	SSL/TLS Configuration uses outdated cipher, making it vulnerable to attacks.
Risk	**5 (Probablity: 2 | Severity: 3)**
Risk Description	Attacker can exploit weak SSL/TLS configurations to manipulate data during transit.
Technical Description	The server is configured to support outdated ciphers, like DHE_EXPORT, which can be exploited by man-in-the-middle attacks.



```
<pre>

                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


</pre>
<ul>
<li><a href="/twiki/">TWiki</a></li>
<li><a href="/phpMyAdmin/">phpMyAdmin</a></li>
<li><a href="/mutillidae/">Mutillidae</a></li>
<li><a href="/dvwa/">DVWA</a></li>
<li><a href="/dav/">WebDAV</a></li>
</ul>
</body>
</html>


┌──(kali㉿kali)-[~]
└─$ 
```



```
└─$ nmap -sV --script ssl-enum-ciphers 192.168.1.46

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-12 11:42 EST
Nmap scan report for 192.168.1.46
Host is up (0.00068s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA (dh 512) - F
|       TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 1024) - F
|       TLS_DHE_RSA_WITH_DES_CBC_SHA (dh 1024) - F
|       TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA (dh 512) - F
|       TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 (dh 512) - F
|       TLS_DH_anon_WITH_3DES_EDE_CBC_SHA (dh 1024) - F
|       TLS_DH_anon_WITH_AES_128_CBC_SHA (dh 1024) - F
|       TLS_DH_anon_WITH_AES_256_CBC_SHA (dh 1024) - F
|       TLS_DH_anon_WITH_DES_CBC_SHA (dh 1024) - F
|       TLS_DH_anon_WITH_RC4_128_MD5 (dh 1024) - F
|       TLS_RSA_EXPORT_WITH_DES40_CBC_SHA (rsa 64) - F
|       TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (rsa 64) - F
|       TLS_RSA_EXPORT_WITH_RC4_40_MD5 (rsa 64) - F
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 1024) - F
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 1024) - F
```

Countermeasures	Disable weak ciphers. Use modern cipher “AES” Regularly check and test SSL/TLS configurations using SSL Tools