

M12 Group **Metasploitable** Activity

Parth Patel, Joseph Shiller, Evan Noyes, Devin Rankin, Andy
Olshansky

OS end of Support - NOCVE Severity: 10/10

```
msfadmin@metasploitable:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 8.04
Release:        8.04
Codename:       hardy
msfadmin@metasploitable:~$ _
```

Ubuntu 8.04, codename Hardy Heron, hit end of life on **May 12, 2011**. The reason why this is a high priority issue is because an EOL operating system will **not** get security fixes and updates for new vulnerabilities.

Backdoor - NOCVE Severity: 10/10

```
msfadmin@metasploitable:~$ grep "1524/tcp" /etc/services
ingreslock      1524/tcp
```

On Port **1524** there is a backdoor installed called “ingresslock”. The Ingress DB that binds to this port has a backdoor due to its use of telnet and that fact that telnet sends data over the wire **unencrypted**.

Weak Passwords for SQL DB Severity: 10/10

```
msfadmin@metasploitable:~$ grep "5432/tcp" /etc/services
postgresql      5432/tcp      postgres      # PostgreSQL Database
```

The PostgreSQL DB runs on this port. By itself it is not a vulnerability however the credentials are open to a password cracking attack (default password).

Insecure Login Service- NOCVE (Item 55) Severity: 10/10

```
msfadmin@metasploitable:/home/user$ grep "513/tcp" /etc/services
login           513/tcp
```

Unlike alternatives like SSH, *rlogin* sends data over an unencrypted channel. Leaves user open for man-in-the-middle attacks where a threat actor can see cleartext communication transfers.

Running insecure rsh service Severity: 7.5/10

```
msfadmin@metasploitable:~$ cat /etc/services | grep "rsh"
kshell          544/tcp        krcmd          # Kerberized 'rsh' (v5)
sgi-cmsd        17001/udp      # Cluster membership services daemon
sgi-gcd         17003/udp      # SGI Group membership daemon
```

Environment is running rsh which does not use encryption for data transfer.

We can run a wireshark and login into see that when it transmits passwords it will send them in clear text.

Short Password for Tomcat Webserver Admin Severity: 10/10

```
msfadmin@metasploitable:~$ cat /etc/tomcat5.5/tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<tomcat-users>
  <role rolename="admin"/>
  <role rolename="tomcat"/>
  <role rolename="manager"/>
  <role rolename="role1"/>
  <user username="tomcat" password="tomcat" roles="tomcat,admin,manager"/>
  <user username="role1" password="tomcat" roles="role1"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
</tomcat-users>
```

Tomcat admin (see roles) has a very short password (<1 sec guess time for a password cracker see next slide)

Time required for a password cracker to input 'tomcat':

Take the Password Test

Tip: Try to make your passwords at least 15 characters long

Show password: ☒

tomcat

Very Weak

6 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:

0.01 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it is a common password.

CVE-2016-7144

UnrealIRCd version 3.2.8.1 is installed, making the host vulnerable to authentication spoofing.

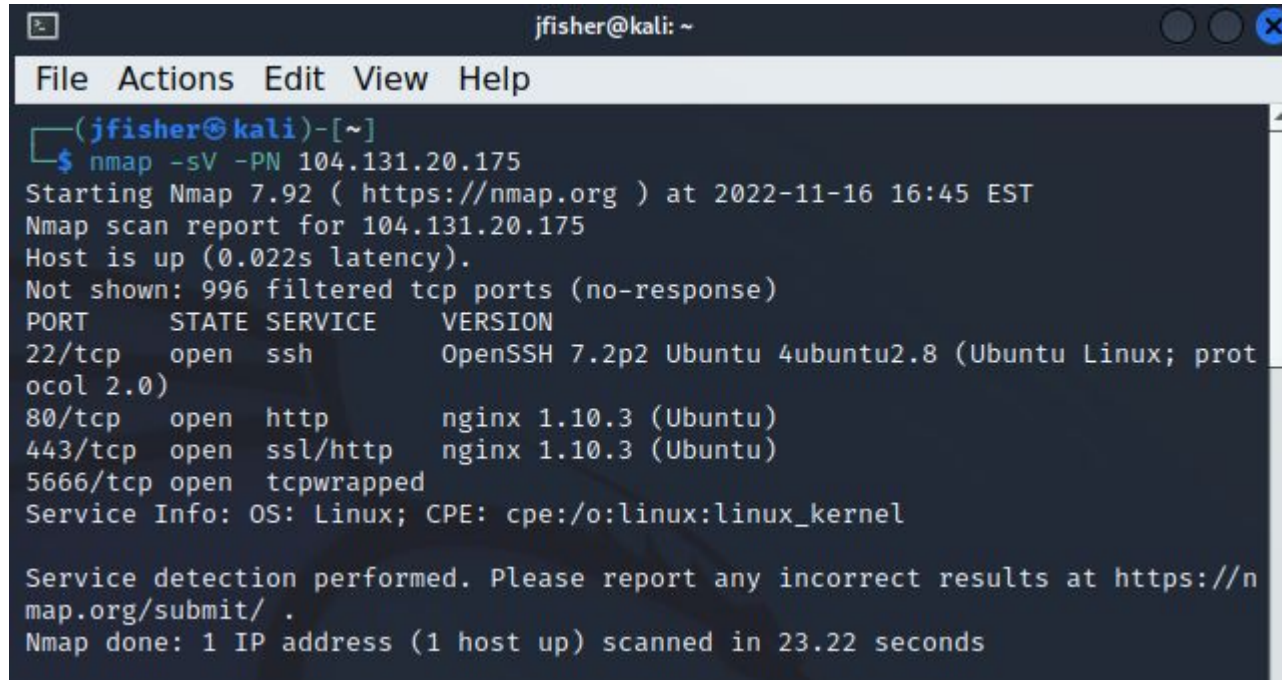
```
msfadmin@metasploitable:~$ sudo unrealircd
[sudo] password for msfadmin:
UnrealIRCd
v3.2.8.1
using TRE 0.7.5 (LGPL)
using libcurl/7.18.0 OpenSSL/0.9.8g zlib/1.2.3.3 libidn/1.1
```

CVE-2007-2447

Samba version 3.0.20 can be used by attackers to execute shell commands because it does not sanitize user input.

```
msfadmin@metasploitable:~/vulnerable/samba$ ls  
3.0.20  3.0.6  deps  
msfadmin@metasploitable:~/vulnerable/samba$
```

Used nmap to find open ports on the system



```
jfisher@kali: ~  
File Actions Edit View Help  
(jfisher@kali)-[~]  
$ nmap -sV -PN 104.131.20.175  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-16 16:45 EST  
Nmap scan report for 104.131.20.175  
Host is up (0.022s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; prot  
ocol 2.0)  
80/tcp    open  http         nginx 1.10.3 (Ubuntu)  
443/tcp   open  ssl/http     nginx 1.10.3 (Ubuntu)  
5666/tcp  open  tcpwrapped  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://n  
map.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 23.22 seconds
```


Used metasploitable ssh_login exploit

```
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > options
```

Module options (auxiliary/scanner/ssh/ssh_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 values: none, user, user@realm)
PASSWORD		no	A specific password to authenticate with
PASS_FILE	/home/jfisher/Desktop/pass.txt	no	File containing passwords, one per line
RHOSTS	104.131.20.175	yes	The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT	22	yes	The target port
STOP_ON_SUCCESS	true	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	/home/jfisher/Desktop/pass.txt	no	File containing usernames, one per line
VERBOSE	true	yes	Whether to print output for all attempts

```
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

Set correct options for the exploit

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 104.131.20.175
RHOSTS => 104.131.20.175
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/jfisher/Desktop/users.txt
USER_FILE => /home/jfisher/Desktop/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/jfisher/Desktop/users.txt
PASS_FILE => /home/jfisher/Desktop/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > █
```

Service detection
map.org/submit/
Nmap done: 1 IP ad

5.1 █

Ran exploit to attempt to get into the system

```
PASS_FILE => /home/jffisher/Desktop/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 104.131.20.175:22 - Starting bruteforce
[-] 104.131.20.175:22 - Failed: 'user:user'
[!] No active DB -- Credential data will not be saved!
[-] 104.131.20.175:22 - Failed: 'user:msfadmin'
[-] 104.131.20.175:22 - Failed: 'msfadmin:user'
[-] 104.131.20.175:22 - Failed: 'msfadmin:msfadmin'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > 
```

```
5666/tcp open 104.131.20.175
Service Info: OS: Linux
Service detection map.org/submit/...
Nmap done: 1 IP address scanned
<img alt="Nmap scan results for 104.131.20.175 showing port 5666/tcp open and service info." data-bbox="864 240 1000 480"/>
```

Exploit I was attempting to use

104.131.20.175	metasploitable.vmdk-s-1vcpu-1gb-nyc3-01	Canonical Ubuntu Linux	22/tcp	
----------------	---	------------------------	--------	--

it was possible to login into the remote SSH server using default credentials.

As the VT 'SSH Brute Force Logins With Default Credentials' (OID: 1.3.6.1.4.1.25623.1.0.108013) might run into a timeout the actual reporting of this vulnerability takes place in this VT instead. The script

HIGH

7.5

NOCVE

It was possible to login with the following credentials <User>:<Password>

msfadmin:msfadmin
user:user

Rpcinfo to report status of Remote Procedure Call

This can be used to find the port of users and process. This is fairly low vulnerability

```
msfadmin@metasploitable:~$ rpcinfo -p
```

program	vers	proto	port	
100000	2	tcp	111	portmapper
100000	2	udp	111	portmapper
100024	1	udp	39597	status
100024	1	tcp	39466	status
100003	2	udp	2049	nfs
100003	3	udp	2049	nfs
100003	4	udp	2049	nfs
100021	1	udp	51382	nlockmgr
100021	3	udp	51382	nlockmgr
100021	4	udp	51382	nlockmgr
100003	2	tcp	2049	nfs
100003	3	tcp	2049	nfs
100003	4	tcp	2049	nfs
100021	1	tcp	39065	nlockmgr
100021	3	tcp	39065	nlockmgr
100021	4	tcp	39065	nlockmgr
100005	1	udp	41366	mountd
100005	1	tcp	51682	mountd
100005	2	udp	41366	mountd
100005	2	tcp	51682	mountd
100005	3	udp	41366	mountd
100005	3	tcp	51682	mountd

```
msfadmin@metasploitable:~$
```

Item	Description
-a	Specifies the complete IP address and port number of the host.
-b	Makes an RPC broadcast to procedure 0 of the specified <i>prognum</i> and <i>versnum</i> and reports all hosts that respond. If <i>transport</i> is specified, it broadcasts its request only on the specified <i>transport</i> . If broadcasting is not supported by any <i>transport</i> , an error message is printed. Using broadcasting (-b flag) should be limited because of the possible adverse effect on other systems.
-d	Deletes registration for the RPC service of the specified <i>prognum</i> and <i>versnum</i> . If <i>transport</i> is used, unregister the service only on that <i>transport</i> , otherwise unregister the service on all the transports where it was registered. This option can be exercised only by the root user.
-l	Displays a list of entries with the specified <i>prognum</i> and <i>versnum</i> on the specified host. Entries are returned for all transports in the same protocol family as those used to contact the remote portmap daemon.
-m	Displays a table of portmap operations statistics on the specified host. The table contains statistics for each version of portmap (Versions 2, 3, and 4), the number of times each procedure was requested and successfully serviced, the number and type of remote call requests that were made, and information about RPC address lookups that were handled. This information is used for monitoring RPC activities on the host.
-n <i>Portnum</i>	Use the <i>Portnum</i> parameter as the port number for the -t and -u options instead of the port number given by the portmap. Using the -n options avoids a call to the remote portmap to find out the address of the service. This option is made obsolete by the -a option.
-p	Probes the portmap service on the host using Version 2 of the portmap protocol and displays a list of all registered RPC programs. If a host is not specified, it defaults to the local host.
-s	Displays a concise list of all registered RPC programs on the host. If host is not specified, the default is the local host.
-t	Makes an RPC call to procedure 0 of <i>prognum</i> on the specified host using TCP, and reports whether a response was received. This option is made obsolete when using the -T option as shown in the third syntax.
-T	Specifies the transport where the service is required.
-u	Makes an RPC call to procedure 0 of <i>prognum</i> on the specified host using UDP, and reports whether a response was received. This option is made obsolete when using the -T option as shown in the third syntax.

Summary

Total 10 - Validations

- OS Outdated
 - Ubuntu 8.04 has reached EOS (open to newer attack vectors since updates won't be released)
- Port 1524 Backdoor
 - Port 1524/TCP/Ingreslock may be used as a backdoor which may exploit RPC. It also allows unencrypted data to be transferred via telnet.
- Weak Passwords / Default Passwords
 - The Postgress Database and the Tomcat Webserver use short and common passwords.
- Sending *unencrypted* data
 - Running services listed below transmit data over unencrypted channels
 - rlogin
 - Rsh
 - rexec
- Unsanitized Input
 - Metasploitable uses Samba 3.0.2 which does not sanitize user input, allowing for malicious commands.
- Open Ports
 - Using nmap, it is possible to find many open ports on Metasploitable.