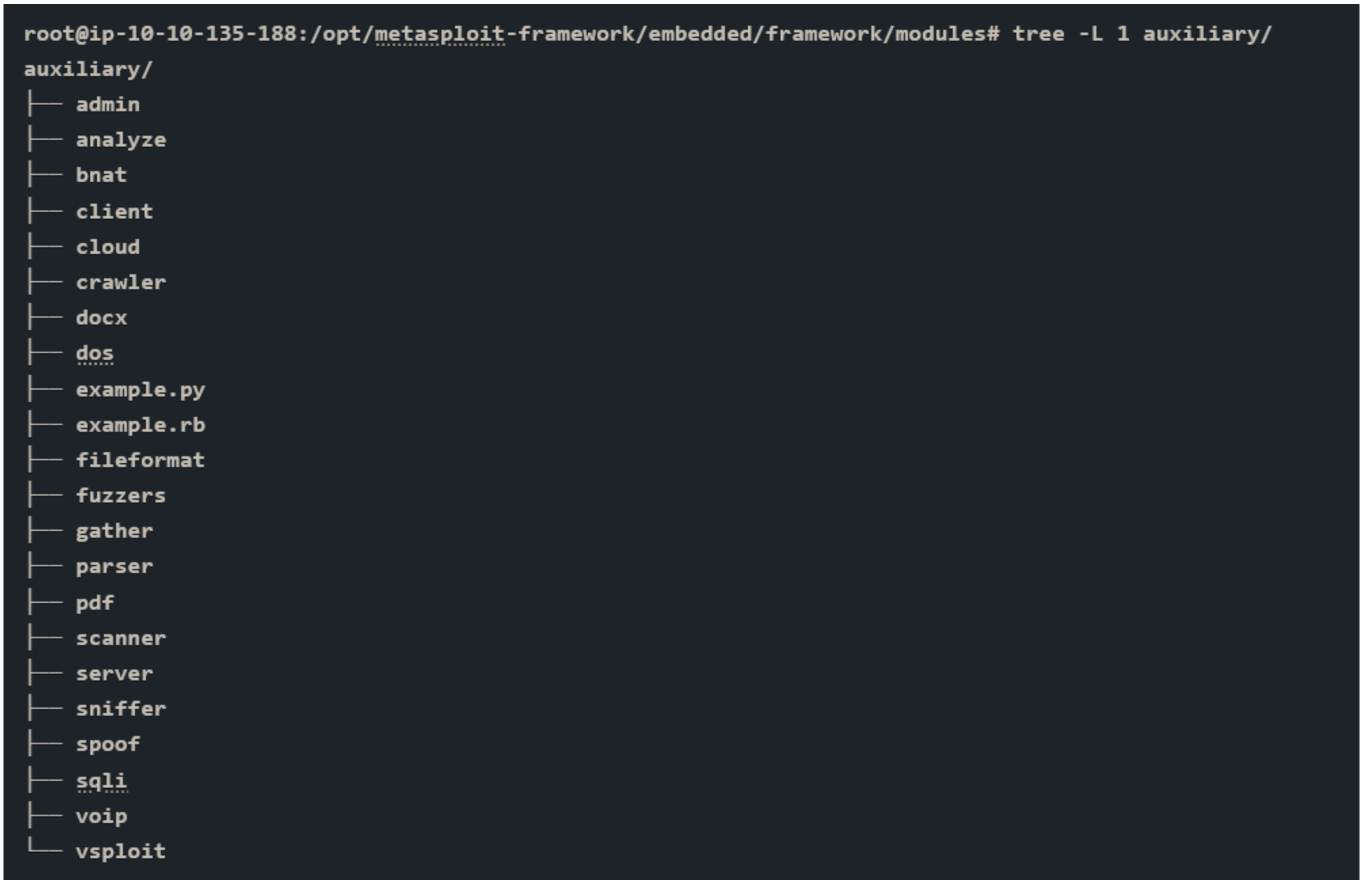
Metasploit

Day 27/365

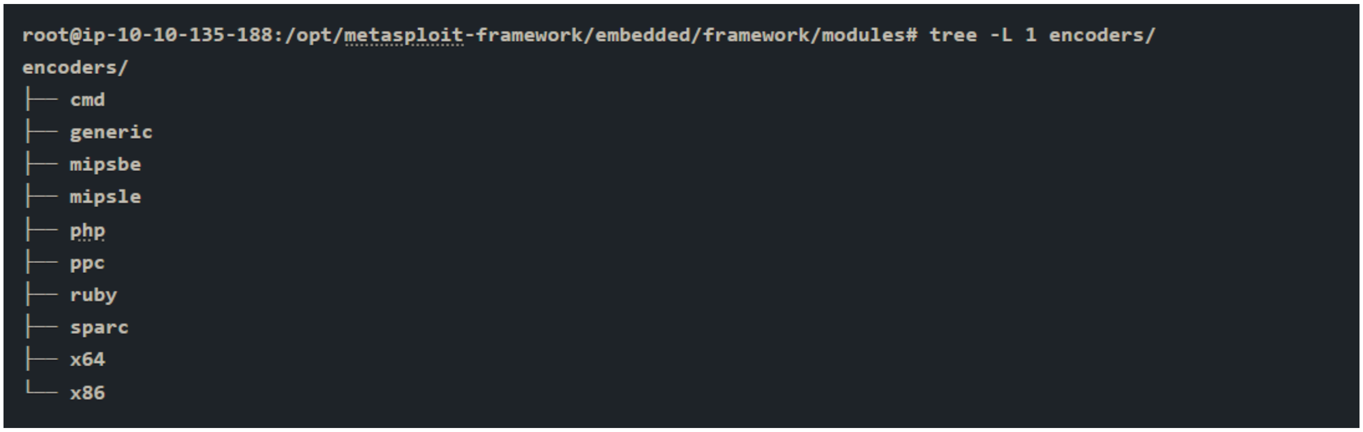
Before diving into modules, it would be helpful to clarify a few recurring concepts: vulnerability, exploit, and payload.

- **Exploit:** A piece of code that uses a vulnerability present on the target system.
- **Vulnerability:** A design, coding, or logic flaw affecting the target system. The exploitation of a vulnerability can result in disclosing confidential information or allowing the attacker to execute code on the target system.
- **Payload:** An exploit will take advantage of a vulnerability. However, if we want the exploit to have the result we want (gaining access to the target system, read confidential information, etc.), we need to use a payload. Payloads are the code that will run on the target system.



```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 auxiliary/
auxiliary/
├── admin
├── analyze
├── bnat
├── client
├── cloud
├── crawler
├── docx
├── dos
├── example.py
├── example.rb
├── fileformat
├── fuzzers
├── gather
├── parser
├── pdf
├── scanner
├── server
├── sniffer
├── spoof
├── sqli
├── voip
└── vsploit
```

auxiliary modules

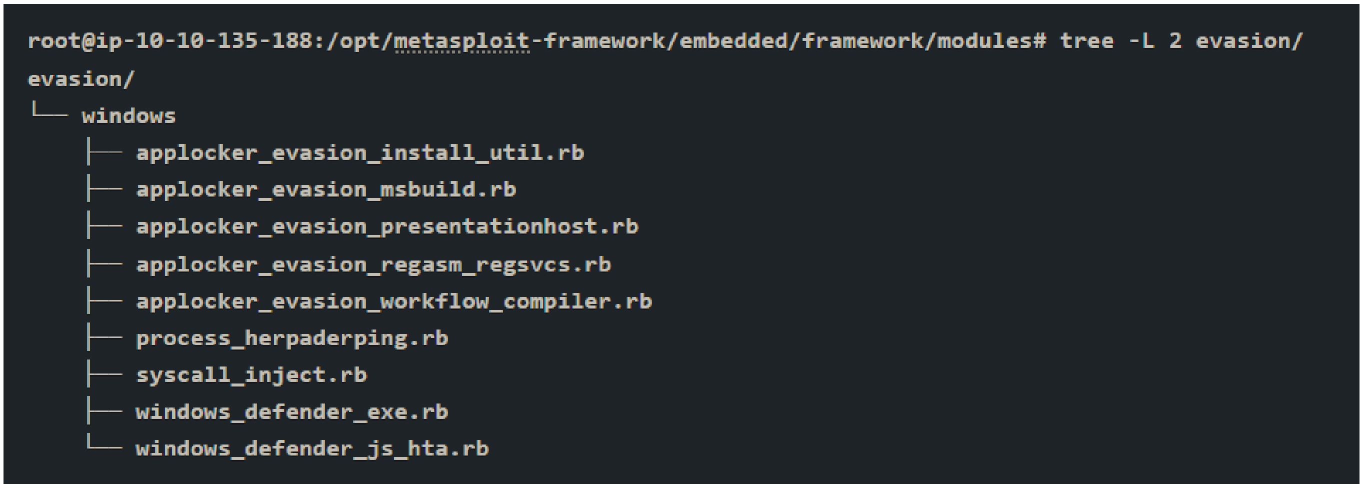


```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 encoders/
encoders/
├── cmd
├── generic
├── mipsbe
├── mipsle
├── php
├── ppc
├── ruby
├── sparc
├── x64
└── x86
```

Encoders

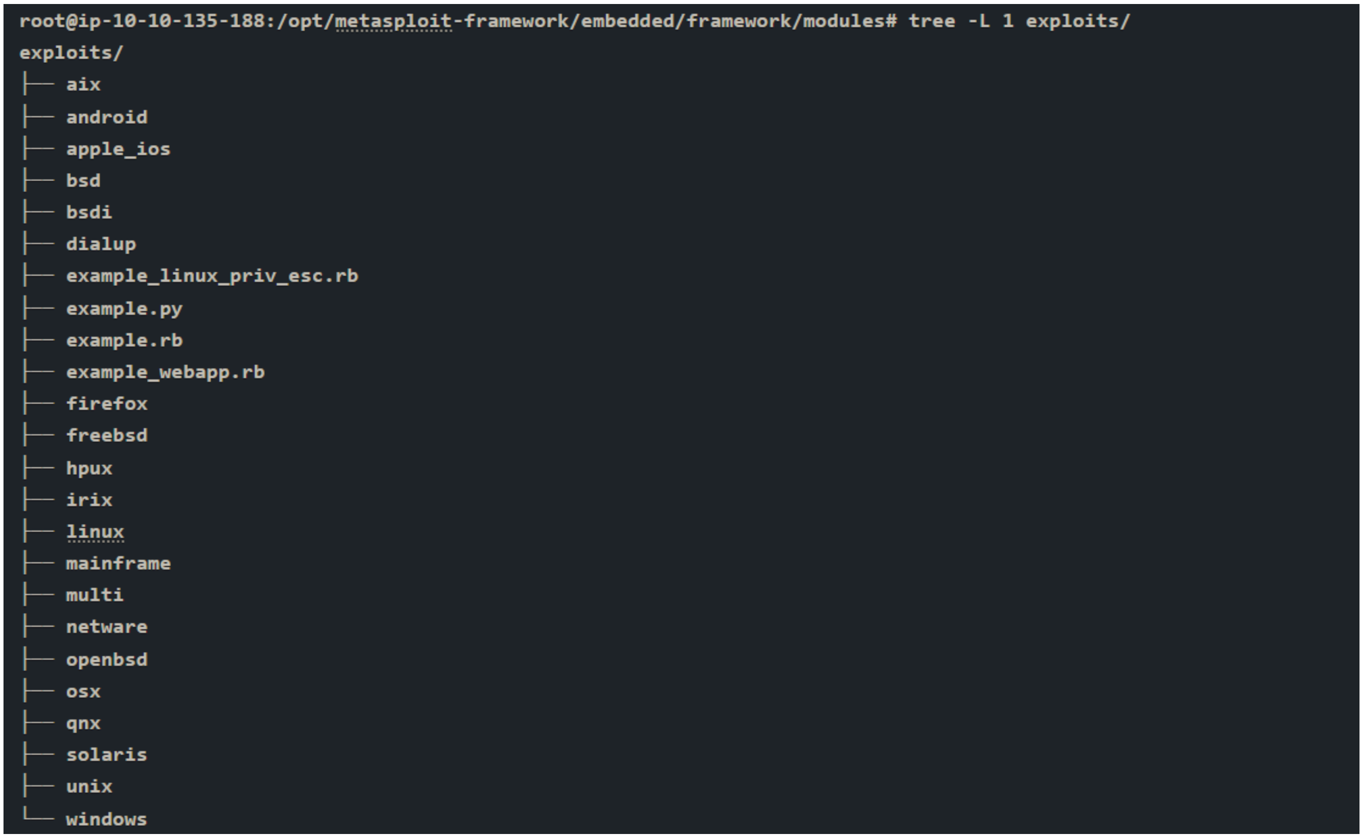
Encoders will allow you to encode the exploit and payload in the hope that a signature-based antivirus solution may miss them.

Signature-based antivirus and security solutions have a database of known threats. They detect threats by comparing suspicious files to this database and raise an alert if there is a match. Thus encoders can have a limited success rate as antivirus solutions can perform additional checks.



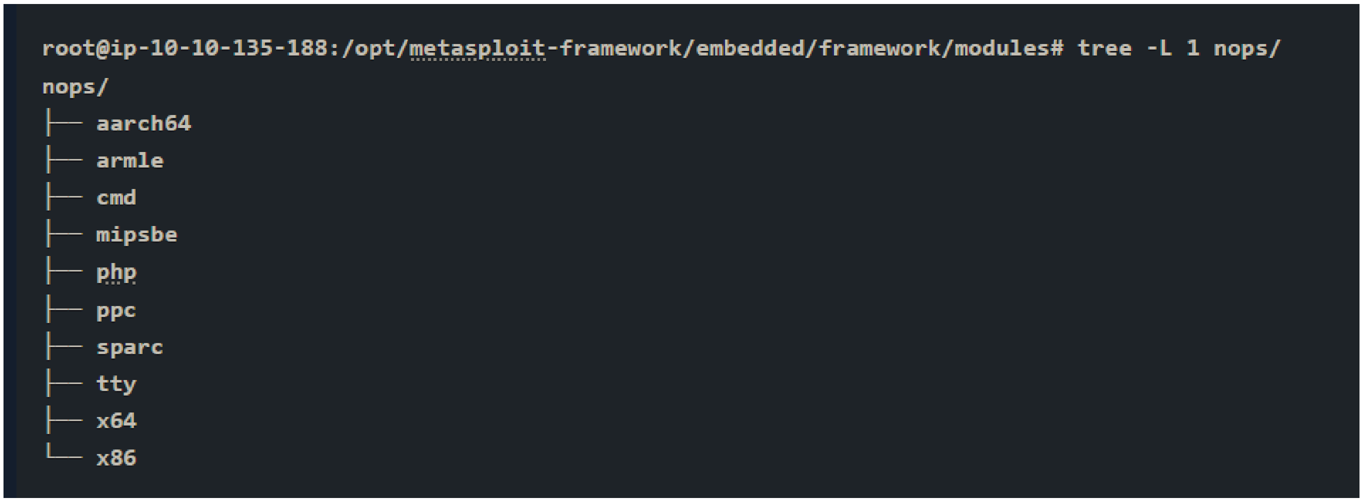
```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 2 evasion/
evasion/
└── windows
    ├── applocker_evasion_install_util.rb
    ├── applocker_evasion_msbuild.rb
    ├── applocker_evasion_presentationhost.rb
    ├── applocker_evasion_regasm_regsvcs.rb
    ├── applocker_evasion_workflow_compiler.rb
    ├── process_herpaderping.rb
    ├── syscall_inject.rb
    ├── windows_defender_exe.rb
    └── windows_defender_js_hta.rb
```

Evasion



```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 exploits/
exploits/
├── aix
├── android
├── apple_ios
├── bsd
├── bsdi
├── dialup
├── example_linux_priv_esc.rb
├── example.py
├── example.rb
├── example_webapp.rb
├── firefox
├── freebsd
├── hpux
├── irix
├── linux
├── mainframe
├── multi
├── netware
├── openbsd
├── osx
├── qnx
├── solaris
├── unix
└── windows
```

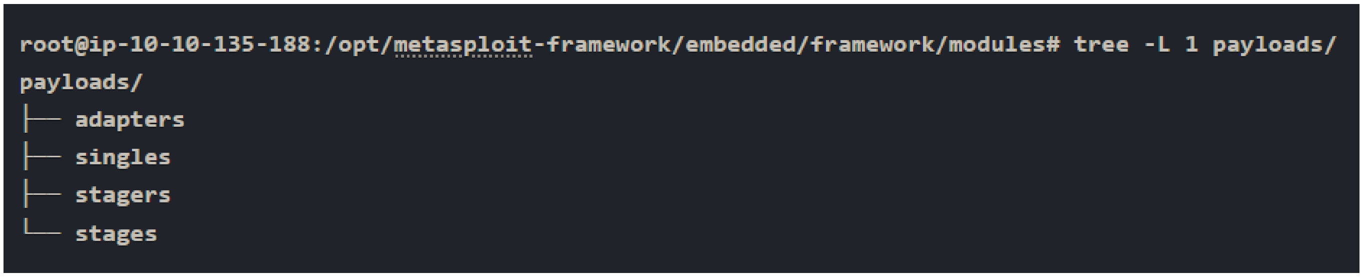
Exploits



```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 nops/
nops/
├── aarch64
├── armle
├── cmd
├── mipsbe
├── php
├── ppc
├── sparc
├── tty
├── x64
└── x86
```

NOPs

the CPU will do nothing for one cycle, often used as a buffer to achieve consistent payload sizes.



```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 payloads/
payloads/
├── adapters
├── singles
├── stagers
└── stages
```

Payloads

Codes that will run on the target system

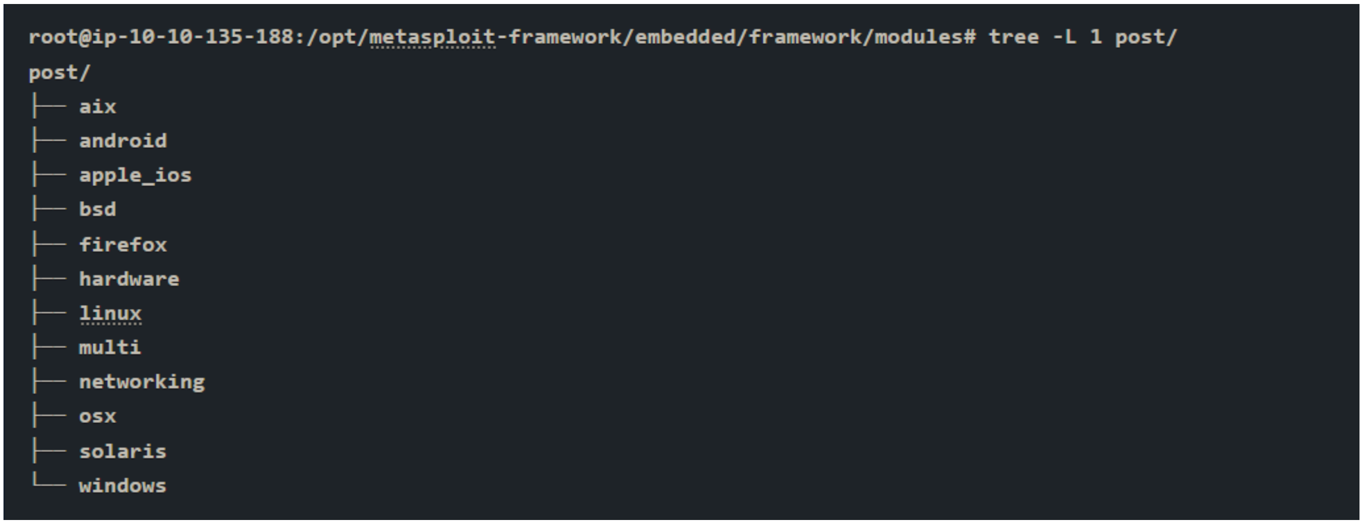
Exlpoits will leverage a vuln on target system, but to achieve the desired result, we will need a payload

Examples

- getting a shell
- loading malware
- backdoor to the target system
- running a command (calc.exe as a benign proof of concept)

4 dif directories

- **Adapters:** An adapter wraps single payloads to convert them into different formats. For example, a normal single payload can be wrapped inside a Powershell adapter, which will make a single powershell command that will execute the payload.
- **Singles:** Self-contained payloads (add user, launch notepad.exe, etc.) that do not need to download an additional component to run.
- **Stagers:** Responsible for setting up a connection channel between Metasploit and the target system. Useful when working with staged payloads. “Staged payloads” will first upload a stager on the target system then download the rest of the payload (stage). This provides some advantages as the initial size of the payload will be relatively small compared to the full payload sent at once.
- **Stages:** Downloaded by the stager. This will allow you to use larger sized payloads.
- generic/shell*reverse_tcp ---> inline or single payload (*)
- windows/x64/shell/reverse_tcp ---> staged payload (/)

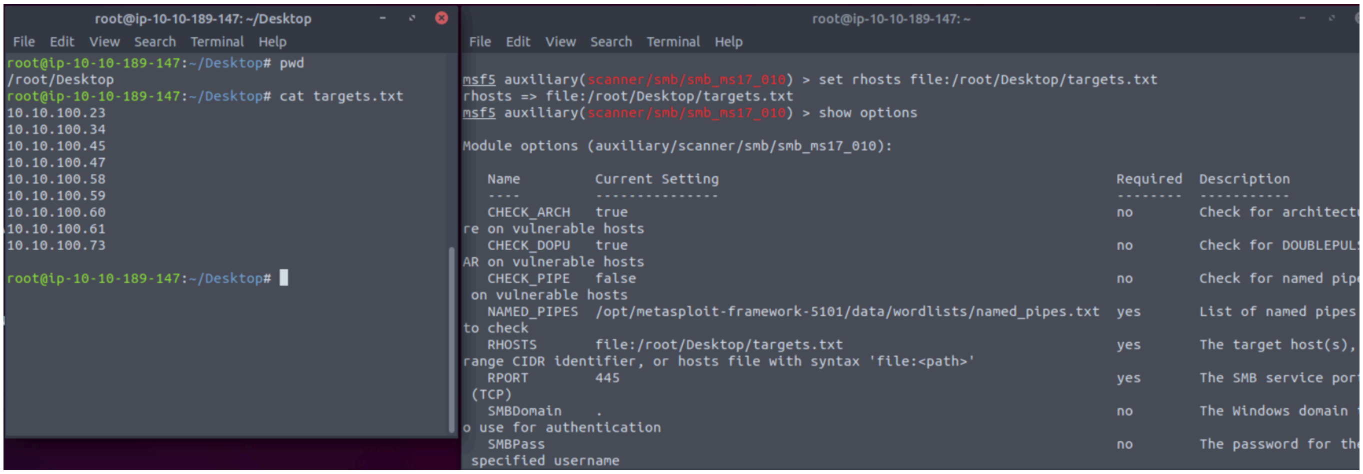


```
root@ip-10-10-135-188:/opt/metasploit-framework/embedded/framework/modules# tree -L 1 post/
post/
├── aix
├── android
├── apple_ios
├── bsd
├── firefox
├── hardware
├── linux
├── multi
├── networking
├── osx
├── solaris
└── windows
```

post modules

Commonly used parameters

- **RHOSTS:** “Remote host”, the IP address of the target system. A single IP address or a network range can be set. This will support the CIDR (Classless Inter-Domain Routing) notation (/24, /16, etc.) or a network range (10.10.10.x – 10.10.10.y). You can also use a file where targets are listed, one target per line using file:/path/of/the/target_file.txt, as you can see below.



root@ip-10-10-189-147: ~/Desktop
File Edit View Search Terminal Help

```
root@ip-10-10-189-147:~/Desktop# pwd
/root/Desktop
root@ip-10-10-189-147:~/Desktop# cat targets.txt
10.10.100.23
10.10.100.34
10.10.100.45
10.10.100.47
10.10.100.58
10.10.100.59
10.10.100.60
10.10.100.61
10.10.100.73

root@ip-10-10-189-147:~/Desktop# 
```

root@ip-10-10-189-147: ~
File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > set rhosts file:/root/Desktop/targets.txt
rhosts => file:/root/Desktop/targets.txt
msf5 auxiliary(scanner/smb/smb_ms17_010) > show options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                          Required  Description
   ----         ---------------                                          --------  -----------
   CHECK_ARCH   true                                                     no        Check for architectu
re on vulnerable hosts
   CHECK_DOPU   true                                                     no        Check for DOUBLEPULS
AR on vulnerable hosts
   CHECK_PIPE   false                                                    no        Check for named pipe
 on vulnerable hosts
   NAMED_PIPES  /opt/metasploit-framework-5101/data/wordlists/named_pipes.txt  yes       List of named pipes
to check
   RHOSTS       file:/root/Desktop/targets.txt                           yes       The target host(s),
range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        445                                                      yes       The SMB service port
 (TCP)
   SMBDomain    .                                                        no        The Windows domain t
o use for authentication
   SMBPass                                                               no        The password for the
 specified username
```

- **RPORT:** “Remote port”, the port on the target system the vulnerable application is running on.
- **PAYLOAD:** The payload you will use with the exploit.
- **LHOST:** “Localhost”, the attacking machine (your AttackBox or Kali Linux) IP address.
- **LPORT:** “Local port”, the port you will use for the reverse shell to connect back to. This is a port on your attacking machine, and you can set it to any port not used by any other application.
- **SESSION:** Each connection established to the target system using Metasploit will have a session ID. You will use this with post-exploitation modules that will connect to the target system using an existing connection.

Port Scanning

```
msf6 > search portscan
```

Options

- **CONCURRENCY:** Number of targets to be scanned simultaneously.
- **PORTS:** Port range to be scanned. Please note that 1-1000 here will not be the same as using Nmap with the default configuration. Nmap will scan the 1000 most used ports, while Metasploit will scan port numbers from 1 to 10000.
- **RHOSTS:** Target or target network to be scanned.
- **THREADS:** Number of threads that will be used simultaneously. More threads will result in faster scans.

`scanner/discovery/udp_sweep` module will allow you to quickly identify services running over the UDP

SMB Scans

Metasploit offers several useful auxiliary modules that allow us to scan specific services. Below is an example for the SMB. Especially useful in a corporate network would be `smb_enumshares` and `smb_version`

---

msfvenom

creates payloads