**Reference Material**

# UNIT-2 FOOT PRINTING OR RECONNAISANCE

**FOOT PRINTING** The act of gathering information about a targeted system and creating a network and systems map of an organization is known as Footprinting. It falls in the preparatory pre-attack phase, where all the details regarding an organization's network architecture, application types, and physical location of the target system are collected. Post Footprinting, the hacker gets a better understanding and picture of the location, where the desired information is stored, and how it can be accessed.

## Types of Footprinting :

There are 2 types of Footprinting:

- Active Footprinting
- Passive Footprinting

### Active Footprinting

When the hacker tries to perform footprinting by getting directly in touch with the targeted system, it is known as Active Footprinting.

### Passive Footprinting

On the other hand, when the attacker gathers information about the target system through openly available sources, it is known as Passive Footprinting. There are many such sources available on the internet from where hackers can get the necessary information about the organizations or individuals.

### Types of Information Collected through Footprinting

Following are the various types of information that are generally aimed at by the hackers through Footprinting:

- IP Addresses
- Applications used
- Presence of a Firewall
- Security Configurations
- Domain Names
- Network Numbers
- Authentication Mechanisms
- E-Mail addresses and Passwords

**Forms of Footprinting**

There are various forms and varieties of Footprinting. Some of them are as follows:

- E-Mail Footprinting
- Google Hacking
- Social Engineering
- Whois Footprinting
- Network Footprinting
- Website Footprinting

**USING PING AND NS LOOKUP COMMANDS IN WINDOWS COMMAND LINE:**

- **ping command**

Now let's examine one of the most popular utilities related to network connectivity.

Probably the first command that every computer user runs on the command line when having connectivity problems is the "**ping**" command.

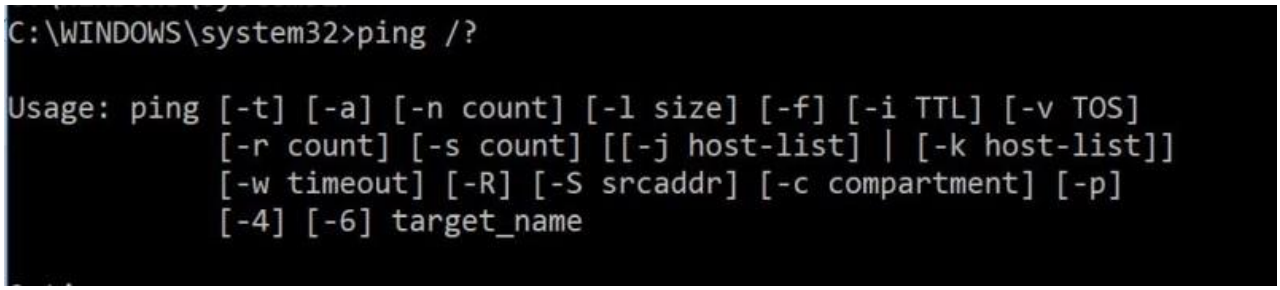
This will quickly show you if can send and receive packets (**icmp** packets to be exact) from your computer and hence shows whether you have network connectivity or not.

Note also that “ping” is useful for testing connectivity for both the local computer from where you execute the command and also for a remote computer or server which you try to reach.

If for example you try to “ping” your local default gateway IP address and you get replies back (icmp echo replies), this means your local computer is properly connected to the network.

Now, if you “ping” a remote server on the Internet and you get replies back, it means that the remote server is properly connected to its network as well.

**ping /?** : Displays all available options as shown below:




- **Ping [IP Address]** : By default it will send 4 ICMP packets to the stated IP address.

## Whois Lookup

Hackers use Whois Lookup to extract information from basic database queries like IP Address Block, Domain name, Location, and other critical data of the organization. Whois Lookup also acts as a pathway to Website Footprinting for hackers. The below steps form the initial phase of Whois Lookup:

- Open your browser and search for http://whois.domaintools.com/
- Feed the IP address or name of the organization to be targeted and click on ‘Search’
- The final output will display the details of the organization’s online presence

Following is an example of Who is Lookup:




## nslookup command

"nslookup" stands for "Name System Lookup" and is very useful in obtaining Domain Name System (DNS) related information about a domain or about an IP address (reverse DNS lookup).

**nslookup [domain name]:** The most popular usage of this command is to find quickly the IP address of a specific domain name (A-record) as shown below:

Example:

**nslookup www.networkstraining.com**

As shown above, the “nslookup” command followed by a domain name will show you the IPv4 and IPv6 addresses (A records and AAAA records) assigned to the specific domain.

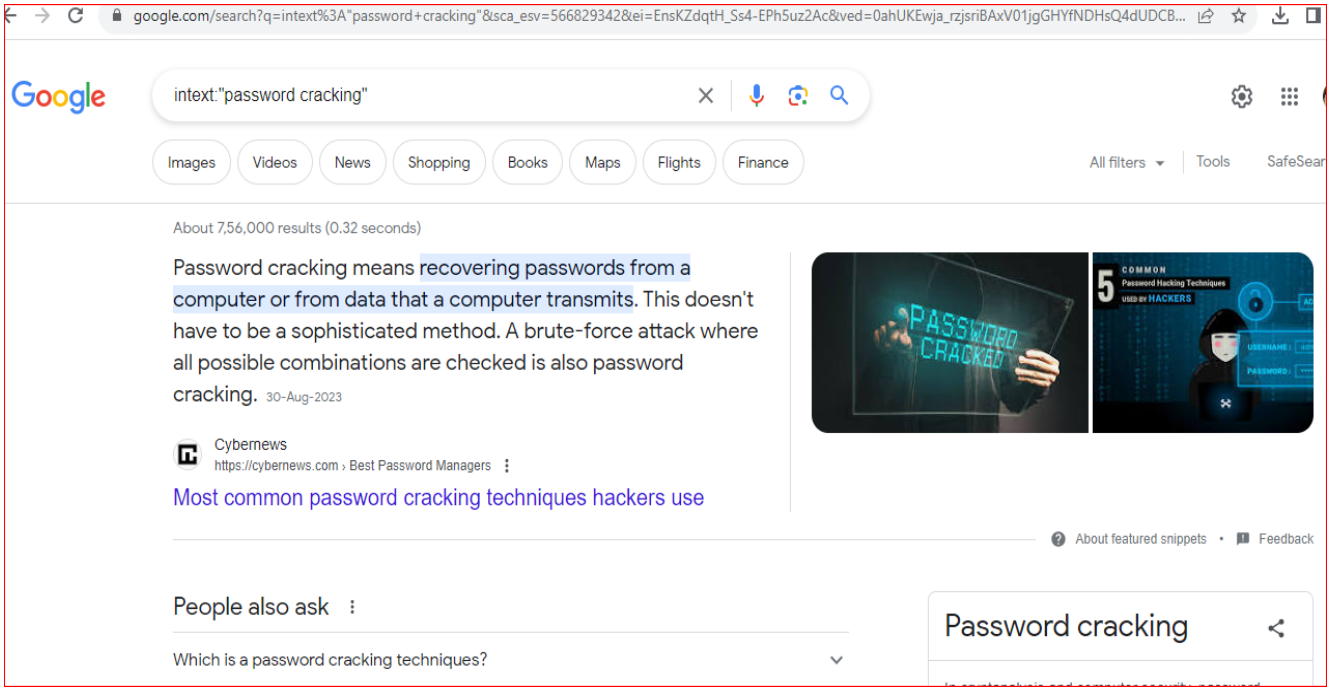
**nslookup [IP Address]:** This will perform a reverse-DNS lookup and will try to match the given IP address in the command with its corresponding domain name.

Example:

**nslookup 8.8.8.8**


As shown on the screenshot above, the IP address 8.8.8.8 is mapped with the name “**google-public-dns-a.google.com**”. You should note however that not all IP addresses are assigned to a domain name so a lot of times you will not get any information from the command above.

Google Search Engine



# TOPIC: Scanning

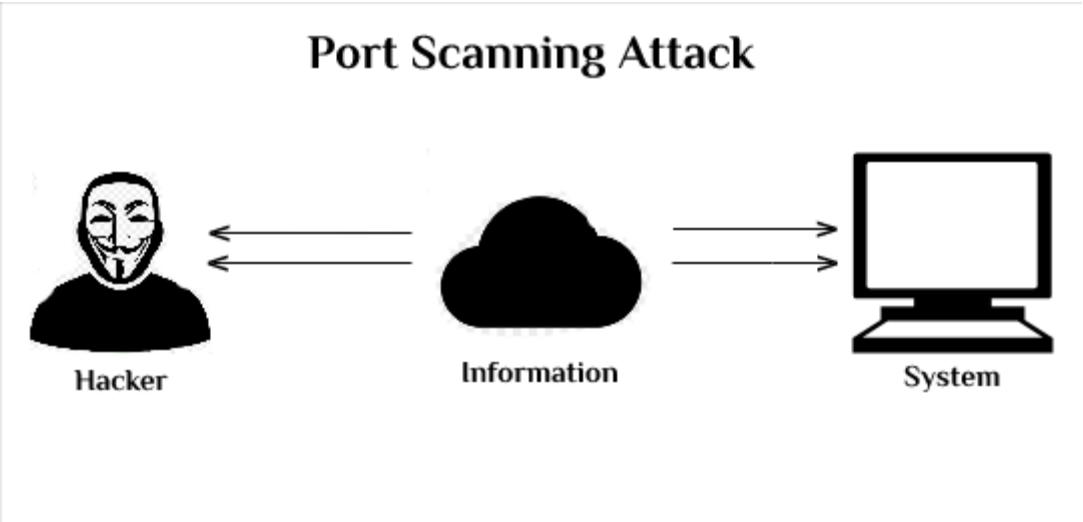
## What is Scanning?

Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization.Scanning refers to collecting more information using complex and aggressive reconnaissance techniques. Scanning in ethical hacking is a network exploration technique used to identify the systems connected to an organization's network. It provides information about the accessible systems, services, and resources on a target system. Some may refer to this type of scan as an active scan because it can potentially disrupt services on those hosts that are susceptible. Scanning is often used during vulnerability assessment when probing weaknesses in existing defenses.

**Basics of scanning** There are two ways of scanning:

- Active Scanning
- Passive Scanning

Scanning is more than just port scanning, but it is a very important part of this process. Scanning allows you to identify open ports on the target system and can be used for port mapping, performing an interactive session with the operating system via those ports, or even redirecting traffic from these open ports. There are many tasks that can be performed with a scanning tool.




## Active Scanning

Active scanning is a type of network scanning technique that is used to gather information about a target system or network. Unlike passive scanning, which only gathers information that is readily available, active scanning actively interacts with the target system to gather information.

It involves sending requests or packets to a target system and analyzing the responses to gather information about the target. This type of scanning is more aggressive and intrusive than passive scanning and is often used to identify vulnerabilities and weaknesses in a target system or network.

## Passive Scanning

Passive scanning is a type of network scanning technique that is used to gather information about a target system or network without actively interacting with the target. Unlike active scanning, which sends requests or packets to the target and analyzes the responses, passive scanning only gathers information that is readily available, such as information transmitted over the network or stored in system logs.

It is used to gather information about a target system or network for a variety of purposes, including network mapping, vulnerability

assessment, and compliance testing. By analyzing network traffic and system logs, passive scanning can provide valuable information about a target's infrastructure, servers, and devices, as well as the types of services and applications that are running.

## Scanning Methodology

- **Check for Live Systems:** Ping scan checks for the live system by sending ICMP echo request packets. If a system is alive, the system responds with ICMP echo reply packet containing details of TTL, packet size etc.
- **Check for Open Ports:** Port scanning helps us to find out open ports, services running on them, their versions etc. Nmap is the powerful tool used mainly for this purpose.

## BASIC TECHNIQUES OF SCANNING:

**Types of Scanning Techniques:**

1. **TCP connect scan**: This is a scan that sends TCP SYN packets to each port on the target system, waiting for an RST/ACK. This is a steal their type of scan because it does not show the open ports on the target system. The last port that responds is its open port, and you can use this to your advantage to determine which ports are open.
2. **TCP (transmission control protocol) syn port scan:** This is a similar type of scan, but the packets are TCP SYN packets and not TCP ACK. This type of scan sends packets to ports that are open and waiting for a reply.
3. **Network Scanning:** Network scanning is used to identify the devices and services that are running on a target network, determine their operating systems and software versions, and identify any potential security risks or vulnerabilities. Network scanning can be performed manually or automated using software tools, and can target specific systems or an entire network.

**EXAMPLE Network Scanning** — IP addresses, Operating system details, Topology details, trusted routers information etc

4. **Vulnerability Scanning:** Vulnerability scanning is a process of identifying, locating, and assessing the security vulnerabilities of a computer system, network, or application. This process is performed using automated software tools that scan for known vulnerabilities, as well as weaknesses in the configuration or implementation of the system being tested.

## Enumeratiung DNS:

DNS enumeration is one of the most popular reconnaissance tasks there is for building a profile of your target.

In plain english, it's the act of detecting and enumerating all possible DNS records from a domain name. This includes hostnames, DNS record names, DNS record types, TTLs, IP addresses, and a bit more, depending on how much informationWith effective DNS enumeration, you can clone DNS zones manually, using scripts or by exploiting DNS zone transfer vulnerabilities, known as AXFR (Asynchronous Transfer Full Range) Transfer.

## Tools for DNS Enumeration

There are several tools that you can use for DNS enumerations. Luckily most of these tools come pre-installed on security-focused distributions like Kali Linux or Parrot. This post will look at five tools you can use for DNS enumeration.

- NMAP
- DNSEnum
- DNSRecon
- Host Command
- NsLookup
-

## 1. NMAP

NMAP is a security tool mainly used for Network scanning and Port discovery. It also comes with various scripts that you can use to carry out penetration testing on multiple services. For example, the below command will list all the NMAP scripts for DNS enumeration.

```
bash
ls -al /usr/share/Nmap/scripts/ | grep -e "dns-"
```

```
golinux@kali:~$
golinux@kali:~$ ls -al /usr/share/nmap/scripts/ | grep -e "dns-"
-rw-r--r-- 1 root root  1499 Jul 13  2020 broadcast-dns-service-discovery.nse
-rw-r--r-- 1 root root  5329 Jul 13  2020 dns-blacklist.nse
-rw-r--r-- 1 root root 10100 Jul 13  2020 dns-brute.nse
-rw-r--r-- 1 root root  6639 Jul 13  2020 dns-cache-snoop.nse
-rw-r--r-- 1 root root 15152 Jul 13  2020 dns-check-zone.nse
-rw-r--r-- 1 root root 14826 Jul 13  2020 dns-client-subnet-scan.nse
-rw-r--r-- 1 root root 10168 Jul 13  2020 dns-fuzz.nse
-rw-r--r-- 1 root root  3803 Jul 13  2020 dns-ip6-arpa-scan.nse
-rw-r--r-- 1 root root 12702 Jul 13  2020 dns-nsec3-enum.nse
-rw-r--r-- 1 root root 10580 Jul 13  2020 dns-nsec-enum.nse
-rw-r--r-- 1 root root  3441 Jul 13  2020 dns-nsid.nse
-rw-r--r-- 1 root root  4364 Jul 13  2020 dns-random-srcport.nse
-rw-r--r-- 1 root root  4363 Jul 13  2020 dns-random-txid.nse
-rw-r--r-- 1 root root  1456 Jul 13  2020 dns-recursion.nse
-rw-r--r-- 1 root root  2195 Jul 13  2020 dns-service-discovery.nse
-rw-r--r-- 1 root root  5679 Jul 13  2020 dns-srv-enum.nse
-rw-r--r-- 1 root root  5765 Jul 13  2020 dns-update.nse
-rw-r--r-- 1 root root  2123 Jul 13  2020 dns-zeustracker.nse
-rw-r--r-- 1 root root 26574 Jul 13  2020 dns-zone-transfer.nse
golinux@kali:~$
```

## 2. DNSEnum

DNSEnum is a powerful Perl script that performs DNS enumerations on domain names. Some of the tasks that you can accomplish with this tool include:

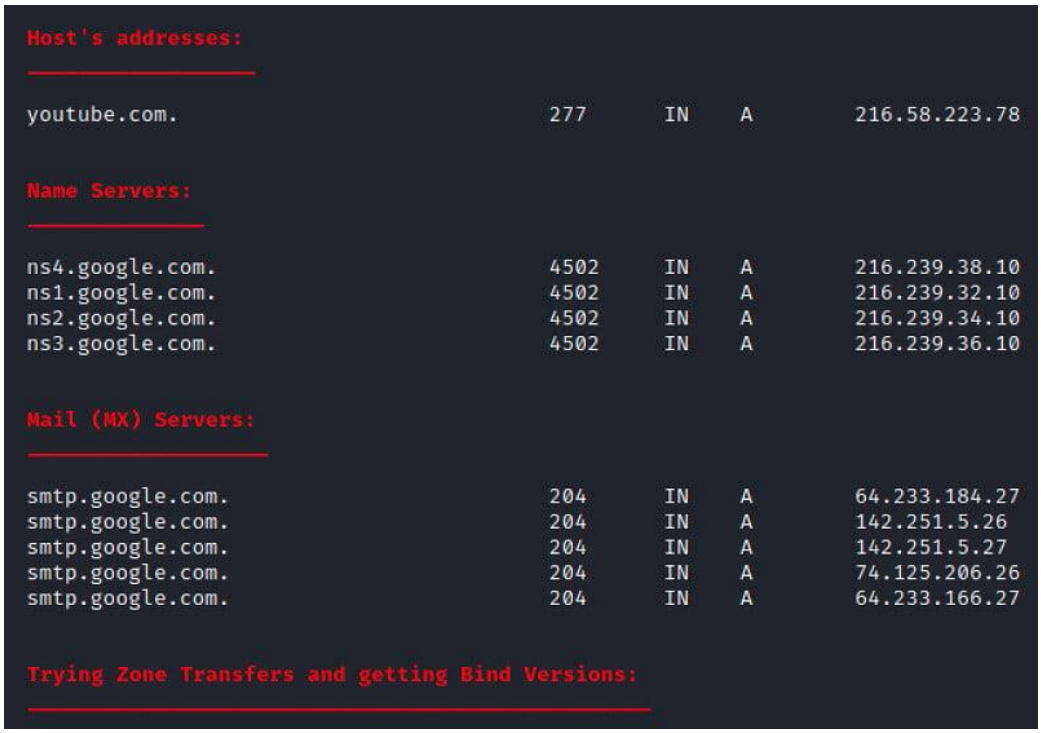
- Enumerate hostnames
- Enumerate “A” records
- Enumerate MX records
- Make AXFR queries
- Bruteforce subdomains
- Reverse lookups.

The DNSEnum command below performs a DNS enumeration but avoid reverse lookups since we passed the --noreverse argument. The output is stored in an XML file.

```
bash
dnsenum --noreverse -o mydomain.xml [target-domain]

E.g

dnsenum --noreverse -o mydomain.xml youtube.com
```




### 3. DNSRecon

DNSRecon is another powerful utility used to perform DNS enumeration. This tool is pre-installed on penetration testing distributions like Kali Linux or Parrot. To list all the available options for DNSRecon, execute the command below.

```bash
dnsrecon -help
```

Let’s carry out a simple DNS enumeration using the DNSRecon tool. Execute the command below.

```bash
dnsrecon -d [target-domain]


e.g.


dnsrecon -d youtube.com
```

### 4. Host Command

The host command is widely used to determine the IP address of a domain name. For example, the command below shows the IP address of Youtube.

```bash
host youtube.com
```

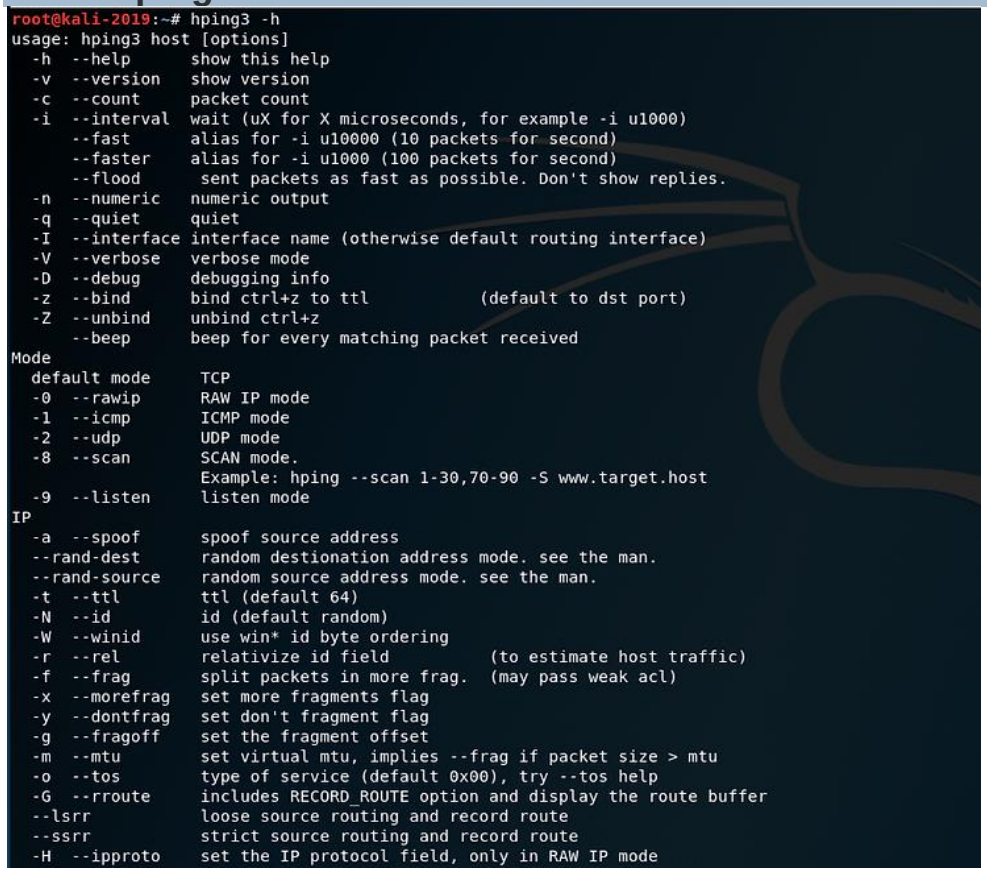

## PERFORMING FLAG SCAN USING HPING3

### Step 1: Finding Hping3

hping3 is a powerful tool with numerous features and functions. We'll look at some of the basic functions that are applicable to hackers here,

but investing a little time to learn additional features will be time well invested.
Let's look at the help screen first.

**kali > hping -h**

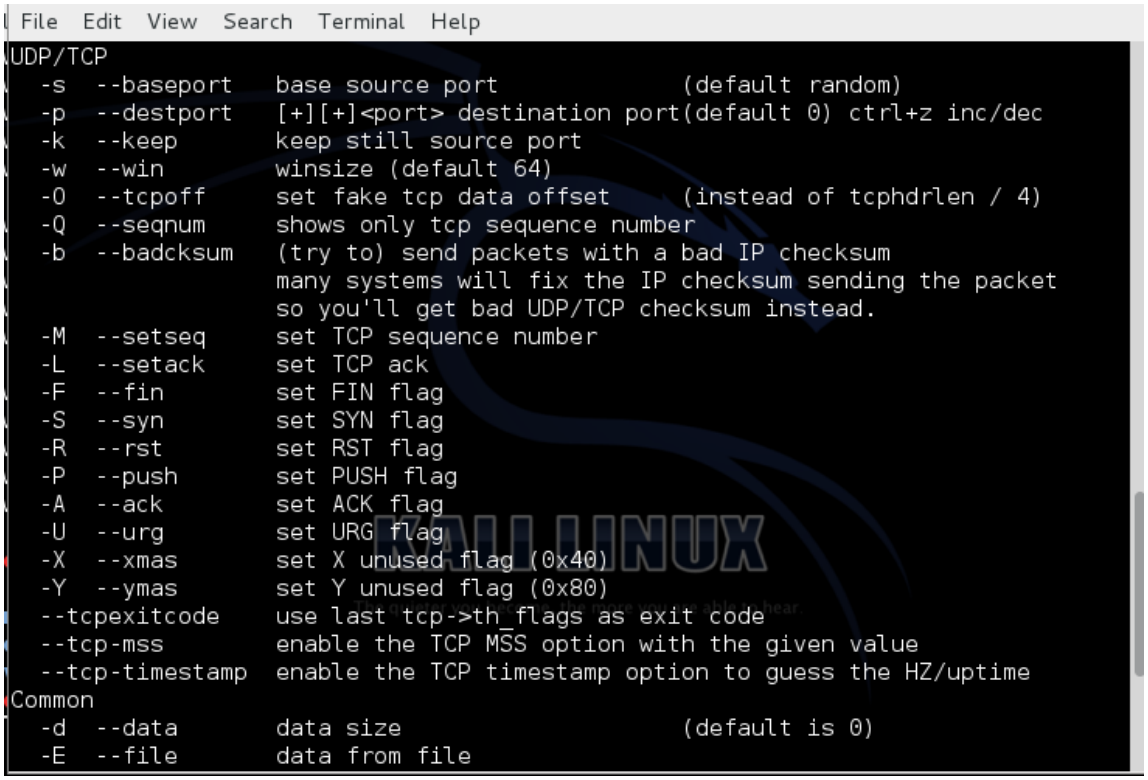



As you can see, the help screen for hping3 is very long and detailed. To better view it, let's pipe it out to **more**.

**kali >hping3 -h |more**

After hitting the enter key a few times to move down the screen, we come to the following information. Please note that hping3 can create TCP, RAW IP, ICMP, and UDP packets with TCP being the default.

- **-a** switch enables us to spoof our IP address
- **--rand-des**t produces packets with random destination ports
- **--rand-source** produces packets with random addresses
- **-t** sets the Time to Live (TTL) for the packets
- **-f** fragments the packets
-




If we now scroll down the help page a bit, we will see the following options. Note that like **nmap,** we can set any of the flags in the packet (FSPURA).
the following switches.

- **-Q** shows only the sequence number
- **-S** scan using SYN packets
- **--tcp-timestamp** grabs the timestamp from the tcp packet

**Step 2: hping3 Default**

One of the most important features to understand about hping3 is that its default packet is TCP. This means that when a network device such a router or firewall is blocking ICMP (ping), we can still do host discovery and reconnaissance with hping3.

Let's try setting the SYN flag (this would be essentially the same as nmap -sS scan) and checking whether port 80 is open (-p 80).

**kali > hping3 -S 192.168.1.116 -p 80**

```
root@kali:~# hping3 -S 192.168.1.116 -p 80
HPING 192.168.1.116 (eth0 192.168.1.116): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.116 ttl=128 DF id=17420 sport=80 flags=RA seq=0 win=0 rtt=1.
3 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17422 sport=80 flags=RA seq=1 win=0 rtt=1.
0 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17423 sport=80 flags=RA seq=2 win=0 rtt=0.
9 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17425 sport=80 flags=RA seq=3 win=0 rtt=7.
5 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17426 sport=80 flags=RA seq=4 win=0 rtt=0.
9 ms
len=46 ip=192.168.1.116 ttl=128 DF id=17428 sport=80 flags=RA seq=5 win=0 rtt=0.
5 ms
```

## Step 3: Fragment Packets with hping3

TCP was designed to be a robust protocol that would continue to communicate even in unfavorable or difficult circumstances. One feature that ensures this robustness is its ability to deal with packets that have been fragmented or broken into multiple pieces. TCP will reassemble those packets when they arrive at the target system.

This feature of TCP can be used against itself by using a tool like hping3 to fragment an attack across multiple packets to evade the IDS and firewall and then have the malware reassembled at the target.
Let's try the hping3 fragmentation.

**kali> hping3 -f 192.168.1.105 -p 80**

```
root@kali:~# hping3 -S -f 192.168.1.116 -p 445
HPING 192.168.1.116 (eth0 192.168.1.116): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.116 ttl=128 DF id=18306 sport=445 flags=SA seq=0 win=8192 rt
t=1.8 ms
len=46 ip=192.168.1.116 ttl=128 DF id=18307 sport=445 flags=SA seq=1 win=8192 rt
t=1.5 ms
len=46 ip=192.168.1.116 ttl=128 DF id=18308 sport=445 flags=SA seq=2 win=8192 rt
t=1.3 ms
len=46 ip=192.168.1.116 ttl=128 DF id=18309 sport=445 flags=SA seq=3 win=8192 rt
t=1.1 ms
len=46 ip=192.168.1.116 ttl=128 DF id=18310 sport=445 flags=SA seq=4 win=8192 rt
t=1.4 ms
len=46 ip=192.168.1.116 ttl=128 DF id=18311 sport=445 flags=SA seq=5 win=8192 rt
t=1.8 ms
len=46 ip=192.168.1.116 ttl=128 DF id=18312 sport=445 flags=SA seq=6 win=8192 rt
t=6.5 ms
```

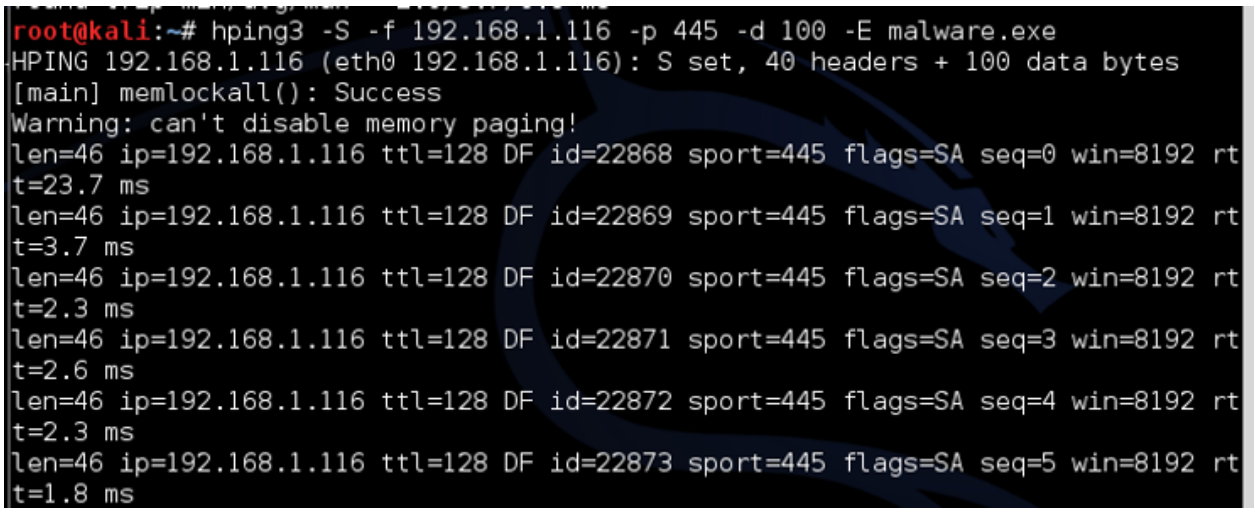
## Step 4: Flooding/Sending Data with hping3

In addition to being able to craft a packet with just about any characteristics we can imagine, hping3 will also allow us to place whatever data we want in those packets. Note in the help screen from Step 1 that the -E switch enables us to denote a file we want to use to fill the payload of the packet.

Let's say we have a file named malware that contains an exploit we're trying to send to the target. In addition, we are concerned

that this malware might be detected by the IDS. We could use the fragmentation switch and load the malware across multiple packets where it will be reassembled by the target, while evading the IDS or AV software.

**kali > hping3 -f 192.168.1.116 -p 445 -d 100 -E malware**




- **-d** is the data payload size (here, we've designated it as 100 bytes)

- **-E** tells hping3 to grab data from the following file

This command then sends the content of the file malware 100 bytes at a time to the target on port 445.