Commands

Reconnaissance:

The initial step a hacker takes to gather information.

Two Type of Reconnaissance (Active , Passive) :

- **Active**: Information collection is done by knowing the target
- **Passive**: Information is collected without the knowledge of the target through DNSs.

Important commands:

- $ ns lookup *facebook.com* (*Passive*)
  - **Information like (Facebook IPv4 , Facebook IPv6 , server)**
- $ ns lookup -type = mx *facebook.com* (*Passive*)
  - **Information about (mail Server)**
- $ host *facebook.com* (*Passive*)
  - **Information like (IPv4 , IPv6 , mail server)**
- $ ns lookup *facebook.com* (*Passive*)
  - **Information like (IPv4 , IPv6 , server name)**
- $ nmap *facebook.com* (*Active*)
  - **Find open ports At the target (by default scan first 1000 port)**

- $ nmap *facebook.com -p 1000 -1500 (Specify specific ports)*

- $ Whois *facebook.com*

    - Information *(Domain name , Registrar , Registrant , Abuse , name server*)

- $ recon -ng *(Collect information as before in more detail)*

- *[recon-ng] [default] >* ***marketplace search hacker*** *(Search for specific module)*

- *[recon-ng] [default] >* ***marketplace install hackertarget (install the module)***

- *[recon-ng] [default] >* ***marketplace load hackertarget (load the module)***

- *[recon-ng] [default] [hackertarget] > option set SOURCE google.com*

    - **Set a specific domain to find the all subdomains in this domain**

- *[recon-ng] [default] [hackertarget] > show hosts*

    - **It will show all the subdomains**

- $ sudo nmap -sS *facebook.com* *-p 1000 -1500* *(Specify specific ports)*

  Using *-sS will be faster It doesn’t complete three way hand shake*

- $ ip *add*

  - Information about *(your IP*)

- $ nmap --script http-enum -p 80 192.168.1.1

  (use http-enum.nse to find information about the target)

- *$ enum4linux* ***192.168.1.2*** *(transfer to numeric to find information)*

- *Sudo* ***Scapy***

- *>> send* ***(ip (dst=” ”,src” ”) / Icmp (type =” echo – reqest ”)***

  send Ping to another machine

- *$ sudo* ***tshark host 192.168.1.1 -- src***

  - **To find the packets in the network**