Recon

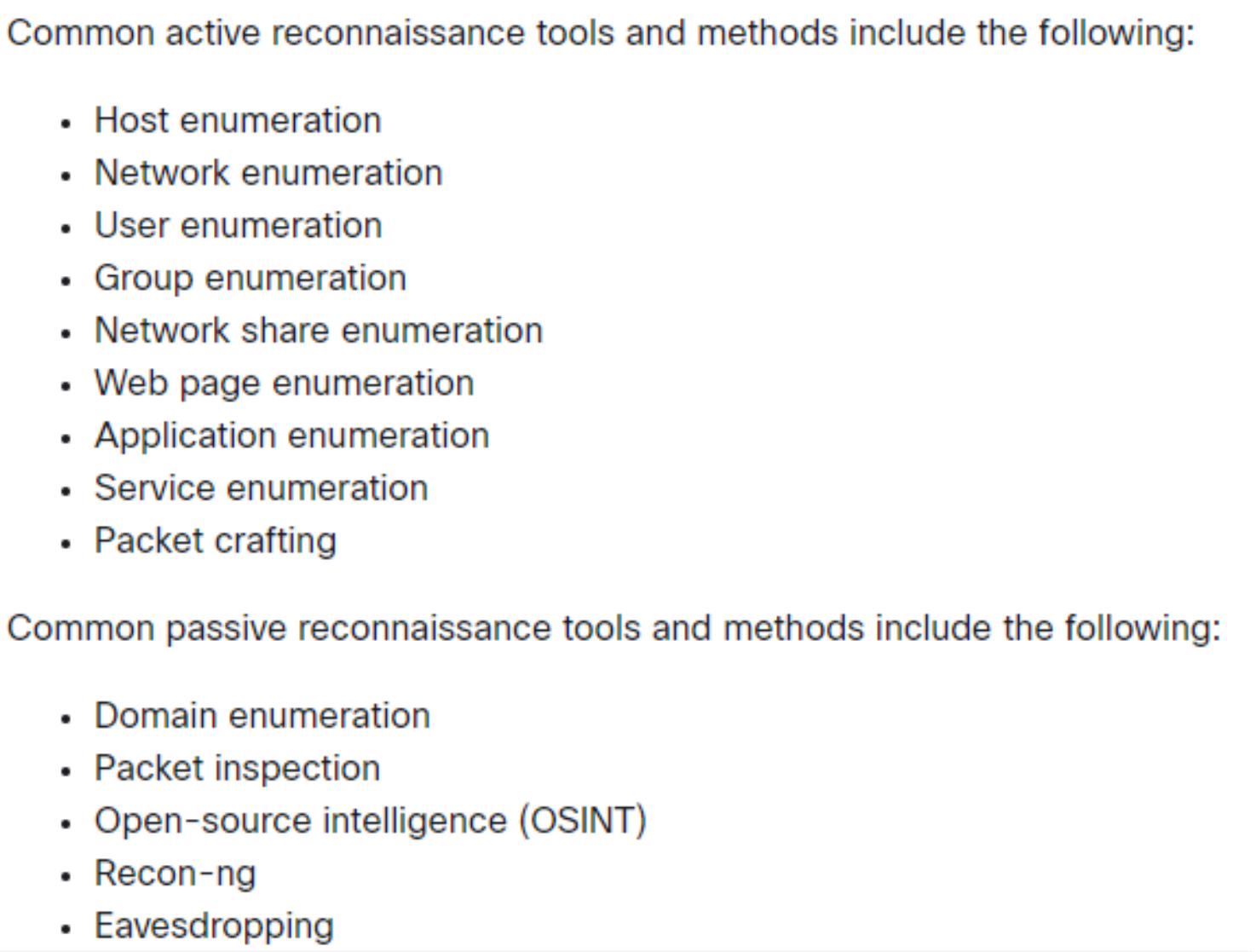
Footprinting and Reconnaissance

Hacking is NOT a Crime hackingisnotacrime.org is a nonprofit organization that attempts to raise awareness about the pejorative use of the term hacker. Historically, hackers have been portrayed as evil or illegal. Luckily, a lot of people already know that hackers are curious individuals who want to understand how things work and how to make them more secure.

You can collect information about the target organization through the means of footprinting in four steps:

1. Collect basic information about the target and its network.
2. Determine the operating system used, platforms running, web server versions, etc.
3. Perform techniques such as Whois, DNS, network and organizational queries.
4. Find vulnerabilities and exploits for launching attacks.

Information Gathering



1° Passive Recon

Domain Enumeration

$ ping -c 3 site.com

$ traceroute site.com

$ host site.com

$ host 72.163.5.201

$ nslookup site.com 1.1.1.1

$ nslookup 72.163.5.201

$ nslookup
>server 8.8.8.8
>set type=mx
>set type=ns
>set type=any

>site.com

$ dig website.com

$ dig website.com AAAA

$ dig website.com MX

$ dig @1.1.1.1 website.com

$ dig website.com 1.1.1.1 ns

$ dig -x 72.163.5.201

$ whois site.com

$ whois 72.163.5.201

DNS, BGP, WHOIS, IP ADDRESS

https://dnsdumpster.com/

https://dnslytics.com/

https://www.iana.org/whois

https://bgp.he.net/

https://ipinfo.io/

https://talosintelligence.com

https://registro.br/tecnologia/ferramentas/whois/

https://registro.br/tecnologia/ferramentas/

SSL Certificates Analysis

$sslscan site.com

#Scan Online
https://ssltools.com/

https://crt.sh/

https://www.ssllabs.com/ssltest/index.html

Site Analysis

https://sitereport.netcraft.com/

https://top.nic.br/

Plugin Wappalyser Firefox

website.com/robots.txt

website.com/sitemap.xml

view-source:https://website.com

http headers analisys

favicon icon discovery framework

Banner Grabbing with Netcat
$ nc -v <IP Address> <TCP port>
$ openssl s_client -quiet -connect <IP Address:443>
$ dig @<DNS Server> version.bind txt chaos
$ sudo nmap -Pn -sV --script=banner <IP Address>

Web Page Enumeration
$ proxychains dirb http://<IP Address> -w /usr/share/dirb/wordlists/common.txt
$ proxychains gobuster dir --url http://www.onlineshop.thm/ -w /usr/share/wordlists/dirbuster/directory-list.txt

E-mail analysis

http://whatismyipaddress.com/

https://haveibeenpwned.com/

https://www.kali.org/tools/theharvester/

#Search from e-mail addresses from a domain, limiting the results to 500, using DuckDuckGo
$ theHarvester -d kali.org -l 200 -b duckduckgo
$ theHarvester -d website.com -l 500 -b all

Sn1per
$ sudo git clone https://github.com/1N3/Sn1per
$ cd Sn1per

$ sudo ./install.sh

Google Hacking

Operator	Description
allintext:	Restricts results to pages with all query words in the page text.
filetype:	Restricts results to pages of the specified file type (.pdf, .ppt, .doc, etc.)
intitle:	Restricts results to pages with a certain word (or words) in the title.
inurl:	Restricts results to pages with a certain word (or words) in the URL.
site:	Restricts results to pages from the specified domain.

ExifTool

https://www.exploit-db.com/google-hacking-database

#Logs Files
allintext:username filetype:log

#Vuln Web Server
inurl:/proc/self/cwd**ExifTool**

#Open FTP Servers
intitle:"index of" inurl:ftp

#ENV Files
intitle:"index of" "env.bak"

#SSH Logins
filetype:log username putty

#Apache Servers
intitle:"Apache2 Ubuntu Default Page: It works"

#PHP Admin
"Index of" inurl:phpmyadmin

#cPanel Passwords reset
inurl:_cpanel/forgotpwd

#SQL Dumps
"index of" "database.sql.zip"

#E-mails lists
filetype:xls inurl:"email.xls"
site:.edu filetype:xls inurl:"email.xls"

Live Cams
inurl:top.htm inurl:currenttime
intitle:"webcamXP 5"
inurl:"lvappl.htm"

Enumeration
site:*.domain.com -www
site:..domain.com -www
site:*.domain.com ext:pdf
site:*.domain.com ext:php

OSINT Tools

https://osintframework.com/

https://whatsmyname.app/

Username searching can identify accounts that important enterprise personnel may have on various sites. Because other sites can be vulnerable, it is possible that hackers could gain access to personnel information from those accounts, including passwords, addresses, and telephone numbers. The types of sites that personnel have registered for can also provide details of their lives and interests. These details could be used in social engineering attacks.

FOCA

Fingerprinting Organization with Collected Archives (FOCA) is a tool designed to find metadata and hidden information in documents. FOCA can analyze websites as well as Microsoft Office, Open Office, PDF, and other documents. You can download FOCA from https://github.com/ElevenPaths/FOCA FOCA analyzes files by extracting EXIF (exchangeable image file format) information from graphics files, as well as information discovered through the URL of a scanned website.

ExifTool

ExifTool is a popular tool for extracting EXIF information from images. EXIF is a standard that defines the formats for images, sound, and ancillary tags used by digital equipment such as digital cameras, mobile phones, and tablets. You can download ExifTool from https://exiftool.org Example 10-4 shows output from ExifTool when it is run against an image called omar_pic.jpg.

Lab - Using OSINT Tools

Footprint Full

Start Run SpiderFoot

$spiderfoot -l 127.0.0.1:5001

http://127.0.0.1:5001

Perform scan in **h4cker.org**

$spiderfoot -M | grep **[search term]**

Register API Keys Spiderfoot [Settings tab]

Lab – Using OSINT Tools

Module	Type of Information	Your API Key, etc
Builtwith	web software in use	Answers will vary.
Hunter.io	email address search	Answers will vary.
Onion.link	Tor onion site search	Answers will vary.
IntelligenceX	everything	Answers will vary.

Recon-ng
https://hackertarget.com/recon-ng-tutorial/

Create a workspace

$recon-ng

#Commands
marktplace, workspaces, help, list, create, remove

#Search Modules Available
[recon-ng] [default] > marketplace search, info, refresh

#Install Modules
[recon-ng] [default] > marketplace install recon/domains-hosts/bing_domain_web

#Show Modules Installed
[recon-ng] [default] > modules search

#Load Module
[recon-ng] [default] > module load recon/domains-hosts/bing_domain_web

#Change the Source

[recon-ng][default][bing_domain_web] > options set SOURCE h4cker.org
SOURCE => h4cker.org
[recon-ng][default][bing_domain_web] > run

#Tasks
install hackertarget module

modules load hackertarget

options set source

target = hackxor.net

dashboard

recon-web

discovery/info_disclosure/interesting_files

Shodan

https://www.shodan.io/

https://securitytrails.com/blog/top-shodan-dorks

Shodan Basic Filters:

https://www.shodan.io/search/filters

https://www.shodan.io/search/examples

product:Apache
country:BR
city:"São Paulo"
hostname:domain.com
ip:8.8.8.8
net:
os:"windows 7"
port:22
has_vuln:
geo:"51.5074, 0.1278"
vuln:CVE-2014-0160

Examples Shodan Dorks:
"port: 53" Recursion: Enabled
http.title:"Index of /"
"Authentication: disabled" port:445
"220" "230 Login successful." port:21
"Server: IP Webcam Server" "200 OK"
html:"DVR_H264 ActiveX"
mysql port:3306
PostgreSQL port:5432
proftpd port:21
openssh port:22
product:nginx port:8080
product:"Microsoft IIS httpd"

port:8291 os:"MikroTik RouterOS 6.45.9"
vsftpd 2.3.4 port:21
220 ProFTPD 1.3.3a Server (Debian) country:AR
remote desktop port:3389 os:"windows 7" country:"BR" city:"São Paulo"

Legacy Windows operating systems

1. os:"Windows 5.0" – Windows 2000; support ended in 2010.
2. os:"Windows 5.1" – Windows XP; support ended in 2014.
3. os:Windows 2003 – Windows Server 2003; support ended in 2015.
4. os:"Windows Vista"– Windows Vista; support ended in 2017.
5. os:Windows 2008 – Windows Server 2008; support ended in 2020.
6. os:"Windows 7" – Windows 7; support ended in 2020.
7. os:"Windows 8" – Windows 8; support ended in 2016.
8. os:Windows 2011 – Windows Home Server 2011; support ended in 2016.
9. os:"Windows 8.1" – Windows 8.1; support ended in 2018.
10. os:Windows 2012 – Windows Server 2012; support ended in 2018.

Shodan CLI
$ shodan init <paste your API key here>
$ shodan -h
$ shodan search webcam
$ shodan info
$ shodan myip
$ shodan count port:22 country:BR
$ shodan count apache
$ shodan domain website.com
$ shodan host <IP Address>
$ shodan search port:3389 country:"BR" city:"Sao Paulo"
$ shodan search hacked by
$ shodan honeyscore <IP Address>

Maltego

https://www.maltego.com/maltego-community/

Machines> Run Machine

2° Active Recon

Basic Tools = ping, traceroute, mtr, telnet

Become Secure and Anonymous (VPN, TOR, Proxys)

Stealth Active Recon TOR+Proxychains (Anonymizing)

Install TOR Proxychains
$ sudo apt update
$ sudo apt upgrade
$ sudo apt install -y tor proxychains
$ sudo apt autoremove

Configure Proxychains
$sudo vi /etc/proxychains4.conf
...
dynamic_chain
#strict_chain
...
defaults set to "tor"
#socket4 127.0.0.1 9050
socks5 127.0.0.1 9050

Start TOR Service
$ sudo systemctl start tor
$ systemctl status tor
$ curl ipinfo.io
$ proxychains curl ipinfo.io

Init Firefox via Proxychains
$ proxychains firefox https://bgp.he.net/
$ proxychains4 firefox https://whatismyipaddress.com

#Browsers TOR/Brave
https://www.torproject.org/download/

https://brave.com/pt-br/

https://www.dnsleaktest.com/

#Search Leaks via TOR
http://pwndb2am4tzkvold.onion/

#Proton Mail
https://proton.me/pt-br/mail

#OpenVPN Account Free

https://www.vpnbook.com/

https://openvpn.net/community-downloads/

# Install and configure OpenVPN
$ sudo apt -y install openvpn

$ sudo openvpn --client --config /home/dir-files/file.ovpn
$ curl ipinfo.io

Proxys
https://hidemy.io/en/proxy-list/

DNS Enumeration
$ locate dnsenum
$ dnsenum -h
$ proxychains dnsenum -f file.txt <website.com>

DNS Recon
$ proxychains dnsrecon -d website.com
$ proxychains dnsrecon -t crt -d website.com
$ proxychains dnsrecon -t bing -d website.com
$ proxychains dnsrecon -t std -d website.com -D /usr/share/wordlists/dnsmap.txt --xml dnsrecon.xml
$ proxychains dnsrecon -t brt -d website.com -n 1.1.1.1 -D /usr/share/wordlists/dnsmap.txt --xml dnsrecon.xml

Target Enumeration PortScan Nmap via Proxychains

Performing active reconnaissance involves enumeration, which is the process of gathering information about a target during a penetration test. The first step is to identify the target's internet-facing hosts, followed by a port scan to enumerate the services running on those hosts. Nmap is a popular tool for such scans, including SYN scans, TCP connect scans, UDP scans, and TCP FIN scans.

A SYN scan sends a TCP SYN packet to the target port and analyzes the response to determine if the service is listening. TCP connect scans use the operating system's networking mechanism to establish a full TCP connection, which may trigger alarms on intrusion detection systems. UDP scans are useful for enumerating services like DNS, SNMP, or DHCP, which use UDP for communication. TCP FIN scans send a FIN packet to the target port, and if no response is received, the port is considered open.

Host discovery scans help determine if a host is online and responding on a network. Nmap also provides six timing templates (-T 0-5) to dictate the aggressiveness of a scan, ranging from very slow for IDS evasion to very aggressive, which may overwhelm targets or miss open ports.

Enumeration techniques used in the information-gathering include:

- **Host Enumeration**: Performed internally and externally, it involves scanning the IP addresses of a target using tools like Nmap or Masscan.
- **User Enumeration**: Collects a list of valid users to crack credentials by manipulating the Server Message Block (SMB) protocol on a Windows network.
- **Group Enumeration**: Helps determine authorization roles in the target environment by enumerating SMB groups using the Nmap NSE script **smb-enum-groups**.
- **Network Share Enumeration**: Identifies systems sharing files, folders, and printers on a network using the Nmap **smb-enum-shares** NSE script.
- **Web Page Enumeration/Web Application Enumeration**: Maps the attack surface of a web application using Nmap's **http-enum** NSE script and other tools like Nikto.
- **Service Enumeration**: Identifies services running on a remote system, primarily through Nmap's port scanning functionality.
- **Enumeration via Packet Crafting**: Scapy, a Python-based framework, can be used to perform network reconnaissance through packet generation.

#Nmap Docs
https://nmap.org/book/man.html

https://www.codelivly.com/nmap-cheat-sheet

Nmap flag	Description
-sV	Attempts to determine the version of the services running
-p <x> or -p-	Port scan for port <x> or scan all ports
-Pn	Disable host discovery and scan for open ports
-A	Enables OS and version detection, executes in-build scripts for further enumeration
-sC	Scan with the default Nmap scripts
-v	Verbose mode
-sU	UDP port scan
-sS	TCP SYN port scan

Simple Host Enumeraton and Discovery LAN
$ sudo nmap -v scanme.nmap.org [Default Scan with Verbose Option]
$ sudo nmap -p ssh scanme.nmap.org [Port Scan via Name Service]
$ sudo nmap --dns-servers 1.1.1.1,9.9.9.9 scanme.nmap.org [Use Public DNS Servers]
$ sudo nmap -sn 192.168.0.0/24 [Ping Scan]
$ sudo nmap -Pn 192.168.0.0/24 [No Ping Scan, Basic Firewall Evasion]
$ sudo nmap -sn --traceroute website.com [Nmap Traceroute]
$ sudo nmap -A -T 4 scanme.nmap.org [Agressive Host Scan]
$ sudo nmap -p 1-65535 -T4 -A -v <IP Address Target> [Intense Scan All TCP Ports]
$ sudo nmap -sn -PR 192.168.0.1/24 [ARP Scan]
$ sudo nmap -sn --script broadcast-ping 192.168.0.1/24
$ sudo nmap --script http-headers,http-title scanme.nmap.org
$ sudo nmap --traceroute --script traceroute-geolocation scanme.nmap.org [Geolocation]

$ sudo nmap -sn --script hostmap-* <IP Address Target>
$ sudo nmap -p 443 --script http-grep nmap.org
$ sudo nping --tcp website.com

Ex Network IP Ranges 192.168.0.*, 192.168.0.0-255, 192.168.0.0./24
--exclude 192.168.0.1

Nmap Time Options
Paranoid = -T 0
Sneaky = -T 1
Polite = -T 2
Default = -T 3
Aggressive = -T 4
Insane = -T 5

Nmap Out Options
Normal Text = -oN
XML = -oX
Grep = -oG

Nmap Scripts

https://nmap.org/nsedoc/scripts/

$ ls -l /usr/share/nmap/scripts | grep ssh

$ sudo nmap --script-updatedb

$ sudo nmap -sV -p 21 --script=ftp-vsftpd-backdoor <IP Addres Target>

Types of Port Scanning Public Internet
$ proxychains nslookup website.com 1.1.1.1
$ sudo proxychains nmap -sn 203.0.113.0/24 [Discovery Hosts Network Scan]
$ sudo proxychains nmap -sS <IP Address> [Stealth Scan]
$ sudo proxychains nmap -sS -T1 <IP Address> [IDS Evasion]
$ sudo proxychains nmap -sT <IP Address> [TCP full Scan]
$ sudo proxychains nmap -sU -p 53 <IP Address> [UDP Scan]
$ sudo proxychains nmap -sV -p 21,80,443 <IP Address> [Port List + Version Service Detection Scan]
$ sudo proxychains nmap -sS -p 1024-65535 <IP Address> [Port Range Scan]
$ sudo proxychains nmap -O <IP Address> [OS Detection]
$ sudo proxychains nmap -Pn <IP Address> [Firewall ICMP Block Evasion]
$ sudo proxychains nmap -sC <IP Address> [Run Commons NSE Scripts]
$ sudo proxychains nmap -sV -p 80 --script=http-enum <Domain or IP Address> [Web Page Enumeration]
$ sudo proxychains nmap -sV -p 80 --script=http-methods <Domain or IP Address> [Supported Methods]
$ sudo proxychains nmap -sV --script=banner <IP Address> [Banner Grab]
$ sudo proxychains nmap -sV -p 139,445 --script=smb-enum-users <IP Address> [Samba User Enumeration]
$ sudo proxychains nmap -sn --script=dns-brute website.com [Subdomains Enumeration]
$ sudo proxychains nmap -Pn -v -p 22 --script=ssh-auth-methods <IP Address Target> [Scan SSH Authentication Methods]

FTP Server Anonymous Login

Enum4linux

Enum4linux is a great tool for enumerating SMB shares, vulnerable Samba implementations, and corresponding users. Example 10-14 shows the output of a detailed scan using Enum4linux

#enum4linux -v <IP_Traget>

Scapy

https://scapy.readthedocs.io/en/latest/introduction.html

https://github.com/The-Art-of-Hacking/h4cker/blob/master/python_ruby_and_bash

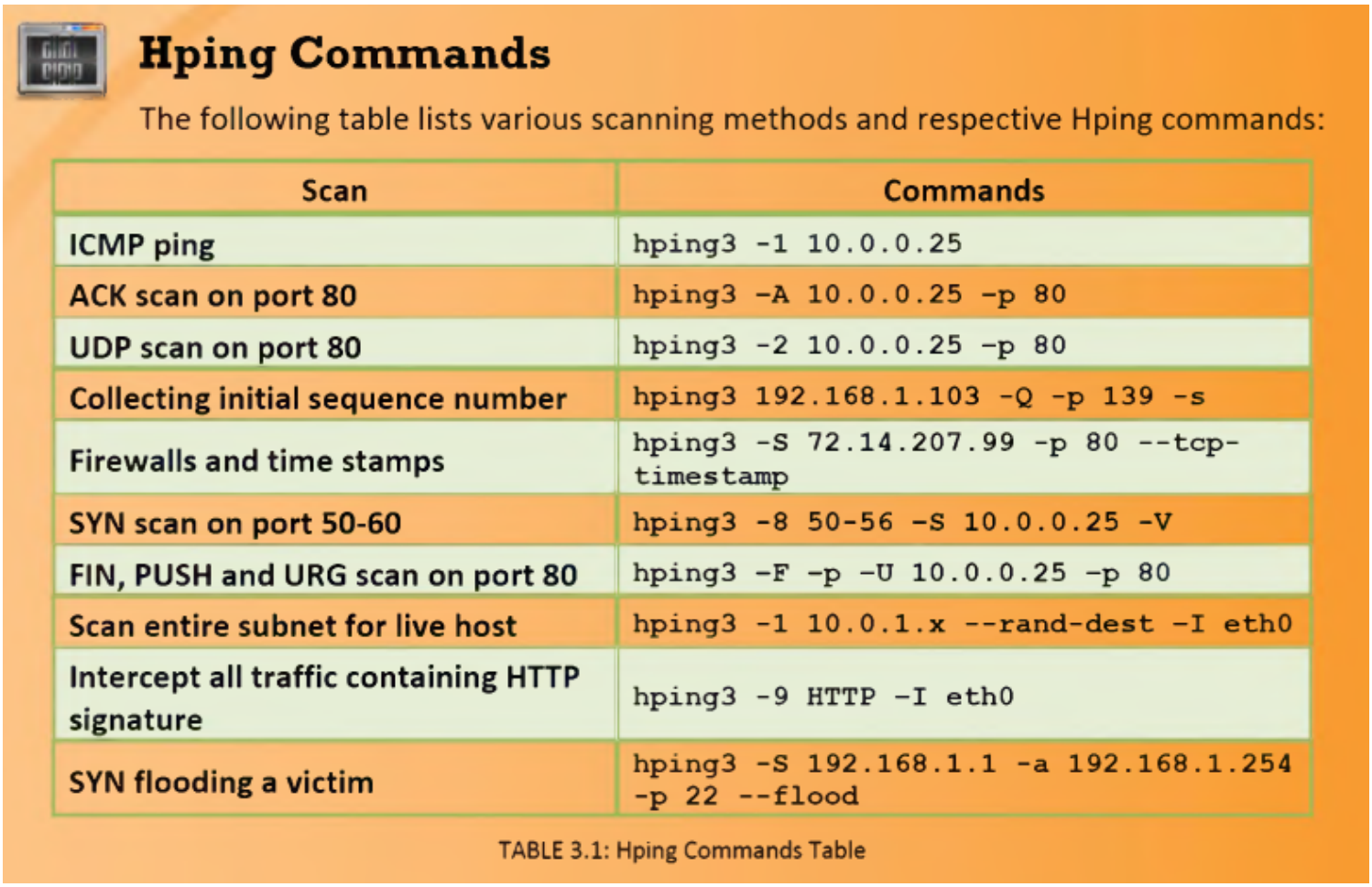
$ sudo su
# scapy
>>> ?
>>> ls()
>>> ls(IP)

Use Scapy to Sniff Network Traffic
>>> sniff()

$ ping -c 5 website.com

$ Crtl+c

Hping3



Hping Commands

The following table lists various scanning methods and respective Hping commands:

Scan	Commands
ICMP ping	hping3 -1 10.0.0.25
ACK scan on port 80	hping3 -A 10.0.0.25 -p 80
UDP scan on port 80	hping3 -2 10.0.0.25 -p 80
Collecting initial sequence number	hping3 192.168.1.103 -Q -p 139 -s
Firewalls and time stamps	hping3 -S 72.14.207.99 -p 80 --tcp-timestamp
SYN scan on port 50-60	hping3 -8 50-56 -S 10.0.0.25 -V
FIN, PUSH and URG scan on port 80	hping3 -F -p -U 10.0.0.25 -p 80
Scan entire subnet for live host	hping3 -1 10.0.1.x --rand-dest -I eth0
Intercept all traffic containing HTTP signature	hping3 -9 HTTP -I eth0
SYN flooding a victim	hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

TABLE 3.1: Hping Commands Table

Google Search = Do Not Scan These IP Addresses Table

Network Sniffing with Wireshark TCPDump

$ sudo tcpdump -i eth0 -s 0 -w packetdump.pcap

The -i command option allows you to specify the interface. If not specified, the tcpdump will capture all traffic on all interfaces.

The -s command option specifies the length of the snapshot for each packet. Setting this option to 0 sets it to the default of 262144.

The -w command option is used to write the result of the tcpdump command to a file. Adding the extension .pcap ensures that operating systems and applications will be able to read the file. All recorded traffic will be printed to the file packetdump.pcap in the home directory of the user.

Open packetdump.pcap with Wireshark
$ wireshark

Footprinting Countermeasures

Configure routers to restrict the responses to footprinting requests.

Lock the ports with suitable firewall configuration.

Evaluate and lim it the am ount of inform ation available before publishing it on the web_site/Internet and disable the unnecessary services.

Prevent search engines from caching a webpage and use anonymous registration services.

Configure web servers to avoid information leakage and disable unwanted protocols.

Use an IDS that can be configured to refuse suspicious traffic and pick up footprinting patterns.

Perform footprinting techniques and remove any sensitive information found.

Enforce security policies to regulate the information that employees can reveal to third parties.