Lab Module 02: Footprinting and Reconnaissance

Task 1: Perform Footprinting Through Search Engines

- Google Dorks

lab 2 Module 02: Perform Footprinting Through Internet Research Services

Task 1: Find the Company’s Domains, Subdomains and Hosts using Netcraft and DNSdumpster

- https://www.netcraft.com → resources → research tool → site report → domain
- dnsdumpster.com

Lab 3: Perform Footprinting Through Social Networking Sites

- sherlock: búsqueda por nombre en redes sociales

Lab 4: Perform Whois Footprinting

- https://whois.domaintools.com

Lab 5: Perform DNS Footprinting

Task 1: Gather DNS Information using nslookup Command Line Utility and Online Tool

- `nslookup`
  - ```
    set type=a # respuesta no autoritativa (no responde el servidor del dominio)
    <dominio>
    set type=cname # respuesta autoritativa
    ```
  - http://www.kloth.net/services/nslookup.php

Lab 6: Perform Network Footprinting

Task 1: Perform Network Tracerouting in Windows and Linux Machines

- `tracert <domain>` (windows)
  - -h : número de saltos máximos
- `traceroute <domain>` (Linux)
    ```

- https://www.pingplotter.com/
- https://www.solarwinds.com → traceroute NG

Lab 7: Perform Email Footprinting

Task 1: Gather Information about a Target by Tracing Emails using eMailTrackerPro

- eMailTrackerPro
- https://mxtoolbox.com/
- https://socialcatfish.com/
- https://www.ip2location.com

Lab 8: Perform Footprinting using Various Footprinting Tools

Task 1: Footprinting a Target using Recon-ng

- recon-ng

```
help
marketplace install all
modules search
workspaces [list]
workspaces create CEH
db insert domains
<domains>
show domains
modules load brute
modules load recon/domains-hosts/brute_hosts
run
back
modules load reverse_resolve
modules load recon/hosts-hosts/reverse_resolve
run
show hosts
back
modules load reporting/html
options set FILENAME /home/attacker/Desktop/results.html
options set CREATOR [your name]
options set CUSTOMER Certifiedhacker Networks
run
back

# información personal
workspaces create reconn
modules load recon/domains-contacts/whois_pocs
info command
options set SOURCE facebook.com

# información subdominios
modules load recon/domains-hosts/hackertarget
options set SOURCE certifiedhacker.com
```

```
run
```

Lab 9: Perform Footprinting using AI

Task 1: Footprinting a Target using ShellGPT

Ethical Hacker : shellgpt