CEH Lab - Mod2 - Footprinting and Reconnaissance

▼ Lab 1: Perform Footprinting Through Search Engines

Lab Objectives:

Organization Information:

Employee details, addresses and contact details, partner details, weblinks, web technologies, patents, trademarks, etc.

Network Information:

Domains, sub-domains, network blocks, network topologies, trusted routers, firewalls, IP addresses of the reachable systems, the Whois record, DNS records, and other related information

System Information:

Operating systems, web server OSes, location of web servers, user accounts and passwords, etc.

intitle:login site:eccouncil.org

Searches for login pages of target organization’s website

EC-Council filetype:pdf ceh

Searches for EC-Council, filetype of PDF, name containing CEH

May provide sensitive information about the target's products and services

Search Operator	Purpose
[cache:]	Displays the web pages stored in the Google cache
[link:]	Lists web pages that have links to the specified web page
[related:]	Lists web pages that are similar to the specified web page
[info:]	Presents some information that Google has about a particular web page
[site:]	Restricts the results to those websites in the given domain

Search Operator	Purpose
[allintitle:]	Restricts the results to those websites containing all the search keywords in the title
[intitle:]	Restricts the results to documents containing the search keyword in the title
[allinurl:]	Restricts the results to those containing all the search keywords in the URL
[inurl:]	Restricts the results to documents containing the search keyword in the URL
[location:]	Finds information for a specific location

▪ **filetype**: This operator allows you to search for results based on a file extension.

For Example, [jasmine:jpg] will provide jpg files based on jasmine.

▪ **source**: This operator displays information from a specific website in Google News.

For example, [Malware news source:"Hacker News"] returns articles from Hacker News containing the word "Malware".

▪ **phonebook**: This operator finds the residential and business phone numbers of a person or organization.

For example, [phonebook:Sundar Pichai] will provide Sundar Pichai's phone number.

▪ **before**: This operator filters search results to include only content published before a specified date.

For example, [ransomware before:2020-06-29] will give results about the ransomware that occurred before June 29, 2020.

▪ **after**: This operator finds information that was published after a certain date.

For example, [site:wikipedia.org after:2023-01-01 artificial intelligence] will retrieve Wikipedia articles about artificial intelligence published after January 1, 2023.

Footprinting Using Advanced Google Hacking Techniques *with AI*

ShellGPT can be used to perform the above tasks via a prompt in plain english:

“Use filetype search operator to obtain pdf files on the target website eccouncil.org and store the result in the recon1.txt file”

Google Hacking Database

Focuses on using Google search queries (often referred to as "Google Dorks") to find sensitive information inadvertently exposed on the web

- Sensitive files, database dumps, log files
- Exposed directories
- Error messages
- Vulnerable devices / software versions

SearchSploit: a command-line search tool for Exploit-DB that allows taking a copy of the Exploit database for remote use

Useful for security assessments of segregated or air-gapped networks without internet access

VPN Footprinting through GHDB:

Google Dork	Description
inurl:"/sslvpn_logon.shtml" intitle:"User Authentication" "WatchGuard Technologies"	Finds pages containing login portals
inurl:/sslvpn/Login/Login	Finds VPN login portals
site:vpn.*.*/ intitle:"login"	
inurl:weblogin intitle:("USG20-VPN"|"USG20W-VPN"|USG40|USG40W|USG60|USG60W|USG110|USG210|USG310|USG1100|USG1900|USG2200|"ZyWALL110"|"ZyWALL310"|"ZyWALL1100"|ATP100|ATP100W|ATP200|ATP500|ATP700|ATP800|VPN50|VPN100|VPN300|VPN000|"FLEX")	Finds hosts with the Zyxel hardcoded password vulnerability
intext:Please Login SSL VPN inurl:remote/login intext:FortiClient	Finds Fortinet VPN login pages
site:vpn.*.*/ intext:"login" intitle:"login"	Retrieves various VPN login pages
intitle:"index of" /etc/openvpn/	Retrieves juicy information and sensitive directories
"-----BEGIN OpenVPN Static key V1-----" ext:key	Finds OpenVPN static keys
intitle:"index of" "vpn-config.*"	Retrieves juicy information about the vpn-config file
Index of / *.ovpn	Finds OpenVPN configuration files, some certificates, and keys
inurl:"/vpn/tmindex.html" vpn	Finds Netscaler and Citrix Gateway VPN login portals
intitle:"SSL VPN Service" + intext:"Your system administrator provided the following information to help understand and remedy the security conditions:"	Finds Cisco Adaptive Security Appliance (ASA) login web pages

Table 2.1: Google search queries for VPN footprinting

Footprinting through SHODAN Search Engine

Used to detect devices and networks with vulnerabilities.

- VPN and VoIP related information

Meta Search engines

- Startpage, MetaGer, and eTools.ch

FTP search engines

- NAPALM FTP Indexer, FreewareWeb FTP File Search, Mamont, Globalfilesearch.com
- https://filezilla-project.org - Client that can access FTP accounts

Google Dork	Description
site:.in | .com | .net intitle:"index of" ftp	Finds files containing juicy information
intitle:"index of" "*/ftp.txt"	
intext:"index of" "ftp"	
inurl:WS_FTP.log	
intitle:index.of /cftp /robots.txt	
intitle: "Index of ftp passwords"	Finds files containing passwords
inurl: /ftp intitle:"office"	Detects the web server
inurl:/web-ftp.cgi	Finds pages containing login portals
site:sftp.*.*/ intext:"login" intitle:"server login"	
intitle:"Index of" ws_ftp.ini	Finds the "ws_ftp.ini" file, which contain usernames and passwords of FTP users
inurl:ftp -inurl:(http|https) intext:"@gmail.com" intext:subject fwd|confidential|important|CARD|cvv	Finds archived email conversations, at times revealing full credit-card numbers and customer information as well as private company emails
allintitle:"CrushFTP WebInterface"	Detects various pages of CrushFTP WebInterface, which includes login portals as well password reset/recovery page
"ws_ftp.log" ext:log	Finds sensitive directories
intitle:"Monsta ftp" intext:"Lock session to IP"	Shows websites that use the FTP service of Monsta FTP
"index of" /ftp/logs	Finds potential log files
intitle:"index of" inurl:ftp intext:admin	Lists admin folders on FTP servers

Table 2.2: Google search queries to find FTP servers

IoT search engines

- Shodan, Censys, and ZoomEye

▼ Lab 2: Perform Footprinting Through Internet Research Services

Lab Objectives:

Find the Company's Domains, Subdomains, and Hosts using **Netcraft** and **DNSdumpster**

Netcraft:

1. Navigate to https://www.netcraft.com
2. Resources → Research Tools → Site Report
3. Search target domain

Can see **Background, Network, Hosting History**

4. Under 'Network', click website link in Domain field to view **subdomains/netblock/OS information**

Find DNS Servers along with Geo IP and domain mapping:

DNS Dumpster:

1. Navigate to https://dnsdumpster.com/
2. Search target domain

View the list of DNS Servers, MX Records, Host Record (A)

3. 'Download .xlsx of Hosts' to export to Excel sheet

Displays Hostname, IP, Reverse DNS, Netblock owner, COuntry, HTTP / Title, etc.

Additional Tools:

Pentest-Tools Find Subdomains (https://pentest-tools.com), to identify the domains and subdomains of any target website

▼ Lab 3: Perform Footprinting Through Social Networking Sites

Lab Objective:

Gather personal information from various social networking sites using **Sherlock**

1. Login to Parrot VM
2. In cmd - ***sudo su*** → ***cd sherlock***
3. Syntax: ***sherlock <"name">***

Social Searcher (https://www.social-searcher.com) to gather additional information related to the target company and its employees from social networking sites.

▼ Lab 4: Perform Whois Footprinting

Provides target domain information such as the owner, its registrar, registration details, name server, contact information, etc

Lab Objective:

Perform Whois lookup using DomainTools
http://whois.domaintools.com

You can also use other Whois lookup tools such as **SmartWhois** (https://www.tamos.com), **Batch IP Converter** (http://www.sabsoft.com), etc. to extract additional target Whois information.

▼ Lab 5: Perform DNS Footprinting

DNS zone data include DNS domain names, computer names, IP addresses, domain mail servers, service records, etc.

Lab Objective:

Gather DNS information using nslookup command line utility and online tool

nslookup:

1. In cmd - run ***nslookup*** **(Note:** This specifies that the result was directed to the default server hosted on the local machine (Windows 11) that resolves your requested domain)
2. ***set type=a*** - Queries IP address of given domain
3. Type target domain
4. To find authoritative name server - ***set type=cname*** → type target domain
5. Now to find IP of name server - change ***set type=a*** → type target name server (ex. ns1.bluehost.com)

The authoritative name server stores the records associated with the domain. So, if an attacker can determine the authoritative name server (primary name server) and obtain its associated IP address, he/she might attempt to exploit the server to perform attacks such as DoS, DDoS, URL Redirection, etc

To use **online nslookup interface**:

http://www.kloth.net/services/nslookup.php

▼ Lab 6: Perform Network Footprinting

Next task is to perform network footprinting to gather the network-related information of a target organization such as network range, traceroute, TTL values, etc. This information will help you to create a map of the target network and perform a man-in-the-middle attack

Lab Objectives:

Perform network tracerouting in Windows and Linux Machines

Network Tracerouting in Windows and Linux Machines

tracert /?

Shows tracert flags and parameters

PingPlotter (https://www.pingplotter.com/)

Traceroute NG (https://www.solarwinds.com),
etc. to extract additional network information of the target organization.

▼ Lab 7: Perform Email Footprinting

To find email headers:

> In Gmail, find the email header by following the steps:
>
> - Open an email; click the dots (**More**) icon arrow next to the **Reply** icon at the top-right corner of the message pane.

> - Select **Show original** from the list.
> - The **Original Message** window appears in a new browser tab with all the details about the email, including the email header

> In Outlook, find the email header by following the steps:
>
> - Double-click the email to open it in a new window
> - Click the **... (More actions)** icon present at the right of the message-pane to open message options
> - From the options, click **View**
> - The **view message source** window appears with all the details about the email, including the email header

eMailTrackerPro:

1. My Trace Reports
2. Trace Headers → New Email Trace → Trace email I have received
3. Copy/Paste email header

MxToolbox (https://mxtoolbox.com/)

Social Catfish (https://socialcatfish.com/)

IP2Location Email Header Tracer (https://www.ip2location.com/)

▼ Lab 8: Various Footprinting tools (recon-ng)

Lab Objectives:

Footprinting a target using Recon-ng

Network Recon with recon-ng

cd into the correct directory

1. Run ***recon-ng***
2. Run help command to view all the commands that allow you to add/delete records to a database, query a database, etc.
3. Run ***marketplace install all*** command to install all the modules available in recon-n (ignore errors while running the command)
4. ***modules search*** displays all modules available in recon-ng
5. Run ***workspaces*** command to view the commands related to the workspaces
6. Create a workspace in which to perform network reconnaissance:
    a. ***workspaces create <workspace name>***
7. ***workspaces list*** - displays list of workspaces present
8. Add a domain in which you want to perform network recon:
    a. ***db insert domains***
    b. **domain (TEXT):** <input website here> (certifiedhacker.com)
    c. **notes (TEXT):** optional
9. Domains added can be viewed with ***show domains***
10. Harvest host related info by loading network reconnaissance modules such as brute_hosts, Netcraft, and Bing:
    a. ***modules load brute*** - shows all modules related to brute forcing
11. To load module: ***modules load <module-name> (modules load recon/domains-hosts/brute_hosts)***
12. ***Run*** to run the module
    a. Observe that hosts will be added
13. Use ***back*** command return to previous terminal

14. To resolve hosts using the bing module
    a. ***modules load recon/domains-hosts/bing_domain_web → run***

15. Perform a reverse lookup for IP address obtained during recon process:
    a. ***modules load reverse_resolve -*** View all modules associated with ***reverse_resolve*** keyword
    b. ***modules load recon/hosts-hosts/reverse_resolve → run***
    c. Run ***show hosts -*** displays all hosts harvested so far
16. Create report of hosts:
    a. ***modules load reporting***
    b. ***modules load reporting/html***
    c. Assign values for CREATOR and CUSTOMER, set FILENAME and filepath:
        i. ***options set FILENAME /home/attacker/Desktop/results.html***
        ii. ***options set CREATOR <name>***
        iii. ***options set CUSTOMER <name>***

Personnel Info Gathering with recon-ng

1. ***workspaces create <workspace name>***
2. Set a domain: ***db insert domains***
3. Specify a domain
4. ***modules load recon/domains-contacts/whois_pocs -*** uses the ARIN Whois RWS to harvest POC data from Whois queries for the given domain
5. Run ***options set SOURCE <domain>***
6. ***Run***

Subdomain and IP Gathering with recon-ng

1. ***modules load recon/domains-hosts/hackertarget***
2. ***options set SOURCE <domain>***

▼ Lab 9: Perform Footprinting using AI

Lab Objectives:

Footprinting a target using ShellGPT

bash sgpt.sh to configure shell gpt if necessary

Harvesting emails pertaining to a target organization:

sgpt --chat footprint --shell "Use theHarvester to gather email accounts associated with 'microsoft.com', limiting results to 200, and leveraging 'baidu' as a data source"

Perform footprinting through social networking sites:

sgpt --chat footprint --shell "Use Sherlock to gather personal information about '<individual's name>' and save the result in recon2.txt"

Run ***ls*** to view contents of working directory

Run ***pluma <filename.txt>*** to view contents

Perform website footprinting using ShellGPT:

sgpt --chat footprint --shell "Footprint the target website www.certifiedhacker.com and save the result in website_footprint.txt"

Run ***pluma website_footprint.txt*** to view contents

Gather a word list from specified website:

sgpt --chat footprint --shell "Use cewl to gather a wordlist from the target website https://www.certifiedhacker.com and save the result in recon4.csv file"

Navigate to **/home/attacker** location and open **recon4.csv**

Perform website mirroring:

sgpt --chat footprint --shell "Use website mirroring tool to clone the target website www.certifiedhacker.com"
Navigate to **/home/attacker/www.certifiedhacker.com** and double-click **index.html** file to view the cloned website

Perform DNS lookup using ShellGPT:

sgpt --chat footprint --shell "Install and use DNSRecon to perform DNS enumeration on the target domain www.certifiedhacker.com"

Traceroute target:

sgpt --chat footprint --shell "Perform network tracerouting to discover the routers on the path to a target host www.certifiedhacker.com"

Python script to automate footprinting tasks:

sgpt --chat footprint --shell "Develop a Python script which will accept domain name microsoft.com as input and execute a series of website footprinting commands, including DNS lookups, WHOIS records retrieval, email enumeration, and more to gather information about the target domain"