Ecole Supérieure d'Informatique et du Numérique
COLLEGE OF ENGINEERING & ARCHITECTURE

- Lab 01: FootPrinting and reconnaissance
- Nom de l'enseignant : Pr Anass Sebbar
- Niveau : 4th Year Cybersecurity Track

Lab n° 01
FootPrinting and reconnaissance

1- Objective :

The purpose of this lab is to provide hands-on experience with various footprinting and reconnaissance techniques, helping students understand how attackers gather information about a target before launching an attack.

Lab Outline :

- Part 1: Footprinting Through Search Engines, Web Services, and Social Networking Sites
- Part 2: Footprinting Using WHOIS, DNS, Network Footprinting, and Website Analysis
- Part 3: Using Specialized Tools and Automating Footprinting

Instructions:

The lab report must be submitted one week after the lab session on the Moodle application by the deadline mentioned on the platform.
The lab work must be done individually in class, but the report is to be submitted in groups of up to 2 students. Lab groups must remain the same for all reports throughout the semester.

ATTENTION:

This work demonstrates some basic techniques that can be used to commit illegal acts. This is considered useful within the course to better understand the types of attacks that can be carried out on systems we aim to protect, BUT these tests should not be applied to real systems without written authorization.

Part 1: Footprinting Through Search Engines, Web Services, and Social Networking Sites

Description: This part focuses on passive footprinting using search engines, online services, and social media information. Participants will use search engines to identify useful information about a target domain, collect public data via web services, and discover social profiles through specialized tools.

Task: Using Network Diagnostic Tools for Footprinting

1. Finding the IP Address of a Domain

1. Open Command Prompt or PowerShell on Windows.
2. Type the following command to find the IP address of `www.certifiedhacker.com`:

   ```
   ping www.certifiedhacker.com
   ```

   Results:

   ```
   Reply from 162.241.216.11: bytes=32 time=160ms TTL=40
   ```

   - The response may vary depending on your environment.

- What is the IP address of `www.certifiedhacker.com`?
- How long did it take for the packet to travel (time in milliseconds)?

2. Finding the Maximum Frame Size on the Network

1. Use the `-f` parameter to prevent packet fragmentation and `-l` to set the frame size:

   ```
   ping www.certifiedhacker.com -f -l 1500
   ```

2. If the output indicates that the packet needs to be fragmented, reduce the frame size until the command works. For example:

   ```
   ping www.certifiedhacker.com -f -l 1472
   ```

- What is the maximum frame size supported by your network?

3. Investigating TTL (Time to Live)

1. Ping `www.certifiedhacker.com` with a low TTL value to observe its effect:

   ```
   ping www.certifiedhacker.com -i 3
   ```

   Results `: TTL expired in transit.`

   - This means the router discarded the packet since TTL reached 0.

- What does TTL represent in networking?

- Why is TTL important in packet routing?

4. Tracing the Route to a Domain

1. To determine the path packets take to reach `www.certifiedhacker.com`, type:

```
tracert www.certifiedhacker.com   # For Windows
traceroute www.certifiedhacker.com # For Linux
```

2. Observe the hops taken by the packet to reach the destination.

- How many hops does it take for the packet to reach `www.certifiedhacker.com`?
- What information does each hop provide?

5. Checking the Life Span of the Packet

1. Set the TTL value to gradually observe the packet's journey:

```
ping www.certifiedhacker.com -i 2 -n 1
ping www.certifiedhacker.com -i 3 -n 1
```

2. Repeat with higher values until the destination IP responds.

- At what TTL value did you receive a response from the target?
- How does this value correlate with the number of hops found in the traceroute?

6. Using nslookup for DNS Information

1. Open Command Prompt or PowerShell and start `nslookup`:

```
nslookup
```

2. Set the query type to `A` and look up the target domain:

```
> set type=a
> www.certifiedhacker.com
```

3. To find the authoritative name server:

```
> set type=cname
> certifiedhacker.com
```

- What is the IP address of `www.certifiedhacker.com`?
- What is the primary name server for the target domain?

7. Using nslookup to Find the Authoritative Name Server's IP Address

1. Set the type to `A` to find the IP address of the primary name server:

```
> set type=a
> ns1.bluehost.com
```

- What is the IP address of the primary name server (`ns1.bluehost.com`)?
- Why is the authoritative name server important for DNS resolution?

Tasks2:

1. **Footprinting Through Search Engines:**
    - Use Google to perform advanced searches (Google Dorking):
        - Find PDF documents related to the target domain:
          `site:certifiedhacker.com filetype:pdf`
        - Locate login portals of the target website:
          `site:certifiedhacker.com inurl:login`
        - Search for email addresses:
          `site:certifiedhacker.com "@certifiedhacker.com"`
2. **Footprinting Through Social Networking Sites:**

Syntax: **`theharvester -d [domain] -l [amount of depthness] -b [search engines] -f [filename]`**

- Example which scans google.com and returns 500 results while searching in all available search engines

```
theharvester -d google.com -l 500 -b all
```

- Same example as above, but this one outputs all gathered information to an HTML file

```
theharvester -d google.com -l 500 -b all -f results.html
```

- Use `theHarvester` to collect social media and email addresses:

```
theHarvester -d certifiedhacker.com -l 300 -b google
```

This will search Google for the first 300 mentions of the target domain, extracting emails and hostnames.

Go to these Github repository then interpret and analyze the content :

- https://github.com/jakejarvis/awesome-shodan-queries
- https://github.com/opsdisk/pagodo/

Reply to these questions when you do the report (please for each capture you need to interpret the result):

1. **Which Google search operator was the most effective for finding potentially sensitive information?**
2. **What social media information did you find that could be used for social engineering?**
3. **What kind of data did you collect from Shodan, and how might it be used by an attacker?**

Part 2: Footprinting Using WHOIS, DNS, Network Footprinting, and Website Analysis

Description: In this part, participants will gather domain registration information, DNS records, network details, and website configurations to gain a deeper understanding of the target's infrastructure.

Tasks 1:

1. **WHOIS Footprinting:**
   - Use the `whois` command to gather information about the target domain:

     ```
     whois certifiedhacker.com
     ```

   - Document the registrar, administrative contacts, and nameservers.
2. **DNS Footprinting:**
   - Use `dig` to gather all DNS records of the target domain:

     ```
     dig certifiedhacker.com any
     ```

   - Use `nslookup` to identify the nameservers of the domain:

     ```
     nslookup -type=ns certifiedhacker.com
     ```

3. **Network Footprinting:**
   - Perform a basic network scan using `nmap` to identify open ports and services:

     ```
     nmap -sV certifiedhacker.com
     ```

   - Run an OS detection scan:

     ```
     nmap -O certifiedhacker.com
     ```

4. **Website Footprinting:**
   - Use `wget` to mirror the website:

     ```
     wget -r -l 1 certifiedhacker.com
     ```

   - Scan the target web server for vulnerabilities using `Nikto`:

     ```
     nikto -h certifiedhacker.com
     ```

Reply to these questions when you do the report (please for each capture you need to interpret the result):

1. **What useful information did you obtain from the WHOIS lookup, and how might it be leveraged in an attack?**
2. **What did the DNS footprinting reveal about the target's infrastructure?**
3. **What vulnerabilities were identified with `Nikto`, and what measures could be taken to mitigate them?**

Task2:

Exercise 1: DNS Information Gathering Given a domain, example.com, use online tools to determine its IP address, Mail Exchange (MX) records, and Name Server (NS) records.

Exercise 2: Google Dorking Find a way to search for PDF files related to cybersecurity on a domain sampledomain.com using Google.

Exercise 3: Directory Discovery Given a website http://testwebsite.com, use tools to find hidden directories or files.

Exercise 4: Email Harvesting What tool in Kali Linux can be used to gather emails associated with a domain, and how would you use it for the domain **somedomain.com**?

Exercise 5: Server Analysis You find that a website **http://webdomain.com** runs on an Apache server. Using Kali Linux, how would you scan this server for potential vulnerabilities?

Part 3: Using Specialized Tools and Automating Footprinting

Objective: Develop a shell script to automate several footprinting and reconnaissance tasks using the tools available in Kali Linux.

Instructions:

1. **DNS Analysis:** a. Write a command to extract DNS information for the target domain. b. Save this information in a file named `dnsenum_result.txt`.
2. **Subdomain Search:** a. Find all subdomains associated with the target domain. b. Save these subdomains in a file called `sublist3r_result.txt`.
3. **Nmap Scan:** a. Perform a quick scan of the target domain to identify open ports. b. Save the results in a file named `nmap_result.txt`.
4. **Web Server Scan with Nikto:** a. If the target domain has a web server, scan it with Nikto to identify any potential vulnerabilities. b. Save the results in a file called `nikto_result.txt`.
5. **Organize Results:** a. Create a directory with the name of the target domain to organize all the result files.
6. you can add other tools into you script.

Questions:

1. What command would you use to extract DNS information for the target domain?
2. How would you save the subdomains to a file?
3. What is the Nmap command to perform a quick scan?
4. How do you direct the output of a command to a specific file in Linux?
5. How do you check if a directory exists, and if it doesn't, how do you create it?