OSINT and Recon

Importance of Recon

The first step in hacking

Gathering information about network and system architecture, like:

- Layout of network
- Type and number of devices
- Location of servers and other assets
- Network topology
- User accounts and permissions

> Anything that helps understand the network structure and how the different systems and devices are connected.

Example, through images posted online, the attacker might gather info on:

- Operating systems
- Apps installed
- Notes

How Hackers Breach Companies

Different Levels of Initial Access

Breach Forms

Searching through online forums for potential breached info on the target.

- **Dark Web Forum Dumps**
  Dark web dumps.
- **Discord/Telegram sales**
  Online sales on info.
- **RaaS Markets**

Other markets selling access.

- **Web Based Exploitation**
- **Phishing Campains**
- **0day**
- **Insider Threats**

Passive and Active Recon

Passive Information Gathering

Collects data without direct interaction with the target.

Active Information Gathering

Collects data with direct interaction with the target.

> This means that passive avoids detection, while active risks detection.

Attack Surface

In recon our job is to understand the **scope** of our attack, and the **potential vulnerabilities** that we might find.

You might also find **forgetten/unmaintained** infrastructure.

Typically focus on:

- **Domains/Subdomains**
- **IP-Ranges/ASNs/Network Services**

> We need to find all subdomains, ip addresses, network services, open ports...

Root Domains Enumeration

We should gather as much domains as possible to have a larger attack surface.

Each root domains boosts the chance of finding a vulnerability by 4 times.

- **Crunchbase**

  By finding the acquisitions of the target.
- **Trademarks**

  By googling "trademark".
- Using **chatgpt**
- Using **favicons**

  By using a favicon hash generator, and using that on shodan.
- Using **whois**

> You can defend against whois using whoisgaurd.

- Using **viewdns.info**

  By searching via email.
- **Reverse Whois**

  Does the whois and viewdns by itself.
- **TLD Hunt**

  Finds all available domains.

CIDR Recon

ASN

Autonomous System Number.

Manual Enumeration: http://bgp.he.net

Automated Enumeration: metabigor, ASNLookup, asnmap

Passive Subdomain Enumeration

- **Virustotal**

through relations
- **Github/Gitlab Subdomains**
- **Waybackurls**

Active Subdomain Enumeration

DNS Enumeration

NS Record:

- A records: IP address
- MX records: mail servers
- PTR records: reverse lookup
- CNAME records: link one to another
- TXT records: text data

DNS Brute Forcing:

- gobuster

Tech Stack Enumeration

- whatweb (web and tool)
- httpx (check live subdomains)
- wappalyzer (browser extension)
- wafw00f (for web app firewall)

Screenshotting Assets

Aquatone

pipe subdomains to it.

Subdomain Takeover

when a subdomain expires, while the cname is still pointing to it, the attacker would register the expired subdomain for himself, so the website would point to the attackers subdomain.

Google Dorking

- **site:<site>**
  Only stuff form the site.
  -<sub> to remove sub (-www to remove www)
- inurl:<sub>
  Only stuff with sub in the url (inurl:admin would find from site with admin in url)
- "<word>"
  would find sites with this word
- filetype:<filetype>
  pdf for example

Google Hacking DataBase

dorks.faisalahmed.me/#

Search Engine

Shodan

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

- **shosubgo**
- **smap**

Github Dorking

org:orgName "password"

trufflehog

OSINT

Holehe

A tool that takes in an email address and tries it on a large set of websites.

whatsmyname.app

website, takes in username and searches for it.

Sherlock

similar to whatsmyname, but tool.

Hunter.io

looks up emails in an organization.

Email Verification

- email-checker.net
- truemail.io
- email-format.com

Email Reputation

- apivoid

Breach Checks

- DeHashed
- Haveibeenpwned

Reverse Image Lookup

- images.google.com

Image EXIF data

- exiftool