

A decorative graphic on the left side of the slide, consisting of white lines and circles on a dark teal background, resembling a circuit board or a stylized tree structure.

# OSINT AND RECON

# Attacker's Methodology



Give me 6 hours to chop down a tree and I will spend the first 4 sharpening the axe. AL

# RECON

Systematic attempt to locate, gather, identify and record information about the target

## Passive Recon

(I can see you but you can't see me)

- ⑩ Open source Intelligence
- ⑩ Social engineering
- ⑩ Dumpster diving

## Active Recon

- ⑩ Scanning

# OSINT AND RECON WHY?

- Discover useful information from online, infrastructure and domain mapping
- Data collection from open sources (privacy)
- Different take depending on which side you come from
  - Penetration Tester
  - Red Teamer
  - Bug bounty Hunter
  - Investigator





## Phase I - External, Web, Online OSINT

- Nowadays, a number of web based resources can be leveraged and at times overwhelming
- Free, paid access and most have APIs
- Domain Infrastructure
  - [dnsdumpster.com](https://dnsdumpster.com)
  - [centralops.net](https://centralops.net)
  - [mxtoolbox.com](https://mxtoolbox.com)
  - [ultratools.com](https://ultratools.com)
  - [shodan.io](https://shodan.io)
  - [censys.io](https://censys.io)
  - [crt.sh](https://crt.sh)
  - [viewdns.info](https://viewdns.info)
  - search engines

## The Big Picture So far

- We have Domain Names, ASN, SPF, DMARC, DKIM, IP Ranges and a few services
- Network setup/ rough infrastructure of what we are attacking/ defending
- This is general Information, we need to use to further our directives
- Scaling and tactical OSINT

## Phase II - Pivoting

- Whois Data, reverse whois lookup
- theHarvester data
- Spider foot
- Gotcha.pw
- Haveibeenpwnd.com
- Hunter.io
- Hacked-emails.com
- Recon-ng

# SOCMINT

- Twitter, facebook usually
- Tinfoleak
- Tweets\_analyzer,

[https://github.com/x0rz/tweets\\_analyzer](https://github.com/x0rz/tweets_analyzer)

- Tracking people MITM style,

<https://github.com/boxug/trape>

<https://github.com/jivoi/awesome-osint>



## Phase III - Bug Bounty Hunters and Pen Testers

- Finding sub-domains for one or more domains
- Subdomain Enumeration
  - web resources
  - `git clone https://github.com/ZephrFish/AttackDeploy`
  - `git clone https://github.com/nahamsec/bbht`
  - `git clone https://github.com/nahamsec/lazyrecon`

## Phase IV – Internal, Offline Recon

- Internal security assessments
- Mapping internal infrastructures
- “our job as attackers is to map and understand your network better than you do”, Rob Joyce, Former TAO lead
- Routers, Servers, Workstations, Mobile devices etc.

- Internal Recon continued ...
- Nmap
  - `nmap -sSUV -top-ports=250 -T4 -v -O -version-light -traceroute -script=ms-sql-info,nbstat,smb-os-discovery,snmp-sysdescr -script-args snmpcommunity=public -oA network_map`
  - other service scans for ports 21, 22, 23(duh),25,53, 69,80,143,443,445 and others
- Scripting Languages
  - python, PowerShell, bash, Perl(yes), batch(I know)
- Different operating systems and devices Examples:
  - powerview from powersploit (windows)
  - sharphound/bloodhound (windows)
  - adrecon (powershell, windows)
  - bash for recon (\*nix)

# HOW TO DEFEND AGAINST OSINT-

- ✓ Firewalls
- ✓ Don't publish sensitive information
- ✓ Disable unnecessary services
- ✓ Prevent search engines from caching your web page
- ✓ Use anonymous registration services
- ✓ Configure web servers to avoid information leakage
- ✓ Carry out footprinting and remove sensitive information found

# HOW TO DEFEND AGAINST OSINT- CONTINUED

- ✓ Use TCP/IP and IPSec filters
- ✓ Configure IIS against banner grabbing
- ✓ Configure IDS to refuse suspicious connections and pick up on patterns
- ✓ Educate employees
- ✓ Encrypt and password protect sensitive information.

WELL, IT DEPENDS!!!