OSINT AND RECON

Daniel Craig

dannycraig@summitcl.com

github.com/secterug

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
  - centralops.net
  - mxtoolbox.com
  - ultratools.com
  - shodan.io
  - censys.io
  - crt.sh
  - 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
- Haveibeenpwnd.com

```
$ curl --insecure
https://haveibeenpwned.com/api/v2/breachedaccount/<email> | json_pp
```

- Hunter.io
- Hacked-emails.com
- Recon-ng

SOCMINT

- Twitter, facebook usually
- Tinfoleak
- 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(more on this in the next slide)

  - python, PowerShell, bash, Perl(yes), batch(I know)

Internal Recon Automation aka scripting

- It requires its own workshop / bootcamp
- 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

- Well, It depends