Recon (OSINT)

Thomas Quig

SIGPWNY

What is Recon

- Gathering information before an attack/pentest
- OSINT
  - Open Source Intelligence
  - Professional Term for Recon

Network Information (The Technical Part)

- IP addresses
  - Lots of ways to get this
  - What ports/local IPs are open on the IP you now have
    - nmap
    - Netkitten

Human Information

- This is easiest thing to learn
- Continuous username
  - Consistent usernames are easier to map a person
    - Misspellings
  - Profile pictures
  - Reverse image searching

Challenge Start

There is an existentialist, vexillology loving, totally not a robot, redditor who has been posting on r/uiuc and r/vexillology (5 months ago). Find him, don’t tell people if you find him.

An Actual Link

https://www.reddit.com/r/totallynotrobots/comments/b87iuo/this_man_who_is_undoubtedly_100_totally_not_a/ (short link https://bit.ly/2kohZEN)

One of these people is definitely a Human.

How do you find removed posts on reddit?

Literal CTF

Go out into the real world (siebel) and find some of the flags

Thank you very much

The next 3 slides have information about specific websites that you can use for specific challenges -- open them on your own computer if you’d like to browse them.

There is also a more in-depth version of this presentation here. See if it you’d like a reference.

Follow @Thomas_Quig on twitter ;) Find something about me I didn’t know/forgot was on the internet for 300 pts.

SIGPWNY

Reddit

- Reddit is a semi-anonymous website
  - Some people deanonymize themselves.
    - Ex. President Obama, u/Giga_Gamby
  - Some people deanonymize themselves accidentally
    - u/Badongschlong, Yours truly.
  - Everyone gets sloppy.
- If you look long enough, you can usually link someone to a different account
- Search techniques
  - https://www.reddit.com/wiki/search
  - Author:
  - Selftext:
  - Boolean Operators
  - Comments NOT included in searching on reddit.
- Believe it or not you can actually have profiles

Twitter

- Always check Twitter bios, they often give out information you may need.
  - Twitter has a location and an advanced
  - Twitter has an advanced search bar, but it also has extra parameters.
  - https://lifehacker.com/search-twitter-more-efficiently-with-these-search-opera-1598165519
  - from:@ vs to:@ vs @
  - near: and within:
  - since: , until: , before:
  - :) , :(, ? operator, all boolean operators
  - “” vs just typing it in
- Check who they are following, check who is following them
- LOOK FOR MENTIONS OF OTHER ACCOUNTS
  - The more accounts, the more information you can gather.

Youtube

- Youtube doesn’t allow you to search for comments, which makes makes finding information by comment searching difficult.
- Look for information that the channel left public. There is A LOT of it
  - Even if the discussion page is not visible, you can usually go there by adding /discussion at the end of the link.
- Youtube sends you the full banner image, not just the crop.
- About page
  - Often has EMAIL if the person was not paying attention on setup.
- Advanced search queries
  - Many are same as the other websites
  - https://tubularinsights.com/advanced-youtube-search-tips/