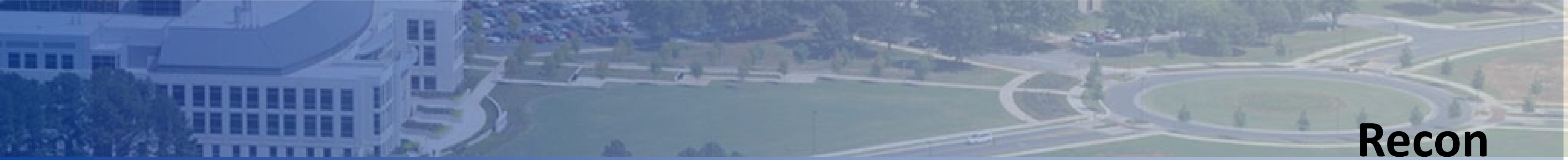
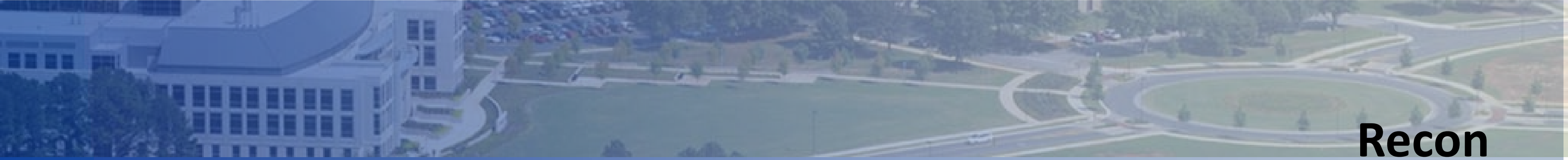


Phase 1: Recon

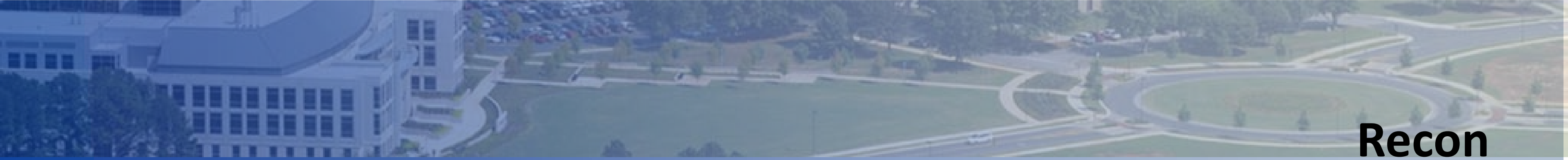
Using the Public Domain to Plan an Intrusion



Recon

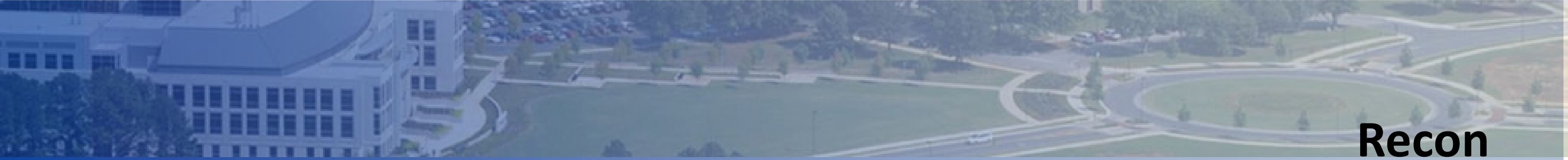
Who and why?

- Recon is a tool of the 3l1t3
  - Not script kiddies trolling the web for unpatched systems
- Like bank robbers
  - Visit the branch
  - Note security cameras
  - When do guards rotate, how are they armed?
  - What type of vault?



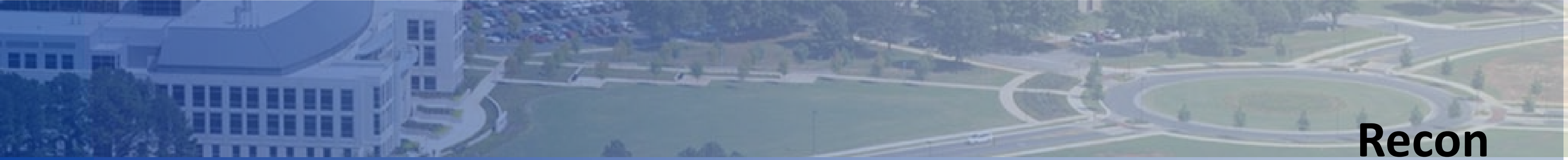
So what do they look for?

- Social Engineering
- Whois database analysis
- Information about staff
  - Social Networks and message boards
- Job ads
- DNS interrogation
- Google Hacks



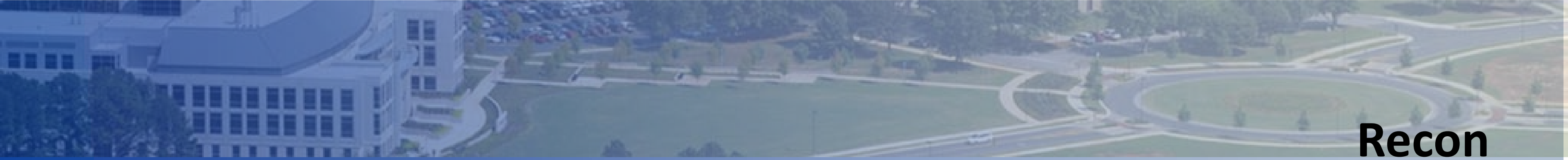
Social Engineering Greatest Hits

- Call the help desk
  - Hi, I’m new and I’m having some trouble finding any policy info on password complexity requirements…
- Call a user
  - Hi, I’m from IT security and I need to ask you a few things about your activity. We’ve seen some odd traffic and you could have a virus. Can I get you to check a few things…
  - Spoofing caller ID is trivial
- In person…
  - Hi, I’m from IT. We’ve got some extra new monitors, mice, and keyboards. Want one? (complete with keylogger)
- In the parking lot…
  - [unsuspecting user] Ah, somebody dropped their thumbdrive. I should look at what’s on it and maybe I can figure out who it belongs to.
- Dumpster diving – People throw away the darndest things - an oldie, but goodie



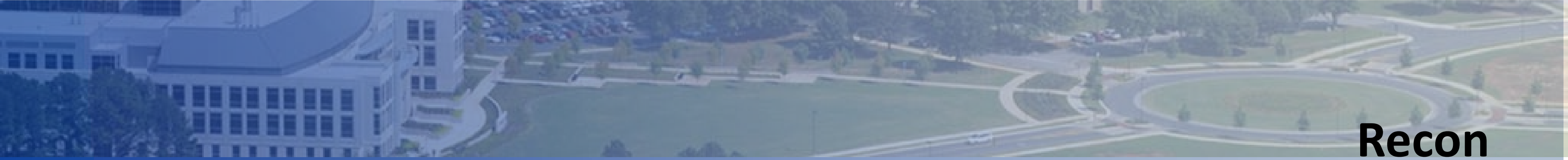
Search the Fine Web (STFW)

- Whois Database – www.whois.net
  - Contains Administrative and Technical POCs
    - LinkedIn? Facebook?
    - What are they're technical specialties?
    - Maybe I should call them posing as a recruiter? What would they tell me about themselves? What does that tell me about their network and systems?
  - Name servers with IPs
    - Now use www.arin.net to get assigned IP range
  - Email format
  - Physical address
  - Phone number format



Job Ads – quick hypothetical example

- Wanted: Network Administrator
  - Must have experience with Cisco Pix firewalls, IOS 5.3(x), knowledge of BGP. Linux, Window, Macintosh, s system administration experience a plus.
  - What do we know?
    - They're running an old firewall
    - Without having updated IOS
    - They're either very large, or manage their internet router
    - They're probably small because they like to double-up on duties
    - They run a mixed OS environment
    - Chances are, they don't have anyone watching their firewall right now

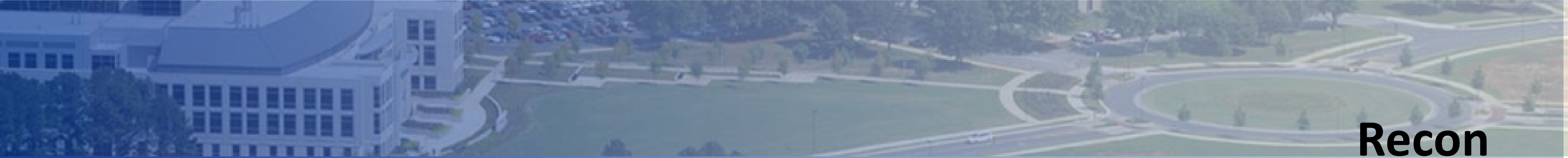


Phone Directories

- Here’s everyone in my organization’s…
  - Name
  - Office Phone
  - Email
  - Department
  - Title
    - Gold mine for social engineers – often first stop for spear-fishers

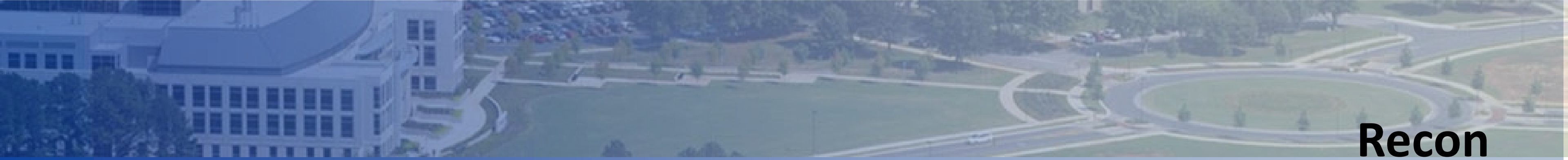
DNS Interrogation

- Zone Transfers
  - Nslookup - If your DNS is vulnerable, can provide attackers with:
    - System names
    - Do your system names indicate function? (ftp.uah.edu)
    - IP addresses
    - OS Types
  - $ dig @[IP address] [domain] –t AXFR
    - Command can perform zone transfers on modern linux (gets around limitations on nslookup)
  - Now we’ve got a list of targets and OS’s for some vulnerability scanning



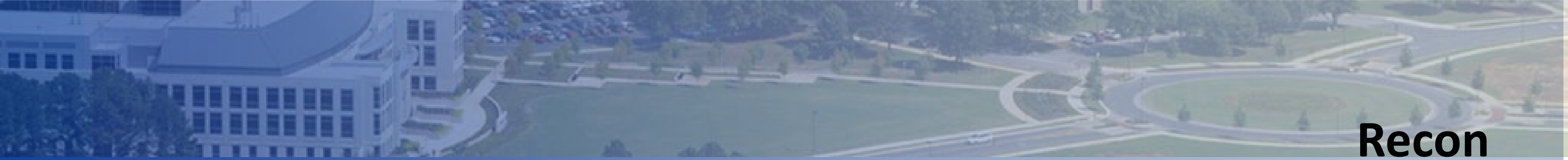
Google Hacks

- In an interview after being imprisoned, noted hacker Adrian Lamo was asked what his favorite hack tool was. He answered…Google.
- Google Directives – Maximize the precision of your searches
  - Site:[domain] – allows you to restrict your search to a specific domain
  - Link:[web page] – see everyone who links to a site…useful for identifying business relationships



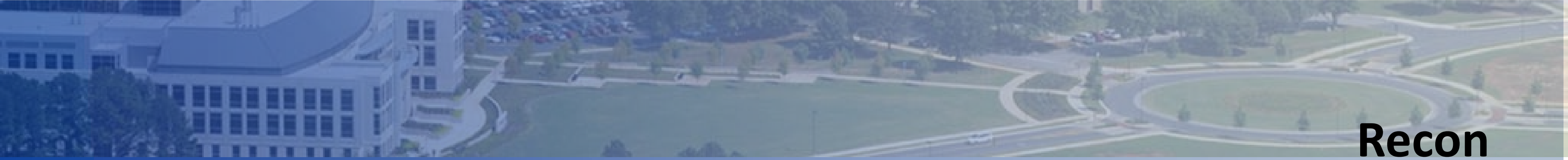
Google Hacks (Cont.)

- Intitle:[terms] – searching for “index of” can show you directory structure of web folders if developers forgot to put an index page
  - Any source code in there?
- Filetype:[suffix] – show me all the powerpoint files in your domain
- Literal matches (“ “) – searches for particular strings
- Up to 10 can be chained together
  - Site:somebigbank.com filetype:xls “ssn”
    - This will search all of Some Big Bank’s web content, searching for any Excel spreadsheets that have the abbriviation SSN in them.
    - You could use “cache:” to search older content that they’d removed, but google had crawled in in the recent past.



The Moral of the Story?

- Be careful what you put in the public domain!
- Check your DNS for vulnerability to Zone Transfers
- Restrict access to information that could be used against you
- Use these techniques on yourself and your organization – know what's there



Recon

Questions?