# Reconnaissance

Comp 199

# Admin

- No class/university Shut next Monday
  - Monday schedule on classes next Wednesday
- Current events
  - Greg/Jeffery presenting today
- Next Wednesdays presenters:
  - William and David
- Assignment update.

# Reconnaissance

- Process of discovering just what a target system is all about
  - Active Reconnaissance
    - Leaves traces with the target system
  - Passive Reconnaissance
    - Still active from your point of view
    - But no connections to target system

# The beginning

- Often pen testers are given nothing more than the name of the institution they are testing
  - Not always well known place
  - Find out all you can about this institution
  - Using first passive, then perhaps active techniques.
  - Where are you going to go for this?

# The beginning

- Often pen testers are given nothing more than the name of the institution they are testing
  - Not always well known place
  - Find out all you can about this institution
  - Using first passive, then perhaps active techniques.
  - Where are you going to go for this?
    - Keeping it passive
      - Web aggregators like google/wiki sites.
      - Then what?

# Now you know who you are after

- What do you want to know now?

# Now you know who you are after

- What do you want to know now?
  - Who runs their IT/sys admin group
  - What the infra structure is
  - What skills are they lacking
  - More?

# How do you find that out

- How can you find answers to those questions?
  - Who runs their IT/sys admin group

# How do you find that out

- How can you find answers to those questions?
  - Who runs their IT/sys admin group
    - Personnel websites on actual page
    - Linked in
    - Other social media?
    - etc

# How do you find that out

- How can you find answers to those questions?
  - What the infra structure is
  - What skills are they lacking

# How do you find that out

- How can you find answers to those questions?
  - What the infra structure is
  - What skills are they lacking
    - Job postings
      - Often list particular skills
      - Look at current BSU posting
    - Help requests on common sites
      - Professional clearinghouse sites and discussion lists often have really detailed information.

# Google-FU

- Using “Google-FU” is a great passive recon tool
  - Google directives
    - Site:
    - Filetype
    - Inurl/intitle/allintitle
  - Google cache
    - As long as you stay in the cache you are passive
    - Also preserve short lived mistakes.
  - Demo with stackover flow and bridgew.edu

# Reading

- Read Chapter 2 pg 15-26

# Admin

- Quizzes to return Thanksgiving week (we meet both days)
- Todays current events presenters.
- Papers and office hours.
- Monday's Presenters.
  - John and Jason

# Using theHarvester for subdomains

- Show demo

# Using netcraft

- Nice easy approach to finding some of the public facing technology.
- demo

# Discovering the servers

- So you have discovered who works at the target
  - And perhaps a little about their tech.
  - Now you want to learn what they have for servers
  - What is your first target?

# Discovering the servers

- So you have discovered who works at the target
  - And perhaps a little about their tech.
  - Now you want to learn what they have for servers
  - What is your first target?
    - Name servers? Web server? Email server?

# Name server

- How do you find the name server for your target?
  - We did it in passing last week.

# Name server

- How do you find the name server for your target?
  - We did it in passing last week.
    - Use whois
    - Should give the three name servers for the domain

# So you have the name servers

- How can you find the IP address for those name servers
  - Use the host command
  - Host <server name>
  - demonstrate

# Getting Name Servers to give up data

- Name servers have the complete map of names to IP addresses for their area.
  - Sometimes need to communicate that list to other name servers
  - Used to be that any server could pose as a DNS server
    - And main DNS would give all the info
    - “zone transfer”
    - Not so common now
    - Show using dig that BSU doesn't support this

# Email server

- How can we find out what the email server of the target is?
-
- How can we find information about the email server?

# Email server

- How can we find out what the email server of the target is?
  - Lets send an email to a bogus address
  - Happens all the time, nothing really unusual
- How can we find information about the email server?
  - Lets look at the returned email
  - What about potentially malicious files?

# Social engineering

- Refer to web article
  - Social engineering attacks the weakest link.
  - A couple of examples.

# Reading

- Finish reading chapter 2