# Anatomy of a Hack

Footprinting

# Description

- Goal: Research target
  - Find publicly available information
  - Find DNS information
  - Find IP address ranges
  - Etc
- This stage of hacking is non-intrusive
  - ie should not set off IDS or IPS

# Description

- Things to find:
  - Network information – try to diagram the network
  - Financial documents
  - Names & personal info of network administrators and other staff
  - Names & personal info of disgruntled employees (why?)

# Tools

- Google
- 411.com
- Whois
- Nslookup ls -d
- traceroute

# 411.com

- Basic personal info
  - Name
  - Address
  - Phone number
  - Phone provider
- Basic white page info

# Whois

- whois iseage.net
- Provides information about a domain name
  - DNS servers
  - Admins
  - Providers

# Nslookup ls -d

- Performs a zone transfer
- Sends a replication of the dns entries back to the requestor
- Allowing zone transfer from slave dns only
  - Secure method
  - Often not implemented

# Traceroute

- Discover the number and IP addresses of all the hops between the client and a specified destination

# Google Hacking

- [Directory String] can be any of the following :
  - "index of"
  - "last modified"
  - "parent of"

# Google Hacking

- [file type] can be any of the following :
  - "mp3"
  - "shn"
  - "wma"
  - "txt"
  - "doc"
  - "jpg"
  - etc

# Google Hacking

- [limitors]
  - -html
  - -htm
  - -php
  - -asp
  - -txt
- Example
  - -filetype:txt

# Google Hacking

- (inurl:) is optional and may be omitted and in fact must be omitted if not using a search tool other than google.
- (intitle:) can be used in place of (inurl:) and has a similar effect you must be using google.

# Google Hacking

- "robots.txt" "disallow:" filetype:txt
- "#-Frontpage-" inurl:administrators.pwd
- http://www.trinity.edu/jdunn/googlemusic.htn
- inurl:"ViewerFrame?Mode="
- http://johnny.ihackstuff.com/ghdb/?function=