Investigative Techniques

Dr. Carl Pulley
c.j.pulley@hud.ac.uk

Anatomy of an Attack

- 5 phases to an attack:
  - **Reconnaissance**
  - **Scanning** (see week 9)
  - **Gaining Access** (see weeks 7 and 10)
  - **Maintaining Access** (see weeks 7 and 11)
  - **Covering Tracks** (see week 12)

Reconnaissance

- Attacker gains as much information about a target as possible
  - **passive** reconnaissance
  - **active** reconnaissance

Passive Reconnaissance

- No direct interaction with the target system
  - **only** using publicly available information
  - internet searches
    - whois, google, 192.com, way back machine, news groups, social networks, etc.
  - dumpster diving

Domain Names

- Use host, dig or nslookup to grab A, CNAME, MX and TXT records for a domain
- Use whois to find contact/admin/billing information on a domain's owner
- Use GeoIP to locate the geographical location of a target system

Google Hacks

- Can learn a great deal about a target system by using a variety of Google *hacks*
  - http://johnny.ihackstuff.com/ghdb.php
  - +WS_FTP.LOG filetype:log
  - intitle:login
  - inurl:/tmp
- Use Google for anonymous web browsing!

192.com

- 192.com is a website that allows users to search:
  - electoral register
  - census records
  - birth, deaths and marriage records
  - telephone directory (land and mobile!)
  - company house data

Way Back Machine

- Way back machine can hold past copies of a target's web site
  - http://www.archive.org
- For example, can gleam:
  - previous administrators
  - server age and type
  - past configuration issues

Newsgroups

- Looking for technical queries that target staff may have raised
  - can gleam data about systems target uses
  - can profile technical proficiency of target technicians
  - can even get configuration data!

Social Websites

- Useful for getting data and interests about individuals
  - aids any future social engineering
- Example sites:
  - most past-times have a support forum!
  - FriendsReunited, MySpace, Facebook, etc.
  - dating sites!

Dumpster Diving

- Grabbing rubbish from external and internal (may need to get a part-time job!) bins
- Need to work out refuse collection day first!
  - use local government web site
- Looking for passwords, accounting data, user names, system information, etc.

Active Reconnaissance

- Interaction with target system, but a *low* risk of detection
  - limited port scans of networks
  - telephone calls or even visits to (for example) help desks or technical departments
  - social engineering of target staff (inside or outside of work)

Scanning

- Use reconnaissance data to target specific system vulnerabilities
  - traceroute
  - port scanning (eg. nmap), vulnerability scans (eg. nessus), banner grabbing (eg. telnet), etc.
  - map firewall rules (eg. firewalk) and network infrastructure