Lab 4. Information Gathering and Information Sniffing

What is Information Gathering?

- Information Gathering
  - Also known as Passive Attacks
  - Used for both hacking and security purposes
  - Hackers will use network information to gain illegal access
  - The Security administration will use to audit/test the security of the enterprise/network
    - Done with permission from the management
    - If weakness is spotted
    - Measures are taken to tighten the security

Oath of Sincerity

- Repeat After me

All the knowledge that I acquire from this course and the tools I learn, I solemnly swear I will use it only for ethical learning and practice purposes and will never cause any harm to anyone for fun

Ethical Hacking

- What does and Ethical Hacker do?
  - A security auditor possessing the same skills of that of a hacker.
  - Hacks the network under the consent of the management to identify security loopholes
  - Doesn’t exploit them but reports and recommends action plan to fix them
  - Operates on Networks, Servers and Other network devices

How is Hacking Realized?

- Generally, the hacker will hack after:
  - Locate the victim (host) by **foot printing** and **scanning**.
  - Once located, identify the vulnerability in the host
  - Exploit the vulnerabilities to unload the mayhem
  - Leave backdoors for revist
  - Robber-Home-Thinking-Security

What is Foot Printing?

- Foot printing simply, means:
  - AKA External Intrusion Techniques
  - Categorized into:
    - Passive
    - Active
  - Passive: Gathering Information through non-intrusive methods such as from related companies, website and other online resources.
  - Active: Gathering information through intrusive methods with the target network or computer.

Passive Techniques

- Tools and techniques used
  - Google, the biggest yet the most simplest and freely available hacking tool.
  - Lookup any organization in Google and you find
    - Location
    - Branches
    - Related sites

Next Steps- Going Technical

- Netcraft.com
  - Lookup a domain name and you find:
    - IP Address(s)
    - Registration Authority
    - Location of web server
    - Site Report
    - Background
    - Network
    - Technology/Platform being used

Other resources for foot printing

- Whois.net
  - Gives more useful information about the target
    - Contact person
    - Date of registration
    - Date of expiry or renewal
    - Contact Number
    - Address within organization

Online Resources … Contd

- Archive.org
  - Gives historical information about the target
    - How the victims website looked
    - Some real critical details can be found such as:
      - Name of web admin
      - Email of web admin
    - Hackers collect as much as information about target to disguise the active attacks

Online Network Tools

- Network-tools.com
  - To check the communication and response of the target site without relaying hackers information
    - Ping
    - Trace
    - Network Lookup
    - DNS Server
- http://www.nabber.org/projects/geotrace

Foot printing Software

- Active Whois:
  - http://www.johnru.com/download.html
- DNSDataView
  - http://www.nirsoft.net/utils/dns_records_viewer.html
- IDServe
  - https://www.grc.com/id/idserve.htm
- IP2Country
  - https://ip2country.jaleco.com/
- WebDataExtractor
  - http://www.webextractor.com/
  - http://www.emailtrackerpro.com/

Packet Sniffing using Wireshark

- Refer to students manual for exercise

Report Work

Download the Webdata extractor (link available in the slides) and track and email and provide the screen shot of the source country and ip address of any email from your inbox