IT3789 Cyber Security Attack & Defence

L5 – Information Gathering (1)

WITH KNOWLEDGE COMES RESPONSIBILITY

Information Gathering

Reconnaissance

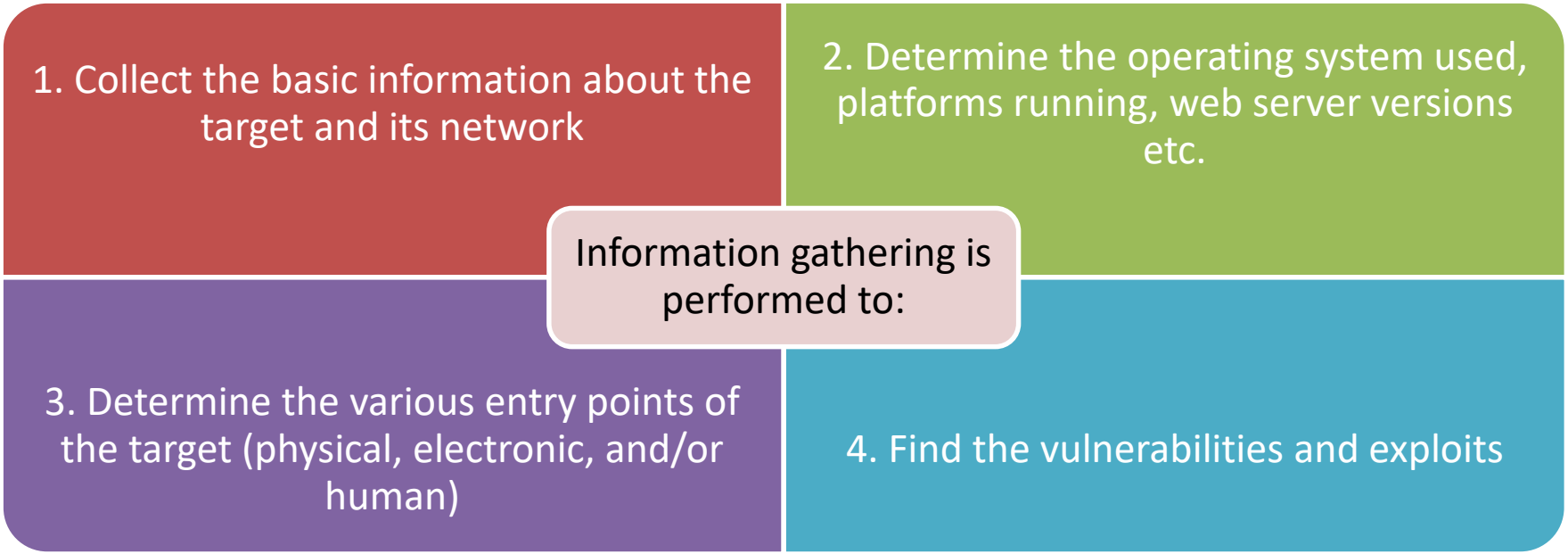
Passive Information Gathering

Active Information Gathering

Social Engineering

What is Information Gathering?

- Information gathering refers to uncovering and collecting as much information as possible about a target



Reconnaissance

- The attacker gathers information from public sources.
  - People and culture
  - Terminology
  - Technical infrastructure
- Identifying patterns of behaviour of people or system.
  - Aim is to find loopholes or flaws to exploit.
- Generally, a hacker spends 90% of the time profiling and gathering information on a target.

Reconnaissance Tools

- Whois databases
  - Offers information on registrar.
- Search the Fine Web
  - Through target's website, search engine etc.
- DNS Enumeration
  - Using nslookup and dig on Domain Name System.
- Low-Technology Reconnaissance
  - Social Engineering
  - Physical Break-in
  - Dumpster Diving

Information Gathering

Reconnaissance

Passive Information Gathering

Active Information Gathering

Social Engineering

Passive Information Gathering

- Gather information about a target without using any intrusive means, usually from publicly accessible sources
  - Focus on collecting information on systems that is not located in the target's network.
  - Most information that can be obtained publicly.
    - Examples
      - Company website
      - Company literature
      - Financial information
      - Partner sites
      - Job openings sites
    - Search for internet archive pages about the company
      - https://archive.org
- Very difficult to defend by target organisation.

Passive Information Gathering

- Examples of information obtained.
  - Name of company staffs
  - Address of locations
    - e.g. data centers
  - Partner networks and connections
  - Types of systems used
    - Firewalls, Intrusion Detection Systems (IDS), etc
  - Domain names
  - IP address spaces
- These information can be used to launch a social engineering attack.
  - e.g. Calling customer service dropping a few high level executives' name and mentioning a few technical details.

Competitive Intelligence

- A process of identifying, gathering analysing, verifying and using information about your competitors from publicly accessible sources
  - competitors' products, marketing and technologies.
- Tools for gathering competitive intelligence are available.
  - ACRA, https://www.bizfile.gov.sg
  - EDGAR Databases, https://www.sec.gov/edgar.shtml
  - ChangeDetect, http://www.changedetect.com
  - InfoTracer, https://infotracer.com
  - Google Alerts, https://www.google.com/alerts
- Hackers can use these tools to gather information about a target.

Footprinting

- The process of creating a map of network and systems of target organisation.
  - Determine target system, applications or physical location.
  - Information to look for is anything that gives clues to network architecture, server and application types.
- Part of preparatory pre-attack phase
  - Learn as much as possible about target systems.
    - Remote access?
    - Ports & services?
    - Security mechanisms?

Footprinting Tools

- Common tools for footprinting and information gathering.
  - Whois
  - Search engine such as Google.
  - Domain lookup
  - NSlookup
  - Sam Spade

Whois Databases

- The Internet Corporation for Assigned Names and Numbers (ICANN) requires registration of domain names.
  - To ensure only a single organisation uses a specific domain name.
  - Domain registrar will submit contact information about the individual or organisation that holds the domain registration.
  - Each registrar will maintain a Whois database.
  - A central registry Whois database is maintained by InterNIC.

Whois Lookup

- Whois databases contains:
  - Technical, administrative, and billing contact names
  - Phone numbers and e-mail addresses
  - Domain Name Servers
  - Other juicy tidbits
- Identifies who has registered domain names used for email or websites.
  - Kali, “whois” command
    - *whois <ip address/name of the website you want to access the information to>*
    - Example: whois nyp.edu.sg

Whois Lookup

Domain	
Status:	OK, VerifiedID@SG-Not Required
Created:	1996-07-15 00:00:00 +0000 (over 21 years ago)
Expires:	2018-07-15 00:00:00 +0000 (in 2 months)
Nameservers	
Name:	ns1.nyp.edu.sg
IPv4:	202.12.95.1, 2401:2f00:ffff:eeee::1
Name:	ns2.nyp.edu.sg
IPv4:	202.12.94.4, 2401:2f00:ffff:eeee::4
Name:	dnssec1.singnet.com.sg
IPv4:	165.21.83.11
Name:	dnssec2.singnet.com.sg
IPv4:	165.21.100.11
Name:	dnssec3.singnet.com.sg
IPv4:	165.21.100.11

Registrant:

Name: NANYANG POLYTECHNIC (SGNIC-ORG1422820)

Administrative Contact:

Name: KOK CHUEN WONG (SGNIC-PER20188585)

Technical Contact:

Name: FRANCIS LEE (SGNIC-PER20010362)
Email: francis_lee@nyp.edu.sg

Name Servers:
NS1.NYP.EDU.SG (202.12.95.1, 2401:2f00:ffff:eeee::1)
NS2.NYP.EDU.SG (202.12.94.4, 2401:2f00:ffff:eeee::4)
DNSSEC1.SINGNET.COM.SG (165.21.83.11)
DNSSEC2.SINGNET.COM.SG (165.21.100.11)
DNSSEC3.SINGNET.COM.SG (165.21.100.11)

Whois Lookup

- Some Whois web interfaces:
  - https://tools.whois.net
  - http://whois.online-domain-tools.com
  - https://www.ultratools.com/whois
  - http://www.internic.com/whois.html
  - http://www.networksolutions.com

Whois Reverse Lookups

- Whois can also perform reverse lookups.
  - Instead of input a domain name, IP address is used.
  - Result will usually include the whole network range which belongs to the organisation.

Search The Fine Web

- Search the web for interesting target information
- Information revealed include …
  - Business partner relationships
    eg. “We just launch a joint venture with …”
  - Contacts and addresses
    eg. “For more information, please call …”
  - Technology in use
    eg. “We use a Microsoft IIS Web Server with a back-end Oracle Database, tied together using…”
  - “Hidden” comments on webpages
  - “link:” option shows
    - Every site that links to the target
    - Business partners, suppliers, customers, etc

Google Hacking

- Google will violently crawl websites.
  - Expose sensitive information on that web site due to various web server misconfigurations (such as directory indexing, etc.)
  - Google can be used in creative ways to gather information.
- Google hacking was first introduced by Johnny Long.
- Google Hacking Database (GHDB)
  - http://www.hackersforcharity.org/ghdb/
  - http://www.exploit-db.com/google-dorks/

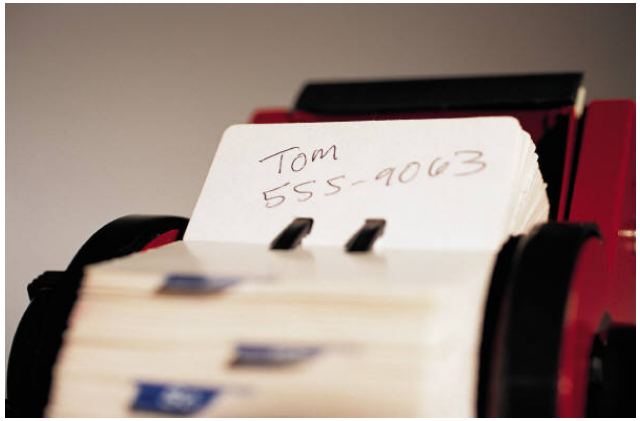
Google Search Operators

- The following operators can be used in the Google search engine.
  - Supply search term after a colon.
  - e.g. *application server site:oracle.com filetype:pdf*

Operators	Description
site	Searches a specific website or domain.
filetype	Search for a particular file type.
link	Searches within hyperlinks for a specific term.
cache	Identifies the version of a web page.
intitle	Searches for a term within the document title.
inurl	Searches only within the URL of a document.

Domain Name System

- DNS is a distributed hierarchical database
  - Maps domain name (www.google.com.sg) to IP address (74.125.235.17)
  - Most organisations have one or more DNS servers.
  - Each domain has at least one authoritative DNS server which publishes:
    - Information about that domain.
    - Name servers of any domains subordinate to it.



Domain Name System

- Any DNS server that contains a complete copy of the domain's zone file is considered to be authoritative for that domain only.
- A complete copy of a zone file must have:
  - A valid Start of Authority (SOA) record.
    - A special resource record included in every database file (also called zone files).
    - Supplies certain basic information about the zone.
  - Valid Name Server (NS) records for the domain.
- The zone file also contains all resource records for a domain.
  - Mappings between domain names and IP addresses.

Zone File Example

```
$TTL    86400 ; 24 hours could have been written as 24h or 1d
$ORIGIN example.com.
@  1D  IN        SOA ns1.example.com.   hostmaster.example.com. (
                              2002022401 ; serial
                              3H ; refresh
                              15 ; retry
                              1w ; expire
                              3h ; minimum
                             )
       IN  NS     ns1.example.com. ; in the domain
       IN  NS     ns2.smokeyjoe.com. ; external to domain
       IN  MX  10 mail.another.com. ; external mail provider
; server host definitions
ns1    IN  A      192.168.0.1  ;name server definition
www    IN  A      192.168.0.2  ;web server definition
ftp    IN  CNAME  www.example.com.  ;ftp server definition
; non server domain hosts
bill   IN  A      192.168.0.3
fred   IN  A      192.168.0.4
```

1. Two name servers are used one internal (ns1) and one external (ns2) to the domain.
2. The mail service is external to the domain (provided by a third party).
3. FTP and WWW services are provided by the same host.
4. There are two hosts named bill and fred.
5. The host addresses are all in the class C private address range 192.168.0.0.

NOTE: Both externally visible (public) services and internal hosts are defined in this file.

Domain Name System

- Besides resolving domain names into IP addresses, names servers also indicates useful information.
  - e.g. Indicating which machine is the mail server.
- DNS servers house a variety of different records.

Common DNS Record Types

- A: Address Record
  - Maps a domain name into IP address.
- SOA: Start of Authority Record
  - Indicates that a server is authoritative for that DNS zone.
- NS: Name Server Record
  - Indicates the name servers associated with a given domain.
- MX: Mail Exchange Record
  - Identifies the mail servers for a given domain.

Common DNS Record Types

- CNAME: Canonical Name Record
  - Indicates aliases and alternative names for a given host.
- PTR: Pointer for inverse lookups records (Reverse Record)
  - Indicates an IP address to domain name mapping.
- SRV: Service Records
  - Identifies services such as directory services.

The nslookup Command

- The nslookup command is available in Windows, Linux and Unix systems.
- Two ways to query DNS servers:
  1. Type nslookup followed by the target domain name.
  2. Type nslookup to invoke interactive mode then key in the target domain name after the “>”

Example 1 (nslookup)

- The local DNS server (*192.168.186.2*) resolves *nyp.edu.sg* with the address *202.0.127.1*.

```
root@bt:~# nslookup nyp.edu.sg
Server:         192.168.186.2
Address:        192.168.186.2#53

Non-authoritative answer:
Name:   nyp.edu.sg
Address: 202.0.127.1
```

Example 2 (nslookup)

- With the following query, DNS servers that are authoritative for *nyp.edu.sg* can be identified.

```
root@bt:~# nslookup
> set q=ns
> nyp.edu.sg
Server:         192.168.186.2
Address:        192.168.186.2#53

Non-authoritative answer:
nyp.edu.sg      nameserver = dnssec2.singnet.com.sg.
nyp.edu.sg      nameserver = dnssec3.singnet.com.sg.
nyp.edu.sg      nameserver = ns1.nyp.edu.sg.
nyp.edu.sg      nameserver = ns2.nyp.edu.sg.
nyp.edu.sg      nameserver = dnssec1.singnet.com.sg.

Authoritative answers can be found from:
ns1.nyp.edu.sg  internet address = 202.12.95.1
ns2.nyp.edu.sg  internet address = 202.12.94.4
dnssec1.singnet.com.sg  internet address = 165.21.83.11
dnssec2.singnet.com.sg  internet address = 195.13.10.226
dnssec3.singnet.com.sg  internet address = 165.21.100.11
>
```

Example 3 (nslookup)

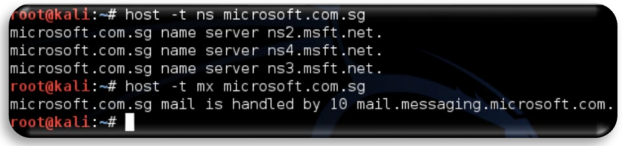
- With the following query, mail exchange servers for *nyp.edu.sg* can be identified.

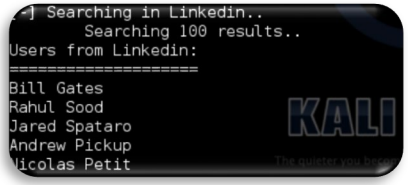
```
root@bt:~# nslookup
> set q=mx
> nyp.edu.sg
Server:         192.168.186.2
Address:        192.168.186.2#53

Non-authoritative answer:
nyp.edu.sg      mail exchanger = 15 mx4.nyp.edu.sg.
nyp.edu.sg      mail exchanger = 15 mx3.nyp.edu.sg.

Authoritative answers can be found from:
nyp.edu.sg      nameserver = dnssec3.singnet.com.sg.
nyp.edu.sg      nameserver = ns1.nyp.edu.sg.
nyp.edu.sg      nameserver = ns2.nyp.edu.sg.
nyp.edu.sg      nameserver = dnssec1.singnet.com.sg.
nyp.edu.sg      nameserver = dnssec2.singnet.com.sg.
mx3.nyp.edu.sg  internet address = 202.12.95.9
mx4.nyp.edu.sg  internet address = 202.12.94.9
dnssec1.singnet.com.sg  internet address = 165.21.83.11
dnssec2.singnet.com.sg  internet address = 195.13.10.226
dnssec3.singnet.com.sg  internet address = 165.21.100.11
>
```

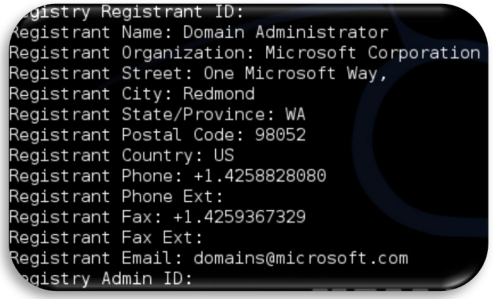
Reconnaissance Tools

- Whois databases
  - Offers information on registrar.
    - whois microsoft.com
- Search the Fine Web
  - http://www.exploit-db.com/google-dorks/ (Google Hacking Database)
    - Example: Finding PDF – site:microsoft.com filetype:pdf
    - Example: Finding subdomains - site:microsoft.com -site:www.microsoft.com
- Email Harvesting
  - ./theHarvester.py –d microosft b linkedin
- DNS Enumeration
  - host –t ns microsoft.com.sg, host –t mx microsoft.com.sg
- Low-Technology Reconnaissance
  - Social Engineering
  - Physical Break-in
  - Dumpster Diving

Operators	Description
site	Searches a specific website or domain.
filetype	Search for a particular file type.
link	Searches within hyperlinks for a specific term.
cache	Identifies the version of a web page.
intitle	Searches for a term within the document title.
inurl	Searches only within the URL of a document.







Information Gathering (1)

Reconnaissance

- Reconnaissance Tools Recap
- Low-Tech Reconnaissance

Passive Information Gathering

- Footprinting
- Whois Lookups
- Google Hacking