IT3789 Cyber Security Attack & Defence

L6 – Information Gathering (2)

WITH KNOWLEDGE COMES RESPONSIBILITY

Reconnaissance Tools Recap

- Whois databases
  - Offers information on registrar.
- Search the Fine Web
  - Through target's website, search engine etc.
- Enumeration
  - Gathering and compiling relevant information the target systems from specific services.
- Low-Technology Reconnaissance
  - Social Engineering
  - Physical Break-in
  - Dumpster Diving

Information Gathering

Reconnaissance

Passive Information Gathering

Active Information Gathering

Social Engineering

Active Information Gathering

- Use more intrusive methods to gather information, usually through social engineering on-site visits, interviews and questionnaires.
- Actively interact with target without dropping to the level of scanning.
  - May show up in intrusion review.
  - e.g. Pose as website visitor.
- Does not involve hacking the system.
- May involve social engineering.

Enumeration

- Enumeration is the process of gathering and compiling relevant information the target systems from specific services.
- Information to look out for includes:
  - Usernames
  - Machine names
  - Network resources
  - Shares
  - Services
- Involves querying and connecting to target system to acquire information.

DNS Enumeration

- Process of locating all the DNS servers in a target organisation and retrieving corresponding records from them.
  - Useful information such as IP addresses, server names and server functions can be obtained.
  - e.g. MX record will indicate server is a mail server.

DNS Enumeration

DNS Forward Lookup Brute Force

DNS Reverse Lookup Brute Force

DNS Zone Transfer

DNS Forward Lookup

- Resolve a given name.
- Use method to guess valid names of servers.
  - If it resolves, then server exists.

```
root@bt:~# host www.nyp.edu.sg
www.nyp.edu.sg has address 202.0.127.1
```

  - If the server does not exists, a "not found" result will be returned.

```
root@bt:~# host idontexist.nyp.edu.sg
Host idontexist.nyp.edu.sg not found: 3(NXDOMAIN)
```

DNS Forward Lookup Brute Force

- Automate the discovery process.
- A complete list of DNS names in */pentest/enumeration/dnsenum/dns.txt or /usr/share/dnsenum/dns.txt*
- For example, a simple script can be written to find out if servers which are alive within the

```
#!/bin/bash
for name in $(cat /pentest/enumeration/dnsenum/dns.txt);do
host $name.nyp.edu.sg
done
```

DNS Forward Lookup Brute Force

- Whois can be used to find out the new IP range using the IP of the servers that were found in the forward lookup brute force.

```
root@bt:/# host ns1.nyp.edu.sg
ns1.nyp.edu.sg has address 202.12.95.1
root@bt:/# whois 202.12.95.1
% [whois.apnic.net node-5]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        202.12.94.0 - 202.12.95.255
netname:        NETBLK-NYPNET202
descr:          Nanyang Polytechnic
descr:          Ang Mo Kio Campus
descr:          180 Ang Mo Kio Ave 8
descr:          Singapore 569830
country:        SG
admin-c:        FL595-AP
tech-c:         FL595-AP
notify:         dbmon@apnic.net
mnt-by:         APNIC-HM
mnt-routes:     MAINT-SG-NYP
changed:        hostmaster@apnic.net 19930416
changed:        hostmaster@apnic.net 20010804
changed:        hm-change@apnic.net 20020604
changed:        hm-changed@apnic.net
status:         ASSIGNED PORTABLE
changed:        hm-changed@apnic.net 20090108
source:         APNIC

person:         Francis Lee
nic-hdl:        FL595-AP
e-mail:         Francis_Lee@nyp.gov.sg
address:        180 Ang Mo Kio Ave 8 S(569830)
phone:          +65 65500275
fax-no:         +65 64525115
country:        SG
changed:        Francis_Lee@nyp.gov.sg 20081125
mnt-by:         MAINT-SG-NYP
changed:        hm-changed@apnic.net 20081127
source:         APNIC
```

DNS Reverse Lookup

- Relies on the existence of PTR records on the name server.
- PTR records are becoming widely used as many mail systems require PTR verification before accepting email.

```
root@bt:/# host 202.12.94.9
9.94.12.202.in-addr.arpa domain name pointer mx4.nyp.edu.sg.
```

DNS Reverse Lookup Brute Force

- Using the host command, a PTR DNS query on an IP will return its Fully Qualified Domain Name (FQDN).
- Host names will give clues on the use of specific servers.
  - Web server: *www.nyp.edu.sg*
  - SMTP server: *smtp.gmail.com*
- For example, a simple script can be written to find out all the host in a particular domain.

```
#!/bin/bash
range="192.168.186"
for ip in `seq 1 254`;do
host $range.$ip
done
```

DNS Zone Transfer

- Zone transfer can be compared to a "database replication“ act between related DNS servers.
  - Changes to zone files are made on the Primary DNS server
  - These files are replicated to the secondary servers by zone transfer.
- If misconfigured DNS servers, a hacker can perform a zone transfer to obtain the zone information.
  - Equivalent to telling the hacker what is the network topology.
  - Countermeasure: Configurations should separate internal DNS namespace and external DNS namespace into different unrelated zones.
- Successful zone transfer might not result in penetration.
  - However, it aids the hacker.

Zone File Example Recap

```
$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.

The dig Command

- The dig command will query name servers for information about the target.
  - Can perform zone transfers unlike the nslookup command.
  - Syntax: *dig @[server] [name] [type]*
    - Type can be ANY, A, MX, etc.
    - Default is A records.
  - With –t flag, zone transfer can be performed.
    - Full zone transfer: -t AXFR
    - Incremental zone transfer: -t IXFR=N
      - N is an integer refering to the serial number of a SOA record.
      - Provides records changed since SOA serial number was N.
    - e.g. *dig @10.10.10.60 target.tgt –t AXFR*

DNS Query Example (dig)

```
root@bt:~# dig nyp.edu.sg

; <<>> DiG 9.5.0-P2.1 <<>> nyp.edu.sg
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18755
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 5, ADDITIONAL: 3

;; QUESTION SECTION:
;nyp.edu.sg.                    IN      A

;; ANSWER SECTION:
nyp.edu.sg.             5       IN      A       202.0.127.1

;; AUTHORITY SECTION:
nyp.edu.sg.             5       IN      NS      dnssec3.singnet.com.sg.
nyp.edu.sg.             5       IN      NS      ns1.nyp.edu.sg.
nyp.edu.sg.             5       IN      NS      ns2.nyp.edu.sg.
nyp.edu.sg.             5       IN      NS      dnssec1.singnet.com.sg.
nyp.edu.sg.             5       IN      NS      dnssec2.singnet.com.sg.

;; ADDITIONAL SECTION:
dnssec1.singnet.com.sg. 5       IN      A       165.21.83.11
dnssec2.singnet.com.sg. 5       IN      A       195.13.10.226
dnssec3.singnet.com.sg. 5       IN      A       165.21.100.11

;; Query time: 259 msec
;; SERVER: 192.168.186.2#53(192.168.186.2)
;; WHEN: Wed Mar 23 06:30:57 2011
;; MSG SIZE  rcvd: 206
```

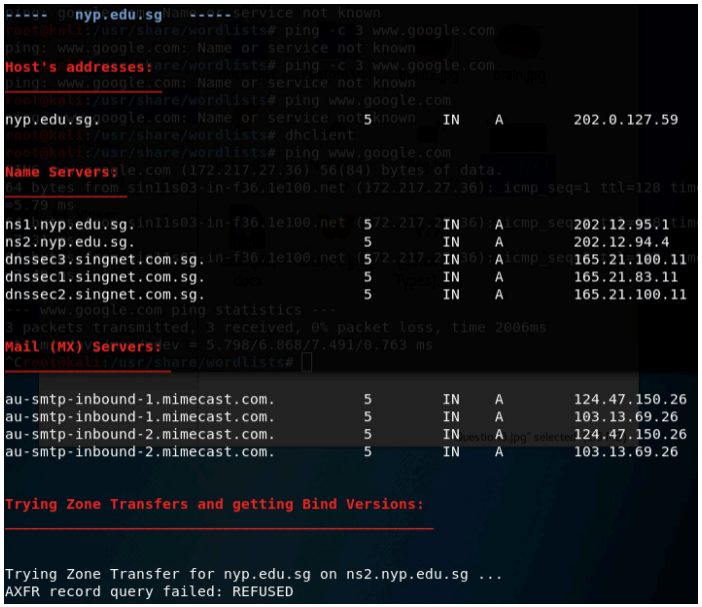
DNS Zone Transfer Example (dig)

```
root@bt:~# dig @192.168.186.3 nyplab.com -t AXFR

; <<>> DiG 9.5.0-P2.1 <<>> @192.168.186.3 nyplab.com -t AXFR
; (1 server found)
;; global options:  printcmd
nyplab.com.             3600    IN      SOA     ns.nyplab.com. cklam.nyplab.com.
 65 900 600 86400 3600
nyplab.com.             3600    IN      NS      ns.nyplab.com.
mail.nyplab.com.        3600    IN      A       192.168.186.101
mail.nyplab.com.        3600    IN      MX      10 mail.nyplab.com.
ns.nyplab.com.          3600    IN      A       192.168.186.3
pop.nyplab.com.         3600    IN      CNAME   mail.nyplab.com.
www.nyplab.com.         3600    IN      A       192.168.186.103
nyplab.com.             3600    IN      SOA     ns.nyplab.com. cklam.nyplab.com.
 65 900 600 86400 3600
;; Query time: 1 msec
;; SERVER: 192.168.186.3#53(192.168.186.3)
;; WHEN: Fri Mar 25 04:51:18 2011
;; XFR size: 8 records (messages 1, bytes 239)
```

Other DNS Utilities

- dnsrecon –d <domain> -t axfr
  - dnsrecon -d nyp.edu.sg -t axfr
- dnsenum <domain>
  - dnsenum nyp.edu.sg
- dnswalk -r -d <domain>.
  - dnswalk –r –d nyp.edu.sg.
- dnsmap <domain>
  - dnsmap nyp.edu.sg -w /usr/share/wordlists/dnsmap.txt



NetBIOS Enumeration

- A null session is an unauthenticated NETBIOS session between two machines.
- Null sessions are a vulnerability found in…
  - Unix/Linux: Common Internet File System (CIFS).
  - Windows: Server Message Block (SMB).
- Information about the machine can be obtained once connected.
  - These information include usernames, groups, shares, permissions, policies and services.
- Tools include nbtscan and auxiliary scanner in Metasploit framework
  - nbtscan <IP>
  - auxiliary/scanner/netbios/nbname
  - auxiliary/scanner/smb/smb_version

SNMP Enumeration

- SNMP employs 2 major types of software components for communication.
  - SNMP agent
  - SNMP management station
- SNMP management station sends requests to agents to manage the system or device.
  - The requests from management station and replies from agents refer to configuration variables accessible by the agents.
- Management Information Base (MIB) is the database of configuration variables that resides on a networking device.

SNMP Enumeration

- SNMP has 2 passwords to access and configure SNMP agent from the management station.
  - Public (r) community string
    - Password for viewing of configuration of device/system.
  - Private (rw) community string
    - Password for changing and editing of configuration on device.
- SNMP v1 and v2 passes these community strings across the network unencrypted.
  - SNMP v1 and v2 are subjected to packet sniffing.
- SNMP v3 has added security and remote configuration enhancements such as encryption and message integrity.
- Tools include snmp-check, snmpwalk, onesixtyone and auxiliary scanner in Metasploit framework
  - snmpwalk <IP> -c public –v 2c
  - auxiliary/scanner/snmp/snmp_enum; auxiliary/scanner/snmp/snmp_enumshares; auxiliary/scanner/snmp/snmpusers; auxiliary/scanner/snmp/snmp_login

SNMP Enumeration

- Information can be obtained from SNMP enumeration includes.
  - Hardware/Operating System
  - Windows Users
  - Running Services
  - Open TCP Ports
  - Installed Software

SMTP Enumeration

- Under certain misconfigurations, mail server can be used to gather information about host and network.
- SMTP supports interesting commands such as VRFY and EXPN.
  - A VRFY request asks the server to verify an email address.
  - A EXPN asks the server for membership of a mailing list.
- These can be abused to verify existing users on a mail server which can aid the attacker later.
  - e.g. Windows usernames may be the same as the email account.
  - e.g. Verified email accounts used to send malicious emails.
- Tools include smtp-user-enum.pl and auxiliary scanner in Metasploit framework
  - smtp-user-enum.pl -M VRFY -U users.txt -t 10.0.0.1
  - auxiliary/scanner/smtp/smtp_enum

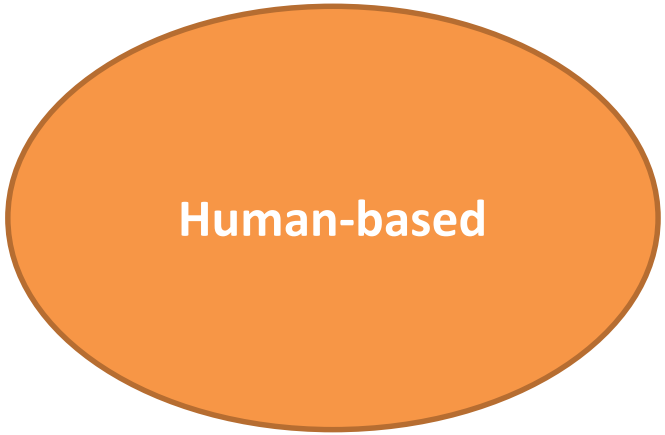
Social Engineering

- Social engineering is a nontechnical method of breaking into a system or network.
  - Deceive users of a system.
  - Convince them to perform acts that is useful to an attacker.
    - e.g. Giving information that can defeat or bypass security mechanism.
- Hackers can use social engineering to attack the human element of a system and circumvent technical security measure.
  - Used to gather information before or during an attack.

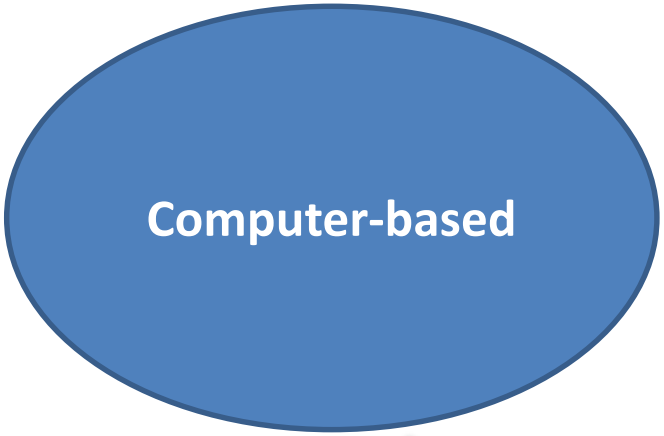
Social Engineering

- Telephone or Internet are common tools for social engineering.
- A social engineer tries to…
  - trick users into revealing sensitive information.
  - get users to do something that is against the security policies of the organisation.
- Exploit human trust rather than system vulnerabilities.
  - Users is the weak link in security.

Types of Social Engineering Attacks

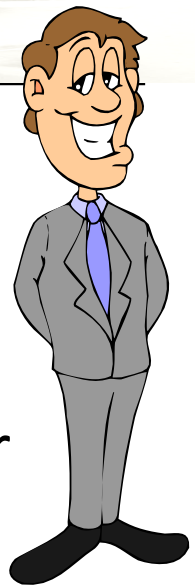


- Person to person interaction to retrieve desired information.
- Example: Calling helpdesk to find out a password.



- Use software that attempts to retrieve the desired information.
- Example: phishing

Human-Based Social Engineering Techniques



- Impersonating an employee or valid user
  - May gain access by pretending to be a cleaner, employee or contractor.
  - Once inside the facilities, the hacker gathers information from trash cans desktops or computer systems.
- Posing as an important user (e.g. High-level manager)
  - Intimidate lower-level employees (e.g. helpdesk staff) to assist them in gaining access to the system.
  - Most low-level employees will not question someone who appears to be in position of authority.

Human-Based Social Engineering Techniques

- Using a third party
  - Hacker pretends to have permission from an authorised source to use a system.
  - Effective if the supposed authorised source cannot be contacted for verification.
- Calling technical support
  - Helpdesk and technical support staffs are trained to help users.
    - Good prey for social engineering attacks.

Human-Based Social Engineering Techniques

- Shoulder surfing
  - Gather passwords by watching over a person's shoulder while they log into a system.
- Dumpster diving
  - Favourite trick of hack master Kevin Mitnick.
  - Also known as "trashing".
  - Can be disgusting … but very rewarding!
  - Network diagrams and system documentation.
  - Post-it notes with passwords.

Computer-Based Social Engineering Techniques

- Attacks may be based on the following:
  - Email attachments
    - Can be used to send malicious code to a target system.
      - e.g. Malicious code that installs and executes a keylogger to capture password.
    - Virus, Trojans and worms can be included in specially crafted emails to entice victim to open the attachment.
  - Popup Windows
    - Can be used in a similar manner as email attachment.
    - Uses special offers or free stuffs to encourage user to install malware unintentionally.
    - e.g. Fake antivirus scams.

Computer-Based Social Engineering Techniques

- Fake websites
  - Phishing
    - Send email usually posing as a bank, credit card company or financial organisation. Why?
    - Usually email requests the recipient to confirm banking information or reset passwords.
    - User is redirected to fake website when the link in the email is clicked.
    - Hacker will be able to capture the information.
  - Online scams
    - Websites make free offers or other special deals to lure a victim to enter a username and password or to click on malicious links.

Computer-Based Social Engineering Techniques

- URL Obfuscation may be employed to hide fake URL in what appears to be a legitimate website.
  - Makes phishing attacks and some online scams to look more convincing.
    - http://204.13.144.2/Citibank
  - Address can be obfuscated in malicious links by using hex encoding or decimal or hexadecimal notation.
    - Decimal Notation
      - New address = First octet * 256 + second octet = * 256 + third octet = * 256 + fourth octet
    - Example: *http://www.google.com* or *http://74.125.235.50*
      - Hex encoding: %77%77%77%2E%67%6F%6F%67%6C%65%2E%63%6F%6D
      - Decimal notation: http://1249766194
      - Hexadecimal notation: http://0x4A7DEB32
  - URL shortening is a technique on the World Wide Web in which a Uniform Resource Locator (URL) may be made substantially shorter and still direct to the required page.
    - Bitly.com, nyp.edu.sg -> https://bit.ly/25SimHE

Social Engineering Countermeasures

- Good policies & security awareness programmes
  - Good policies alone are not effective unless they are taught and reinforced to employees.
  - Employee education is important.
    - Employees should be trained on how to keep confidential data safe.
- One advantage of a strong security policy is that it helps employees decide how to response to hacker's request.
  - If requested action is denied in policy, the employee follows the guidelines and deny it.

Information Gathering (2)

Active Information Gathering

- Reconnaissance Tools Recap
- Enumeration
  - DNS
  - NetBIOS
  - SNMP
  - SMTP

Social Engineering

- Types of social engineering
- Human-Based Social Engineering Techniques
- Computer-Based Social Engineering Techniques
- Social engineering countermeasures