CSCI369 Ethical Hacking

Lecture 1-2: Penetration Testing Concept and Information Gathering

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Defining Penetration Testing

- Penetration tester?
  - ➢A penetration tester or a pentester is a white hat hacker employed either as an internal employee or as an external entity to conduct a penetration test.
- Penetration testing?
  - ➢Surveying, assessing and testing the security of a given organization by using the same techniques, tactics and tools that a malicious hacker (black hat hacker and/or cyberterrorist) would use.
  - ➢In this subject (CSCI369), I would equate “penetration testing” with “ethical hacking”.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

1. Determining the objectives and scope of the job
   - ➢A pentester and a client should meet to discuss the objectives of the test
   - ➢Examples of objectives
     - ✓To determine security weakness
     - ✓To test an organisation’s security policy compliance, its employees’ security awareness
     - ✓To test an organisation’s ability to identify and respond to security incidents

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

- ➢Scope of the test
  - ✓Usual network penetration testing
  - ✓Social engineering testing: Human aspect in vulnerability
  - ✓Application security testing: Finding flaws in software applications
  - ✓Physical penetration testing: Testing the security of premises where digital assets and network resources are stored

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

2. Choosing the type of test to perform

   ➢Three typical types of testing

   1) Black-Box Testing

      - Most closely resembles the situation of an outside attack → This test is called "external test"
      - Execute the test from a remote location much like a real attacker
      - The pentester will be extremely limited on information of the target

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

2) Grey-Box Testing

- The pentenster will have some limited knowledge on the target, for example, (at least) what operating system the target is mainly using

3) White-Box Testing

- This gives the pentester full knowledge on the target
- Basically this test simulates “insider attack” → This test is called “internal test”

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

3. Gaining permission via a contract
   - ➢It is vitally important to get clear and unambiguous permission to perform a pentest: A written form of authorisation rather than a verbal authorisation is important. It should include
     - ✓Systems to be evaluated
     - ✓Perceived risks
     - ✓Timeframe
     - ✓Actions to be performed when a serious problem is found
     - ✓Deliverables

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology

4. Performing penetration testing (More to come regarding this)
5. Creating a Risk Mitigation Plan (RMP)
   - Purpose: RMP is to develop options and actions to enhance opportunities and reduce threats in an organisation
   - Contents: RMP should clearly document all the actions took place including the results, interpretations and recommendations
6. Cleaning up any changes made during the test
   - This is obvious step needed to prevent possible mishaps

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Penetration Testing Methodology (Overview)

1. Determining the objectives and scope of the job
2. Choosing the type of test to perform
3. Gaining permission via a contract
4. Performing penetration testing
   - ➢Process of penetration testing specifies steps 4.1 to 4. 6
5. Creating a risk mitigation plan (RMP)
6. Cleaning up any changes made during the test

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Process of Penetration Testing

4.1 Information (Intelligence) Gathering

- Gather information about a target before performing active attacks

4.2 Scanning

- Based on the information gathered, target the attack much more precisely

4.3 Exploitation

- Following enumeration, execute the attack

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Process of Penetration Testing

4.4 Covering tracks

- ➢Make all attempts to remove evidence of being in a system

4.5 Maintaining Access

- ➢Plant backdoors or other means to leave something behind

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Introduction to Information Gathering

- Information Gathering is a process of ethical hacking through which a pentester locates information about a target, which will be useful for later steps of the attack.
- Information gathered about a target may refine the steps that will come later.
- Anything that have potential to be exploited should be sought.
- It is important to develop an "eye" to detect the useful information carefully, but sheer "luck" could work.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Introduction to Information Gathering

- Terms
  - ➢There are a few similar terms in the literature, referring to information gathering such as intelligence gathering and information reconnaissance, which are regarded as the same.
- Information gathering as an attack
  - ➢Information gathering itself can be regarded as an attack that causes considerable damages.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Categorising the Types of Information to Be Gathered

- Technical information
  - ➢Information regarding operating system, network and applications, IP addresses and/or IP address ranges, and device information. Additionally, information regarding webcams, alarm systems, mobile devices and etc.
- Administrative information
  - ➢ Organisational structure, corporate policies, hiring procedures, details of employees, phone directories, vendor information, and etc.
- Physical details
  - ➢Data about location and facility.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Categorising Information Gathering Methods

- Passive
  - ➢Methods that do not engage the target. If the target is not engaged, little or no indication of an impending attack will be given to the target.
- Active
  - ➢Methods that do engage the target by, for example, making phone calls to the company, help desk, employees and/or other personnel. Care should be taken not to give the target an indication of the attack.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Categorising Information Gathering Methods

- Open Source Intelligence (OSINT) gathering
  - ➢Gathering information from those sources that are typically publicly available and open.
  - ➢A kind of passive information gathering method.
  - ➢The least aggressive method.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- Domain Name System (DNS)
  - ➢The DNS is used for resolving hostnames into IP addresses and vice versa. All internetworking applications require DNS to function.
  - ➢DNS makes use of a hierarchical naming scheme: Queries work in a top-down manner, beginning at the top of the DNS tree and working their way down.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- ➢In the hierarchy, three classes of DNS servers exist:
  - ✓Root DNS servers: There are 13 root servers in the world.
  - ✓Top-Level Domain (TLD) servers: These servers are responsible for top-level domain such as .com, .org, .net, .edu, gov, au, uk, ca, kr, jp and etc.
  - ✓Authoritative DNS servers: These DNS servers of every organisation with publicly accessible hosts provide publicly available DNS records that map the names of hosts to IP addresses.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- DNS scenario
    1. A user makes a query for `www.amazon.com`. (by typing the URL or clicking a link…)
    2. The browser sends the DNS query to the DNS resolver (local DNS server).
    3. The DNS resolver queries the root servers to get a list of IP addresses for TLD servers responsible for `.com`
    4. The DNS resolver then queries one of those TLD servers to get the IP address of the authoritative DNS server server for amazon
    5. The DNS resolver queries the authoritative DNS server to get the IP address of `www.amazon.com`, which is 130.130.213.213

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- DNS records
  - ➢DNS servers store DNS records, which are also called "resource records (RRs)".
  - ➢Each DNS record is a four-tuple and contains the following fields:

    `{Name, Value, Type, TTL}`
  - ➢TTL is "time to live" for that DN dS record.
  - ➢There are quite a few types, but we look at the most essential four types, A, CNAME, MX, NS and SOA.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `Type = ` A (IPv4) or AAAA (IPv6)
  - ➢Stores IP address for a name.
  - ➢That is, Name is a hostname and `Value` is its IP address.
  - ➢Example: `{www.example.com, 13.54.131.40, A, TTL}`
  - ➢This is the most common type.
- `Type = CNAME`
  - ➢This is an alias record or alternative record for another record.
  - ➢It is referred to as “Canonical Name”.
  - ➢That is, Name is a hostname and `Value` is its alias.
  - ➢Example: `{www.example.com, web1.example.com, CNAME, TTL}`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `Type = MX`
  - ➢Identifies mail server for that domain.
  - ➢Here, `Name` is a domain name and `Value` is its mail server name.
  - ➢Example: `{example.com, mail1.example.com, MX, TTL}`
- `Type = NS`
  - ➢Identifies authoritative DNS servers (name servers) for that DNS name.
  - ➢Here, `Name` is a domain name and `Value` is its name server.
  - ➢Example: `{example.com, ns1.example.com, NS, TTL}`

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `Type = SOA`
  - ➢Provides "start of authority (SOA)", which is the authoritative information about the domain, the e-mail address of the domain admin, the domain serial number, etc…
    - ✓NS also gives authoritative name servers, but SOA provides primary one (primary name server).
  - ➢Here, `Name` is a domain name and `Value` is its primary name server (only one).
  - ➢Example: `{example.com, dns1.example.com, SOA, TTL}`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- Managing DNS
  - ICANN (Internet Corporation for Assigned Names and Numbers): The authority for domain name assignments → Thousands of Domain Name Registrars have been accredited by ICANN to sell domain names and make this information available.
  - The decentralized nature of domain name registration means there is no single location for obtaining information about a given domain.
  - After purchasing a domain name, the owner of the authoritative domain can create as many subdomains as desired, whether they be actual subdomains or individual hosts.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `nslookup`
  - A tool for querying the Domain Name System (DNS) to obtain domain name or IP address mapping, or other DNS records. (Available in many OSs including Windows, Unix and MacOS.)
  - This is a tool for sending a DNS query directly from the client to any type of DNS server, regardless of whether it is root, TLD or authoritative.
  - Usage: `nslookup www.example.com`
  - By adding –type option, one can specify the type of DNS record. For example, `nslookup –type=ns example.com`
  - Reverse DNS is also possible, for example, `nslookup 11.22.33.44`

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- `whois`
  - A protocol for querying about the owner of a domain name, IP network
  - Information returned by WHOIS contains information about the owner, including email addresses, contact numbers, street addresses, etc.
  - As WHOIS servers exist all over the Internet and are administered by different organizations, the quality of the results may vary.
  - All WHOIS services have mechanisms in place to prevent data mining.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domain

- Web-based `whois` service
  - URL: https://whois.domaintools.com
  - Easier to navigate and view information provided by whois
  - Sometimes, more information can be found

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

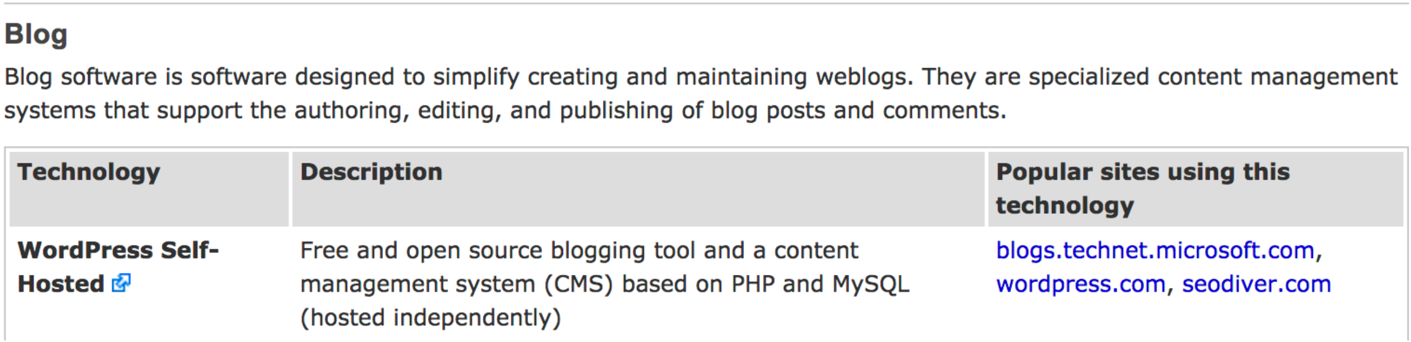
Gathering Information about Technologies a Website Uses

- Netcraft
  - ➢A website that provides comprehensive information about technologies that a website uses
  - ➢URL: https://sitereport.netcraft.com/
  - ➢It provides information about web hosting company, hosting history, type of web server, whether it sends spam, server-side and client-side technologies, web applications used and etc.
  - ➢All the above information can be exploited to find vulnerabilities of the target.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Technologies a Website Uses

- Netcraft example
  - ➢As an example, query www.howtogeek.com on netcraft
  - ➢You can see this site is using WordPress as blog software



Blog

Blog software is software designed to simplify creating and maintaining weblogs. They are specialized content management systems that support the authoring, editing, and publishing of blog posts and comments.

Technology	Description	Popular sites using this technology
WordPress Self-Hosted	Free and open source blogging tool and a content management system (CMS) based on PHP and MySQL (hosted independently)	blogs.technet.microsoft.com, wordpress.com, seodiver.com

  - ➢Then go to www.exploit-db.com and search wordpress
  - ➢A long list of exploitable vulnerabilities exist!

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Subdomains

- Finding subdomains
  - ➢Subdomain: A subdomain is a domain which is a part of a larger domain
  - ➢Example: `uow.edu.au` has subdomains `ro.uow.edu.au`, `jobs.uow.edu.au`, and etc.
- Reasons for having subdomains
  - ➢To organise content more effectively by giving different divisions or departments their own subsite that they can control and manage
  - ➢Or companies may want to "hide" contents by having subdomain sites, for example: `beta.facebook.com`

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Subdomains

- A few other web tools for searching for subdomains:
  - ➢ https://searchdns.netcraft.com/
  - ➢ https://pentest-tools.com/information-gathering/find-subdomains-of-domain

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

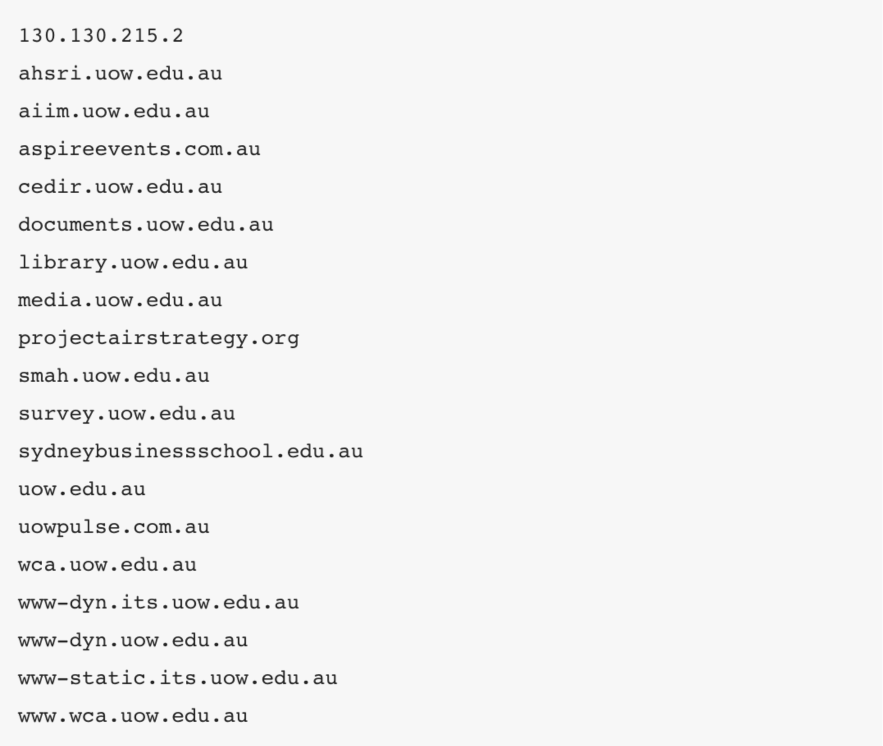
Gathering Information about Domains on the Same Server

- The same server different websites
  - ➢One server can serve/handle multiple websites.
  - ➢Gaining access to one of those websites on the same server can be helpful to attack others.
  - ➢Visit https://hackertarget.com/reverse-ip-lookup/ and query a website you know.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Domains on the Same Server

- Example



```
130.130.215.2
ahsri.uow.edu.au
aiim.uow.edu.au
aspireevents.com.au
cedir.uow.edu.au
documents.uow.edu.au
library.uow.edu.au
media.uow.edu.au
projectairstrategy.org
smah.uow.edu.au
survey.uow.edu.au
sydneybusinessschool.edu.au
uow.edu.au
uowpulse.com.au
wca.uow.edu.au
www-dyn.its.uow.edu.au
www-dyn.uow.edu.au
www-static.its.uow.edu.au
www.wca.uow.edu.au
```

These websites share the same IP address as www.uow.edu.au

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Network Topology

- `traceroute` (`tracert` on Windows)
  - A tool that can help determine network topology.
  - It shows the path a packet takes as it travels from the source to the destination.
  - Importantly it gives information about routers between the source and destination.
  - After running `traceroute` to several systems on their network, one can start drawing a network diagram
  - More information on `www.traceroute.org`

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information from Website

- What can be found
  - ➢People (personnel)
  - ➢Email addresses
  - ➢Physical addresses
  - ➢Job postings leaking information
  - ➢Product, project and service information

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Website

- Electronic dumpster diving (finding websites that do not exist any more)
  - ➢Process of looking for old, obsolete and obscure old data
  - ➢The Wayback Machine (`archive.org`) can be used
  - ➢The Wayback Machine project which started in 1996 contains around 435 billion web pages that have been archived
  - ➢Visit `web.archive.org` to get old web pages of our university

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information about Website

- Viewing a website offline
  - ➢Useful if websites/webpages can be saved locally and examine them
  - ➢A tool called website downloader or website crawler can be used
  - ➢On (Kali) Linux/Unix, “`wget`” can be used
    - ✓Try `(sudo) wget –m http://<website name>`

      Note that “`m`” here means “mirror”, another term for “downloading”
  - ➢Viewing a website offline can allow an attacker to find the “type=hidden” vulnerability
    - ✓Example) `<input type=”hidden” id=”1008” name=”price” value=”150.00”>`
    - ✓Here, the website owner might think that the filed “`value`” is hidden from the view of public but a malicious hacker can modify the value stored in his web browser and repost it(using a tool like web Proxy or Tamper Data)!

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information on Email Addresses

- `theHarvester`
  - ➢The Harvester is a tool in Kali Linux for collecting e-mail addresses, subdomains, employee names and etc.
  - ➢E-mail addresses on their own provide an opportunity to launch phishing attacks, attempt to get Trojans installed, and other direct attacks
  - ➢Another opportunity is that the local part (everything to the left of the @) is often the username and having a list of usernames gives an attacker a list of accounts to use when trying to log in other critical systems.
  - ➢The Harvester can be configured to use Google, Bing, PGP, LinkedIn, as well as a number of other sources.

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Gathering Information on Email Addresses

- `theHarvester`
  - ➢ Usage
    - ✓ -d: specifying domain
    - ✓ -b: specifying search engine
    - ✓ -l: specifying the number of entries
    - ✓ Example1) `theharvester –d uow.edu.au –b google –l 100`
    - ✓ Example2) `theharvester –d uow.edu.au –b linkedin –l 100`
    - ✓ Example3) `theharvester –d uow.edu.au –b pgp –l 100`

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

Putting things all together: Comprehensive Information Gathering tool

- `DMitry`
  - ➢A UNIX tool for comprehensive Information Gathering:
    - ✓Whois look up (– does not work in the recent version.)
    - ✓Retrieving possible server data using Netcraft
    - ✓Subdomain search
    - ✓Finding emails
    - ✓TCP port scan
  - ➢Manual: https://linux.die.net/man/1/dmitry

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

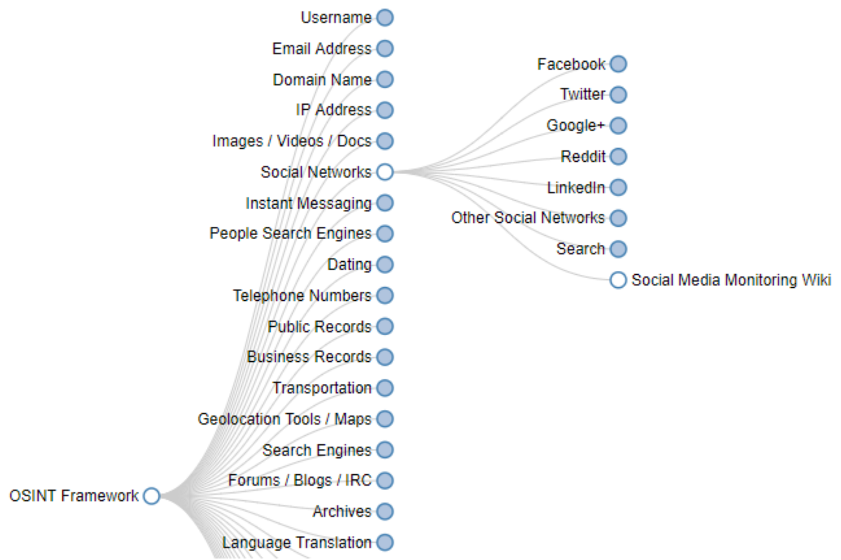
Gathering Information about IoT

- Webcams
  - ➢The website www.shodan.io has a capability to search for webcams as well as other devices
  - ➢Webcams can be used to extract information about the target’s physical location and facility
  - ➢Privacy issues can arise too

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek

More Tools?

- OSINT Framework
  - ➢ https://osintframework.com/
  - ➢ This site provide useful links for Open Source Intelligence.
  - ➢ Try them and build your own way to perform successful information gathering!



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from Joonsang Baek