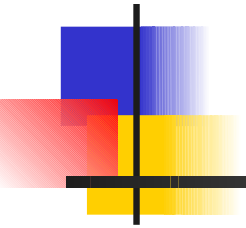


SEC520

Penetration Testing (part 1): Reconnaissance

Today's Objectives

Internet Security Overview:

- 8 Rules of Internet Security
- Purpose of Penetration Testing
- Phases of Penetration Testing

The Reconnaissance Phase:

- Purpose
- Information Gathering
- Foot-printing
- User Information
- Verification

8 Rules of Internet Security

- The following concepts are contained in the textbook: "*Inside the Security Mind, Making the Tough Decisions*", Kevin Day
- *There is a tendency for people to rely on technology and "gimiks" as opposed to consistently* ***following a set of essential practices or "guidelines"****.*
- *We have discussed general virtues to follow regarding Internet Security, but we can expand on these virtues by following 8 simple rules or guidelines to ensure more secured (hardened) computer systems.*

8 Rules of Internet Security

From "*Inside the Security Mind: Making the Tough Decisions*", Kevin Day

Rules	Description
1. **Rule of Least Priviledge**	Allow only as much access as is required to do the job, nothing more.
2. **Rule of Change**	Any change must be managed, coordinated, and considered for possible security implications.
3. **Rule of Trust**	Understand the full effect before extending trust to anyone or anything.
4. **Rule of the Weakest Link**	Focus must be evenly "spread-out" in all aspects of security, not just on specific areas.
5. **Rule of Separation**	Diversity server tasks (don't put all eggs in one basket)
6. **Rule of 3-Fold Process**	Implementation, Monitoring, Maintenance
7. Rule of Preventative Action	Stay current, Regular testing, Find vulerablities
8. **Rule of Response**	Response plan, React quickly, Enforce Rules, Education

Pentration Testing

Penetration Testing is "*a method of evaluating the security of a computer system or network by simulating an attack from malicious outsiders (who do not have an authorized means of accessing the organization's systems) and malicious insiders (who have some level of authorized access).*"

WIKIPedia: http://en.wikipedia.org/wiki/Penetration_test

In Penetration Testing, there are **two methodologies**:

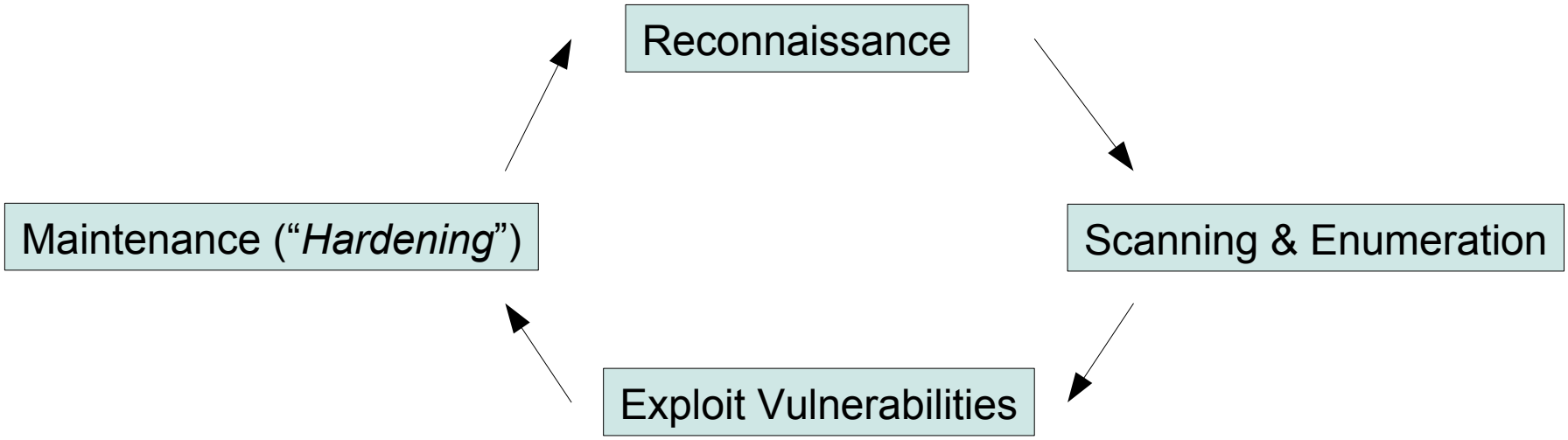
- **White Hat Hacker**, where an individual has full knowledge of the system, and is testing the "targeted system" to simulate a malicious internal (i.e. pre-existing knowledge of system) attack.

- **Black Hat Hacker**, where an individual has no prior knowledge of the system being attacked, and is testing to simulate an external hacking or cyber warfare attack.

Pentration Testing

Penetration Testing Phases:

The diagram below illustrates the phases of Pentration Testing. Note that these phases never end, but are an on-going process. (Source: x)

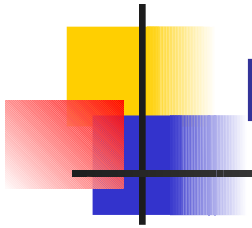


Reconnaissance

Some may compare **reconnaissance** as the act of an army using scouts to hide near the opposing army in order to gather as much information (intelligent) regarding the enemy.

This comparison is well-suited when applied to Internet Security:

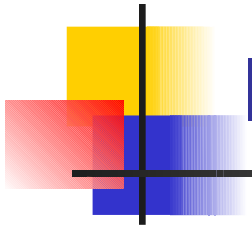
- Relative “safe” method of intelligence gathering (i.e. less chance of being caught if hidden).
- Success from an attack requires accurate intelligence and verification of appropriate targets.
- As it applies to Internet Security, you are looking to obtain as much information to gain an advantage, with emphasis on IP address(es) of target system, and IP addresses of other systems that are associated with the targeted system.



Phases of Reconnaissance

(From "*Penetration Tester's Open Source Toolkit*", Jeremy Faircloth)

- Information (Intelligence) Gathering
- Foot-printing
- User Information
- Verification



Information Gathering

Information Gathering Tools:

Search Engine (Google)

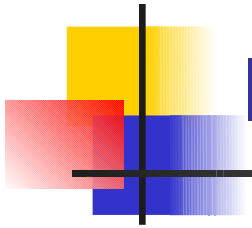
- In Google, using “**site:URL**”, “**filetype:[extension]**”, and “**link:siteURL**”.
  Note: These methods can be used together as separate directives, for example: **link:url filetype:pdf security**

Netcraft (http://netcraft.com/)

- Contains database of host servers with possible detailed information of the server including: IP address, Name servers, Domain Registry, (possibly type of OS).

– **BiLE.pl** , **BiLE-Weigh** (https://github.com/sensepost/BiLE-suite)

- Defines relationships among servers and target server.

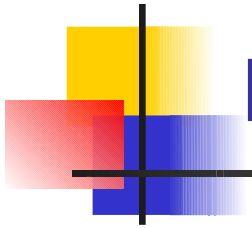


Information Gathering

Information Gathering Tools / Continued:

Domain Name Expansion:

- Manual Method: **host -t ns siteURL**
- Application: **tld-expand.pl**
  (From BiLE Suite)



Foot-Printing

- We are all familiar with the term **Footprint**.
  For example: a human footprint, or the footprint (internal structure) of an organization.

- As it relates to this course, **Foot-printing** is the method of gathering information regarding an organization's computer system (and related servers).

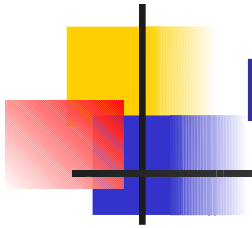
- As opposed to the *Information Gathering* phase (that collects information such as IP Addresses), the *Foot-printing* phase tends to gain a “clearer picture” of the structure of the organization's computer system. This can include relationships among servers, as well as noting IP Address ranges.

- The process of the foot-printing process to gain a physical sense of how these computer networks are related is also referred to as **Network Mapping**.

Foot-Printing

There are several general approaches in obtaining a **Network Foot-print**:

DNS	Records contained in a name server (NS) look-up may provide a great source of information for later exploitation, and verification (Reverse DNS).
WHOIS	Common protocol to determine domain name ownership, IP network. Depending on restrictions, it may provide other info such as e-mail addresses, and other contact information.
SMTP	MX Records contain useful information. Headers from “bounced” e-mail messages can provide IP addresses (at heart of organization's network).



Foot-Printing: DNS

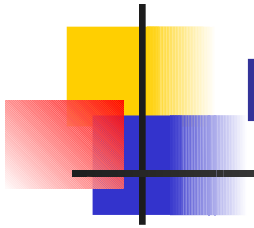
Purpose:

Utitilies (tools):

- **whois**
- **host**
- **dig** (like host, different report format)

Other:

- dnsenum.pl (Perl Script to automate host, dig Google scrapes in a bruteforce fashion)
- Digdug (Suite of Python Scripts ***forcedns.py*** and ***dnsreverse.py*** Similar to dnsenum.pl, but automates brute forcing, and provides Reverse DSN lookups to help save time during verification.)

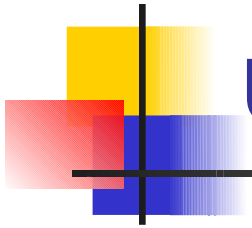


Foot-Printing: SMTP

MX Records contain useful information. Headers from “bounced” e-mail messages can provide IP addresses (at heart of organization's network).

Utitilies (tools):

- **Mail Bounce** (send non-existent e-mails to server and obtain information from server's response)
- **theHarvester** (A Python Script used to gather **e-mails**, subdomains, hosts, employee names, open ports, and banners from targeted server(s)...)



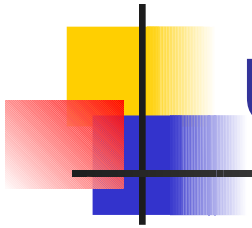
User Information

Mapping a network is important, but we also need to recognize that computer systems contain users.

The more information that can be gathered from the **employees (users)** of an organization, the better the changes of gaining access to exploit a vulnerability.

Types of Information include:

- E-mail addresses
- Names
- Business Relationships (organization chart)
- Social Networking Information



User Information

Utilities (tools):

theHarvester.py

- A Python Script used to gather information from server such as e-mail accounts from Google database.

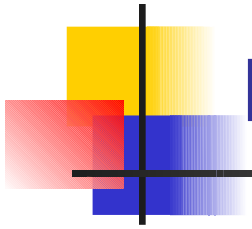
Metagoofil.py

- A Python Script used to download document files (various types) from organizations whose links are stored on Google.

Verification

Verification is the final step of the Reconnaissance Phase. It is important to verify your gathered information to help reduce the amount of time during the Scanning and Enumeration Phase.

- **Utitilies (tools):**
  - **Banners & Websites**
  - **www.bing.com**
  - **dnsmap**
  - **IPWHOIS**
  - **dsnreverse.pl**



Lab Time

Perform:

Lab 2: Penetration Testing (part 1)