CS 455 – Computer Security Fundamentals

Dr. Chen-Yeou (Charles) Yu

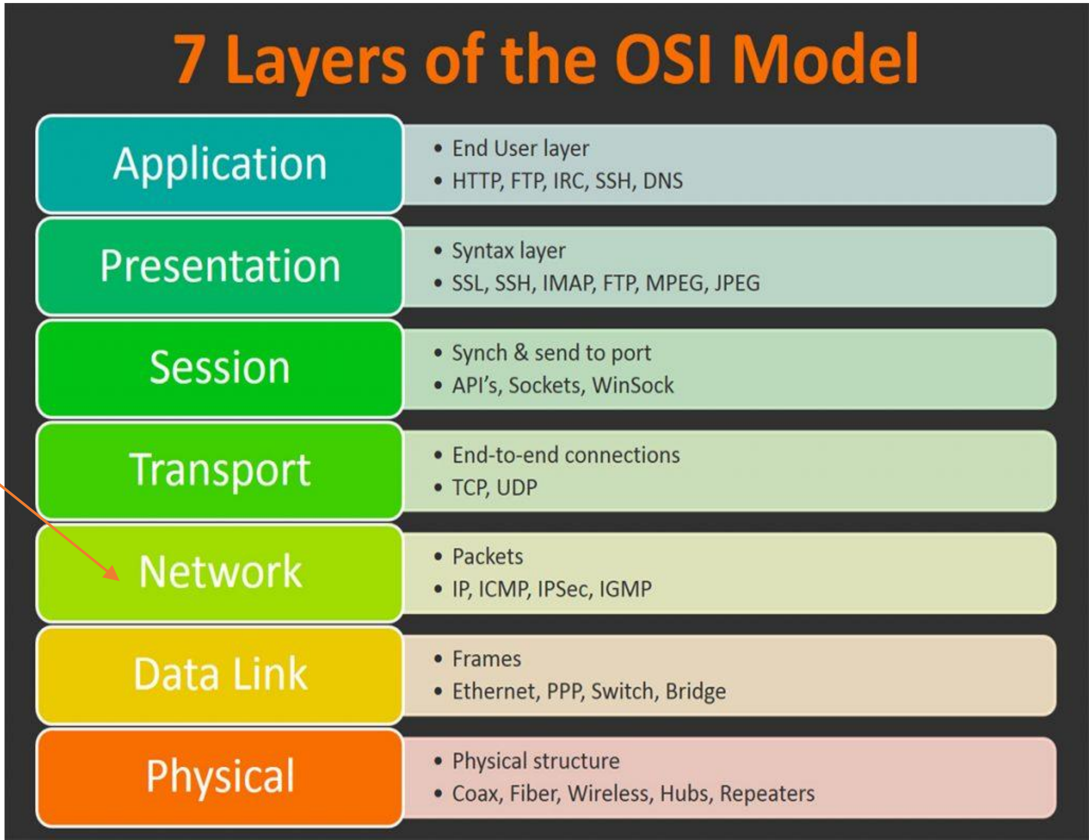
- Vulnerability
  - Vulnerability in the networks, an example
  - Zero Day
- Hacker’s steps. Catch me if you can?
  - Footprinting (reconnaissance)
  - Scanning
  - Enumeration
  - Systems hacking

Vulnerability

- Vulnerabilities can be weaknesses in either the hardware, software or computer systems ← There is not a perfect computer system
- To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can attach to the system weakness
- Security risk and the vulnerability are not equivalent:
  - For example, what if the affected asset has no value? **This kind of asset is vulnerable but is without risk**
- A window of vulnerability means the period from the security hole was introduced or manifested in the deployed software, or systems, to the time when security fix was deployed or the attacking is disabled.

Vulnerability in the networks, an example

- Previously, we talked about the DDoS attack (Ping (ICMP) flood)
- ICMP stands for Internet Control Message Protocol and is the most used protocol in networking technology.
    - It is connectionless.
    - ICMP does not use any port numbers
    - ICMP works in the network layer
- ICMP is originally used for diagnostic purposes, error reporting or querying any server, and right now attackers are using ICMP to send payloads,
    - We will talk about this in the later classes



7 Layers of the OSI Model

Application	• End User layer • HTTP, FTP, IRC, SSH, DNS
Presentation	• Syntax layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session	• Synch & send to port • API's, Sockets, WinSock
Transport	• End-to-end connections • TCP, UDP
Network	• Packets • IP, ICMP, IPSec, IGMP
Data Link	• Frames • Ethernet, PPP, Switch, Bridge
Physical	• Physical structure • Coax, Fiber, Wireless, Hubs, Repeaters

Zero Day

- Also known as a 0-day
- This means a kind of computer system or software vulnerability is known to those who should do something in its mitigation, for example, software vendors.
- Until the vulnerability is mitigated, hackers can exploit to the affected programs, data in several computers or a network.
- From the release of the news of vulnerability to the time the software get cracked, or a system get hacked, it could be just 0 day (on the same date)

Hacker’s steps. Catch me if you can?

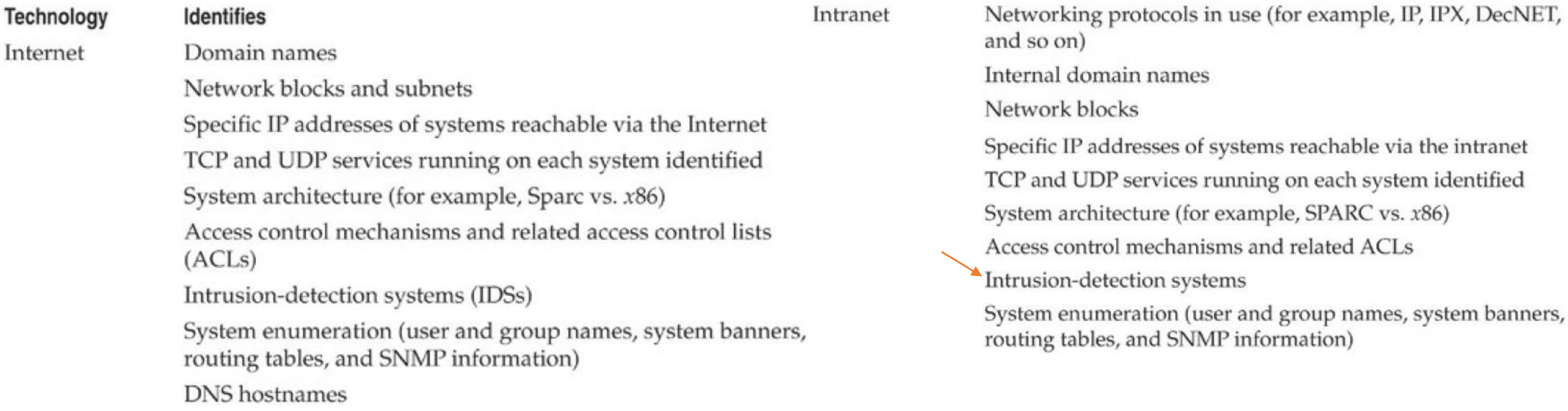
- Normally, a hacker will follow these steps to hack a system. Before a system / data damage really happens, everything is “reversible”. You can do your best to interrupt a hacker in any of the stages --- {Footprinting, Scanning, Enumeration, and Systems hacking}
- That is why we need a intrusion detection system
  - We will talk about this in the later class.
- We briefly go through these 4 stages and dive into the details, on each of them, in the later classes

Footprinting (reconnaissance)

- Before the real fun for the hacker begins, we need to do our good job in our first step --- the footprinting, the art of gathering information.
- Footprinting is about scoping out your target of interest, understanding everything connected around it, often without sending a single packet to your target. (info. about the target hardware / software and its role in the networks)
- It is like when bandits decide to rob a bank, they don’t just walk in and start demanding money (not the high IQ ones, anyway), instead, they take great pains to gather information about the bank—the armored car routes and delivery times, the security cameras and alarm triggers, the number of tellers and escape exits, the money vault access paths and authorized personnel, and anything else that will help in a successful attack.

Footprinting (reconnaissance)

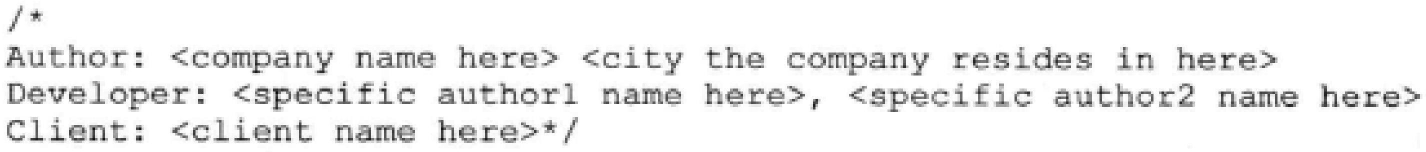
- Footptinting is a **systematic** way to help hackers to create a complete profile of a target’s (sometimes, it is a target’s organization) security posture.
- Here is a table. Those are the tasty footprinting nuggets



Technology	Identifies
Internet	Domain names
	Network blocks and subnets
	Specific IP addresses of systems reachable via the Internet
	TCP and UDP services running on each system identified
	System architecture (for example, Sparc vs. *x*86)
	Access control mechanisms and related access control lists (ACLs)
	Intrusion-detection systems (IDSs)
	System enumeration (user and group names, system banners, routing tables, and SNMP information)
	DNS hostnames
Intranet	Networking protocols in use (for example, IP, IPX, DecNET, and so on)
	Internal domain names
	Network blocks
	Specific IP addresses of systems reachable via the intranet
	TCP and UDP services running on each system identified
	System architecture (for example, SPARC vs. *x*86)
	Access control mechanisms and related ACLs
	Intrusion-detection systems
	System enumeration (user and group names, system banners, routing tables, and SNMP information)

Footprinting (reconnaissance)

- How to get the valuable information?
  - Patience! Patience! And Patience!
  - Publicly Available Information (Websites)
    - Seriously? I think there is nothing special?
    - Except for normal information, i.e. products, services they provide, recent events, emails, believe or not, sometimes, there are very interesting info. is hiding in the HTML “comment tags”.
      - It begins with a “<!--” and ends with a “-->”
    - You might easily find out the developer’s info. (If you are lucky enough)
    - You might easily find out the company who is in charge of the webpage developments



```
/*
Author: <company name here> <city the company resides in here>
Developer: <specific author1 name here>, <specific author2 name here>
Client: <client name here>*/
```

Footprinting (reconnaissance)

- Have a hard time to browse target's website? (So many levels of hierarchy in the links?)
  - Not a big deal! There is a tool called "**Teleport Pro**" in Windows.
  - By using this tool, I won't say you can 100% download the target company's website, but at least, to a level or some degrees.
  - You can find out something NOT in the current website because IT guys, they just **unlinked** the webpage.
    - For example, a retired professor's webpage or a retired product
- Little bit Luckiness ("Not" very publicly announced info.)
  - Some of the developers or IT, they are just getting lazy or forget to remove something.
  - So they forgot to turn off or remove the address like, http://www.companyname.com/test
  - It could be test1, test2,…
  - Similarly, "www" can be replaced as test1, test2,…
  - Let's try our Truman's webpage (A live demo here…don't tell them…)

Footprinting (reconnaissance)

- Social Engineering
  - We professors get lots of email from our Dean. In the email, he asks as to do something immediately
  - An angry customer who is complaining about the product. In this scenario, the “customer” can easily get the customer support manager or director’s email
- … (There are still many approaches, we will cover that in the later classes)

Scanning

- Generally speaking, there are 2 different types of scans
  - Port Scans
    - For example, in Windows, we can use a tools called “Advanced Port Scanner”
    - If we can know the ports are working in the target, we can know what types of the services, even the **version of the software**, are working in the target machine.
    - For example, in several **old** versions of Apache or MySQL, there are tons of vulnerabilities

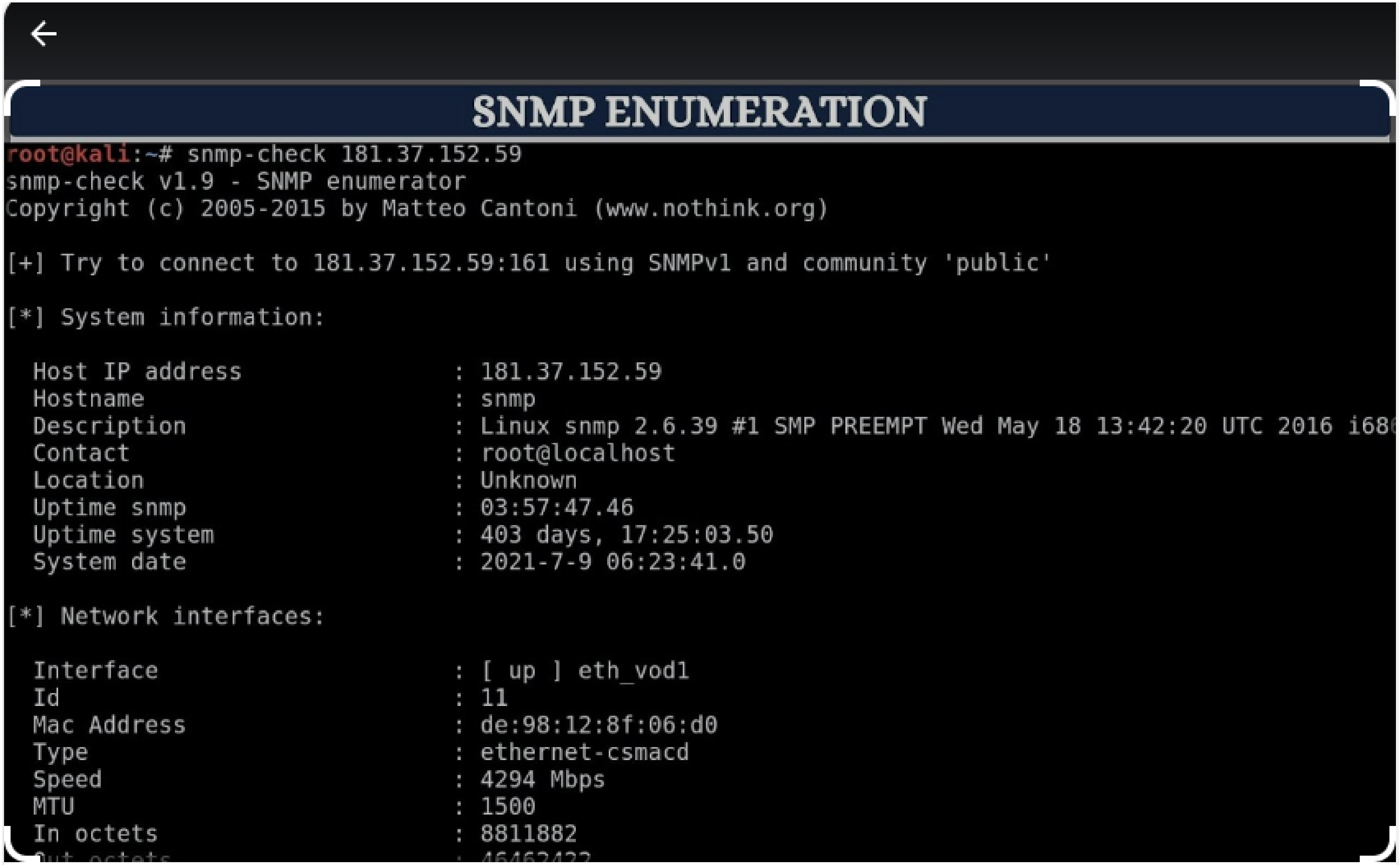
Scanning

- Network Scanning
  - How many hosts (computers) are touchable? What are they?
  - How many hosts are active now? What are they?
  - The ways of scanning?
    - **TCP connect**: see if the connection onto some port is working or not?
    - **FTP Bounce Scan**: see if some target can be used as our springboard to conduct the FTP Attack
    - **ICMP Scan**: it can stealthily scan the TCP port without being caught.
  - Normal users can install a firewall to block the hackers in this stage

Enumeration

- Hackers, they like to use some approach to enumerate user accounts, shared resources or applications in the target machine or a network.
- If a network is using SNMP…
  - SNMP stands for Simple Network Management Protocol.
  - It is originally used to do some management jobs
  - It can be used to “**do queries**” as well
  - There is a tool in Kali Linux called “snmp-check”
  - Check the next page for detail

Enumeration



SNMP ENUMERATION

```
root@kali:~# snmp-check 181.37.152.59
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 181.37.152.59:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address                : 181.37.152.59
  Hostname                       : snmp
  Description                    : Linux snmp 2.6.39 #1 SMP PREEMPT Wed May 18 13:42:20 UTC 2016 i68
  Contact                        : root@localhost
  Location                       : Unknown
  Uptime snmp                    : 03:57:47.46
  Uptime system                  : 403 days, 17:25:03.50
  System date                    : 2021-7-9 06:23:41.0

[*] Network interfaces:

  Interface                      : [ up ] eth_vod1
  Id                             : 11
  Mac Address                    : de:98:12:8f:06:d0
  Type                           : ethernet-csmacd
  Speed                          : 4294 Mbps
  MTU                            : 1500
  In octets                      : 8811882
  Out octets                     : 46462422
```

Systems hacking

- Password hacking (The most commonly seen approach)
  - Dictionary: Try all the possible vocabulary words
  - Brute force: Try all the possible permutation in the characters or symbols
  - Hybrid:
    - For example: Dictionary + Brute force. This is even more efficient
    - If we can know the length of the system password. That would be perfect!
    - For example, in some of the commercial website, an user’s password in an account has a limitation in its length. The hybrid approach would be very effective in this kind of use case
- … (Still many approaches)