

HCIA Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 5



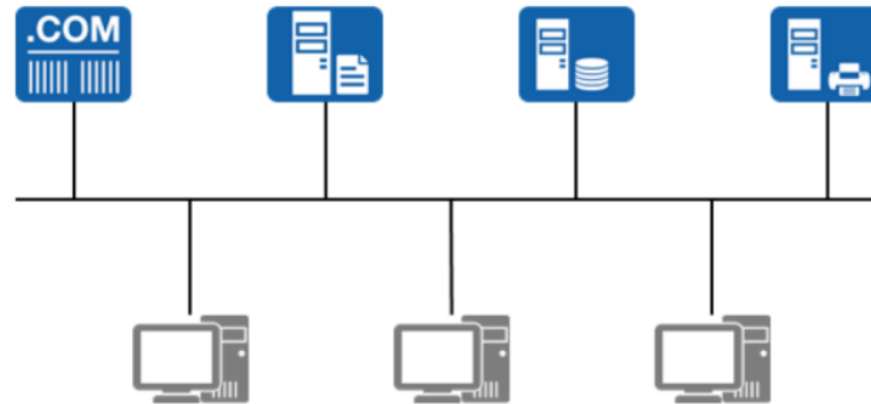
جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

Common Server Types and Threats

- In a broad sense, a server is a computer system that provides services to other machines over a network.
- More specifically, a server is a high-performance computer that provides business services to external computers through a network. Therefore, servers require higher stability, security, and performance than common PCs.

- **Upon completion of this course, you will be able to describe:**
 - ❑ **Categories of servers**
 - ❑ **Functions of common servers**
 - ❑ **Security threats to common servers**
 - ❑ **Vulnerabilities and patches**

- A server is a high-performance computer that provides services (including query, storage, and computing) to clients over a network.
- A server mainly provides services such as web application, file download, database-based storage, and printing.
- Today, servers are in wide use. Online games, websites, and most software need to be stored on servers. Some enterprises may deploy their own servers and store the most important work-related documents on hard disks of these servers.
- All servers are, to put it simply, just like the computers we use from day to day, but with better stability, security, and data processing performance. Our home computers can also be used as servers if a server system is installed. However, as mentioned already, servers have high requirements on hardware stability and quality. Common computers cannot stay powered on for a long time, and important data is generally stored on servers. Therefore, common computers are not suitable for use as servers.



- **Availability:** A server must be reliable because it provides services to the clients on the entire network, not to the users who log in to the server. The server must not be interrupted as long as there are users on the network. In some scenarios, a server cannot be interrupted even if nobody is using the server. This is because the server must continuously provide services for users. Servers in some large enterprises, such as website servers and web servers used by public users, need to provide 24/7 services.
- **Usability:** A server needs to provide services to multiple users and therefore requires high connection and computing performance. When using a PC, we sometimes feel it is slow. If a server has the same performance as a PC, can it be accessed by so many users at the same time? The answer is obviously no. Therefore, the performance of a server must be much higher than that of a PC. To achieve high-speed performance, a symmetric multiprocessor is installed, and a large number of high-speed memory modules are inserted to improve the processing capability.
- **Scalability:** With the continuous development of services and the increasing number of users, servers should be scalable. To ensure high scalability, a server must provide scalable space and redundant parts (such as disk array space, PCI-E slots, and memory slots).
- **Manageability:** To ensure high reliability of services, a server must support technologies that common PCs cannot, such as two-node cluster backup, system backup, online diagnosis, and fault warning. Faults in a server should be rectified without having to shut the server down.

Indicator	Servers	PCs
Processor performance	Multiprocessor supported High performance	Multiprocessor usually not supported Low performance
Availability	High	Relatively low
Usability	High	Relatively low
Scalability	High	Relatively low
Manageability	High	Relatively low

Classification Criteria	Server type
By application level	Entry-level server Work group server Department-level server Enterprise-level server
By system architecture	Non-x86 server x86 server
By appearance	Rack server Blade server Tower server Cabinet server
By usage	General-purpose server Function server

- **Entry-level server:** Small departments typically use an entry-level server for file and printing services. Generally, an entry-level server will suffice.
- **Work group server:** If the application is not complex, for example, no large database needs to be managed, a work group server is usually used.
- **Department-level server:** Department-level servers feature high availability, reliability, scalability, and manageability. They are applicable to websites and data centers of medium-sized enterprises.
- **Enterprise-level server:** Enterprise-level servers are mainly used in large enterprises and industries with important services (such as finance, transportation, and communications), for which a large amount of data must be processed and there is a high requirement for fast processing as well as high reliability.
- **x86 server:** A CISC server, that is, a PC server. Such a server uses Intel or other processors that are compatible with the x86 instruction set.
- **Non-x86 servers:** include mainframe, midrange, and Unix servers. They use RISC or EPIC processors.
- **General-purpose server:** Not designed for a specific service and can provide various service functions.
- **Function server:** Specially designed for providing one or several functions and supports plug-and-play, eliminating the need for trained personnel to configure software and hardware.

- Best-selling servers
- Small chassis
- Multiple servers can be installed in one cabinet.

- What is U?
- U is the unit for the height of a rack server.
- $1\text{U} = 1.75\text{ inch} = 1.75 \times 25.4\text{ mm} = 44.45\text{ mm}$
- Common Huawei rack servers include RH1288H, RH2288H, RH5288, RH2488/2488H, and RH5885H.



1U rack server



2U rack server



4U rack server

- Traditional server type
- Large chassis dimensions
- Strong internal scalability
- Large area occupied



- High-density server
- Energy efficient
- Centralized management
- Quick deployment



- High-end enterprise server with a complex internal structure that includes a large number of devices
- With a cabinet server, many different device units or several servers may be placed in the same cabinet.



- **Server software works in client/server (C/S) or browser/server (B/S) mode.**

There are many forms of servers, including

- ☐ **File server**
- ☐ **Database server**
- ☐ **Mail server**
- ☐ **Web server**
- ☐ **FTP server**
- ☐ **Domain Name System (DNS) server**
- ☐ **Time synchronization server (NTP server)**
- ☐ **Proxy server**

- A file server is a computer that can provide file sharing services to clients. It may be a general-purpose server that can run other applications or a function server that provides only file services.
- In C/S mode, a file server is a computer used for central storage and data file management. It enables other computers on the same network to access these files. A file server allows users to share information on the network without the need for floppy disks or other external storage media to physically move files. Any computer can be set up as a file server, of which the simplest form is a PC. It processes file requests and sends them over the network. On a more complex network, a file server may also be a dedicated network attached storage (NAS) device. It can also be used as a remote hard disk drive of another computer, and allows users on the network to store files on the server in the same way as on their own hard disks.

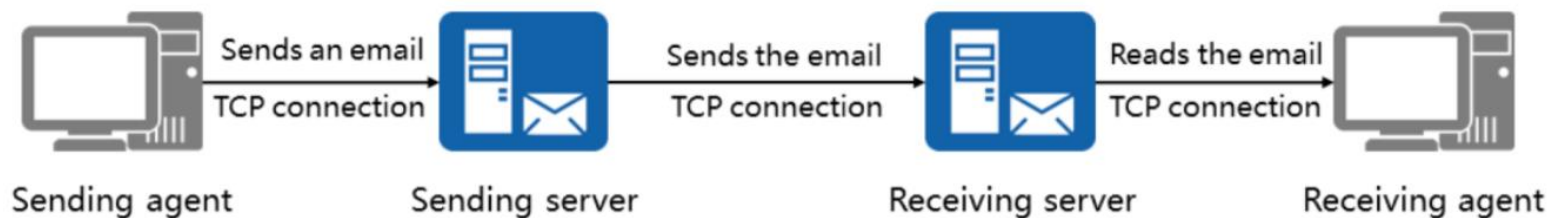


- One or more computers and database management system software running on a LAN form a database server that provides services for customer applications. These services include query, update, transaction management, index, high-speed cache, query optimization, security, and multi-user access control.
- A database server is built with a database system as its foundation. Such a server has the features of a database system as well as its own unique functions. These functions are:
 - Database management, including system configuration and management, data access and update management, data integrity management, and data security management.
 - Database query and manipulation, including database retrieval and modification.
 - Database maintenance, including data import and export management, database structure maintenance, data restoration, and performance monitoring.
 - Database concurrent operations: Because more than one user accesses a database simultaneously, the database server must support concurrent operations so that multiple events can be processed at the same time.

- A mail server is a device used to manage the sending and receiving of emails. It is more secure and efficient than free email services on the Internet, making it a must-have for enterprises.

➤ Mail servers that work in C/S mode:

- An email system consists of three components: user agent, mail server, and mail transfer protocol.
- User agent: application that handles the sending and receiving of emails
- Mail server: used to receive emails from a user agent and send the emails to the receiving agent.
- Mail transfer protocol: protocol used in the mail transfer process



- An FTP server is a computer that provides file transfer and access services on the network.

❖ FTP:

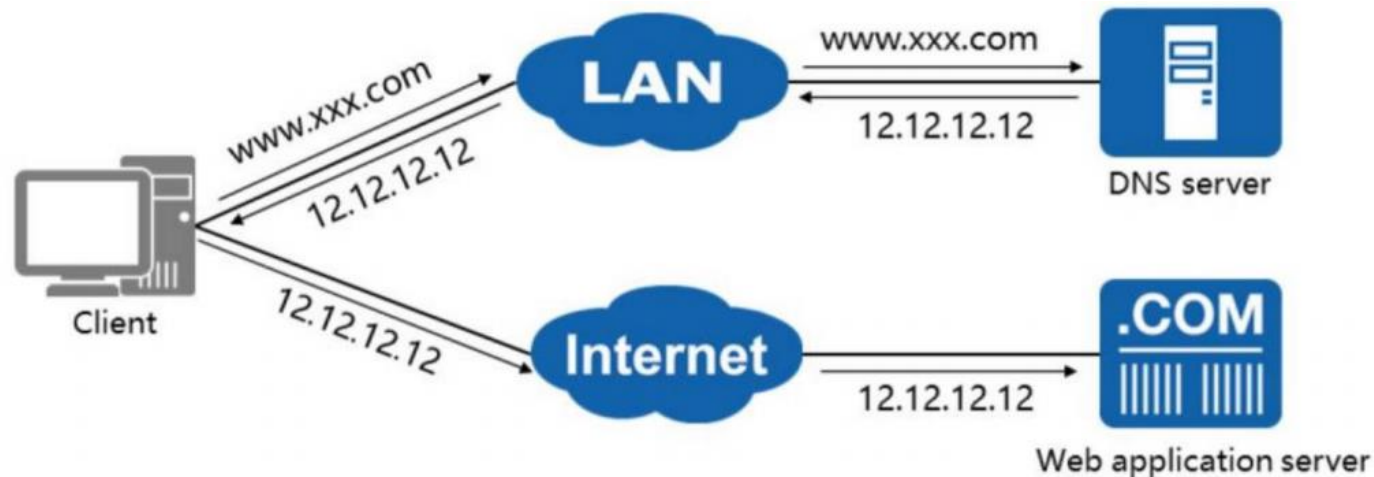
- ☐ Transfers and manages files.
- ☐ Provides user identities of different levels: user, guest, and anonymous.
- ☐ Records commands and login files.
- ☐ Changes the root directory of a user (chroot).



- An FTP server provides upload and download functions in text transmission.
 - ☐ Upload: A file is sent from a PC to an FTP server.
 - ☐ Download: The file is transferred from the FTP server to the PC.

- FTP works in client/server mode. The client and server are connected using TCP. An FTP server mainly uses ports 21 and 20. Port 21 is used to send and receive FTP control information and keep FTP sessions open. Port 20 is used to send and receive FTP data.

- A DNS consists of a DNS resolver and a DNS server.
- A DNS server is a computer that stores the domain names and IP addresses of all hosts throughout the network and can convert a domain name into the corresponding IP address.
- Computers use an IP address to find websites on the internet. However, IP addresses can be difficult to remember for users. Therefore, an IP address has a corresponding web address, called a domain name. Computers use a DNS server to convert a domain name into its corresponding IP address and find its location on the network.
- Note:
 - A domain name must correspond to a unique IP address. An IP address can correspond to multiple domain names or have no corresponding domain name.



- Which security threats may affect the running of a server?



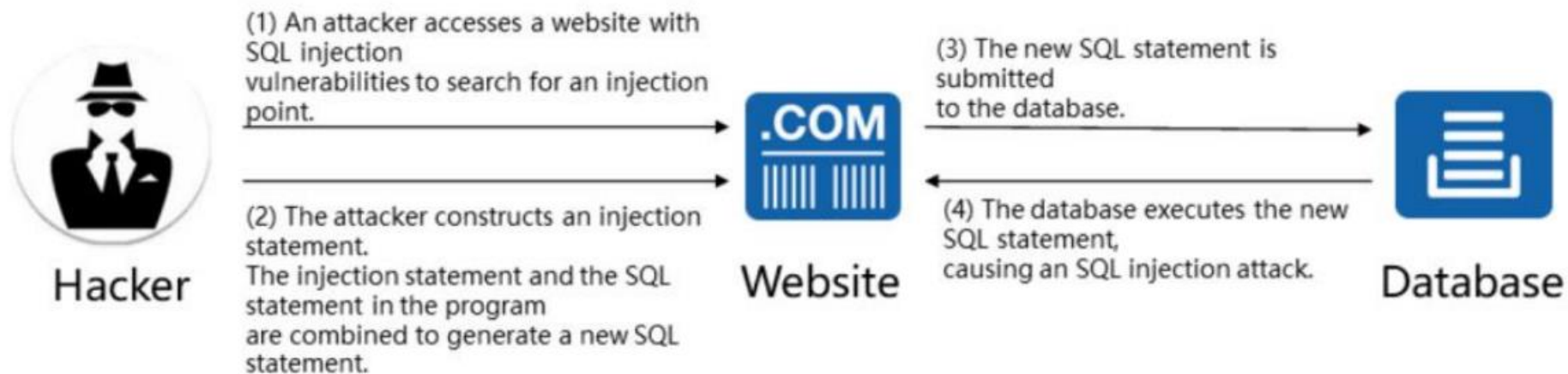
- Malicious programs are usually written with attack intention.
- Threats from malicious programs can be divided into two categories:
 - Threats dependent on host programs that cannot take effect without an application.
 - Independent threats in a self-contained program that can be scheduled and run by an operating system
- Malicious programs include Trojan horses, worms, and viruses.
- Trojan horse: A Trojan horse is a program or command procedure that appears harmless but is in fact malicious. It contains hidden code that, when invoked, performs an unwanted or harmful function.
- Worm: A worm is a virus program that can replicate itself and send copies from computer to computer across network connections.
- Virus: A virus is an aggressive program that embeds a copy of itself in other files to infect computer systems.



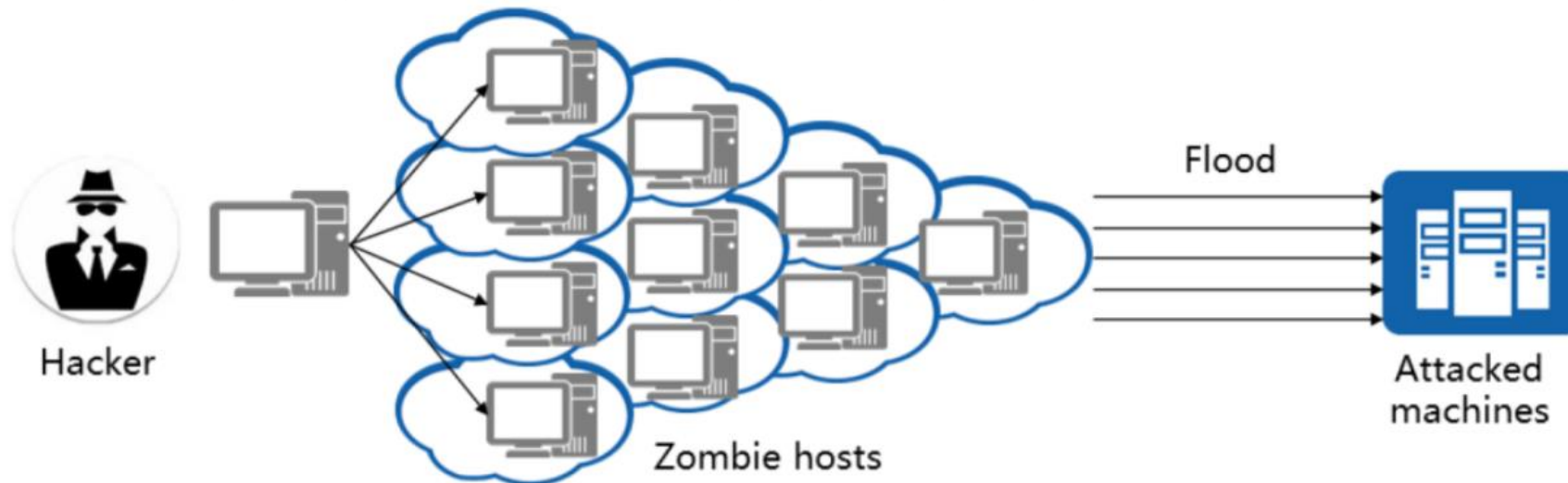
- If hackers fail to acquire a password by conventional means, they may use brute force to crack the password.
- Brute force cracking is an exhaustive search method in which a hacker tries many combinations to obtain the password.



- An SQL injection attack inserts malicious SQL commands into the input field of a web form or the query string of a page request to deceive the server to execute malicious SQL commands.
- The commands entered are used to build (or manipulate) dynamic SQL commands or as input parameters for storage procedures. Such forms are particularly vulnerable to SQL injection attacks. For non-web CS framework systems, SQL injection risks also exist.



- Distributed denial of service (DDoS) attacks target large sites such as commercial companies, search engines, and government departments. A DDoS attack is launched by multiple controlled machines to a specified target. It is destructive and difficult to prevent.
- An attack that causes denial of service is called a DoS attack. A DoS attack is designed to disrupt a computer or network service.
- Most DoS attacks are based on flooding a network with requests in order to disrupt its systems; however, it is difficult for individual hackers to overload high-bandwidth resources. To overcome this disadvantage, DoS attackers develop distributed denial-of- service (DDoS) attacks.
- In a DDoS attack, Trojan horses are used by hackers to control other computers. More and more computers are turned into zombies and are exploited by hackers to launch attacks. Hackers utilize many zombies to initiate many attack requests to the same target and overwhelm its system. Because the requests come from multiple computers, they cannot be stopped by locating a single source.



Security Threat	Defense Method
Malicious program	1. Do not install suspicious software. 2. Do not open a link from an unknown sender. 3. Install antivirus software. 4. Do not access suspicious websites.
Brute force cracking by hackers	1. Set complex passwords. 2. Change the default port number. 3. Disable password login, and only allow login using an authenticated secret key.
SQL injection attack	1. Use regular expressions to filter input parameters. 2. Use PreparedStatement instead of Statement. 3. Invoke this function in JavaServer Pages to check for invalid characters.
DDoS	1. Source authentication 2. Fingerprint learning 3. Domain name redirection

- A vulnerability is a defect or weakness in the hardware, software, or protocols of computer systems or in system security policies.
- In 1990, Dennis Longley and Michael Shain defined vulnerability as follows in The Data and Computer Security Dictionary of Standard, concepts, and Terms:
 - In computer security, a weakness in automated system security procedures, administrative controls, internal controls, etc. that could be exploited by a threat to gain unauthorized access to information or to disrupt critical processing.
- Vulnerabilities are unknown and cannot be discovered in advance.
- Vulnerabilities are security risks, which may expose computers to attacks by viruses or hackers.
- If a vulnerability is exploited, the consequences are unpredictable.
- Vulnerabilities can be exploited remotely.
- Generally, vulnerabilities can be fixed.



- **Permission bypass and permission escalation are mainly used to obtain expected data operation capabilities, for example, increasing the permissions of common users and obtaining administrator permissions.**
- **In a DoS attack, the attacker obtains the control rights of certain services in the system to stop the services.**
- **Data leakage is mainly caused by hackers' accessing protected data, such as reading restricted files and publishing server information.**
- **The execution of an unauthorized instruction forces a program to execute input content as code. This obtains the access permission of the remote system or higher permissions of the local system. Examples are SQL injection and buffer overflow.**
- **The existence of vulnerabilities is one of the necessary conditions for successful network attacks. The key to successful invasions is the early detection and exploitation of vulnerabilities in the target network system.**
- **The security threats of vulnerabilities to network systems include escalation of common users' rights, obtaining local and remote administrator rights, local and remote DoS, server information leakage, unauthorized remote file access, reading restricted files, and spoofing.**

Vulnerability Classification

- By exploitation method: local and remote attack vulnerabilities

- By location:

- | | |
|---|---|
| ☐ Operating system | ☐ Hardware |
| ☐ Network protocol stack | ☐ Communication protocol |
| ☐ Non-server program | ☐ Password recovery |
| ☐ Server program | ☐ D Other types |

- System security threat vulnerabilities based on the potential threats to systems and possibility of being exploited:

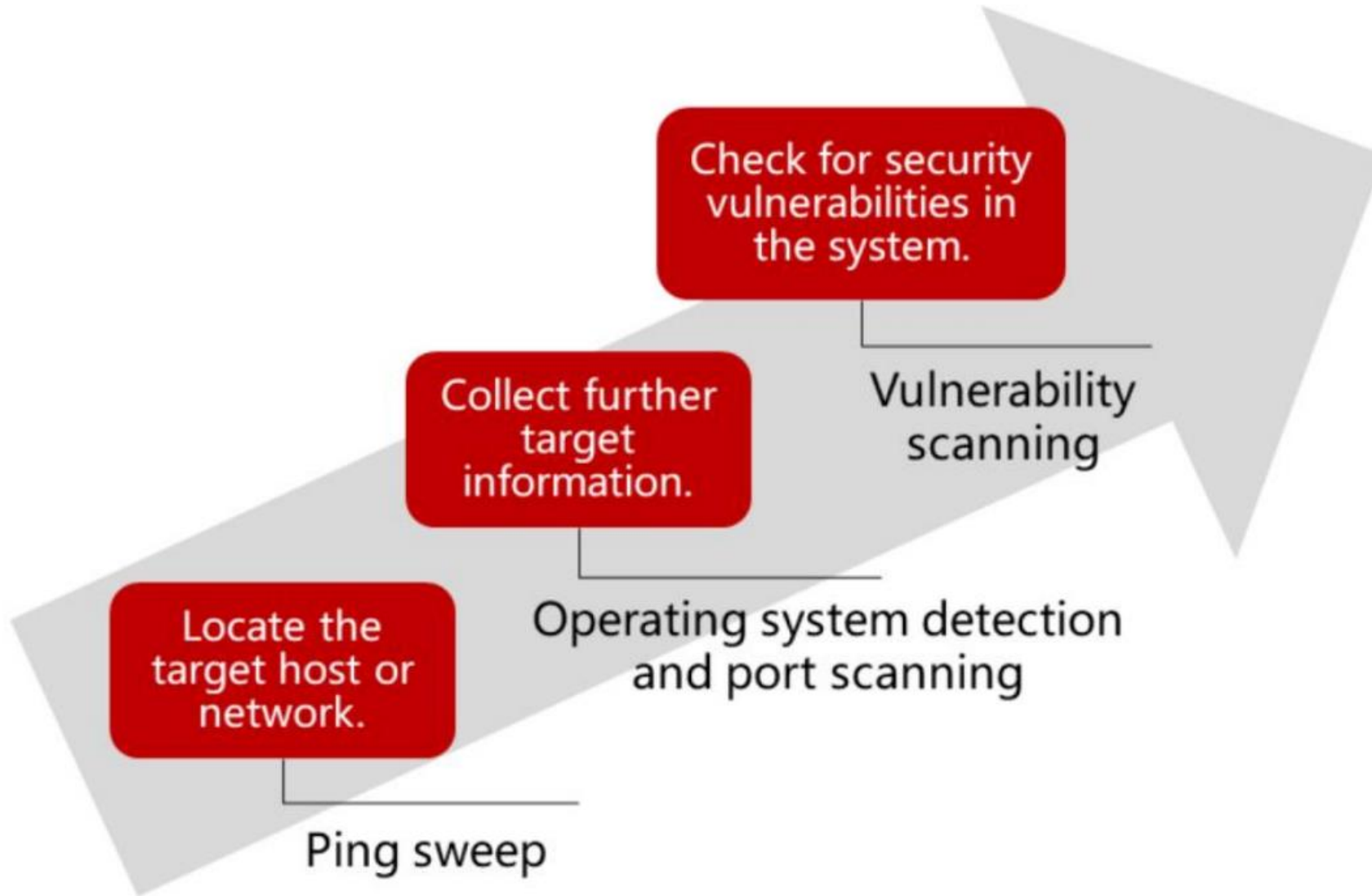
- ☐ High-level vulnerabilities
- ☐ Medium-level vulnerabilities
- ☐ Low-level vulnerabilities

- Attackers who exploit local attack vulnerabilities can be local authorized users or unauthorized users who have obtained local rights through other methods.
- Attackers who exploit remote attack vulnerabilities attack remote hosts on networks.
- High-level vulnerabilities can be exploited to obtain administrator permissions.
- Medium-level vulnerabilities can be exploited to obtain the permissions of common users, read restricted files, and reject services.
- Low-level vulnerabilities can be exploited to read unrestricted files and leak server information.
- Of course, there are more vulnerability categories. For example, the status of a vulnerability can be known, unknown, and zero-day.

Vulnerabilities can also be classified by user groups, such as Windows, Linux, Internet Explorer, and Oracle vulnerabilities.

- Defects in software or protocol design
 - Bugs in software compilation
 - Improper system configuration
 - Limited security awareness
-
- Vulnerabilities are "inevitable". This is determined by the complexity of systems.





- Port scanning
 - Full connection scanning
 - SYN scanning
 - Stealth scanning
- System vulnerability scanning
 - Passive scanning
 - Active scanning



Common scanning methods

- **Full connection scanning:** The scanning host establishes a complete connection with a specified port on the target host through a three-way TCP/IP handshake. If the port is in the listening state, the connection is successful. Otherwise, the port is unavailable.
- **SYN scanning:** The scanner sends an SYN packet to the target host. If an RST packet is received in reply, it indicates that the port is disabled. If the response packet contains SYN and ACK, the port is in the listening state. Then, the scanner can send an RST packet to the target host, to stop the host's connection with the port.
- **Stealth scanning:** The scanner sends a FIN packet to the target host. If the FIN packet reaches a disabled port, the packet is discarded, and an RST packet is returned. If the port is enabled, the FIN packet is simply discarded.
- **Passive scanning:** Based on host detection. It checks inappropriate settings, weak passwords, and other objects that do not comply with security rules.
- **Active scanning:** Based on networks. It attacks the system by executing some script files and records the system response. In this way, vulnerabilities can be detected.

Definition of Patch

- Issues with operating systems are often discovered by hackers or virus designers or generated during the use of a system. Developers collect these errors and develop a patch. A patch is a set of changes designed to update a program and fix security vulnerabilities.
- A patch is a small piece of cloth used to mend or cover a hole in a garment or blanket. It also refers to a small program that is released to solve issues (usually discovered by hackers or virus designers) exposed during the use of a large software system (such as Microsoft operating system). Bugs cannot be avoided in software. If any bugs are found, a patch can be developed for the software and installed to fix them. Developers release patches for download on their official websites.



Now I know how to scan vulnerabilities. But how can I harden my host if vulnerabilities are found?

It's very simple. If your clothes have a hole, what should you do?



Well, I will patch them. Oh, got it. If my computer has a vulnerability, I can use a patch to fix it.

WannaCry Ransomware Attack

On May 12, 2017, the WannaCry worm that exploited the MS17-010 vulnerability spread globally and infected a large number of computers. Ransomware viruses were implanted in infected computers and encrypted a large number of files on the computers. After a victim's computer was locked by a hacker, the virus demanded the user pay \$300 (USD) of Bitcoin to retrieve their files.

- WannaCry uses the vulnerabilities of port 445 in the Windows operating system to propagate and self-replicate.
- After a computer is penetrated by the ransomware, many types of files in the user host system, such as photos, pictures, documents, audios, and videos, are encrypted. The file name extension of the encrypted files is changed to .WNCRY, and a ransom dialog box is displayed on the desktop, asking the victim to pay \$300 (USD) of Bitcoin to the attacker's bitcoin wallet. The ransom increases over time.



- In March 2016, a new security vulnerability, DROWN, was found in the open-source encryption tool OpenSSL used by about two-thirds of the world's website servers.
- The vulnerability allowed hackers to attack websites and read encrypted information such as passwords, credit card accounts, business secrets, and financial data. This was a huge security challenge for global websites. More than 100,000 websites in China were affected.
- Users must periodically scan their computers, upgrade software to the latest versions, check software configurations, disable insecure options, and pay attention to the recommendations of security companies. These are effective means to avoid vulnerabilities.

OPEN SSL

How Do You Defend Against These Vulnerabilities?

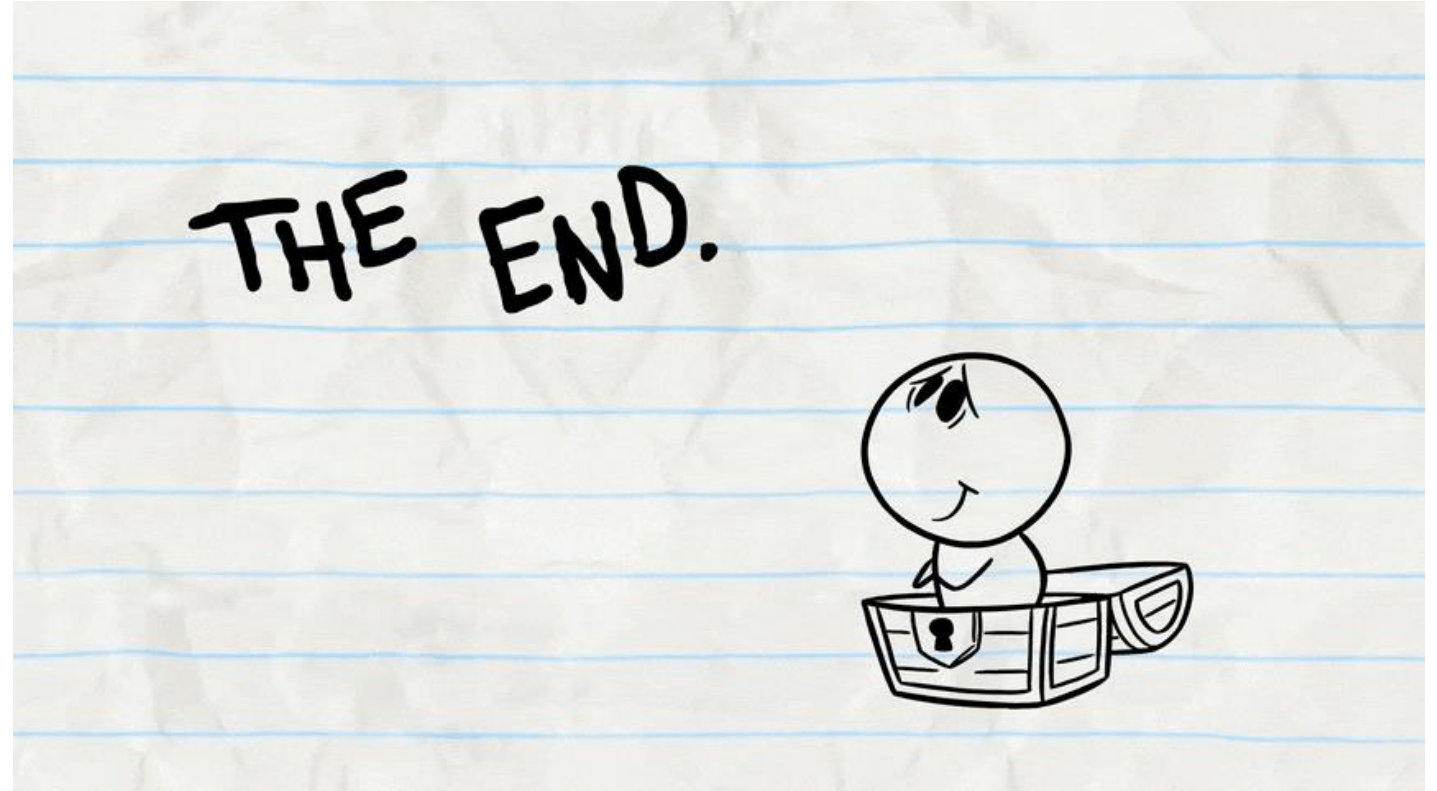
- How to implement these defenses?



The End

Please feel free to contact me anytime if you have any questions

Abdelrhman Ahmed Refaat:
abdelrhmanahmedrefaat@gmail.com



جامعة القادسية
EVERYONE'S SMART UNIVERSITY