中山大學
SUN YAT-SEN UNIVERSITY

Module II. Internet Security

Chapter 5

Network Attack and Defence

Web Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- ❑ **5.1 Introduction**
  - Network Security Crisis
  - Hacking & Hackers
  - Network Threats
  - Steps of Network Attack
  - Methods of Network Defense
- ❑ **5.2 Network Attacks**
  - Computer Network Attack
  - Common Types of Network Attack
  - Port Scan
  - Idle Scan
- ❑ **5.3 Password Cracking**
  - The Vulnerability of Passwords
  - Password Selection Strategies
  - Password Cracking
  - Password Cracking Tools

Outline

- ❑ **5.4 Buffer Overflow**
  - ◆ Background
  - ◆ Classification
  - ◆ Practicalities
  - ◆ Protection
- ❑ **5.5 Spoofing Attack**
  - ◆ ARP Cache Poisoning
  - ◆ DNS Spoofing
  - ◆ Web Spoofing
  - ◆ IP Spoofing

5.1 Introduction

5.1.1 Network Security Crisis

❑ Cyber Space and Cybersecurity

- **ISO/IEC 27032:2012:** Information technology – Security techniques – Guidelines for cybersecurity
  - ✧ "the *Cyberspace*" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.”
  - ✧ *Cybersecurity* is "preservation of confidentiality, integrity and availability of information in the Cyberspace"

5.1 Introduction

5.1.1 Network Security Crisis

❑ Cyber Space and Cybersecurity

- **ITU:** *Cybersecurity* is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.
  - ✧ Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.
  - ✧ Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality.

5.1 Introduction

5.1.1 Network Security Crisis

❑ **Network Security Crisis**

- 网络安全危机主要来自两方面
  - ✧ 利用网络进行有害信息的传播活动，或利用网络对正常信息进行不正当使用，包括污染和滥用信息、攻击和破坏信息等。
  - ✧ 利用各种技术手段直接侵害网络本身，扰乱信息传播的顺利进行，包括利用信息手段窃取、利用信息手段欺诈和勒索等。
- 网络安全危机主要表现为
  - ✧ 病毒、蠕虫和木马
  - ✧ 黑客和黑客程序
  - ✧ 信息生态恶化

5.1 Introduction

5.1.1 Network Security Crisis

❑ **Virus**

- A *virus* is a malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Infected computer programs can include, as well, data files, or the "boot" sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Viruses usually lead to some sort of data loss and/or system failure.
- There are numerous methods by which a virus can get into a system:
  - ✧ Through infected plug-in devices like U-disks
  - ✧ Through an e-mail attachment infected with the virus
  - ✧ Through downloading software infected with the virus

5.1 Introduction

5.1.1 Network Security Crisis

❑ **Virus**

- 计算机病毒
  - ✧ 《中华人民共和国计算机信息系统安全保护条例》：编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。
  - ✧ 病毒程序在计算机系统运行的过程中将自身复制到其他程序体内，造成数据丢失或系统失效。病毒具有传染性、隐蔽性、激发性、复制性、破坏性等特点，既可以感染桌面计算机，也可以感染网络服务器。随着网络技术的发展，计算机病毒的种类越来越多，扩散速度不断加快，具有很大的破坏性。
  - ✧ 病毒必须满足两个条件：(1) 自行执行。病毒代码通常置于另一个程序的执行路径中。(2) 自我复制。例如，它可能用受病毒感染的文件副本替换其他可执行文件。

5.1 Introduction

5.1.1 Network Security Crisis

❑ **Virus**

- A few common types of viruses are:
  - ✧ *Boot sector viruses*
    - ◌ 引导区病毒
    - ◌ infect a hard drive’s master boot record, loaded into memory whenever the system starts or is rebooted.
  - ✧ *File viruses or program viruses or parasitic viruses*
    - ◌ 文件病毒/程序病毒/寄生病毒
    - ◌ attached to executable programs, loaded into memory whenever the particular program is executed.
  - ✧ *Multipartite viruses*
    - ◌ 综合病毒
    - ◌ a combination of a boot sector virus and a file virus.

5.1 Introduction

5.1.1 Network Security Crisis

❑ **Virus**

- A few common types of viruses are:
  - *Macro viruses*
    - 宏病毒
    - written in macro languages that applications use, of which Microsoft Word is one. Macro viruses usually infect systems through e-mail.
  - *Polymorphic viruses*
    - 多态病毒
    - These viruses can be considered the more difficult viruses to defend against because they can modify their code. Virus protection software often find polymorphic viruses harder to detect and remove.

5.1 Introduction

5.1.1 Network Security Crisis

❑ Worm

- A *worm* is an autonomous code that spreads over a network, targeting hard drive space and processor cycles. Worms not only infect files on one system, but spread to other systems on the network. The purpose of a worm is to deplete (耗尽) available system resources, hence the reason for a worm repeatedly making copies of itself. Worms basically make copies of themselves or replicate until available memory is used, bandwidth is unavailable, and legitimate network users are no longer able to access network resources or services. Whereas viruses almost always corrupt or modify files on a targeted computer.

5.1 Introduction

5.1.1 Network Security Crisis

❑ Worm

- A few previously encountered worms are:
  - The *ADMw0rm worm* took advantage of a buffer overflow in Berkeley Internet Name Domain (BIND).
  - The *Code Red worm* utilized a buffer overflow vulnerability in Microsoft Internet Information Services (IIS) version 4 and IIS version 5.
  - The *LifeChanges worm* exploited a Microsoft Windows weakness, which allowed scrap shell files to be utilized for running arbitrary code.
  - The *LoveLetter worm* used a Visual Basic Script to replicate or mass mail itself to all individuals in the Windows address book.
  - The *Melissa worm* utilized a Microsoft Outlook and Outlook Express vulnerability to mass mail itself to all individuals in the Windows address book..

5.1 Introduction

5.1.1 Network Security Crisis

❑ **Worm**

- A few previously encountered worms are:
  - ✧ The *Morris worm* exploited a Sendmail debug mode vulnerability.
  - ✧ The *Nimda worm* managed to run e-mail attachments in HTML messages through the exploitation of HTML IFRAME tag.
  - ✧ The *Slapper worm* exploited an Apache Web server platform buffer overflow vulnerability.
  - ✧ The *Slammer worm* exploited a buffer overflow vulnerability on unpatched machines running Microsoft SQL Server.
  - ✧ Stuxnet, in development since at least 2005, is first uncovered in 2010 by Kaspersky Labs. Stuxnet targets SCADA control system architectures and was responsible for causing substantial damage to Iran‘s nuclear program. Although neither country has admitted responsibility, since 2012 stuxnet is frequently described as a jointly built American/Israeli cyberweapon.

5.1 Introduction

5.1.1 Network Security Crisis

❑ **Worm**

- 蠕虫是一种广义的计算机病毒，通过网络进行传播。它具有病毒的一些共性，如传播性、隐蔽性、破坏性等等，同时与一般的计算机病毒又有很大区别。蠕虫是一类独立存在的恶意程序，不必寄生在宿主程序或文件中 (有的只存在于内存中)，和黑客技术相结合，利用系统漏洞进行传播，传染目标是互联网络的所有计算机。
- 蠕虫程序控制受感染的计算机进行传播和大量复制到其他计算机上，其主要目的是大量消耗系统资源，破坏系统可用性 (实施 DoS 攻击)。互联网络的发展使得蠕虫可以在短短的时间内蔓延到整个网络，其主动攻击性和突然爆发性会造成巨大的破坏，其危害远大于一般病毒。

5.1 Introduction

5.1.1 Network Security Crisis

❑ Trojan

- A *Trojan horse* or Trojan is a file or e-mail attachment disguised as a friendly, legitimate file. When executed though, the file corrupts data and can even install a backdoor that hackers can utilize to access the network.
- A Trojan horse differs from a virus or worm in the following ways:
  - Trojan horses disguise (伪装) themselves as friendly programs. Viruses and worms are much more obvious in their actions.
  - Trojan horses do not replicate like worms and viruses do.

5.1 Introduction

5.1.1 Network Security Crisis

❑ Trojan

- A few different types of Trojan horses are listed here:
  - ✧ *Keystroke loggers* monitor the keystrokes that a user types and then e-mails the information to the network attacker.
  - ✧ *Password stealers* are disguised as legitimate login screens that wait for users to provide their passwords so that hackers can steal them. Password stealers are aimed at discovering and stealing system passwords for hackers.
  - ✧ *Remote administration tools (RATs)* are used *to* gain control over the network from some remote location.
  - ✧ *Zombies* are typically used to initiate distributed denial of service (DDoS) attacks on the hosts within a network.

5.1 Introduction

5.1.1 Network Security Crisis

❑ Trojan

- “计算机木马/特洛伊木马”源于希腊神话的“特洛伊木马”，指那些经过表面伪装、实际目的却是危害计算机安全并导致严重破坏的计算机程序。
- 木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。隐蔽性是指木马的设计者为了防止木马被发现，会采用多种手段隐藏木马，这样服务端即使发现存在感染木马的症状，也难以确定其具体位置；非授权性是指一旦控制端与服务端成功连接，控制端将可能窃取服务端的操作权限，如修改文件、修改注册表、控制鼠标键盘、窃取信息等。

5.1 Introduction

5.1.1 Network Security Crisis

❑ Trojan

- 木马与一般计算机病毒的主要区别是木马不具传染性，它并不能像病毒那样复制自身，也并不刻意地去感染其他文件。木马将自身伪装起来，吸引用户下载执行，以窃取用户相关信息为主要目的，通常由控制端触发或由预设条件触发，而在日常例行运行中刻意掩盖其存在的痕迹。
- 木马中包含在触发时危害系统信息安全的恶意代码，并在宿主计算机上得到有效启用。例如将代码作为电子邮件附件，引诱用户下载执行；或者将木马程序捆绑在应用软件中，上传到资源网站，引诱用户下载执行等。
- 典型的特洛伊木马有灰鸽子、网银大盗等。

5.1 Introduction

5.1.1 Network Security Crisis

❑ Deterioration of Information Ecology

- Information Ecology
  - ✧ 信息生态是信息、人、信息环境 (技术) 的协调结构 (Cyber Space Ecology)。
  - ✧ 人类对信息资源开发和管理不当，会导致信息生态失衡甚至恶化 (Deterioration)，使人类和信息环境的冲突日益尖锐。网络技术的快速发展和网络信息的泛滥，使人类处理与利用信息的能力大大落后于信息的生产和传播能力。
- Information Poverty and Worldwide Digital Divide
  - ✧ 信息分布不均导致了信息贫富差距扩大。占世界人口20%的发达国家拥有全世界信息量的80%，而占世界人口80%的发展中国家只拥有信息总量的20%，发展中国家正面临着一种新形式贫困 - 信息贫困的威胁，全球性的数字鸿沟已经形成。

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The term *hacking* initially referred to the process of finding solutions to rather technical issues or problems. Now hacking refers to the process whereby intruders maliciously attempt to compromise the security of corporate networks to destroy, interpret, or steal confidential data or to prevent an organization from operating.
- Terminologies that refer to criminal hacking
  - ✧ Cracking
  - ✧ Cybercrime
  - ✧ Cyberespionage (网络间谍)
  - ✧ Cyberweapon
  - ✧ Phreaking (Phone-breaking)

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Footprinting* (跟踪)
    - This is basically the initial step in hacking a corporate network. Here the intruder attempts to gain as much information on the targeted network by using sources that the public can access. The aim of footprinting is to create a map of the network to determine what operating systems, applications, and address ranges are being utilized and to identify any accessible open ports.
    - The methods used to footprint a network
      - Access information publicly available on the company website to gain any useful information.
      - Try to find any anonymous FTP sites and intranet sites that are not secured.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Footprinting*
    - The methods used to footprint a network
      - Gather information on the company’s domain name and the IP address block being used.
      - Test for hosts in the network’s IP address block. Tools such as Ping or Flping are typically used.
      - Using tools such as Nslookup, the intruder attempts to perform DNS zone transfers.
      - A tool such as Nmap is used to find out what the operating systems are that are being used.
      - Tools such as Tracert are used to find routers and to collect subnet information.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Port scanning* (端口扫描)
    - Port scanning or scanning is when intruders collect information on the network services on a target network. Here, the intruder attempts to find open ports on the target system.
    - The different scanning methods that network attackers use
      - Vanilla (unexciting) scan/SYNC scan: TCP SYN packets are sent to each address port in an attempt to connect to all ports. Port numbers 0 – 65,535 are utilized.
      - Strobe scan: The attacker attempts to connect to a specific range of ports that are typically open on Windows based hosts or UNIX/Linux based hosts.
      - Sweep: A large set of IP addresses are scanned in an attempt to detect a system that has one open port.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ **Hacking**

- The activities of hacking
  - *Port scanning*
    - The different scanning methods that network attackers use
      - Passive scan: All network traffic entering or leaving the network is captured and traffic is then analyzed to determine what the open ports are on the hosts within the network.
      - UDP scan: Empty UDP packets are sent to the different ports of a set of addresses to determine how the operating responds. Closed UDP ports respond with the Port Unreachable message when any empty UDP packets are received. Other operating systems respond with the ICMP error packet.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Port scanning*
    - The different scanning methods that network attackers use
      - FTP bounce: To hide the attacker’s location, the scan is initiated from an intermediary FTP server.
      - FIN scan: TCP FIN packets that specify that the sender wants to close a TCP session are sent to each port for a range of IP addresses.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Enumeration* (枚举)
    - The unauthorized intruder uses a number of methods to collect information on applications and hosts on the network and on the user accounts utilized on the network.
    - Enumeration is particularly successful in networks that contain unprotected network resources and services:
      - Network services that are running but are not being utilized.
      - Default user accounts that have no passwords specified.
      - Guest accounts that are active.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - ✧ *Acquiring access* (存取权限探测)
    - ○ Access attacks are performed when an attacker exploits a security weakness so that he/she can obtain access to a system or the network. Trojan horses and password hacking programs are typically used to obtain system access. When access is obtained, the intruder is able to modify or delete data and add, modify, or remove network resources.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Acquiring access*
    - The different types of access attacks are:
      - *Unauthorized system access* entails the practice of exploiting the vulnerabilities of operating systems or executing a script or a hacking program to obtain access to a system.
      - *Unauthorized privilege escalation* is a frequent type of attack. Privilege escalation occurs when an intruder attempts to obtain a high level of access, like administrative privileges, to gain control of the network system.
      - *Unauthorized data manipulation* involves interpreting, altering, and deleting confidential data.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - ✧ *Privilege escalation* (提权)
    - ◌ When an attacker initially gains access to the network, low level accounts are typically used. Privilege escalation occurs when an attacker escalates his/her privileges to obtain a higher level of access, like administrative privileges, in order to gain control of the network system.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Privilege escalation*
    - The *privilege escalation methods* that attackers use are:
      - The attacker searches the registry keys for password information.
      - The attacker can search documents for information on administrative privileges.
      - The attacker can execute a password cracking tool on targeted user accounts.
      - The attacker can use a Trojan in an attempt to obtain the credentials of a user account that has administrative privileges.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- The activities of hacking
  - *Install backdoors* (安插后门)
    - A hacker can also implement a mechanism such as some form of access granting code with the intent of using it at some future stage. Attackers typically install back doors so that they can easily access the system at some later date. After a system is compromised, users can remove any installed backdoors by reinstalling the system from a backup that is secure.
  - *Removing evidence of activities.*
    - Attackers typically attempt to remove all evidence of their activities.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacking

- 黑客程序 (hacking program) 是指一类通过远程网络非法进入计算机系统，进而控制、盗取、破坏信息或系统的软件程序。
  - ✧ 黑客程序经常和木马一起出现，但其目的主要在于控制目标设备。

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacker

- A *hacker* (骇客) is someone who maliciously attacks networks, systems, computers, and applications and captures, corrupts, modifies, steals, or deletes confidential company information.
- A hacker can refer to a number of different individuals who perform activities aimed at hacking systems and networks, and it can also refer to individuals who perform activities that have nothing to do with criminal activity:
  - Programmers who hack complex technical problems to come up with solutions.
  - Script kiddies (初学者) who use readily available tools on the Internet to hack into systems.
  - Criminal hackers who steal or destroy company data.
  - Protesting activists (抗议活动积极分子) who deny access to specific Web sites as part of their protesting strategy.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacker

- Hackers these days are classified according to the hat they wear. This concept is illustrated below:
  - ✧ *Black hat hackers* (黑客) are malicious or criminal hackers who hack at systems and computers to damage data or who attempt to prevent businesses from rendering their services. Some black hat hackers simply hack security protected systems to gain prestige in the hacking community.
  - ✧ *White hat hackers* (白帽子) are legitimate security experts trying to expose security vulnerabilities in operating system platforms. White hat hackers have the improvement of security as their motive. They do not damage or steal company data nor do they seek any fame. These security experts are usually quite knowledgeable about the hacking methods that black hat hackers use.
  - ✧ *Grey hat hacker* (灰客)

5.1 Introduction

5.1.2 Hacking & Hackers

❑ **Hacker**

- Motives that hackers attempt to attack networks
  - Possible motives for *structured external threats* include:
    - Greed 贪心
    - Industrial espionage 工业间谍
    - Politics 政治目的
    - Terrorism 恐怖行为
    - Racism 种族主义
    - Criminal payoffs 犯罪收益
  - Individuals seeking fame or some sort of recognition.
  - Displeased employees.
  - There are some network attackers that simply enjoy the challenge of trying to compromise highly secured networks' security systems. These types of attackers simply see their actions as a means of exposing existing security vulnerabilities.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacker

- Types of malicious activities that hackers perform are
  - ✧ Illegally using user accounts and privileges
  - ✧ Stealing hardware
  - ✧ Stealing software
  - ✧ Running code to damage systems
  - ✧ Running code to damage and corrupt data
  - ✧ Modifying stored data
  - ✧ Stealing data
  - ✧ Using data for financial gain or for industrial espionage
  - ✧ Performing actions that prevent legitimate authorized users from accessing network services and resources.
  - ✧ Performing actions to deplete network resources and bandwidth.

5.1 Introduction

5.1.2 Hacking & Hackers

❑ Hacker

- 黑客采用各种手段获得计算机系统口令，非法进入计算机系统，截取数据、窃取情报、篡改文件，甚至扰乱和破坏系统。
  - ✧ 黑客有时扮演网络侠客的角色，有时就是网络罪犯。黑客行为的发展对网络安全构成了巨大威胁。黑客中有的已不再是单纯出于经济目的或出于好奇或展示自己能力的高超，而是出于危害国家安全等动机。

5.1 Introduction

5.1.3 Network Threats

❑ Internal threats & External threats

- Network threats can be classified into the following types:
  - Internal threats
  - External threats
    - Unstructured threats
    - Structured threats
- Internal threats
  - Internal attacks originate from dissatisfied or unhappy inside employees or contractors. Internal attackers have some form of access to the system, even some administrative rights on the network, and usually try to hide their attack as a normal process. An Intrusion Detection System can be used to scan for both external and internal attacks. All forms of attacks should be logged and the logs should be reviewed and followed up.

5.1 Introduction

5.1.3 Network Threats

❑ Internal threats & External threats

- External threats
  - ✧ Individuals carry out external threats or network attacks without assistance from internal employees or contractors. A malicious and experienced individual, a group of experienced individuals, an experienced malicious organization, or inexperienced attackers (script kiddies) carry out these attacks. Such attackers usually have a predefined plan and the technologies (tools) or techniques to carry out the attack. One of the main characteristics of external threats is that they usually involve scanning and gathering information. Users can therefore detect an external attack by scrutinizing (详细检查) existing firewall logs. Users can also install an Intrusion Detection System to quickly identify external threats.

5.1 Introduction

5.1.3 Network Threats

❑ Internal threats & External threats

- External threats
  - ✧ *Structured External Threats.*
    - ○ These threats originate from a malicious individual, a group of malicious individual(s), or a malicious organization. Structured threats are usually initiated from network attackers that have a *premeditated thought* (预谋) on the actual damages and losses that they want to cause. Possible motives for structured external threats include greed, politics, terrorism, racism, and criminal payoffs. These attackers are highly skilled on network design, avoiding security measures, IDS, access procedures, and hacking tools. They have the necessary skills to develop new network attack techniques and the ability to modify existing hacking tools for their exploitations. In certain cases, an internal authorized individual may assist the attacker.

5.1 Introduction

5.1.3 Network Threats

❑ **Internal threats & External threats**

- External threats
  - ✧ *Unstructured External Threats.*
    - These threats originate from an inexperienced attacker, typically from a *script kiddie*. Script kiddie refers to an inexperienced attacker who uses cracking tools or scripted tools readily available on the Internet to perform a network attack. Script kiddies are usually inadequately skilled to create the threats on their own. They can be considered bored individuals seeking some form of fame by attempting to crash websites and other public targets on the Internet.

5.1 Introduction

5.1.3 Network Threats

❑ Internal threats & External threats

- External threats
  - *Remote External Attacks.*
    - These attacks are usually aimed at the services that an organization offers to the public.
    - Remote attacks aimed at the services available for internal users. This remote attack usually occurs when there is no firewall to protect these internal services.
    - Remote attacks aimed at locating modems to access the corporate network.
    - DoS attacks to place an exceptional processing load on servers in an attempt to prevent authorized user requests from being serviced.
    - War dialing (拨号探测) of the corporate private branch exchange (PBX, 专用分组交换机).
    - Attempts to brute force password authenticated systems.

5.1 Introduction

5.1.3 Network Threats

❑ **Internal threats & External threats**

- External threats
  - *Local External Attacks.*
    - These attacks typically originate from situations where computing facilities are shared and access to the system can be obtained.

5.1 Introduction

5.1.4 Steps of Network Attack

❑ Three Steps of Network Attack

- Preparation 准备阶段
  - ✧ Object Selecting & Information Collecting
- Implementation 实施阶段
  - ✧ Authority & Extension
- Post Events 善后工作
  - ✧ System log erasing, Trace hiding & Backdoor reserving

5.1 Introduction

5.1.4 Steps of Network Attack

❑ **Three Steps of Network Attack**

- 网络攻击的准备阶段
  - ✧ 确定攻击的目标
    - ◌ 攻击者在进行攻击之前首先要确定攻击要达到什么样的目的，造成什么样的后果。
  - ✧ 信息收集
    - ◌ 收集尽量多的关于攻击目标的信息是攻击前最主要的工作。主要包括目标的操作系统类型及版本，提供的服务，各服务器程序的类型与版本以及相关的社会信息。

5.1 Introduction

5.1.4 Steps of Network Attack

❑ Three Steps of Network Attack

- 网络攻击的实施阶段
  - ✧ 获得权限
    - ◌ 对于破坏性攻击, 只需利用工具发动攻击。而对于入侵性攻击，要利用收集到的信息，找到其系统漏洞，然后利用该漏洞获取一定的权限。能够被攻击者利用的漏洞主要包括系统软件的安全漏洞，也包括由于管理配置不当而造成的漏洞。
  - ✧ 扩大权限
    - ◌ 系统漏洞分为远程漏洞和本地漏洞两种。攻击者可以在其它机器上直接利用远程漏洞对本机进行攻击，并获取一定的权限。但是利用远程漏洞往往只是获取一个普通用户的权限，要想获取更大的权限就需要配合本地漏洞来把获得的权限扩大，最终获得系统管理员权限。

5.1 Introduction

5.1.4 Steps of Network Attack

❑ **Three Steps of Network Attack**

- 网络攻击的善后工作
  - ✧ 日志系统善后
    - ○ 所有的网络系统都提供日志功能，记录系统上发生的动作。为了隐蔽攻击身份或行为，攻击者可能会抹掉自己在日志系统中留下的痕迹。
  - ✧ 隐匿踪迹
    - ○ 攻击者在获得系统最高管理员权限之后可以修改系统上的文件，包括日志文件。例如通过对日志进行适当的修改来隐藏攻击者的踪迹 (而不是简单的删除日志文件)。
  - ✧ 安插后门
    - ○ 一般攻击者都会在攻入系统后再次进入该系统，为此攻击者会留下一个后门，如特洛伊木马程序。后门程序能与系统同时运行，而且能在系统重新启动时自动启动。

5.1 Introduction

5.1.5 Methods of Network Defence

❑ Methods of Network Defence

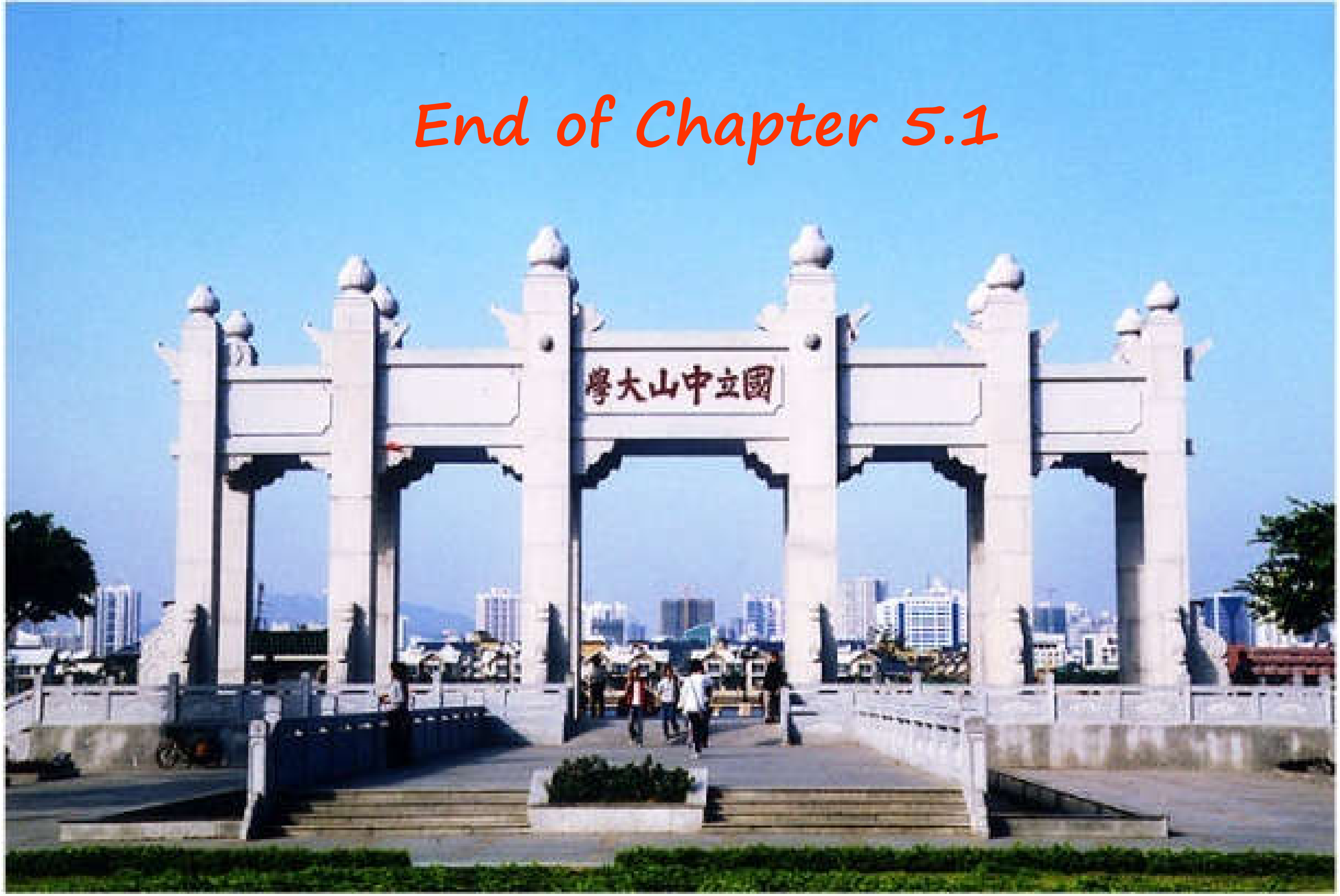
- ◆ Regular security defend **常规的安全防护策略**
- ◆ Prohibit remote procedure call 禁止远程调用
- ◆ Prohibit messenger service
- ◆ Correct administor management
- ◆ ……

5.1 Introduction

5.1.5 Methods of Network Defence

❑ **Regular security defend**

- 采用备份来避免损失
- 帮助用户自助
- 预防引导病毒
- 预防文件病毒
- 将访问控制加到个人终端
- 防止无意的信息披露
- 使用服务器安全功能
- 使用网络操作系统的安全功能
- 阻止局外人攻击
- 不要促成过早的硬件故障
- 为灾难准备硬件
- 学习数据恢复的基本知识
- 制定安全恢复策略



End of Chapter 5.1