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 Overview**
  - 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**
  - DNS Spoofing
  - Web Spoofing

5.2 Network Attacks

5.2.1 Computer Network Attack

- **What are Computer Network Attacks**
  - A *computer network attack*, or *cyberattack*, can be defined as any method, process, or means used to maliciously attempt to compromise network security. The individuals performing network attacks are commonly referred to as network attackers, hackers, or crackers.
  - A *cyberattack* is any type of offensive manoeuvre (攻击策略/操纵) employed by nation-states, individuals, groups, or organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labelled as either a cyber campaign, cyberwarfare or cyberterrorism in different context. Cyberattacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations. Cyberattacks have become increasingly sophisticated and dangerous as the Stuxnet worm demonstrated.

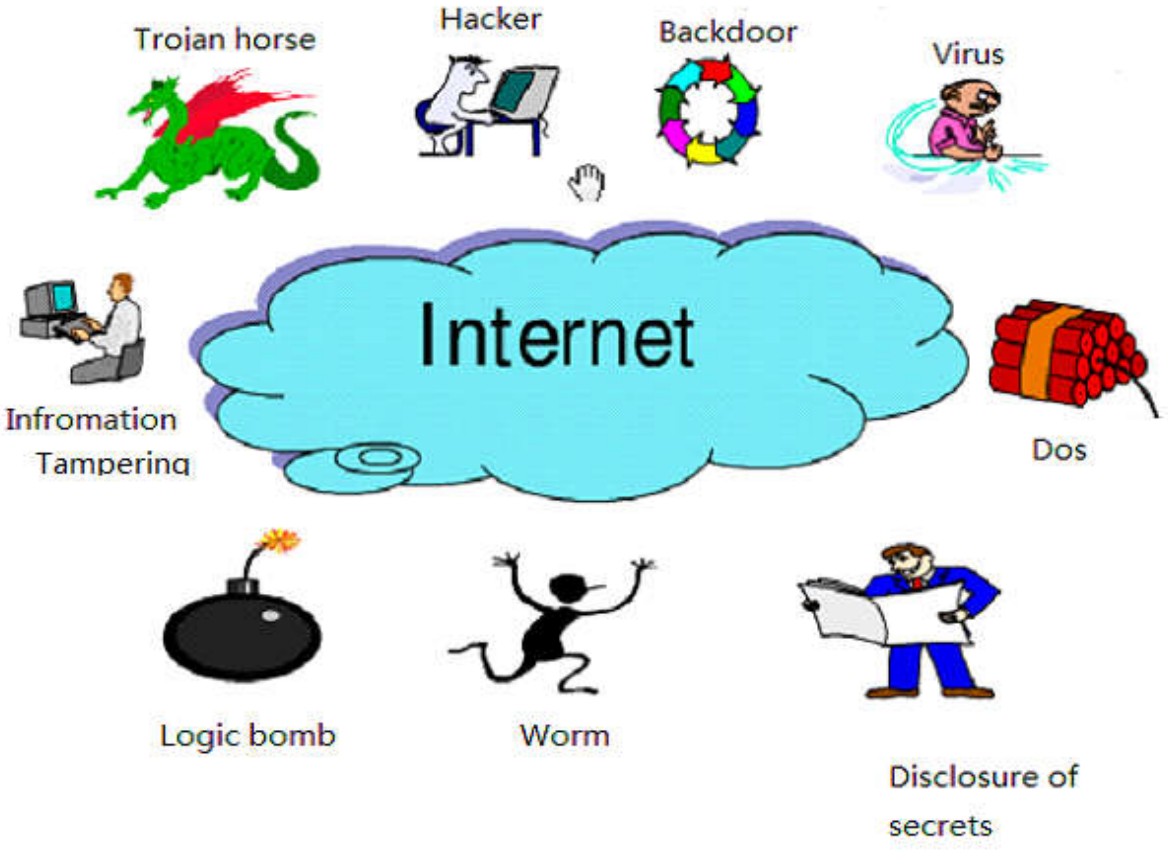
5.2 Network Attacks

5.2.1 Computer Network Attack

- **What are Computer Network Attacks**
  - Cyberattacks may include the following consequences:
    - ✧ Identity theft, fraud, extortion (身份盗取 欺骗 勒索)
    - ✧ Malware, pharming (嫁接), phishing, spamming (垃圾邮件), spoofing, spyware, Trojans and viruses
    - ✧ Stolen hardware, such as laptops or mobile devices
    - ✧ Denial-of-service and distributed denial-of-service attacks
    - ✧ Breach of access (违背存取控制)
    - ✧ Password sniffing
    - ✧ System infiltration (渗透)
    - ✧ Website defacement (网站损毁)
    - ✧ Private and public Web browser exploits
    - ✧ Instant messaging abuse (即时通信的滥用)
    - ✧ Intellectual property (IP 知识产权) theft or unauthorized access

5.2 Network Attacks

5.2.2 Common Types of Network Attack



5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Common Types of Network Attack**
  - Eavesdropping 窃听
  - Data Modification 数据篡改
  - Identity Spoofing (IP Address Spoofing) 身份欺骗
  - Password-Based Attacks 盗用口令攻击
  - Denial-of-Service Attack (DoS) 拒绝服务攻击
  - Man-in-the-Middle Attack (MITM) 中间人攻击
  - Brute Force Attack 暴力破解攻击
  - Compromised-Key Attack 盗取密钥攻击
  - Sniffer Attack 嗅探器攻击
  - Application-Layer Attack 应用层攻击

5.2.2 Common Types of Network Attack

- **Common Types of Network Attack**
  - 其他网络攻击分类
    - ✧ 破坏型和入侵型
      - ◌ 破坏型攻击：攻击目的不在于控制目标系统的运行，而是使其攻击目标不能正常工作，典型如拒绝服务攻击。
      - ◌ 入侵型攻击：攻击者设法获得一定的权限以控制攻击目标。入侵者一旦获取目标的管理员权限，就可以对目标恶意操纵，包括施行破坏型攻击。这种攻击比破坏型攻击更具普遍性，威胁性更大。入侵攻击一般是利用系统漏洞、密码泄露等实施。
    - ✧ 被动型和主动型
      - ◌ 被动攻击通常指信息受到非法侦听，而主动攻击成功则往往意味着数据甚至网络本身受到恶意的篡改和破坏。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Eavesdropping**
  - *Eavesdropping* occurs when an attacker monitors or listens to network traffic in transit then interprets all unprotected data. While users need specialized equipment and access to the telephone company switching facilities to eavesdrop on telephone conversations, all they need to eavesdrop on an IP based network is a sniffer technology to capture the traffic being transmitted. This is basically due to the TCP/IP being an open architecture that transmits unencrypted data over the network.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Eavesdropping**
  - A few methods of preventing intruders from eavesdropping on the network are:
    - ✧ Implement IPSec to secure and encrypt IP data before it is sent over the network.
    - ✧ Implement security policies and procedures to prevent attackers from attaching a sniffer on the network.
    - ✧ Install anti-virus software to protect the corporate network from Trojans. Trojans are typically used to discover and capture sensitive, valuable information such as user credentials.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Eavesdropping**
  - 窃听
  - 一般情况下，绝大多数网络通信都以一种不安全的 “明文” 形式进行，这就给攻击者很大的机会，只要获取数据通信路径，就可轻易 “侦听” 或者 “解读” 明文数据流。“侦听” 型攻击者虽然不破坏数据，却可能造成通信信息外泄，甚至危及敏感数据安全。对于多数普通企业来说，这类网络窃听行为已经构成了网管员所面临的最大的网络安全问题。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Data Modification**
  - *Data modification or data manipulation* pertains to a network attack where confidential company data is interpreted, deleted, or modified. Data modification is successful when data is modified without the sender actually being aware that it was tampered with.
  - A few methods of preventing attacks aimed at compromising data integrity are listed here:
    - ✧ Use digital signatures to ensure that data has not been modified while it is being transmitted or simply stored.
    - ✧ Implement access control lists (ACLs) to control which users are allowed to access your data.
    - ✧ Regularly back up important data.
    - ✧ Include specific code in applications that can validate data input.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Identity Spoofing**
  - *IP address spoofing/IP spoofing/identity spoofing* occurs when an attacker assumes the source IP address of IP packets to make it appear as though the packet originated from a valid IP address. The aim of an IP address spoofing attack is to identify computers on a network. Most IP networks utilize the user's IP address to verify identities and routers also typically ignore source IP addresses when routing packets. Routers use the destination IP addresses to forward packets to the intended destination network.
  - These factors could enable an attacker to bypass a router and to launch a number of subsequent attacks, including:
    - ✧ Initiation of a DoS attacks.
    - ✧ Initiation of MITM attacks to hijack sessions.
    - ✧ Redirect traffic.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Identity Spoofing**
  - A few methods of preventing IP address spoofing attacks are:
    - ✧ Encrypt traffic between routers and external hosts
    - ✧ Define ingress filters on routers and firewalls to stop inbound traffic where the source address is from a trusted host on the internal network

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Identity Spoofing**
  - 身份欺骗/IP 地址欺骗
  - 通常指 IP Address Spoofing，大多数网络操作系统使用 IP 地址来标识网络主机的身份。
  - 在一些情况下，貌似合法的 IP 地址很有可能是经过伪装的，这就是所谓 IP 地址欺骗，或身份欺骗。
  - 网络攻击者还可能通过修改某个从合法地址传来的信息内容，借此侵入目标网络。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Password-Based Attacks**
  - *Password attacks* are aimed at guessing the password for a system until the correct password is determined.
  - One of the primary security weaknesses associated with password based access control is that all security is based on the user ID and password being utilized. But who is the individual using the credentials at the keyboard?
  - Attackers can use dictionary attacks or brute force attacks to gain access to resources with the same rights as the authorized user. A big threat would be present if the user has some level of administrative rights to certain portions of the network.
  - An even bigger threat would exist if the same password credentials are used for all systems. The attacker would then have access to a number of systems.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Password-Based Attacks**
  - Password based attacks are performed in two ways:
    - ✧ *Online cracking:* The network attacker sniffs network traffic to seize authentication sessions in an attempt to capture password based information. There are tools that are geared at sniffing out passwords from traffic.
    - ✧ *Offline cracking:* The network attacker gains access to a system with the intent of gaining access to password information. The attacker then runs some password cracker technology to decipher valid user account information.
  - A *dictionary attack* occurs when all the words typically used for passwords are attempted to detect a password match. There are some technologies that can generate a number of complex word combinations and variations.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Password-Based Attacks**
  - Modern operating systems only store passwords in an encrypted format. To obtain password credentials, users have to have administrative credentials to access the system and information. Operating systems these days also support password policies. Password policies define how passwords are managed and define the characteristics of passwords that are considered acceptable.
  - Password policy settings can be used to specify and enforce a number of rules for passwords:
    - ✧ Define whether passwords are simple or complex
    - ✧ Define whether password history is maintained
    - ✧ Define the minimum length for passwords
    - ✧ Define the minimum password age
    - ✧ Define the maximum password age
    - ✧ Define whether passwords are stored with reversible encryption or irreversible encryption

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Password-Based Attacks**
  - Account lockout policies should be implemented if the environment is particularly vulnerable to threats arising from passwords that are being guessed. Implementing an account lockout policy ensures that the user's account is locked after an individual has unsuccessfully tried for several times to provide the correct password. The important factor to remember when defining an account lockout policy is that a policy that permits some degree of user error, but that also prevents hackers from using the user accounts should be implemented.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Password-Based Attacks**
  - The following password and account lockout settings are located in the Account Lockout Policy area in Account Policies:
    - ✧ Account lockout threshold: This setting controls the number of times after which an incorrect password attempt results in the account being locked out of the system.
    - ✧ Account lockout duration: This setting controls the duration that an account that is locked remains locked. A setting of 0 means that an administrator has to manually unlock the locked account.
    - ✧ Reset account lockout counter after: This setting determines the time duration that must pass subsequent to an invalid logon attempt occurring prior to the reset account lockout counter being reset.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Password-Based Attacks**
  - 盗用口令攻击
  - 基于口令的访问控制是一种最常见的安全措施。这意味着我们对某台主机或网络资源的访问权限决定于我们是谁，访问权限基于我们的用户名和帐号密码。
  - 攻击者通过多种途径尝试获得合法用户的帐号密码。取得帐号密码的攻击者拥有与该合法用户同等的网络访问权限。因此，如果具有网管权限用户的帐号密码被盗，攻击者甚至可以借此给自己创建一个合法帐号以备后用。获得合法权限的攻击者有可能盗取合法用户信息以及网络信息；修改服务器和网络配置，包括访问控制方式和路由表；篡改、重定向、删除数据等等。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - A *DoS attack* is aimed at preventing authorized, legitimate users from accessing services on the network. The DoS attack is not aimed at gathering or collecting data. It is aimed at preventing authorized, legitimate users from using computers or the network normally. The SYN flood from 1996 was the earliest form of a DoS attack that exploited a TCP vulnerability. A DoS attack can be initiated by sending invalid data to applications or network services until the server hangs or simply crashes. The most common form of a DoS attack is TCP attacks.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - DoS attacks can use either of the following methods to prevent authorized users from using the network services, computers, or applications:
    - ✧ Flood the network with invalid data until traffic from authorized network users cannot be processed.
    - ✧ Flood the network with invalid network service requests until the host providing that particular service cannot process requests from authorized network users. The network would eventually become overloaded.
    - ✧ Disrupt communication between hosts and clients through either of the following methods:
      - ◌ Modification of system configurations.
      - ◌ Physical network destruction. Crashing a router, for instance, would prevent users from accessing the system.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - There are a number of tools easily accessible and available on the Internet that can initiate DoS attacks:
    - ✧ Bonk
    - ✧ LAND
    - ✧ Smurf
    - ✧ Teardrop
    - ✧ WinNuke
  - A network attacker can increase the enormity of a DoS attack by initiating the attack against a single network from multiple computers or systems. This type of attack is known as a *Distributed Denial of Service (DDoS) attack.* Network administrators can experience great difficulty in fending off DDoS attacks, simply because blocking all the attacking computers can also result in blocking authorized users.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - The following measures can be implemented to protect a network against DoS attacks:
    - ✧ Implement and enforce strong password policies
    - ✧ Back up system configuration data regularly
    - ✧ Disable or remove all unnecessary network services
    - ✧ Implement disk quotas (磁盘配额) for user and service accounts.
    - ✧ Configure filtering on the routers and patch operating systems.
  - The following measures can be implemented to protect a network against DDoS attacks:
    - ✧ Limit the number of ICMP and SYN packets on router interfaces.
    - ✧ Filter private IP addresses using router access control lists.
    - ✧ Apply ingress and egress filtering on all edge routers. (在所有边界路由器上实施流入/流出过滤)

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - DoS 攻击的目的不在于窃取信息，而是要使某个设备或网络无法正常运行。这类攻击者惯用的攻击手法有：
    - ✧ 设法转移网管员注意力，使之无法立刻察觉被入侵，从而给攻击者自己争取时间
    - ✧ 向某个应用系统或网络服务系统发送非法指令，至使系统出现异常行为或异常终止
    - ✧ 向某台主机或整个网络发送大量数据洪流，导致网络因不堪过载而瘫痪
    - ✧ 拦截数据流，使授权用户无法取得网络资源

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - DoS 攻击的分类
    - ✧ DoS 攻击可以从很多个角度进行分类，例如攻击方式、攻击的协议等。
    - ✧ DoS 攻击方式主要有两种，分别是过载和摧毁。
      - ◌ 过载 (Flooding)：攻击者通过发送大量请求消耗服务器资源，使得服务器不能提供服务。
      - ◌ 摧毁 (Crashing)：攻击者通过一些手段让服务器崩溃，让其不能正常运行，例如通过恶意代码攻击导致服务器出错。
    - ✧ 各种协议都可以成为 DoS 攻击的对象。 例如：
      - ◌ TCP/IP Attack
      - ◌ UDP Flood
      - ◌ ICMP Flood

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - TCP/IP Attack
    - ✧ TCP/IP 攻击是攻击者向目标系统发送连续的 SYN 请求的一种 DoS 攻击形式。
    - ✧ TCP/IP 连接建立时需要进行3次握手
      1) 请求方发出 SYN (同步) 请求
      2) 应答方在收到上述 SYN 请求之后需要发回一个 SYN-ACK (同步-确认) 给请求方
      3) 请求方收到 SYN-ACK 之后，需要再发一个 ACK (确认)给应答方
    - ✧ 应答方在发送 SYN-ACK 之后需要等待请求方发回 ACK，如果在规定的等待时间内请求方还未发回 ACK，该连接就会因超时失效。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - TCP/IP Attack
    - ✧ 攻击流程：
      - ◌ 攻击者作为请求方每次都只发送 SYN，不发回 ACK，让应答方一直等待，直到超时。对于攻击者发的每一个 SYN，应答方都需要响应一个 SYN-ACK，这样极大地消耗了应答方的资源。
      - ◌ TCP/IP 攻击通常会配合 IP 欺骗。因为如果攻击者发送了大量的 SYN，攻击者将会接收到大量的 SYN-ACK，同样要花费大量的资源来处理这些信息。如果攻击者在发送给应答方的包中使用一个伪造的 IP 地址 (通常是不可达到的 IP 地址)，应答方发送的 SYN-ACK 不会到达攻击者，攻击者从而省下了处理 SYN-ACK 的资源，可以进行更有效的攻击。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - UDP Flood
    - UDP Flood is a DoS attack using the User Datagram Protocol (UDP), a stateless computer networking protocol.
      - A stateful protocol expects a response, like TCP/IP. A stateless protocol doesn't care. A stateless protocol is akin to a TV broadcast which doesn't care if you watch it, if you like it, if you talk to it, etc. The TV broadcast has no expectations!
    - The attacker sends a large number of UDP packets to random ports on a remote host. The distant host will:
      - Check for the application listening at that port;
      - See that no application listens at that port;
      - Reply with an ICMP Destination Unreachable packet.
    - The victimized system will be forced into sending many ICMP packets, eventually unreachable by other clients.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **DoS, Denial-of-Service Attack**
  - UDP Flood
    - ✧ UDP Flood 使用 UDP 协议进行 DoS 攻击。攻击者通常利用 IP 欺骗向目标主机的随机端口发送大量的 UDP 包。对每个 UDP 包，目标主机需要执行3个步骤：
      - ◌ 检查监听该端口的应用程序。攻击者可能会尽量选择目标主机服务器的应用程序不会使用的目的端口。
      - ◌ 发现并没有应用程序在使用这个端口。
      - ◌ 向源 IP 地址回复一个 ICMP 包。此地址实际上是不可用的。
    - ✧ 结果目标主机被迫大量发送 ICMP 包，阻塞了其他用户的使用。
  - 思考：
    - ✧ 适当描述 ICMP Flood 和 DDoS 攻击的技术细节，并搜寻实例加以说明。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **MITM, Man-in-the-Middle Attack**
  - *A man in the middle* (MITM) attack occurs when a hacker eavesdrops on a secure communication session and monitors, captures, and controls the data being sent between the two parties communicating. The attacker attempts to obtain information so that he/she can impersonate the receiver and sender communicating.
  - For an MITM attack to be successful, the following sequence of events has to occur:
    - ✧ The hacker must be able to obtain access to the communication session to capture traffic when the receiver and sender establish the secure communication session.
    - ✧ The hacker must be able to capture the messages being sent between the parties and then send messages so that the session remains active.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **MITM, Man-in-the-Middle Attack**
  - There are some public key cryptography systems such as the *Diffie-Hellman* (DH) key exchange that are rather susceptible to man in the middle attacks. This is due to the *Diffie-Hellman* (DH) key exchange using no authentication.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **MITM, Man-in-the-Middle Attack**
  - 中间人攻击
  - 中间人攻击发生在通信对象之间，通信过程以及通信数据遭到第三方的监视、截取和控制。如果通信中使用网络低层协议，通信两端的主机很难区分出不同的对象，因此不容易察觉到这类攻击。
    - ✧ 例如：攻击者可以对合法双方的数据交换进行重定向。
    - ✧ 中间人攻击在一定程度上类似于身份欺骗。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Brute Force Attack**
  - *Brute force attacks* simply attempt to decode a cipher by trying each possible key to find the correct one. This type of network attack systematically uses all possible alpha, numeric, and special character key combinations to find a password that is valid for a user account. Brute force attacks are also typically used to compromise networks that utilize Simple Mail Transfer Protocol (SNMP). Here, the network attacker initiates a brute force attack to find the SNMP community names so that he/she can outline the devices and services running on the network. (从而得到网络上的设备和服务的大致情况)
  - A few methods of preventing brute force attacks are listed here:
    - ✧ Enforce the use of long password strings.
    - ✧ For SNMP, use long, complex strings for community names.
    - ✧ Implement an intrusion detection system (IDS). By examining traffic patterns, an IDS is capable of detecting when brute force attacks are underway.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Compromised-Key Attack**
  - 盗取密钥攻击
  - 盗取密钥是困难的，但并非不可能。被攻击者盗取的密钥称为“已泄密的密钥”。攻击者可以利用已泄密的密钥对数据进行解密和修改，甚至可能利用该密钥计算其他密钥，以获取更多加密信息。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Sniffer Attack**
  - *Sniffer Attack* or *Sniffing* refers to the process that attackers use to capture and analyze network traffic. The packets' contents on a network are analyzed.
  - The tools that attackers use for sniffing are called sniffers or more correctly, protocol analyzers. While protocol analyzers are really network troubleshooting tools, hackers also use them for malicious purposes.
  - Sniffers monitor, capture, and obtain network information such as passwords and valuable customer information. When an individual has physical access to a network, he/she can easily attach a protocol analyzer to the network and then capture traffic.
  - Remote sniffing can also be performed.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Sniffer Attack**
  - There are sniffers available for most networking technologies including:
    - ✧ Asynchronous Transfer Mode (ATM)
    - ✧ Ethernet
    - ✧ Fiber Channel
    - ✧ Serial connections
    - ✧ Small Computer System Inter-face (SCSI)
    - ✧ Wireless

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Sniffer Attack**
  - There are a number of common sniffers that network security administrators and malicious hackers use:
    - ✧ Dsniff
    - ✧ Ethereal
    - ✧ Etherpeek
    - ✧ Network Associates's Sniffer
    - ✧ Ngrep
    - ✧ Sniffit
    - ✧ Snort
    - ✧ Tcpdump
    - ✧ Windump
  - To protect against sniffers, implement IPSec to encrypt network traffic so that any captured information cannot be interpreted.

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Sniffer Attack**
  - 嗅探器攻击
  - 嗅探器 (Sniffer) 指能解读、监视、拦截网络数据交换以及可以阅读数据包的程序或设备。 Sniffer 可以直接解读没有加密的数据包内容，对经过封装的隧道数据包，Sniffer 可以尝试解封装后再进行解读。利用 Sniffer，攻击者除了可以读取通信数据外，还可以对目标网络进行分析，进一步获取所需资源，甚至可以导致目标网络的崩溃或瘫痪。

5.2 Network Attacks

5.2.2 Common Types of Network Attack

- **Application-Layer Attack**
  - 应用层攻击
  - 应用层攻击直接将目标对准应用系统服务器。攻击者利用协议漏洞或故意在服务器操作系统或应用系统中留下后门，绕过正常的访问控制进行植入攻击。
  - 成功的攻击者可以控制整个用户应用系统，还可以：
    - ✧ 阅读、添加、删除、修改用户数据或操作系统
    - ✧ 在用户应用系统中引入病毒程序
    - ✧ 引入 Sniffer，对用户网络进行分析，以获取所需信息，并导致用户网络的崩溃或瘫痪
    - ✧ 引起用户应用系统的异常终止
  - 特洛依木马就是一种典型的应用层攻击程序。

5.2 Network Attacks

5.2.3 Port Scan

- **Port Scanner**
  - A *port scanner* is a software application designed to probe a server or host for open ports. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to compromise it.
- **Port Scan**
  - A *port scan* or *portscan* is "An attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service"

5.2 Network Attacks

5.2.3 Port Scan

- **NMap**
  - **NMap** (**N**etwork **Map**per, latest V7.60) is a security scanner originally written by Gordon Lyon used to discover hosts and services on a computer network, thus creating a "map" of the network.
  - Nmap sends specially crafted packets to the target host and then analyzes the responses. Unlike many simple port scanners that just send packets at some predefined constant rate, Nmap accounts for the network conditions during the run such as
    - ✧ latency fluctuations 响应变化规律
    - ✧ network congestion 网络拥堵情况
    - ✧ the target interference with the scan
  - Nmap has succeeded to extend its discovery capabilities beyond basic host being up/down or port being open/closed to being able to determine operating system of the target, names and versions of the listening services, estimate uptime, the type of device, presence of the firewall.

5.2 Network Attacks

5.2.3 Port Scan

- **SuperScan** (Foundstone/Mcafee/Intel Security Group)
  - **SuperScan** is a free connect-based port scanning software designed to detect open TCP and UDP ports on a target computer, determine which services are running on those ports, and run queries such as whois, ping, ICMP traceroute, and Hostname lookups. The latest version is Superscan 4.1.
  - Superscan is a tool used by both system administrators and crackers to evaluate a computer's security. System administrators can use it to test for possible unauthorized open ports on their computer networks, whereas crackers use it to scan for a potentially insecure port in order to gain illegal access to a system.

5.2 Network Attacks

5.2.3 Port Scan

- **NMap & SuperScan**
  - NMap 和 SuperScan 是常用的端口扫描工具。
  - NMap 是主流 OS 下的网络扫描和嗅探工具包，其基本功能包括：
    - ✧ 探测一组主机是否在线
    - ✧ 扫描主机端口，嗅探所提供的网络服务
    - ✧ 推断主机所用的操作系统

5.2 Network Attacks

5.2.3 Port Scan

- **NMap & SuperScan**
  - Results of an Nmap scan

```
[root@darkstar ~]#
[root@darkstar ~]# nmap -PN -sS  -O Scanme.Nmap.Org

Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency).
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed auth
8009/tcp  open   ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26

OS detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 16.99 seconds
[root@darkstar ~]#
```

5.2 Network Attacks

5.2.3 Port Scan

- **NMap & SuperScan**
  - SuperScan 是一种功能强大的端口扫描工具。
    - ✧ 通过 Ping 来检验 IP 是否在线；
    - ✧ IP 和域名相互转换；
    - ✧ 检验目标计算机提供的服务类别；
    - ✧ 检验一定范围目标计算机的是否在线和端口情况；
    - ✧ 工具自定义列表检验目标计算机是否在线和端口情况
    - ✧ 自定义要检验的端口，并可以保存为端口列表文件；
    - ✧ 软件自带一个木马端口列表 trojans.lst，通过这个列表可以检测目标计算机是否有木马；同时，也可以自己定义修改这个木马端口列表。 图为使用 SuperScan 进行端口扫描的演示。

5.2 Network Attacks

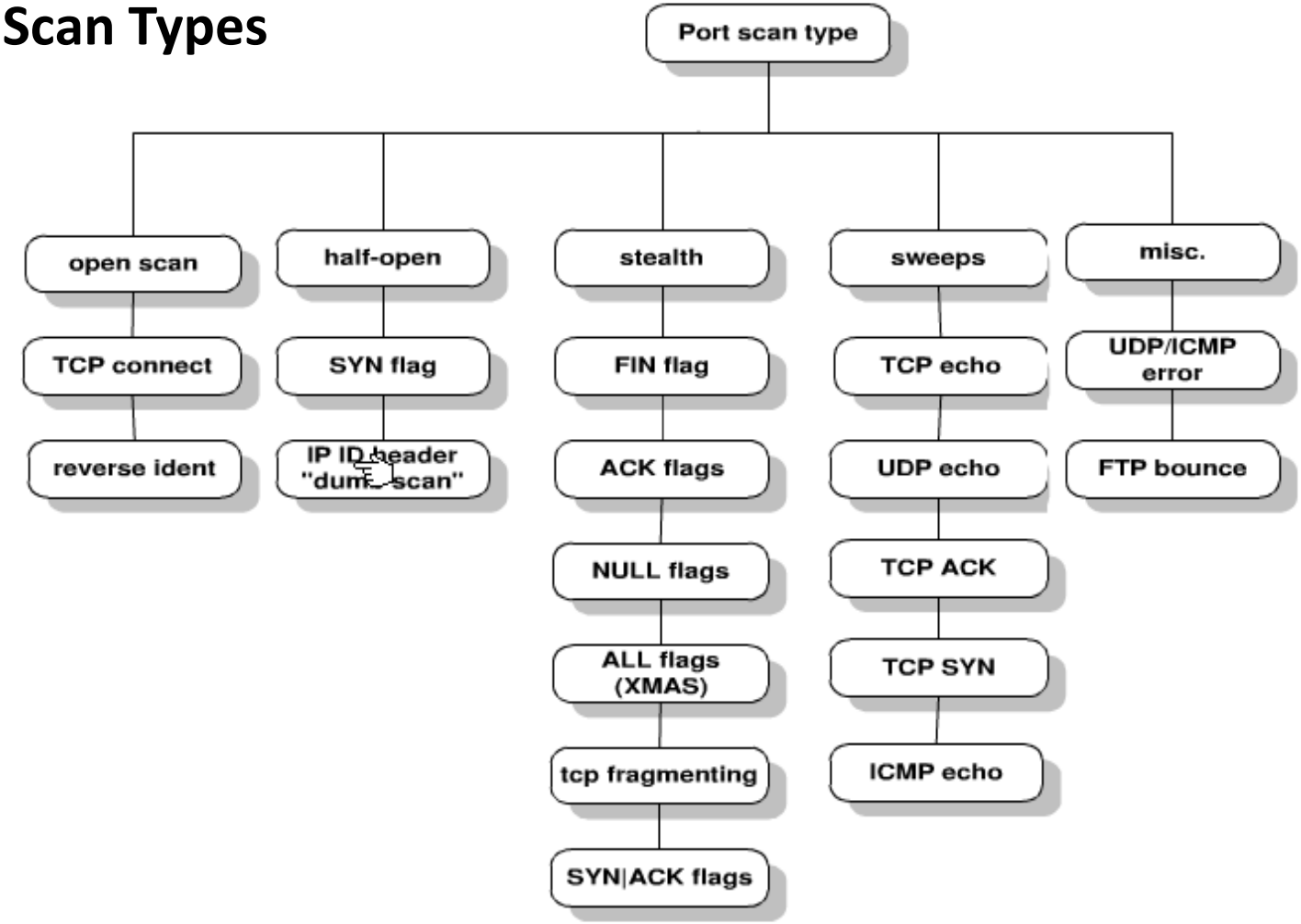
5.2.3 Port Scan

- **NMap & SuperScan**

5.2 Network Attacks

5.2.3 Port Scan

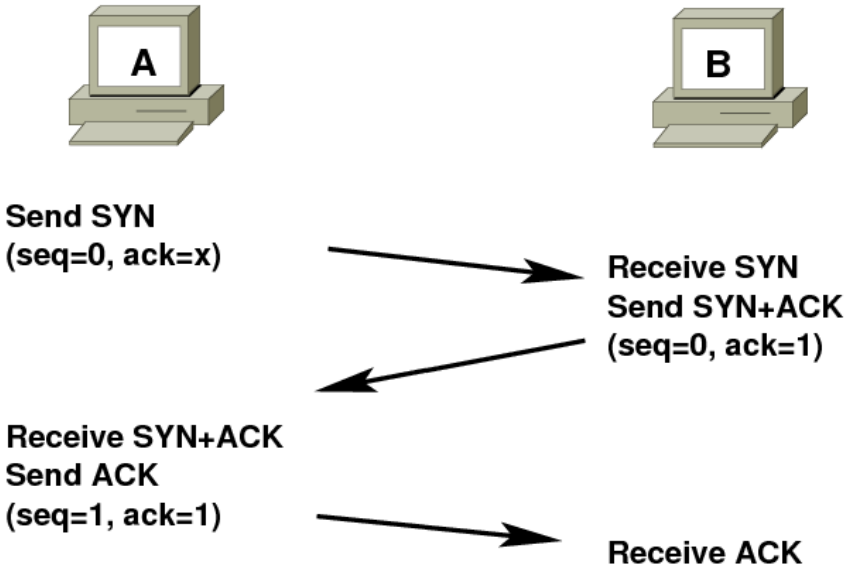
- **Port Scan Types**



5.2 Network Attacks

5.2.3 Port Scan

- **Review: The TCP three-way handshake**
  - The TCP three-way handshake in Transmission Control Protocol (also called the TCP-handshake; three message handshake and/or SYN-SYN-ACK) is the method used by TCP set up a TCP/IP connection over an Internet Protocol based network.



5.2 Network Attacks

5.2.3 Port Scan

- **TCP Scanning /Open Scanning**
  - TCP scanning is the next option to go to when SYN scanning is not a feasible option.
  - The simplest port scanners using the operating system's network functions
  - Nmap calls this mode “connect scan”, named after the Unix connect() system call.
  - If a port is open, the operating system completes the TCP three-way handshake, and the port scanner immediately closes the connection to avoid performing a kind of Denial-of-Service attack. Otherwise an error code is returned.

5.2 Network Attacks

5.2.3 Port Scan

- **TCP Scanning /Open Scanning**
  - This scan mode has the advantage that the user does not require special privileges. However, this scan type is less common because making use of OS network functions can prevent low-level controls.
  - This method is "noisy", particularly if it is a "*portsweep*": the services can log the sender IP address and Intrusion Detection Systems can raise an alarm.
  - 完整的 TCP 全开放扫描，缺点是容易被对方的防火墙、入侵检测设备拦截，而得不到真实的端口开放情况

5.2 Network Attacks

5.2.3 Port Scan

- **SYN Scanning**
  - Rather than use the operating system's network functions, the port scanner generates raw IP packets itself, and monitors for responses.
  - This scan type is also known as “half-open scanning (半开扫描)", because it never actually opens a full TCP connection. The port scanner generates a SYN packet. If the target port is open, it will respond with a SYN-ACK packet. The scanner host responds with a RST packet, closing the connection before the handshake is completed.
  - The use of raw networking has several advantages, giving the scanner full control of the packets sent and the timeout for responses, and allowing detailed reporting of the responses.

5.2 Network Attacks

5.2.3 Port Scan

- **SYN Scanning**
  - There is debate over which scan is less intrusive on the target host. SYN scan has the advantage that the individual services never actually receive a connection while some services can be crashed with a connect scan.
    - ✧ 究竟哪种扫描方式对目标计算机的入侵程度更低有所争论。SYN扫描的好处是目标计算机不会建立一个真正的连接，因为有的机器在连接扫描下会崩溃。
    - ✧ The RST during the handshake can cause problems for some network stacks, in particular simple devices like printers.

5.2 Network Attacks

5.2.3 Port Scan

- **UDP Scanning**
  - UDP scanning is also possible, although there are technical challenges. UDP is a connectionless protocol so there is no equivalent to a TCP SYN packet. However, if a UDP packet is sent to a port that is not open, the system will respond with an ICMP port unreachable message (Type=3, Code=3). Most UDP port scanners use this scanning method, and use the absence of an ICMP response to infer that a port is open.
  - However, if a port is blocked by a firewall, this method will falsely report that the port is open. If the port unreachable message is blocked, all ports will appear open. This method is also affected by ICMP rate limiting (ICMP 带宽限制).
  - An alternative approach is to send application-specific UDP packets, hoping to generate an application layer response. For example, sending a DNS query to port 53 will result in a response, if a DNS server is present. This method is much more reliable at identifying open ports.

5.2 Network Attacks

5.2.3 Port Scan

- **UDP Scanning**
  - Note: ICMP 报文 (RFC 792-1981 to RFC 6918-2015)
    - ✧ IP 头部的 Protocol 值为1时，说明封装数据是一个 ICMP 报文。
    - ✧ 一个 ICMP 报文包括 ICMP 头部 (12字节) 和 ICMP 报文内容
    - ✧ ICMP header

```
// ICMP header, 12bytes
typedef struct _tagX_icmphdr
{
   unsigned char i_type;          //类型 0, 3, 4, 5, 8-18.
   unsigned char i_code;          //代码
   unsigned short i_cksum;        //检验和
   unsigned short i_id;           //标识符 或其它
   unsigned short i_seq;          //序列号 或其它
   unsigned long i_timestamp;     //时间戳 或其它
                                  //时间戳 = (unsigned long)::GetTickCount();
};
```

5.2 Network Attacks

5.2.3 Port Scan

- **UDP Scanning**
  - It is limited to scanning ports for which an application specific probe packet is available. Some tools (e.g., NMap) generally have probes for less than 20 UDP services, while some commercial tools (e.g., nessus) have as many as 70. In some cases, a service may be listening on the port, but configured not to respond to the particular probe packet.
  - To cope with the different limitations of each approach, some scanners offer a hybrid method. For example, using NMap with the -sUV option will start by using the ICMP port unreachable method, marking all ports as either "closed" or "open|filtered". The open|filtered ports are then probed for application responses and marked as "open" if one is received.

5.2 Network Attacks

5.2.3 Port Scan

- **ACK Scanning**
  - ACK scanning is one of the more unique scan types, as it does not exactly determine whether the port is open or closed, but whether the port is filtered or unfiltered. This is especially good when attempting to probe for the existence of a firewall and its rule sets.
  - Simple packet filtering will allow established connections (packets with the ACK bit set), whereas a more sophisticated stateful firewall might not.
    - ✧ 可以用于确定防火墙的规则集，或者使单个包穿过简单的包过滤防火墙。策略完善的防火墙将拒绝那些与防火墙状态表中的会话不相符合的 ACK 响应包；而简单的包过滤防火墙将允许 ACK 连接请求。

5.2 Network Attacks

5.2.3 Port Scan

- **FIN Scanning**
  - Since SYN scans are not surreptitious enough, firewalls are, in general, scanning for and blocking packets in the form of SYN packets. FIN packets are able to pass by firewalls with no modification to its purpose. Closed ports reply to a FIN packet with the appropriate RST packet, whereas open ports ignore the packet on hand. This is typical behavior due to the nature of TCP, and is in some ways an inescapable downfall.
    - ✧ 向目标主机端口发出单个的 FIN 包，如果端口关闭，目标系统将返回 RST 包。

5.2 Network Attacks

5.2.4 Idle Scanning

- **What is Idle Scanning**
  - The idle scan (空闲扫描) is a TCP port scan method that consists of sending spoofed packets to a computer to find out what services are available. This is accomplished by impersonating another computer called a "***zombie***" (that is not transmitting or receiving information) and observing the behavior of the *zombie* system.
  - The action can be done through common software network utilities such as NMap and hping. The attack involves sending forged packets to a specific machine ***target*** in an effort to find distinct characteristics of another ***zombie*** machine. The attack is sophisticated because there is no interaction between the attacker computer and the ***target***: the attacker interacts only with the "***zombie***" computer.

5.2 Network Attacks

5.2.4 Idle Scanning

- **What is Idle Scanning**
  - In 1998, security researcher Antirez (*Salvatore Sanfilippo*, who also wrote the hping2 too) posted to the Bugtraq mailing list an ingenious new port scanning technique. Idle scan, as it has become known, allows for completely blind port scanning. Attackers can actually scan a target without sending a single packet to the target from their own IP address! Instead, a clever side-channel attack allows for the scan to be bounced off a dumb “zombie host”. Intrusion detection system (IDS) reports will finger the innocent zombie as the attacker. Besides being extraordinarily stealthy (隐秘), this scan type permits discovery of IP-based trust relationships between machines.

5.2 Network Attacks

5.2.4 Idle Scanning

- **How Idle Scanning Works**
  - Idle Scan can be put together from these basic facts:
    - ✧ One way to determine whether a TCP port is open is to send a SYN (session establishment) packet to the port. The target machine will respond with a SYN/ACK (session request acknowledgment) packet if the port is open, and RST (reset) if the port is closed. This is the basis of the previously discussed SYN scan.
    - ✧ A machine that receives an unsolicited SYN/ACK packet (the packet not expected) will respond with a RST. An unsolicited RST will be ignored.
    - ✧ Every IP packet on the Internet has a fragment identification number (IP-ID). Since many operating systems simply increases this number for each packet they send, probing for the IP-ID can tell an attacker how many packets have been sent since the last probe.

5.2 Network Attacks

5.2.4 Idle Scanning

- **How Idle Scanning Works**
  - By combining these traits, it is possible to scan a target network while forging your identity so that it looks like an innocent ***zombie*** machine did the scanning.

5.2 Network Attacks

5.2.4 Idle Scanning

- **How Idle Scanning Works**
  - 攻击者利用空闲扫描探查攻击目标的某个端口是否开放
    - ✧ 攻击者寻找一台僵尸主机。首先探查僵尸主机的 IP-ID，可以通过向该主机发数据包，观察其 IP-ID 的变化情况，如果呈现线性增长，则该主机适合用来作为僵尸主机；
    - ✧ 攻击者用僵尸主机的 IP 地址伪造一个 SYN 数据包发送给目标主机，目标主机在接收到该数据包后，会根据对应端口是否开放采取不同的措施。如果端口是开放的，则会发送一个 SYN/ACK 数据包给僵尸主机，但僵尸主机实际上并未与目标主机建立应答，因此会直接向目标主机回复一个 RST 包，并将自身的 IP-ID 增1；相反，端口关闭的目标主机会发送一个不可达的 ICMP 包，僵尸主机没有响应步骤，其 IP-ID 也不会增加；
    - ✧ 攻击者再次探查僵尸主机的 IP-ID，根据其增长情况推断目标主机端口的是开放的还是关闭的。

5.2 Network Attacks

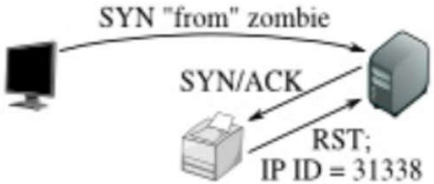
5.2.4 Idle Scanning

- **Idle Scan of an open port**

Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID.

Step 2: Forge a SYN packet from the zombie.



The target sends a SYN/ACK in response to the SYN that appears to come from the zombie. The zombie, not expecting it, sends back a RST, incrementing its IP ID in the process.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by 2 since step 1, so the port is open!

 the attacker

 the zombie

 the target

5.2 Network Attacks

5.2.4 Idle Scanning

- **Idle Scan of a closed port**

Step 1: Probe the zombie's IP ID.

The attacker sends a SYN/ACK to the zombie. The zombie, not expecting the SYN/ACK, sends back a RST, disclosing its IP ID. This step is always the same.

Step 2: Forge a SYN packet from the zombie.

The target sends a RST (the port is closed) in response to the SYN that appears to come from the zombie. The zombie ignores the unsolicited RST, leaving its IP ID unchanged.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open.

 the attacker

 the zombie

 the target

5.2 Network Attacks

5.2.4 Idle Scanning

- **Idle Scan of a filtered port**

Step 1: Probe the zombie's IP ID.

Just as in the other two cases, the attacker sends a SYN/ACK to the zombie. The zombie discloses its IP ID.

Step 2: Forge a SYN packet from the zombie.

The target, obstinately filtering its port, ignores the SYN that appears to come from the zombie. The zombie, unaware that anything has happened, does not increment its IP ID.

Step 3: Probe the zombie's IP ID again.

The zombie's IP ID has increased by only 1 since step 1, so the port is not open. From the attacker's point of view this filtered port is indistinguishable from a closed port.

 the attacker

 the zombie

 the target

End of Chapter 5.2