CSET 105

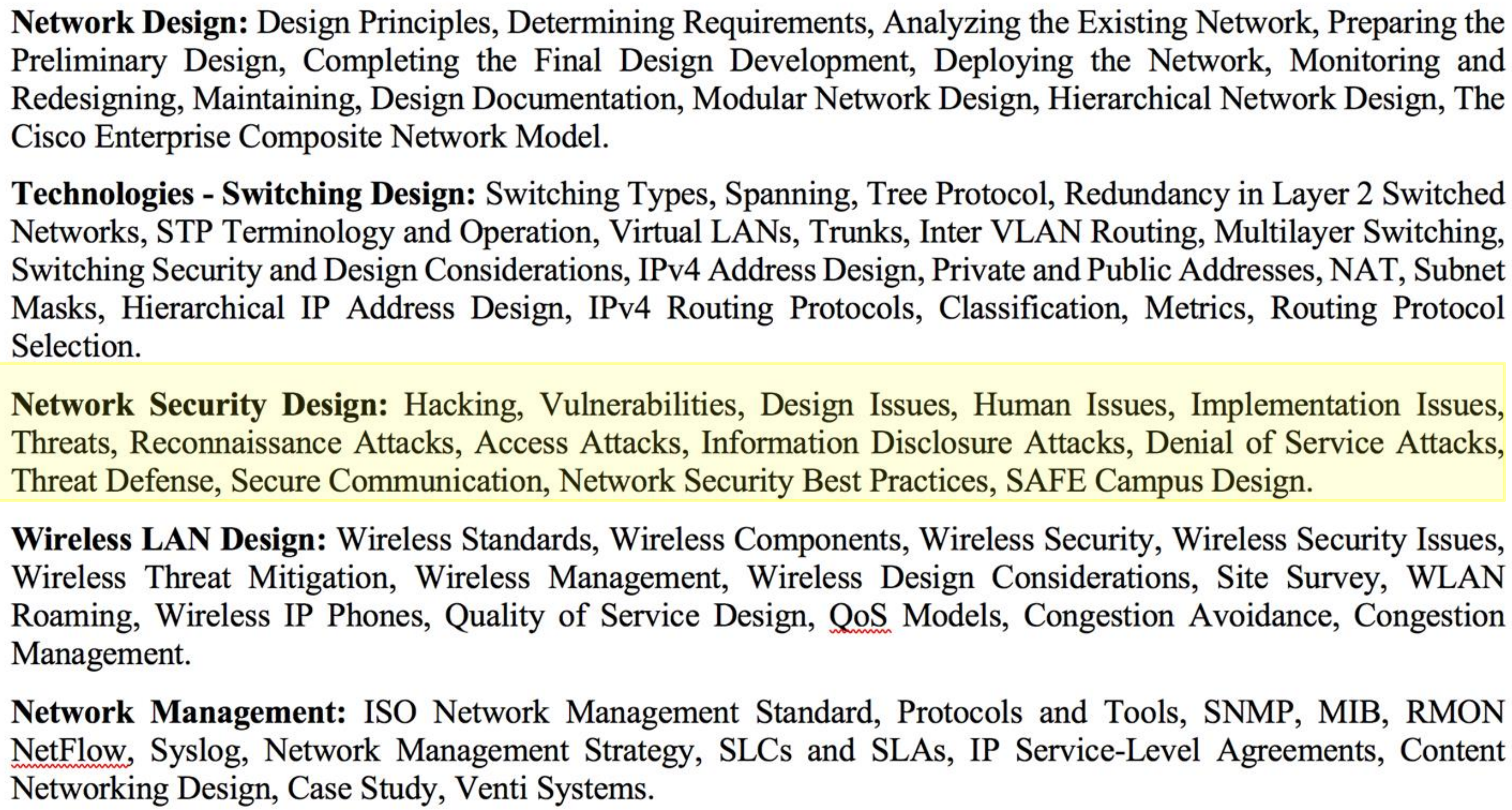
Network Design and Management

Evening Masters Edition

Dr. Mahboob Qaosar

Associate Professor, CSE, RU

COURSE CONTENTS



Network Design: Design Principles, Determining Requirements, Analyzing the Existing Network, Preparing the Preliminary Design, Completing the Final Design Development, Deploying the Network, Monitoring and Redesigning, Maintaining, Design Documentation, Modular Network Design, Hierarchical Network Design, The Cisco Enterprise Composite Network Model.

Technologies - Switching Design: Switching Types, Spanning, Tree Protocol, Redundancy in Layer 2 Switched Networks, STP Terminology and Operation, Virtual LANs, Trunks, Inter VLAN Routing, Multilayer Switching, Switching Security and Design Considerations, IPv4 Address Design, Private and Public Addresses, NAT, Subnet Masks, Hierarchical IP Address Design, IPv4 Routing Protocols, Classification, Metrics, Routing Protocol Selection.

Network Security Design: Hacking, Vulnerabilities, Design Issues, Human Issues, Implementation Issues, Threats, Reconnaissance Attacks, Access Attacks, Information Disclosure Attacks, Denial of Service Attacks, Threat Defense, Secure Communication, Network Security Best Practices, SAFE Campus Design.

Wireless LAN Design: Wireless Standards, Wireless Components, Wireless Security, Wireless Security Issues, Wireless Threat Mitigation, Wireless Management, Wireless Design Considerations, Site Survey, WLAN Roaming, Wireless IP Phones, Quality of Service Design, QoS Models, Congestion Avoidance, Congestion Management.

Network Management: ISO Network Management Standard, Protocols and Tools, SNMP, MIB, RMON NetFlow, Syslog, Network Management Strategy, SLCs and SLAs, IP Service-Level Agreements, Content Networking Design, Case Study, Venti Systems.

NETWORK SECURITY

- **Hacking**
  - Most of us equate hacking with malicious (nasty or cruel) activities
  - Reality: hacking is defined as **working diligently (carefully) on a computer system until it performs optimally**.
  - Right now hacking is more related to cracking,
  - Cracking ⇨ which is defined as the act of unlawfully accessing a network infrastructure to perform unethical activities.
  - hacking denotes malicious activities directed at networks and systems.

TYPES OF HACKER

- There are as many motivating factors for hacking as there are hacker types.
- From the **script-kiddy** who downloads hacking shareware and follows on-screen instructions to the cyber-terrorist, one thing is certain: **They want to inflict pain on your organization.**
- Also, although they are not necessarily qualifying as hackers, careless employees can also be dangerous to your organization.

TYPES OF HACKER

- Types of Hacker
  1. White Hat Hacker
  2. Black Hat Hacker
  3. Grey Hat Hacker
  4. Elite Hacker
  5. Script Kiddiy

TYPES OF HACKER

- **White-Hat Hackers**
  - Not all hackers spell trouble.
  - White-hat hackers are either reformed hackers or network professionals who have achieved mastery of the art and science of hacking.
  - White-hat hackers are paid to provide penetration testing of the corporate network and to produce a detailed report of their findings.

Types of Hacker

- **Black-Hat Hackers - Alternative**

- **White-Box and Black-Box Hacking**
  - White-box hackers are provided with some design and knowledge of an organization's network infrastructure prior to attempting their hacks of the system.
  - Black-box hackers have no prior knowledge of the network before attempting to hack it.

VULNERABILITIES

- Vulnerabilities ⇨ Vulnerability ⇨ weakness
- Regardless of whether the hacking motivation is benevolence, carelessness, or maliciousness, hackers wouldn't exist if **vulnerabilities** weren't available to exploit.

- Vulnerabilities usually fall into one of the following categories:
  1. Design issues
  2. Human issues
  3. Implementation issues

VULNERABILITIES

- **Design Issues**
  - Design issues refer to inherent problems with functionality because of operating system, application, or protocol flaws.
- **Human Issues**
  - The human issues category of vulnerabilities refers to administrator and user errors, such as unsecured user accounts, unsecured devices, or open devices (devices that have not been hardened).
- **Implementation Issues**
  - Implementation issues deal with creation, configuration, and enforcement of security policies, such as password policies, remote-access policies, Internet usage policies, e-mail policies, and so on.

THREATS

- Threat ⇨ risk
- The following is a generic list of attack categories:
  1. Reconnaissance attacks
  2. Access attacks
  3. Information disclosure attacks
  4. Denial of Service Attacks

RECONNAISSANCE ATTACKS

- Reconnaissance – investigation
- Reconnaissance attacks consist of intelligence gathering, often using tools like network scanners or packet analyzers.
  - The information collected can then be used to compromise networks.
- Such as:
  - **Ping sweeping**
    - To discover network addresses of live hosts

Reconnaissance Attacks

- **Network and port scanning**
  - To discover active ports on target hosts
- **Stack fingerprinting**
  - To determine the target operating system (OS) and the applications running on targeted hosts
- **Enumeration** (meaning list)
  - To infer network topology

THREATS

- Threat ⇨ risk
- The following is a generic list of attack categories:
  1. Reconnaissance attacks
  2. **Access attacks**
  3. Information disclosure attacks
  4. Denial of Service Attacks

ACCESS ATTACKS

- During an access attack, the hacker exploits the vulnerabilities he has discovered during the reconnaissance attack.
- Some common access attacks are as follows:
  - **Entry** ⇨Unlawful entry to an e-mail account or database.

ACCESS ATTACKS

- **Collect** ⇨The hacker gathers information or passwords.
- **Plant** ⇨ The hacker might create a back door so that he can return at a later time.
- **Occupy** ⇨ The hacker might elect to control as many hosts as he wants.
- **Cover** ⇨ The hacker might cover his tracks by attempting to change the system logs.

ACCESS ATTACKS

- **Access Subterfuges** (trick)
  - Hackers continuously come up with crafty (cleverly) access attacks.
  - The originator could be a spammer who plans to use this information for future spamming.
  - Proper dissemination and enforcement of an e-mail security policy would have taught the user not to open an attachment from an unknown source
  - **Alternatively**, the organization might have considered installing an e-mail filtering service to purge the message of **executable attachments**.

THREATS

- Threat ⇨ risk
- The following is a generic list of attack categories:
  1. Reconnaissance attacks
  2. Access attacks
  3. **Information disclosure attacks**
  4. Denial of Service Attacks

Information Disclosure Attacks

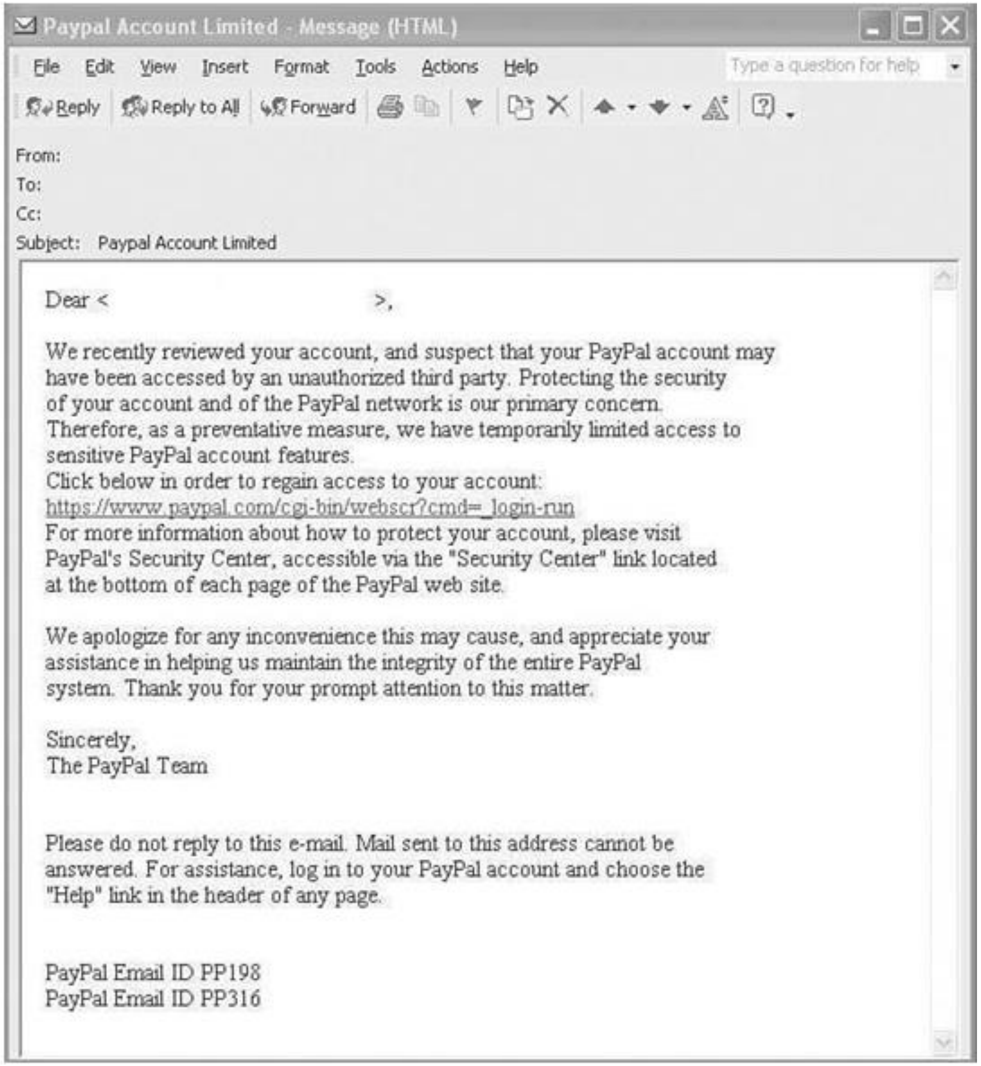
- Information disclosure attacks are different from an access attack in the sense that the information is provided voluntarily through a sophisticated subterfuge.
- The following attacks, though considered information disclosure attacks, could fall into the category of white-collar crimes:
  - Social engineering
  - Phishing

INFORMATION DISCLOSURE ATTACKS

- **Social Engineering**
  - Social engineering, a form of low-tech hacking, is defined as someone, claiming to be someone he is not, who approaches a user either through e-mail or through a phone call for the purpose of infiltrating the organization. Great technical ability is not necessary to perform social engineering.
- **Phishing**
  - Internet scammers who **cast about for people's financial information** have a new way to lure unsuspecting victims: they go phishing.
  - Phishing is a high-tech scam that uses spam or pop-up messages to deceive readers into disclosing credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information.

EXAMPLE

- Figure 4-1 is an example of an e-mail that looked legitimate but was actually a scam
- Unfortunately, no security systems can protect against information disclosure. Only the dissemination and enforcement of sound security policies can help users learn to be suspicious and to confirm the origin of these e-mails prior to taking actions.



Paypal Account Limited - Message (HTML)

From:
To:
Cc:
Subject: Paypal Account Limited

Dear < >,

We recently reviewed your account, and suspect that your PayPal account may have been accessed by an unauthorized third party. Protecting the security of your account and of the PayPal network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive PayPal account features.
Click below in order to regain access to your account:
https://www.paypal.com/cgi-bin/webscr?cmd=_login-run
For more information about how to protect your account, please visit PayPal's Security Center, accessible via the "Security Center" link located at the bottom of each page of the PayPal web site.

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the integrity of the entire PayPal system. Thank you for your prompt attention to this matter.

Sincerely,
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the header of any page.

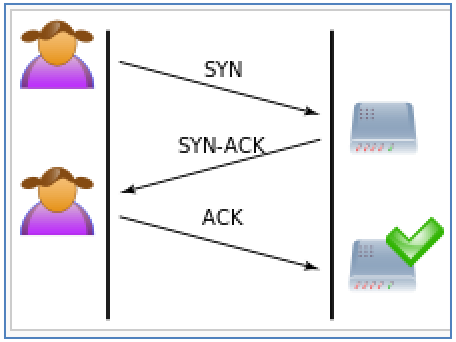
PayPal Email ID PP198
PayPal Email ID PP316

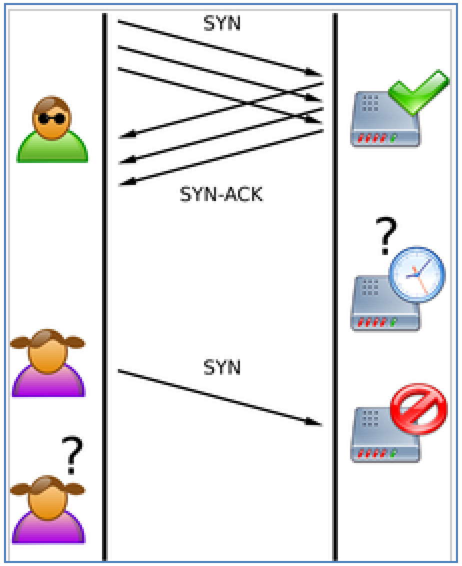
Denial of Service Attacks

- With a DoS attack, a hacker **attempts to render** a network or an Internet resource, such as a web server, worthless to users.
- A DoS attack typically achieves its goal by **sending large amounts of repeated requests** that paralyze the network or a server.
- A common form of a DoS attack is a **SYN flood**, where the server is overwhelmed by embryonic connections.

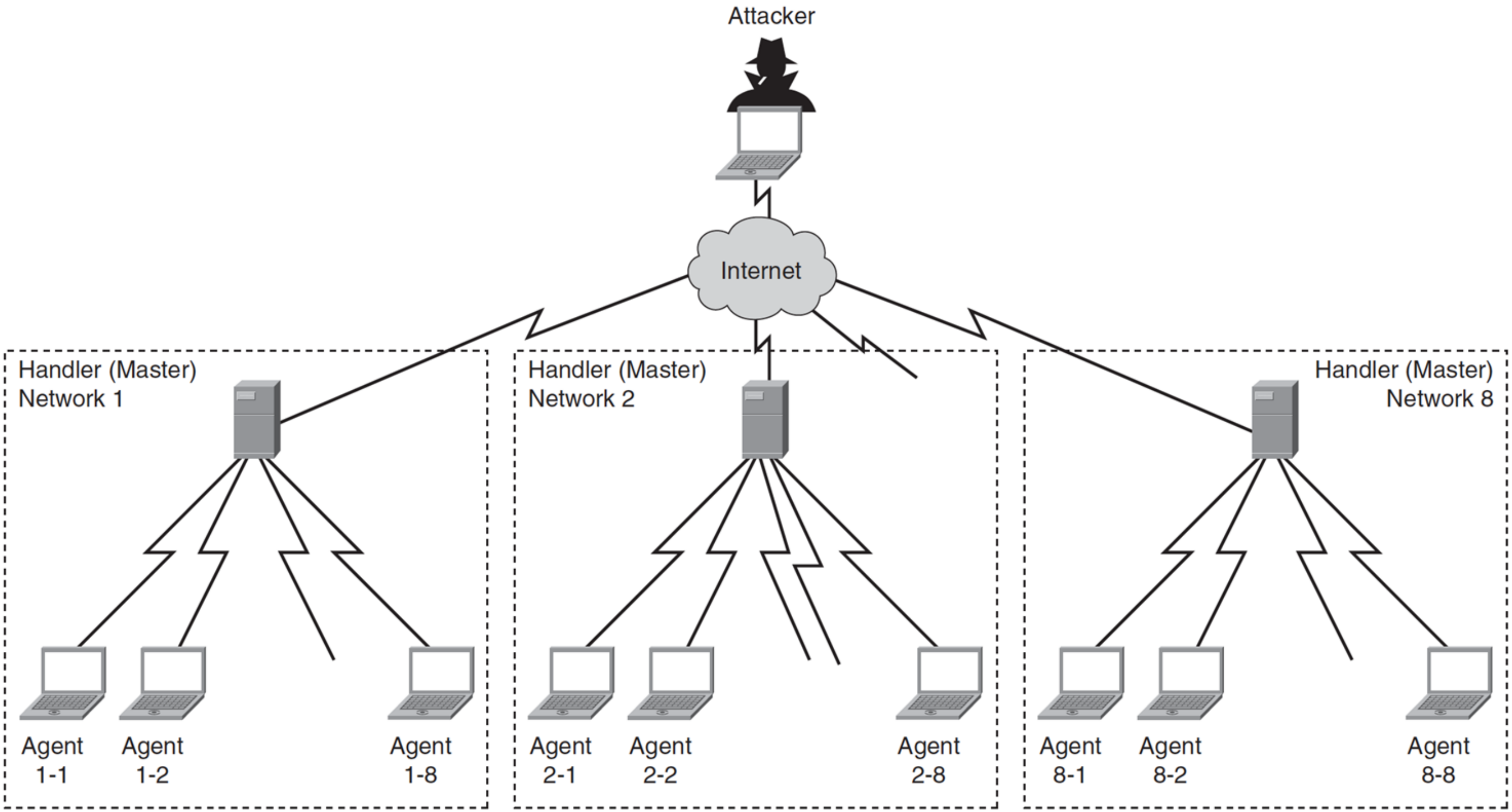
Denial of Service Attacks

- A hacker sends to a server countless Transmission Control Protocol (TCP) synchronization attempts known as SYN requests.
- The server answers each of those requests with a SYN ACK reply and allocates some of its computing resources to servicing this connection when it becomes a "full connection."
- Connections are said to be embryonic **or half-opened** until the originator completes the three-way handshake with an ACK for each request originated.
- A server that is inundated with half-opened connections soon runs out of resources to allocate to upcoming connection requests, thus the expression **"denial of service attack**





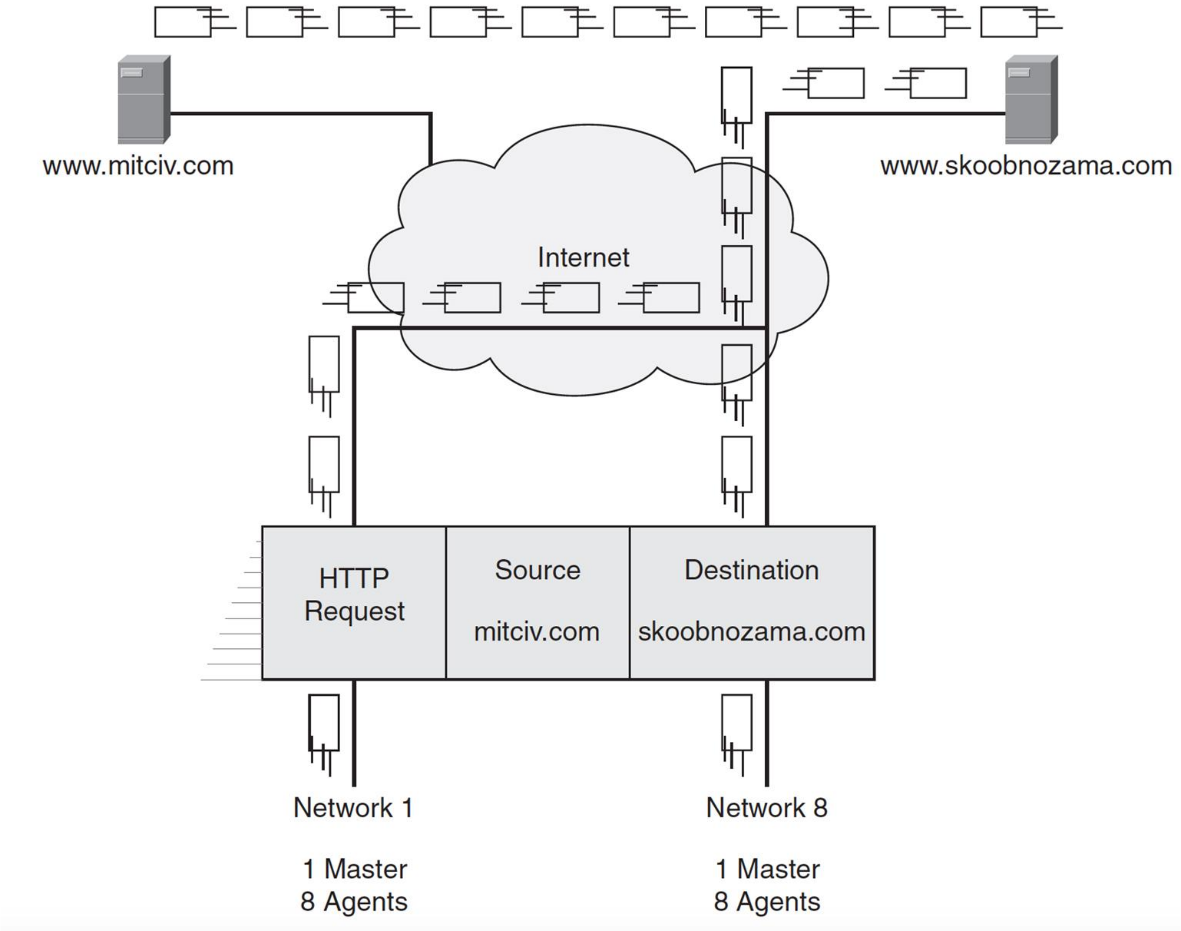
DISTRIBUTED DOS ATTACK



DDoS agents. ⇨ referred to as bots, thus the expression of botnets.

DISTRIBUTED DOS ATTACK

The crafty hacker might have requested that the agents use a spoofed source IP address when sending the large quantities of packets to the destination



MITIGATING TECHNOLOGIES

- Known threats can usually be mitigated by security equipment and sound security policies.
- The most pervasive mitigation techniques, which are grouped in these four major categories:
  - Threat defense
  - Secure communication
  - Trust and identity
  - Network security best practices