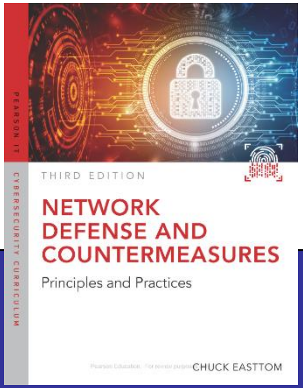
# *Types of Network Attacks*

Based on slides accompanying the book

*Network Defense and Countermeasures*

by Chuck Easttom (2018)



# Objectives

- Describe the most common network attacks
- Explain how these attacks are executed
- Identify basic defenses against those attacks

A. Denial of service attacks
B. Buffer overflow attacks
C. IP Spoofing attacks
D. Session Hijacking attacks
E. Viruses
F. Trojan horse attacks

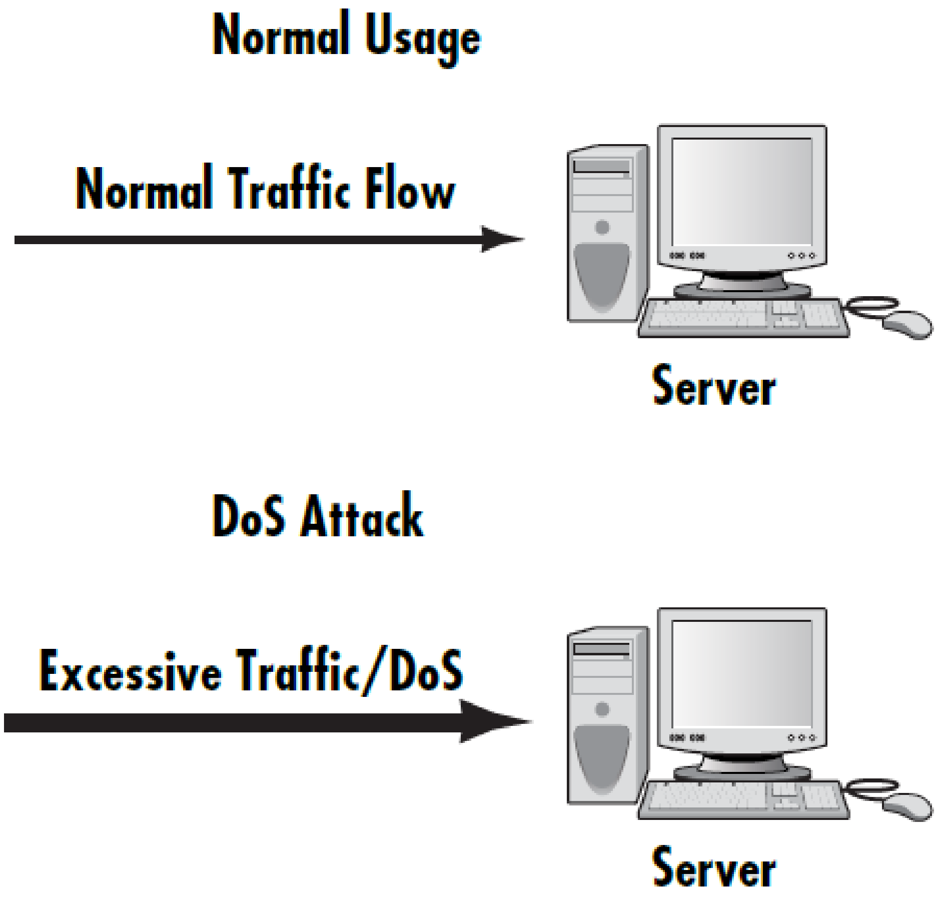
# A. Denial of Service Attacks

- Denial of Service (DoS)
- Distributed Denial of Service (DDoS)
- SYN Flood
- Smurf Attack
- The Ping of Death
- UDP Flood
- ICMP Flood
- DHCP Starvation
- HTTP Post DoS
- PDoS
- Distributed Reflection Denial of Service

# Denial of Service (DoS) Attacks

- Based on the premise that all computers have operational limitations

e.g., cpu cycles, memory space, network bandwidth



- Use the **ping** utility to execute the attack

# Distributed Denial of Service (DDoS) Attacks

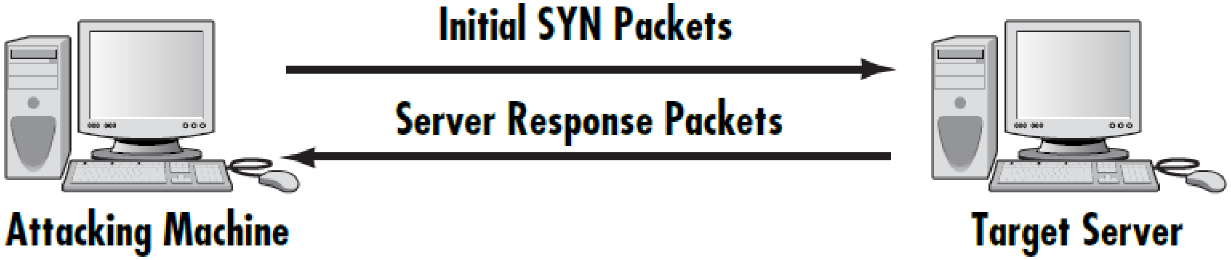
- Variation of a Denial of Service
- Launched from multiple clients
- More difficult to track due to the use of zombie machines

c.f., bots – “A bot (short for "robot") is an automated program that runs over the Internet. Some bots run automatically, while others only execute commands when they receive specific input.”

(source: https://techterms.com/definition/bot)

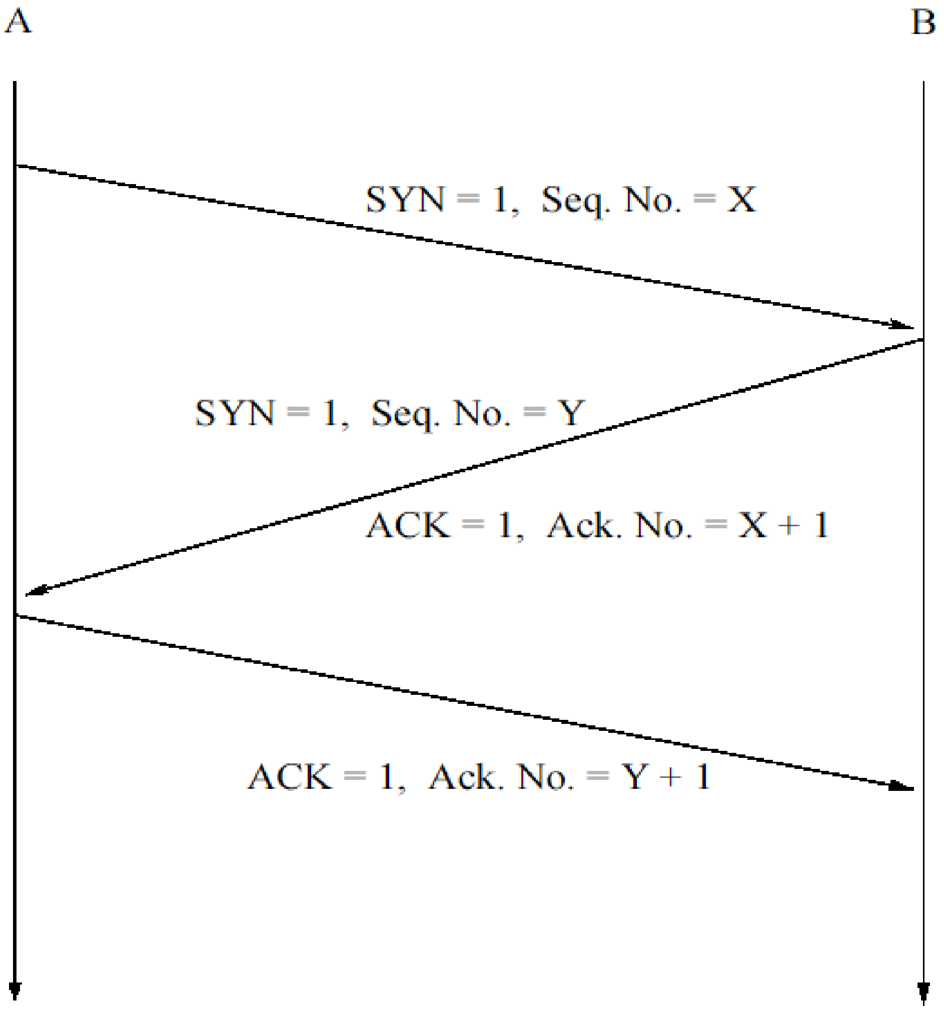
# SYN Flood

- Takes advantage of the *TCP handshake* process
- The target server’s buffer space for handling TCP connection are exhausted; preventing legitimate sessions to be established
- All protocols relying on TCP are vulnerable (e.g., HTTP)



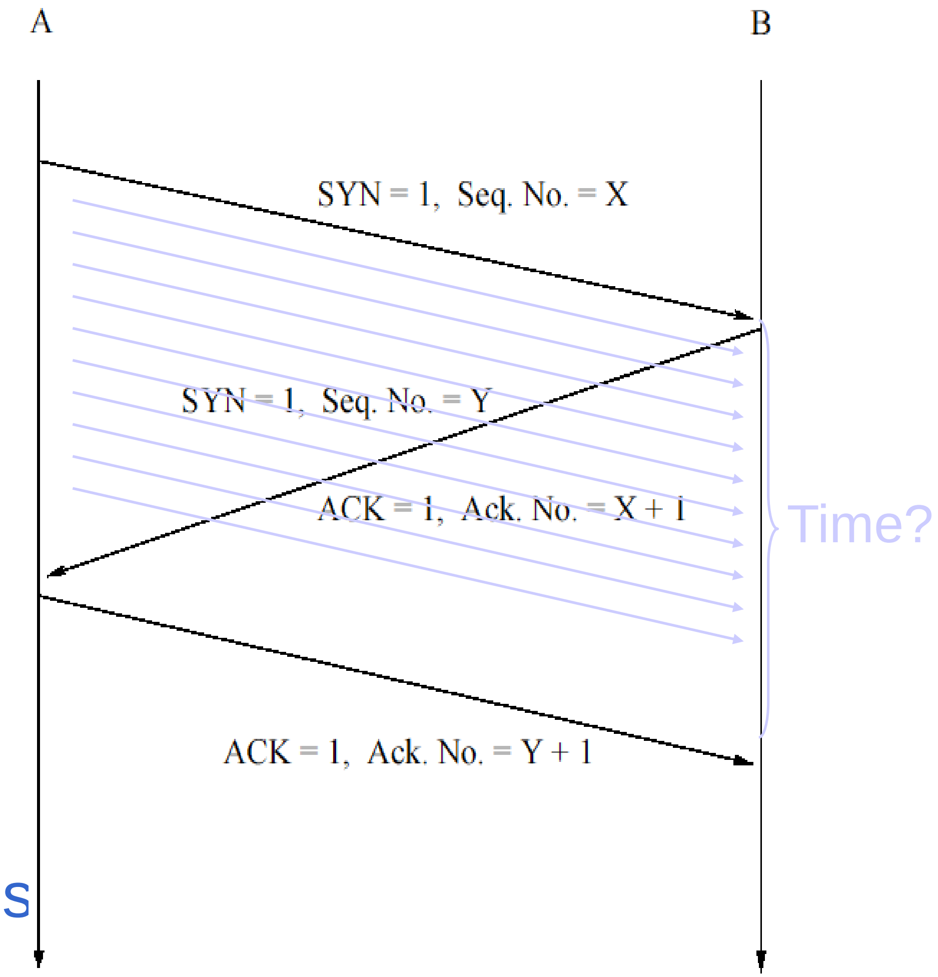
# SYN Flood

- TCP connection multi-step
  - SYN to initiate
  - SYN+ACK to respond
  - ACK gets agreement
- Sequence numbers then incremented for future messages
  - Ensures message order
  - Retransmit if lost
  - Verifies party really initiated connection



# SYN Flood

- Implementation
  - Receive SYN
  - Allocate connection
  - Acknowledge
  - Wait for response
- See the problem?
  - What if no response
  - And many SYNs
- All space for connections allocated
  - None for legitimate ones



# SYN Flood: Mitigations

- Micro Blocks

  Instead of a complete connection object, the server only allocates a few bytes to the incoming SYN request.

  **Q:** Would this be effective against the attack?

- Bandwidth Throttling

  Excessive SYN traffic from a IP causes that source’s bandwidth to be restricted (by the firewall or IDS)

# SYN Flood: Mitigations

- SYN Cookies - When receiving the SYN request, the server does not allocate memory space, but rather send a cookie to the requester.

  **Q:** Trade-offs?

- RST Cookies - The server sends a wrong SYNACK back to the requester.

  Problem? May not be effective (because of firewalls)

- Stack Tweaking - Reduce timeout time set in the server's stack

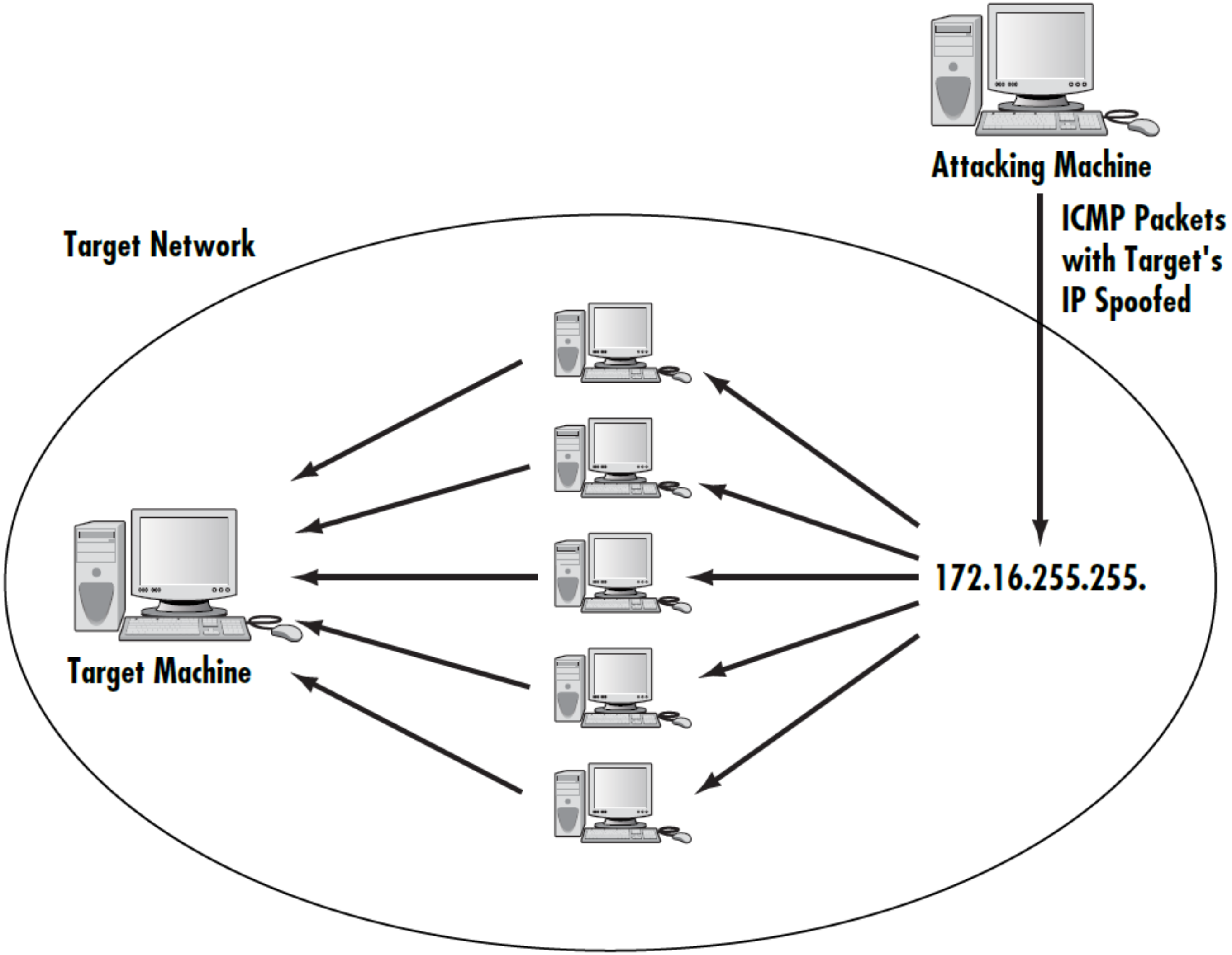
  Problem? (a) Only decrease (but doesn't prevent) the danger; (b) complicated

# SYN Flood: Mitigations

- Mitigations using intermediate hosts
  - **TCP intercept**
    - Router establishes connection to client
    - When connected then establish connection with server
  - **Synkill**
    - Monitor machine behaves like a “firewall”
    - Good addresses:  history of successful connections
    - Bad addresses:  previous timeout attempt
    - Block and terminate attempts from bad addresses

# Smurf Attack

- Sends an **ICMP** packet to the network’s broadcast address (with the victim’s spoofed IP as the source)



# Ping of Death (PoD)

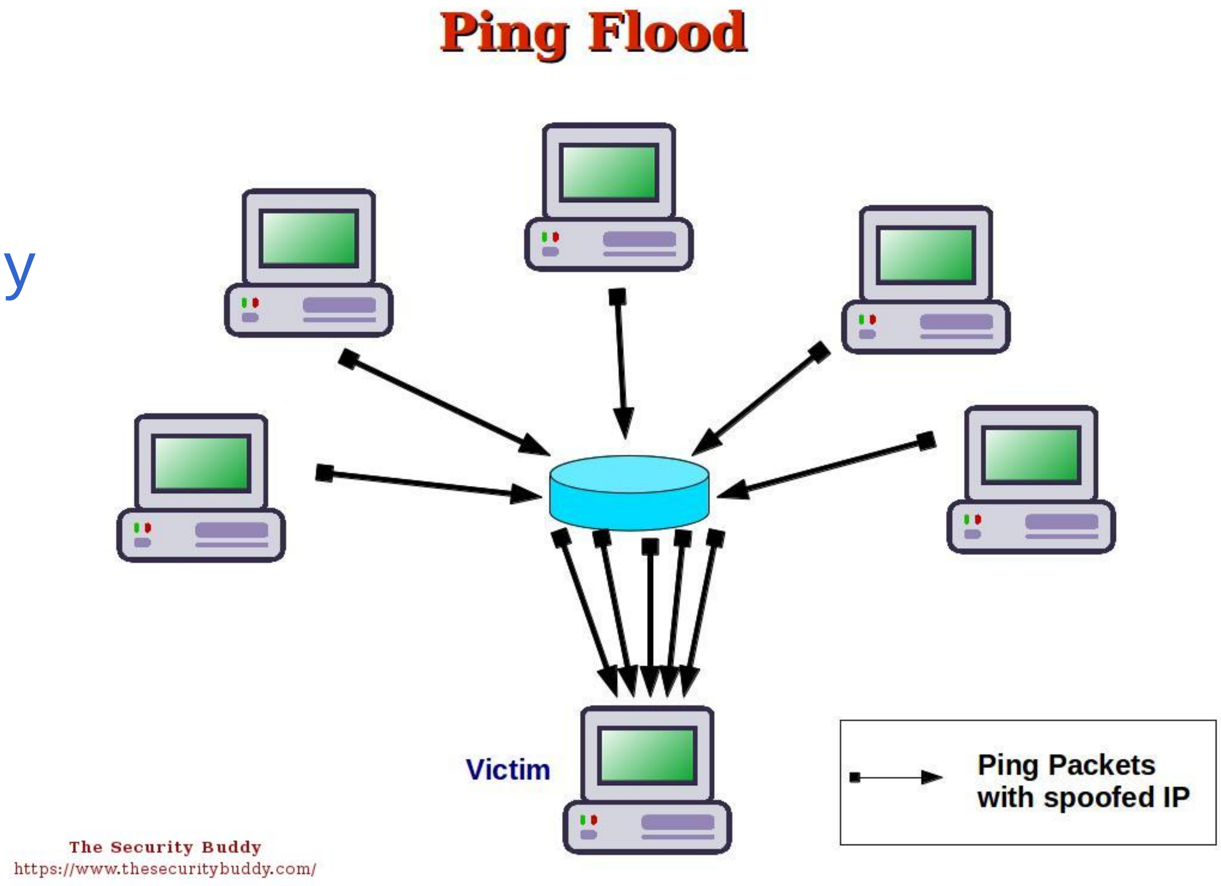
- Attacks machines that cannot handle oversized packets
- Causes the victim to crash

- Mitigations?
  - Ensure that systems are patched and up to date
  - Most current operating systems automatically drop oversized packets

# Ping Flood

- Sends a large number of ICMP Echo requests or ping packets to the victim

- The victim responds with ICMP Echo Reply packets
- Both the victim’s incoming and outgoing bandwidth are used.



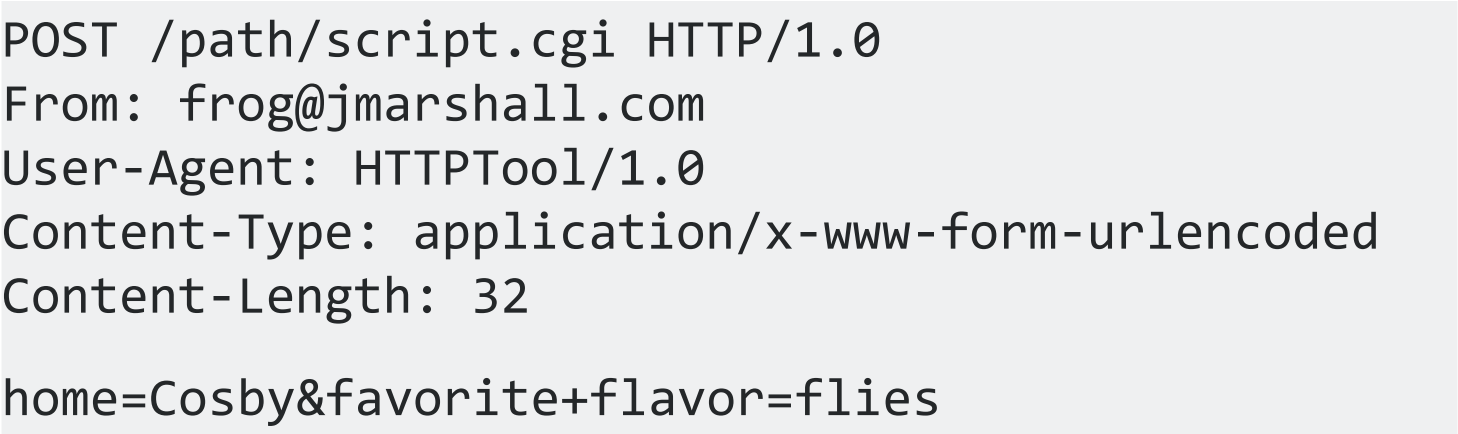
The Security Buddy
https://www.thesecuritybuddy.com/

# UDP Flood and IMCP Flood

- UDP (User Datagram Protocol) Flood
  - Targets a victim machine’s open ports
  - Sends packets to random ports of the victim
  - If enough are sent, the target computer will be overwhelmed.

- ICMP Flood
  - Another name for the Ping Flood

# HTTP Post DoS



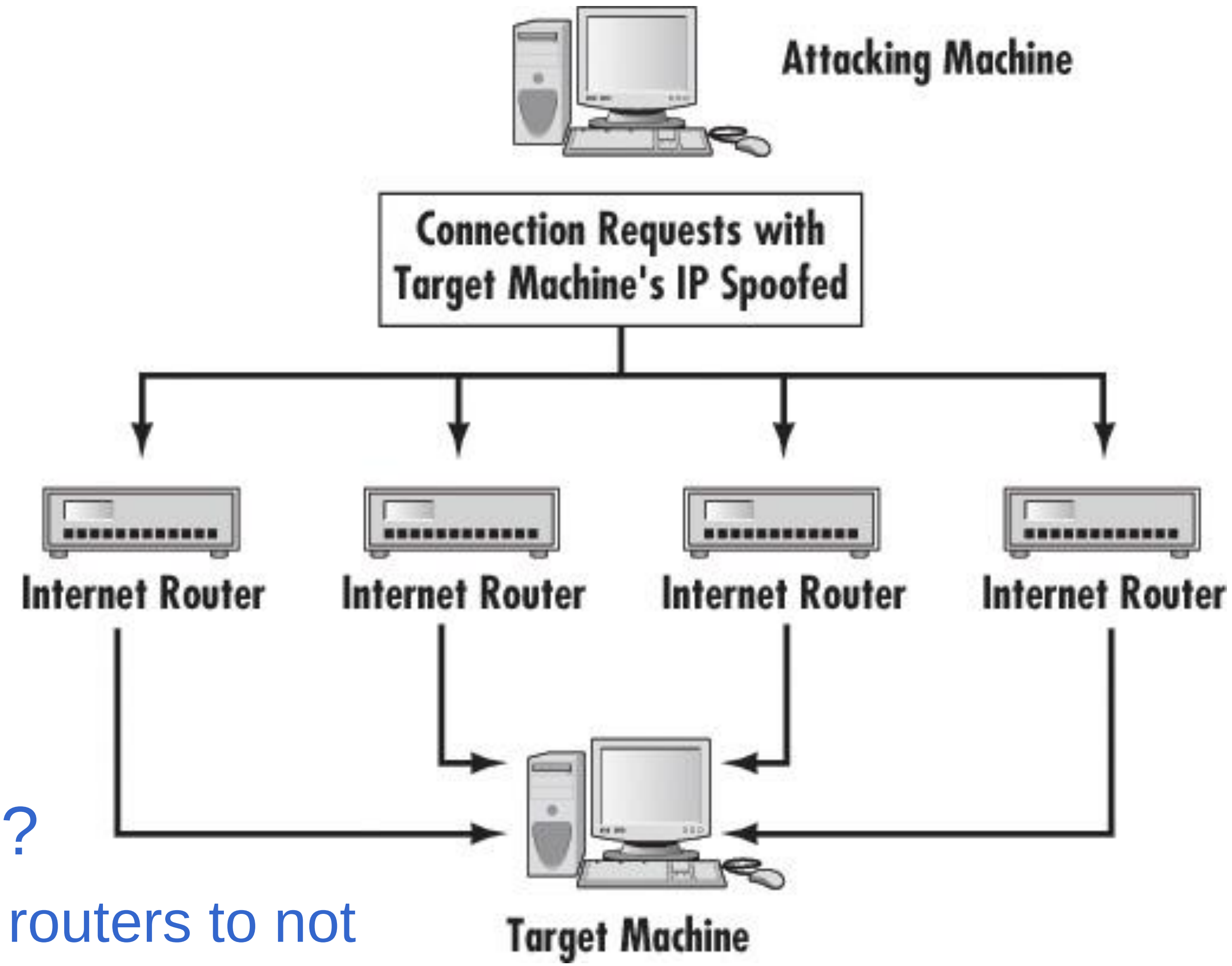
```
POST /path/script.cgi HTTP/1.0
From: frog@jmarshall.com
User-Agent: HTTPTool/1.0
Content-Type: application/x-www-form-urlencoded
Content-Length: 32

home=Cosby&favorite+flavor=flies
```

- Hangs server with slowly delivered **HTTP Post** message
- The *‘content-length’ is in the HTTP Post header, while the actual content is in the HTTP Post payload/body.*
- *The attacker sends the actual message body at an extremely slow rate, causing the HTTP server to ‘hung’.*

# Other Denial-of-Service Attacks

- DHCP Starvation
  - Dynamic Host Configuration Protocol
  - A DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network.
  - The attacker sends lots of DHCP Request to the server, causing the DHCP server's IP addresses to be depleted.
- Permanent DoS (PDoS) (a.k.a. *phlashing*)
  - Often attacks the device's firmware
  - Causes OS reboot or damaged hardware

# Distributed Reflection DoS (DRDoS)



- Mitigations?
  - Configure routers to not forward broadcast packets

# DoS Tools

- Tools are downloadable from the Internet.
- Ease of access facilitates widespread use.
- Example DoS tools:
  - Low Orbit Ion Cannon
  - High Orbit Ion Cannon
  - DoSHTTP

- **Warning:** Use a test system. DO NOT try these tools on a live system.

# Real World Examples of DoS Attacks

| Viruses | Started in | Purpose |
|---|---|---|
| FakeAV | 2012 | Fake Anti-Virus |
| Flame | 2012 | Spyware |
| MyDoom | 2004 | Cyber Terrorism |
| Gameover ZeuS | 2001 (src: https://www.knowbe4.com/gameover-zeus) | Peer-to-peer botnet |
| CryptoLocker & CryptoWall | 2013 (CryptoLocker)<br>2014 (CryptoWall) | Ransomware<br>+ bot (CryptoWall) |

# Defending Against DoS Attacks

- Understand how attack is perpetrated
- Configure firewall to disallow incoming protocols or all traffic
    - This may not be a practical solution.
- Disable forwarding of directed IP broadcast packets on routers
- Maintain virus protection on all clients on your network
- Maintain up-to-date operating system patches
- Establish policies for downloading software.

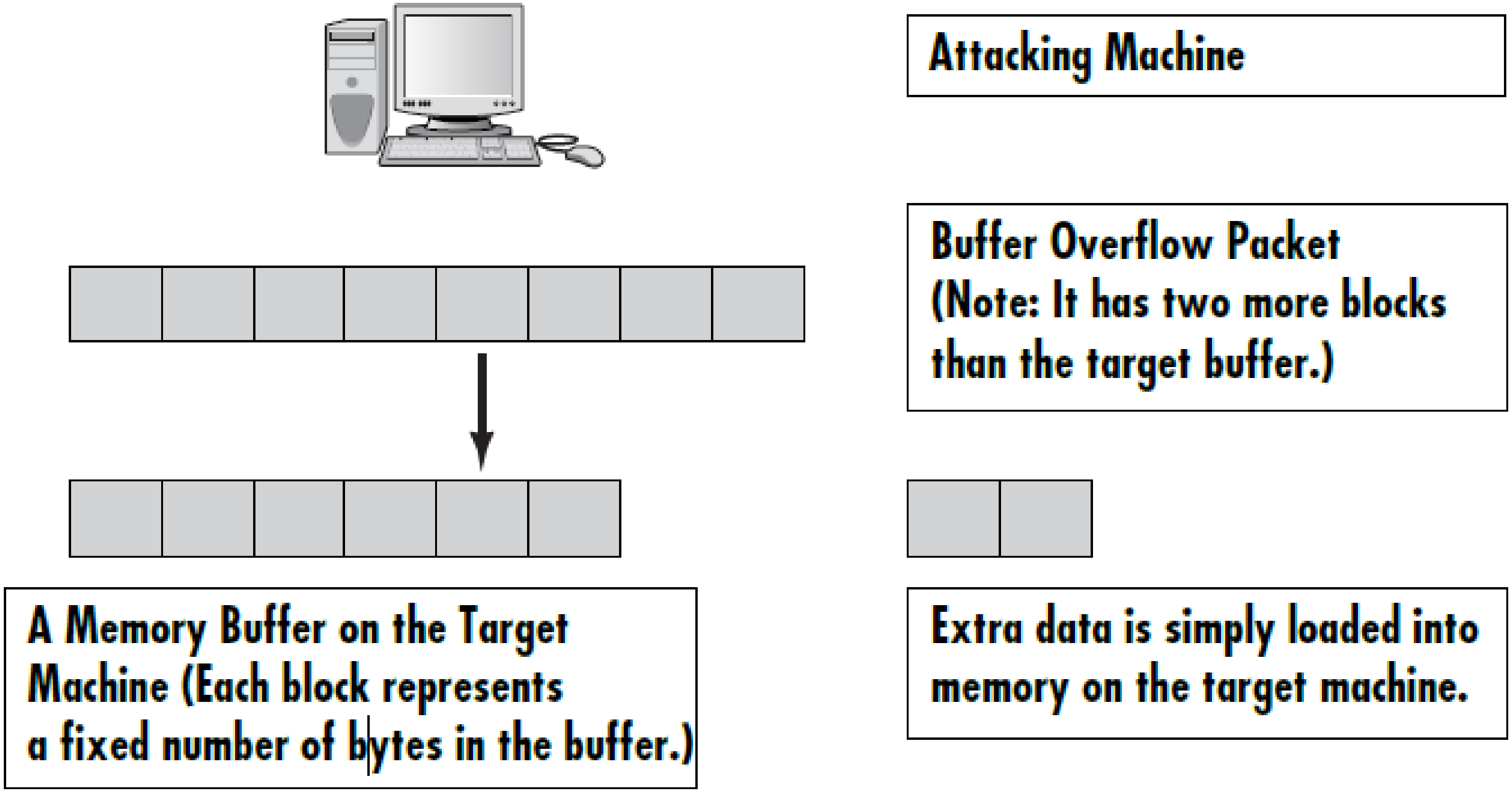
**Q.** Example policies?

# B. Buffer Overflow Attacks

- More common than DoS a few years ago
- Still a very real threat
- Designed to put more information in the buffer than it is meant to hold
- More difficult to execute (than DoS attacks)
- Can only occur if some flaw exists in the software
- Mitigations? ‘Good’ application design can reduce this threat.

# Buffer Overflow Attacks

- How do buffer overflow attacks occur?



Attacking Machine

Buffer Overflow Packet
(Note: It has two more blocks
than the target buffer.)

A Memory Buffer on the Target
Machine (Each block represents
a fixed number of bytes in the buffer.)

Extra data is simply loaded into
memory on the target machine.

# C. IP Spoofing

- Used to gain unauthorized access to computers by spoofing an authorized computer's IP address
- Source address of packet is changed
- Often used as part of a DoS attack
- Becoming less frequent due to security

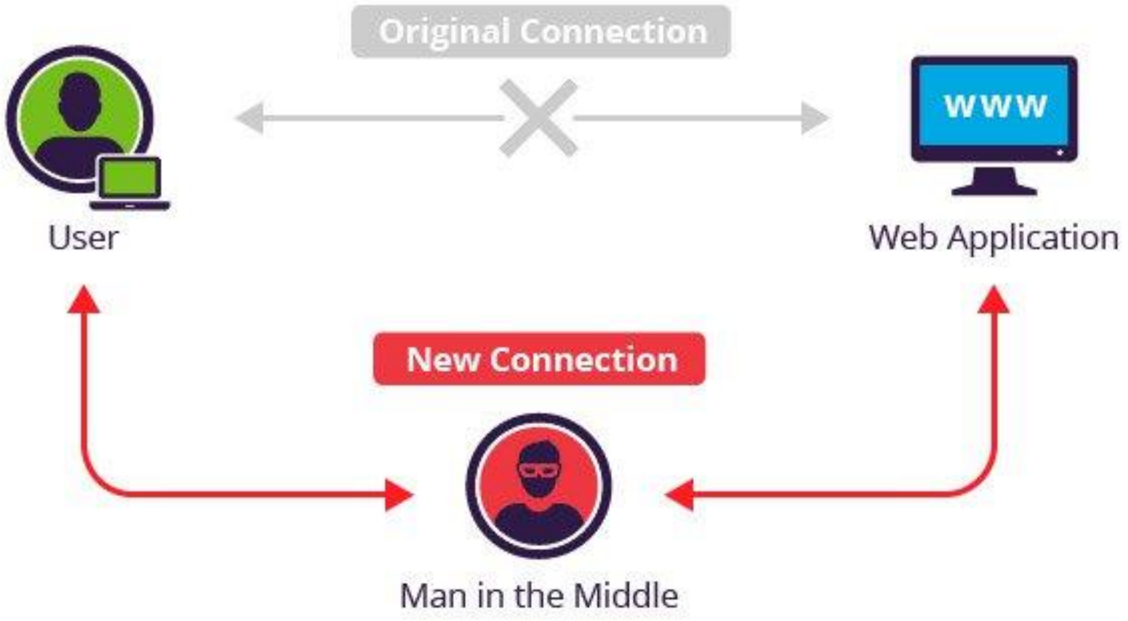
- Potential vulnerabilities with routers:
  - External routers connected to multiple internal networks
  - Proxy firewalls that use the source IP address for authentication
  - Routers that subnet internal networks
  - Unfiltered packets with a source IP on the local network/domain

# D. Session Hacking or Hijacking

- TCP Session Hijacking: The hacker takes over an established TCP session.
  - Possible because authentication often is done at the start of a TCP session (one time only).
- “Most common is the *man-in-the-middle* attack.” ← **Correction:** The attack described in the book is actually *eavesdropping* attack.
- **Q:** What is man-in-the-middle (MITM) attack?

# MITM attacks

- "… a **man-in-the-middle attack** (**MITM**) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other." -- https://en.wikipedia.org/wiki/Man-in-the-middle_attack



Src: https://www.incapsula.com/web-application-security/man-in-the-middle-mitm.html

# Session Hacking or Hijacking (cont.)

- An example of session hijacking:
  - Launch a DoS attack against one of the communicating entities, say X
  - Impersonate entity X while communicating with the remaining entity

**Q:** Why is session hijacking possible?

- Encryption may be the only way to combat this type of attack (because …)

# E. Virus Attacks

- Most common threat to networks
- Propagate in two ways
  - Scanning computer for network connections
  - Reading e-mail address book and sending to all
- Examples:
  - Sobig Virus
  - Mimail and Bagle
  - Sasser

# Protecting Against Viruses

- Always use virus scanner software
- Do not open unknown attachments
- Establish a code word with friends and colleagues
- Do not believe security alerts sent to you

**Q:** Other advices?

# F. Trojan Horse Attacks

- Program that looks benign but has malicious intent
- They might:
  - Download harmful software
  - Install a key logger or other spyware
  - Delete files
  - Open a backdoor for hacker to use

# Trojan Horse Caution

Students are strongly cautioned against attempting to create any of these Trojan horse scenarios. Release of this type of application is a criminal offense and likely to result in a prison sentence and civil penalties.

# Summary

- Most common network attacks
  - Session hacking
  - Virus and Trojan horse attacks
  - Denial of Service/Distributed Denial of Service
  - Buffer overflow

# Summary (cont.)

- Defenses against attacks
  - Antivirus software
  - Router configuration
  - Smart e-mail policies and procedures
  - Monitor network traffic
  - Maintain a current patch policy to keep systems up to date with security patches

# Summary (cont.)

- Defenses against DoS attacks
  - Proxy servers
  - Established policies on maintenance
    - Keep systems up to date with latest patches
- Defenses against Trojan horse and virus attacks:
  - Have an established policy for e-mail attachments and downloading software
    - Do not open unknown attachments
    - Strictly monitor software downloads and what can be downloaded

# Summary (cont.)

- Defenses against buffer overflow attacks
  - Routinely update systems
  - Keep security patches up to date