

CSc 466/566

Computer Security

25 : Network Security — DOS

Version: 2019/12/02 11:15:21

Department of Computer Science
University of Arizona

collberg@gmail.com
Copyright © 2019 Christian Collberg

Christian Collberg

1/38

Outline

- 1 Denial-of-Service Attacks
 - ICMP Attacks
 - SYN Flood Attacks
 - Exercises
- 2 Port Scanning
- 3 Intrusion Detection
- 4 Summary

Denial-of-Service Attacks

2/38

Denial-of-Service Attacks

- Web servers have limited bandwidth.
- Once the server has used up bandwidth/CPU, it starts dropping requests.
- **Denial-of-Service Attacks**: Any attack that targets a machine/software's availability.
- Source addresses are spoofed to hide the attacker's identity.

Denial-of-Service Attacks

3/38

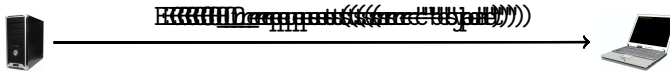
Internet Control Message Protocol

- The Internet Control Message Protocol (ICMP) is used for network diagnostics.
- ICMP messages:
 - 1 **Echo request**: please acknowledge receipt of packet.
 - 2 **Echo response**: packet receipt is acknowledged.
 - 3 **Time exceeded**: notify that packet has expired (TTL=0).
 - 4 **Destination unreachable**: notify that packet could not be delivered.

Denial-of-Service Attacks

4/38

DoS Attack 1: Ping Flood Attack



- A powerful machine can attack a less powerful one by sending it a large number of ECHO_requests.

DoS Attack 2: Smurf

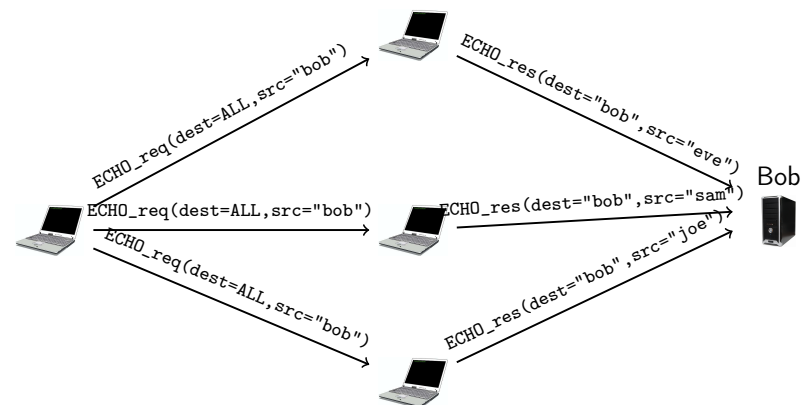
- A **broadcast** address sends to all IP addresses on the network.
- In a **smurf attack**, we get an amplification effect by creating an ECHO_request with a spoofed source address (of the target) and broadcasting this to all nodes on the network.
- Attack:
 - 1 Broadcast the packet
ECHO_request(src="target",dest="EVERYBODY") to the nodes on the network.
 - 2 Each node *N* will respond with
ECHO_response(src=*N*,dest="target").

DoS Attack 2: Smurf...

Definition (Smurf Attack)

The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. ... the name comes from the idea of very small, but numerous, attackers overwhelming a much larger opponent.

https://en.wikipedia.org/wiki/Smurf_attack



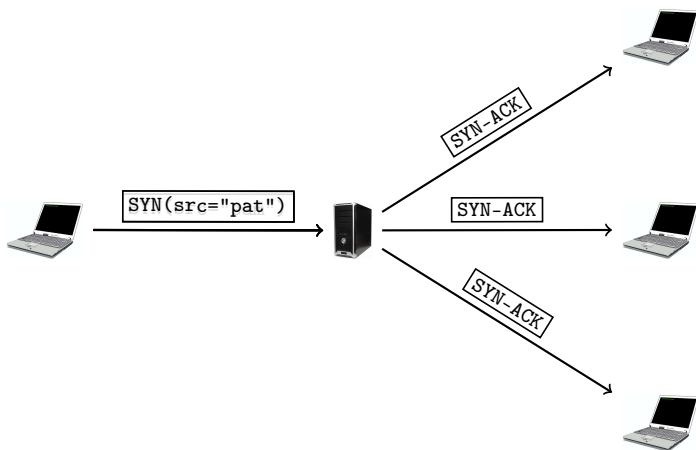
DoS Attack 2: Smurf...

- Countermeasures:
 - 1 Make hosts and routers ignore broadcasts.
 - 2 Make servers ignore all PINGs.

DoS Attack 3: SYN Flood

- Idea: Start lots of connections to a server, but never finish the SYN/SYN-ACK/ACK sequence, causing the server's memory to fill up.
- Attack:
 - 1 Eve sends a `SYN(src="joe")` packet to Alice's server.
 - 2 Server responds with SYN-ACK, sent to joe.
 - 3 Eve repeats from 1.

DoS Attack 3: SYN Flood...



DoS Attack 3: SYN Flood — Countermeasures



- SYN Cookies (see the book).
- Microsoft Windows:
 - A special queue for half-open connections.
 - Don't allocate resources for the TCP connection until the ACK has been received.

- Want to hear a SYN FLOOD joke?
- Want to hear a SYN FLOOD joke?
- Want to hear a SYN FLOOD joke?
- Want to hear a SYN FLOOD joke?
- Want to hear a SYN FLOOD joke?
- Want to hear a SYN FLOOD joke?
- Want to hear a SYN FLOOD joke?



DoS Attack 3: SYN Flood — Visualization

- http://williams.comp.ncat.edu/IA_visualization_labs/security_visual_tools/SYNFloodDemo/index.htm
- NOTE: Use Firefox, not Safari.
- For now, use http://williams.comp.ncat.edu/COMP375/IA/security_visual_tools/SYNFloodDemo/index.htm

Exercise I

- Name 3 denial of service attacks:

- What server resources could a DoS target?


Exercise II

- What resource does the SYN flood attack target?

- Briefly describe a SYN flood attack!


Exercise III

- What resource does the Smurf flood attack target?



- Briefly describe a Smurf attack!



Outline

- 1 Denial-of-Service Attacks
 - ICMP Attacks
 - SYN Flood Attacks
 - Exercises
- 2 Port Scanning
- 3 Intrusion Detection
- 4 Summary

Port Scanning

- **Port Scanning** looks for open ports on a server.
- Important first step in a DOS attack.
- Information collected:
 - Open/Closed/Blocked connection?
 - Server operating system?
 - What service is running on a port?
- Can be used by
 - good guys (is my network secure?)
 - bad guys (what vulnerable services can I exploit?)

Port Scanning — nmap

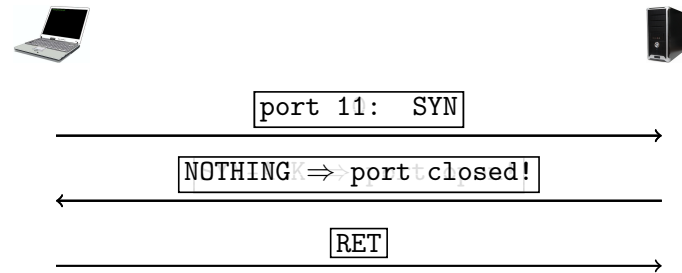
Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

- `nmap -A -T4 scanme.nmap.org`

NMap Videos

- NMap 101: Scanning Networks For Open Ports:
<https://www.youtube.com/watch?v=TyUtn0b-kS0>
- DEFCON 16: Nmap: Scanning the Internet (long):
<https://www.youtube.com/watch?v=Hk-21p2m8YY>

SYN Scans



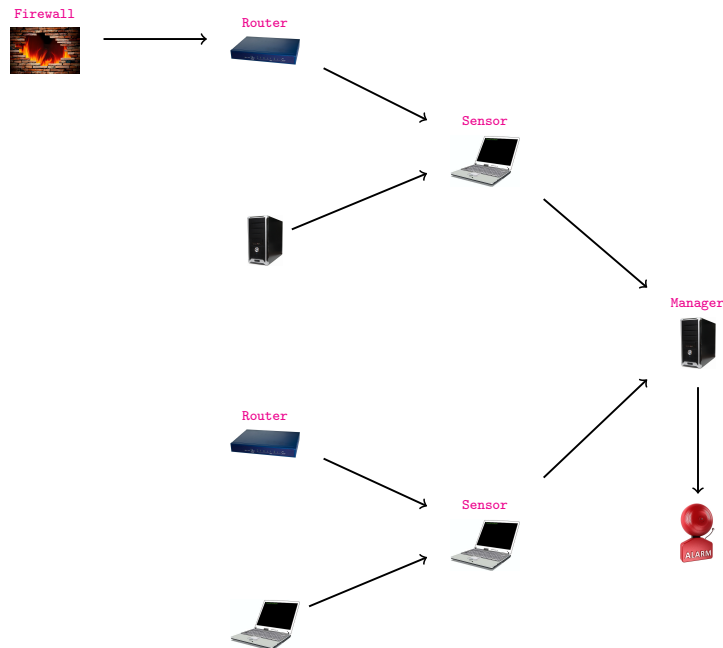
- 1 Send a TCP SYN packet to each port on the target.
- 2 Receive a SYN-ACK packet in return (the port is open!), close with RET.
- 3 Otherwise, try next port.

Outline

- 1 Denial-of-Service Attacks
 - ICMP Attacks
 - SYN Flood Attacks
 - Exercises
- 2 Port Scanning
- 3 Intrusion Detection
- 4 Summary

Intrusion Detection

- An **Intrusion Detection System** detects malicious activity on a network.
- Two components:
 - 1 **IDS sensors**: collect real-time data about the network,
 - 2 **IDS manager**: compiles reports from sensors.
- SNORT: <http://www.youtube.com/watch?v=baxPhuipA2M>
- Research projekt ReMIND: http://www.youtube.com/watch?v=onHg5g1Dg_0



IDS Managers

- The manager
 1. compiles reports from sensors,
 2. decides if an intrusion has occurred,
 3. raises an **alarm**

IDS Techniques — Attacks

- An IDS can detect many types of attack.
- A **masquerader** gains access using legitimate user's identity.
 - Detect unusual behavior using heuristic rules or statistical analysis.
- A **misfeasor** is a legitimate user behaving badly.
 - Detect violations of rules describing (un)authorized actions.
- A **clandestine user** deletes logs/audit files to cover up his actions.
 - Monitor (and log!) changes to log/audit files.

IDS Sensors

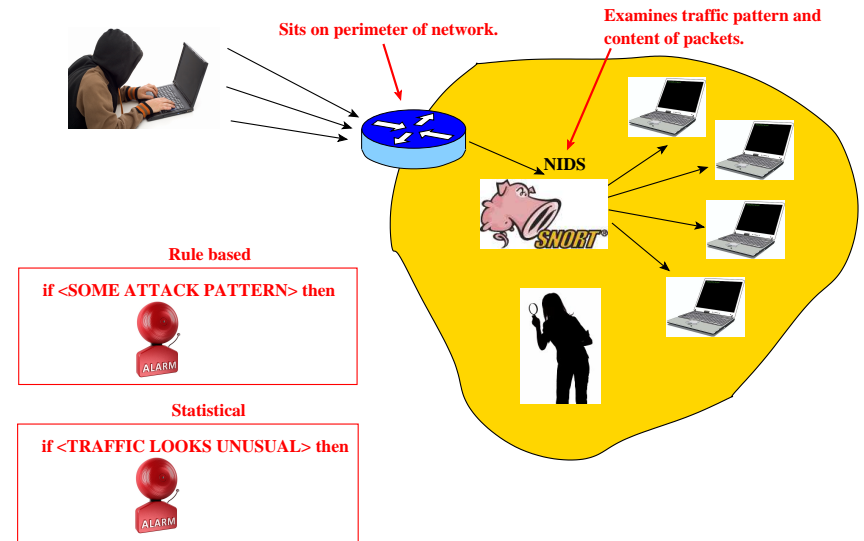
- The sensors
 1. collect information from routers, servers, ... ,
 2. writes records to an audit log.
- Audit log records:

Subject	Object	Action	Error	Usage	Time

Alice	/etc/passwd	read	no-error	5ms	05:30
128.72.100.99	196.200.11.2	HTTP	error-404	1ms	15:23

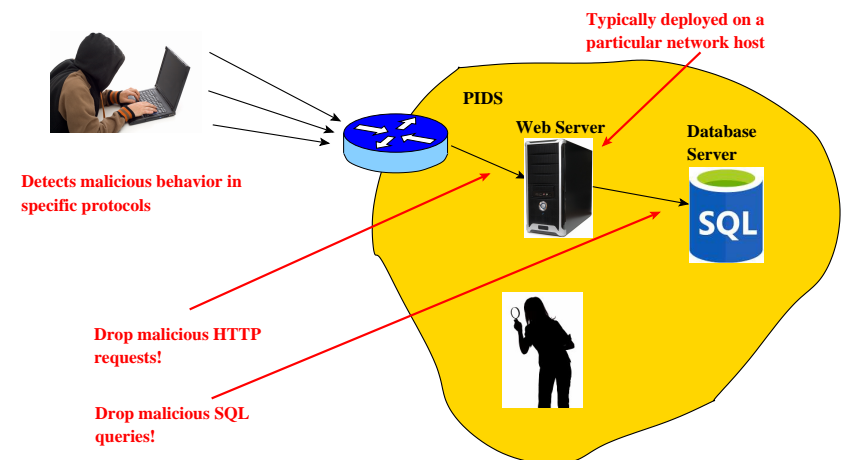
IDS Techniques — NIDS

- **Network Intrusion Detection System (NIDS):**
 - Where: edge of network;
 - Examines: traffic patterns, packet content;
 - Detects: malicious network behavior.
- Performs **deep packet inspection** in incoming and outgoing traffic.
- **Rule based**: compare traffic with a database of attack signatures.
- **Statistical**: compare traffic against baseline network behavior.



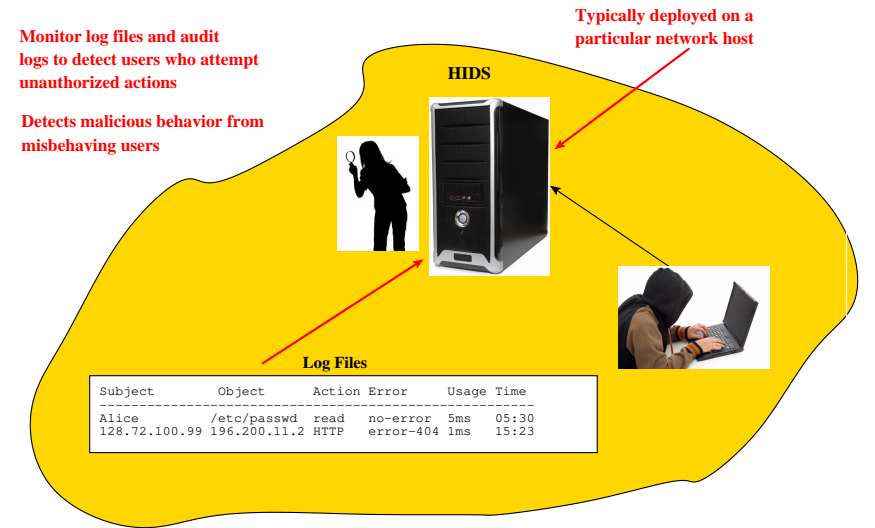
IDS Techniques — PIDS

- **Protocol-Based Intrusion Detection System (PIDS):**
 - Where: network host;
 - Examines: specific protocol traffic;
 - Detects: malicious content.
- Examples:
 - 1 Web server runs a PID to detect and drop malicious HTTP requests.
 - 2 PIDS detects malformed SQL queries between web server and database server.



IDS Techniques — HIDS

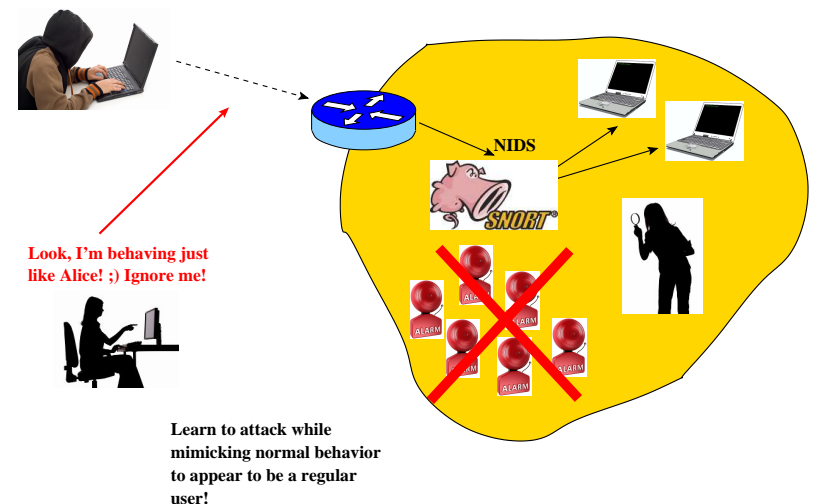
- **Host-Based Intrusion Detection System (HIDS):**
 - Where: single machine;
 - Examines: system calls, resource usage, interprocess communication, system logs;
 - Detects: malicious users.



Attacks on IDSs

What can an attacker do to get past the intrusion detection system?

- 1 Deliberately trigger many intrusion alerts (DOS against the IDS)!
- 2 Make attack too slow for the IDS to notice!
- 3 Learn the normal behavior of real users, and mimic them during the attack!



Outline

- 1 Denial-of-Service Attacks
 - ICPM Attacks
 - SYN Flood Attacks
 - Exercises
- 2 Port Scanning
- 3 Intrusion Detection
- 4 Summary

Readings and References

- Chapter 5 in *Introduction to Computer Security*, by Goodrich and Tamassia.