

#### **CSE467: Computer Security**

#### 20. Spoofing & Firewalls & IDS

Seongil Wi

Department of Computer Science and Engineering

# HW3 will be released today!

2

• Software Hacking Competition



# The student who is the quickest to complete all the problems will earn bonus points!

#### **Notification: Quiz #2**

- Date: 6/4 (Wed.), Class time
- Scope
  - Everything learned in Network Security!

- T/F problems
- Computation problems

#### Recap: Computer Network

- A telecommunications network that allows computers to exchange data
- Networked computing devices pass data to each other along data connections





## Recap: Distributed Denial-of-Service (DDoS)

• Employ **multiple (compromised) computers** to perform a coordinated and widely distributed DoS attack



## **Recap: Ping Flood Attack**

• The computing device is flooded with tons of Internet Control Message Protocol (ICMP) ping response



#### **Recap: Smurf Attack**

Idea: sending ping request to broadcast address



#### **Recap: Amplification Attack**

- Idea: controlling the size of responses, not the number of responses
- Example: DNS Amplification Attack



#### **Recap: TCP SYN Flooding Attack**

• Floods the server with SYN Packets



#### **Recap: Mitigation**

Set the Queue Size for TCP Backlog

\$ sysctl -w net.ipv4.tcp\_max\_syn\_backlog=1024

✓ Limitation: Arms race! Attackers can easily win

• Set the Firewalls

- E.g., Blocks if similar packets exceed 10 per second

\$ iptables -A INPUT -p TCP --dport 80 --syn -m limit 10/second -j ACCEPT \$ iptables -A INPUT -p TCP --dport 80 --syn -j DROP

✓ Limitation: Performance

SYN Cookie

## Recap: Command and Control (C&C) Server

- Essential for operation and support of botnet
- Two styles
  - Centralized
  - P2P



Image from <a href="https://www.a10networks.com/glossary/what-is-a-botnet-iot-botnet/">https://www.a10networks.com/glossary/what-is-a-botnet-iot-botnet/</a>

# Spoofing

#### Spoofing



- A situation in which a person or program is successfully identified as another by modifying data
- IP spoofing
- ARP spoofing
- DNS spoofing

#### **Recap: IP Spoofing**

 A situation in which a person or program is successfully identified as another by modifying data



## **Recap: IP Spoofing Method**

- How to
  - Network RAW socket programming
  - -Nmap
    - My own IP address is 10.0.0.1
    - \$ nmap -e eth0 -S 10.0.0.5 20.0.0.1
    - Use the network interface eth0 to send a spoofed packet (10.0.0.5) to 20.0.0.1

— . . .





- An attacker sends spoofed Address Resolution Protocol (ARP) response messages
- Also known as ARP cache poisoning attack

• A protocol that maps an *ever-changing* **IP address** to a *fixed* physical machine address (**MAC address**)



• A protocol that maps an *ever-changing* **IP address** to a *fixed* physical machine address (**MAC address**)



#### What is the MAC address of 10.0.0.2?

![](_page_20_Figure_2.jpeg)

#### What is the MAC address of 10.0.0.2?

![](_page_21_Figure_2.jpeg)

*My MAC address is* 00:10:20:30:ac:06

#### What is the MAC address of 10.0.0.2?

![](_page_22_Figure_2.jpeg)

*My MAC address is* 00:10:20:30:ac:06

#### What is the MAC address of 10.0.0.2?

![](_page_23_Figure_2.jpeg)

*My MAC address is* 00:10:20:30:ac:06

![](_page_24_Figure_1.jpeg)

![](_page_25_Figure_0.jpeg)

![](_page_26_Figure_0.jpeg)

![](_page_27_Figure_0.jpeg)

![](_page_28_Figure_0.jpeg)

![](_page_29_Figure_0.jpeg)

![](_page_30_Figure_0.jpeg)

![](_page_31_Figure_0.jpeg)

#### ARP Spoofing – Use Case

33

Home > 전체기사

Public WIFI is vulnerable to MITM attacks (via ARP spoofing)

#### 카페서 와이파이 쓰다 스마트폰 가로채기 당한다?

입력:2015-10-29 11:30

![](_page_32_Picture_6.jpeg)

모바일에서 공유기 통해 외부 접근시 공격자가 스마트폰 정보 가로채기 가능

[보안뉴스 김경애] 올해 1분기 주요 보안 이슈로 떠오른 바 있는 공유기 보안 문제가 좀처럼 해결되지 않고 있다. 사람들이 이용하는 카페 등 공공장소에서 공유기를 통해 무료 와이파이를 이용할 경우 모바 일을 이용해 정보를 가로챌 수 있는 ARP 스푸핑(Spoofing) 공격이 가능한 것으로 드러났기 때문이다. 이에 따라 공공장소나 카페에서 와이파이 접속시 이용자들의 주의가 요구된다.

Not recommended to use public WIFI!

#### How to Mitigate ARP Spoofing Attacks? <sup>3</sup>

- Packet encryption
  - E.g., Visit websites via HTTPs protocol
- Static ARP caches
  - IP-MAC address mappings in the local ARP cache may be statically entered
- Packet filtering
  - Check if many ARP responses are sent without a request

# **Firewalls V**

![](_page_34_Picture_1.jpeg)

#### **Firewalls**

 Isolate organization's internal net from larger Internet, allowing some packets to pass, blocking others

![](_page_35_Figure_2.jpeg)

#### Main Goals of Firewall

- Restrict incoming and outgoing traffic by IP address, ports, or users
  - Block invalid traffic and only authorized traffic is allowed

![](_page_36_Figure_3.jpeg)

#### **Types of Firewall**

- Three types of firewalls:
  Packet filters
  - -Application gateways

#### **Packet Filters**

![](_page_38_Picture_1.jpeg)

- Internal network connected to Internet via router firewall
- Router filters packet-by-packet from the network layer, decision to forward/drop packet based on:
  - Source/destination IP address
  - Source/destination port numbers
  - ICMP message type
  - Protocol status (e.g., TCP SYN, TCP ACK, ...)

#### Packet Filters via Router Firewall

![](_page_39_Figure_1.jpeg)

#### **Packet Filters via Router Firewall**

![](_page_40_Figure_1.jpeg)

## Packet Filters – High-level Example

Policy	Firewall Setting		
No incoming web access	Drop all incoming packets to any IP address, port 80		
No incoming TCP connections, except those for institution's public web server only	Drop all incoming TCP SYN packets to any IP except 130. 207.244.203, port 80		
Prevent your network from being used for a ICMP flooding attack	Drop all ICMP packets going to a "broadcast" address		

# Packet Filters – Detailed Example

Action	Source Address	Dest. Address	Protocol	Source port	Dest port	Flag bit
Allow	222.22/16	Outside of 222.22/16	TCP	> 1023	80	any
Allow	Outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
Allow	222.22/16	Outside of 222.22/16	UDP	> 1023	53	
Allow	Outside of 222.22/16	222.22/16	UDP	53	> 1023	
Deny	all	all	all	all	all	all

# Packet Filters – Pros and Cons

- Pros
  - Simple to implement
  - Low impact on network performance
- Cons
  - Malicious content in application data cannot be filtered out

#### **Packer Filter: Limitation**

![](_page_44_Figure_1.jpeg)

![](_page_44_Figure_2.jpeg)

#### **Application Gateways**

- 46
- Filter packets on application data as well as on IP/TCP/UDP fields

₩

![](_page_46_Figure_0.jpeg)

## Application Gateways – Pros and Cons

• Pros

 Tend to be more secure than packet filters because they can examine every layer of the communication

- Cons
  - Complex to implement
  - High impact on network performance

# Intrusion Detection System (IDS)

#### **Intrusion Detection**

50

Intrusion

- A set of actions aimed to compromise the security goals

- Intrusion detection
  - The process of identifying and responding to intrusion activities

![](_page_49_Figure_6.jpeg)

#### Firewall vs. IDS

![](_page_50_Picture_1.jpeg)

- Firewall
  - Active filtering (prevent intrusion)
  - Location: Between networks (if an attack is from inside the network it doesn't signal)

#### • IDS

- Passive monitoring (detect intrusion)
- Location: Inside the network

![](_page_50_Figure_8.jpeg)

# Detection Methods of IDS

1. Signature-based detection

2. Anomaly-based detection

![](_page_51_Picture_3.jpeg)

## IDS Type #1. Signature-based Detection

- Detects the attacks on the basis of the specific patterns
  - E.g., Snort, Bro

![](_page_52_Figure_3.jpeg)

#### **IDS Type #1. Signature-based Detection**

![](_page_53_Picture_1.jpeg)

![](_page_53_Picture_2.jpeg)

![](_page_53_Picture_3.jpeg)

![](_page_54_Picture_1.jpeg)

#### • Signature example:

# alert tcp 192.168.2.0/24 23 -> any any \ (content: "naver" msg: "NAVER Detected!!")

#### **Example: Snort**

![](_page_55_Figure_1.jpeg)

![](_page_55_Figure_2.jpeg)

## IDS Type #1. Signature-based Detection

- Detects the attacks on the basis of the **specific patterns**
- Limitation: difficult to detect new malware attacks as their pattern is not known

## **IDS Type #2. Anomaly-based Detection**

58

 Detects the attacks on the basis of the statistical models or machine learning models

![](_page_57_Figure_2.jpeg)

## **IDS Type #2. Anomaly-based Detection**

- Detects the attacks on the basis of the statistical models or machine learning models
- Limitation: relatively high false positive rate anomalies can just be new normal activities

#### **Deployment of IDS**

1. Host IDS

![](_page_59_Figure_2.jpeg)

#### HIDS (Host IDS)

![](_page_60_Picture_1.jpeg)

- Using OS auditing mechanisms
  - e.g., BSM on Solaris: logs all direct or indirect events generated by a user
  - -strace for system calls made by a program
- Monitoring user activities
  - -e.g., Analyze shell commands
- Monitoring executions of system programs
  - -e.g., Analyze abnormal system calls

#### Limitations:

- Occupies a certain portion of host resources
- An IDS must be installed and operated on every individual host

#### NIDS (Network IDS)

62

- Deploying sensors at strategic locations
  - -e.g., Packet sniffing via tcpdump at routers
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
- Monitoring user activities
  - Look into the data portions of the packets for malicious command sequences

#### Limitations:

• Easily defeated by encryption

#### **Summary**

- Worm: first network attack
- Denial of Service (DoS)
  - Distributed DoS (DDoS)
  - Ping Flood Attack
  - Amplification Attack
  - SYN Flooding Attack
- ARP Spoofing Attack
- Defense: Firewalls, IDS, IPS

![](_page_63_Picture_0.jpeg)