CSCI369 Ethical Hacking

Lecture 2-2 Scanning

A/Prof Joonsang Baek

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

Introduction to Scanning

- The purpose of scanning (in general)
  - ➢To discover which machines in the target system are available (live): We cannot perform attacks remotely if any of the machines are not available.
  - ➢To discover the underlying operating system used by a target machine: This information can be used for further exploitation.
- Relation to information gathering
  - ➢Scanning gives us *more specific and precise* information that can lead to exploitation (attack).

Introduction to Scanning

- Scan type
  - ➢Ping sweep: This scan is to discover live systems, for example, to identify which IP addresses have a system that is *powered*.
  - ➢Port scanning: A form of scanning that targets individual IP addresses and identifies the ports which are open and closed on a specific system.
    - ✓Total number of ports: 65,535 (= 2^{16}-1)
    - ✓Example: “Port 1433 is open” means that the target is running SQL server, which can be exploited by an attacker.
  - ➢Vulnerability scanning: This scan is to find weaknesses or problems in an environment and generate a report on its findings.

Introduction to Scanning

- A list of detailed information that can be obtained from scanning
  - IP addresses of system that are “live”, which includes phones, tablets, printers, wireless AP as well as regular PCs
  - List of open and closed ports on a target system
  - Operating system versions
  - MAC addresses
  - Service information
  - Other network information

ICMP Scanning (Ping)

- ICMP: A base protocol for ping sweep → This is the reason why ping sweep is called “ICMP scan”.
- According to RFC 1122, every host that receives an ICMP echo request should respond.
- In reality, quite a few networks and hosts block ICMP echo requests to prevent scanning.

Ping Sweep Tools

- `ping`
  - Targets one specific IP.
  - Commonly used.
- `fping`
  - Used to ping multiple IP addresses

```
fping –g BeginningIP-EndingIP
fping –g IP1, IP2,…,IPn
fping –g CIDR
```

  - The multiple addresses can be saved in a file can be read:

```
fping –f ip_address.txt
```

  - `fping –h` will provide information about options

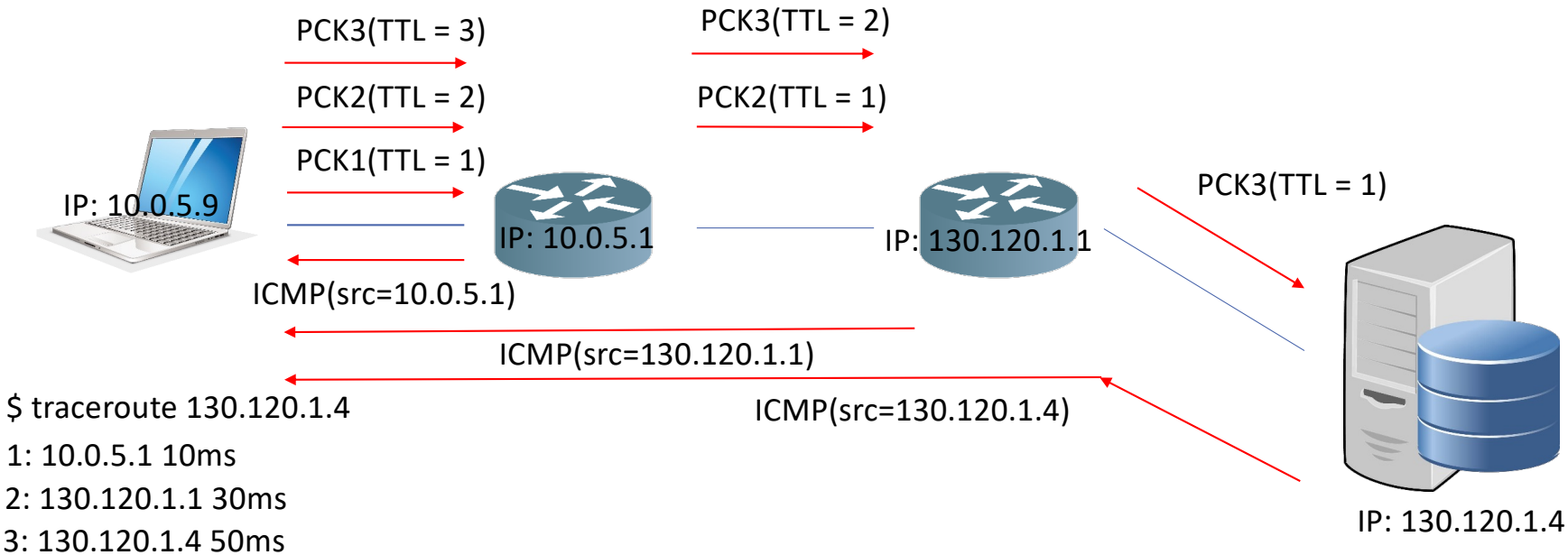
Traceroute

- Traceroute uses the TTL of IPv4 packets
  - Every IPv4 packet has a TTL (Time-to-live), usually 64.
  - TTL is the maximum number of hops from the source to the destination. This prevents the packets which do not reach to the destination from traveling or looping in the network indefinitely.
  - TTL is reduced by 1 when the packet passes a Layer 3 (IP) router.
  - If the IP router receives the packet whose TTL is 1, the router will send ICMP TTL exceeded message to the source (of the packet) and delete the packet.
  - *Traceroute* command uses this property of the network to find a route to the destination.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Traceroute

- For example, if the server is located in 3-hop distance:



$ traceroute 130.120.1.4

1: 10.0.5.1 10ms

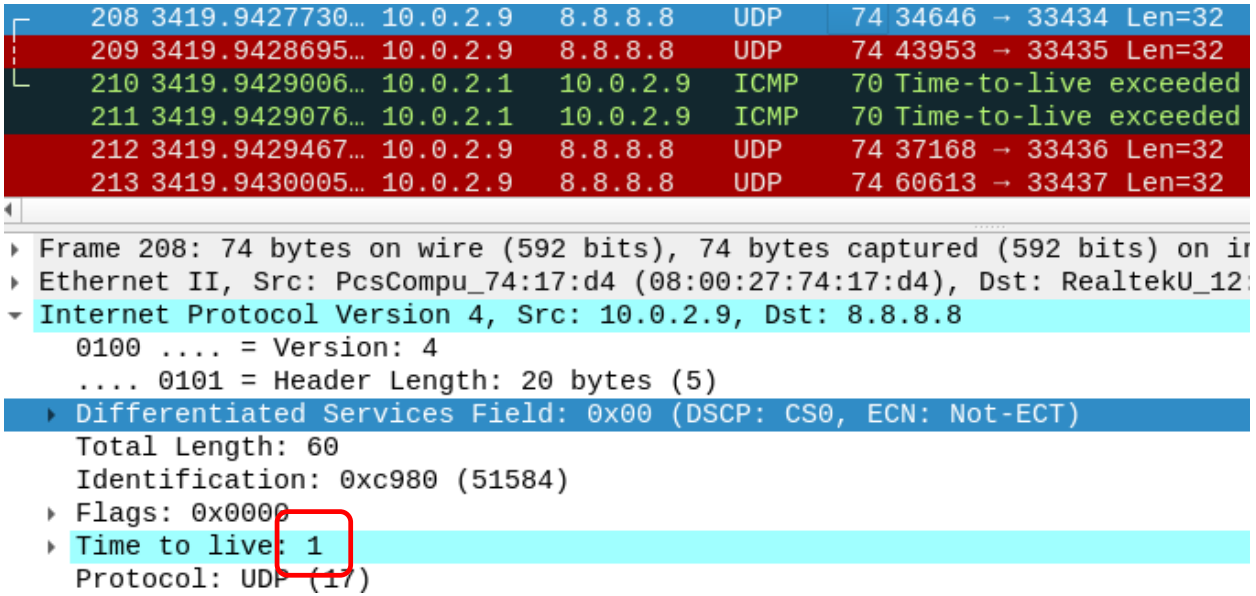
2: 130.120.1.1 30ms

3: 130.120.1.4 50ms

UNIVERSITY OF WOLLONGONG AUSTRALIA

Traceroute

- Traceroute packets captured By Wireshark



Port-Scanning Tools

- Nmap
  - The most popular port scanner.
  - Added many new features including service/version detection, OS detection, network traceroute, multiple ping scanning and scripting functionality
  - Basic command: `nmap option <target IP Address>`
  - Detailed information: https://nmap.org

Port-Scanning Tools

- Nmap target specification
  - ➢The target host IP addresses can be specified in a number of ways:
    - ✓A single host: 192.167.1.1
    - ✓A network using CIDR notation: 192.168.1.0/24
    - ✓Range of IP addresses: 192.168.3-5,7.1 (This implies 192.168.3.1, 192.168.4.1 , 192.168.5.1 and 192.168.7.1)
    - ✓List of IP addresses: 10.0.2.4 10.0.2.5 10.0.2.15
  - ➢IPv6 is also supported

Port-Scanning Tools

- Nmap options
  - ➢By default, TCP SYN scan is used; other options are:
  - –sT (TCP connect): Full open scan (performing three-way handshake)
  - –sS (TCP SYN scan) Half open scan → Nmap default
  - –sN (TCP NULL scan)
  - –sF (TCP FIN scan)
  - –sX (TCP Xmas scan)
  - –sA (TCP ACK scan)
  - –sU (UDP scan)

Port-Scanning Tools

- Nmap port specification
  - ➢By default, Nmap will scan the most common 1000 ports in a random order
  - ➢Other options are:
    - `-p port range`: Scan only the defined ports
    - `-F` : Scan only 100 most common ports (fast)
    - `-r` : Do not randomize port numbers
    - `--top-ports N` : Scan the most common N ports

Port-Scanning Tools

- Nmap six states
  - open
  - closed
  - filtered
  - unfiltered
  - open|filtered
  - closed|filtered → Uncommon

UNIVERSITY OF WOLLONGONG AUSTRALIA

Port-Scanning Tools

- Nmap timing options: `-T<modes>` ex) -T3, -T5, etc.
  - Paranoid (0): A packet is sent every 5 minutes
  - Sneaky (1): A packet is sent every 15 seconds
  - Polite (2): A packet is sent every 0.4 seconds
  - Normal (3): Default (multiple packets to multiple targets sent)
  - Aggressive (4): Nmap will not wait for more than 1.25 seconds for a response
  - Insane (5): Nmap will not wait for more than 0.3 seconds for a response

Port-Scanning Tools

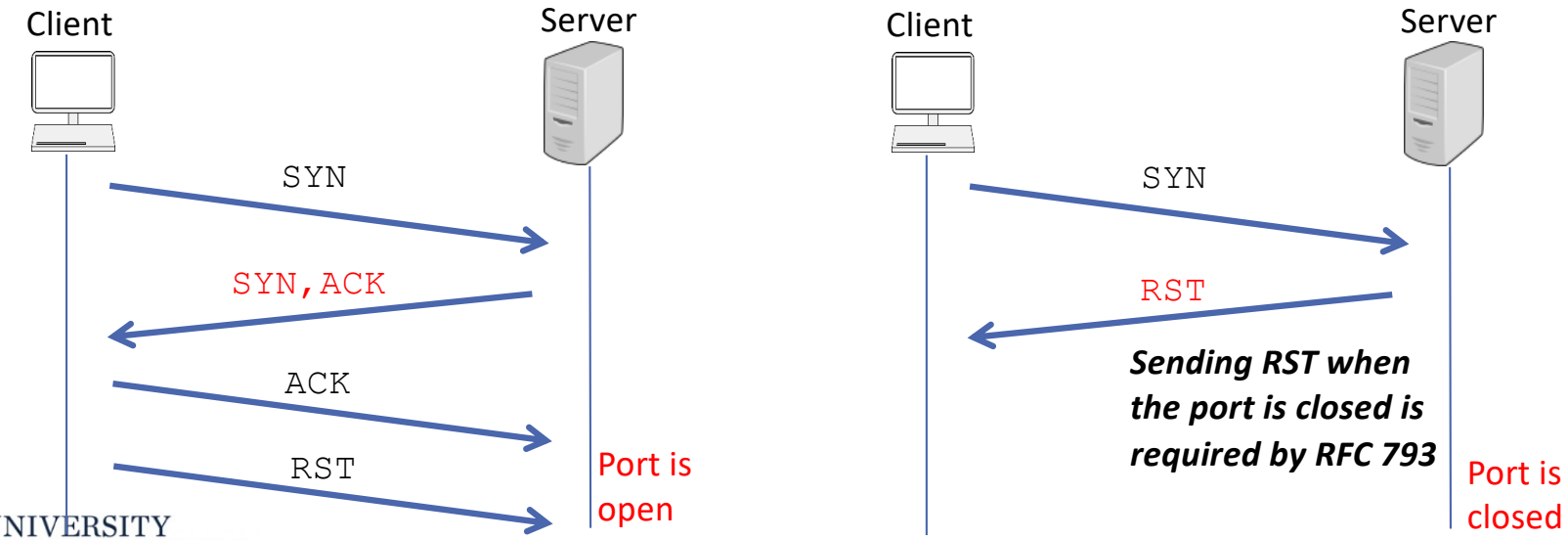
- Nmap output options
  - Interactive output: Default
  - Normal output: `-oN filename`
  - XML output: `-oX filename` (This format can be converted to HTML format)

Scanning Based on TCP

- Determine the states of ports (open, closed, filtered, unfiltered)
- It uses (or exploits) various flags of the basic TCP packet:
  - SYN, ACK, URG, PSH, FIN, RST
  - Using one of the flags means *the flag is set to 1*.
    - ✓For example, SYN, ACK (SYN-ACK) means both SYN and ACK flags are set to 1.
  - Note that the SYN and ACK flags will not be used in NULL, FIN and Xmas scans.

TCP Scan (Full Open Scan)

- TCP scan performs the usual three-way handshake to determine if the host (server)'s port is open



UNIVERSITY OF WOLLONGONG AUSTRALIA

TCP Scan (Full Open Scan)

- Properties of TCP scan
  - ➢The result is reliable.
  - ➢It is “noisy” meaning multiple scanning attempts can be detected.
    - ✓ It creates more traffic.
  - ➢Nmap command:

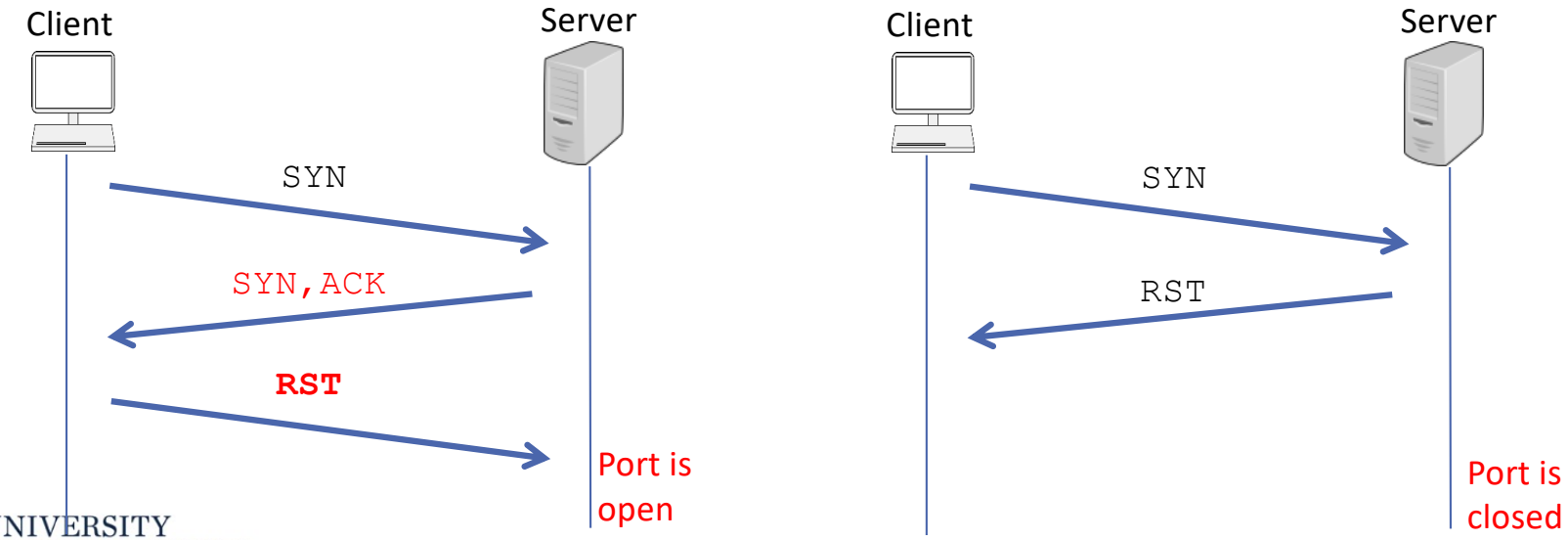
```
nmap -sT -v  <target IP address>
```

    * `-v` (“verbatim”) detailed information about the scanning.

UNIVERSITY OF WOLLONGONG AUSTRALIA

SYN Scan (Half Open Scan)

- In SYN scan, the attacker sends RST instead of ACK upon receiving SYN, ACK (SYN-ACK) at the end of the three-way handshake



UNIVERSITY OF WOLLONGONG AUSTRALIA

SYN Scan (Half Open Scan)

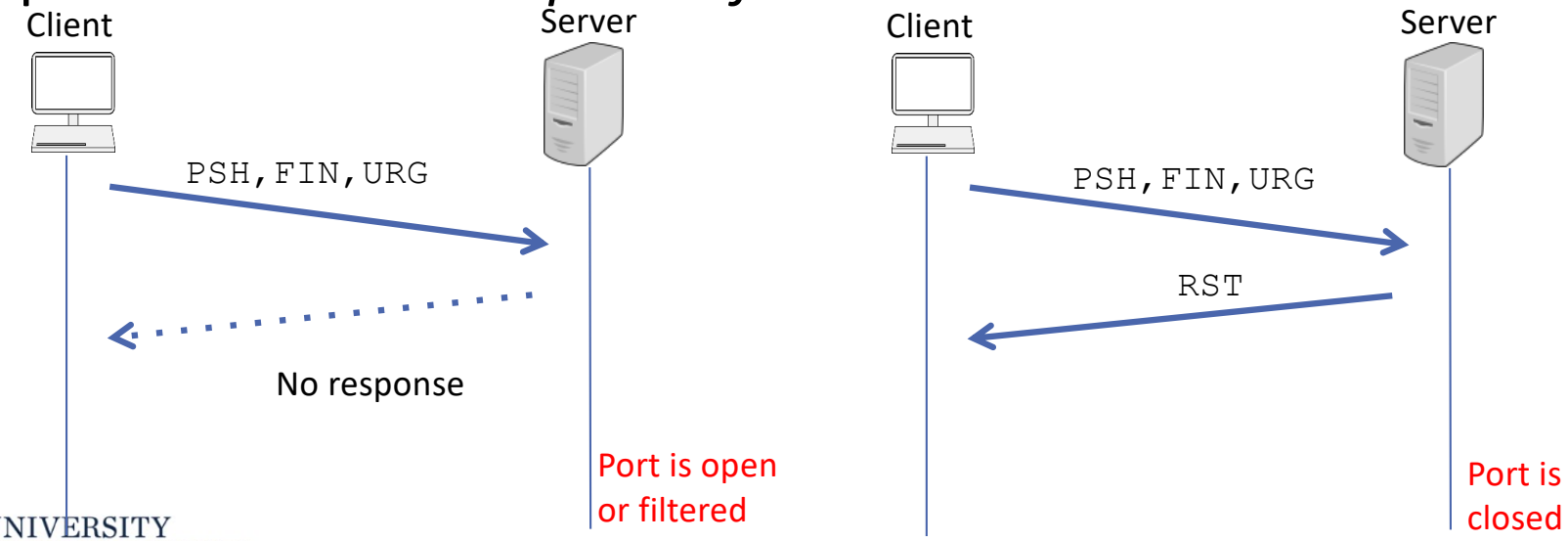
- Properties of SYN scan
  - Less noisy than the TCP scan.
  - Nmap command:

```
nmap –sS –v  <target IP address>
```

  - Arguably, it is *the most frequently-used* scanning method.

Xmas Scan

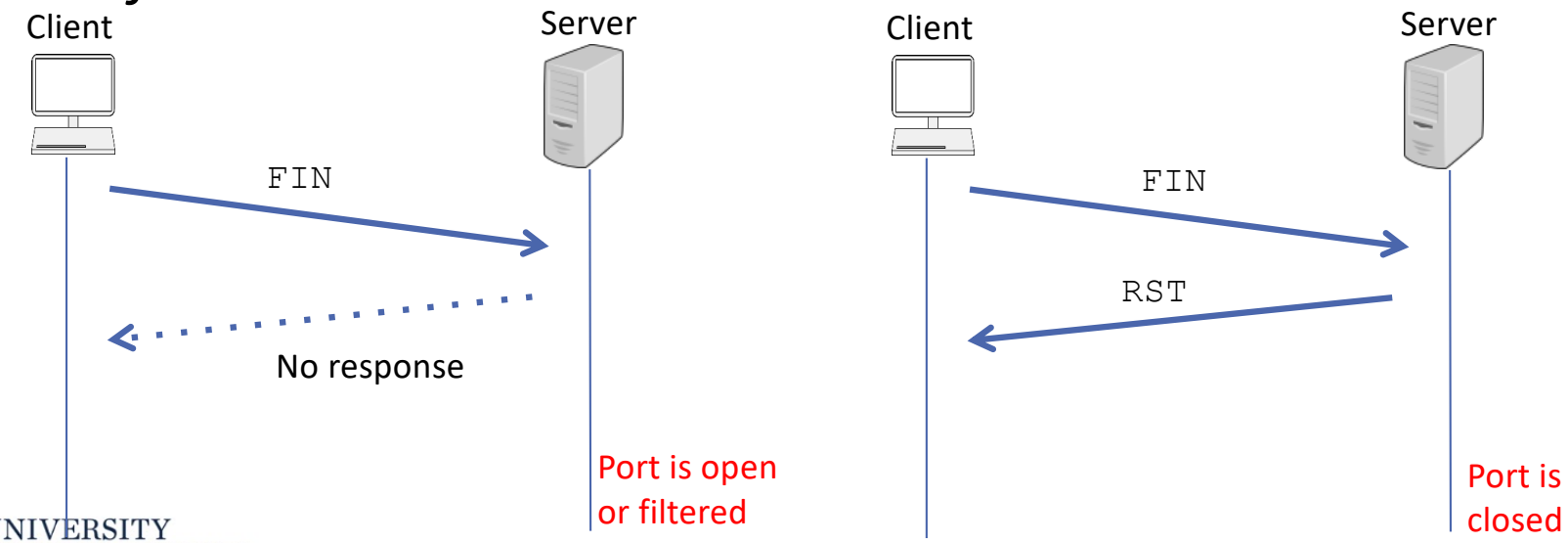
- In Xmas scan, the attacker sends a packet with PSH, FIN, URG flags (to create confusion) → If the server is not responding, the port is considered *open or filtered*.



UNIVERSITY OF WOLLONGONG AUSTRALIA

FIN Scan

- The attacker sends a packet with a FIN flag at the beginning
  → If the server is not responding, the port is considered *open or filtered*.



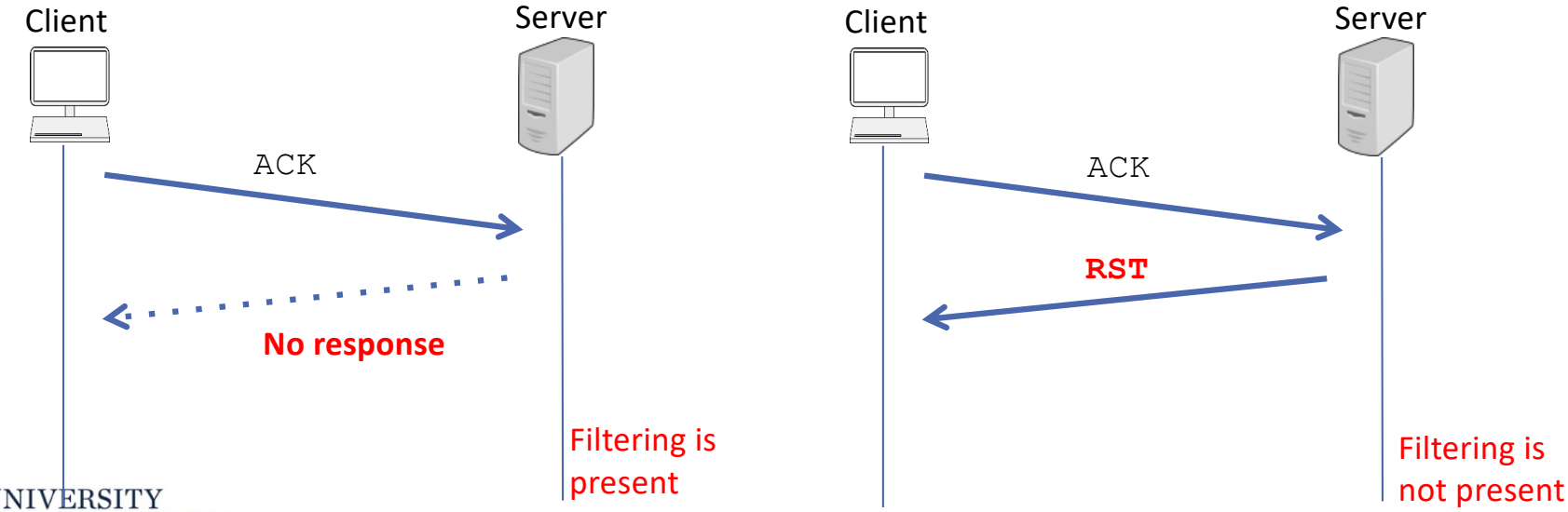
UNIVERSITY OF WOLLONGONG AUSTRALIA

Properties of Xmas and `FIN` Scans

- In fact, the two scans yield the same result.
  - ➢ *Less likely to trigger the firewall* that checks the SYN flag is set.
  - ➢ The result is not reliable and it is known to be slow sometimes.
  - ➢ Nmap commands:
    - ✓ Xmas scan: `nmap -sX -v <target IP address>`
    - ✓ FIN scan: `nmap -sF -v <target IP address>`

ACK Scan

- This scan is based on the fact that when ACK is received, an unfiltered host must respond with RST: Used to determine a port is filtered or unfiltered.



UNIVERSITY OF WOLLONGONG AUSTRALIA

ACK Scan

- Properties of ACK scan
  - The result is less reliable and sometimes slow too.
  - Nmap command:

```
nmap –sA –v  <target IP address>
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

Nmap States Summary

- `open`: There is an application accepting TCP/UDP connection.
  - Can be a result of TCP and SYN scans.
- `closed`: There is no application listening on the port.
  - Can be a result of TCP, SYN, XMAS, NULL and FIN scans.
- `filtered`: There is a packet filtering mechanism or device blocking the probe. (Nmap cannot determine whether the port is open or not.)
  - **Can be a result of ACK scan**.
- `unfiltered`: The port is accessible. (Nmap cannot determine whether the port is open or not.)
  - **Can be a result of ACK scan**.
- `open|filtered`: The port is open or filtered. (Nmap is unable to determine which one.)
  - Can be a result of XMAS, NULL and FIN scans.

UNIVERSITY OF WOLLONGONG AUSTRALIA

ARP Scanning

- ARP host recovery
  - The Address Resolution Protocol (ARP) maps system's MAC address (hardware address) to its IP address.
  - An ARP can send ARP request to every host on a subnet: If an ARP reply is received, that host is considered "live".
  - As it operates below the layers of ICMP/TCP/UDP, it can bypass firewall, the attacker needs to be located on the same local network.
  - Ex) `arp-scan 192.169.8.2 - 192.169.8.10`

ARP Scanning Example

- ARP Scanning can be visualized through Wireshark.
  - ➢ARP scan with Scapy
    - ✓`ans, unans = srp(Ether(dst="ff:ff:ff:ff:ff:ff")/ARP(pdst = ips), timeout = 2, iface = interface, inter = 0.1)` where `ips` is ip addresses such as “10.0.2.0/30” and `iface` is the network interface name such as “eth0”.

Source	Destination	Protocol	Length	Info
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.0? Tell 10.0.2.6
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.1? Tell 10.0.2.6
RealtekU_12:…	PcsCompu_22:a4:…	ARP	60	10.0.2.1 is at 52:54:00:12:35:00
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.2? Tell 10.0.2.6
RealtekU_12:…	PcsCompu_22:a4:…	ARP	60	10.0.2.2 is at 52:54:00:12:35:00
PcsCompu_22:…	Broadcast	ARP	42	Who has 10.0.2.3? Tell 10.0.2.6
PcsCompu_7f:…	PcsCompu_22:a4:…	ARP	60	10.0.2.3 is at 08:00:27:7f:9f:d0

UNIVERSITY OF WOLLONGONG AUSTRALIA

ARP Scanning Example

- ARP addresses is cached in the OS. The `arp -a` command to view and modify the ARP table entries on the local computer.
- The command can be used to display all the known connected hosts on the target's local network segment (if they have been active and in the cache).

```
$ arp -a
Net to Media Table: IPv4
Device   IP Address               Mask      Flags      Phys Addr
------ -------------------- --------------- -------- ---------------
aggr557001 pan-SharedCompute-557-router.its.uow.edu.au 255.255.255.255
00:1b:17:00:01:26
igb0   scylla.cs.uow.edu.au 255.255.255.255 SPLA     00:21:28:f1:a2:dc
igb0   pan-VirtualInfra-553-router.its.uow.edu.au 255.255.255.255          00:1b
:17:00:01:26
```

UNIVERSITY OF WOLLONGONG AUSTRALIA