ROSE-HULMAN
INSTITUTE OF TECHNOLOGY

CSSE 490
Network Security

Day 14: ICMP Wrap Up

Outline

- ICMP Recap
- Spoof Prevention in Linux
- The Smurf Attack
- Other ICMP Attacks
- The Transport Layer
- Port Numbers
- TCP v UDP

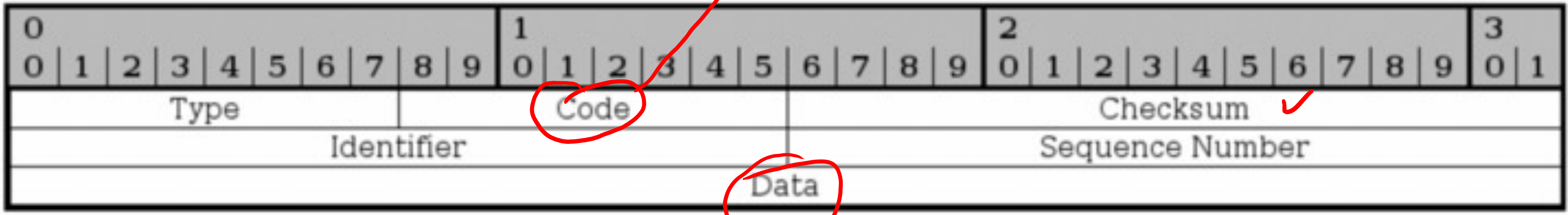
ICMP Header

① Error messages (Destination host unreachable)

② Control messages(echo, ICMP redirect, ...)

subtype

Table 1-4. Internet Control Message Protocol - Echo/Echo Reply Message

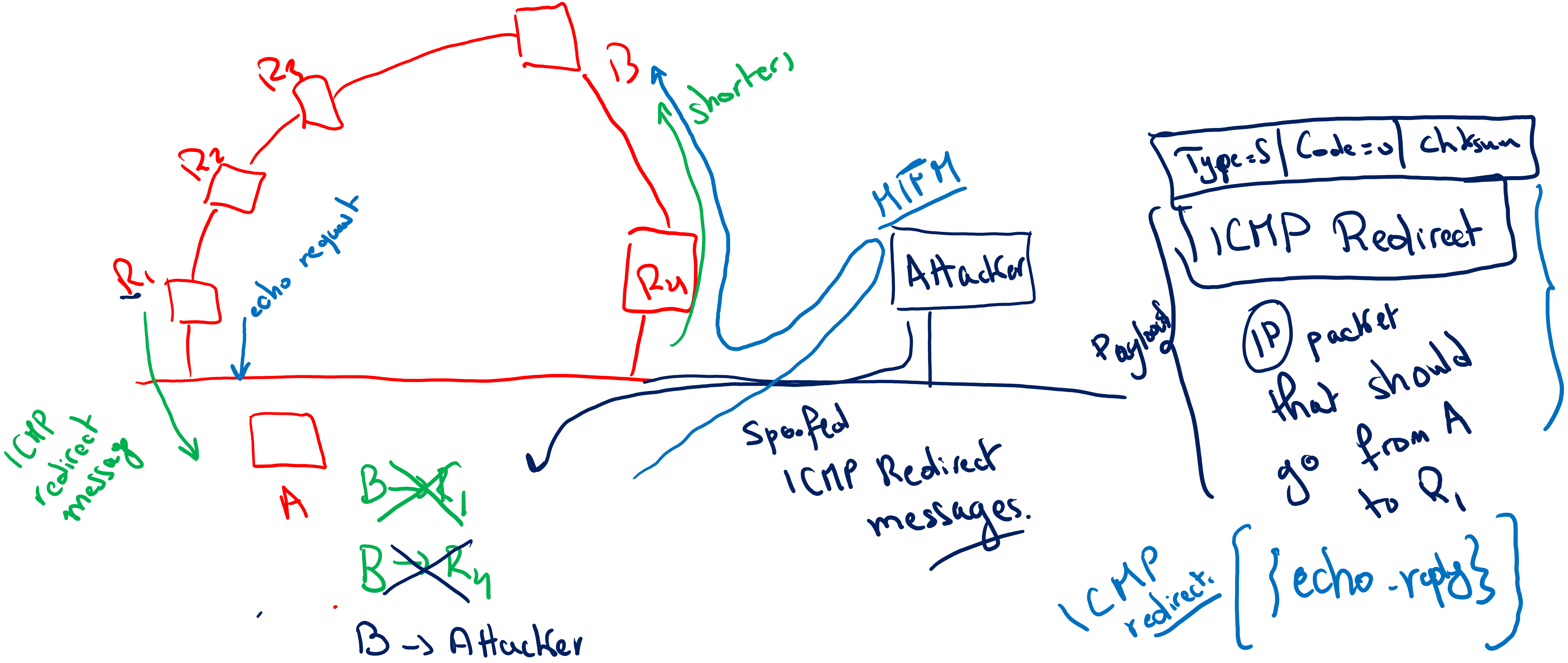


0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
Type								Code								Checksum ✓															
Identifier																Sequence Number															
Data																															

change depending on type & code.

arbitrarily large given MTU (~1500 bytes)

ICMP Redirect Attack



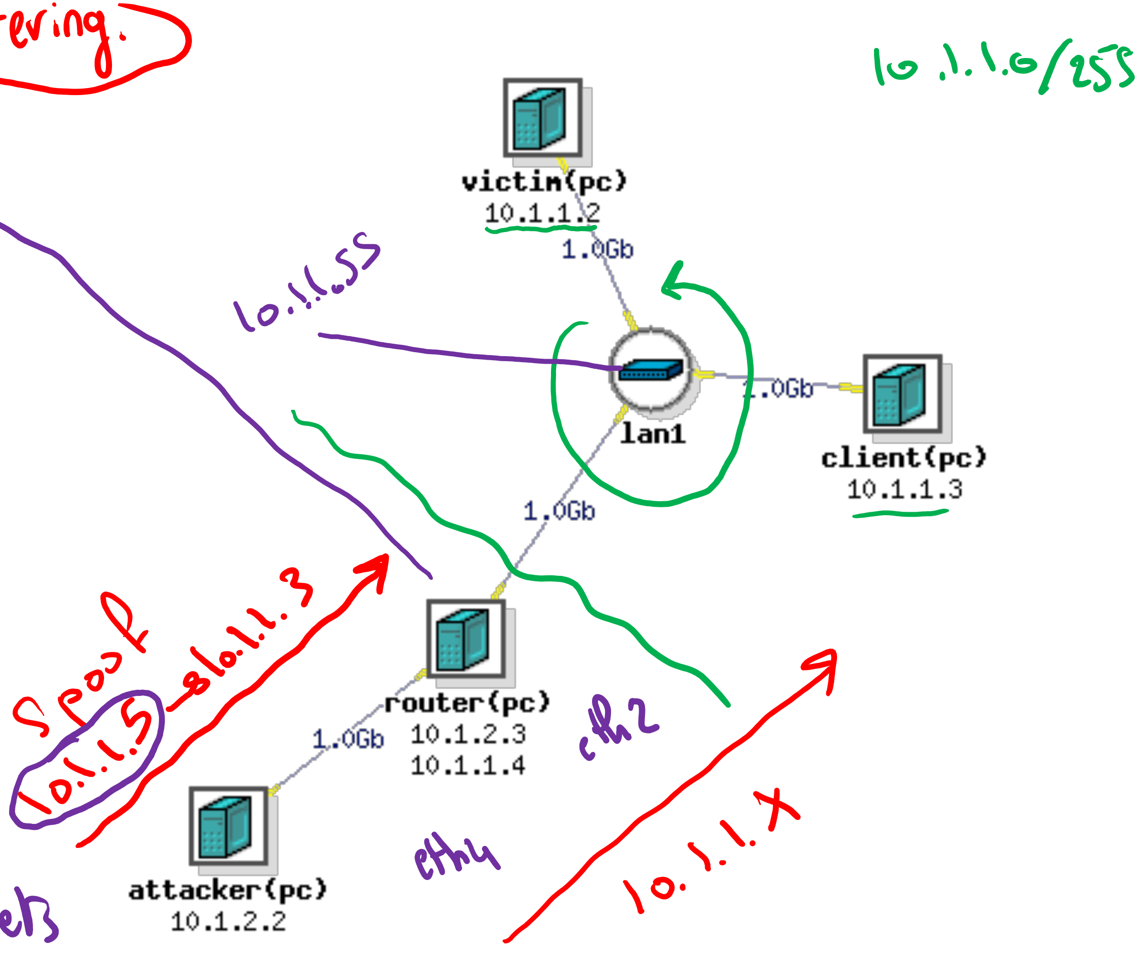
Spoof Prevention in Linux

RPF Demo

Reverse Path Filtering

Reverse lookup on 10.1.1.5

- Symmetric route i.e, it comes from the same interface
  ⇒ route traffic
- Asymmetric route
  ⇒ Drop packets

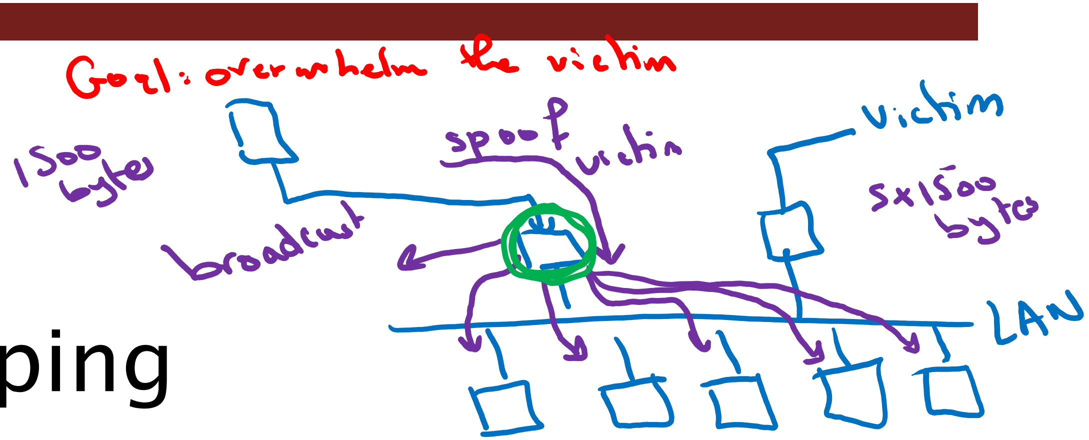


Two Questions

- ❑ Can we launch an ICMP redirect attack from the outside? No bcz of RPF

- ❑ Can you use ICMP redirect to redirect to a non-existing host? No!

Smurf Attack


Goal: overwhelm the victim

- ❑ Magnify your power using ping

- ❑ **Can you send a single packet, get multiple in response?**

Amplification attack on the victim

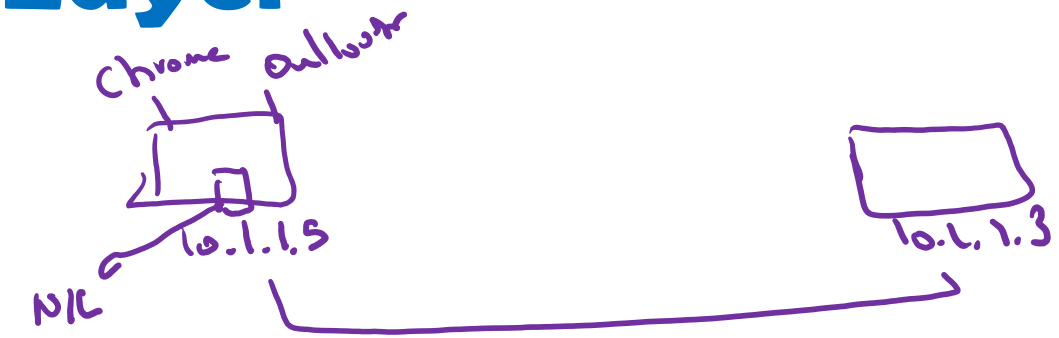
{linear amplification}

Other ICMP Attacks

- ICMP Flooding for DDoS
- Reconnaissance

Transport vs Network Layer

- Why is IP not enough?



- Recall that IP provide end-to-end routing and forwarding

- Source computer to destination computer, but what about applications?

Why IP is not enough?

- ❑ No delivery to the application at L3
- ❑ No reliability
- ❑ No encryption
- ❑ …

kernel
replies to
ICMP

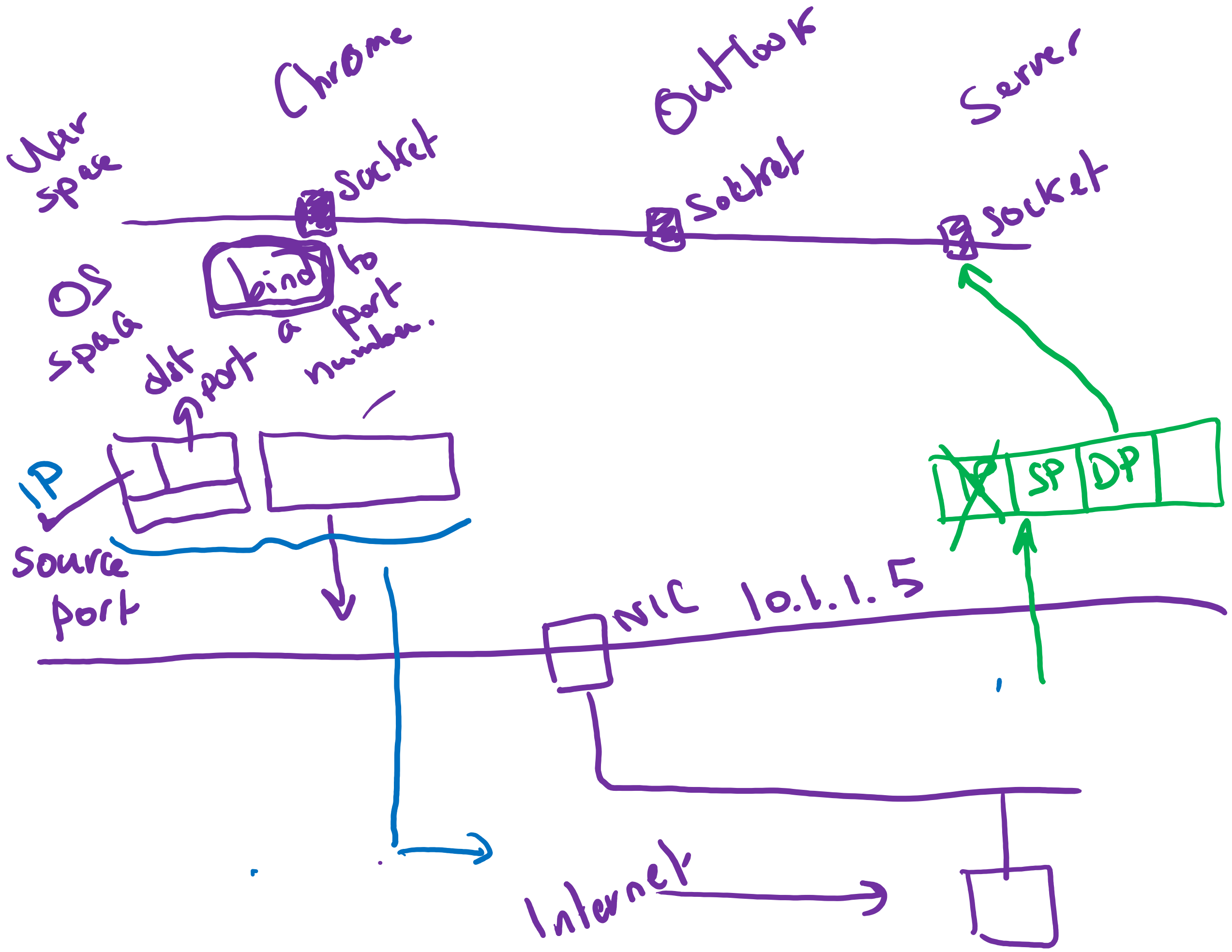
The Transport Layer

- ❑ How would you know which application to send traffic to?

- ❑ E.g., name when sending to a household!

- ❑ **Port numbers**

Port Numbers



Port Numbers – cont'd

- 16 bits value
- 0 – 1023: Well-known ports
  - Need sudo privileges to bind to these ports, why?
  - Http runs on port 80, https on 443, ssh on 22, etc…
- 1024 – 49151: **Lesser well-know ports**
  - SQL Server (1433)
- 49152 – 65535: **Private ports**

Transport Layer Protocols: TCP vs UDP

	TCP	UDP
Connection		
Packet Boundary		
Reliability		
Ordering		
Speed		
Broadcast		