WA5

- Get into groups of 2-3 (or 4)
- Help each other go through the steps in the Canvas announcement
- **When done: PollEv.com/kakiryan**

WA5: Get Ready





Can we make a reply look like it came from someone else?

- Open the starter folder containing compose.yaml.
- Launch Docker Desktop; open two terminal tabs.

```
docker compose up -d --build
docker compose ps
```

Checkpoint: victim, attacker, and target are all running.

Use only the supplied Docker lab network. Raise your hand if setup is stuck.

Checkpoint 1: Watch the Requests

Terminal 1 — start the capture:

```
docker compose exec attacker tcpdump -n -i any icmp
```

Terminal 2 — send three pings:

```
docker compose exec victim ping -c 3 -W 1 10.34.50.20
```

Checkpoint: requests appear, but no replies arrive.

Why can the attacker see the requests?
Why doesn't the real target reply? → WA5, question 1

Checkpoint 2: Build a Reply



Open student/sniff_spoof.py and complete the three TODOs.

- Which source and destination IPs should the reply use?
- Which ICMP ID and sequence number should it carry?
- What should happen to the request's payload?

Stop tcpdump (Ctrl-C). In Terminal 1, run:

```
docker compose exec attacker python /lab/sniff_spoof.py
```

Wait for "Listening…", then repeat the ping in Terminal 2.
Checkpoint: ping accepts replies claiming to be from 10.34.50.20.

soln



```
reply = (
        IP(src=TARGET_IP, dst=VICTIM_IP)
        / ICMP(type=0, id=request[ICMP].id, seq=request[ICMP].seq)
        / Raw(load=bytes(request[ICMP].payload))
    )
```

Checkpoint 3: Inspect the Evidence

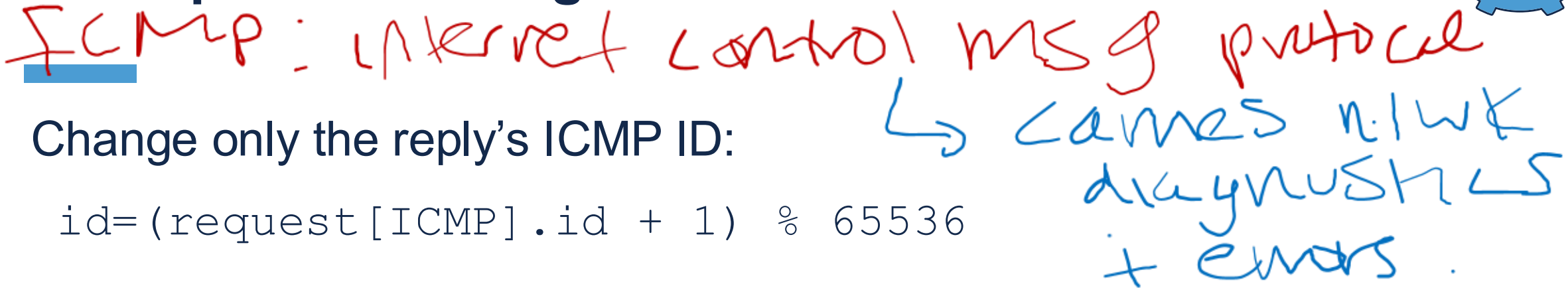
Open captures/icmp_exchange.pcap in Wireshark.

```
Display filter: icmp
```

- Find one echo request and its matching reply.
- Compare addresses, type, ID, sequence, and payload.
- Which fields changed? Which stayed the same?

What source IP does the reply claim?
How do we know who actually made it? → WA5, question 2

Checkpoint 4: Change One Field



Change only the reply's ICMP ID:

```
id=(request[ICMP].id + 1) % 65536
```

- Predict: will ping accept the replies?
- Restart the script, then repeat the ping.
- Explain the result. Does a matching ID prove identity?

Finish WA5 questions 3–4: is a source IP authentication?

When finished: docker compose down