# CAM TABLE OVERFLOW

# MIKE HAM

# 10,000' VIEW

- Disclosure of sensitive information, disruption
  - MITM (sort of)
- Also called MAC table overflow (not *technically* correct)
  - Takes advantage of layer 2 (Data Link) weaknesses
  - CAM = content addressable memory
- High severity and High exploit success/likeliness
- Last resort or very specific tests

# WHY

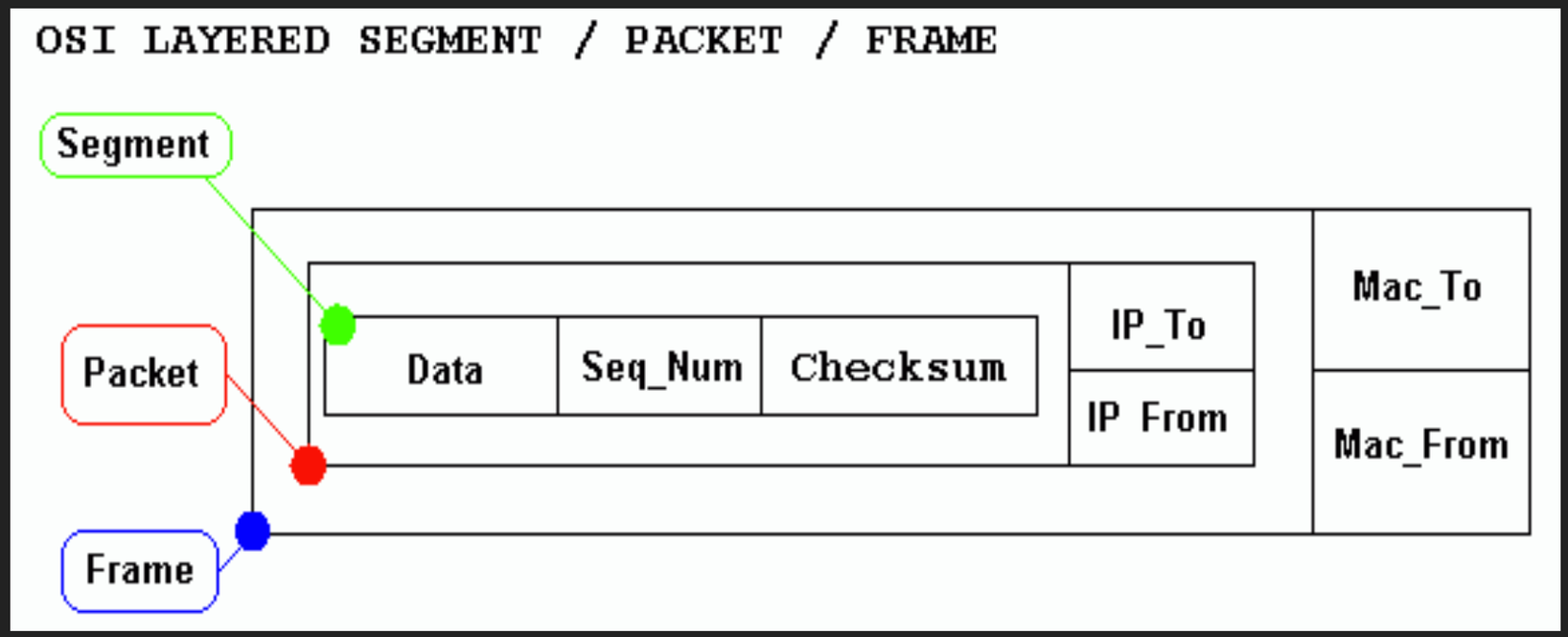
- This attack is applicable in any network that has a switch
- Simplicity is beautiful
- Frankly, I'm a geek for attacking the network side of things and find this type of problem pleasing
- Quite effective
  - lol @ ROP, EMET, endpoint security, patches…you have no power here
  - Clients shouldn't see it as they do with ARP poisoning

# WHAT YOU SHOULD ALREADY KNOW

- Hubs are old and terrible (layer 1), physically repeat signal
  - Everyone sees everything
- Switches operate on layer 2, intelligently separate non-broadcast traffic
  - If it's not for me, I should never see it unless you send a broadcast
  - We only care about frames here, not so much packets
- Remember, routers break up broadcast domains (layer 3)

# ETHERNET FRAME

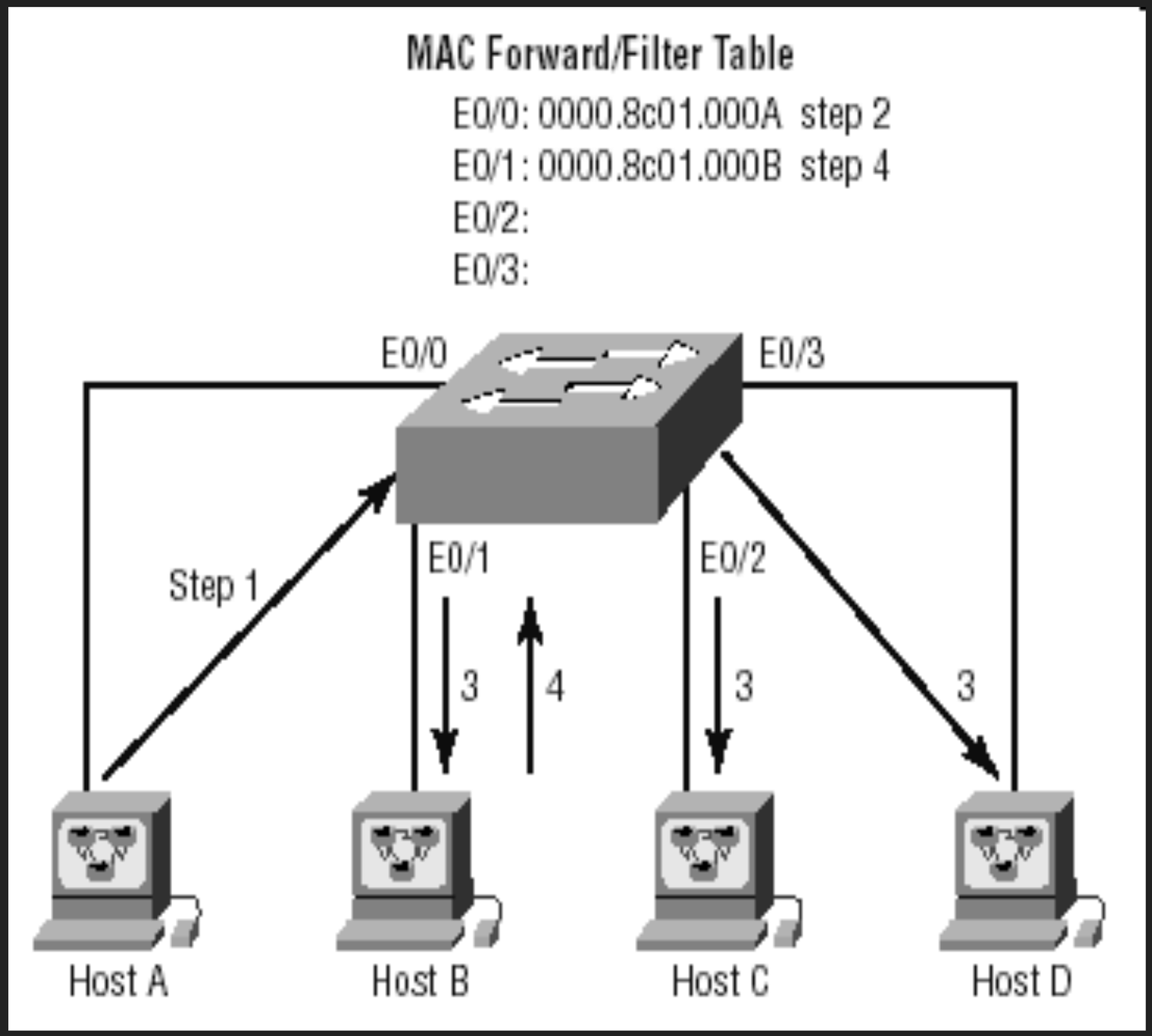
- MAC_TO
- MAC_FROM
- Ignore the rest



# ADDRESS LEARNING

- MAC forward/filter table is empty on boot
- When device transmits and interface receives a frame, switch puts frames source address in MAC table
- Floods the network with the frame except on source port
- If device answers, switch will place that MAC in the database as well (point-to-point)

# ADDRESS LEARNING EXAMPLE



# PROBLEM

- Switches have a finite amount of memory
- The CAM table is allocated a portion of that memory
- When the CAM table fills, the switch can't take new requests and ends up dropping them, that's bad (timeout)
- Switches fail in one of two ways:
  - Closed - everybody is down
  - Open - turns itself back into a hub

```
Ping statistics for 172.16.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\mjham>
```

```
root@kali:~# dsniff -i eth0
dsniff: listening on eth0
root@kali:~#
```

# DEFENSE

- It’s a flaw in the protocol itself
  - Not practical to overhaul layer 2 at the moment, we’re pretty well invested in it
- Cisco recommendation: Port security
  - Dynamically (sticky) or statically learn the MAC of devices plugged in
- Extra VLANs to segment traffic, you should have this in your network already