YERSINIA

MIKE HAM

ANOTHER TOOL?

- For one, it’s fun :)
- The big picture of working towards dissertation is that I plan to do something related to BGP and IPv6 insecurities
- Much of what we built the newer standards on reflects small tweaks in the old stuff, leaving problems behind
- These tools are good for a pen tester to know about and understand how to use
    - Also get’s me thinking about methods of compromise or mitigations that may help me write my dissertation

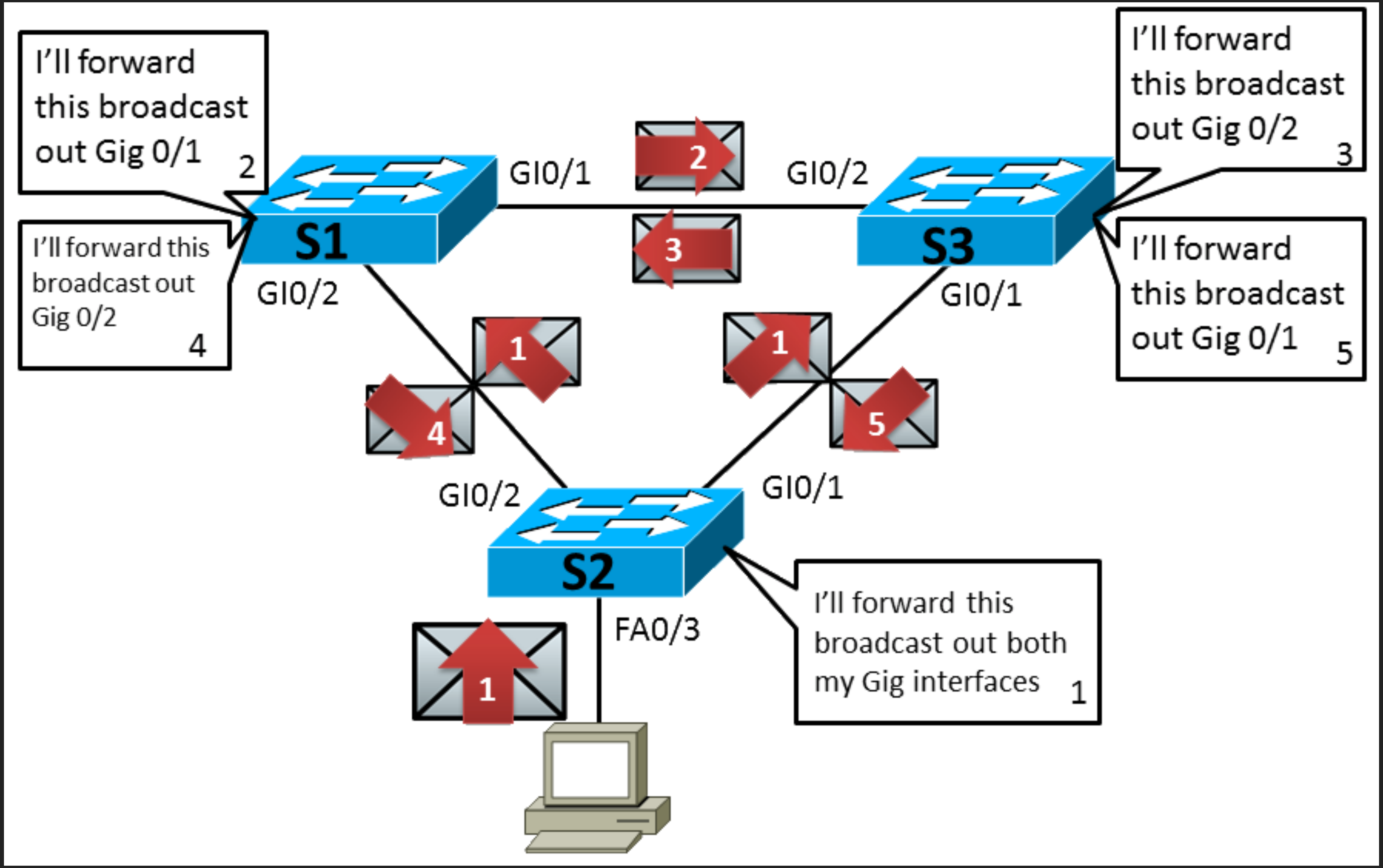
LAYER 2, ROUND 2

- As you know, there's tons of problems in layer 2 of OSI
- ARP, Spanning Tree (STP), Cisco Discovery (CDP), 802.1X, etc. have no auth. or people rarely configure it
- The end result is complete pwnage from a network standpoint in availability and confidentiality
- Same as before, this stuff is often turned on out of the box, configured out of necessity, and the users are blind to it

SPANNING TREE PROTOCOL (STP)

- In a switched network, all ports are typically on the same broadcast domain
  - When one host sends out a broadcast, every <u>other</u> port forwards it on (it'll never go back out the incoming port)
- STP helps prevent broadcast storms in a redundantly switched network
- If a broadcast storm is introduced, you effectively will get a DoS type situation…users don't like this

BROADCAST STORM



I'll forward this broadcast out Gig 0/1 2

I'll forward this broadcast out Gig 0/2 4

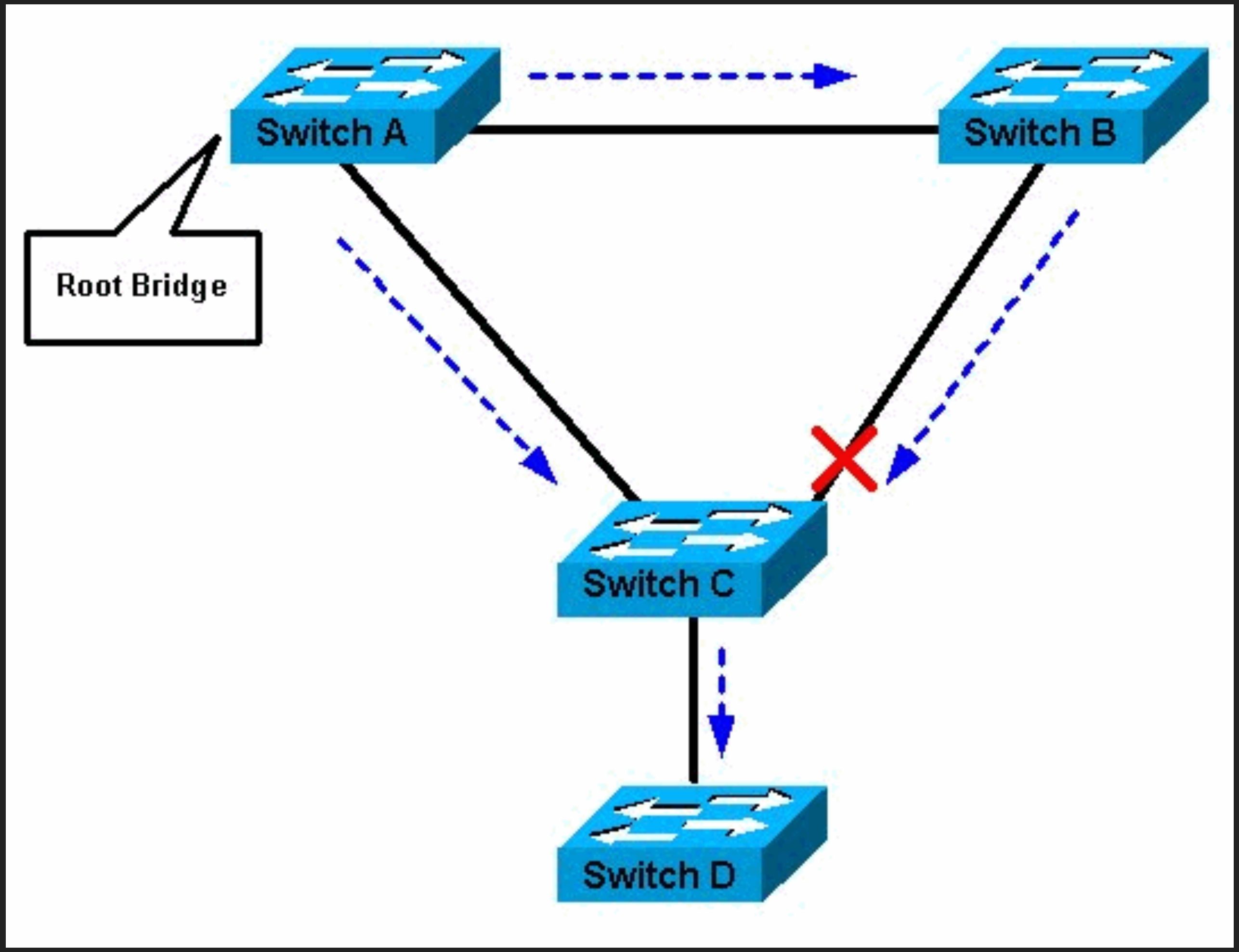
I'll forward this broadcast out Gig 0/2 3

I'll forward this broadcast out Gig 0/1 5

I'll forward this broadcast out both my Gig interfaces 1

STP

- Root Bridge knows about all of the network links
- Intelligently shut down links that will allow for a loop (BPDU packets)
- Priority + MAC



TAKING OVER THE ROOT BRIDGE

- This is super disruptive, but legit (probably don’t do this on a penetration test)
- Yersinia can send BPDUs every 2 seconds
  - LAN will take them at face value
  - STP is too trusty, stateless, poor auth. support
- Same priority + lower MAC = new root bridge

DEMO

WHERE DO WE GO FROM HERE?

- Well, you're root now, so send BPDUs to shut down all links and nobody can get online
- Give the root back to the original and take it again
  - Rinse and repeat, consumes lots of CPU, eventual DoS