WEBER STATE UNIVERSITY

Wireshark: Threat Detection

Kyle Feuz
School of Computing

Introduction

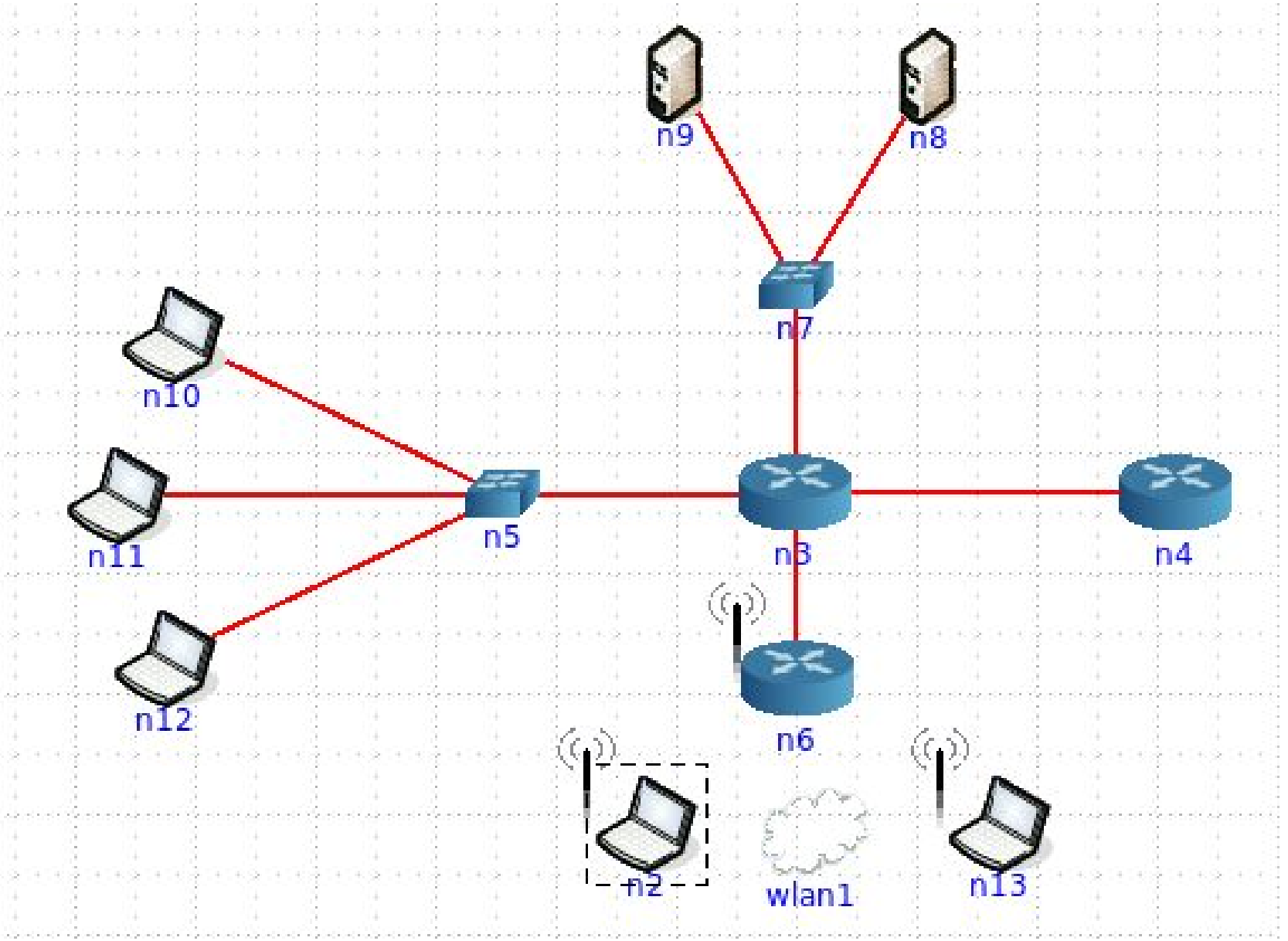
- Download Wireshark and capture files
  - https://www.wireshark.org/download.html
  - http://icarus.cs.weber.edu/~kfeuz/downloads/saintcon2017_captures.zip
- Know the law (and company policy)
- Skills needed and skills covered

Outline

- ~~Introduction~~
- Quick Review
- Advanced sniffing
- Having a baseline
- Network Reconnaissance
- ARP/IP spoofing
- Recent malware sightings

Live Demo/Practice

- Create a new profile for Demo
- Create a new profile for NetworkRecon
- Create a new profile for Spoofing Attacks


n9
n8
n7
n10
n11
n5
n3
n4
n12
n6
n2
wlan1
n13

SSL Decryption

- Private key
- Symmetric key (SSLKEYLOGFILE)
- SSL Proxy (MITM)

Live Demo/Practice

- Files
  - ssl_saintcon
  - ssl_saintcon_key

  - ssl_weber
  - ssl_weber_key

Merge multiple files

- File -> Merge
- Drag-and-Drop
- Mergecap

Live Demo/Practice

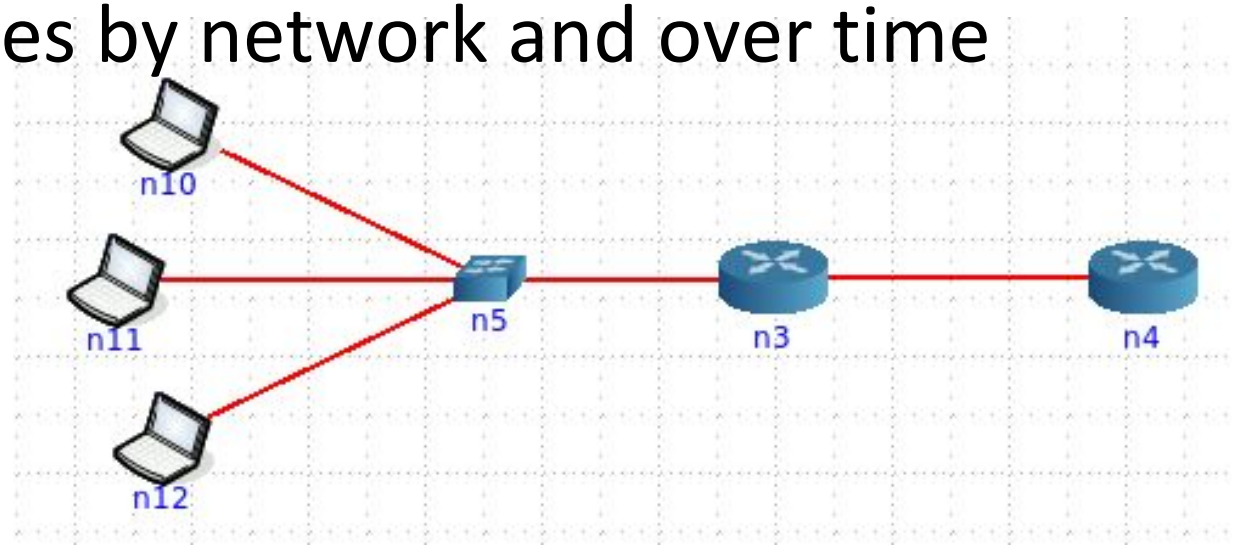
- Merge the files by appending
  - baseline.pcapng
  - double_time.pcapng
- Merge the capture files by timestamp
  - NAT_front.pcapng
  - NAT_back.pcapng

Outline

- ~~Introduction~~
- ~~Quick Review~~
- ~~Advanced sniffing~~
- Having a baseline
- Network Reconnaissance
- ARP/IP spoofing
- Recent malware sightings

Baselining

- What does “normal” look like
- Protocols used and percentage of traffic
- Common hosts and percentage of traffic
- Varies by network and over time



Live Demo/Practice

- Compare
  - baseline.pcapng
  - double_time.pcapng

Outline

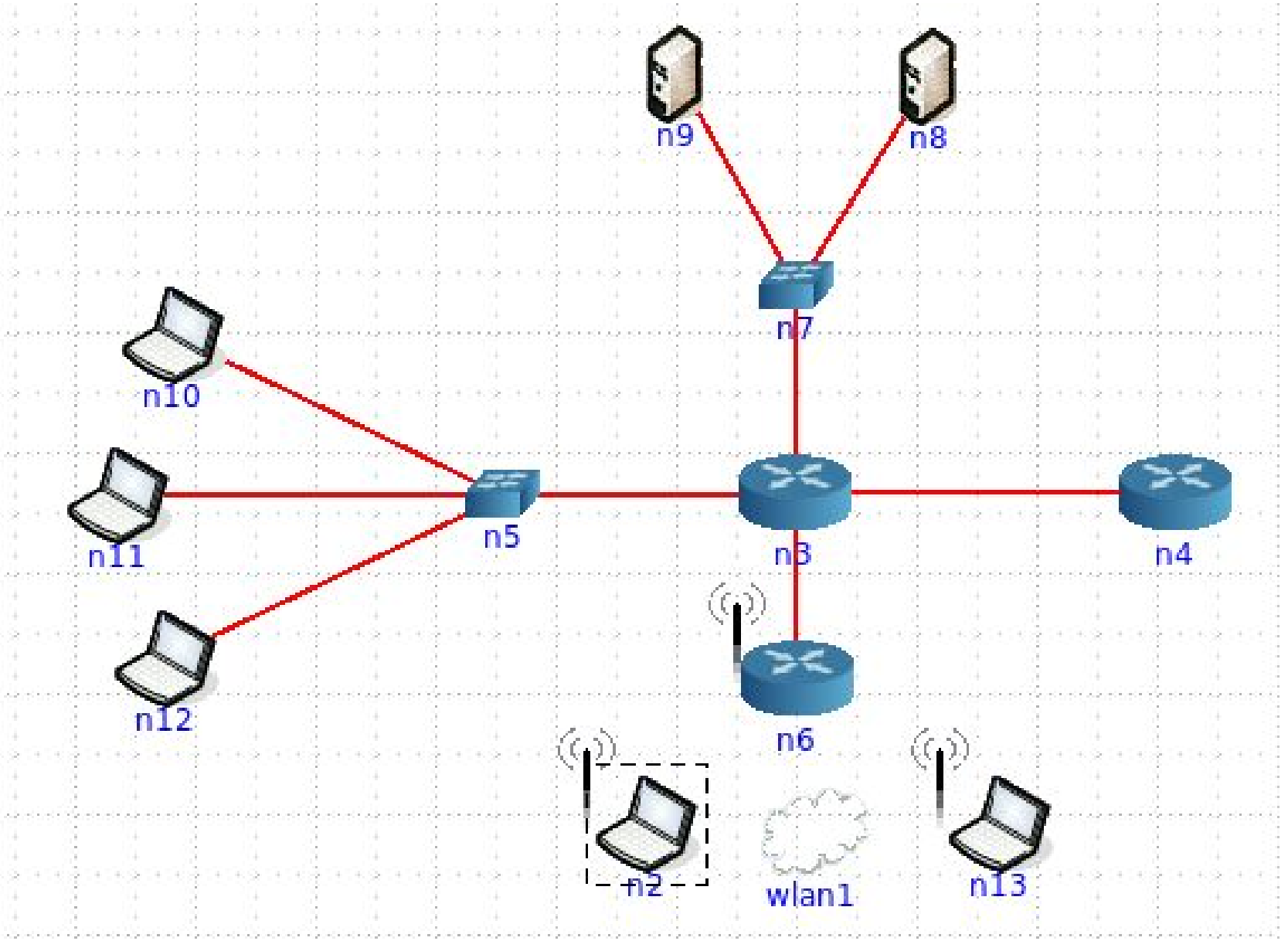
- ~~Introduction~~
- ~~Quick Review~~
- ~~Advanced sniffing~~
- ~~Having a baseline~~
- Network Reconnaissance
- ARP/IP spoofing
- Recent malware sightings

Network Reconnaissance

- Host Scanning
- Port Scanning
- OS Detection

Host Scanning

- DNS
- ARP
- ICMP
- TCP/UDP


n9
n8
n7
n10
n11
n5
n3
n4
n12
n6
n2
wlan1
n13

Live Demo/Practice

- Create coloring rules and filters
- Files
  - nmap_sL*
  - nmap_sn*
  - nmap_external_*

Port Scanning

- Half-open
- Full-connect
- Null scan, Xmas, FIN, ACK scans

Protocol	Port		Protocol	Port
FTP	21		DNS	53
SSH	22		DHCP	67,68
Telnet	23		SNMP	161,162
SMTP	25		NetBIOS	137,139
HTTP	80			
HTTPS	443			

Live Demo/Practice

- Create coloring rules and filters
  - nmap_half*
  - nmap_full*
  - nmap_null*
  - nmap_xmas*
  - nmap_fin*
  - nmap_ack*
  - nmap_udp*

OS Detection

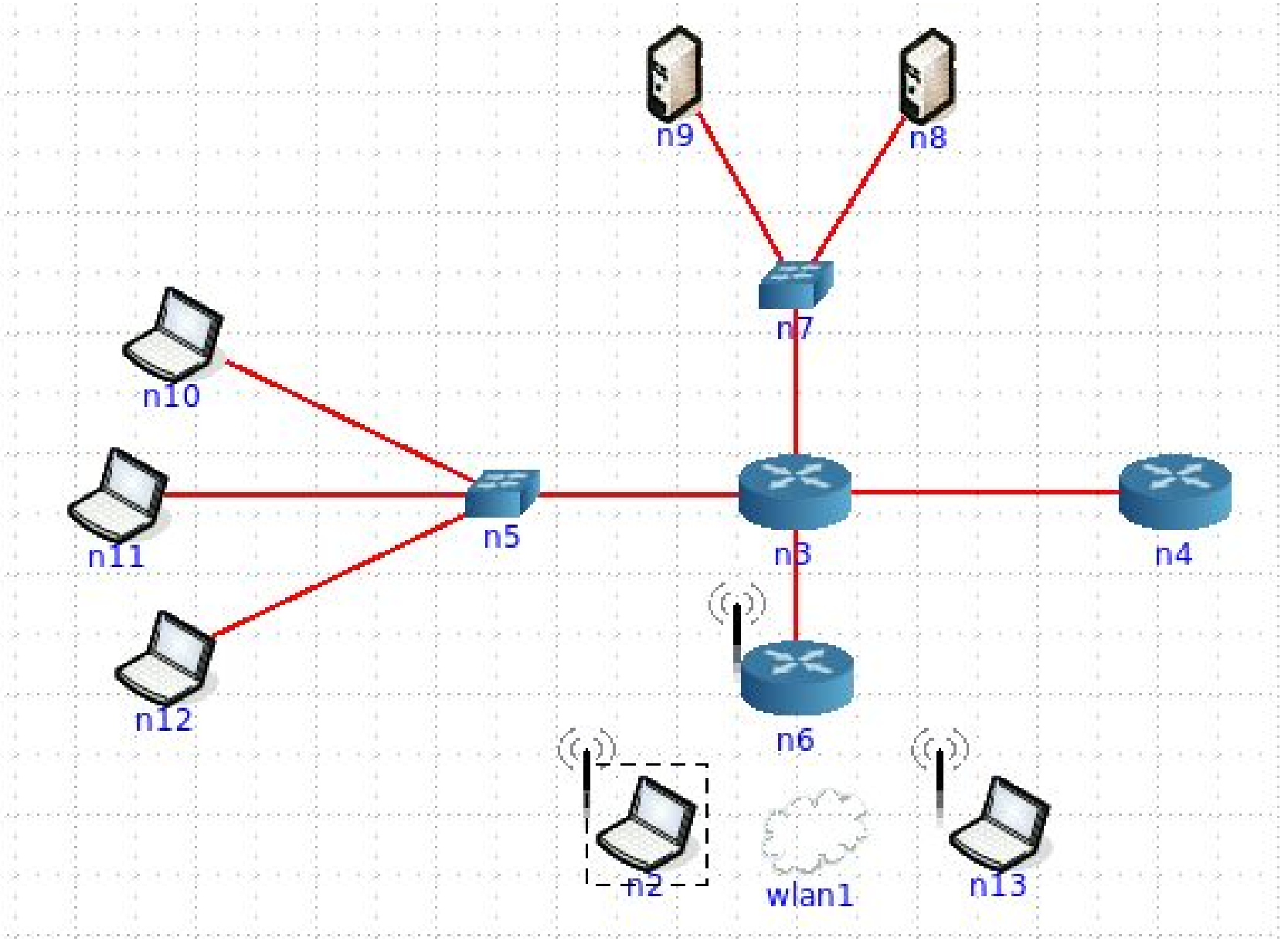
- OS respond differently to different packets
- ICMP type 8 no payload
- ICMP type 8 unusual code (i.e. non-zero)
- ICMP type 13, 15, 17
- TCP with unusual flag/option settings

Live Demo/Practice

- Create coloring rules and filters
  - nmap_os*

Others

- Traceroute
- Zombie scan
- IP Protocol scans


n9
n8
n7
n10
n11
n5
n3
n4
n12
n6
n2
wlan1
n13

Live Demo/Practice

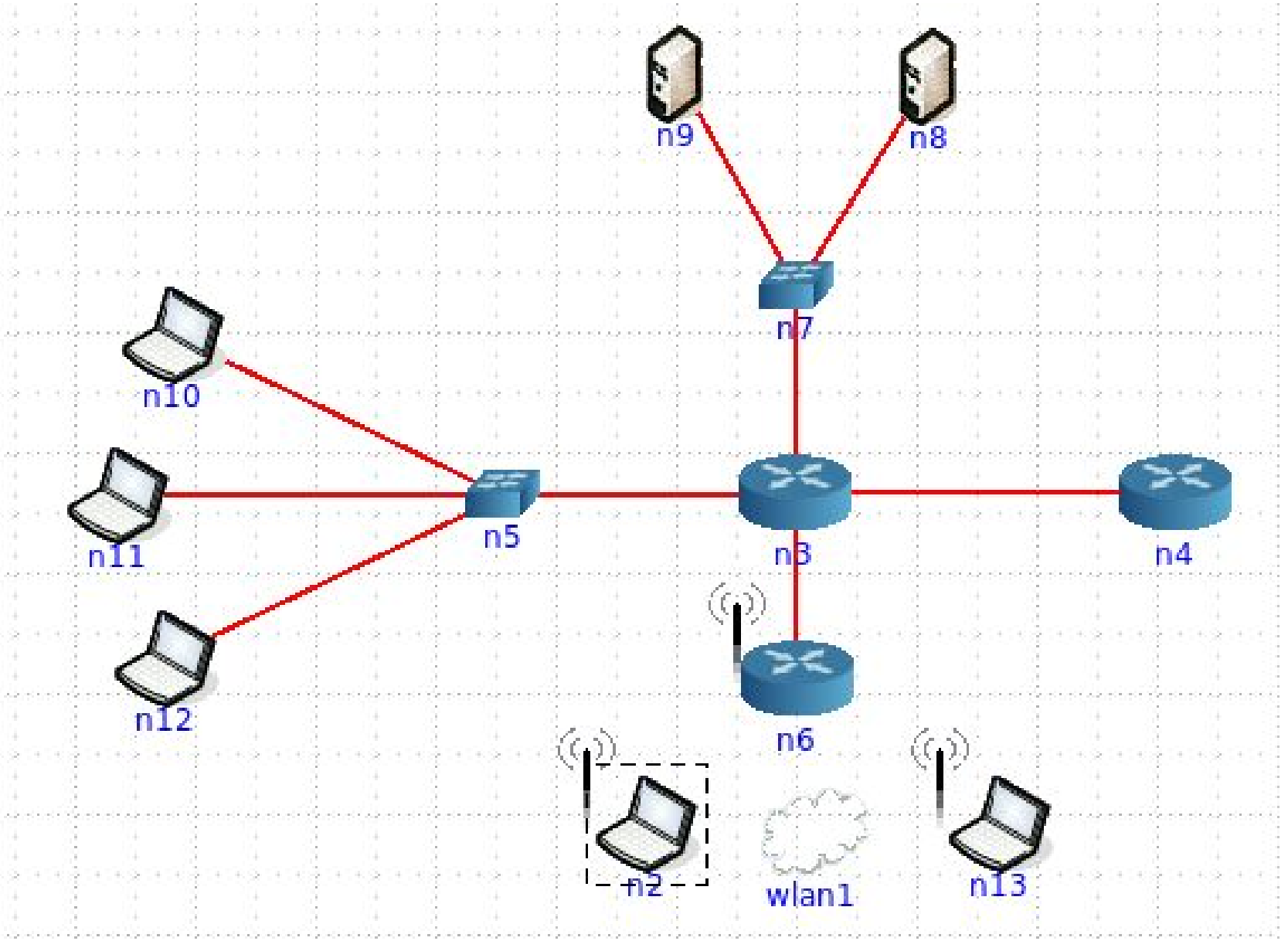
- Create Coloring Rules and Filters
  - nmap_idle*
  - nmap_sO*
  - traceroute*

Outline

- ~~Introduction~~
- ~~Quick Review~~
- ~~Advanced sniffing~~
- ~~Having a baseline~~
- ~~Network Reconnaissance~~
- ARP/IP spoofing
- Recent malware sightings

ARP Spoofing

- Hide true source
- DOS
- MITM
- Force “Hub” behavior


n9
n8
n7
n10
n11
n5
n3
n4
n12
n6
n2
wlan1
n13

Live Demo/Practice

- Create coloring rules and filters
  - nmap_spoofed_mac
  - macof_flood
  - arp_poison

IP Spoofing

- Hide true source
- DOS

Live Demo/Practice

- Create coloring rules and filters
  - nmap_idle
  - nmap_spoofed_ip

Outline

- ~~Introduction~~
- ~~Quick Review~~
- ~~Advanced sniffing~~
- ~~Having a baseline~~
- ~~Network Reconnaissance~~
- ~~ARP/IP spoofing~~
- Recent malware sightings

Heartbleed

- Malformed SSL Heartbeat message
- Payload length invalid

Live Demo/Practice

- Create coloring rules and capture filters
  - heartbleed_encrypted
  - heartbleed_decrypted

Mirai botnet

- Use default login credentials
- Scan Internet for vulnerable hosts

Live Demo/Practice

- Create coloring rules and capture filters
  - mirai

WannaCry

- SMBv1 implemenation bug
- Network Signature

  SMBv1

  port 445

  strange DNS requests

Live Demo/Practice

- Create coloring rules and capture filters
  - wannacry

Live Demo/Practice

- Sharkfest 13 Challenges
  - 1 challengescan
  - 2 challengewhatsup
  - 4 challengeattack
  - 7 challengeboyscout

Outline

- ~~Introduction~~
- ~~Quick Review~~
- ~~Advanced sniffing~~
- ~~Having a baseline~~
- ~~Network Reconnaissance~~
- ~~ARP/IP spoofing~~
- ~~Recent malware sightings~~

Thank You!