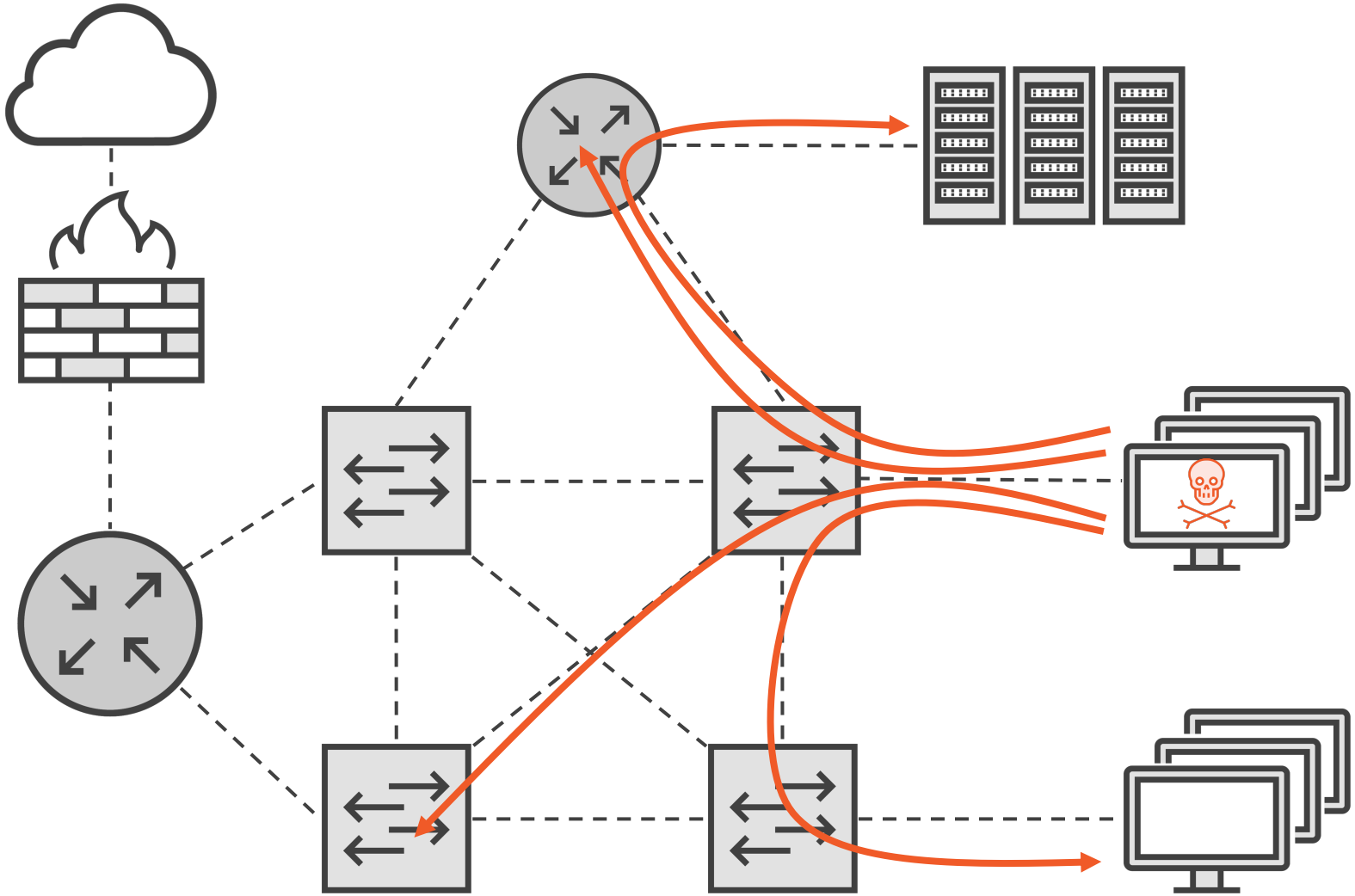
Analyzing Port Scans and Enumeration Methods

Module Overview

- Analyzing Host and Network Discovery
- Detecting Nmap/Masscan Behaviors:
  - TCP SYN Scans, Connect Scans
- Detecting OS Fingerprinting
- HTTP Path Enumeration

Most attackers try to evade detection, may adjust enumeration methods

Network/Host Discovery

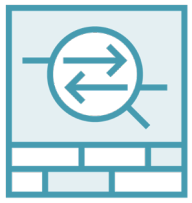


Protocols/Patterns to Watch For

ARP Scans

ICMP Ping Sweeps

TCP SYNs to common ports

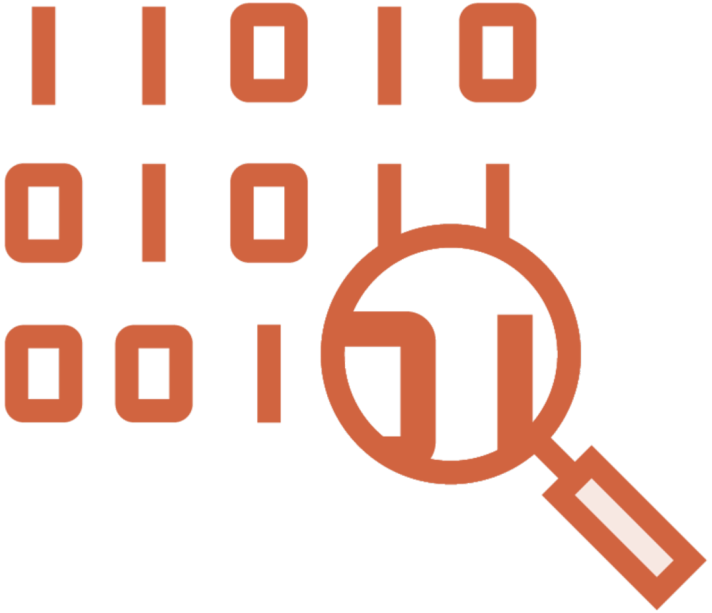


UDP Scans

A Note About Our Sample Labs

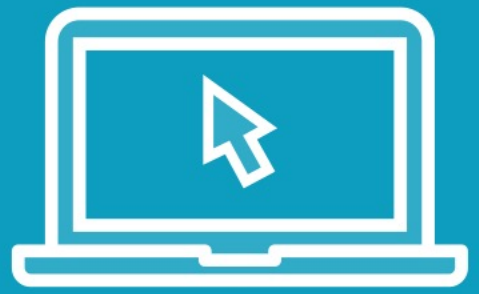
Virtual Lab Environment

Enumeration Tools/Real Malware



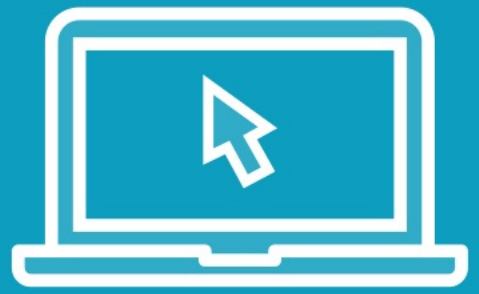
Collect Traffic From Your Own Network!

Demo



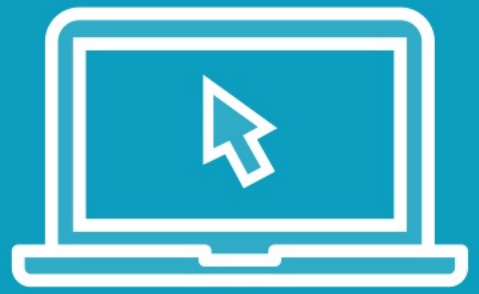
Lab 1 – Detecting Network Discovery Scanning with Wireshark

Demo



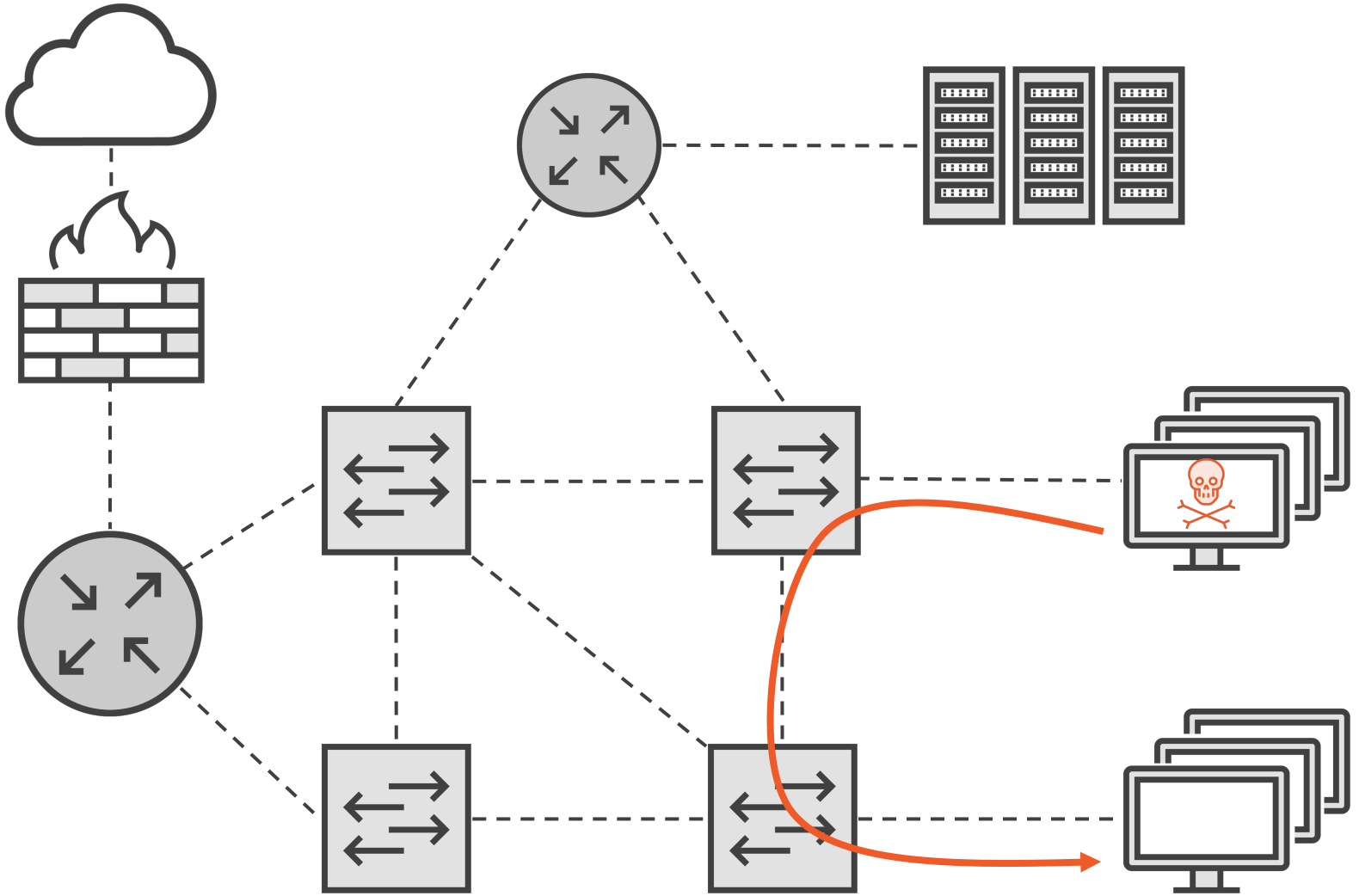
Lab 2 – Detecting Port Scans with Wireshark

Demo



Lab 3 – Threat Hunting: Analyzing a Real Network and Port Scan

Active OS Fingerprinting



Windows 10/Linux/Ubuntu?

Protocols/Patterns to Watch For

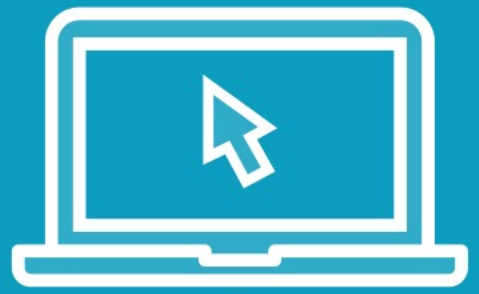
Host to Host Traffic

Unusual TTL Patterns

Duplicate Sequence Numbers in SYNs

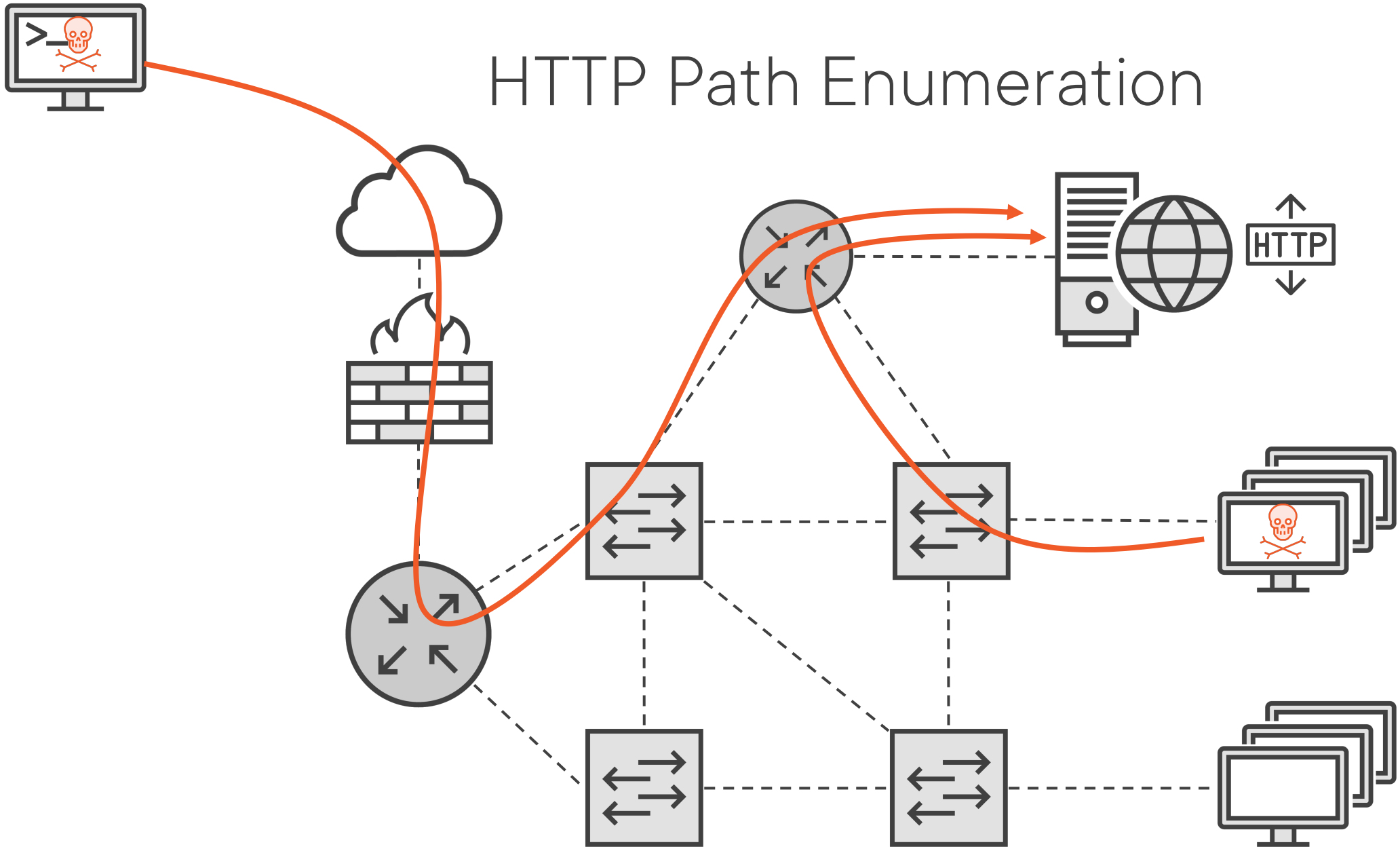
Strange Flags/Few TCP Options

Demo



Lab 4 – Detecting OS Fingerprinting

HTTP Path Enumeration



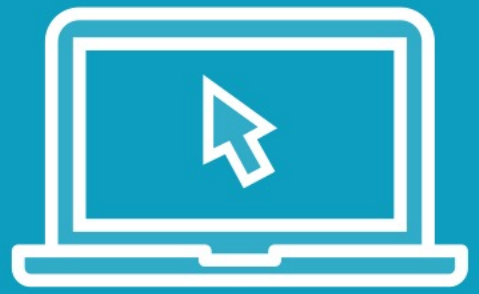
Protocols/Patterns to Watch For

Communications Over TCP Port 80

“Dictionary” Directory Queries

Lots of “404 Not Found” Replies

Demo



Lab 5 – Analyzing Web Server Enumeration

Module Overview

Analyzing Host and Network Discovery

Detecting Nmap/Masscan Behaviors:

- TCP SYN Scans, Connect Scans, Xmas scans, and Null Scans

Detecting OS Fingerprinting

HTTP Path Enumeration