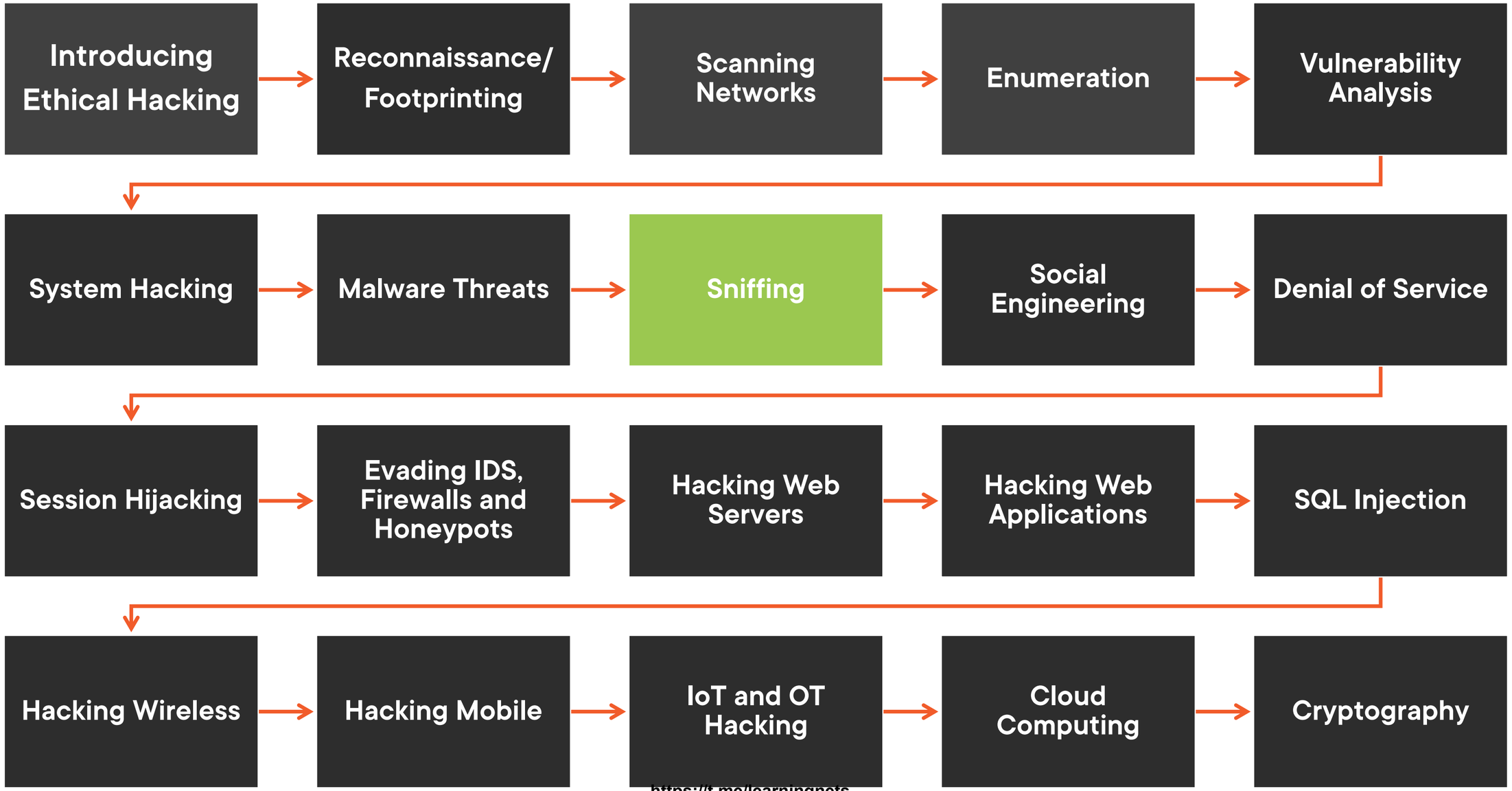
Ethical Hacking: Sniffing

Examining Sniffing Concepts

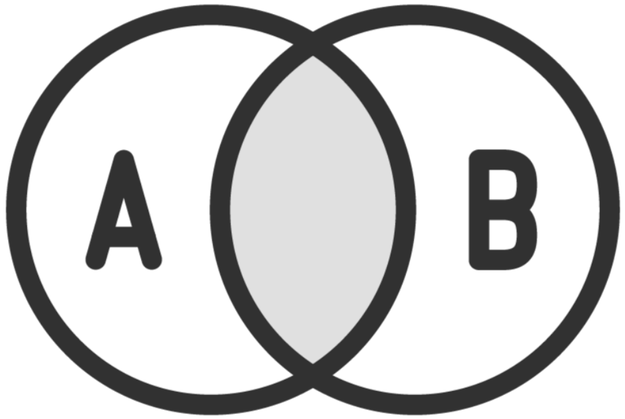
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

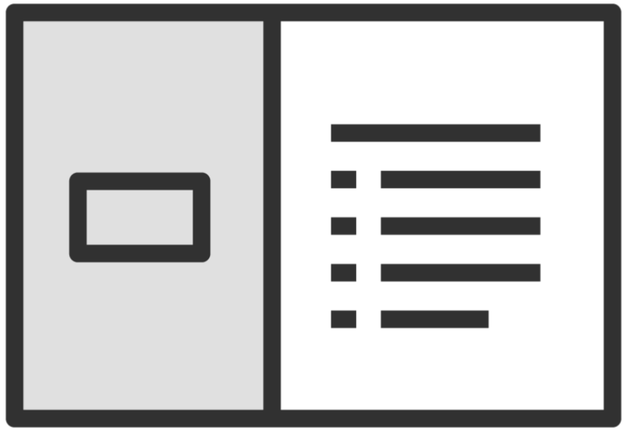
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

Ethical Hacking Series

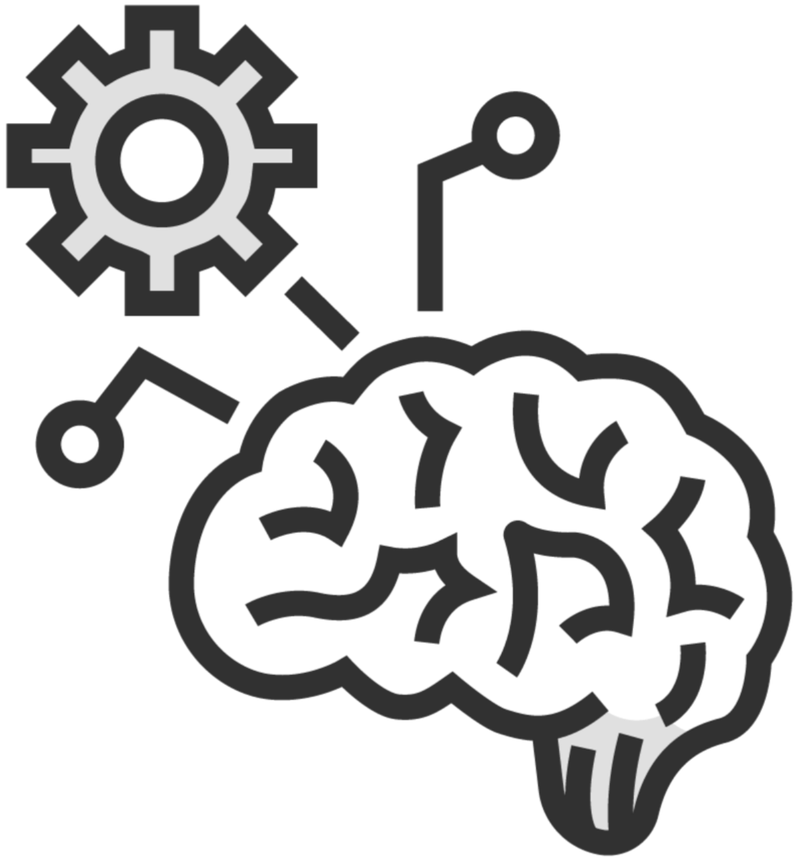


The Method behind My Madness





The Method behind My Madness

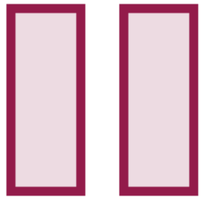


CEH Exam Study Tips

Dale's Study Tips

Study space

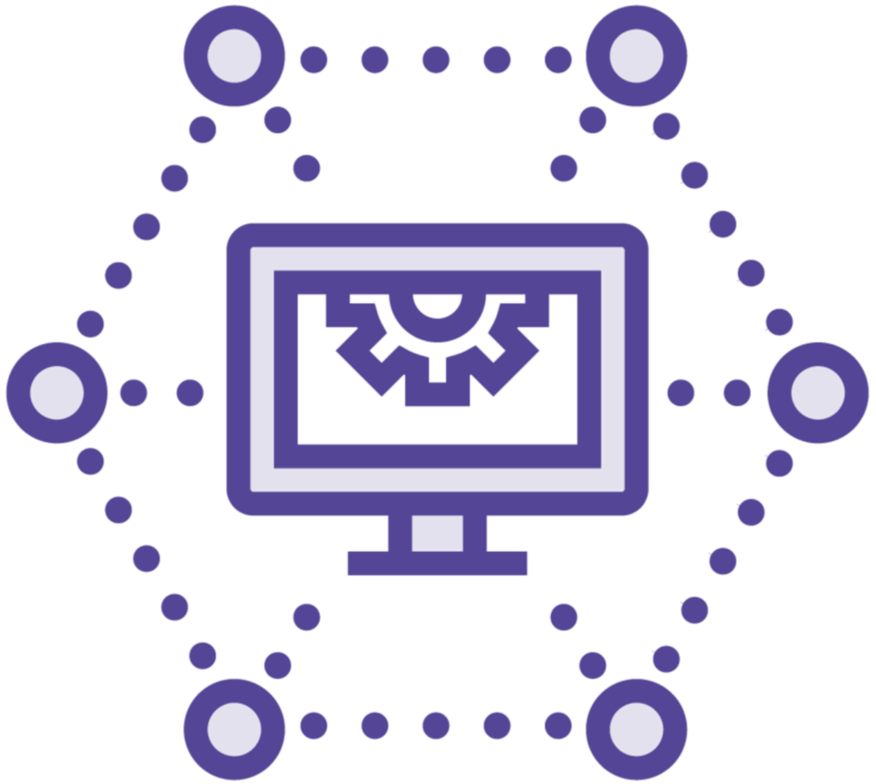
Take notes



Pause, think, repeat

Be kind and rewind

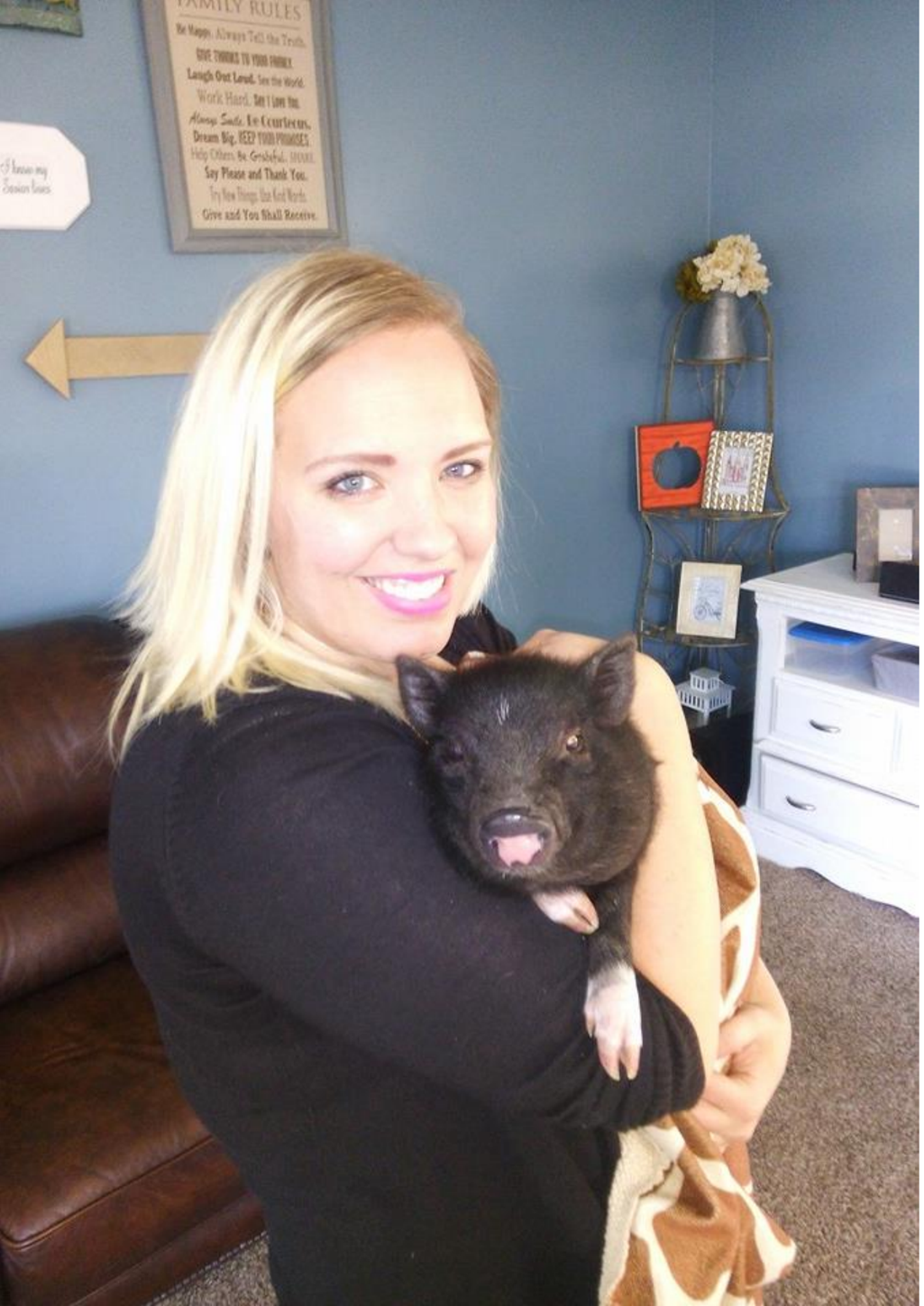
Dale's Study Tips



Continually learning is the key to success!

True genius resides in the capacity for evaluation of uncertain, hazardous, and conflicting information

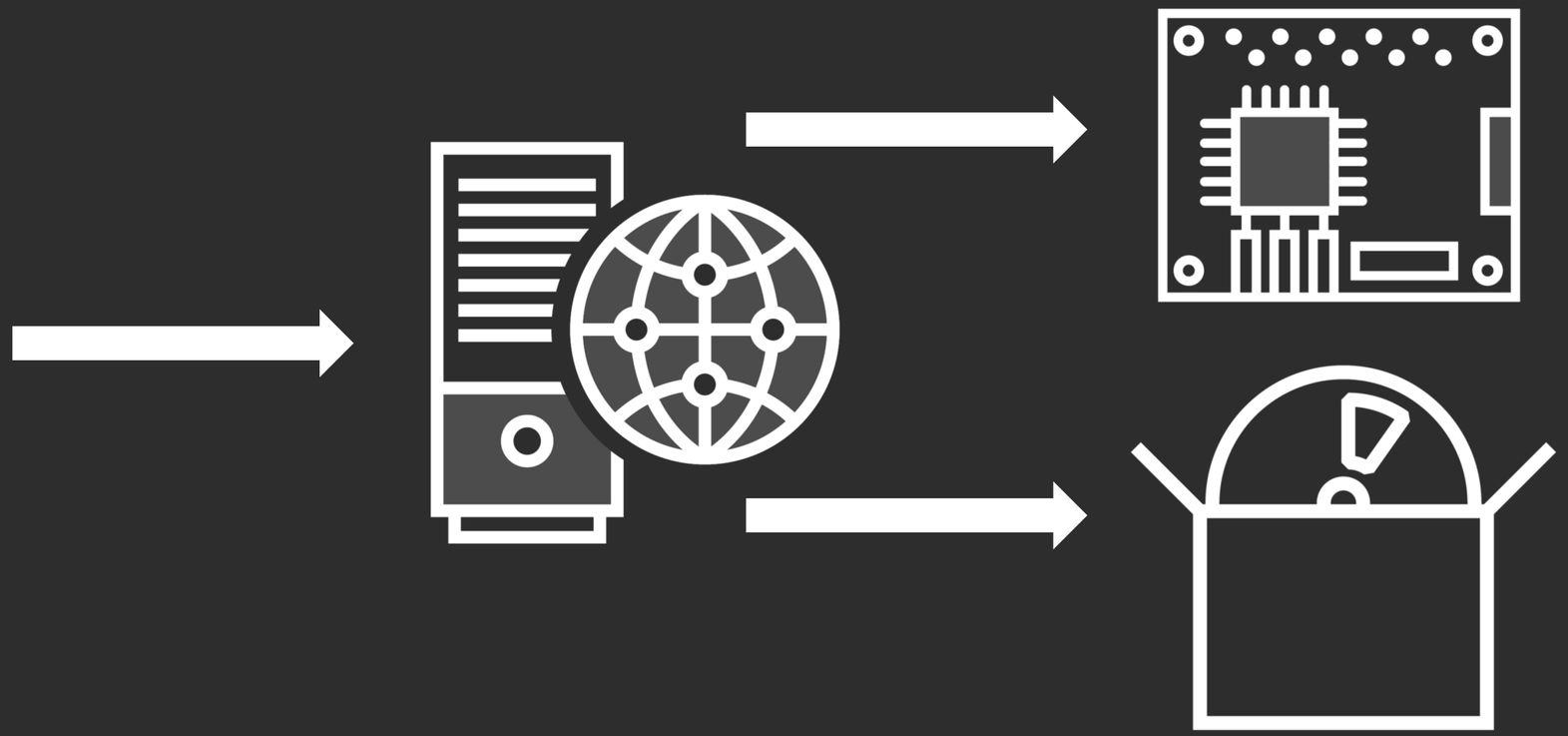
-Winston Churchill



Speaking of Sniffing

Let’s get sniffing!

Sniffing Concepts



Packet Sniffing

Monitors and captures data packets that pass through a network

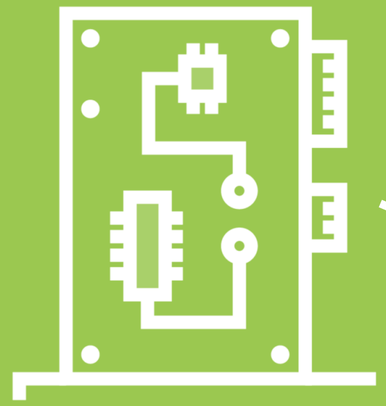
Switch

HUB

Media Access Control (MAC Address)

Ala' Mode

Ala' Mode



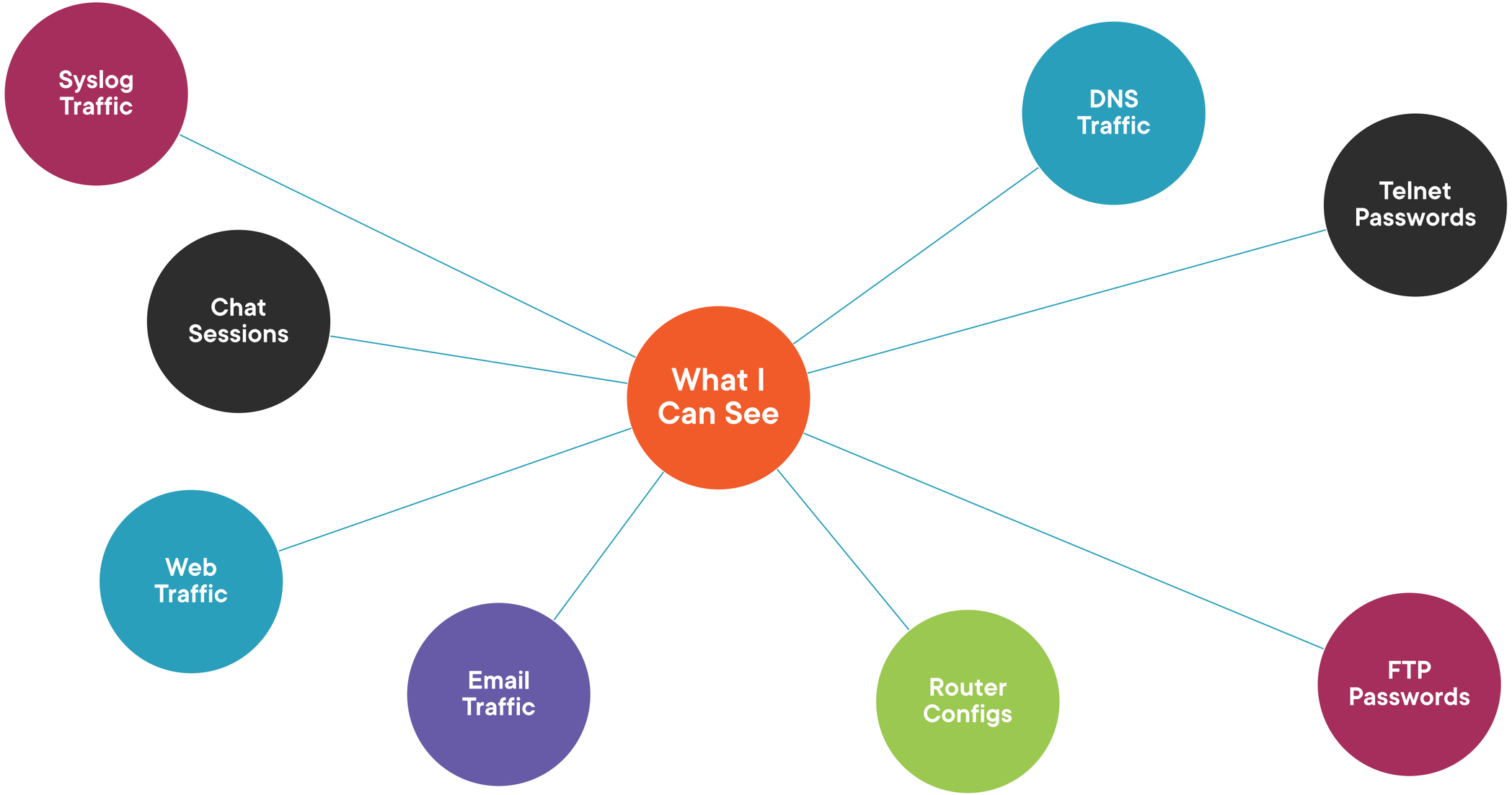
Promiscuous

Ala' Mode

Promiscuous

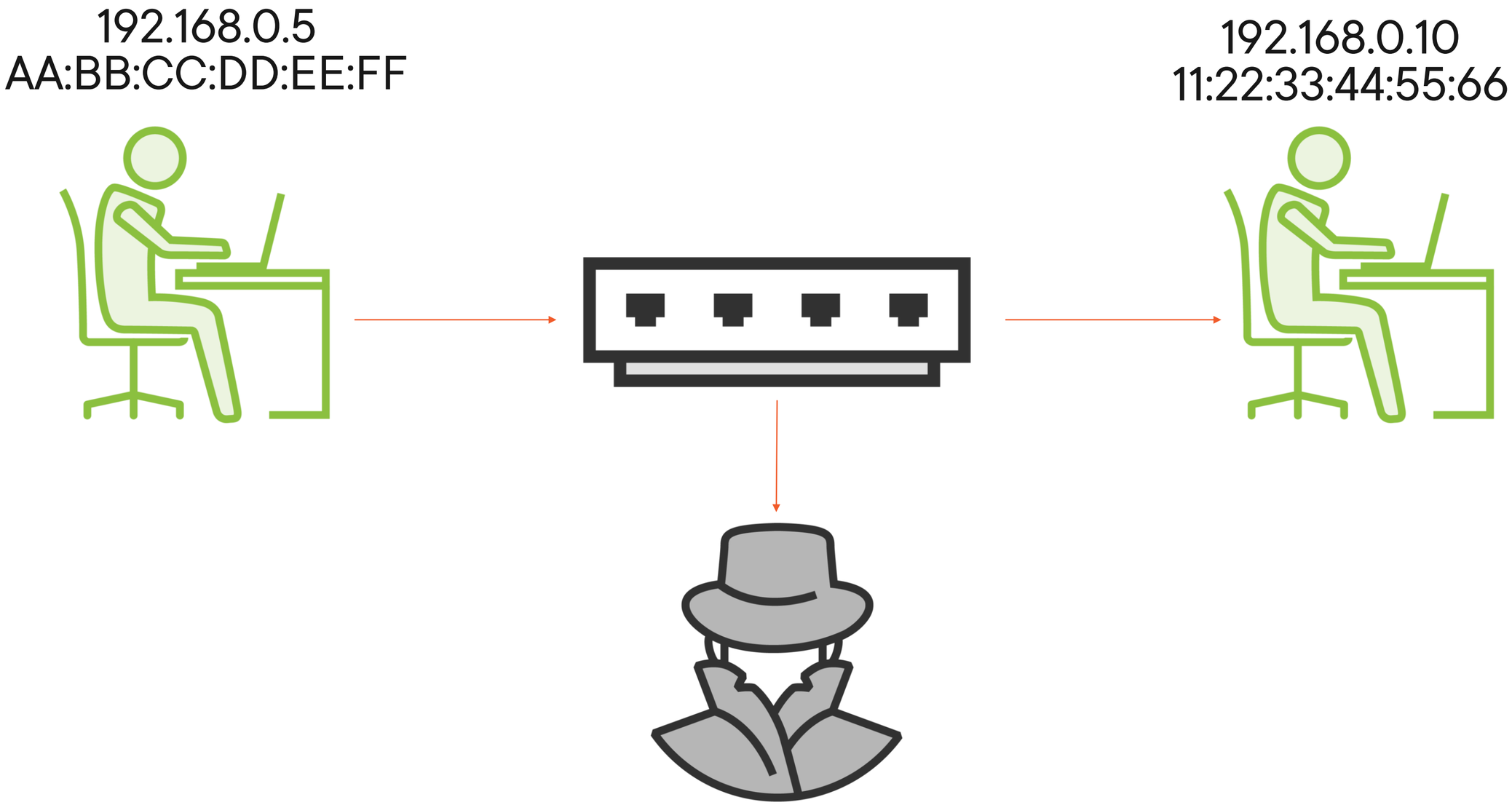
Passes traffic to the CPU instead of discarding frames intended for the NIC card

It's All There!

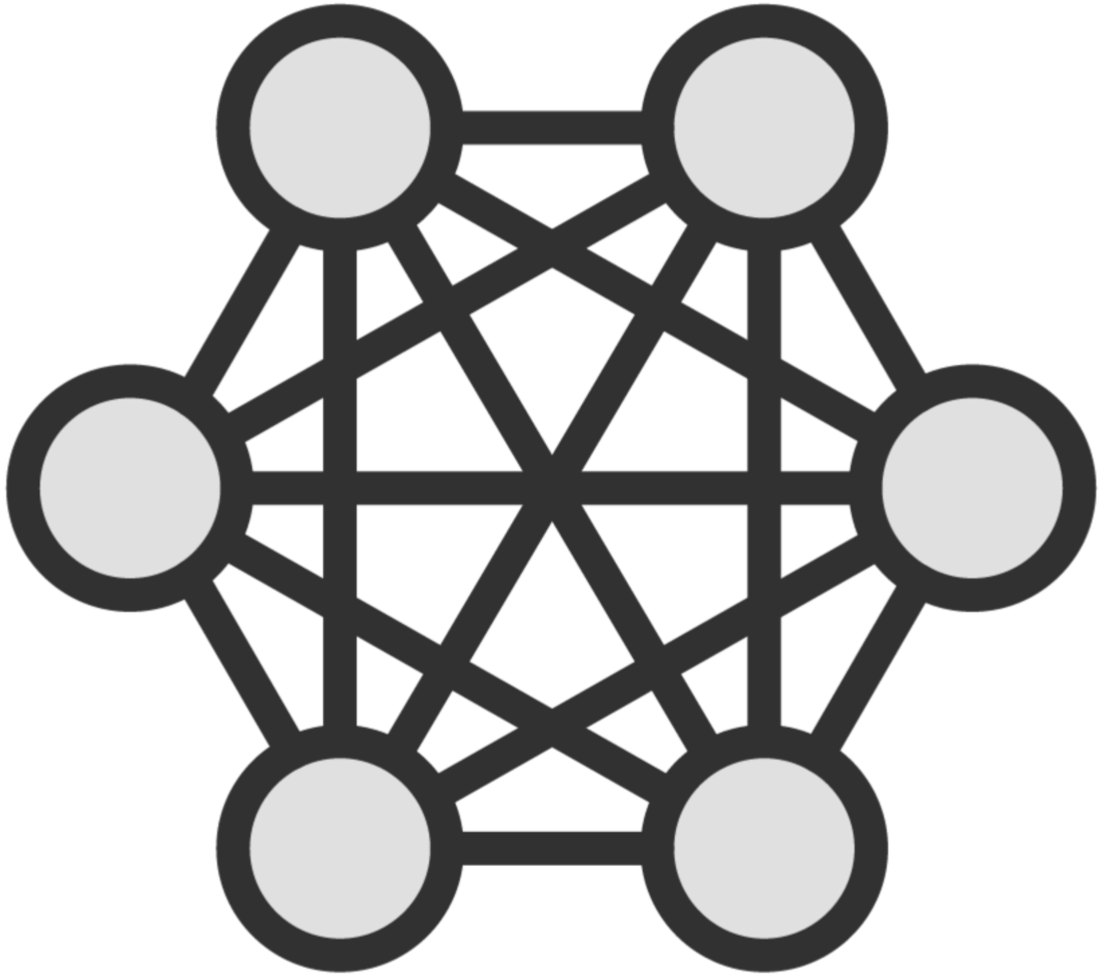


Vulnerable Protocols

HTTP	Telnet	SNMP	POP
NNTP	IMAP	FTP	rlogin



Attacker uses the information captured to break into the network



How a Sniffer Works

Design a slide here if needed

Ethernet Environments

Shared Ethernet

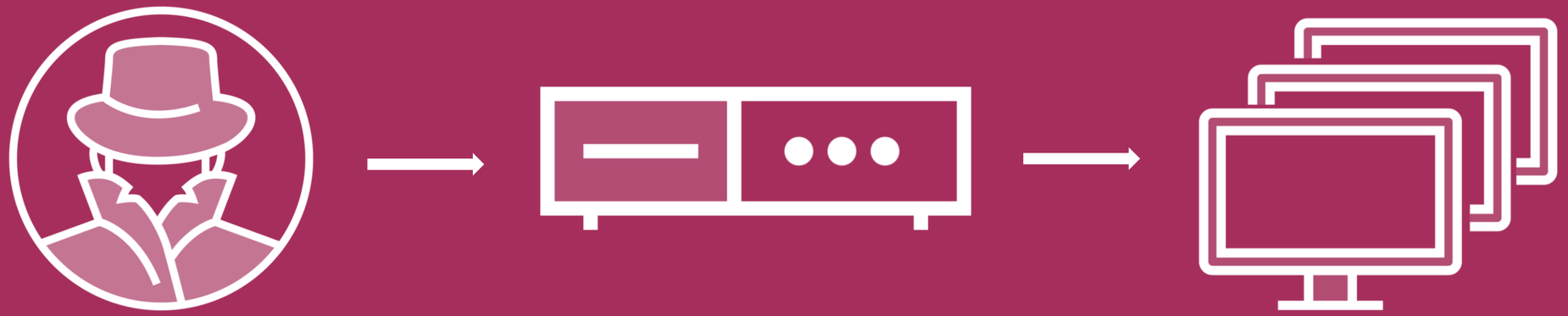
Switched Ethernet

Sniffing through a switch is more secure than a hub

ARP Spoofing

MAC Flooding

Types of Sniffing

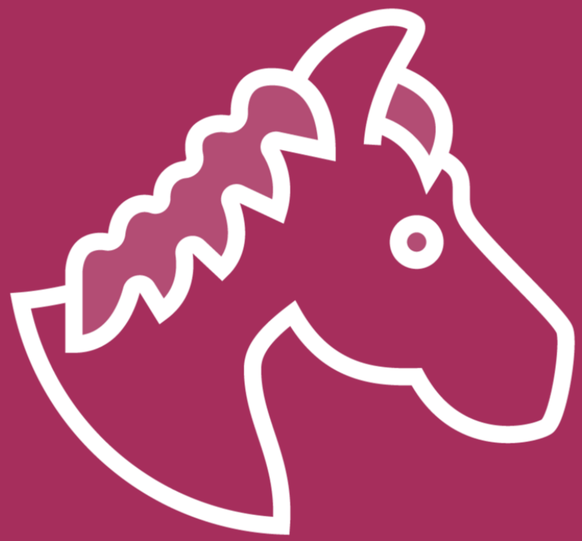


Passive Sniffing

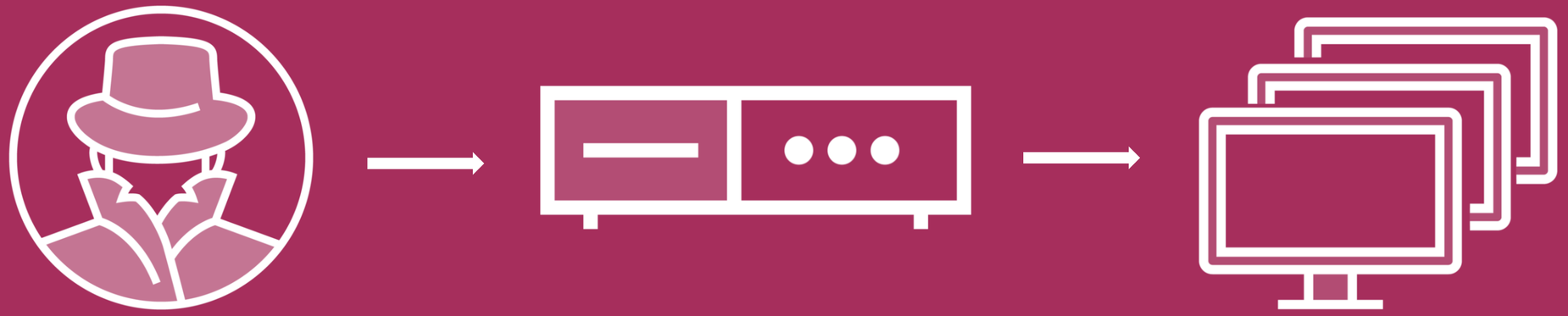
Active Sniffing

Passive Sniffing Methods

Compromise physical security

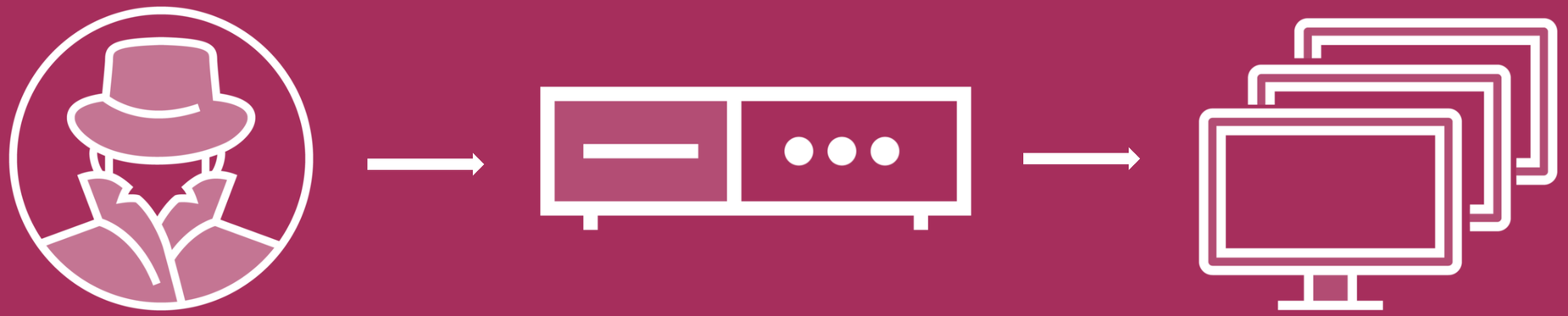


Trojan horse



Passive Sniffing

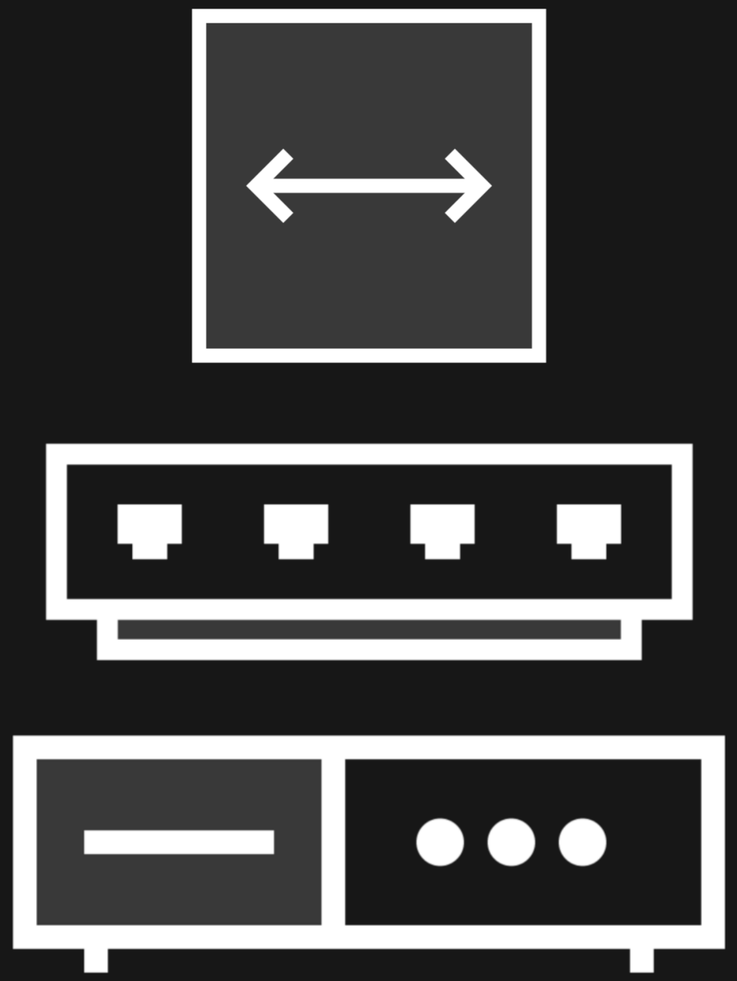
Passive sniffing has significant stealth advantages over active sniffing



Passive Sniffing

Active Sniffing

- MAC Flooding
- DNS Poisoning
- ARP Poisoning
- DHCP Attacks
- Switch Port Stealing
- Spoofing Attack

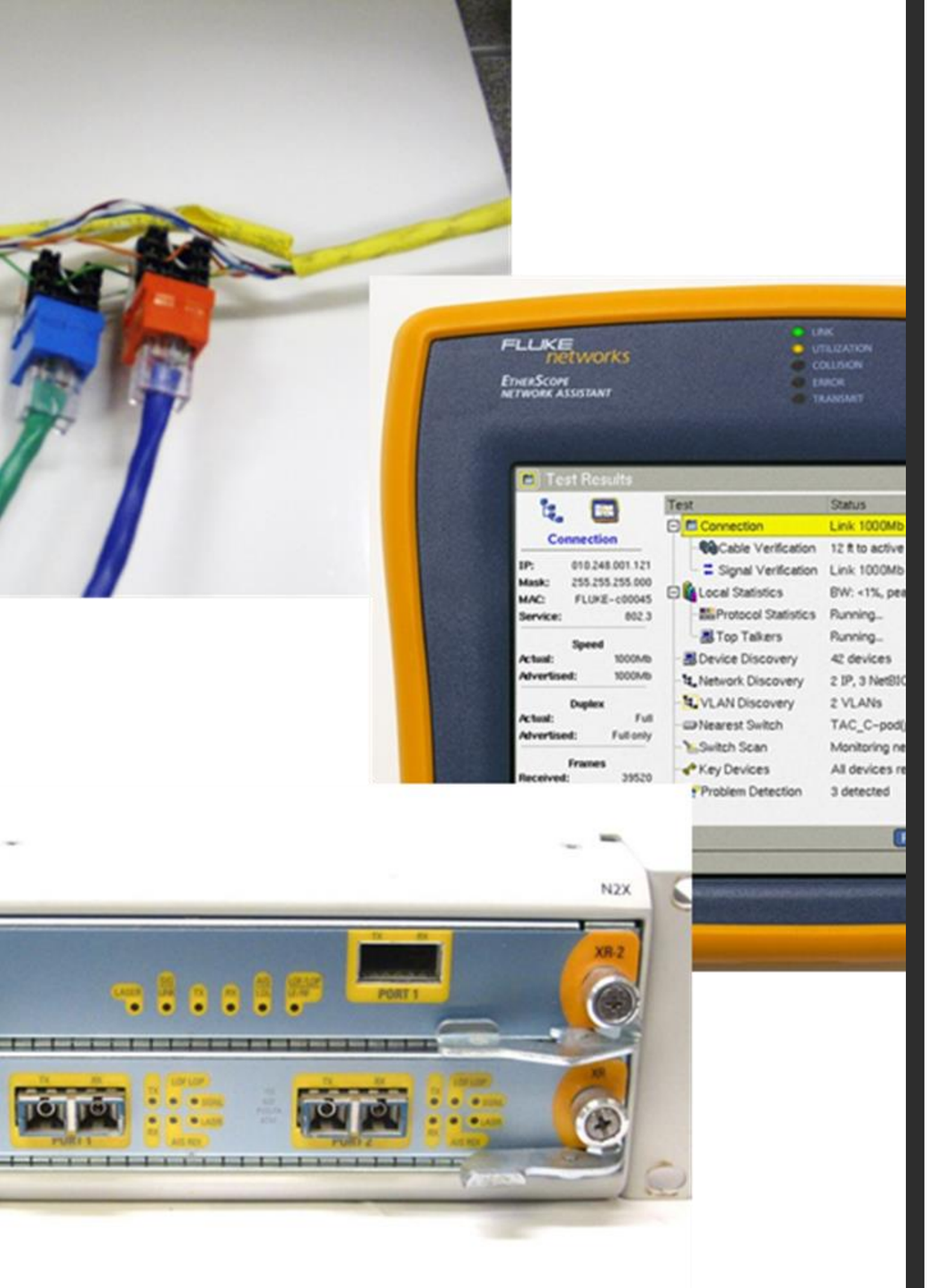


Sniffing through a switch

Active Sniffing

Purpose is to overload the switch and turn it into a HUB

Hardware vs. Software



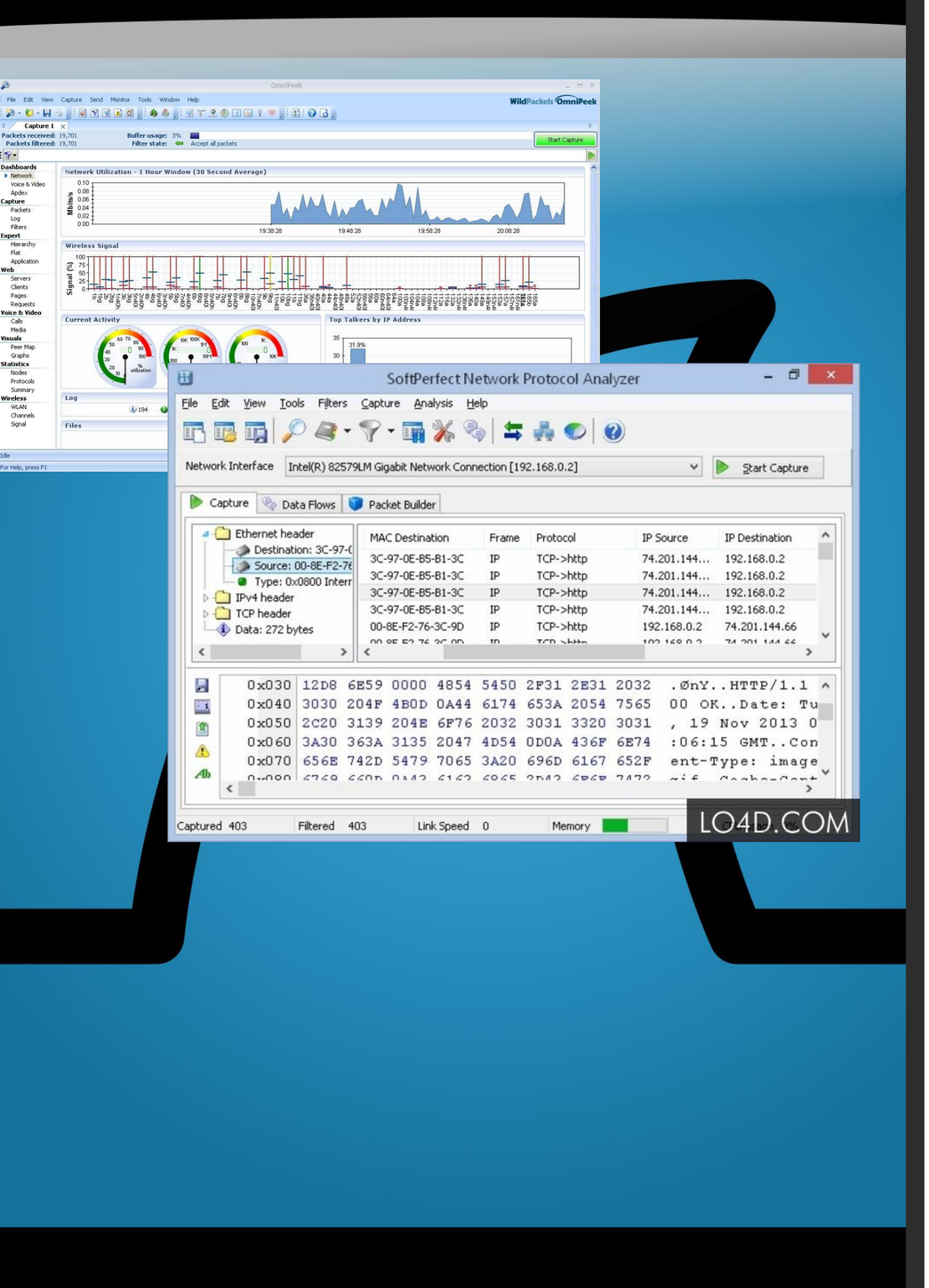
Analyzers

Monitor

Analyze

Capture

Data Packet



Software

Wireshark

OmniPeek

SoftPerfect NPA

Microsoft Network Monitor

“The Dark Side”…

Demo

Let’s sniff with Wireshark

Wiretapping

Same Story - Different Platform

Wiretapping

Unofficial

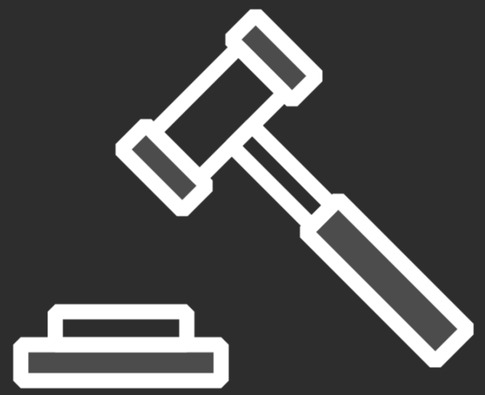
Official

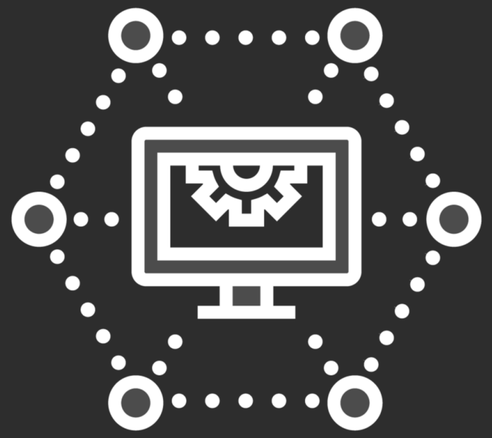
Direct line

Radio

Types of Tapping

Active	Passive
Man-in-the-middle	Eavesdropping or snooping
Monitor or record traffic	Monitor or record traffic
Change data	Doesn't change data





Know the rules for your environment.

Yes, most networks today employ switch technology

Installing remote sniffing programs on networks with heavy traffic flow is relatively easy

What Are We Looking For?

Broll – Virtual Screen with holographic info

- Download process on LED screen background
- modern-multiethnic-man-and-woman-with-tablet-using-laptop-in-server-room

Learning Check

Learning Check

- Passive sniffing
- MAC addresses
- Compromise physical security / Trojan
- Active sniffing
- Promiscuous mode

Learning Check

- ip.addr==10.10.10.85
- Follow the stream
- tcp.port==80
- Man-in-the-middle

Up Next:
Utilizing MAC Attacks