Countermeasures

Defense Techniques

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

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

“Your job isn’t to stop them. Your job is to slow them down.”

Dale Meredith

Sniffing Defense Techniques

Techniques

- Restrict physical access
- Use end-to-end encryption
- Add MAC address to the ARP cache
- Use static IP addresses and ARP tables
- Turn off network identification broadcasts

Techniques Continued

- Use IPv6 instead of IPv4
- Use encrypted sessions
- Use HTTPS instead of HTTP
- Use a switch instead of the hub
- Use Secure File Transfer Protocol (SFTP)

Techniques Continued

- Use PGP and S/MIME, FPN, IPSec, SSL/TLS, SSH, and OTP
- Use POP2 or POP3 instead of POP
- Use SNMPv3 instead of SNMPv1 and SNMPv2
- Use a strong encryption protocol (WPA or WPA2)
- Retrieve MAC addresses from NICs instead of the OS

Techniques Continued

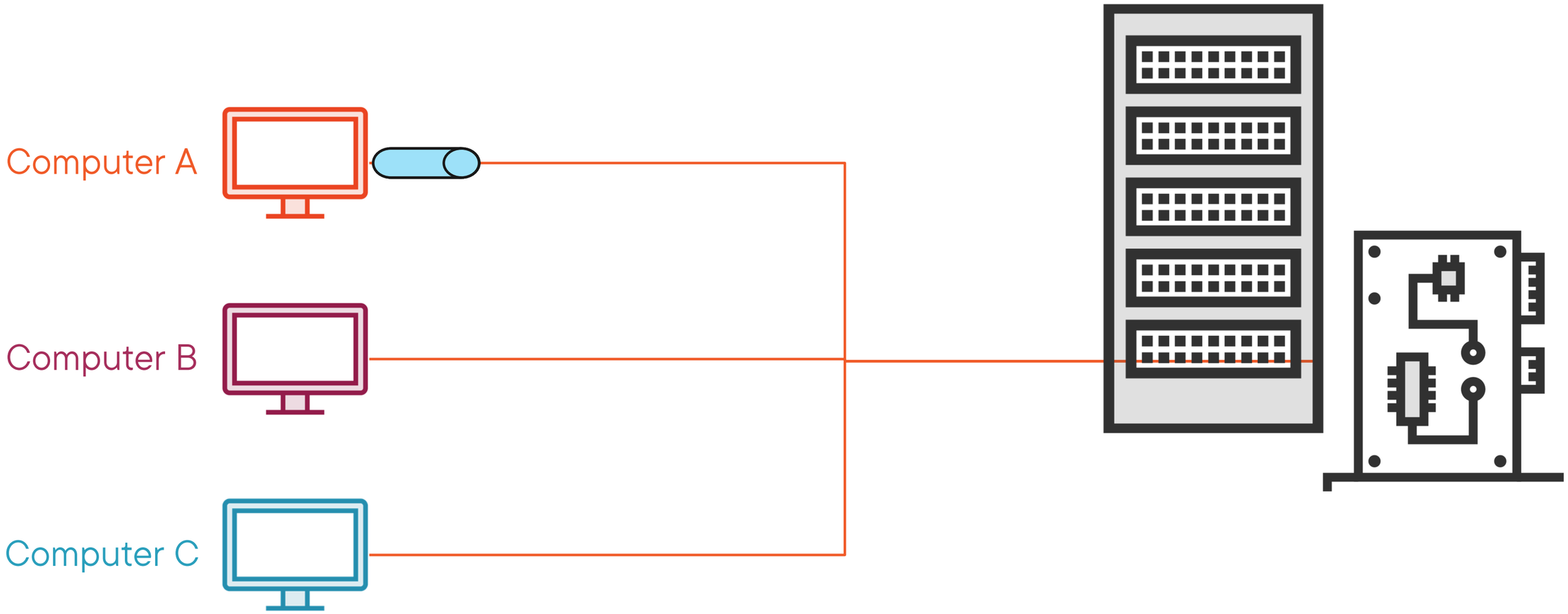
- Check to see if any NICs are running in promiscuous mode
- Use (ACL) to allow access to a fixed range of trusted IP addresses
- Change default passwords to complex passwords
- Avoid broadcasting SSIDs
- Implement a MAC filtering on your router

Implement network scanning and monitoring tools to detect malicious intrustions

Detect Sniffing

Detecting sniffing is rarely easy

Promiscuous mode allows a network device to intercept and read each packet



Tools to Detect Sniffing

Run IDS to see if the MAC address of any of the machines has changed

IDS alerts the administrator about suspicious activities

Tools to Detect Sniffing

Nmap is one of many tools available to detect promiscuous mode

Capsa Portable Network Analyzer will monitor the network for packets with spoofed addresses

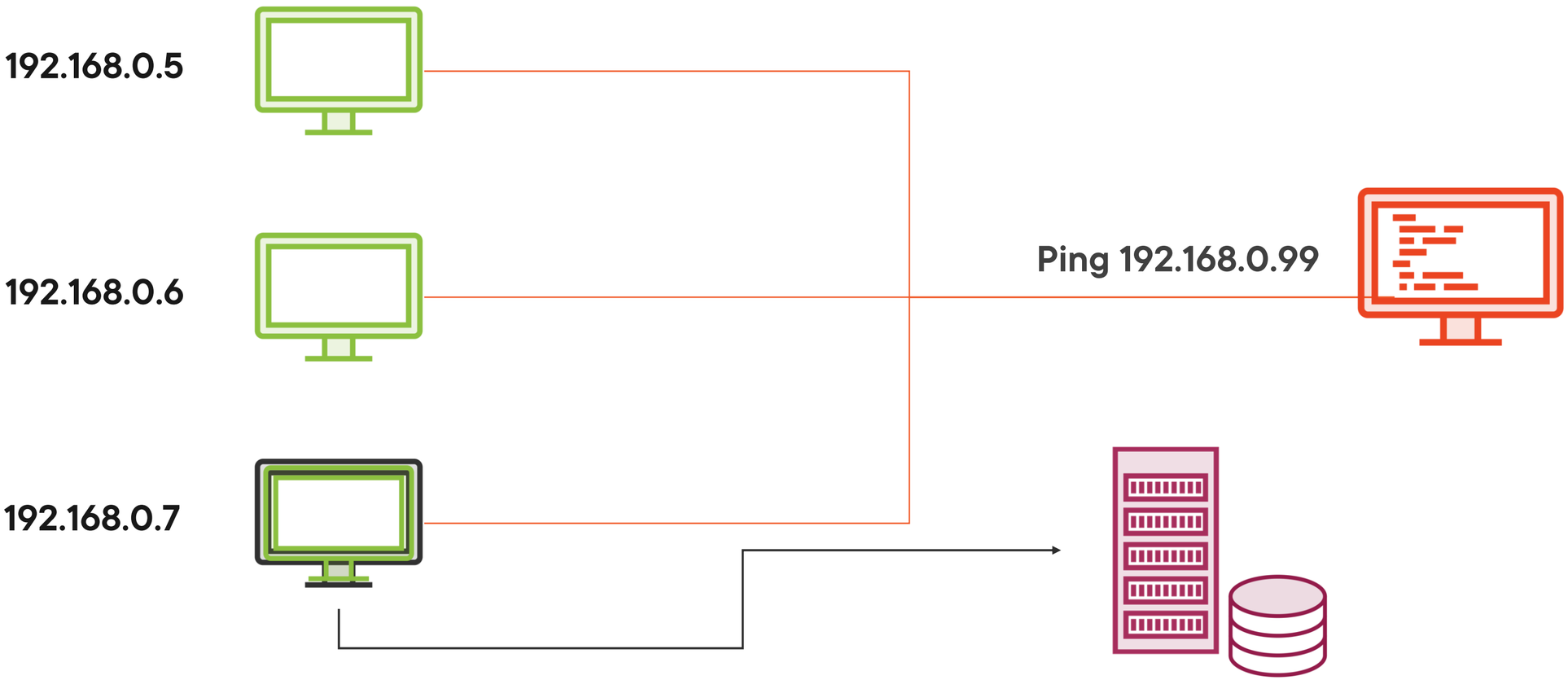
Detect Sniffing via Ping

Detect Sniffing via Ping

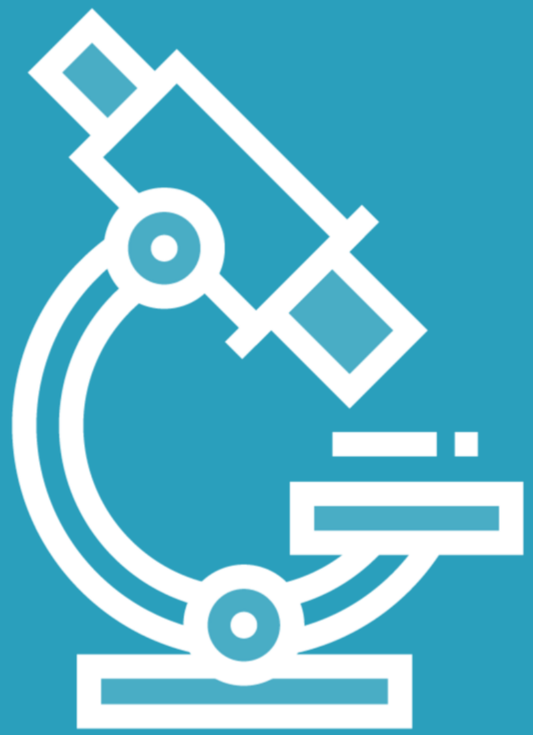
- The Ethernet adapter rejects it because the MAC address does not match
- The suspect machine running the sniffer will respond to it

Detect Sniffing via DNS

Detect Sniffing via DNS



Who is 192.168.0.99?



Detect Sniffing via ARP

Detect Sniffing via ARP

- Non-broadcast ARP is sent to all the nodes in the network
- The node in promiscuous mode caches the local ARP address
- A ping messages is sent with the local IP address but a different MAC address
- Only the node that has the MAC address responds
- The promiscuous mode machine replies to the ping message and remaining machines send an ARP probe to identify the source

Demo

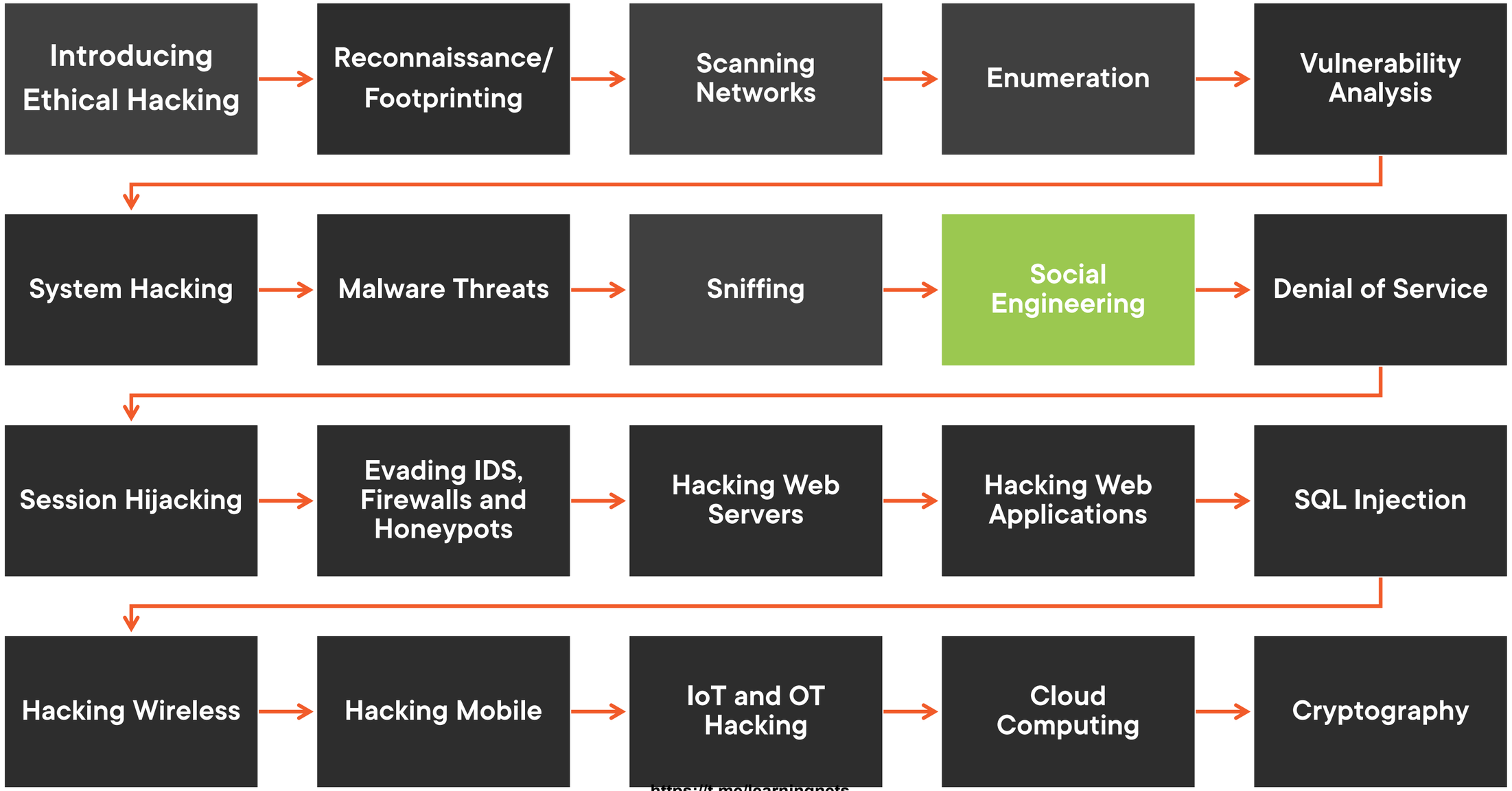
Detecting promiscuous mode with nmap

Learning Check

Learning Check

- Ping method
- ARP method
- DNS method
- Nmap --script=sniffer-detect <ip address/range>
- Plethora

Ethical Hacking Series



Add clip to rate and follow (if you do this at the end of each course

Up Next:
Ethical Hacking: Social Engineering