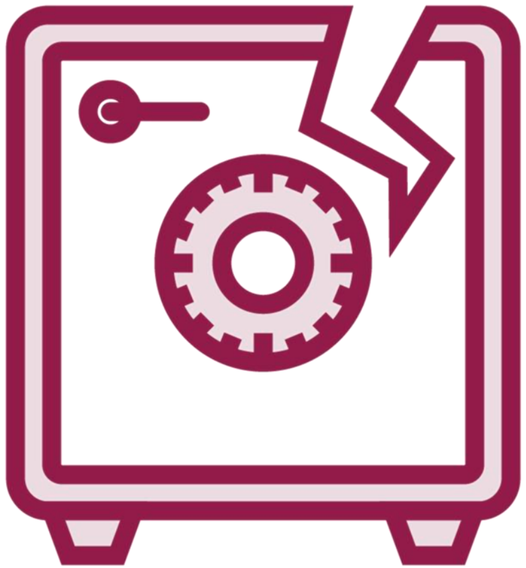
Understanding ARP Poisoning Attacks

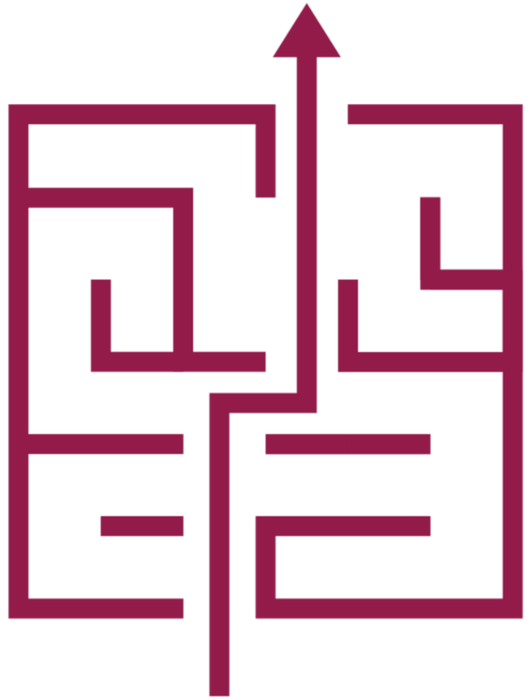
Dale Meredith
MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

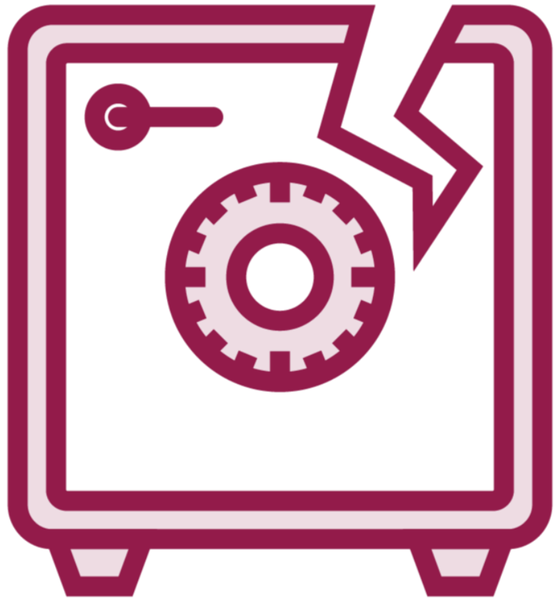
dalemeredith.com | Twitter: @dalemeredith | Linkedin: dalemeredith|

“Magicians are the most honest people in the world. They tell you they’re going to fool you and then they do it.”

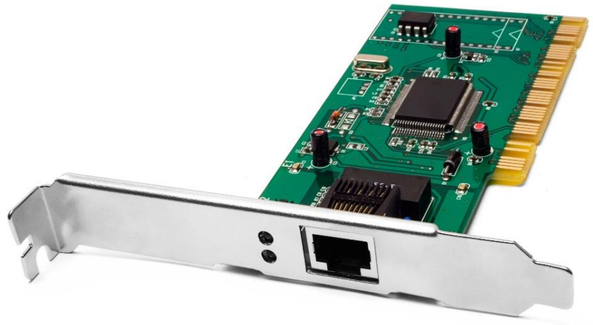
James Randi



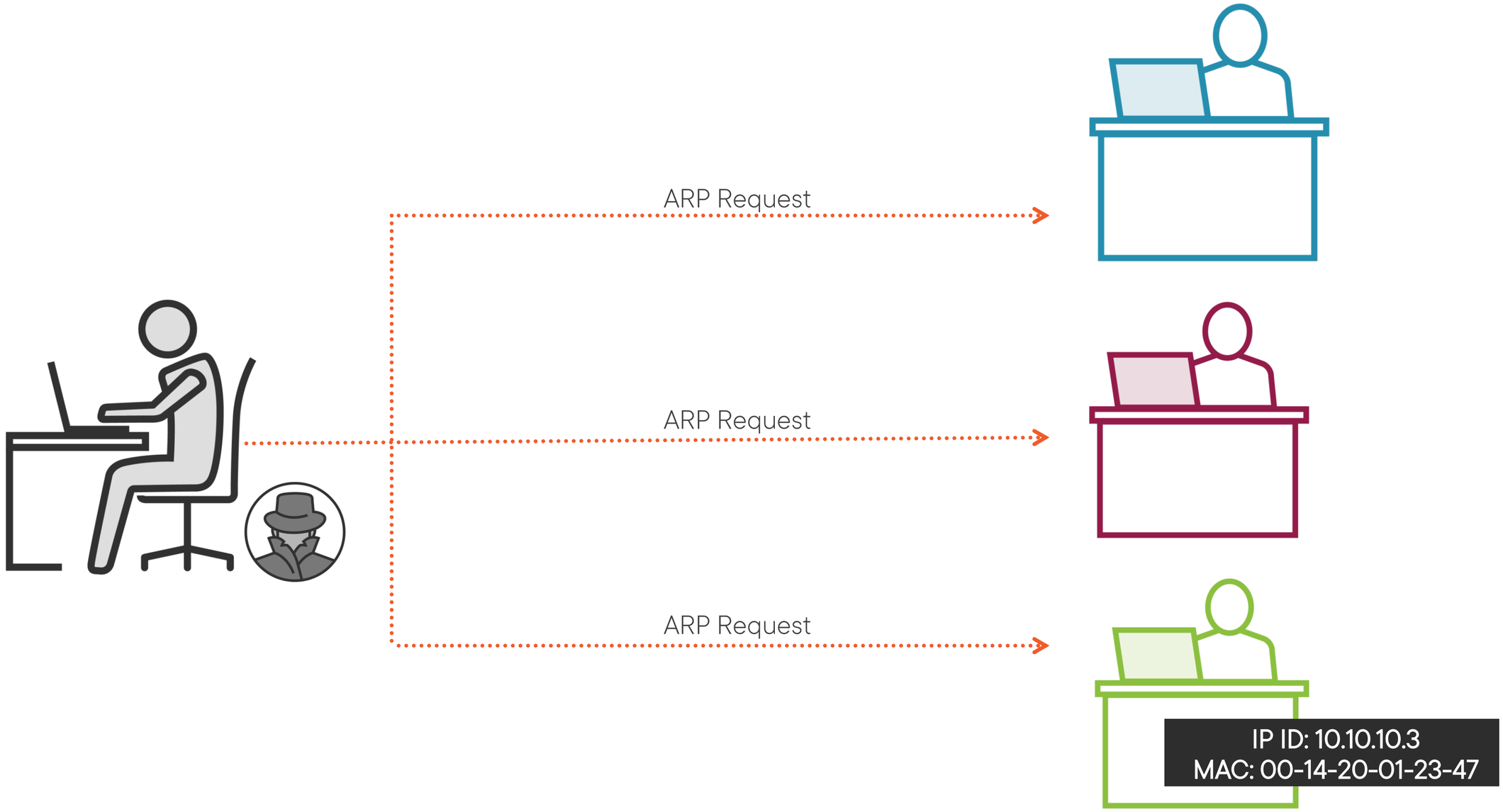




What ARP Does



```
Description . . . . . . . . . . . : Hyper-V Virtual Et
Physical Address. . . . . . . . . : 08-60-6E-75-5C-6D
DHCP Enabled. . . . . . . . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::90a0:f828:93
IPv4 Address. . . . . . . . . . . : 10.10.10.35(Prefer
Subnet Mask . . . . . . . . . . . : 255.255.255.0
```



Set the Table

Stored in memory

Temporary

Easily manipulated

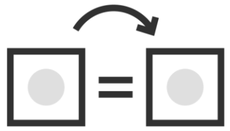
Demo

Let’s checkout our ARP table

ARP Spoofing Attack

ARP Spoofing

ARP packets are forged to send data to the attacker's machine

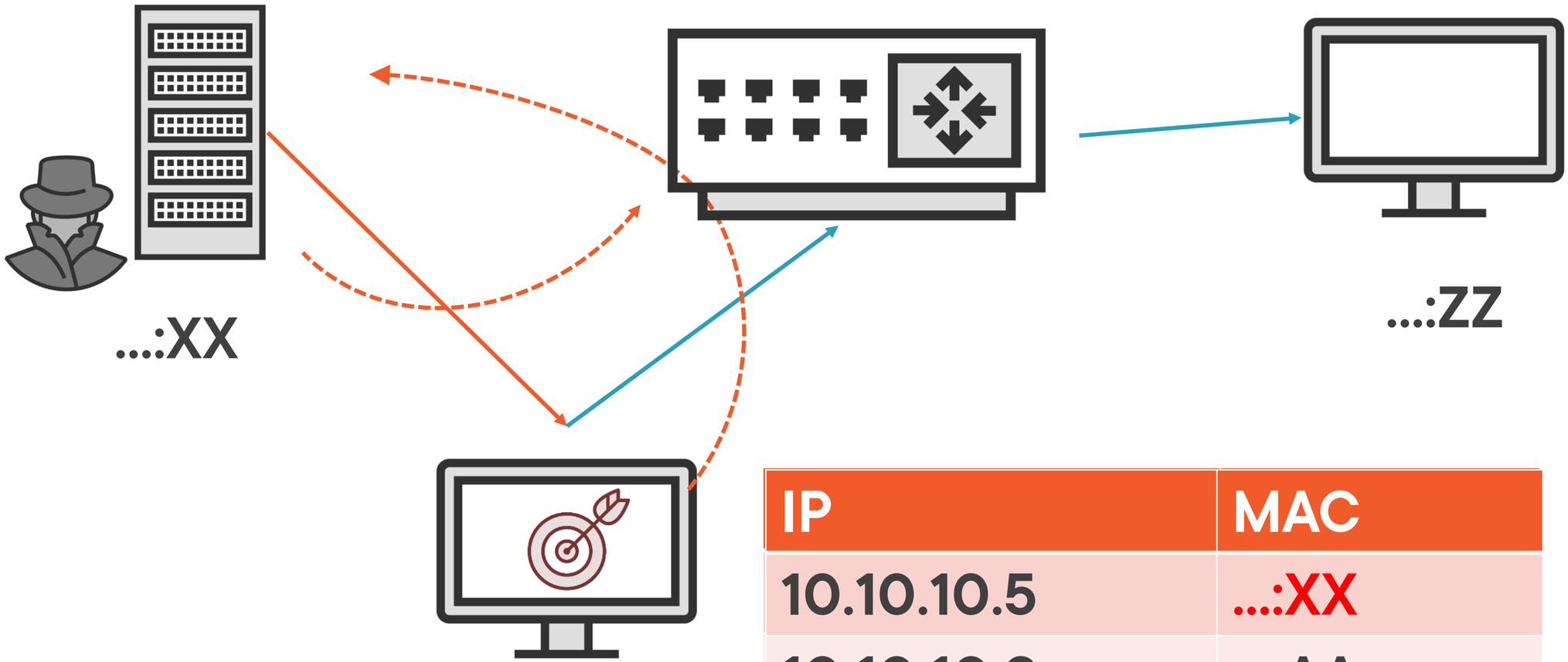


Purpose is to construct multiple ARP requests and reply packets to overload the switch

Switch is set to forward mode allowing attackers to sniff packets

Poisoning occurs when a targeted computer's ARP cache is flooded with forged entries

ARP Poisoning



IP	MAC
10.10.10.5	...:XX
10.10.10.9	...:AA

Tools of the Trade

- arpspoof
- BetterCAP
- dsniff
- MITMf
- arpoison

Demo

Using Cain and Abel to ARP Spoof

Dangers of ARP Poisoning

Threats

- Packet sniffing
- Session hijacking
- VoIP call tapping
- Manipulating data
- Man-in-the-middle attack

Story Time with Dale

Threats

- Data interception
- Connection hijacking
- Connection resetting
- Stealing passwords
- DoS attack

ARP Spoofing Countermeasures

Dynamic ARP Inspection

Validates ARP packets in a network

Triggers all ports to be untrusted by default

Validates using a DHCP snooping binding table

Performs IP-address-to-MAC-address inspection

Discards invalid ARP packets

Ensures the relay of valid ARP requests and responses

Defending Against ARP Poisoning

DHCP Snooping is not possible, if the host systems hold static IP addresses

Perform static mapping that associates an IP address to a MAC address

Cryptographic Protocols

Transport Layer Security (TLS)

Secure Shell (SSH)

HTTP Secure (HTTPS)

Prevent ARP spoofing attacks by encrypting data before transmission and authenticating it after it is received

Configuring DHCP Snooping and Dynamic ARP Inspection on Cisco Switches

Global configuration mode

```
Switch (config)# ip dhcp snooping
```

Configuring for a VLAN

```
Switch (config)# dhcp snooping vlan 10
```

To view DHCP snooping status

```
Switch# show ip dhcp snooping

Switch DHCP snooping is enabled
```

“If you think you know all about cyber-security, then you misunderstand its basic concepts.”

Dale Meredith

Learning Check

Learning Check

- Sends forged packets
- TLS, HTTPS, SSH
- Man-in-The-Middle (MiTM)
- arp -a
- MAC to IP addresses

Up Next:
Executing Spoofing Attacks