HackingDojo.com

Hacking Network Protocols Using Kali Linux

Thomas Wilhelm

Security Consultant

- Education
  - Masters Degrees in Computer Security:
    - Computer Science
    - Management
- Author since 2007
  - Professional Penetration Testing
  - Ninja Hacking
  - Netcat Power Tools
  - Penetration Testing's Open Source Toolkit, V2
- Certifications
  - ISSMP, CISSP, SCSECA, SCNA, SCSA, IEM/IAM

Todd Kendall

Security Consultant

- Education
  - The George Washington University (MA)
  - University of Redlands (BA)
- Author multiple articles
  - Network Forensics: The Tree in the Forest
  - The Security Consulting Sugar High
  - Hack First, Policy Second – A mobile Device Story
- Certifications
  - CISSP
  - CCISO
  - Certified Computer Forensic Specialist

Why are here?

- Learn how to use Kali Linux to attack network protocols
  - CAM Table Overflow
  - VLAN Hopping
  - ARP Poisoning
  - DHCP Spoofing

- If you know how to do this, please give up your seat so others can join in (assuming we have a full class)

What do you need?

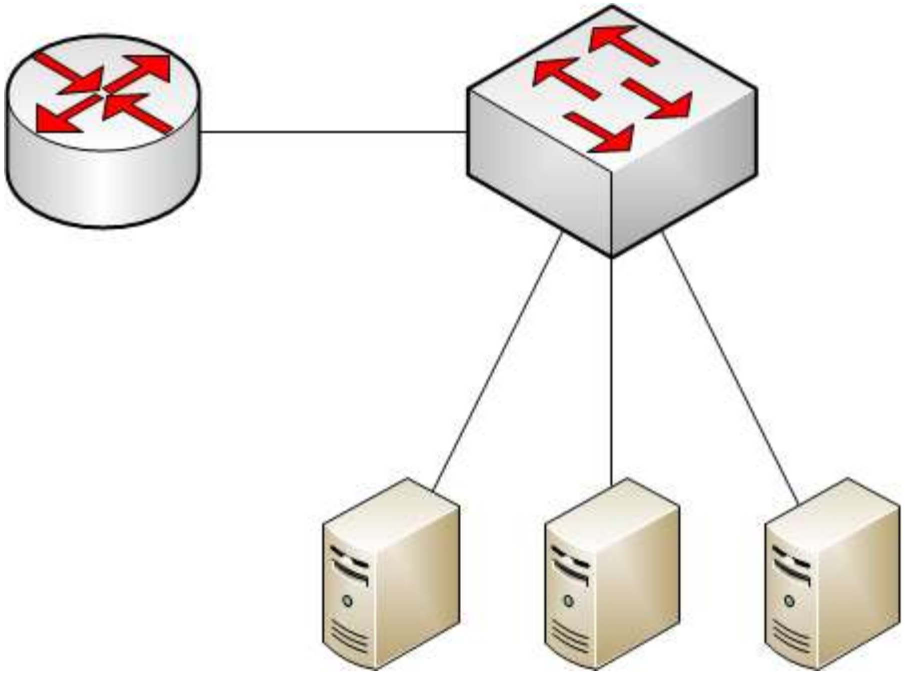
- Pre-installed Kali Linux
  - Prefer to have it as the main OS, not virtualized
- CAT5 cable of sufficient length
  - We didn’t know in advance how the rooms would be, so please bear with us when we get everyone connected
- Patience
  - 4 hours, 4 tasks, a LOT of network congestion
  - This is a HOSTILE NETWORK!!

How this workshop will... work

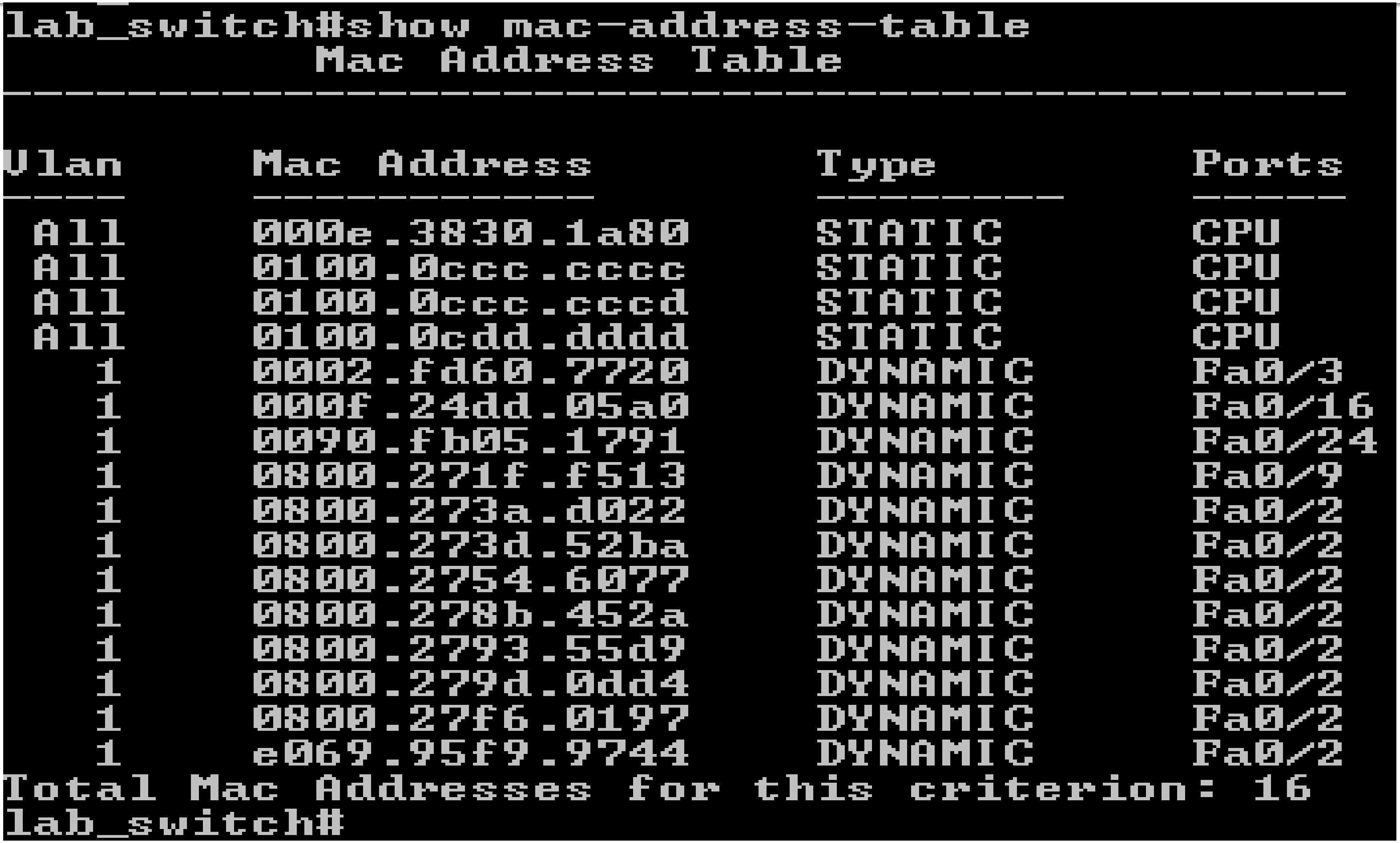
- Do / Don’t
  - Everyone is here to learn, so don’t impede others
  - Embrace other people’s genius
  - Workshop = Group Effort, work as a team
  - Workshop != Taking over someone else’s keyboard
  - We’re here to learn, not be pedantic over terms

CAM Table Overflow

- Content Addressable Memory Table
- Layer 2 (Switch)
- Records MAC addresses and saves them for switching purposes



#show mac-address-table



```
lab_switch#show mac-address-table
                   Mac Address Table
------------------------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000e.3830.1a80    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0002.fd60.7720    DYNAMIC     Fa0/3
   1    000f.24dd.05a0    DYNAMIC     Fa0/16
   1    0090.fb05.1791    DYNAMIC     Fa0/24
   1    0800.271f.f513    DYNAMIC     Fa0/9
   1    0800.273a.d022    DYNAMIC     Fa0/2
   1    0800.273d.52ba    DYNAMIC     Fa0/2
   1    0800.2754.6077    DYNAMIC     Fa0/2
   1    0800.278b.452a    DYNAMIC     Fa0/2
   1    0800.2793.55d9    DYNAMIC     Fa0/2
   1    0800.279d.0dd4    DYNAMIC     Fa0/2
   1    0800.27f6.0197    DYNAMIC     Fa0/2
   1    e069.95f9.9744    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 16
lab_switch#
```

How to Exploit CAM Tables

- Overflow it, and have no mercy!
  - When CAM table fills up, it pushes all data out all ports*
  - Essentially, you turn a Switch (L2) into a Hub (L1)
  - **#macof** <- tool of choice
- Collect the data
  - Need to collect the packets as it leaves the switch
  - Wireshark is probably the best-known tool, but any pcap capturing app will work

When to Exploit CAM Tables

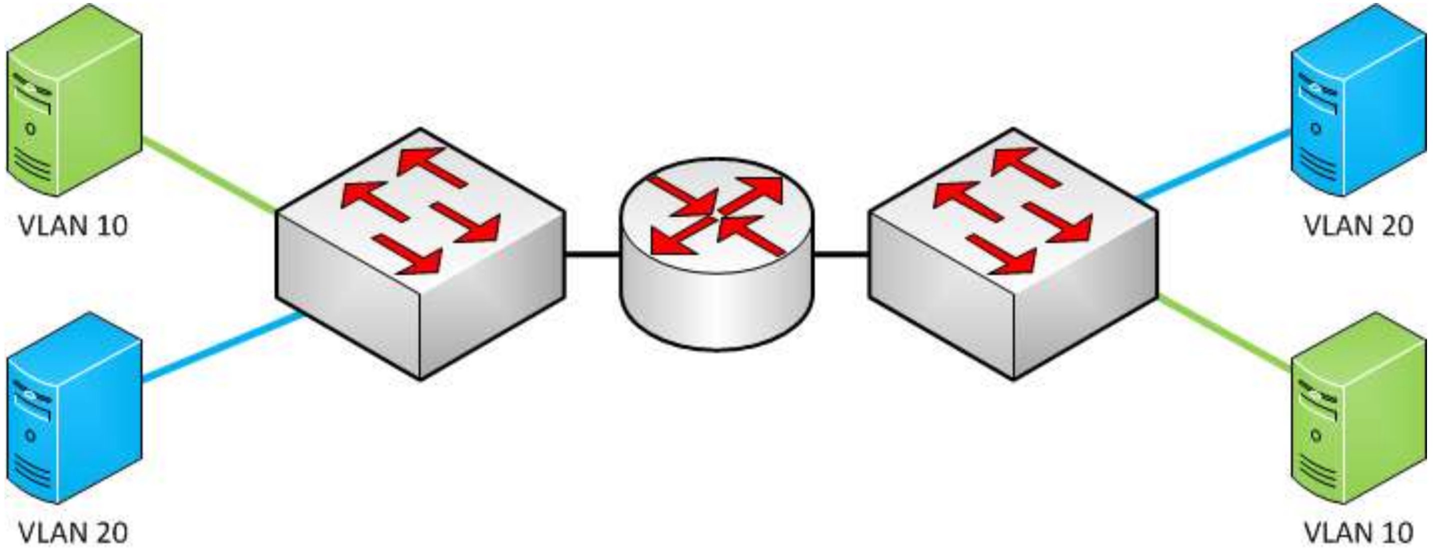
- Good to use when ARP Spoofing is:
  - monitored or blocked
  - Too much traffic across the network
- Want to attack system on your switch, not within the Broadcast Domain

How to Exploit CAM Tables

- DEMO
- Hands-on lab
- Start next topic at top of the hour

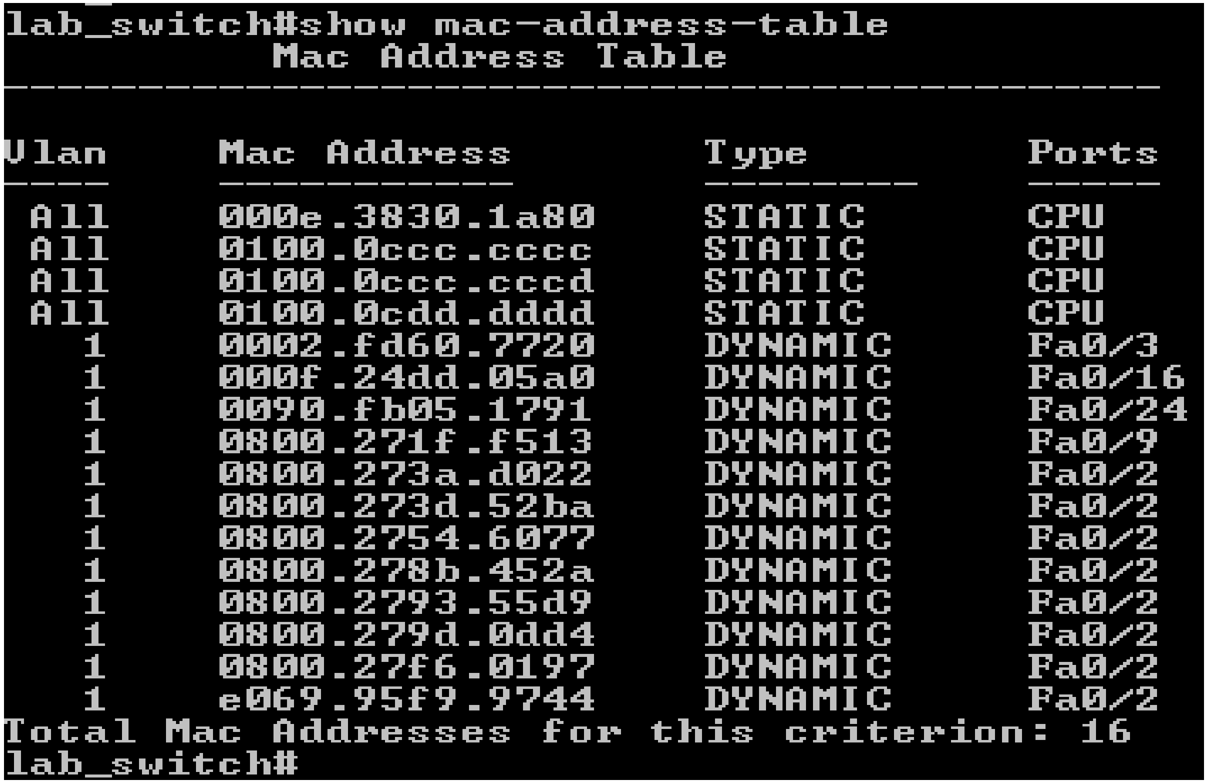
VLAN Hopping

- Virtual Local Area Network (VLAN)
  - Broadcast Domain
  - Allows multiple broadcast domains on a single switch



VLAN Hopping

- Not going to discuss Trunking Protocol Attack
- Double Tagging requires us to be on VLAN1

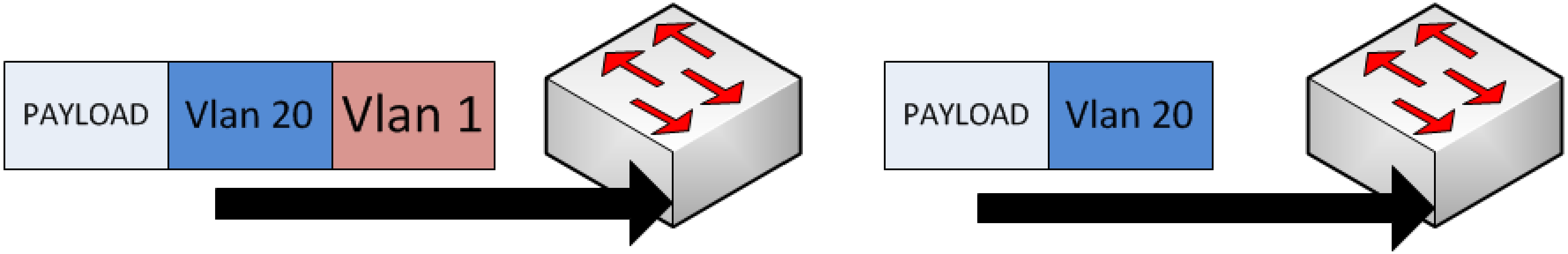


```
lab_switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    000e.3830.1a80    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0002.fd60.7720    DYNAMIC     Fa0/3
   1    000f.24dd.05a0    DYNAMIC     Fa0/16
   1    0090.fb05.1791    DYNAMIC     Fa0/24
   1    0800.271f.f513    DYNAMIC     Fa0/9
   1    0800.273a.d022    DYNAMIC     Fa0/2
   1    0800.273d.52ba    DYNAMIC     Fa0/2
   1    0800.2754.6077    DYNAMIC     Fa0/2
   1    0800.278b.452a    DYNAMIC     Fa0/2
   1    0800.2793.55d9    DYNAMIC     Fa0/2
   1    0800.279d.0dd4    DYNAMIC     Fa0/2
   1    0800.27f6.0197    DYNAMIC     Fa0/2
   1    e069.95f9.9744    DYNAMIC     Fa0/2
Total Mac Addresses for this criterion: 16
lab_switch#
```

VLAN Hopping

- Not going to discuss Trunking Protocol Attack
- Double Tagging:
  - Requires us to be on VLAN1
  - Adds the target VLAN between payload and VLAN1 tag
  - Once the VLAN 1 tag gets stripped, the second switch reads the VLAN 20 tag
- Why does this work? No tag = VLAN 1



PAYLOAD | Vlan 20 | Vlan 1

PAYLOAD | Vlan 20

VLAN Hopping

- Time to crush your hopes
  - Double Tagging only works one way
  - All attacks are blind – the target server follows the rules
  - Attack options include:
    - Reflective
    - DoS
- Reference:
  - https://www.sans.org/reading-room/whitepapers/networkdevs/virtual-lan-security-weaknesses-countermeasures-1090

When to Exploit VLAN Hopping

- You have the ability to redirect the attack
- Proof of concept
- DoS

How to Exploit VLAN Hopping

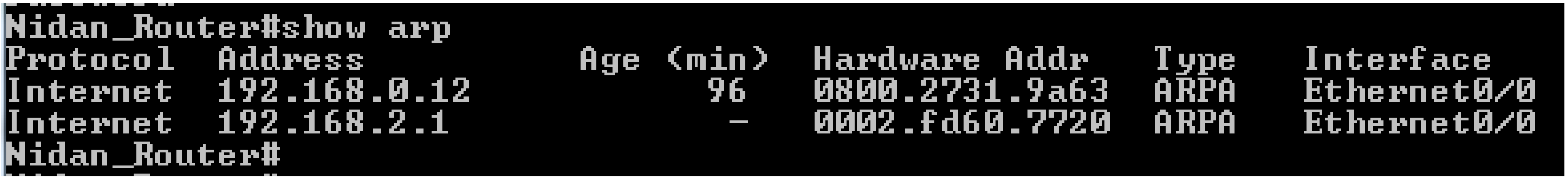
- DEMO
- Hands-on lab
- Start next topic at top of the hour

ARP Poisoning

- Types of Poisoning
  - **ARP**
  - ICMP
  - DHCP
  - Port Stealing
- Perform Man-in-the-Middle Attack
- Need to be able to collect packets
- Limited to BROADCAST DOMAIN only

Address Resolution Protocol

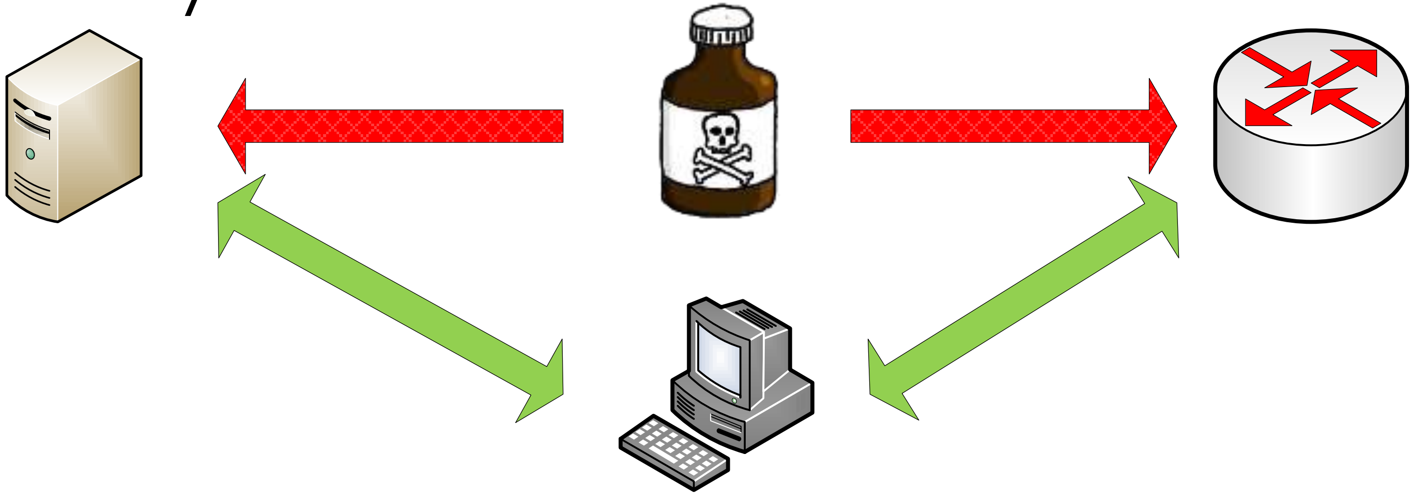
- Trick question:
  - Which OSI Model layer does it reside in?
- We are going to pretend and just say Layer 2
  - Easier on the mind to just play dumb
- What does it do?
  - Takes IP addresses and resolves them to MAC addresses



```
Nidan_Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.0.12            96  0800.2731.9a63  ARPA   Ethernet0/0
Internet  192.168.2.1              -  0002.fd60.7720  ARPA   Ethernet0/0
Nidan_Router#
```

Attack ARP Table

- We can pick two (or more systems) and poison their ARP table
- Typically the targets are:
    - The Default Gateway
    - Everyone else in the Broadcast Domain



Attack ARP Table

- Warnings!
  - When using ettercap, don’t use <CTRL>-C to stop the attack
  - Remote internal pentests are a PAIN!! RDP stops working when you use ettercap (hint: “timeout”)
  - Start slow – you can impact production
  - When conducting a pentest, make sure you’re in a valid employee subnet
  - READ THE PCAP FILE – don’t just trust the logs

When to ARP Spoof Attack

- Any time
  - I use it at the beginning of a test, and when I want to target a specific system (admin, etc.)
- Start slow
  - One or two minutes at first, build up from there once you know you’re not impacting the network

ARP Spoofing Attack

- DEMO
- Hands-on lab
- Start next topic at top of the hour

DHCP Spoofing

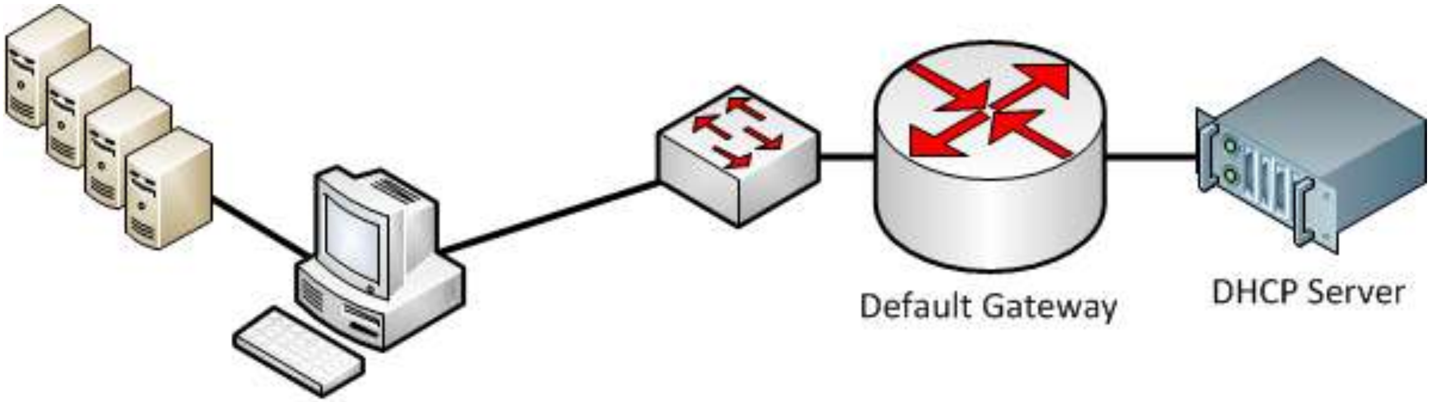
- Saved the worst for last
  - This will mess up your DHCP Table…
  - Mess up the network for hours, days…
  - Great way to create a DoS for a network…
  - Crosses routers into neighboring networks…
- Used to pass bogus information to target systems, like default gateway

DHCP Spoofing

- Mandatory Information passed in DHCP Offer:
  - Client IP address
  - DHCP Address
  - Gateway IP Address
  - ...more
- Optional information:
  - Lease Time (***Cisco default: one day***)
  - Time Server
  - Name Server
  - Domain Name Server
  - Domain Name
  - Host Name

DHCP Spoofing

- To work, we need to either race against the DHCP Server, or starve out ALL the DHCP addresses of the valid DHCP Server



LOOK AT ME.
I'M THE GATEWAY NOW!

When to Use DHCP Spoofing

- As a last resort, only after permission granted
- Proof of concept
- Small organizations
  - There will be calls to help desk

DHCP Spoofing

- DEMO
- Hands-on lab
- Leave when done

- THANKS FOR JOINING US!
- Any feedback, please send to info@hackingdojo.com