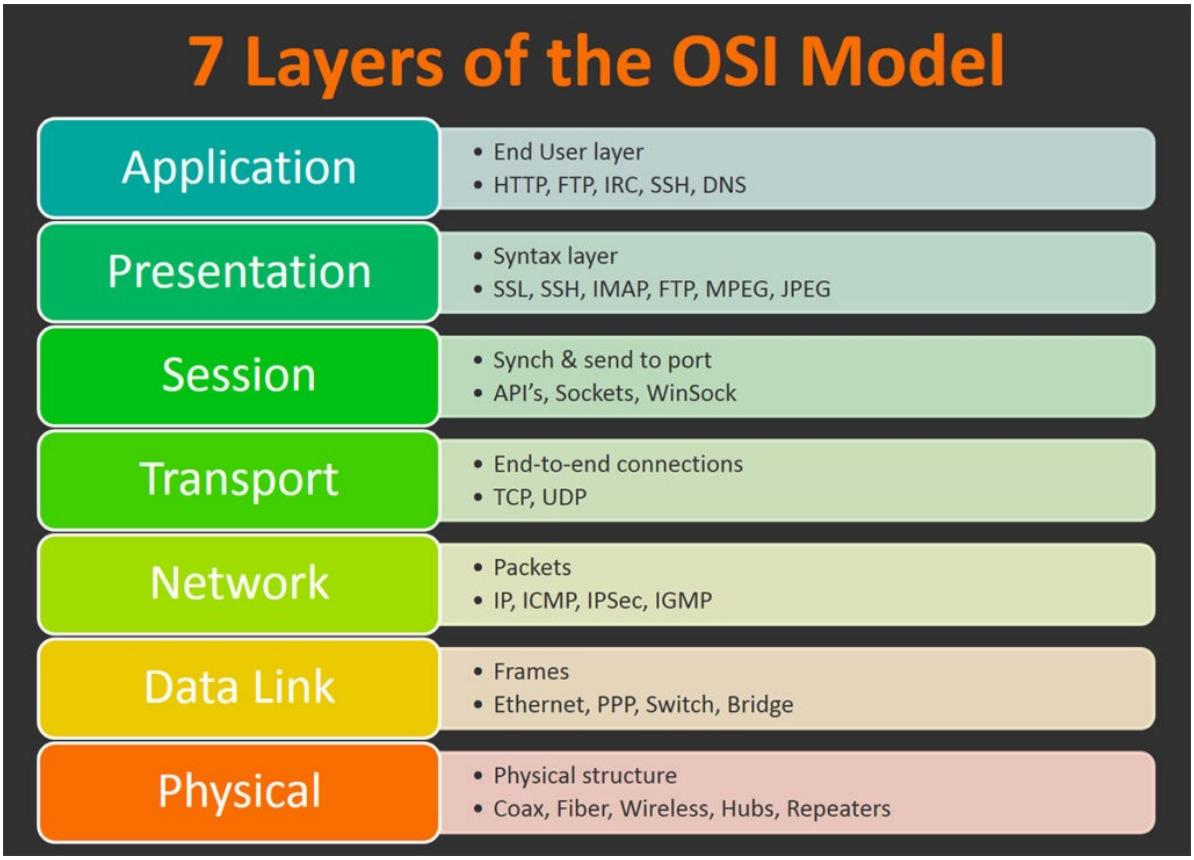
Network and Recon Masterclass from DaVinciCode

Clovis Carlier / Joytide - 27/10

OSI Model



Wireshark

- Most used tool to:
  - Capture packet
  - Display network captures (-> Often very useful in Forensics!)
- Example: IP addr (Layer 3), MAC addr (Layer 2) + Network interfaces

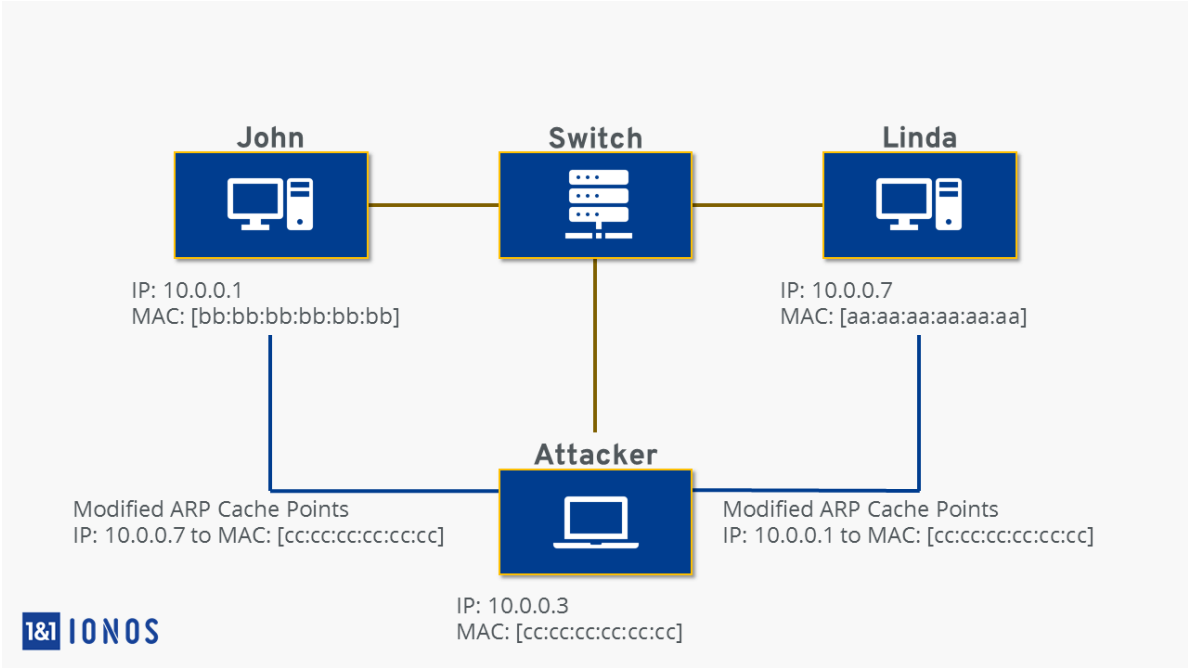
```
ip a
```

ARP

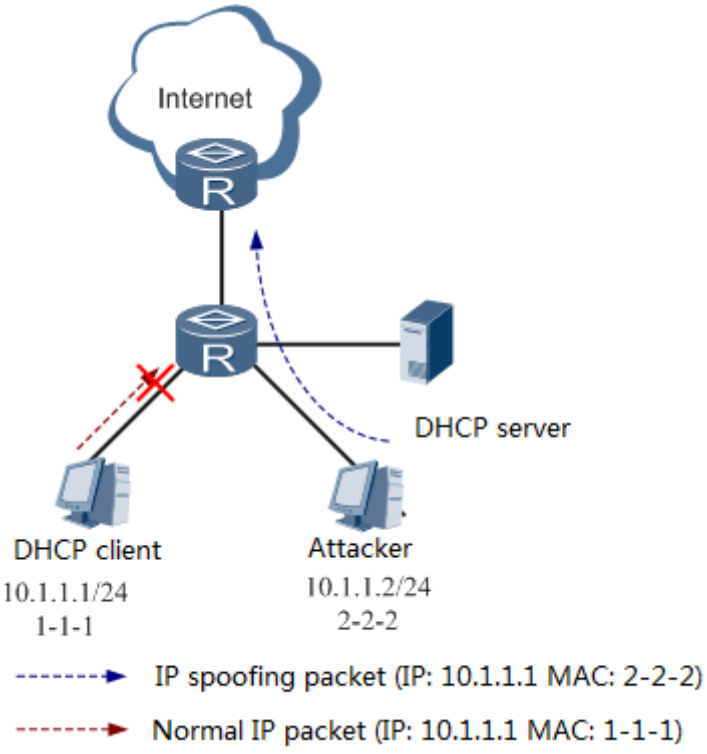
- Link between layer 2 and 3: assign a MAC to an IP

```
arp -a
arp -d
arp -a
```

- Vulnerable to ARP Cache Poisoning (MiTM):



- Another common spoofing attack: MAC Poisoning



Application Layer

DHCP

- Dynamic Host Configuration Protocol
- Gives IP to client on a network

Can be done manually:

```
#Create a network interface
ifconfig eth0 192.168.43.226
ifconfig eth0 netmask 255.255.255.0
ifconfig eth0 broadcast 192.168.43.255
#Add it to routes
route add default gw 192.168.43.1 eth0
```

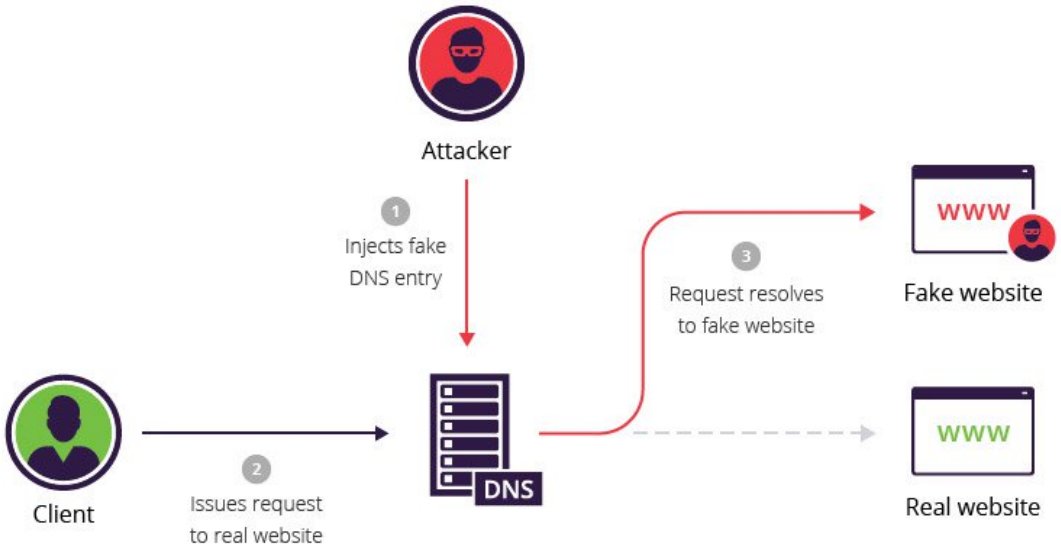
DNS

- Domain Name System
- Often public and managed by big company (Google: 8.8.8.8 and 8.8.4.4), manually added to: `/etc/resolv.conf`
- Assign an IP to a domain name

```
nslookup -type=txt dvc.tf 8.8.8.8
dig @8.8.8.8 dvc.tf TXT
```

- Record DNS: ANY, A, TXT...

DNS Spoofing/Cache poisonning/Hijacking



Zone transfers:

```
dig axfr @$(DNS_IP) $(DOMAIN.COM)
```

Reconnaissance

Nmap

Full in depth port scan

```
sudo nmap -sC -sV -oA box $(ip)
```

Full port scan

```
sudo nmap -p- -v -oA box_allports $(ip) # add --min-rate 1000/10000 if needed
```

In depth port scan :

```
cat allports.nmap | grep open | awk -F/ '{print $1}' | sed-z 's/\n/,/g;s/,$/\n/'
#For open ports
sudo nmap -sC -sV -oA box $(ip) -p $(ports)
```

UDP port scan:

```
sudo nmap -sU -oA box_udp $(ip)
```

sTTL

```
ping $(ip)
# ttl<127   => Windows
# ttl<64    => Linux, BSD, IoT...
# ttl<256   => Network infrastructure, like a cisco router
```

Subdomain enumeration

```
gobuster vhost -u https://dvc.tf -w /opt/SecLists/Discovery/DNS/subdomains # For
subdomains discovery as sub.domain.htb
```