Network101

Introduction to network concepts and vulnerability

DaVinciCode

27/10/2021

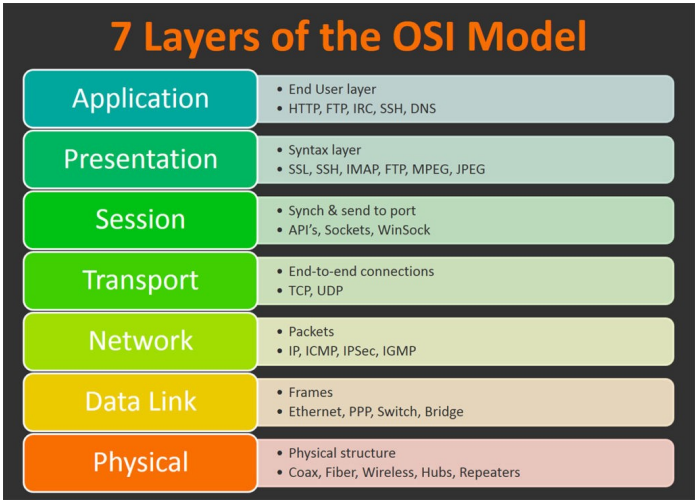
whoami

- Clovis
- A5 IOS
- Co-Founder and VP of DaVinciCode

Network

- OSI Model?
- Addresses???
- ARP, DNS, DHCP, DNS??????

OSI Model


7 Layers of the OSI Model
Application
• End User layer
• HTTP, FTP, IRC, SSH, DNS
Presentation
• Syntax layer
• SSL, SSH, IMAP, FTP, MPEG, JPEG
Session
• Synch & send to port
• API's, Sockets, WinSock
Transport
• End-to-end connections
• TCP, UDP
Network
• Packets
• IP, ICMP, IPSec, IGMP
Data Link
• Frames
• Ethernet, PPP, Switch, Bridge
Physical
• Physical structure
• Coax, Fiber, Wireless, Hubs, Repeaters

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

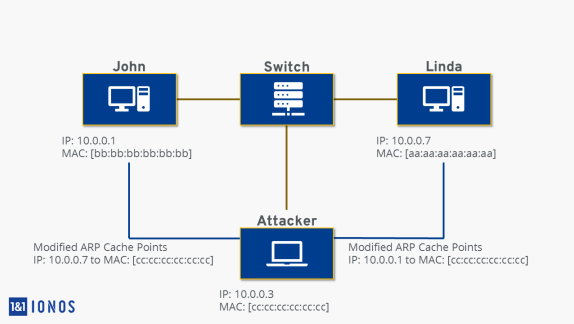
```
ip a
```

ARP

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

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

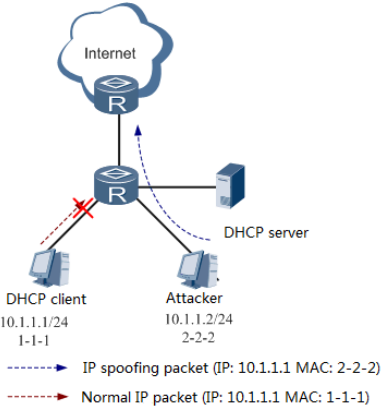
- Vulnerable to ARP Cache Poisoning (MiTM):



ARP

- Another common spoofing attack: MAC Poisoning

Poison the ARP table of the router to spoof with the attacker MAC address of a legitimate connection.



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
```

Application Layer

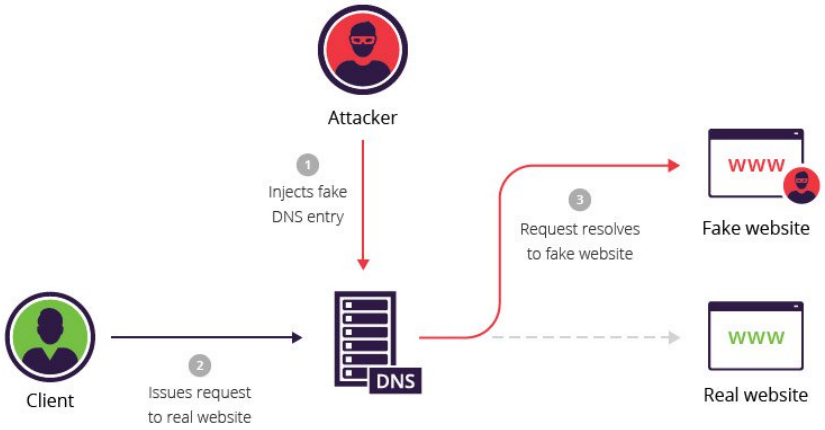
DNS

- 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

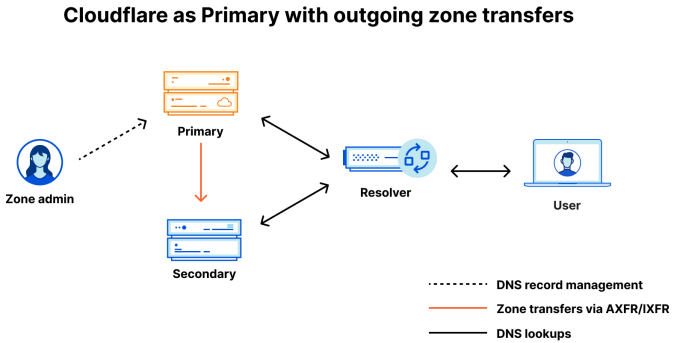
```
nslookup -type=txt dvc.tf 8.8.8.8
dig @8.8.8.8 dvc.tf TXT
```

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

DNS Spoofing/Cache poisonning/Hijacking



DNS Zone transfers:




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

Recon

Nmap

Full in depth port scan

```
sudo nmap nmap -SCV -vv -oA box $(cat ip)
# Add -sT (TCP Connect) to avoid firewall flagging you as a bot who
# only does 2 step of tcp handshakes
```

Full port scan

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

UDP port scan:

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

Recon

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
```