# COMPROMISED COFFEE SHOP CONNECTIONS

Another

**Al Dente Worms**

Production

*featuring:*

David Tran

Greg Kuhn

Anthony Williams

Andrew Sessions

# INTRODUCTION & OVERVIEW

- Public Wi-Fi is a very available means of connecting to the internet, but we know that it can be risky.
- Here ADW demonstrate one way your information might be compromised when accessing public internet connection:
- a ***rogue, evil-twin Wi-Fi network***

# ROGUE, EVIL-TWIN WI-FI? *WHAT'S THAT?*

**Rogue access points** are insecure devices that redirect your connection to the hacker's access point instead.

**Evil twin Wi-Fi networks** are duplicate wireless networks set up by hackers to appear identical to another original network.

# RISKS CONNECTING TO ROGUE NETWORKS

Most public Wi-Fi networks you'll connect to will be open and unencrypted

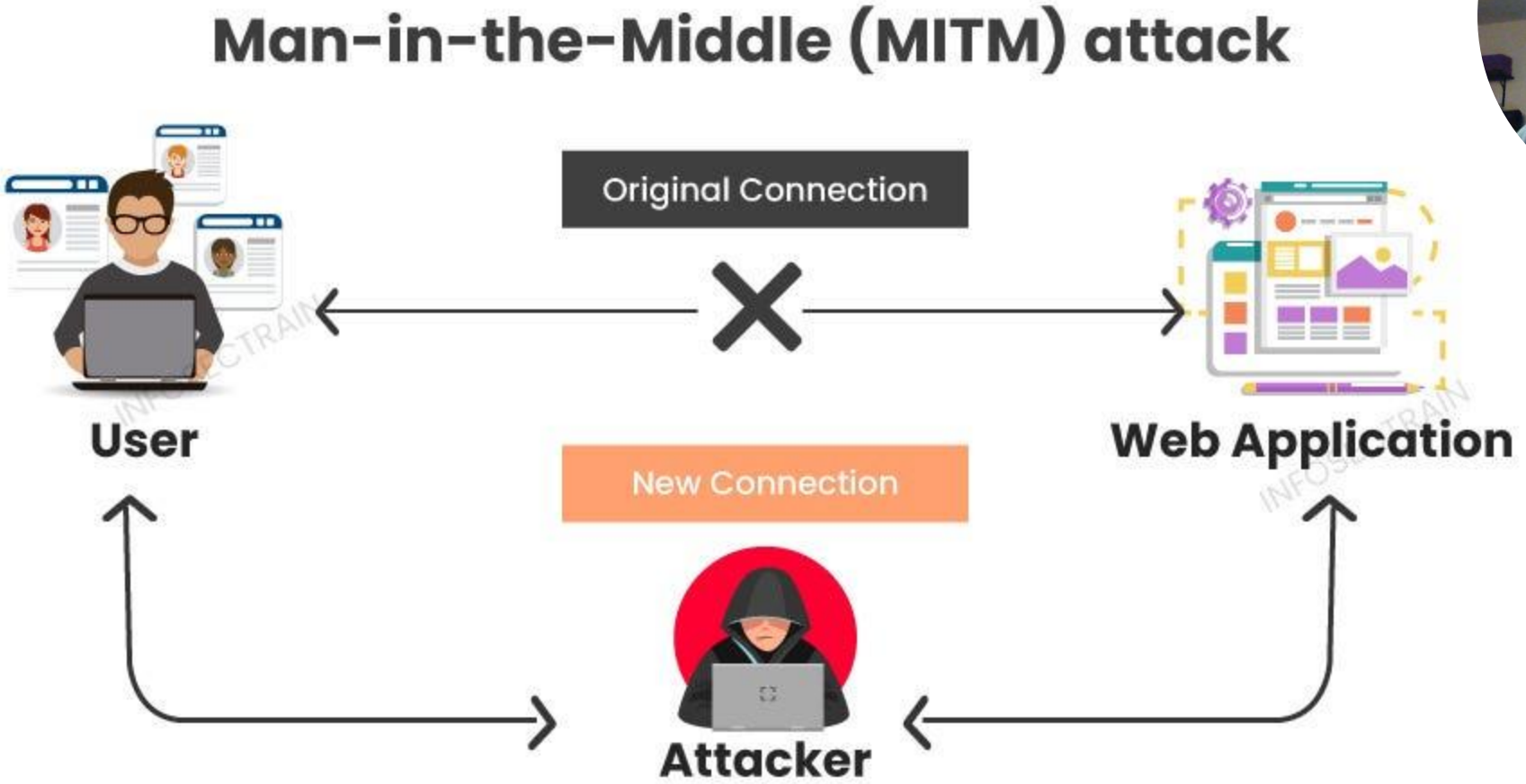
Anyone can connect and scan the network for other clients

One big risk lies in the exposure to packet sniffers, like wireshark

These allow 'sniffers' to read any unencrypted data transmitted

From the hackers POV, this presents an opportunity to freely access your info

Some software manipulates traffic as you send it


Man-in-the-Middle (MITM) attack
Original Connection
User
Web Application
New Connection
Attacker
[Man-in-the-Middle (MITM)]

[2]

# WHAT DATA ARE HACKERS LOOKING FOR

- Local IP and device MAC addresses sent to establish connections
- Port information can be sniffed through SYN scanning
- Usernames and passwords sent to authorize website logins

Burpsuite focuses on HTTP(s) traffic to the web

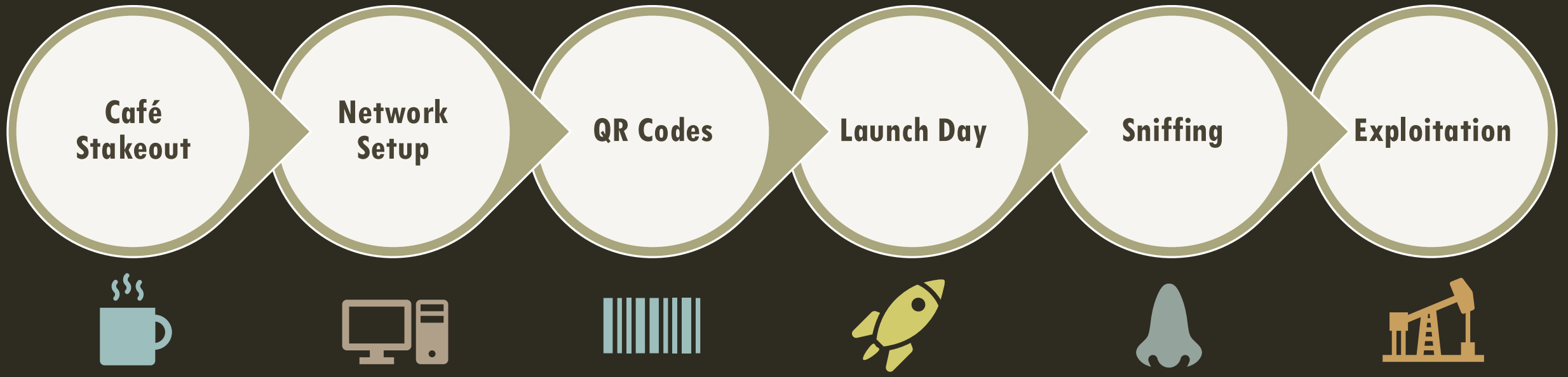
- Interrupting
- Capturing
- Modifying

# COFFEE SHOP CAFÉ CASE STUDY

(actions such as these are often illegal and should only be undertaken in controlled environments.)

**Scenario**: the *Al Dente Worms* hacker group seeks to capture data from patrons at the local café, Steamy Beans Coffee.

# TIMELINE OF EVENTS




CYBER KILL CHAIN STAGES:

Reconnaissance → Weaponization → Delivery → Exploitation → Actions on Objectives [4]

# TOOLS OF THE TRADE

- QR code generation – **QtQr**
- Build & broadcast the network – **Linux WiFi hotspot**
- Deauthentication Attacks software – **Airgeddon**
- Packet sniffing – **Bettercap** & Wireshark

# TOOLS OF CRAFTING QR CODES

Quick-response codes are 2-D matrix barcodes

- Denso Wave in 1994

Codes can link your device to protected networks

Build you own online

- qr-code-generator.com
- qrcreator.com
- myqrcode.com
- qr.io, etc.

or using free software

- qtqr for linux

# TOOLS OF CRAFTING QR CODES

Quick-response codes are 2-D matrix barcodes

- Denso Wave in 1994

Codes can link your device to protected networks

Build you own online

- qr-code-generator.com
- qrcreator.com
- myqrcode.com
- qr.io, etc.

or using free software

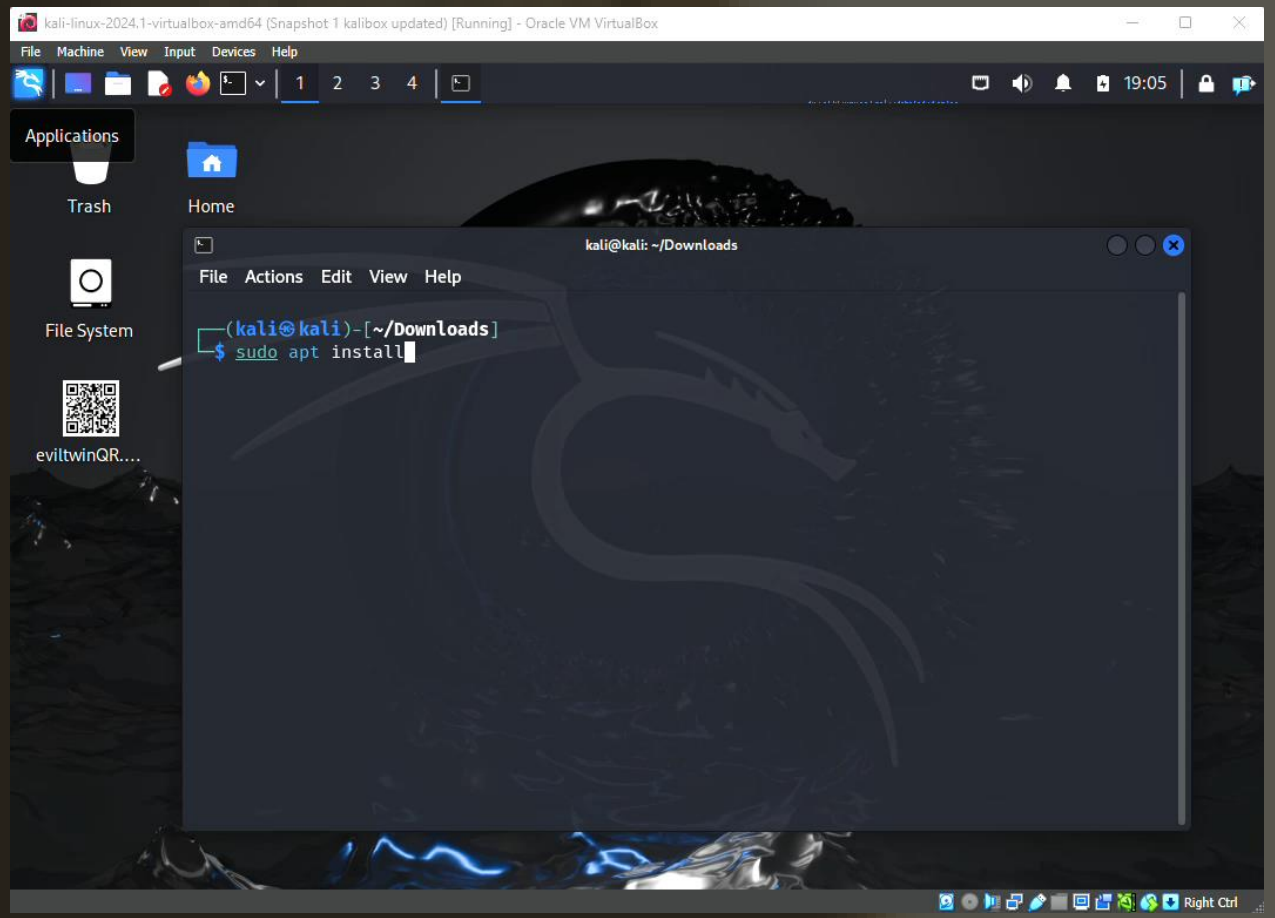
- qtqr for linux

# TOOLS OF CRAFTING QR CODES

QtQr is a free software for customizing QR codes on linux

This demo goes through

- Install / opening
- Create / export
- Decode / edit existing



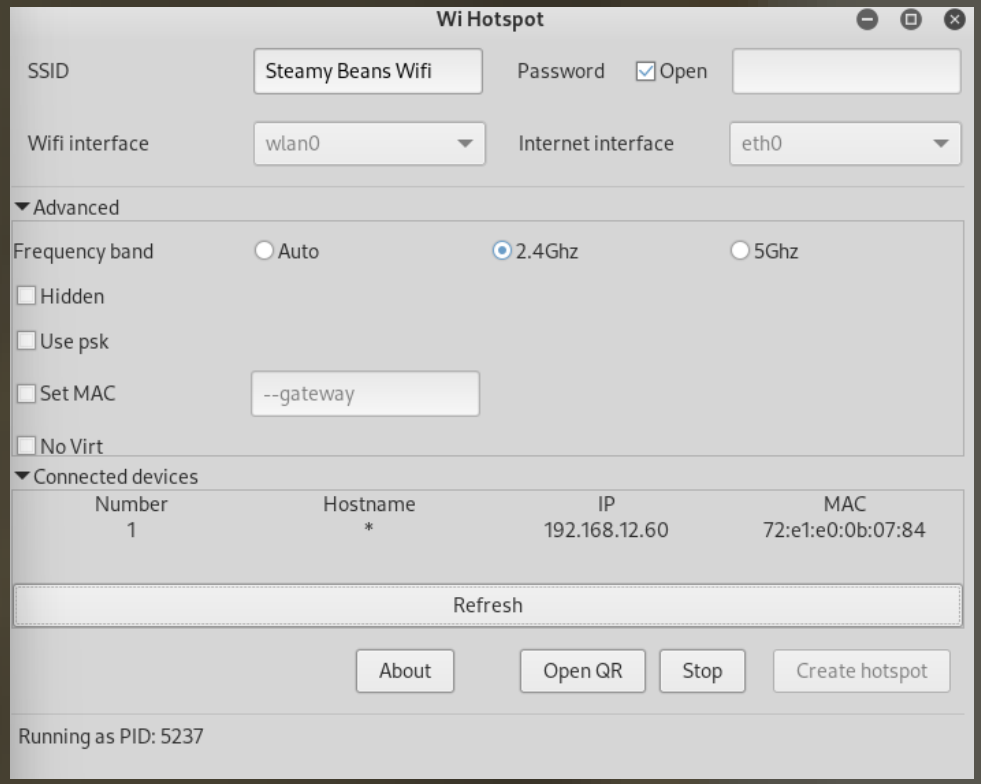
# TOOLS OF BROADCASTING A NETWORK

## Software

- Airgeddon
- Bettercap
- Linux-wifi-hotspot

## Hardware

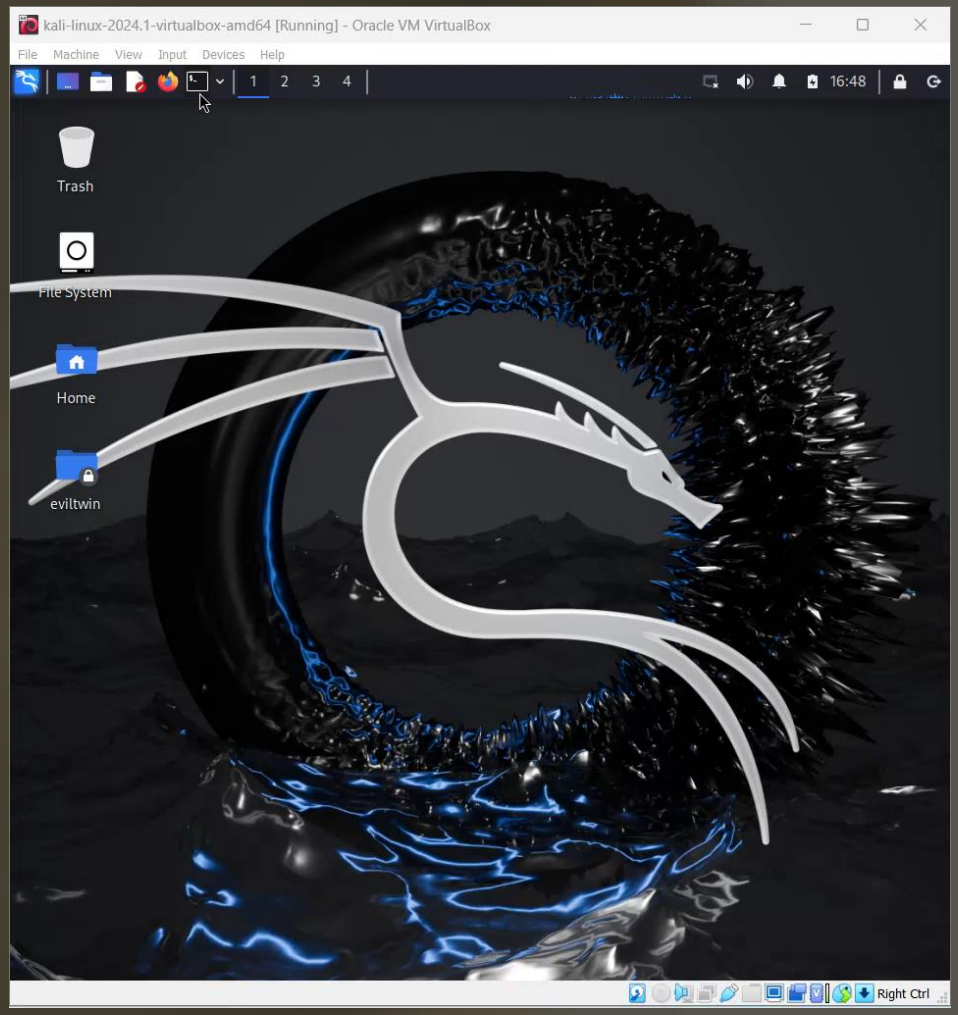
- A wireless router
- A Wi-Fi antenna dongle
- Simply a cell phone



# TOOLS OF BROADCASTING A NETWORK

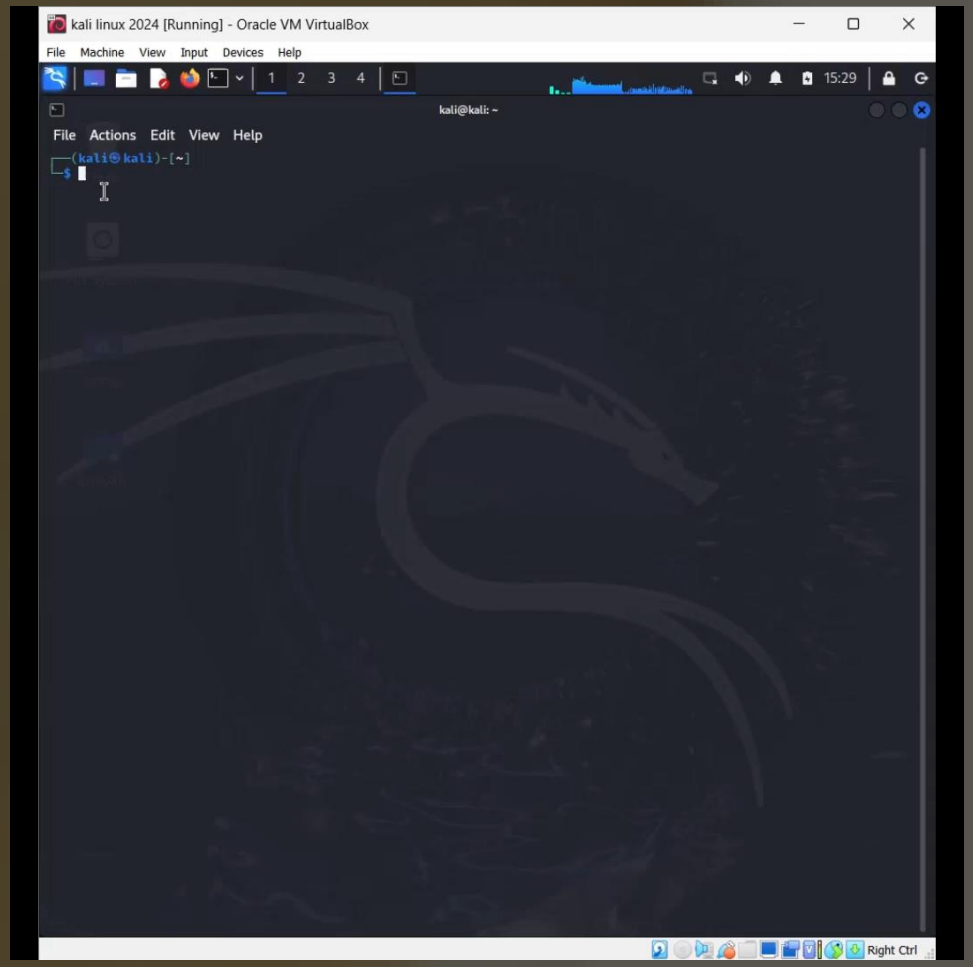
Linux wifi hotspot

- Wireless antenna
- Customizes
- SSID & Password
  - Encryption type



# TOOLS OF DE-AUTHENTICATION

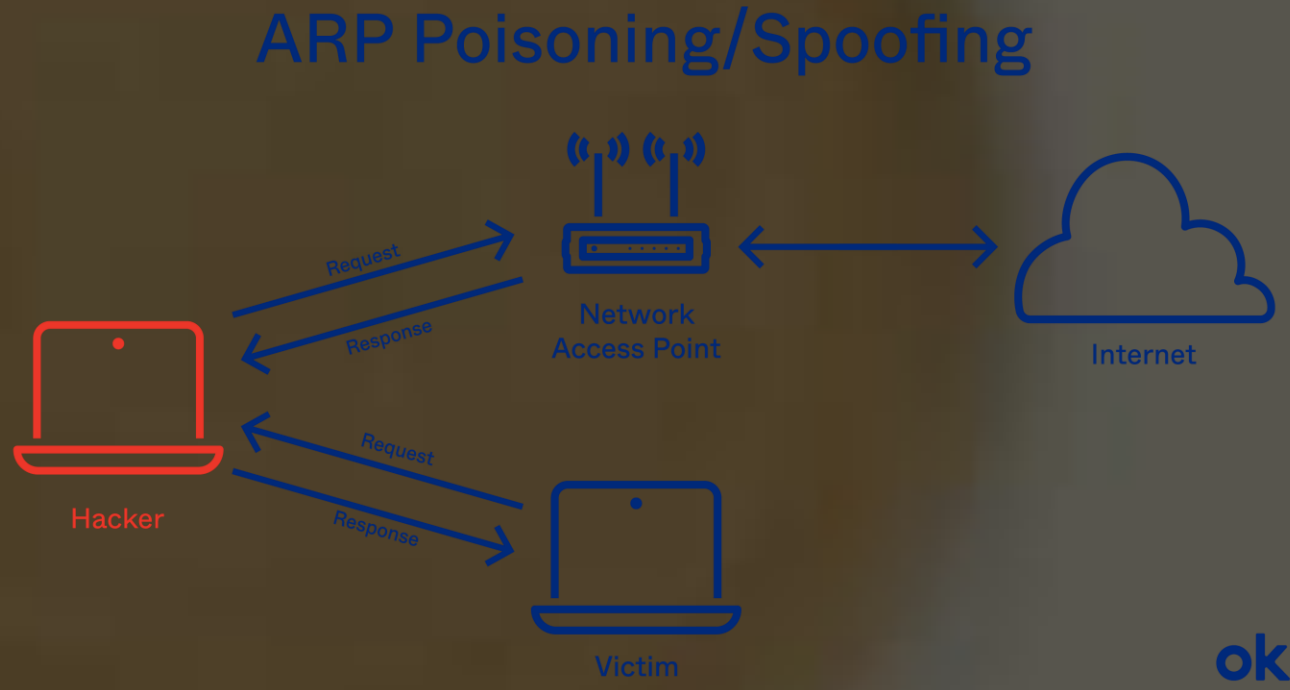
- ‘DEAUTH’ attack force devices off a network,
- Airgeddon is one software capable of launching deauth/disassociate attacks as shown in the example.
- Airgeddon is a combination of many common hacker tools such as (aircrack, airmon, airodump, etc.)
- ADW could also use this tool to crack encryption keys for networks as well as send phishing messages to gain the real APS network password.



# TOOLS OF DATA SNOOPING

ARP poisoning

Is a cyberattack that involves a hacker sending fake ARP (Address Resolution Protocol) messages to a network to associate the hacker's MAC address with the IP addresses of other devices. This Allows threat actor to act as a man in the middle and incept traffic by essential disguising itself as the victim to receive the same traffic as the victim.

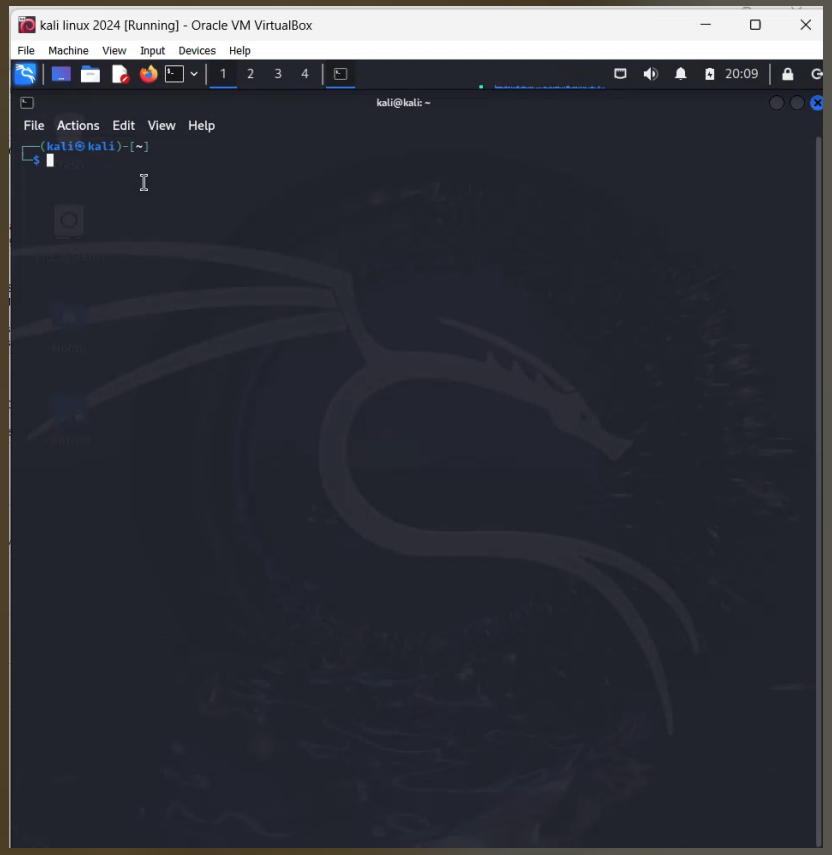


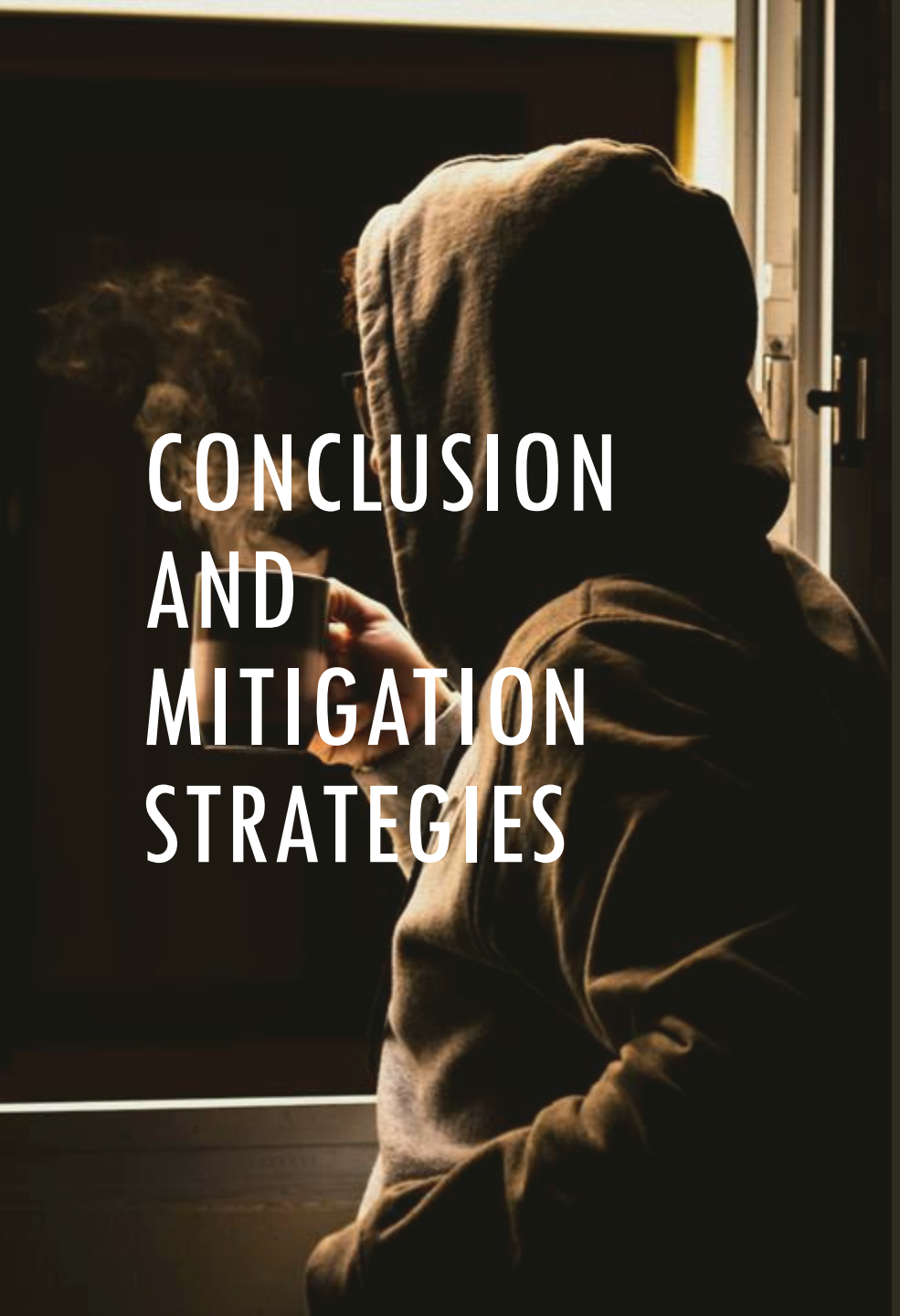

[5]

# TOOLS OF DATA SNOOPING

## Bettercap

- A tool used to run a ARP poison and sniff packets
- Being sent out from a certain device.





# CONCLUSION AND MITIGATION STRATEGIES

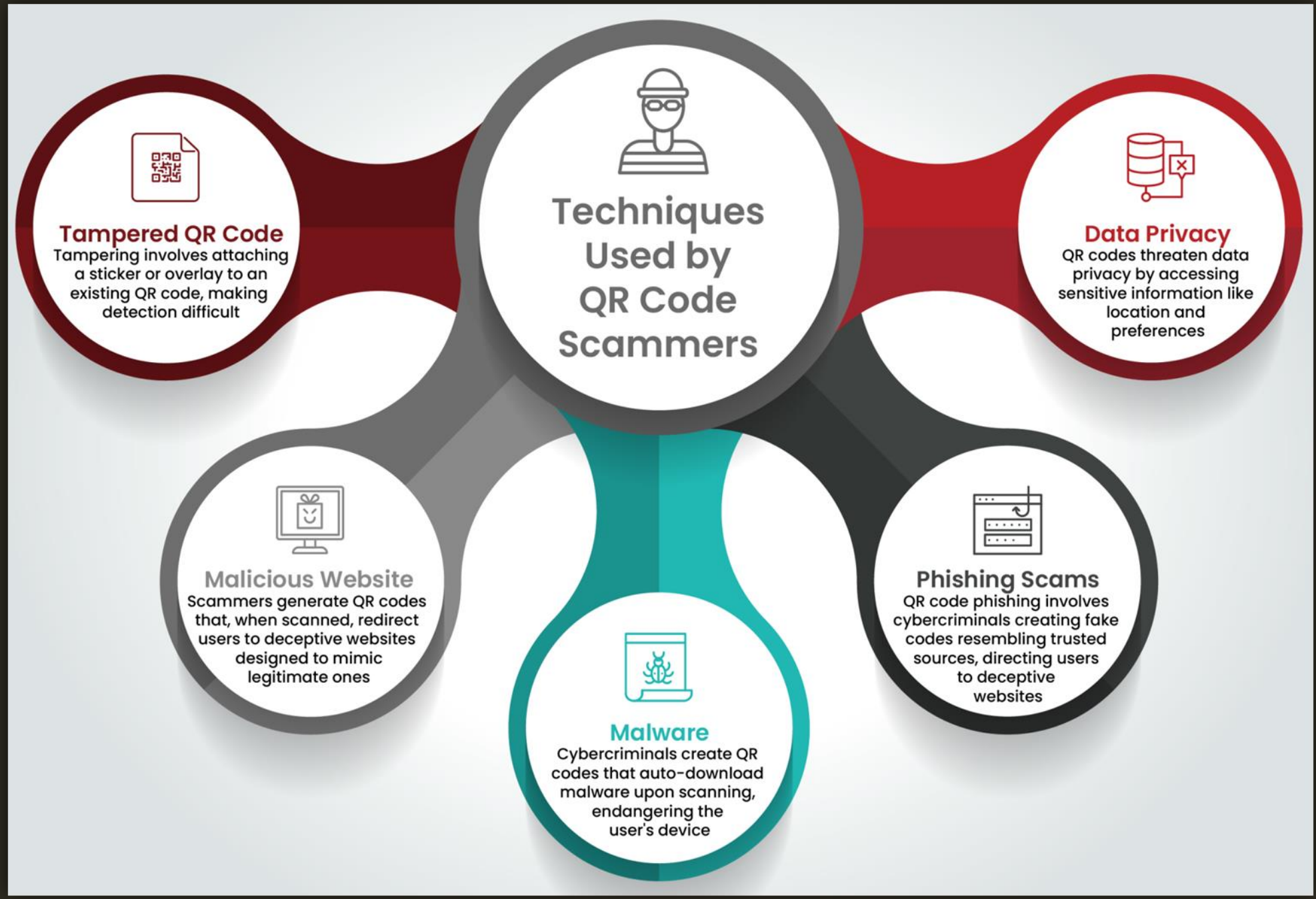
There'll always be risks connecting to public Wi-Fi networks…

**#1** mitigation strategy:

VPNs to encrypt all traffic.

Keep on lookout for SSL cert authenticity and HTTPS connection

Do NOT input sensitive data or personally identifiable information


Techniques Used by QR Code Scammers
Tampered QR Code
Tampering involves attaching a sticker or overlay to an existing QR code, making detection difficult
Data Privacy
QR codes threaten data privacy by accessing sensitive information like location and preferences
Malicious Website
Scammers generate QR codes that, when scanned, redirect users to deceptive websites designed to mimic legitimate ones
Phishing Scams
QR code phishing involves cybercriminals creating fake codes resembling trusted sources, directing users to deceptive websites
Malware
Cybercriminals create QR codes that auto-download malware upon scanning, endangering the user's device

[3]

# Top Tips to Protect Yourself when using QR Codes

## Check the Source

If scanning a QR code, check if it comes from an authorised source. It would help if you had visual clues like a company logo or branding to ensure the information is authentic.

## Avoid Public Wi-Fi

Avoid using public Wi-Fi networks for scanning QR codes, as they are typically unprotected and vulnerable to hackers.

## QR Codes Readers

Select a QR code reader with built-in security features that can detect and block malicious QR codes for enhanced protection.

## Destination Verification

Prior to scanning a QR code, verify the displayed destination URL to ensure it aligns with your expectations.

## Regular Updates

Regularly update your device's security software and operating system.


## Check the URL

Double-check the URL to ensure it's the correct site after scanning the QR code. A hacker can design fake websites that look exactly like genuine ones but have slightly altered URLs.

## Dynamic QR Codes

Dynamic QR codes enhance security by allowing real-time updates to information, making them ideal for businesses needing to modify destination URLs and other data regularly.

## Trusted Code Source

Exercise caution by exclusively scanning QR codes from sources you trust and are familiar with, such as reputable companies or individuals you recognise.

## Tampered Codes

Steer clear of scanning QR codes that exhibit signs of tampering, alteration, or any other suspicious modifications.

[3]

# FROM THE VENDORS POV

- Keep customers well-informed of your network SSID
- Rotate your credentials
- Implement network security measures, e.g.:
  - Update to WPA3
  - Intrusion Detection/Prevention Systems
- Regularly monitor for rogue wireless networks

Questions

Comments

Concerns

# THANKS FOR LISTENING

# CREDITS


[1] MakeUseOf. (n.d.). 5 Ways Hackers Can Use Public Wi-Fi to Steal Your Identity. Retrieved from https://www.makeuseof.com/tag/5-ways-hackers-can-use-public-wi-fi-steal-identity/

[2] InfosecTrain. (2023, June 16). What is a Man-in-the-Middle (MITM) Attack? - InfosecTrain - Medium. Medium. https://medium.com/@Infosec-Train/what-is-a-man-in-the-middle-mitm-attack-e807408baa38

[3] Weldrick, T. (2023, November 9). From convenience to vulnerability: Understanding the security risks of QR codes. OneCollab. https://www.onecollab.co.uk/news-and-insights/from-convenience-to-vulnerability-understanding-the-security-risks-of-qr-codes/

[4] Lockheed Martin. (n.d.). Cyber Kill Chain. Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[5] Okta. (n.d.). ARP Poisoning. Retrieved [Date You Accessed The Webpage], from https://www.okta.com/au/identity-101/arp-poisoning/