Inside the Castle

Using Aircrack-NG to Gain Access to Exploit IOT Devices

By: Alex Ioannou, Brian Martin, Divya Kamath, Owin Garrie, Paul Lindsay, and Walid Tazi

Objective

- Demonstrate the importance of strong wifi security (passwords and protocols) as a personal security perimeter.

Methodology

- Crack WPA standard security by attacking a host on a network
- Run a deauthentication attack to capture a four way handshake
- Perform reconnaissance with nmap and determine exploitable Vulnerabilities

Introduction to Aircrack Suite

Aircrack suite is a network software consisting of tools for assessing wi-fi network security, it focuses on monitoring, attacking, testing, and cracking wireless networks.

Key Features:

- Able to capture packets and analyze them to asses network vulnerabilities.
- WEP and WPA/WPA2-PSK cracking: Aircrack-ng is capable of cracking both WEP and WPA/WPA2-PSK encryption protocols.
- Deauthentication attacks: Aircrack-ng can perform deauthentication attacks to force clients to disconnect from wifi network’s.
- Wifi traffic injection: allows for injecting arbitrary packets into wifi networks, which can be used for various testing purposes

Why Aircrack?

- Attacks are cheap and easy to perform
- 95% of Canadian homes have Wifi (Stats Canada)
- Wi-Fi is usually the perimeter between the internet and home network
- Once an intruder gains access to your network they can effectively impersonate you

https://ised-isde.canada.ca/site/high-speed-internet-canada/en

What is WPA (Wi-Fi Protected Access)?

- Wi-Fi Protected Access is a security standard for computing devices equipped with wireless internet connections.
- WPA is more secure than WEP (Wired Equivalent Privacy) because it uses a 256-bit key for encryption, which is a major upgrade from the 64-bit and 128-bit keys used by the WEP system.
- WPA2 introduced the Advanced Encryption System (AES) to replace the more vulnerable system used in WPA.
- For the purpose of this project, we will focus on WPA.

What are Wi-Fi security protocols?

- Wi-Fi security protocols use encryption technology to secure networks and protect the data of their clients.
- Wi-Fi security protocols use cryptographic keys to randomize data to make it undecipherable. Since Wi-Fi systems use symmetrical encryption, the same key is used to encrypt and decrypt data.
- There are four wireless security protocols currently available: WEP, WPA, WPA2 and WPA3.

Components and Tools

Aircrack-ng suite consists of several tools including:

- airodump-ng : Packet capture tool for wifi networks
- aireplay-ng: Packet injection and manipulation tool
- aircrack-ng: WEP/WPA/WPA2-PSK cracking tool
- airbase-ng: Virtual access point implementation tool
- airmon-ng: Script for managing wireless interfaces.
- airdecap-ng: Decryption tool for encrypted wireless captures

Concepts Involved with Aircrack-ng

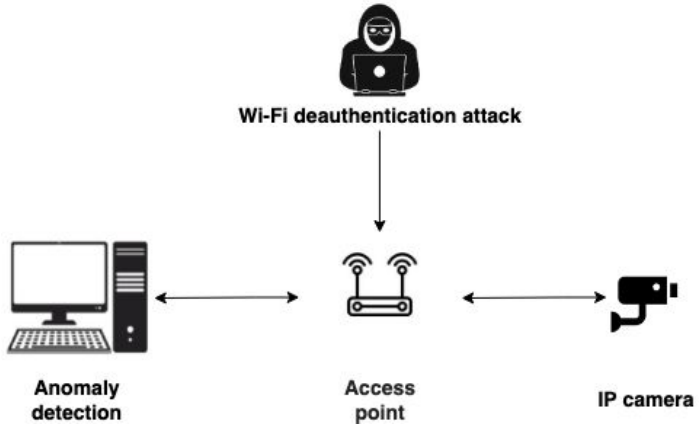
- Offensive security - In discussing the mitigation of this attack we are engaging in vulnerability assessment
- Networking - Understanding of the OSI layers to capture router packets (Router works on layer 3 the network layer and layer 2 data-link layer)
- Cryptography - using aircrack-ng to crack WPA hashes

Deauthentication attack

A router will send a deauthentication packet unencrypted, the router then wants to terminate the connection (kicked out, changed password, inactivity etc).

- “From: router, To:you, Message: disconnect from me”

We need to understand the identity (MAC address) the client will disconnect and then if set to auto connect will try to reconnect to the network, this is when the handshake occurs.



Aircrack Suite VS Weak Wi-Fi Security

- The first step in attacking devices on a network is gaining access to said network.
- The following demo will illustrate how to capture a 4-way handshake between a router (my personal router) and client a device (my personal iPhone) for the purpose of cracking a WPA-level encrypted passphrase.
- IMPORTANT! All subsequent devices and networks attacked in the demos are OUR OWN!
- There is a significant difference in security level between WPA and WPA2
- We will demonstrate how quickly a WPA-level encrypted passphrase can be cracked with the right information and tools.
- Context: Wi-Fi security is on your front line of defence against potential attackers. It is important not to underestimate the importance of using WPA2 vs WPA.
- This demo is the first step in showcasing what damage can be done if an attacker gains access to your password protected network.

Technical Terms

External Network Adapter - USB device that picks up Wi-Fi signals.

Client - Any device connected to a network.

De-Authenticate - Kicks connected clients off a network, forcing them to reconnect if they want to keep using this Wi-Fi signal.

Aircrack Suite - Collection of Linux based tools used for ethical hacking.

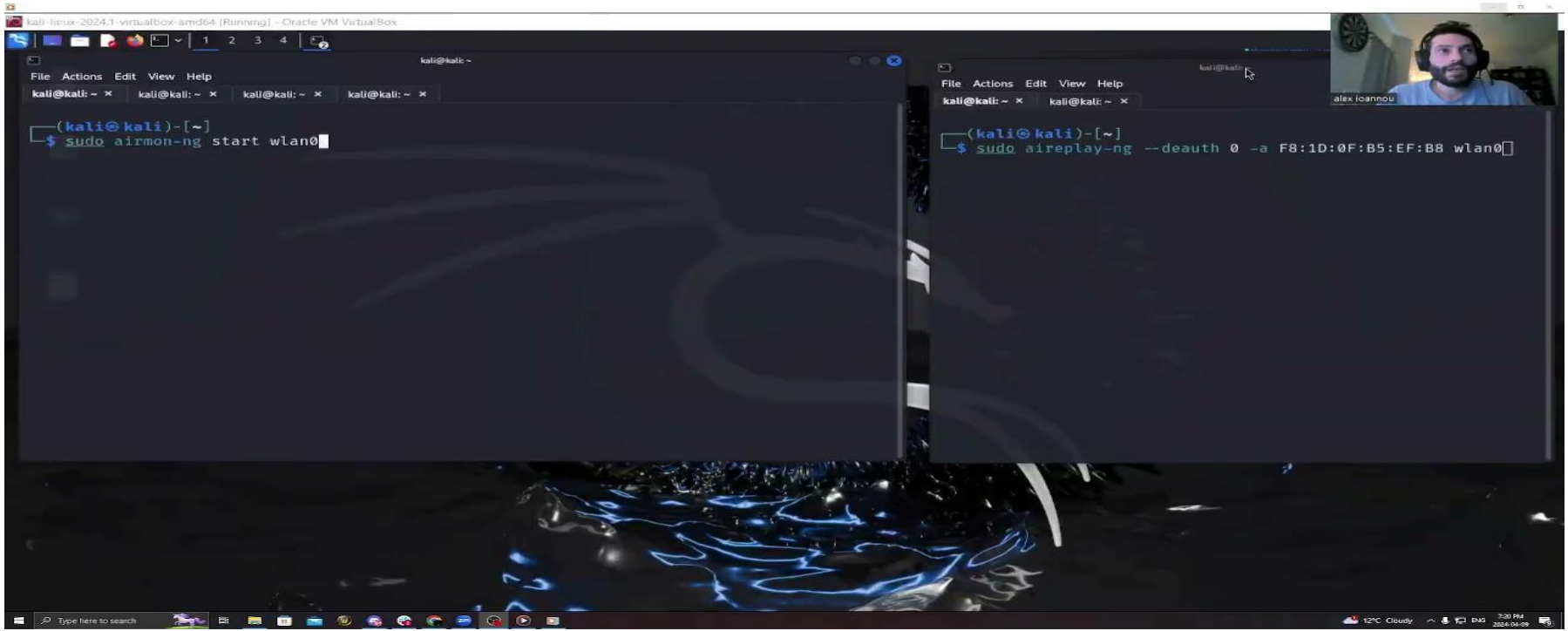
Kali Linux - Linux distribution used primarily by ethical hackers/penetration testers.

WPA & WPA2 - Refers to the encryption(security) level associated with a Wi-Fi network

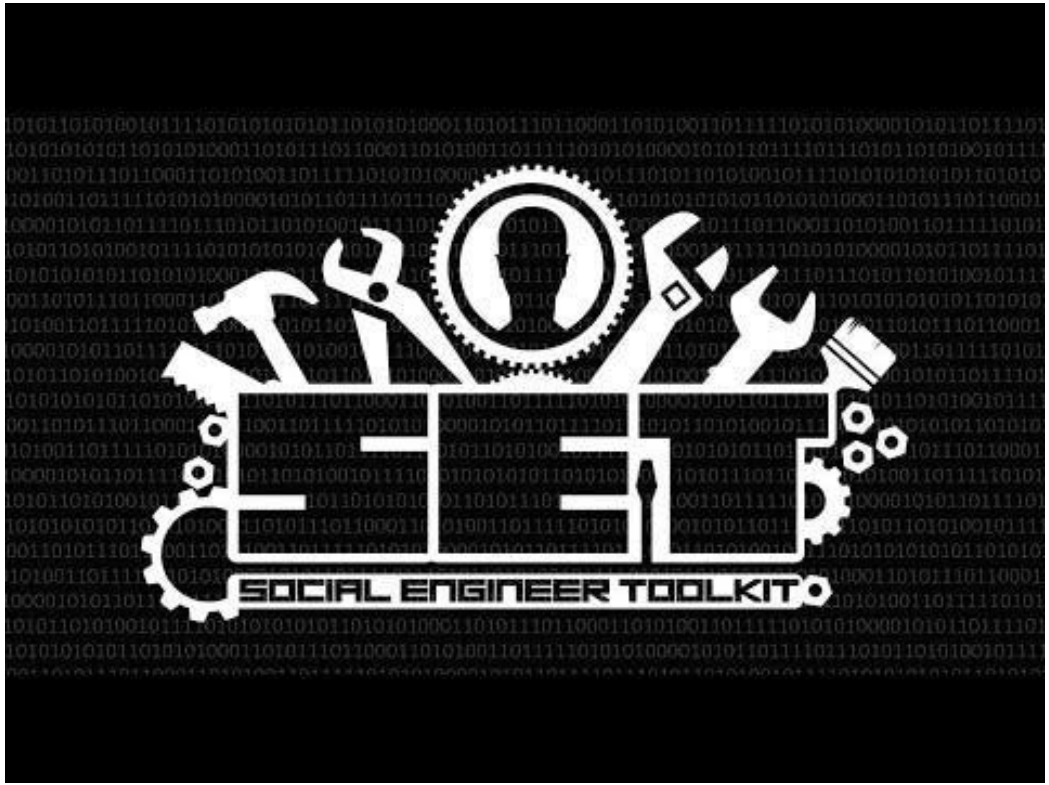
Usage Scenarios

- Aircrack-ng is commonly used by penetration testers, security researchers, and network administrators to:
- Assess the security of Wi-Fi networks.
- Perform penetration testing and vulnerability assessments.
- Conduct security audits and compliance checks.
- Investigate Wi-Fi-related security incidents and breaches.

Gaining Access



Inside the Castle: Social Engineering Toolkit (SET)



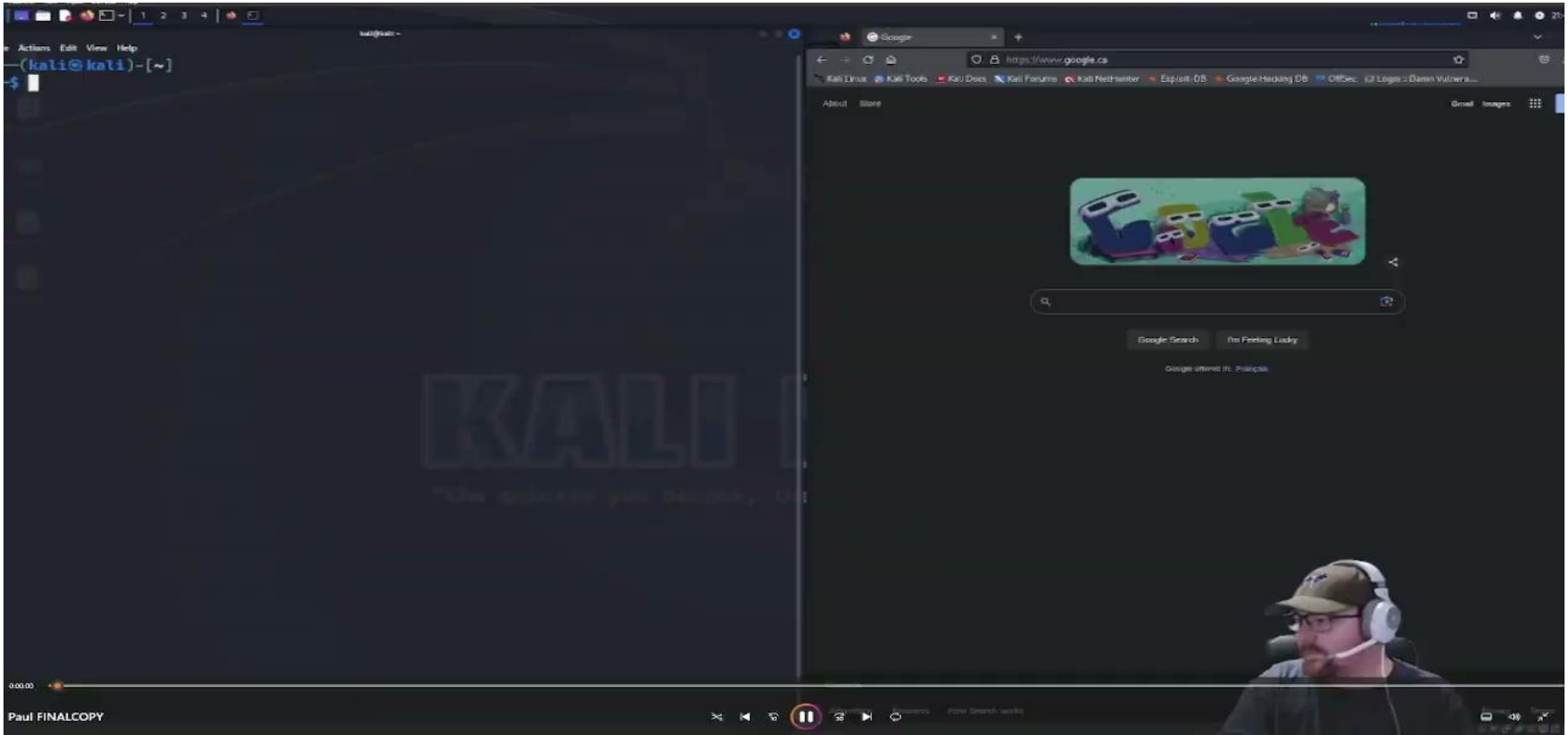
Why Use the SET (Social Engineering Toolkit)?

- Phishing is one of the most prevalent cyber attack methods
- General population needs to be educated on spotting and dealing with phishing scams
- Individuals do not need large amounts of technical knowledge to utilize these attacks against home networks

Concepts Involved with Social Engineering

- Credential Farming - Malicious actors trying to collect/exploit as many credentials possible
- DNS spoofing - Victim believes they are on a legitimate website (they are on a fake page made by the attacker to extort credentials)
- Phishing - attack aimed at revealing personal information through illegitimate web surfing

Credential Farming

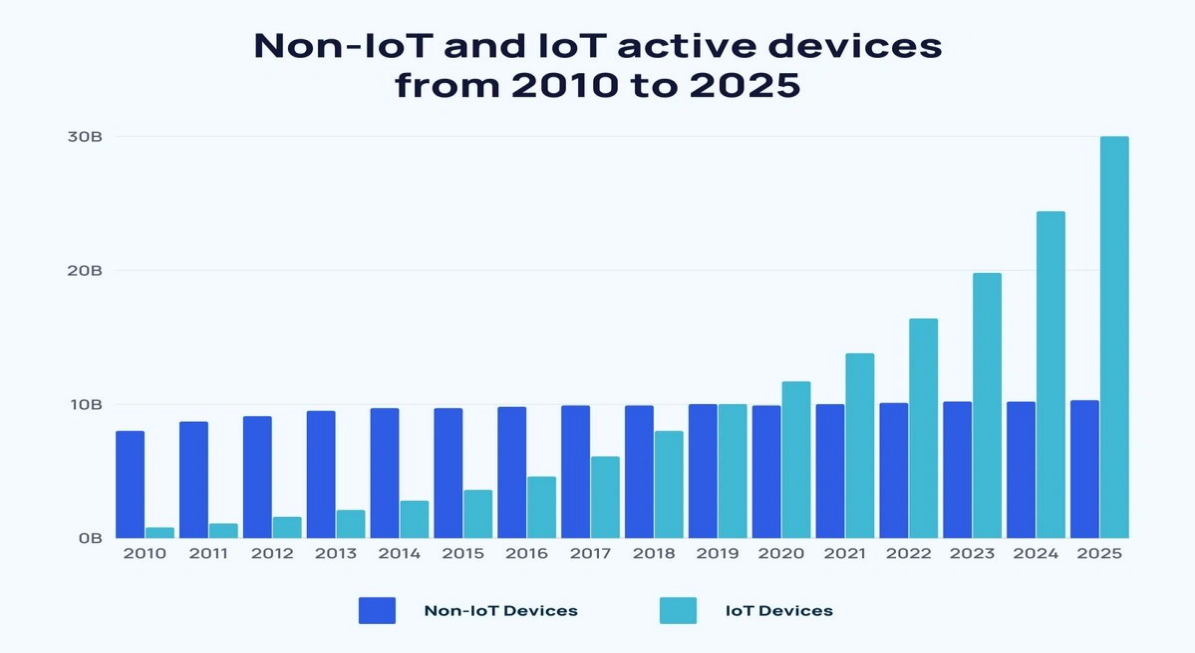


IOT as a Threat Surface

- Home networks typically have 2-3 more devices attached than people realize.
- Manufacturers optimize for ease of use, often at the expense of security.
- Many devices aren’t configured to update automatically and aren’t actively managed by owners.
- Hardware issues can’t be fixed and firmware is often difficult to update, resulting in long term vulnerabilities.

https://www.telecompetitor.com/report-people-underestimate-number-of-iot-devices-in-their-homes/

Growth of IOT Threat Surface



https://explodingtopics.com/blog/iot-stats

Analysis of IOT Malware - Khoury et al 2019

In a 2019 Concordia paper analysing IOT Malware, Khoury et al determined:

- Majority of IOT exploits targeted DOS. (19 of 28 malware families)
- Network access was the most common method.
- 93.8% of the exploits required no human intervention.
- Exploits used for IOT malware are generally less complex to implement.
- Exploits used for IOT malware are higher impact on average.

https://users.encs.concordia.ca/~abdelw/papers/fps20_iot_preprint.pdf

IOT Weaknesses

Khoury et al determined in their research that the Top 6 CWE's were:

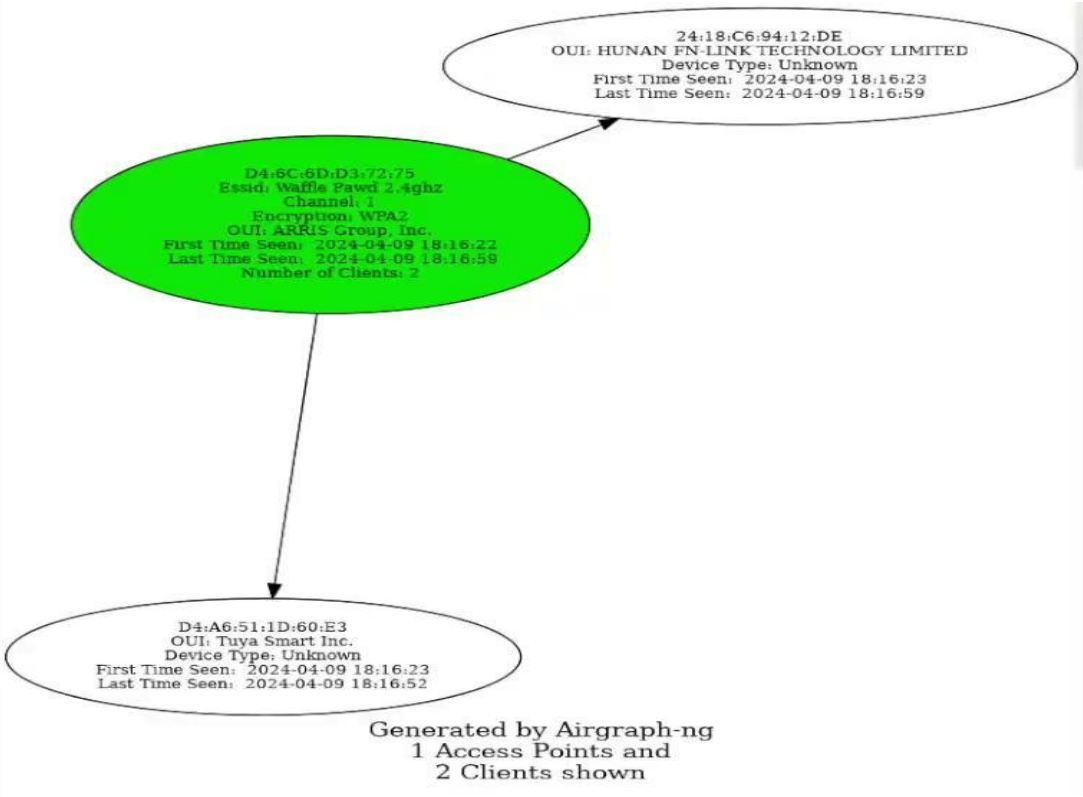
- CWE-20 Improper Input Validation
- CWE-94 Improper Control of Generation of Code
- CWE-78 Improper Neutralization of Special Elements used in an OS Command
- CWE-77 Improper Neutralization of Special Elements used in a Command
- CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer
- CWE-287 Improper Authentication

Distributed Denial of Service (DDoS)

IoT-driven DDoS attacks are a type of cyber attack that targets IoT devices, exploiting their vulnerabilities and using them to flood and overwhelm a victim's system, causing disruption and damage.

- Attacker can force the greater volume of machine to execute a seriously disruptive attack
- Location of where the attack is coming from is very difficult to pinpoint.
- It is a much harder task to shut down multiple machines at once.

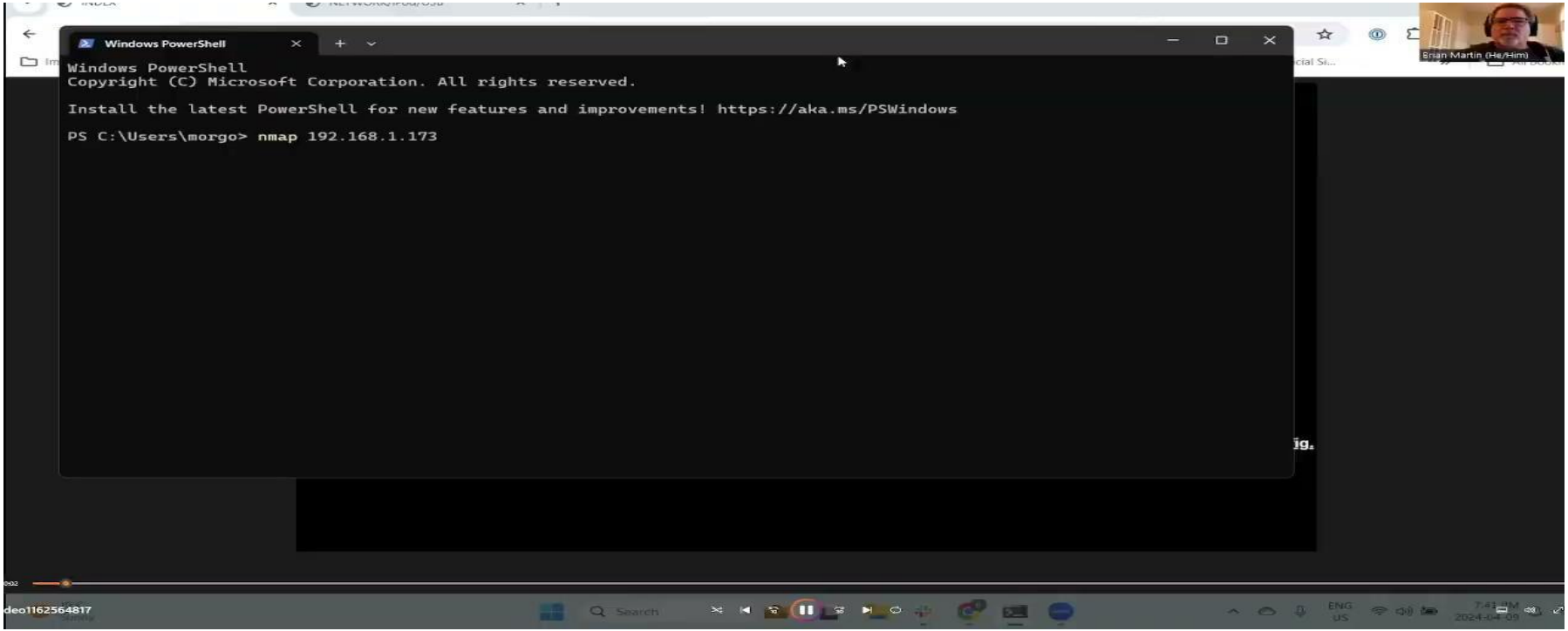
Denial of Service(DDoS)



Universal Plug and Play

- Many consumer devices use a set of protocols called Universal Plug and Play (UPnP)
- This makes setup and communication between network devices seamless and easy.
- Highlights the tension within product development between the desire for ease of use and the need for security.

IoT Plug and Play Risks



Mitigation Strategies for Aircrack-ng

- Implement Complex and Unique Passwords:
  Use complex and unique passwords for Wifi network authentication. Longer passwords with a mix of uppercase and lowercase letters, numbers, and special characters are harder to crack using brute force attacks. Avoid using common or easily guessable passwords.

Mitigation Strategies continued

- Use Strong Encryption Protocols:
  Ensure that your Wi-Fi network uses strong encryption protocols such as WPA2-PSK (Wi-Fi Protected Access II with Pre-Shared Key) or preferably WPA3, which provide robust security mechanisms to protect against unauthorized access. Avoid using outdated and vulnerable protocols like WEP (Wired Equivalent Privacy).

Protecting Plug-and-Play IoT Devices

Introduction:
- Plug-and-play IoT devices enhance convenience but pose security risks if not updated.

Importance of Updates:
- Regular updates patch vulnerabilities and prevent exploitation by hackers.
- Outdated firmware increases the risk of data breaches and malware attacks.

Best Practices:
- Enable Automatic Updates
- Regularly Check for Updates
- Follow Manufacturer Guidelines
- Keep Track of Devices
- Disabling UPnP after initial setup (if supported)

Additional Security Measures:
- Network Segmentation
- Strong Passwords
- Firewall Protection

Conclusion:
- Stay proactive in updating IoT devices to safeguard your network and data.

The End