Ethical Hacking: Cyber Offense and Attack Strategies

Augusta Owens, Fernando Luna, Florence Russell, Selina Loggins, Valentina Jardan

Project Overview

Ethical Hacking: Cyber Offense and Attack Strategies

Social Engineering and Phishing Tactics

Explain what social engineering and phishing are and demonstrate common phishing techniques.

Mastering WiFi Hacking with Kali Linux

Showcase the tools and techniques used to crack WiFi networks: Aircrack-ng suite, Wifite.

Break into Router Gateways

Understanding the vulnerabilities of routers and exploiting them to gain unauthorized access and control over a network's infrastructure.

DNS hijacking using a Router

Explain the risks associated with router vulnerabilities and DNS manipulation by setting up the Raspberry Pi to intercept DNS requests.

Evil Twin Attack: Fake WiFi Access Point

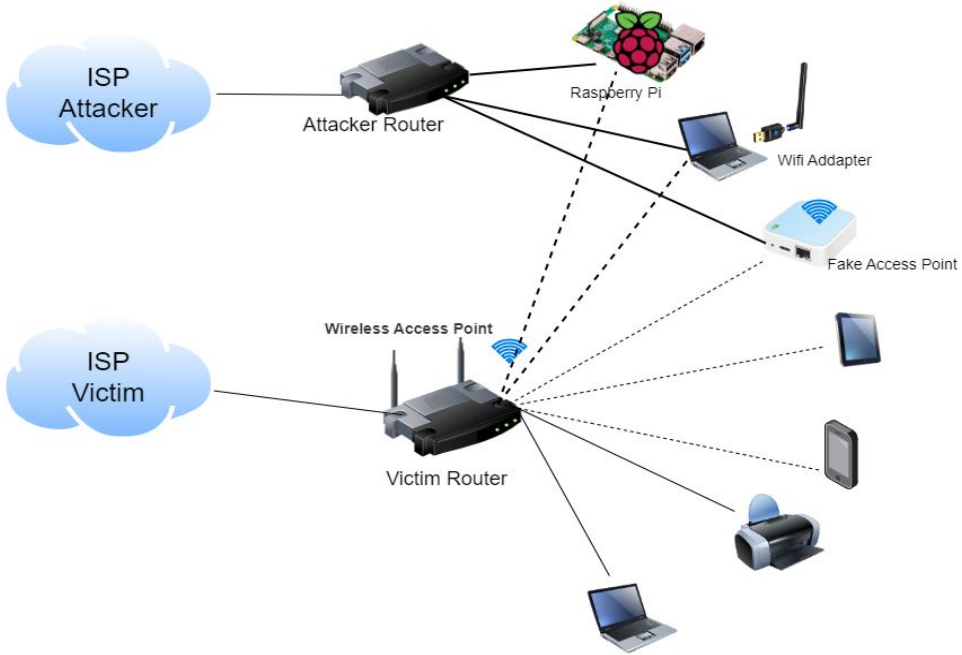
Demonstrate how to create a fake WiFi access point with a similar SSID and encryption as the legitimate network and its potential impact.

Project 4: Network Infrastructure

Our lab setup includes:

- **Victim Router**
- **Attacker Router**
- **Raspberry Pi** (configured as a DNS Server)
- **Mini Router** (acting as a Fake Access Point)
- **Laptop** running Kali Linux with a **Wi-Fi adapter**
- **Victim devices**

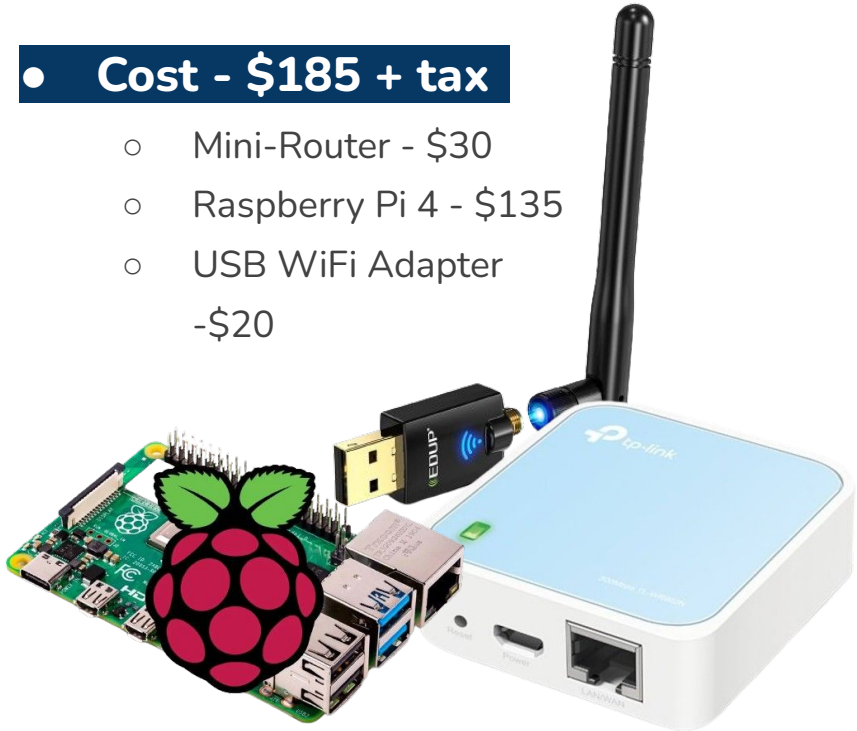
Note: We have exclusive ownership of all devices in our lab environment. All actions performed were within legal bounds.



Devices Utilized in the Hacking Process & Cost

- **Mini- Router** (TP Link with OpenWRT as a system operation and corresponding applications to capture traffic
  - TCPDump
- **Raspberry PI**
  - Raspberry Pi OS
  - Docker Containers for Pi-Hole
  - Docker Container for web server (NGinx)
- **USB WiFi Adapter for PC** (TPLink)

- **Cost - $185 + tax**
  - Mini-Router - $30
  - Raspberry Pi 4 - $135
  - USB WiFi Adapter -$20



Due to time constraints, we may fast-forward through the videos in this presentation. Also, all sensitive information in our videos has been blurred for security reasons. But if you are interested in learning more about our project, please contact our team on Slack or LinkedIn.


Ready? Let's Go!

GONE PHISHING

Social Engineering and Phishing Tactics

by Florence Russell

A Cybersecurity Fairy Tale: Attacking the Wireless Kingdom

You've Been WiFi'd

Here are some tools that can be used for WiFi Hacking

Kismet

Open-source wireless network detector, sniffer and IDS. Unlike tools focused on cracking passwords, Kismet is primarily used for network discovery and monitoring.

Reaver

A tool designed to exploit a vulnerability in the Wi-Fi Protected Setup protocol.
WPS is a feature intended to simplify the process of connecting devices to a wireless network.

Hashcatch

A Bash script designed to automate the process of capturing Wi-Fi handshakes. It's a popular tool among ethical hackers and security enthusiasts for gathering data necessary for cracking Wi-Fi passwords.

Aircrack-ng Suite

A comprehensive suite of tools designed for assessing the security of wireless networks. It's a popular choice among ethical hackers to test the strength of WiFi encryption and identify potential vulnerabilities.

Wifite

A powerful tool designed to simplify the process of cracking wireless network security. It automates many of the tasks involved in wireless penetration testing, making it accessible to users with varying levels of technical expertise.

Fern Wifi Crackers

Is a Python-based GUI tool designed for testing the security of wireless networks. It provides a user-friendly interface for performing various wireless attacks and cracking WEP, WPA, and WPS keys.

Components of the Aircrack-ng Suite

A comprehensive suite of tools designed for assessing the security of wireless networks. It's a popular choice among ethical hackers to test the strength of WiFi encryption and identify potential vulnerabilities.

01

aircrack-ng

The core tool used for cracking WEP and WPA/WPA2-PSK keys.

02

airodump-ng

Captures wireless network traffic and displays information about access points and clients.

03

aireplay-ng

Injects packets into the wireless network for various attacks.

04

airmon-ng

Puts wireless network interface cards into monitor mode.

05

airbase-ng

Creates fake access points (rogue APs).

Devices Required for WiFi-Hacking

TP-Link Adapter

A dual-band adapter supporting monitor mode and packet injection with speeds up to 1300Mbps, offering modern performance and flexibility for Wi-Fi penetration testing.

Alpha Adapter

Features a high-gain antenna for improved range and supports monitor mode and packet injection, enabling it to capture and analyze Wi-Fi traffic, including remote or weak networks.

Pineapple Adapter

Intercepts Wi-Fi traffic by creating rogue access points, facilitating man-in-the-middle attacks, and includes tools for automating common Wi-Fi hacking attacks.

Panda Wireless Adapter

A compact and affordable dual-band adapter with excellent Linux compatibility and solid performance for ethical hacking tasks.

Your WiFi Neighborhood: Unseen connections

The **WiFi Analyzer mobile app** is a tool designed to help users monitor and optimize their Wi-Fi networks.

Analyze Wi-Fi Signal Strength

Provides real-time insights into Wi-Fi signal strength, helping identify the best locations for stronger connections.

Identify and Optimize Channels

Scans Wi-Fi channels to identify the least congested one, reducing interference and boosting Wi-Fi performance.

Troubleshooting Tool

Helps diagnose connectivity issues such as slow speeds and frequent disconnections.

Wi-Fi Optimization

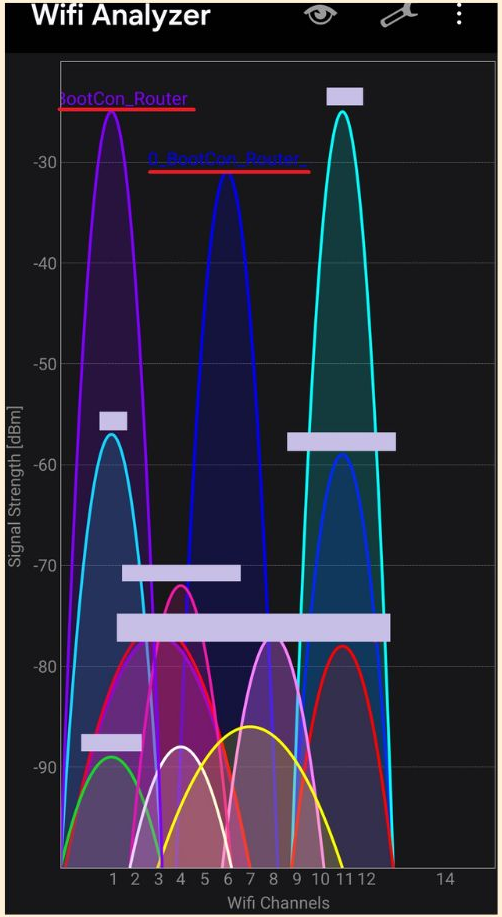
Assists in optimizing router placement, improving coverage, reducing dead zones, and enhancing network security.

Access Point Information

Showing signal strength, channel usage, and network information like SSID, and BSSID.

Graphical Representation

Displays a visual map of nearby Wi-Fi networks.



Steps

HOW TO HACK THE WI-FI

01. Enable Monitor Mode on Wi-Fi Adapter

Use a compatible Wi-Fi adapter and put it into monitor mode with the command `airmon-ng start wlan0`. This allows your adapter to capture all nearby Wi-Fi traffic.

02. Capture Packets with Airodump-ng

Use `airodump-ng wlan0mon` to begin capturing packets from nearby networks. Identify the target network and capture the handshake by running `airodump-ng -c [channel] --bssid [AP_MAC] -w [file_name] wlan0mon`.

03. Deauthenticate a Client Using Aireplay-ng

Run a deauthentication attack to force a device to reconnect to the network, capturing a fresh handshake. The command is `aireplay-ng --deauth 10 -a [AP_MAC] -c [Client_MAC] wlan0mon`

04. Capture handshake

Intercepting the communication exchange between a Wi-Fi router and WIFI adapter. By capturing and analyzing this handshake, attackers can potentially crack the Wi-Fi password.

05. Crack the Handshake with Aircrack-ng

After capturing the handshake, use `aircrack-ng -w [wordlist] -b [AP_MAC] [capture_file]` to attempt cracking the WPA/WPA2 password using a dictionary attack.

Mastering WiFi Hacking with Kali Linux

by Selina Loggins

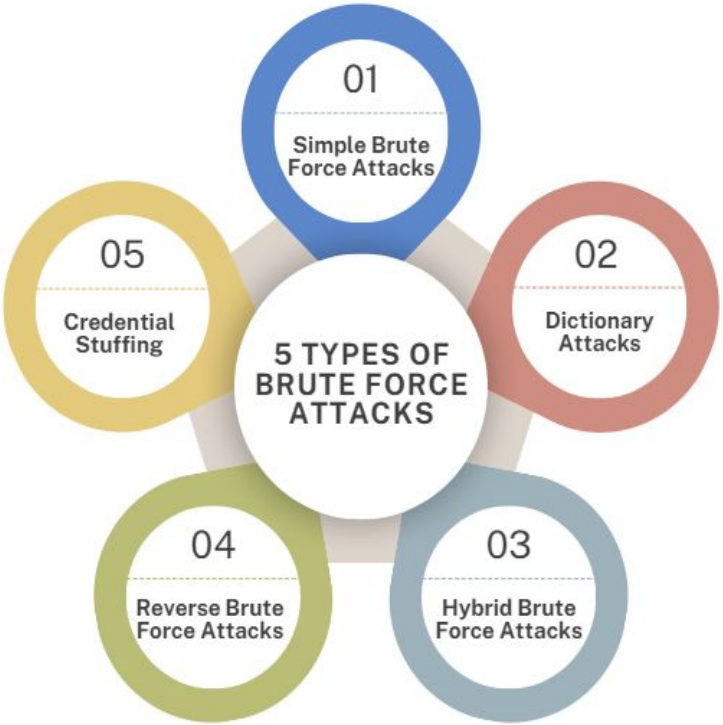
System Breach: We're in!

I'm In!

YOU HAVE BEEN HACKED

5 Types of Brute Force Attacks

- **Simple Brute Force:** trial of all possible combinations of characters.
- **Dictionary Attack:** Uses a list of common words and phrases as potential passwords.
- Hybrid Attack: Combines simple brute force with dictionary attack for increased efficiency.
- **Reverse Brute Force:** Starts with the correct password and works backwards to find the hash.
- **Credential Stuffing:** Reuses stolen credentials from one website to attack others.



Brute Force Attack Tools

01

Hydra

A versatile and speedy network logon cracker designed to perform brute-force attacks on various services like SSH, FTP, and HTTP.

02

Patator

A multi-functional brute-force tool offering greater flexibility and customization, designed to support attacks on numerous protocols.

03

Routersploit

An exploitation toolkit tailored for penetration testers to find and exploit vulnerabilities in routers and IoT devices.

04

Burpe Suite

A robust web application security tool that helps detect vulnerabilities through both automated scans and manual testing.

05

Ncrack

A high-efficiency network authentication cracker built for testing the security of network services like SSH, RDP, and VNC.

06

Hashcat

A powerful tool for password cracking and recovery that leverages high-performance computing and supports a wide range of hashing algorithms such as MD5 and SHA

Lost in the Router Labyrinth

NIGHTHAWK R6900P
AC1900 SMART WIFI ROUTER

NETGEAR - AC1750
DOCSIS 3.0 Cable
Modem + WiFi Router

Motorola SBG6580
(ARRIS SURFboard)

XFinity
Model TG1682G

Linksys
WRT1900AC

Break into Router Gateways

by Fernando Luna

BREAKING NEWS

DNS HIJACKING: THE CYBER WARRIOR'S BATTLE

DNS HIJACKING UNLEASHES WAVE OF CYBERATTACKS: USERS AT RISK OF IDENTITY THEFT, FINANCIAL LOSS.

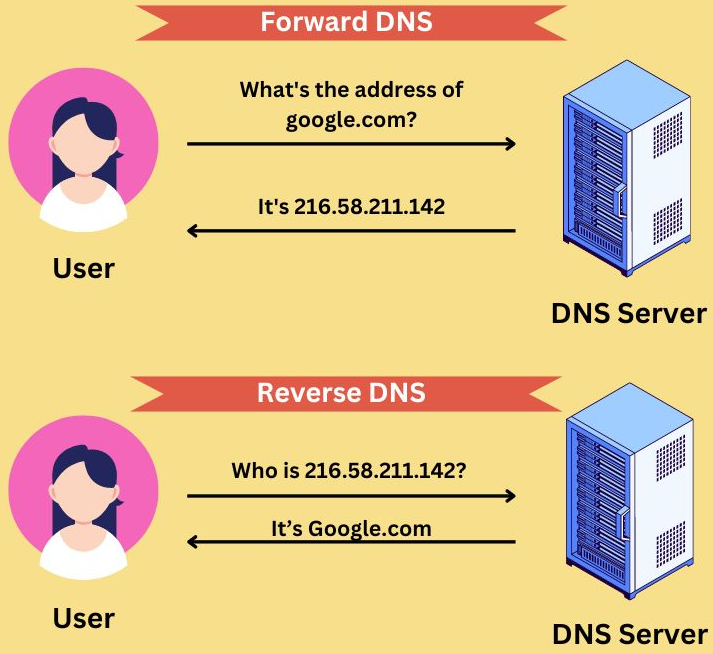
The Magic Behind DNS

What is DNS? DNS stands for Domain Name System. It's essentially the internet's phonebook.

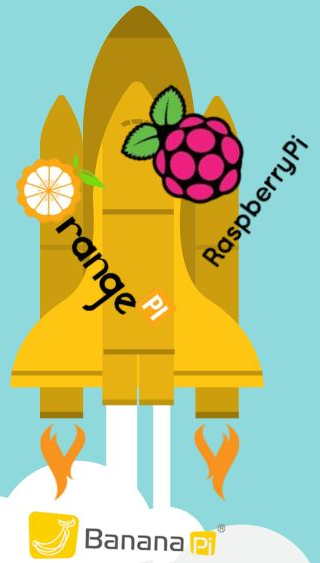
- **Humans** are better at remembering names than numbers.
- **Computers** understand numbers better than names.

DNS makes it possible for us to use easy-to-remember domain names instead of complex IP addresses.

How it works



Types of DNS Attacks



Local DNS Hijacking

Attacker installs Trojan software on a user's computer, then modifies the local DNS settings to reroute the user to harmful websites.

DNS Hijacking using a router

Attackers take advantage of weak routers to hack it and change its DNS settings, which will affect everyone that uses that router.

Man-in-the-middle attacks

Attackers this techniques to intercept communications between users and a DNS server. They then direct the target to malicious websites.

Rogue DNS server

Attackers can alter DNS records on a DNS server, enabling them to reroute DNS requests to malicious websites.

"System online, commencing operation."

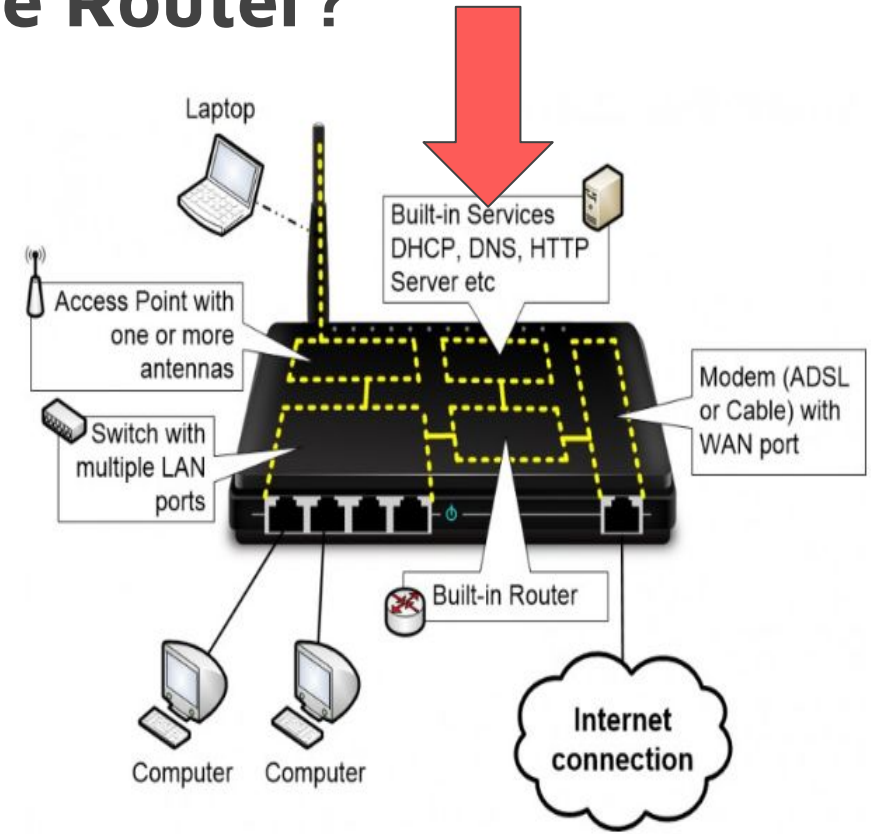
"Payload armed, ready to deploy."

"Strike initiated."

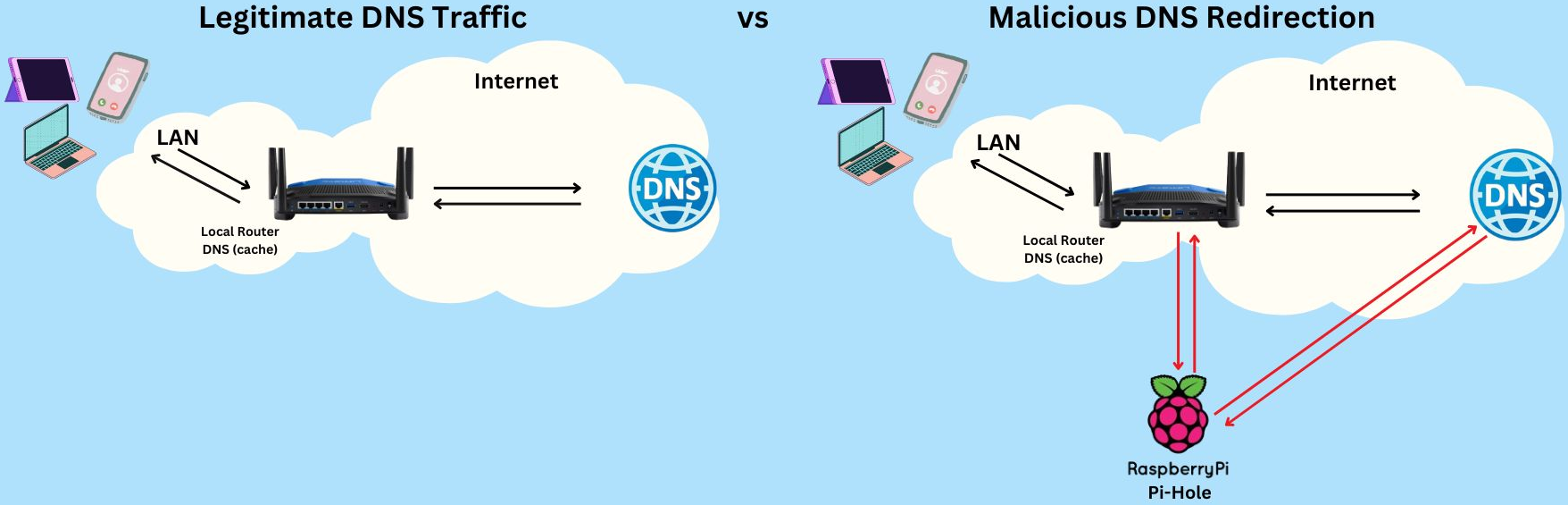
"Mission commenced."

What's inside a Home Router?

- **Integrated Switch**
- **Wireless Access Point**
- **Built-in Modem (**often there is one),
- **WAN port of the router**
- **Built-in Router**
- **Server** that handles additional Services:
  - Handing out IP addresses to devices on our home network.
  - Handles Address Translations and Port Forwards.
  - Takes care of any firewall rules.
  - Replies to DNS-queries.
- **Web interface**



DNS Flow, huh?
Sounds like trouble waiting to happen.

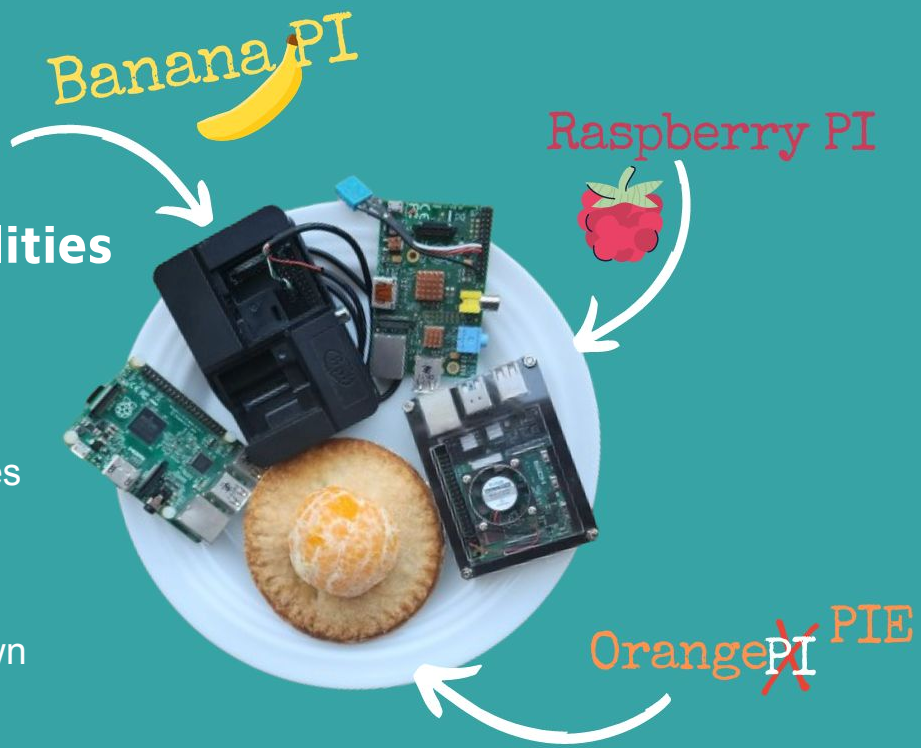


Why Raspberry Pi?

Raspberry Pi has all the features you expect from a computer: wireless internet connectivity, HDMI ports for your monitors, and USB ports for your accessories, along with ample processing power and RAM for all your day-to-day use.

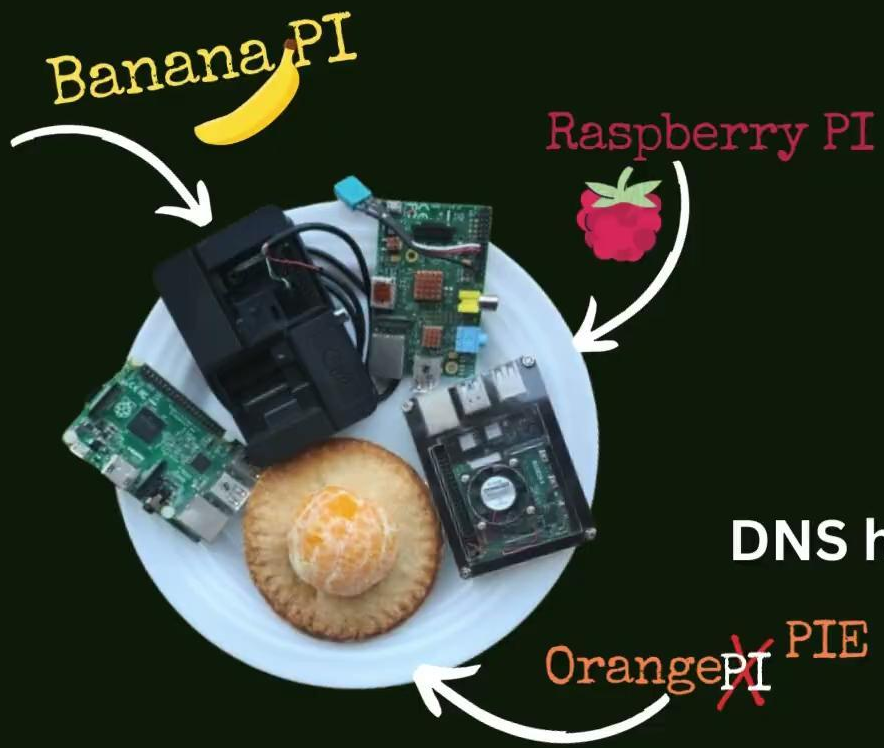
Which Pi are we baking?

Banana, Raspberry, or Orange?



Expanding Raspberry Pi's Capabilities

Pi-Hole: is a fantastic tool for ad blocking and network-wide DNS management.
Plex: Stream your media library to any device.
Home Assistant: Control various smart home devices and create automation routines.
OpenVPN: Set up a secure VPN server for remote access.
WireGuard: A modern alternative to OpenVPN, known for its speed and simplicity.
Nextcloud: Create your own cloud storage solution.



DNS hijacking using a Router

by Valentina Jardan

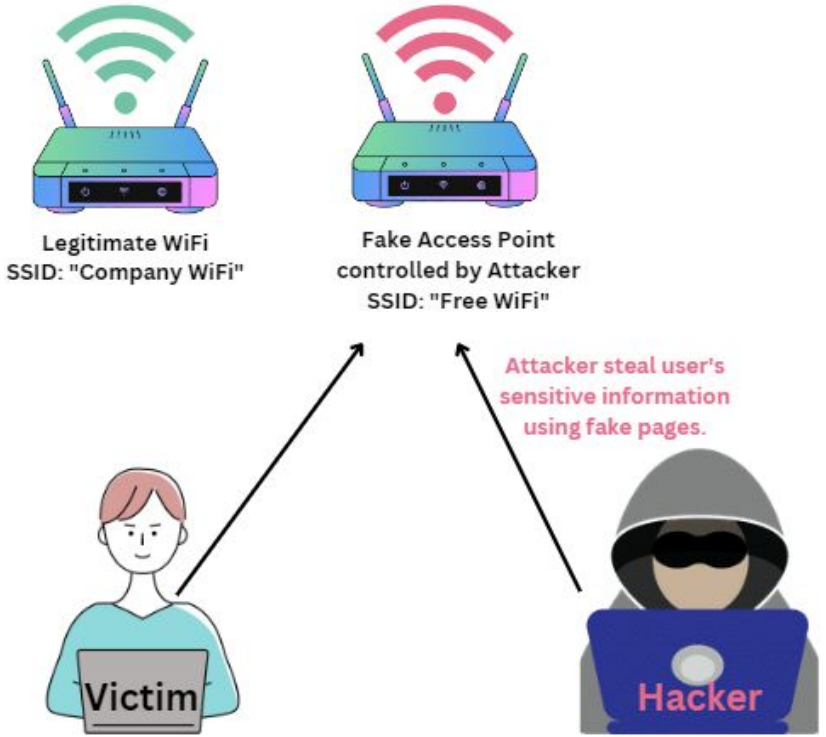
THE LAST
CYBER
SAMURAI

AND
THE BLOOD
OF
FAKE ACCESS POINT

Understanding Fake Access Points

Why do an Evil Twin Attack?

An evil twin attack helps cybersecurity professionals understand vulnerabilities, test defenses, and improve incident response for real-world threats.



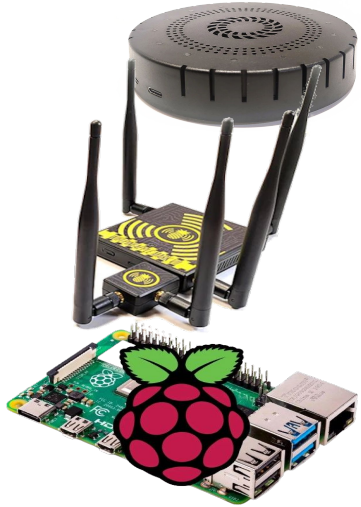
Devices to create a Fake Access Point

Specialized Devices:

- **WiFi Pineapple:** a popular choice known for its user-friendly interface and pre-loaded tools for various attacks.
- **Other similar devices:** There are other devices with similar functionalities, though less well-known.

General-Purpose Hardware:

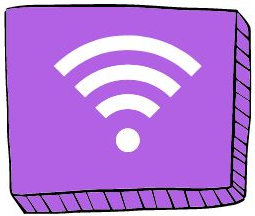
- **Wireless routers:** With custom firmware or specific software, it's possible to configure a router to act as a fake access point.
- **Wireless network adapters:** Can be used in conjunction with software to create a fake access point.
- **Raspberry Pi or other single-board computers:** With suitable software and wireless adapters, these can be configured to act as fake access points.



Software:

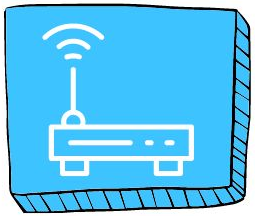
- **Kali Linux:** Tools like Hostapd that can be used to create fake access points.
- **Other penetration testing tools:** There are various software tools designed for network attacks that can be used for this purpose.

Creating a FAKE WIFI ACCESS POINT



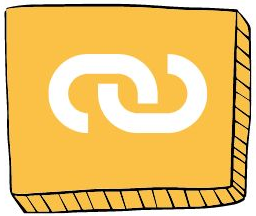
01. Clone Target AP

To clone a target AP, access the OpenWRT router's wifi settings, match the ESSID and password to the target AP, and apply the changes.



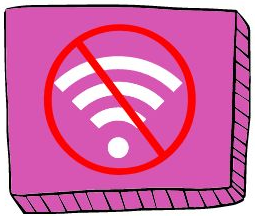
02. Modify Linksys Smart Wifi

To modify a Linksys Smart Wifi AP (Target AP), change the wifi name (adding an underscore our example), ensure 2 GHz is enabled and 5 GHz is disabled, then apply the changes.



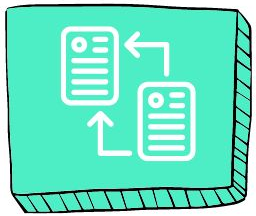
03. Verify Kali Linux Connection

To verify Kali Linux connection, reconnect to wifi and run ‘ifconfig’ in the terminal to confirm the connection details.



04. Activate Fake Access Point

To activate the fake access point, enable it in the OpenWRT router's wifi settings, save the changes, and wait for it to register and refresh.



05. Capture Data

To capture data, SSH into attack router, use ‘tcpdump’ to monitor traffic or save packets, and list the capture file to verify it.

Evil Twin Attack: Fake WiFi Access Point

by Augusta Owens


Mitigation Strategies

Mitigation Strategies

Strong Encryption (WPA3 or WPA2): Essential for securing wireless communications. WPA3 is more secure than WPA2, and both far exceed WEP.

Strong Passwords: Use complex, unique passwords for your router and Wi-Fi. Avoid default passwords.

Firmware Updates: Regularly update router firmware to fix vulnerabilities.

Network Segmentation: Isolate critical devices from public networks to reduce the attack surface.

Monitor Logs: Regularly check router logs and network traffic for suspicious activity.

Multi-Factor Authentication (MFA): Enable MFA where possible to add an extra layer of security.

HIRE US

Florence Russell

Cyber Investigator

@florence-russell

Selina Loggins

Cyber Princess

@selina-t-570386j263

Fernando Luna

Cyber Punk

@fernando-luna

Valentina Jardan

CYBER WARRIOR

@valentina jardan

Augusta Owens

CYBER SAMURAI

@augusta-owens

Resources

- **Installing OpenWRT on the TP-Link WR703N v1.6**

  https://wiki.cementhorizon.com/articles/Tech/Installing%20OpenWRT%20on%20the%20TP-Link%20WR703N%20v1.6.html

- **How to Install Raspbian OS in Your Raspberry PI**

  https://www.instructables.com/HOW-TO-INSTALL-RASPBIAN-OS-IN-YOUR-RASPBERRY-PI/

- **Install Pi-hole on Raspberry PI**

  https://pi-hole.net/