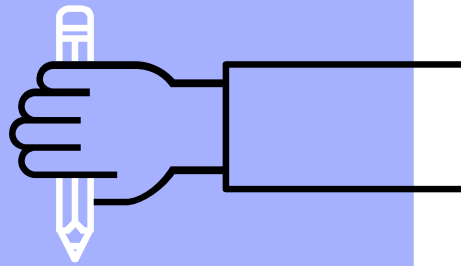
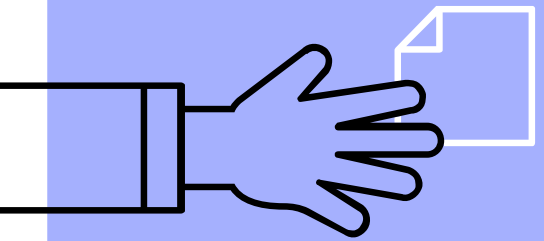


Wifi Hacking

CS 166: Information Security - Sec. 01

Prof. Chao-Li Tarng

Team 19: Michael Huh, Shreya Raj, John Buclatin, Erica Xue, and Natalie Kao



Introduction

Problem Statement:

- Wi-Fi security vulnerability allows unauthorized access and breaches.
- Attackers exploit these vulnerabilities to infiltrate networks, access information, and disrupt operations.
- Specifically targeting WPA2 vulnerabilities inherent in Wi-Fi networks.

Project Focus:

- Analyze WiFi hacking techniques, specifically WPA2 vulnerabilities
- Research strategies to prevent attacks

Approaches

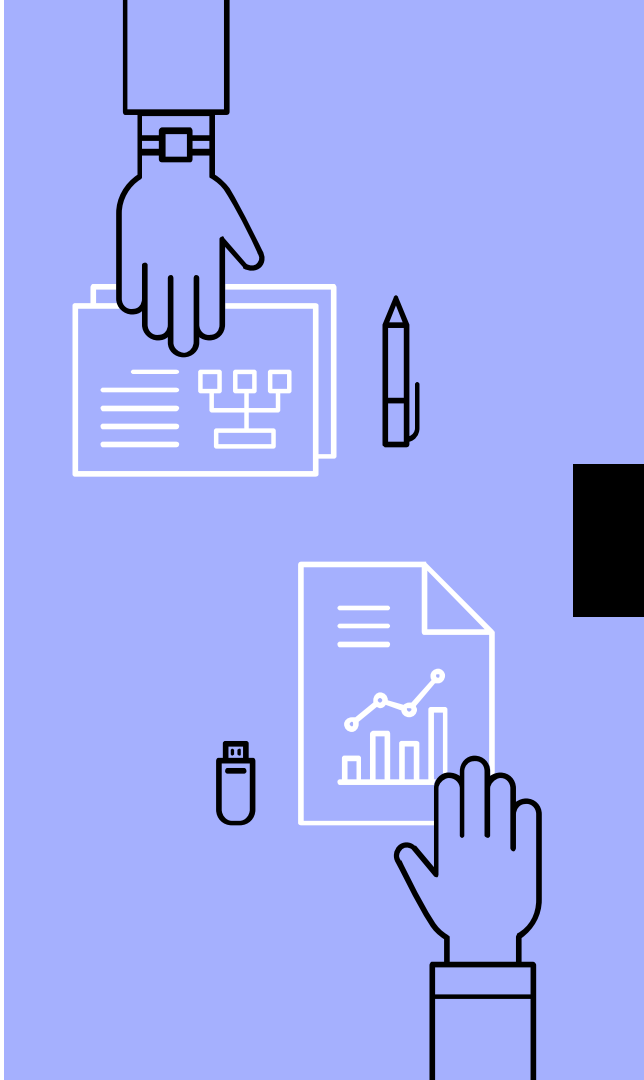
- Conduct penetration tests of Wi-fi networks using router
- Testing in virtual environment to ensure a safe, isolated environment

[redacted]

Architecture

1. **Technologies**
   a. WiFi Network
   b. Kali Linux as primary OS
   c. Aircrack-ng suite

2. **Dictionary Attack**
   a. Rock You wordlist



Technologies

Kali Linux:

- A Linux distribution with built-in tools for security testing.

WiFi Network (Router/Modem/Network Provider):

- Essential components that provide internet connectivity.

Network Adapter – Support Monitor Mode:

- Hardware that can capture all nearby wireless traffic.

Technologies

Aircrack-ng:

- Tools for cracking network security, highlighting vulnerabilities.

Airmon-ng:

- Activates monitor mode on network adapters.

Airodump-ng:

- Captures and logs wireless network packets.

Aireplay-ng:

- Generates and manipulates network traffic for testing.

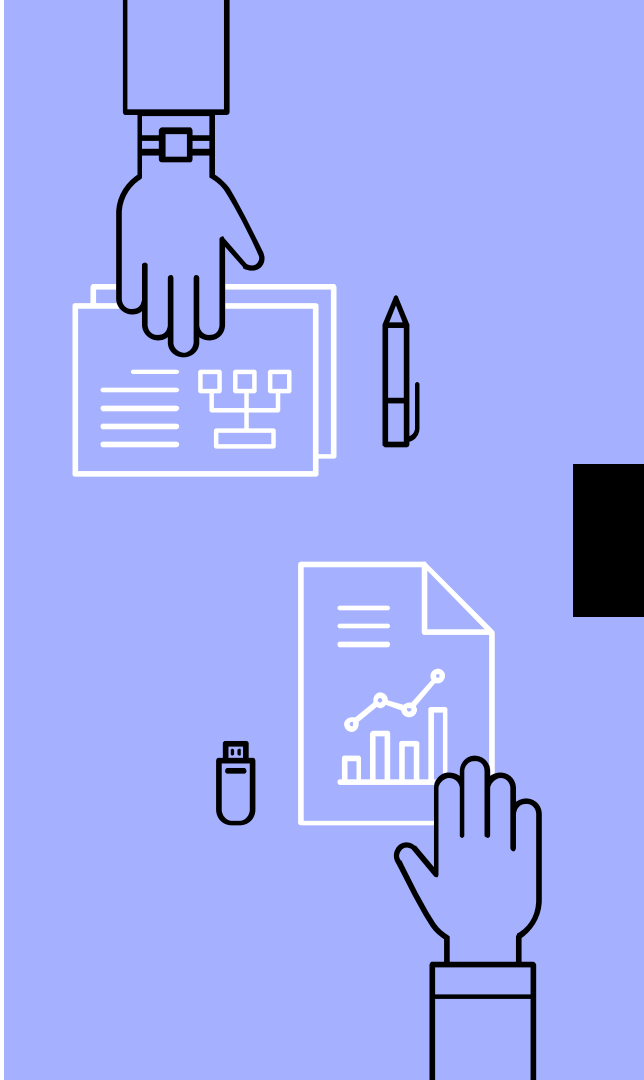
Wireshark:

- Analyzes detailed network traffic for deep insights.

RockYou Word List

History

- Social app and advertising network, RockYou, suffered devastating cyber attack in 2009 that led to exposure of over 32 million user passwords
- Passwords were stored in plaintext
- Leaked passwords compiled into wordlist known as RockYou.txt file
- List is now a standard tool used for password cracking and network testing



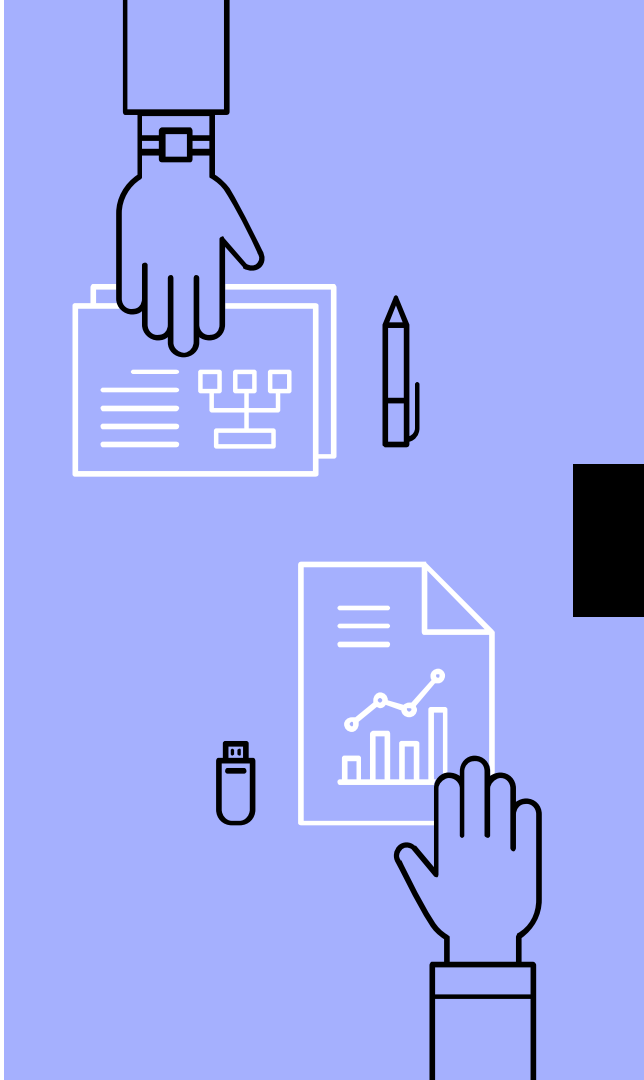
RockYou Word List

Usage from Security Professionals

- Tests strength of network and system security
- Crack hashed passwords or breach

Usage from Attackers

- Use wordlist in **password-spraying attacks** to gain unauthorized access to accounts
  - Dictionary attack where list of usernames are used and passwords from RockYou.txt are tried against each account



RockYou Word List

Our Application

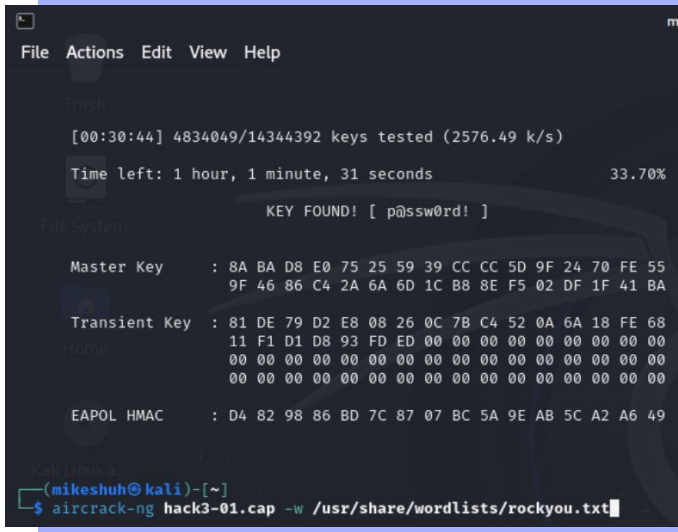
- *Use aircrack-ng to run a dictionary attack to discover password with the wordlist*

Demo

Summary

Result: Successfully cracked password !

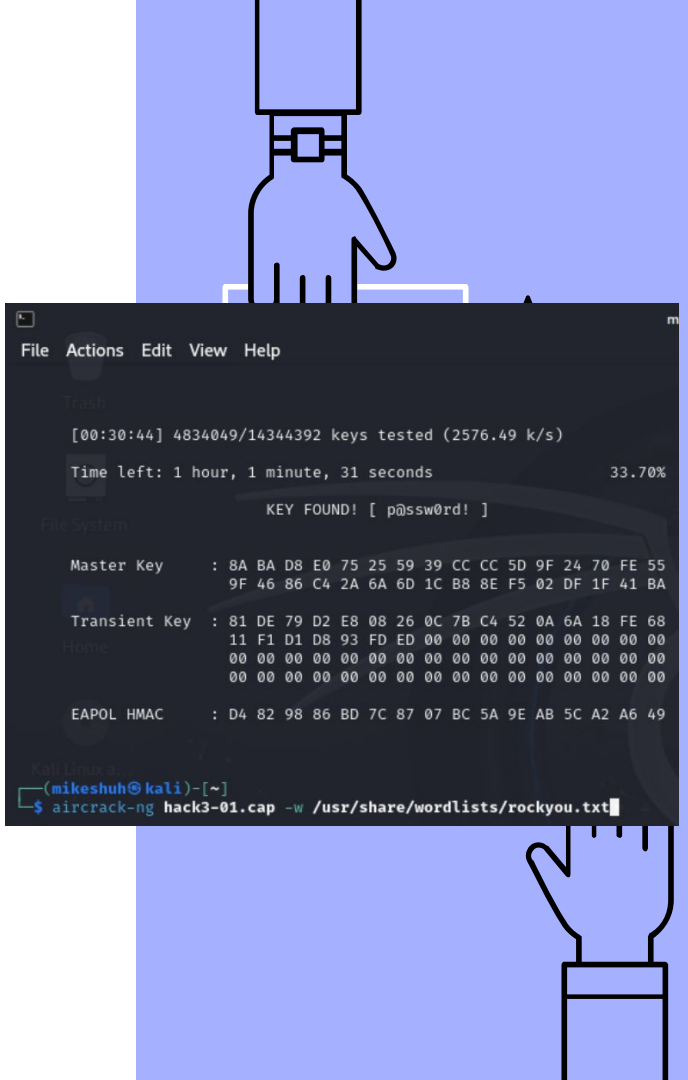
- Password Statistics
  - In 2023, the most common password worldwide was “123456” & runner up was “admin” (Borgeaud)
  - 43 % of all passwords are simply the username (Study: Hackers Attack)
  - Password patterns most commonly indicate that years, names, and personal favorite things (food, sports team, etc) are easily hacked passwords (Cyber News)



Summary (cont.)

Result: Successfully cracked password !

- Success of dictionary attacks rely on:
  - Password Complexity (Wright)
    - Stolen/reused credentials are implicated in 80% of hacking-related breaches
  - Quality of Password Cracking Software and Dictionary
  - Attack Speed and Tools



Future Work

- Explore advanced encryption methods like WPA3
- Brute Force Attacks
  - Method: attempting all possible passwords
    - Document Findings
- Develop further countermeasures
  - Scripts to continually monitor network safety

Conclusion

- Confirmed WiFi security weakness to penetration testing
  - Conducted as described in demo
- Use strong passwords!
  - Longer the password, the better
  - Mixed case letters, numbers, and symbols
  - Random memorable phrases

Works Cited

Benis, M. (2023, January 22). *The TJX Hack: A Case Study in Retail Cybersecurity*. www.linkedin.com. https://www.linkedin.com/pulse/tjx-hack-case-study-retail-cybersecurity-michael-benis/

Borgeaud, A. (2024, March 1). *Most used passwords worldwide 2023*. Statista. https://www.statista.com/statistics/1454162/most-used-passwords-worldwide/

David Tidmarsh. (2023, June 13). *Types of WiFi Hacks, How to Identify and Fix Them, and Preventive Measures*. Cybersecurity Exchange. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/protect-wifi-network-from-hacking/

Works Cited (cont.)

Indira Reddy, B., & Srikanth, V. (2019). Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 5(4), 28–35. https://doi.org/10.32628/cseit1953127

Jester, Timothy. (2023, August 4). *Understanding RockYou.txt: A Tool for Security and a Weapon for Hackers. Keeper.* https://www.keepersecurity.com/blog/2023/08/04/understanding-rockyou-txt-a-tool-for-security-and-a-weapon-for-hackers/

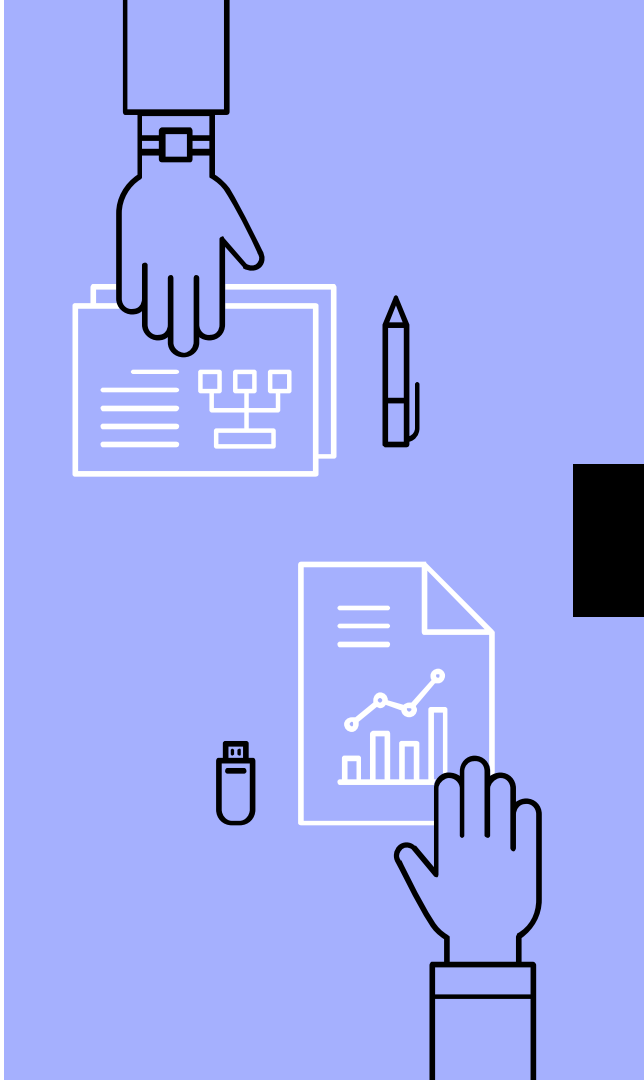
Works Cited (cont.)

StickmanCyber Team. *Top 5 Penetration Testing Risks*. https://www.stickmancyber.com/cybersecurity-blog/top-5-penetration-testing-risks.

Study: Hackers Attack Every 39 Seconds. (2007, February 9). Enme.umd.edu. https://enme.umd.edu/news/story/study-hackers-attack-every-39-seconds

Wright, G. (2024, February). *What is a dictionary attack? - Definition from WhatIs.com*. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/dictionary-attack

Thank you!



The PowerPoint presentation should include minimally the followings:

- Title page, including
  - Topic
  - Course name, number, and section
  - Instructor
  - Time
- Introduction
  - Problem statement
  - Approaches
- Architecture, design, and key algorithm
- (Optional but strongly suggested) live demo or video demo
- Summary of the result
- Suggestion for future work
- Conclusion
- Credit, including the work, guidance, and support you have used and received
  - Open source
  - Key articles