WiFi Pineapple

Penetration testing tool used to test the vulnerability of wireless networks

MITM attack - DNS spoofing

How does it work?

1. Set up rogue access point with identical name as target
2. Force victims to connect to AP
3. Spoof DNS

Practical applications

- Spreading false information
- Forced download of malicious files
- Censorship
- Stealing of credentials

How can we protect against this?

- Make sure to always use HTTPS
- Be careful about using public WiFi

Cracking WPA/WPA2

How does it work?

1. Passively listen to traffic being broadcast by target router
2. Wait and capture WPA 4-way handshake
3. Crack the password

Practical applications

- Exposing networks with weak passwords
- Gaining free internet access from neighbors

How can we protect against this?

- Use stronger WiFi passwords

DNS Spoofing

Ways to crack a password

- Dictionary attack
- Rule attack
- Combination attack
- Mask attack (similar to brute-force)

Possible tools: hashcat, aircrack-ng

Takeaways

- Familiarity with the structure of the internet and how it works
- Learned many new networks-related concepts
- Stronger understanding of the different layers of telecommunication
- Greater awareness of good security practices on the internet

Reflection

- Most innovation in WiFi technology has been to improve convenience, rather than security
  - R&D primarily focused on elements such as radio range, throughput, and connectivity, rather than safeguarding information and improving security protocols
- We need to educate the public about more secure internet practices

https://www.openlearning.com/u/davidgong-q5u6y6/blog/?tag=something-awesome

Disclaimer: This is for educational purposes only. No pineapples were harmed in the making of this project. Spongebob made it home.