InfoSec Write-ups

Hak5 WiFi Pineapple Mark VII: A Comprehensive Toolset for Wireless Network Security Testing and Penetration Testing (Part 2)

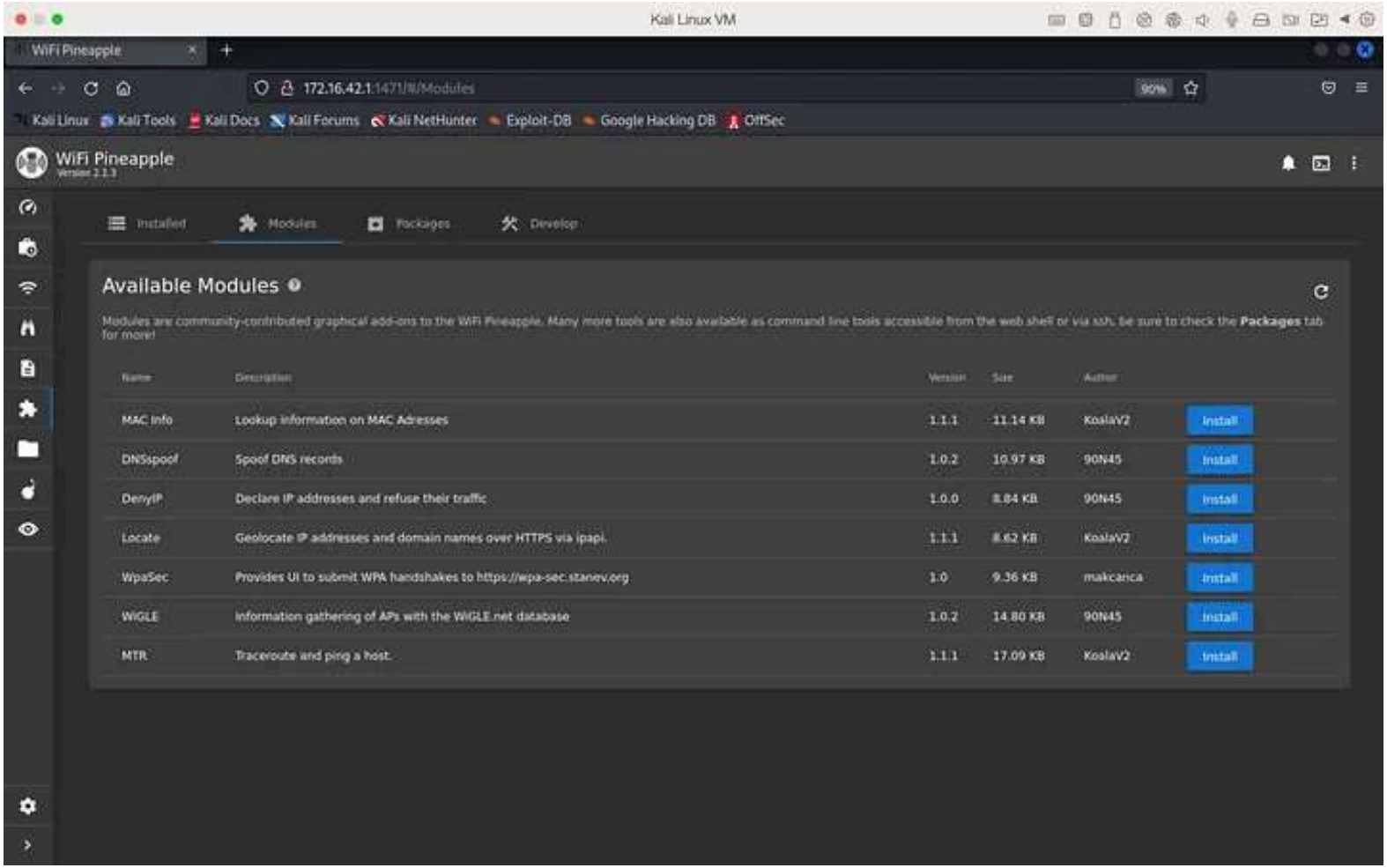
Part 2: WiFi Pineapple Modules, Tips & Tricks, and Concluding Notes

Jason Yee Follow 7 min read · Jul 27, 2023

 11    

Modules

WiFi Pineapple Modules refer are various software components that can be installed on the device to extend the router's functionality and perform specific tasks. Modules can be thought of as plug-ins or add-ons that can be installed on the device to enhance its capabilities.



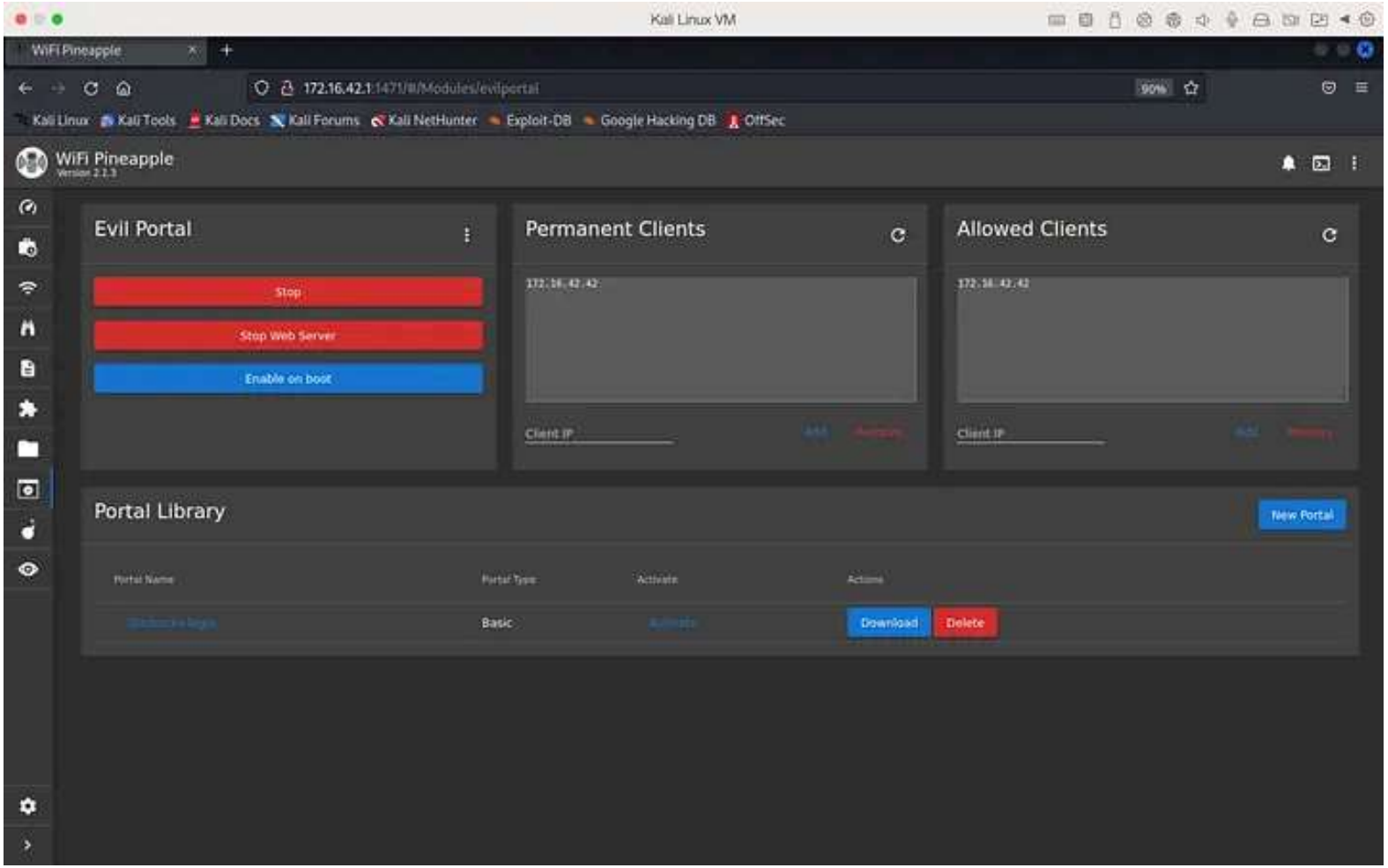
Screenshot of Hak5 WiFi Pineapple Modules.

There are many modules available for the WiFi Pineapple, including modules for performing reconnaissance, sniffing traffic, cracking passwords, spoofing MAC addresses, and more. These modules can be

installed and configured via the web interface of the device, making it easy to customize the WiFi Pineapple for specific testing scenarios.

Examples of Modules

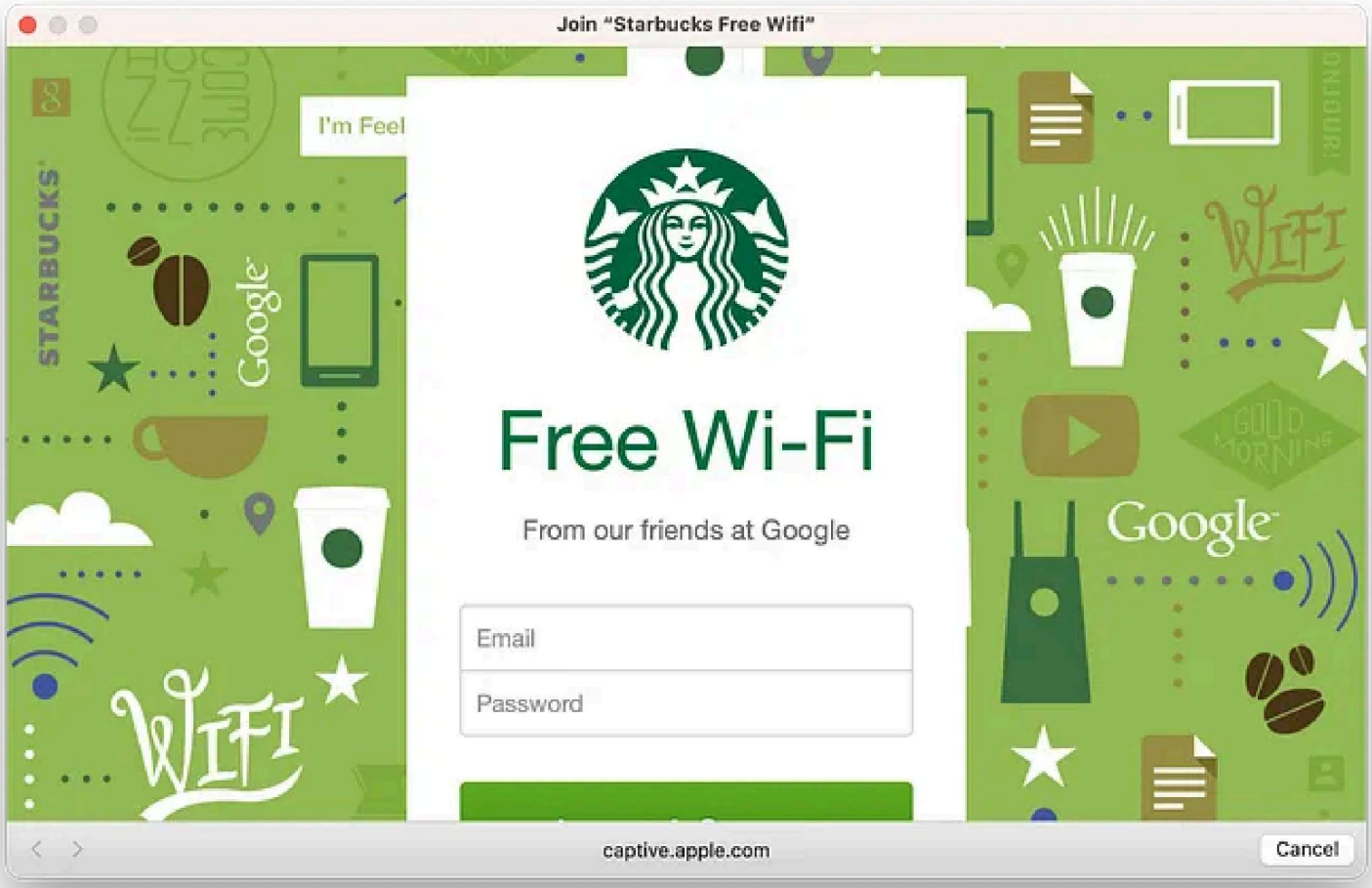
Evil Portal



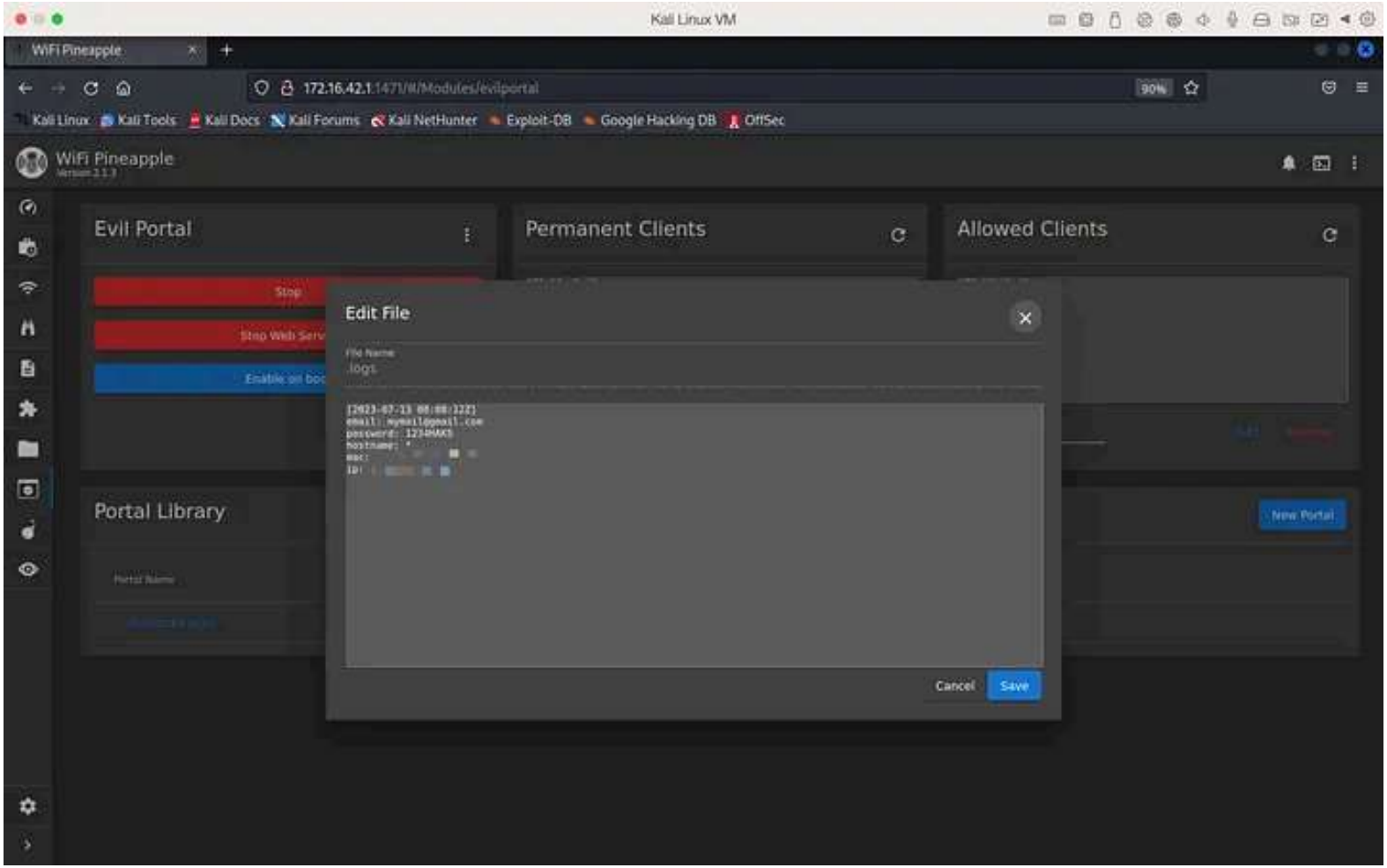
Evil Portal establishes a false captive portal to perform phishing attacks against WiFi clients obtain credentials or infect the victims with malware.

The evil portal module can be modified to emulate other websites, portals, or platforms, such as login pages from other platforms like Starbucks and

Mcdonald's to obtain credentials. Examples of these portal duplicates can be found here: https://github.com/kleo/evilportals



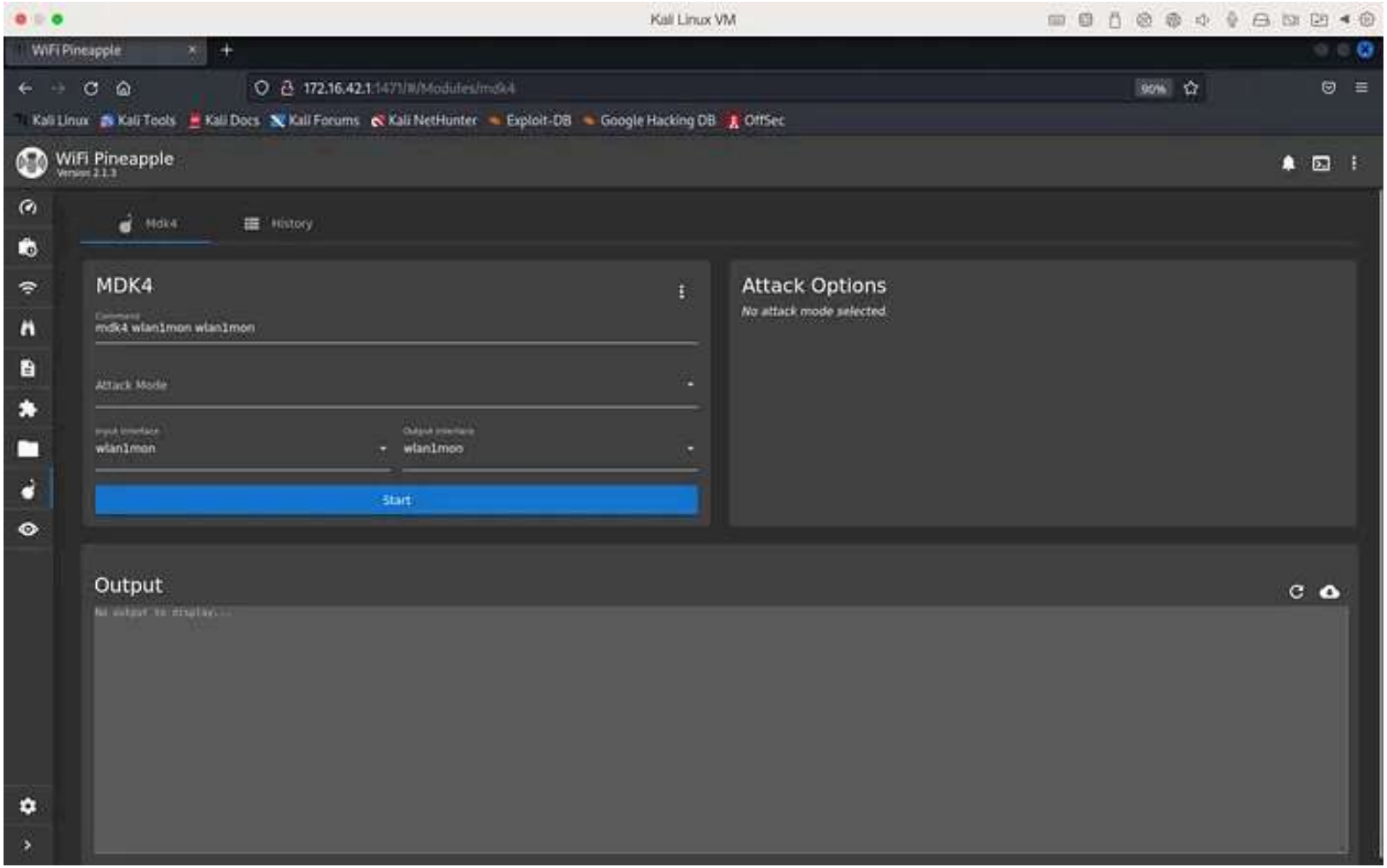
Once a client tries to connect to your PineAP, they will be prompted with a portal that emulates a company or organization login page.



When the client enters their credentials, the information will be recorded in a log file, including their entered email and password, as well as their MAC and IP address.

MDK4

MDK4 is a Wi-Fi testing tool that injects frames on several operating systems. It uses the osdep library from the aircrack-ng project.

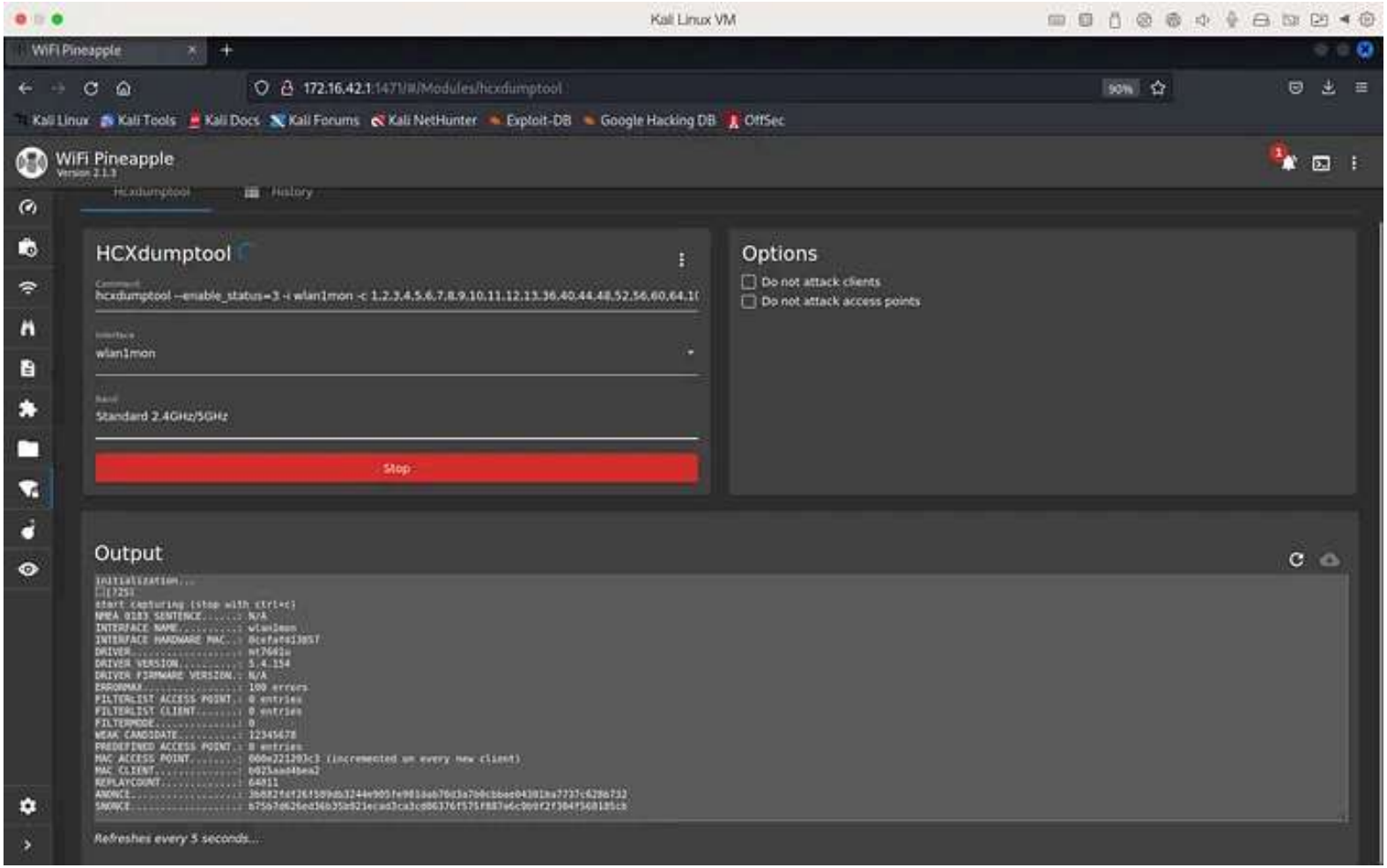


Included in MDK4 are numerous attack modes, and below are 3 prevalent examples:

- **Authentication Denial of Service —** Prevents users from accessive network service. ADoS attacks aim to overwhelm the authentication system with a flood of authentication requests, making it difficult or impossible for legitimate users to authenticate and access the service.
- **Beacon Flooding —** Beacon flooding is a type of wireless network attack that involves flooding an area with fake beacon frames, also known as “probe responses,” to trick wireless clients into connecting to a malicious access point (AP). The attack works by broadcasting fake beacons that appear to be from legitimate APs, in an attempt to lure wireless clients to connect to the attacker’s AP instead of the legitimate one.
- **Deauthentication & Disassociation —** Sends de-authentication and disassociation packets to stations based on data traffic to disconnect all clients from an AP. This type of attack works by exploiting a vulnerability in the 802.11 wireless protocol, which allows wireless devices to disconnect from a network by sending a de-authentication frame. By sending a large number of de-authentication frames, an attacker can force wireless clients or APs to disconnect from the network.

HCXDump

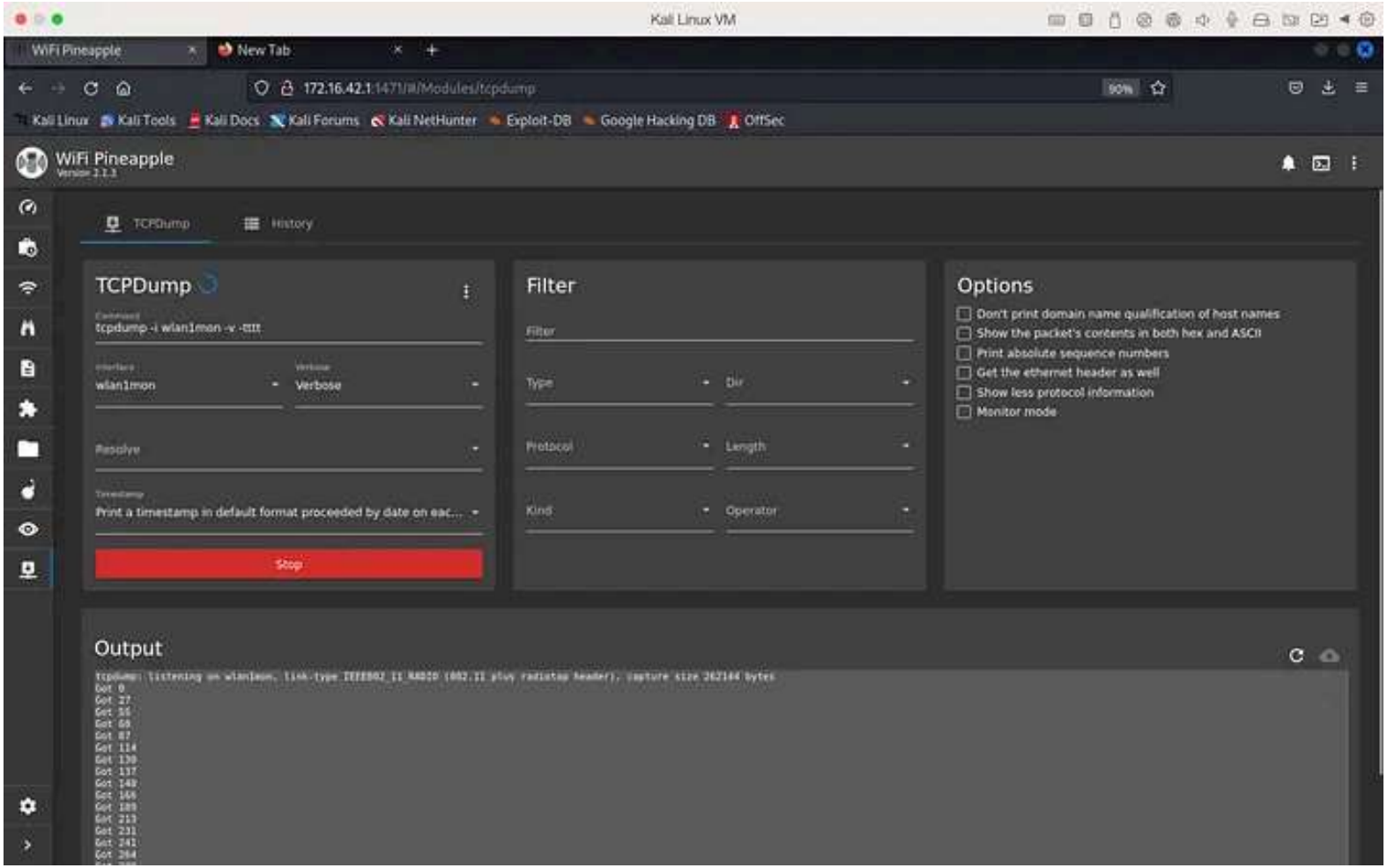
HCXDump is a tool that can be used for capturing WPA handshakes from Wi-Fi networks, as well as running multiple tests to determine whether Wi-Fi access points or clients are vulnerable to brute-force attacks. HCXDump works through beacon and probe response testing to analyze responses and vulnerabilities. It can also be done using association testing and de-authentication testing for further



After completing a scan, the module creates a .pcap file automatically, which can be opened with third-party tools, like Wireshark, to perform additional analysis on the network.

TCPDump

TCPDump is a tool used for network traffic analysis and packet capture. It is available on most Unix-based operating systems and is commonly used by network administrators and security professionals to monitor and troubleshoot network issues. TCPDump captures packets in real time and displays them on the command-line interface, allowing users to analyze network traffic and identify potential security threats.



Like HCXDump, the module creates a .pcap file automatically after completing a scan, which can be analyzed to perform additional analysis on the network.

Real-Life Use Cases of the Hak5 WiFi Pineapple

The Hak5 WiFi Pineapple is a powerful tool that could be used for wireless network penetration testing and security auditing. One example of these use cases is network security testing in physical fields, such as offices and workplaces. The WiFi Pineapple can be used to test the security of wireless networks by simulating various attacks, such as man-in-the-middle attacks, rogue access point attacks, and password cracking attacks. Another example of use cases for the WiFi Pineapple is security researchers, who can use the WiFi Pineapple to study wireless network security and protocols, possibly developing new security tools and techniques.

Furthermore, the information obtained from using the WiFi Pineapple can be invaluable for organizations in providing their clients with the necessary information to prevent potential attacks. For example, if the WiFi Pineapple identifies vulnerabilities in a client's wireless network, the organization can use this information to educate the client on the importance of strong passwords, encryption settings, and other security measures. Additionally, the WiFi Pineapple can simulate attacks on the client's network, demonstrating the potential risks and consequences of a security breach. This can help the client understand the importance of maintaining strong security practices and investing in security solutions to protect their network.

💡 7 Tips & Practices for Real Field Testing

Obtain Permission

Before conducting any testing with the WiFi Pineapple, obtaining permission from the network owner or administrator is essential. Unauthorized testing can lead to legal consequences.

Use in a Controlled Environment

It is recommended to use the WiFi Pineapple in a controlled environment, such as a lab or testing environment, to minimize the risk of affecting other networks or devices unintentionally.

Conduct a Risk Assessment

It is important to conduct a risk assessment before using the WiFi Pineapple to identify potential risks and develop a plan to mitigate them.

Use Proper Network Segmentation

It is essential to ensure that the WiFi Pineapple is properly segmented from other networks to prevent unauthorized access.

Keep the Firmware Updated

It is recommended to keep the WiFi Pineapple firmware updated to ensure that it is protected against the latest security threats.

Use Encryption

Whenever possible, it is recommended to use encryption to protect the data being transmitted between the WiFi Pineapple and other devices.

Document Everything

It is important to keep detailed records of all testing activities, including the tools used, the methods employed, and the results obtained. This can be done through the help of features from the WiFi Pineapple, such as generated reports from Campaigns.

Strengthening Your Digital Devices Against Attacks and Interceptions

In an increasingly interconnected world, the threat of WiFi Pineapple attacks looms large. These malicious activities exploit vulnerabilities in WiFi networks, allowing attackers to intercept and manipulate network traffic. However, there are proactive measures you can take to fortify your digital fortress and protect against these insidious attacks.

First and foremost, ensure that your network is secured with robust encryption, such as WPA2 or WPA3, to make it harder for attackers to breach

your defenses. Implementing a wireless intrusion detection system (WIDS) or wireless intrusion prevention system (WIPS) can provide an extra layer of security by monitoring your network for any signs of suspicious activity, including rogue access points and evil twin attacks.

Regularly updating the firmware and software of your network devices, such as routers and access points, is crucial. These updates often contain patches that address known vulnerabilities, making it harder for attackers to exploit them. Additionally, consider using a virtual private network (VPN) when connecting to public or untrusted networks. A VPN encrypts your internet traffic, making it significantly more challenging for attackers to intercept and manipulate your data.

Education plays a vital role in defending against WiFi Pineapple attacks. Train your users to exercise caution when connecting to WiFi networks, emphasizing the importance of verifying network names and using secure connections whenever possible. Disabling automatic network connections on devices can also prevent unintentional connections to rogue access points.

Conducting regular network audits and security assessments is essential to proactively detect and address any vulnerabilities or signs of unauthorized access. By staying vigilant and implementing these robust security measures, you can fortify your WiFi network against WiFi Pineapple attacks and ensure the safety of your digital communications.

Conclusion

To sum up, the WiFi Pineapple is a highly effective tool that can be used for wireless network security testing and penetration testing. It can simulate various types of attacks, monitor network traffic, and identify potential security threats. The WiFi Pineapple is a valuable tool for network administrators and security professionals who need to ensure the security of their wireless networks. However, it should only be used ethically and for legitimate purposes, as unauthorized use of the device can lead to legal consequences. With proper use and implementation, the WiFi Pineapple can help identify vulnerabilities and improve the overall security of wireless networks, potentially preventing security breaches and protecting against malicious attacks.

Cybersecurity | Network Security | Ethical Hacking | Penetration Testing | Wifi Pineapple

Published in InfoSec Write-ups

70K followers · Last published 1 day ago

Follow

A collection of write-ups from the best hackers in the world on topics ranging from bug bounties and CTFs to vulnhub machines, hardware challenges and real life encounters. Subscribe to our weekly newsletter for the coolest infosec updates: https://weekly.infosecwriteups.com/

Written by Jason Yee

44 followers · 42 following

Follow

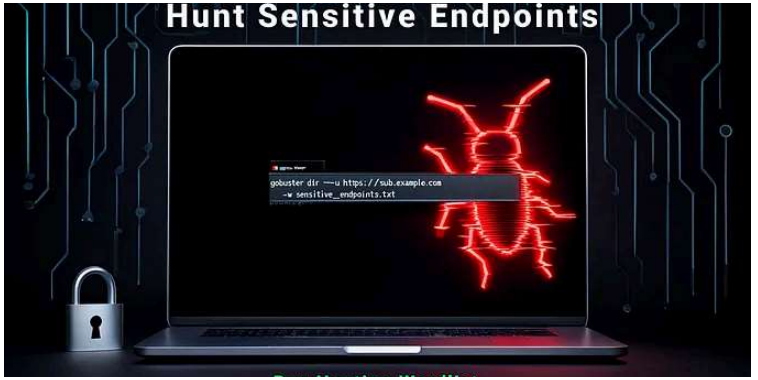
👋 IBDP Student, Front-End & AI Development. Cybersecurity Research
tech.withjasony.com

No responses yet

Write a response

What are your thoughts?

More from Jason Yee and InfoSec Write-ups



In InfoSec Write-ups by Jason Yee

Exploring the Capabilities of Flipper Zero and Ubertooth One:...

Part 2: Ubertooth One Features and Concluding Notes

Jul 24, 2023 45

In InfoSec Write-ups by Monika sharma

Sensitive Endpoint Wordlist for Bug Hunting

Uncover Hidden Flaws: A Powerful Wordlist for Bug Bounty Success

Sep 1 167 2

In InfoSec Write-ups by coffinxp

Mastering WordPress Bug Hunting: A Complete Guide for Security...

Learn step-by-step techniques, tools and strategies to uncover high-impact...

Aug 22 456 8

In InfoSec Write-ups by Jason Yee

Exploring the Capabilities of Flipper Zero and Ubertooth One:...

Part 1: Introduction to Wireless Security Testing, Flipper Zero Features, and...

Jul 24, 2023 60

See all from Jason Yee

See all from InfoSec Write-ups

Recommended from Medium

In Cyber Security Write-ups by Vipul Sonule

Bypassing WAFs Like a Hacker 🧙‍♂️: Tricks Hackers Use

5d ago 171 2

txc

Dissecting a msfvenom TCP reverse shell

Hi all,

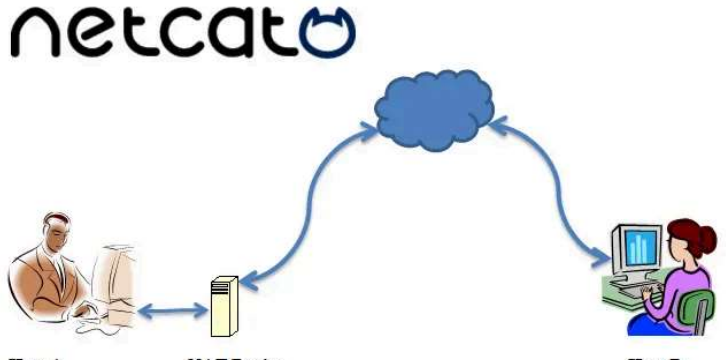
Apr 26 1

In InfoSec Write-ups by Aman Sharma

“Day 8: Mobile Hacking—How I Cracked a Banking App’s PIN in 1...

Two weeks ago, I reverse-engineered a “secure” banking app that claimed to use...

Aug 11 310 4



Hassen Hannachi

Lab 22—Netcat

Please follow these labs to get hands-on experience for CompTIA Security+ exam...

Apr 30 5