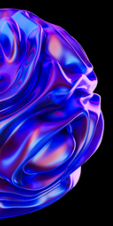
RED TEAMER GADGETS

HADESS

WWW.HADESS.IO



INTRODUCTION

Red team gadgets represent a crucial arsenal in the toolkit of cybersecurity professionals tasked with simulating real-world attacks against organizational defenses. These gadgets encompass a wide array of specialized hardware and software tools designed to exploit vulnerabilities, test defenses, and assess the resilience of systems, networks, and applications. Red teams operate under the premise of mimicking adversaries' tactics, techniques, and procedures (TTPs) to uncover weaknesses before malicious actors do. This introduction explores the significance of red team gadgets in cybersecurity operations and highlights their diverse functionalities and strategic importance.

First and foremost, red team gadgets are instrumental in conducting comprehensive security assessments known as penetration testing or ethical hacking. These tests simulate realistic attack scenarios to identify and mitigate vulnerabilities before they can be exploited maliciously. Gadgets such as network sniffers, wireless routers, and USB-based attack tools enable red teams to perform reconnaissance, exploit weaknesses, and demonstrate potential impact to stakeholders.

The versatility of red team gadgets is evident across various stages of a penetration test. During reconnaissance, tools like WiFi Pineapples and ZigBee auditors facilitate the discovery of target networks and devices, helping red teams map out attack surfaces and vulnerabilities. These gadgets leverage advanced capabilities such as rogue access point creation, packet sniffing, and protocol manipulation to gather intelligence and identify potential entry points.
Moreover, red team gadgets play a critical role in executing sophisticated attack vectors. Devices like USB Rubberducky and Shark Jack enable the deployment of pre-programmed payloads that exploit human and technological weaknesses. These gadgets simulate attacks ranging from USB-based exploits to network intrusions, illustrating the potential impact of real-world threats and demonstrating the need for robust defenses.

In addition to offensive capabilities, red team gadgets also aid in defensive assessments. They help organizations evaluate their incident response procedures, network monitoring capabilities, and overall resilience against sophisticated threats. By mimicking adversary tactics, red teams provide valuable insights into gaps in defenses and opportunities for improving cybersecurity posture.

Furthermore, the rapid evolution of technology and the proliferation of IoT devices have expanded the scope and complexity of red team engagements. Gadgets designed for IoT exploitation, such as Bluetooth sniffers, RFID cloners, and SIM card programmers, enable red teams to test the security of interconnected systems and smart devices thoroughly.
The effectiveness of red team gadgets lies in their ability to emulate real-world threats while adhering to ethical boundaries. By employing these tools, red teams enhance organizations' readiness to defend against cyberattacks, validate security investments, and foster a proactive approach to cybersecurity. Ultimately, red team gadgets serve as indispensable instruments in the ongoing battle to safeguard sensitive data, protect critical infrastructure, and mitigate the ever-evolving landscape of cyber threats.

DOCUMENT INFO

HADESS

To be the vanguard of cybersecurity, Hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish Hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.

At Hadess, our mission is twofold: to unleash the power of white hat hacking in punishing black hat hackers and to fortify the digital defenses of our clients. We are committed to employing our elite team of expert cybersecurity professionals to identify, neutralize, and bring to justice those who seek to exploit vulnerabilities. Simultaneously, we provide comprehensive solutions and services to protect our client's digital assets, ensuring their resilience against cyber attacks. With an unwavering focus on integrity, innovation, and client satisfaction, we strive to be the guardian of trust and security in the digital realm.

Security Researcher
Fazel Mohammad Ali Pour(https://x.com/ArganexEmad)

EXECUTIVE SUMMARY

Red team gadgets encompass a diverse range of specialized hardware and software tools tailored for penetration testing and ethical hacking purposes. These tools are designed to simulate real-world attack scenarios and assess the security posture of systems, networks, and applications comprehensively. Key categories of red team gadgets include network sniffers, WiFi Pineapples for rogue access point creation, USB Rubberducky for automated keystroke injections, SIM card cloners, and logic analyzers for debugging embedded systems. These gadgets enable red teams to perform tasks such as reconnaissance, exploitation, privilege escalation, and data exfiltration, providing valuable insights into vulnerabilities that could be exploited by malicious actors.

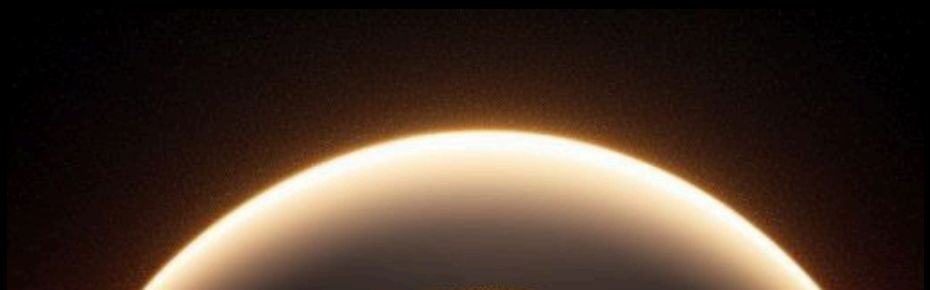
In practice, red team gadgets are utilized to identify vulnerabilities before they can be leveraged for malicious purposes. By mimicking attacker techniques and leveraging tools like WiFi Pineapples to mimic legitimate WiFi networks or USB Rubberducky for automated scripting attacks, red teams can demonstrate potential attack vectors and their impact on an organization's security posture. These assessments help organizations prioritize remediation efforts, enhance incident response procedures, and fortify defenses against real-world cyber threats.

Key Findings

Key findings from red team gadget assessments often highlight critical vulnerabilities in network infrastructure, application security flaws, weaknesses in IoT device security, and gaps in user awareness training. These assessments provide actionable intelligence to stakeholders by demonstrating how adversaries could exploit identified vulnerabilities to gain unauthorized access, steal sensitive information, or disrupt business operations. By uncovering these weaknesses proactively, organizations can implement targeted security measures to mitigate risks and strengthen their overall cybersecurity posture.

01

GADGETS



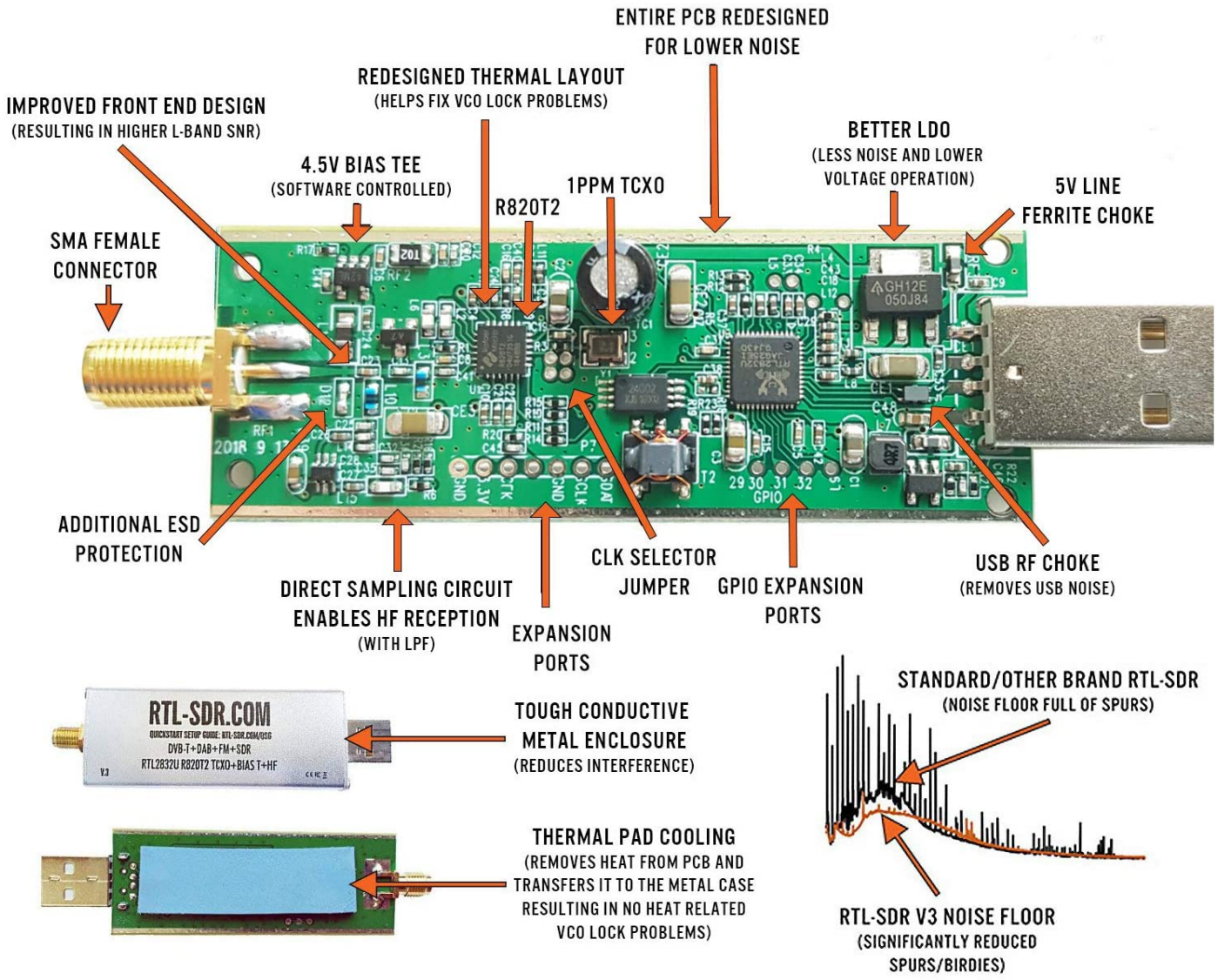
Red Teamer Gadgets

Red teamers, who are cybersecurity professionals specializing in emulating potential attackers to test the defenses of an organization, rely on a variety of gadgets and devices to conduct their activities. The Hacker's Hardware Toolkit on GitHub, curated by yadox666, offers an extensive list of such tools, emphasizing their practical applications in security assessments. Among the standout devices are the Bash Bunny and USB Rubber Ducky from Hak5, which enable red teamers to automate and execute complex scripts through USB ports, facilitating rapid payload deployment and data exfiltration. Another essential tool is the WiFi Pineapple, which is adept at intercepting and manipulating wireless network traffic, making it invaluable for testing Wi-Fi security and conducting man-in-the-middle attacks.

Additionally, the toolkit includes more advanced gadgets such as the HackRF One and Proxmark3, which are used for radio frequency analysis and RFID/NFC testing respectively. These devices empower red teamers to explore vulnerabilities in wireless communications and access control systems. Raspberry Pi and Arduino boards are also prominently featured, highlighting their versatility in creating custom, task-specific tools for physical and network-based attacks. The collection underscores the importance of both off-the-shelf solutions and customizable hardware in a red teamer's arsenal, enabling comprehensive and realistic security evaluations.

RTL-SDR v.3

CHOOSE A GENUINE RTL-SDR BLOG V3



FULL 2-YEAR WARRANTY AGAINST MANUFACTURING FAULTS
EMAIL & FORUM SUPPORT
SUPPORTS THE BLOG FOR NEW CONTENT, TUTORIALS AND PRODUCTS!

GENUINE GUARANTEE:
BE WARY OF INFERIOR
RTL-SDR BLOG V3 COUNTERFEITS!

The RTL-SDR v.3 is a highly popular and versatile USB dongle style software-defined radio (SDR) receiver, known for its wide compatibility and robust features. Equipped with the RTL2832U ADC chip, R820T2 tuner, 1PPM TCXO, SMA F connector, and housed in an aluminum case with passive cooling, this device offers excellent performance for its price. It covers a frequency range from 500 kHz to 1.7 GHz and provides up to 3.2 MHz (2.4 MHz stable) of bandwidth. Operating in direct sampling mode, it can tune to HF frequencies as well. The RTL-SDR v.3 is compatible with various operating systems, including Windows, OSX, Linux, and Android, and works seamlessly with popular SDR software such as SDR#, HDSDR, SDR-Radio, GQRX, and SDR Touch. It is ideal for numerous applications, including general radio scanning, air traffic control monitoring, public safety communication, ADS-B aircraft radar, ACARS, trunked radio, P25/MotoTRBO digital voice, weather balloons, APRS, NOAA APT/Meteor M2 weather satellites, radio astronomy, DAB, and classroom learning. Additionally, it can serve as a low-cost panadapter for ham radios. The V3 model includes several enhancements like an improved R820T2 tuner, a 1PPM TCXO, a

redesigned lower noise PCB, cooling improvements, extra ESD protection, and a software bias-tee for powering LNAs and active antennas.

Attack Scenario

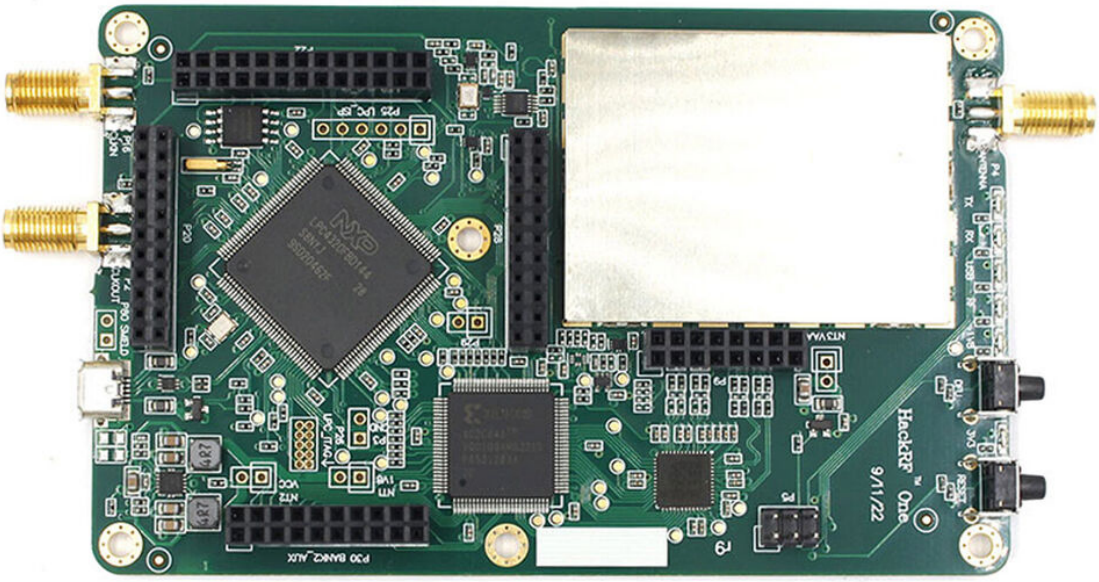
A red teamer can deploy the RTL-SDR v.3 to intercept and analyze a wide range of wireless communications within the device's frequency capabilities. During a penetration test, this device can be utilized to capture unencrypted transmissions from various sources such as air traffic control systems, public safety channels, or trunked radio networks. By using software tools compatible with RTL-SDR v.3, the red teamer can monitor these communications in real-time, potentially extracting sensitive information or identifying exploitable vulnerabilities in the wireless infrastructure. For instance, the device can be used to decode ADS-B signals from aircraft, track ACARS messages, or listen to P25/MotoTRBO digital voice communications. Additionally, the red teamer can leverage its ability to detect and analyze unauthorized transmissions or interference sources, enhancing situational awareness and uncovering potential attack vectors in the target environment.

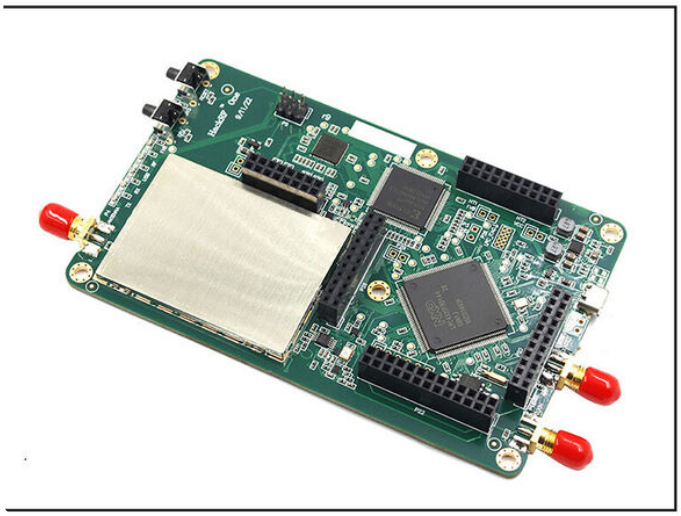
Red Team Attacks List

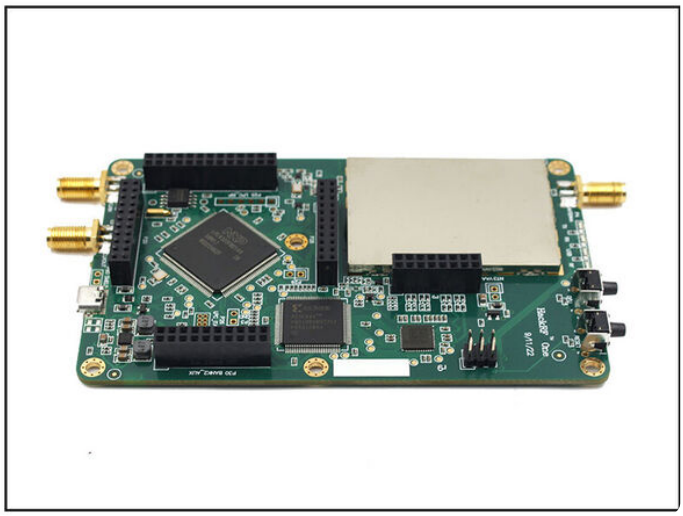
1. **Interception of Air Traffic Control Communications:** Capture and analyze unencrypted air traffic control signals to gather intelligence on flight operations.
2. **Monitoring Public Safety Channels:** Eavesdrop on police, fire, and emergency medical services to obtain real-time operational details.
3. **ADS-B Aircraft Radar:** Track aircraft movements and potentially infer sensitive flight plans or cargo details.
4. **Trunked Radio Systems:** Intercept and decode communications in trunked radio networks used by large organizations and government entities.
5. **P25/MotoTRBO Digital Voice:** Decode encrypted or unencrypted digital voice communications used in secure radio systems.
6. **ACARS Data Capture:** Extract aircraft communication addressing and reporting system messages to analyze flight data.
7. **Weather Balloon Telemetry:** Intercept and decode telemetry data from weather balloons to study environmental monitoring techniques.
8. **NOAA APT/Meteor M2 Satellites:** Capture weather satellite images and data transmissions for analysis.

HackRF One

HackRF One(1MHz-6GHz) Open Source Software Radio Platform SDR Development Board







The HackRF One from Great Scott Gadgets is a versatile and powerful software-defined radio (SDR) peripheral capable of both transmission and reception of radio signals, covering a frequency range from 1 MHz to 6 GHz. Designed for the testing and development of modern and next-generation radio technologies, this open-source hardware platform can operate as a USB peripheral or in a standalone mode. Notable for its ability to function as a half-duplex transceiver, it supports up to 20 million samples per second with 8-bit quadrature sampling. The HackRF One is compatible with popular SDR software like GNU Radio and SDR#, and features software-configurable RX and TX gain, a baseband filter, and an antenna port with power control. It includes SMA female connectors for both the antenna and clock input/output, buttons for user programming, and internal pin headers for expansion. It is powered via USB and is based on an open-source hardware licensing model.

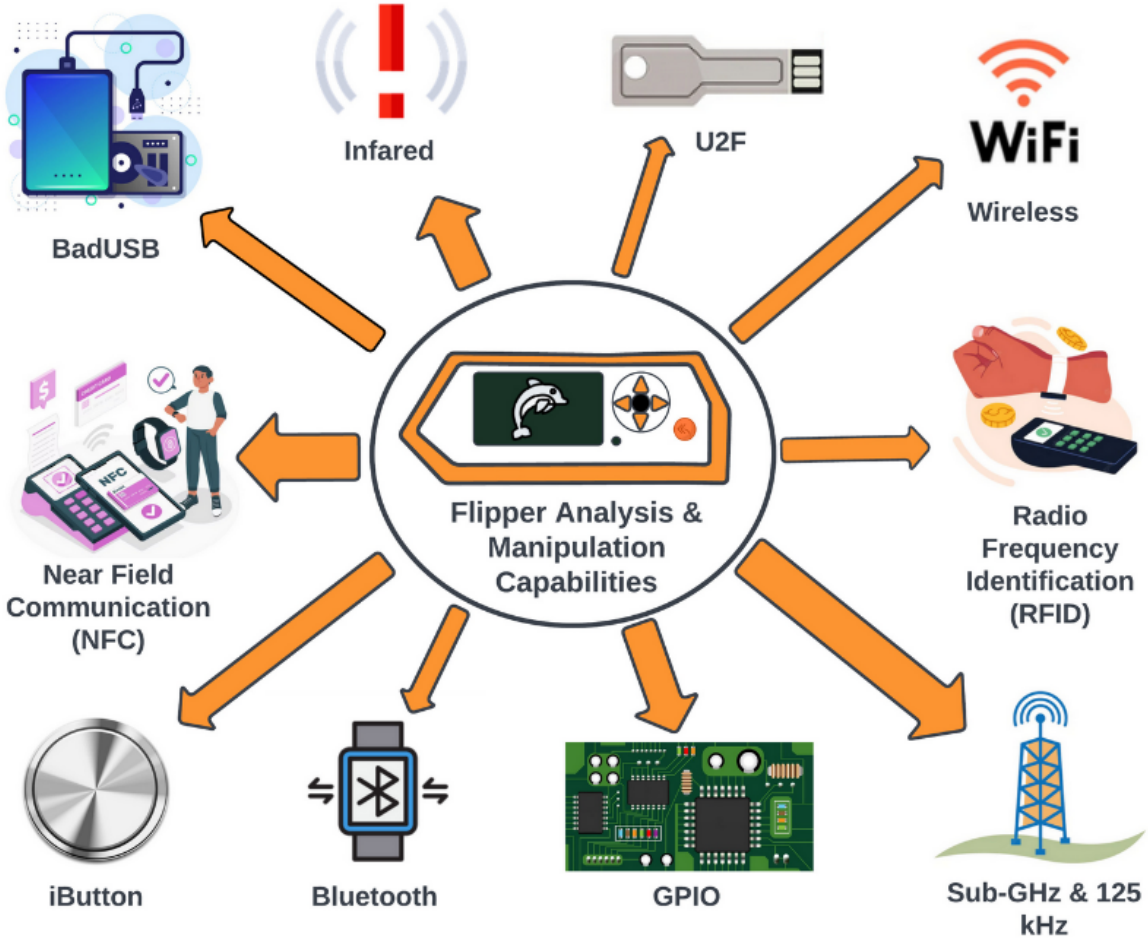
Attack Scenario

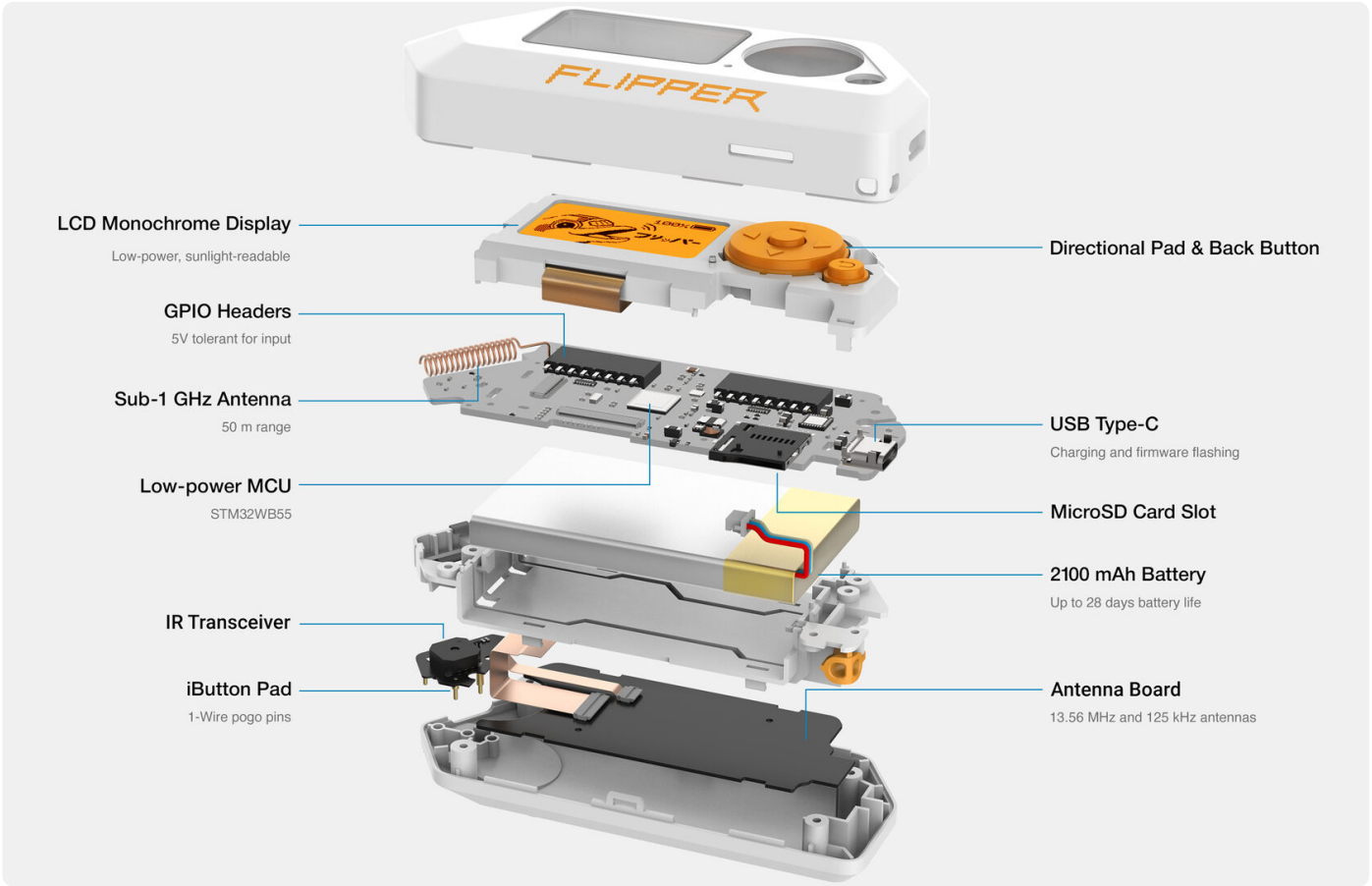
A red teamer can leverage the HackRF One to execute a wide range of attacks that require both the reception and transmission of radio signals. For instance, the device can be used to spoof signals to create false entries in an ADS-B aircraft tracking system, causing confusion or misdirection. Additionally, it can be employed to jam or disrupt legitimate wireless communications within the covered frequency range, including Wi-Fi, Bluetooth, or public safety channels. By using its transmission capabilities, a red teamer can also perform replay attacks, capturing a legitimate signal and retransmitting it to gain unauthorized access to systems or data. The device's wide frequency range and compatibility with various software tools make it a formidable asset in identifying and exploiting vulnerabilities in radio-based systems.

Red Team Attacks List

1. **Signal Spoofing:** Transmit false signals to deceive receivers, such as faking ADS-B aircraft positions or GPS signals.
2. **Jamming Attacks:** Disrupt communication channels like Wi-Fi, Bluetooth, or public safety frequencies by transmitting interference signals.
3. **Replay Attacks:** Capture and retransmit legitimate signals to gain unauthorized access to systems, such as keyless entry systems.
4. **Wireless Protocol Analysis:** Intercept and analyze proprietary wireless communications to discover vulnerabilities.
5. **Testing SDR Applications:** Develop and test custom radio applications or proof-of-concept exploits targeting specific radio technologies.
6. **Frequency Hopping Attacks:** Analyze and disrupt frequency-hopping spread spectrum (FHSS) systems by predicting hopping sequences.
7. **RFID and NFC Exploitation:** Intercept and manipulate RFID or NFC communications for unauthorized access or data extraction.
8. **Broadcast Signal Manipulation:** Inject false information into broadcast systems like FM radio or digital TV.
9. **Remote Control Interception:** Capture and replicate signals from remote controls to manipulate devices like garage doors or drones.

Flipper Zero


BadUSB
Infared
U2F
WiFi
Wireless
Flipper Analysis & Manipulation Capabilities
Near Field Communication (NFC)
Radio Frequency Identification (RFID)
iButton
Bluetooth
GPIO
Sub-GHz & 125 kHz


FLIPPER
LCD Monochrome Display
Low-power, sunlight-readable
GPIO Headers
5V tolerant for input
Sub-1 GHz Antenna
50 m range
Low-power MCU
STM32WB55
IR Transceiver
iButton Pad
1-Wire pogo pins
Directional Pad & Back Button
USB Type-C
Charging and firmware flashing
MicroSD Card Slot
2100 mAh Battery
Up to 28 days battery life
Antenna Board
13.56 MHz and 125 kHz antennas

Flipper Zero is a compact, versatile multi-tool designed for hackers, pentesters, and electronics enthusiasts. This portable device is equipped with a wide range of built-in features, including RFID, NFC, infrared transceiver, GPIO pins, and a sub-1 GHz transceiver. It has a unique playful design with a monochrome LCD screen and a simple user interface, making it accessible for both novices and experts. The Flipper Zero supports various communication protocols and can emulate, read, and write to numerous devices and systems. It is an open-source platform, allowing for custom firmware development and expansion of its capabilities. Its portability and multifunctionality make it an ideal tool for a wide range of hacking and security testing scenarios.

Attack Scenario

A red teamer can utilize the Flipper Zero in numerous ways to assess and exploit vulnerabilities in a target's security infrastructure. For example, the device's RFID and NFC capabilities can be used to clone access cards, enabling unauthorized entry into secure areas. The infrared transceiver can capture and replicate signals from remote controls, allowing the red teamer to control devices like TVs, projectors, or other IR-enabled systems. Additionally, the sub-1 GHz transceiver can intercept and analyze wireless communications, such as those from keyless entry systems, to perform replay attacks. The GPIO pins provide the flexibility to interface with various electronic systems, making it possible to test and manipulate hardware directly.

Red Team Attacks List

1. **RFID Cloning:** Capture and replicate RFID card signals to gain unauthorized access to secure areas.
2. **NFC Manipulation:** Read, write, and emulate NFC tags to interact with contactless payment systems or access control systems.
3. **Infrared Signal Replication:** Capture and transmit infrared signals from remote controls to manipulate IR-enabled devices.
4. **Wireless Communication Interception:** Use the sub-1 GHz transceiver to intercept and analyze wireless communications for vulnerabilities.
5. **Replay Attacks:** Record and replay signals from keyless entry systems to unlock vehicles or buildings.
6. **GPIO Interfacing:** Connect to and manipulate electronic systems using GPIO pins for hardware testing and exploitation.
7. **Custom Firmware Development:** Create and deploy custom firmware to extend the functionality of the Flipper Zero for specific attack scenarios.
8. **Signal Jamming:** Disrupt communication by transmitting noise or interference signals within supported frequency ranges.
9. **Bluetooth Exploitation:** Intercept and manipulate Bluetooth communications to access and control Bluetooth-enabled devices.

M5StickC Plus

The M5StickC Plus is a compact, versatile development board from M5Stack, featuring an ESP32 microcontroller with built-in Wi-Fi and Bluetooth capabilities. It comes with a 1.14-inch TFT display, a six-axis IMU sensor, a built-in battery, and several GPIO pins for expansion. Designed for portability and ease of use, the M5StickC Plus supports various development environments, including Arduino, MicroPython, and UIFlow, making it suitable for both beginners and experienced developers. Its small form factor and rich feature set make it ideal for creating IoT projects, wearable devices, and rapid prototyping.

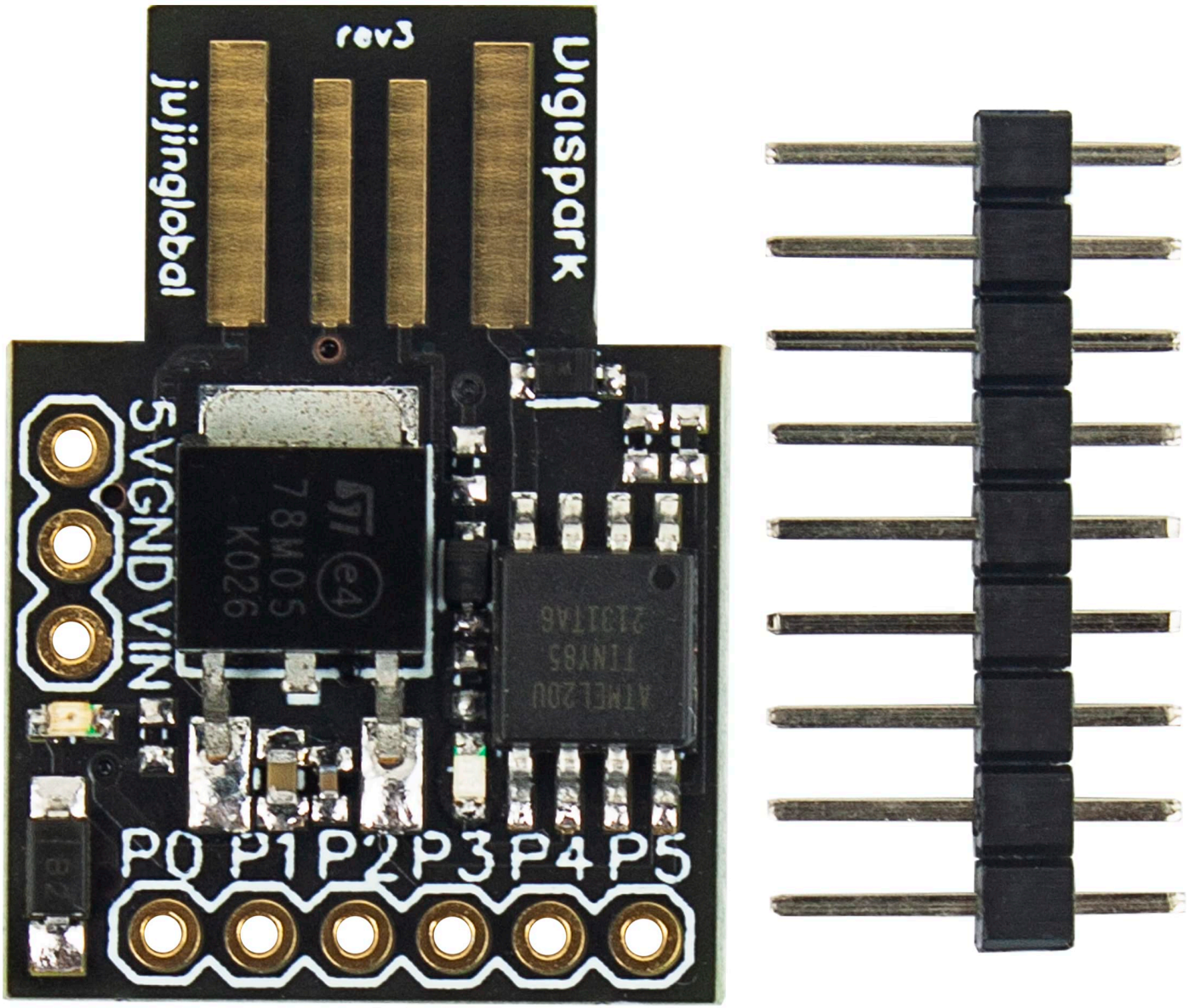
Attack Scenario

A red teamer can leverage the M5StickC Plus to conduct various wireless and hardware-based attacks. For example, its Wi-Fi capabilities can be used to create rogue access points or perform deauthentication attacks to disrupt legitimate Wi-Fi communications. The built-in Bluetooth functionality can be utilized to intercept and manipulate Bluetooth communications. Additionally, the GPIO pins allow the red teamer to interface with and exploit hardware systems directly, such as accessing and manipulating sensors or control systems. Its portability and programmability enable the creation of custom tools tailored to specific attack scenarios.

Red Team Attacks List

1. **Rogue Access Point:** Set up a rogue Wi-Fi access point to capture credentials and monitor network traffic.
2. **Wi-Fi Deauthentication Attack:** Disrupt legitimate Wi-Fi communications by sending deauthentication frames to connected devices.
3. **Bluetooth Interception:** Intercept and manipulate Bluetooth communications to gain unauthorized access to Bluetooth-enabled devices.
4. **Custom Payload Deployment:** Program the device to deploy custom payloads or scripts for automated attacks on networked systems.
5. **Hardware Manipulation:** Use GPIO pins to interface with and exploit hardware systems, such as sensors or control units.
6. **Credential Harvesting:** Capture and store credentials from Wi-Fi networks or Bluetooth devices.
7. **Network Scanning:** Conduct Wi-Fi or Bluetooth scanning to identify and enumerate devices and networks within range.
8. **Sensor Spoofing:** Manipulate sensor inputs to disrupt or deceive systems that rely on accurate sensor data.
9. **Data Exfiltration:** Use Wi-Fi or Bluetooth to exfiltrate sensitive data from compromised systems.

Los Digispark ATTINY85 Micro USB Dev Board Arduino



The Los Digispark ATTINY85 Micro USB Dev Board is a compact and cost-effective development board designed around the ATTINY85 microcontroller. Despite its small size, it features a micro USB interface for programming and power, six I/O pins, and support for the Arduino IDE. The ATTINY85 microcontroller is capable of running at 8 MHz or 16 MHz, making it suitable for a variety of small-scale projects and prototypes. Its simplicity and affordability make it an excellent choice for beginners and experienced developers looking to create compact and efficient electronic projects.

Attack Scenario

A red teamer can use the Digispark ATTINY85 Dev Board to perform various stealthy and low-cost attacks. One possible attack is to deploy it as a HID (Human Interface Device) emulation tool, where it can act as a

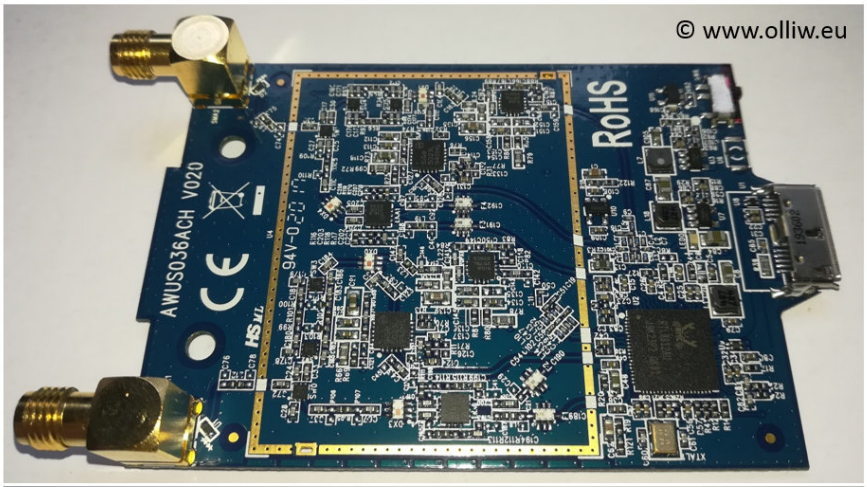
malicious USB keyboard or mouse to inject keystrokes or commands when plugged into a target computer. This can be used to install malware, open backdoors, or exfiltrate data without raising suspicion. Additionally, the board's small size allows it to be easily concealed within other devices or enclosures, making it ideal for covert operations.

Red Team Attacks List

1. **HID Injection Attack:** Program the device to act as a USB keyboard, injecting malicious keystrokes to execute commands or scripts on the target system.
2. **Credential Harvesting:** Use HID capabilities to open terminal or browser windows and extract credentials or sensitive information.
3. **Malware Deployment:** Automate the installation of malware by injecting commands that download and execute malicious software.
4. **Data Exfiltration:** Configure the device to exfiltrate data by typing out sensitive information and sending it via email or uploading it to cloud services.
5. **Automated Exploits:** Deploy automated exploits or payloads that take advantage of known vulnerabilities in the target system.
6. **Network Configuration Manipulation:** Use HID capabilities to change network settings or introduce rogue configurations on the target system.
7. **Phishing Attacks:** Open phishing websites or fake login pages using injected keystrokes to capture user credentials.
8. **System Reconfiguration:** Modify system settings or configurations to weaken security measures or create persistence for further attacks.
9. **Wireless Network Attacks:** Interface with external Wi-Fi or Bluetooth modules to perform wireless network attacks such as rogue access points or deauthentication.

Alfa AWUS-036ACH

Alfa AWUS036ACH



The Alfa AWUS-036ACH is a high-performance dual-band USB wireless adapter, designed to deliver exceptional Wi-Fi connectivity over both 2.4 GHz and 5 GHz frequencies. This device supports the latest 802.11ac standards, providing data transfer speeds of up to 300Mbps on 2.4GHz and up to 867Mbps on 5GHz networks. The adapter connects to PCs via a USB 3.0 interface, ensuring high-speed data transmission. It is equipped with two high-sensitivity dual-band dipole antennas, enhancing signal strength and coverage to eliminate dead zones in your living space. Compatible with Windows, MacOS, and Linux, the AWUS-036ACH is ideal for HD video streaming, large file downloads, and general web browsing.

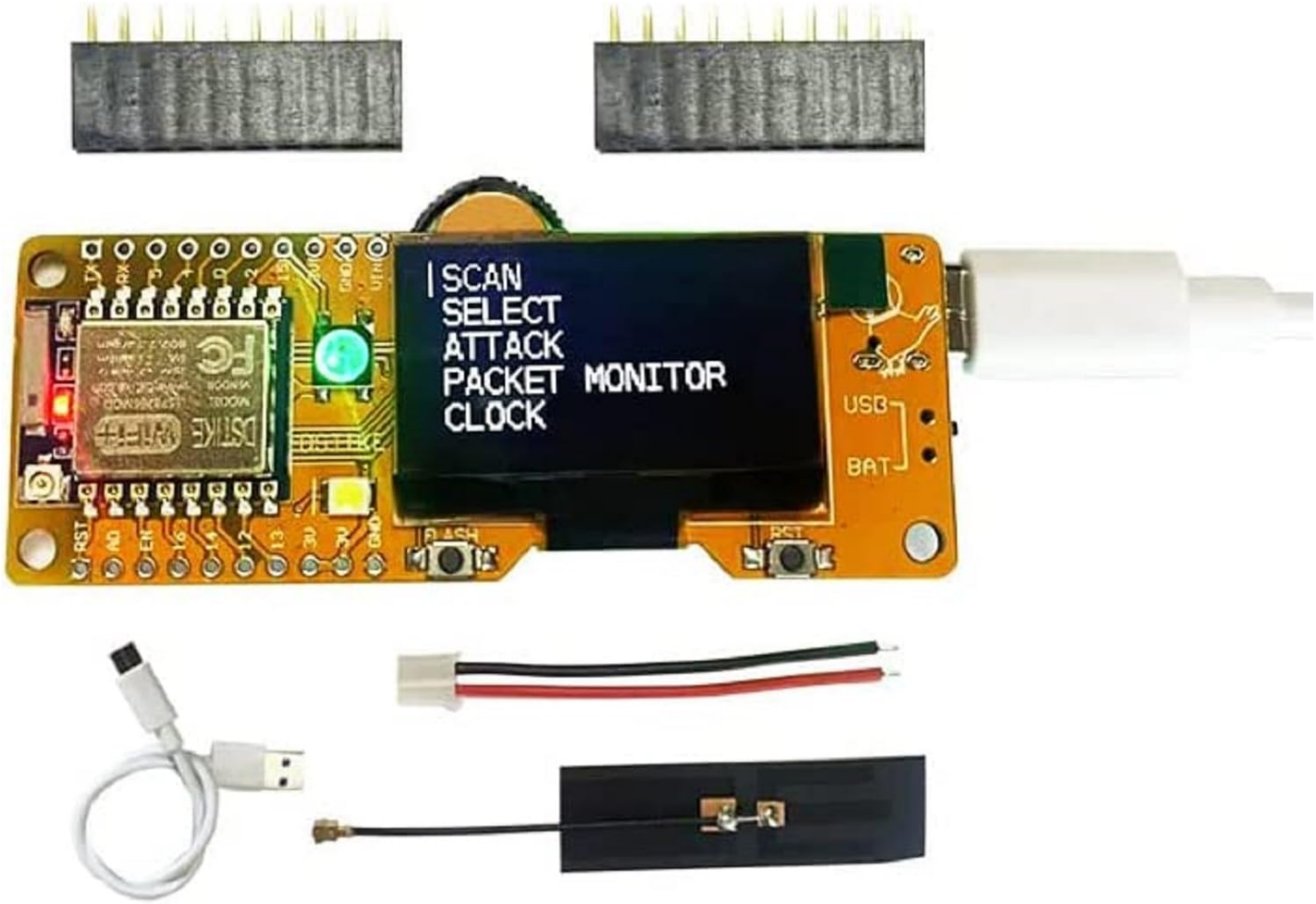
Attack Scenario

A red teamer can exploit the Alfa AWUS-036ACH to conduct a range of Wi-Fi attacks due to its powerful signal reception and transmission capabilities. For example, the device can be used to perform packet sniffing, capturing network traffic for analysis and identifying vulnerabilities. Its ability to connect to both 2.4 GHz and 5 GHz networks allows it to exploit weaknesses in various Wi-Fi protocols and encryption standards. Additionally, the adapter can be employed to create rogue access points, deauthenticate clients from legitimate networks, or perform man-in-the-middle attacks to intercept and manipulate data.

Red Team Attacks List

1. **Packet Sniffing:** Capture and analyze network traffic to identify sensitive information, credentials, or vulnerabilities.
2. **Rogue Access Point:** Set up a fake Wi-Fi access point to intercept and manipulate network traffic from unsuspecting users.
3. **Deauthentication Attack:** Disrupt legitimate Wi-Fi connections by sending deauthentication frames to connected devices.
4. **Man-in-the-Middle (MITM) Attack:** Intercept and alter communications between devices on the network to steal data or inject malicious content.
5. **Evil Twin Attack:** Clone a legitimate Wi-Fi network to trick users into connecting to a malicious access point.
6. **Wi-Fi Jamming:** Transmit interference signals to disrupt Wi-Fi communications and create denial-of-service conditions.
7. **Credential Harvesting:** Capture login credentials and other sensitive information from intercepted network traffic.
8. **WEP/WPA/WPA2 Cracking:** Use the adapter's capabilities to crack weak Wi-Fi encryption and gain unauthorized access to protected networks.
9. **Network Scanning:** Identify and enumerate nearby Wi-Fi networks, devices, and their security configurations for further exploitation.

Wi-Fi Deauther



The Wi-Fi Deauther is a compact and powerful 2.4 GHz Wi-Fi device based on the ESP8266 microcontroller. Unlike traditional jammers that create noise across a frequency range, the deauther exploits a vulnerability in the Wi-Fi (802.11) standard to send deauthentication packets, causing devices to disconnect from the network. This selective targeting makes it a precise tool for network testing. The device features an integrated 18650 charging system, an OLED display, and a 3-axis slide switch, and it comes pre-installed with the latest ESP8266 Deauther software. It is capable of various Wi-Fi network attacks, making it an invaluable tool for penetration testers.

Attack Scenario

A red teamer can utilize the Wi-Fi Deauther to disrupt network communications selectively by sending deauthentication packets to targeted devices. This can be particularly useful in scenarios where a red teamer needs to test the resilience of a network to deauthentication attacks or create opportunities for more sophisticated exploits. For instance, the deauther can be used to kick devices off a network, forcing them to reconnect and potentially capture authentication handshakes for further analysis. The device's small size and OLED display make it convenient for covert operations and real-time monitoring.

Red Team Attacks List

1. **Deauthentication Attack:** Disrupt network connectivity for targeted devices by sending deauth packets, causing them to disconnect from the network.
2. **Handshake Capture:** Force devices to reconnect to the network, capturing WPA/WPA2 handshakes for offline cracking.
3. **Targeted Network Disruption:** Selectively disconnect specific devices without affecting the entire network, useful for isolating and testing security of individual systems.
4. **Client-Side Denial of Service:** Continuously deauthenticate specific clients, effectively preventing them from maintaining a stable connection to the network.
5. **Rogue AP Detection:** Use deauth packets to identify rogue access points by observing their response to the attack.
6. **Access Point Testing:** Evaluate the robustness of access points against deauthentication attacks and other Wi-Fi vulnerabilities.
7. **Security Awareness Training:** Demonstrate the impact of deauthentication attacks in security training sessions to educate users about Wi-Fi security.
8. **Network Reconnaissance:** Identify active devices on a network and their corresponding access points by observing deauth responses.
9. **Evasion Tactics:** Use deauth packets to temporarily disable security cameras or other monitoring devices that rely on Wi-Fi connectivity.

Proxmark3-EVO

The Proxmark3-EVO is an advanced and versatile tool designed for RFID analysis and penetration testing. It supports a wide range of RFID systems operating at both low-frequency (125/134 KHz) and high-frequency (13.56 MHz) bands. Capabilities include reading, writing, analysis, snooping, replaying, emulation, modulation, demodulation, decoding, and encoding for various RFID protocols. Optimized for desktop users and hobbyists, the Proxmark3-EVO features a powerful CPU (AT91SAM7S512), external and internal memory, and pre-tuned antennas for both LF and HF frequencies. It is housed in a durable ABS case and includes various RFID tags/cards for testing and demonstration purposes.

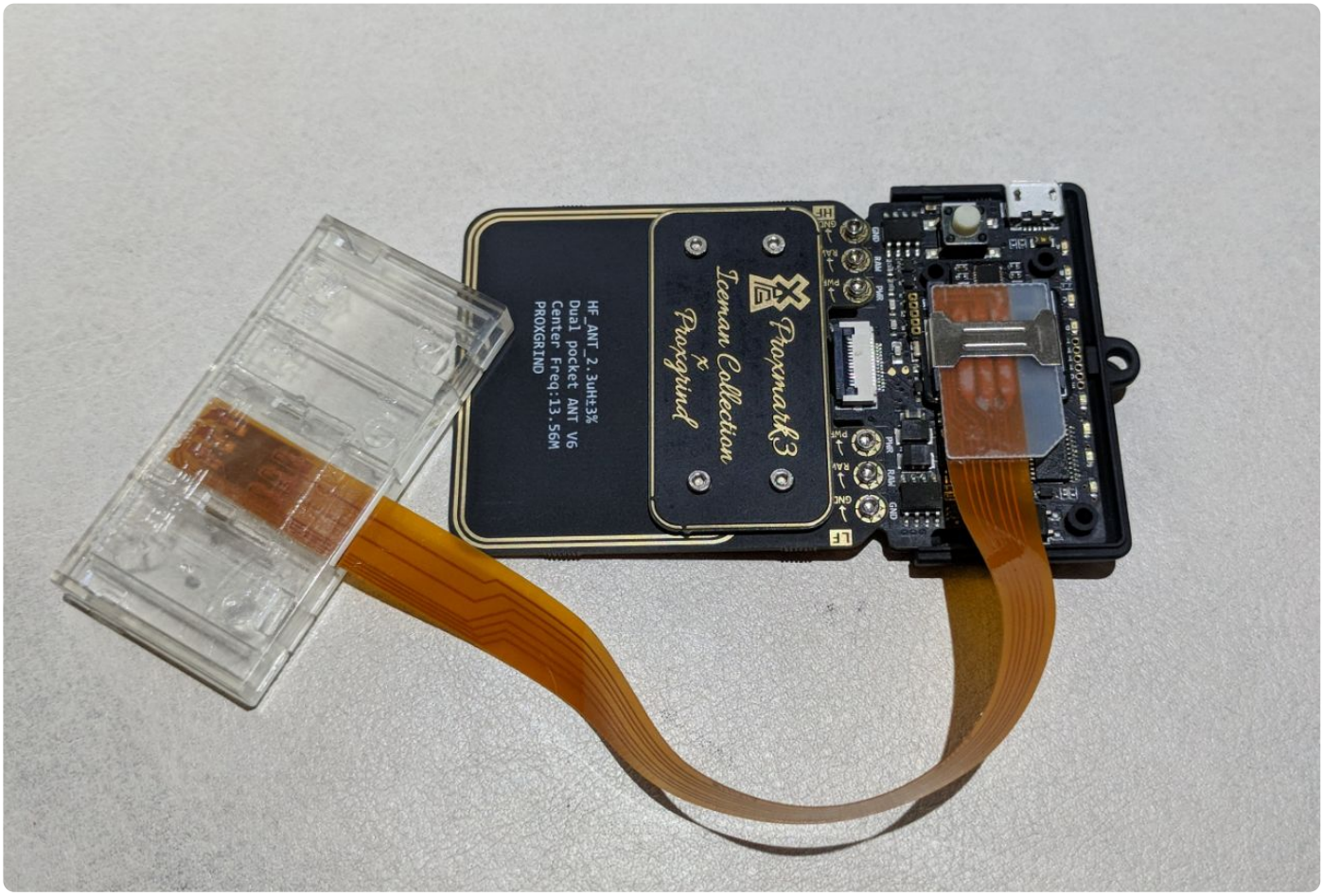
Attack Scenario

Red teamers can leverage the Proxmark3-EVO to exploit vulnerabilities in RFID systems used for access control, identification, and payment purposes. For example, the device can be used to clone RFID cards, allowing unauthorized access to secured areas. It can also intercept and replay RFID signals to spoof legitimate access credentials, bypassing physical security measures. Additionally, the Proxmark3-EVO can sniff RFID communication to capture sensitive data or perform cryptographic attacks to decrypt RFID authentication protocols. Its versatile capabilities make it a crucial tool for assessing the security posture of RFID-based systems.

Red Team Attacks List

1. **RFID Cloning:** Clone RFID cards to gain unauthorized access to secure areas or facilities.
2. **RFID Emulation:** Emulate RFID cards to impersonate legitimate users and bypass access control systems.
3. **Signal Replay:** Capture and replay RFID signals to spoof access credentials and gain entry into restricted areas.
4. **RFID Snooping:** Intercept and analyze RFID communication to capture data exchanged between RFID readers and tags.
5. **Cryptographic Attacks:** Perform cryptographic attacks to crack RFID encryption keys and authenticate as valid users.
6. **Data Extraction:** Extract sensitive information stored on RFID tags, such as personal identification or payment data.
7. **Protocol Analysis:** Analyze RFID protocols to identify vulnerabilities and weaknesses in RFID implementations.
8. **Brute Force Attacks:** Use the Proxmark3-EVO to conduct brute force attacks on RFID systems to guess PINs or authentication codes.
9. **Cloning RFID Tags:** Clone specific RFID tags for testing or exploitation purposes to demonstrate vulnerabilities.

SIM/SAM Extension for Proxmark3 RDV4



The SIM/SAM Extension for Proxmark3 RDV4 is a specialized module designed to enhance the capabilities of the Proxmark3 RDV4 for analyzing and manipulating SIM (Subscriber Identity Module) and SAM (Secure Access Module) cards. It connects directly to the SIM/SAM slot on the Proxmark 3 RDV4 device, expanding its functionality to support various contact card systems based on NFC technology. This extension is crucial for security researchers, penetration testers, and forensic analysts who need to interact with and extract data from SIM and SAM cards used in telecommunications and financial industries.

Attack Scenario

Red teamers can use the SIM/SAM Extension to perform sophisticated attacks targeting SIM and SAM cards. For instance, the module enables researchers to debug, program, and manipulate SIM and SAM cards, allowing for the extraction of sensitive information such as cryptographic keys, PIN codes, and subscriber data. With access to these credentials, attackers can potentially clone SIM cards, impersonate legitimate users, and gain unauthorized access to cellular networks or secure access control systems. This capability is invaluable for assessing the security of SIM and SAM implementations in real-world scenarios.

Red Team Attacks List

1. **Data Extraction:** Extract sensitive information such as IMSI (International Mobile Subscriber Identity) or authentication keys from SIM cards.

2. **SIM Cloning:** Clone SIM cards to impersonate legitimate users and gain unauthorized access to cellular networks.
3. **PIN Manipulation:** Manipulate SIM card PIN codes to bypass authentication or disable security features.
4. **Authentication Bypass:** Use extracted credentials to bypass authentication mechanisms and gain access to secured systems.
5. **Man-in-the-Middle (MITM) Attacks:** Intercept and modify communications between SIM cards and network operators to eavesdrop or inject malicious content.
6. **SIM Toolkit (STK) Exploitation:** Exploit vulnerabilities in SIM Toolkit applications to perform actions on behalf of the user without their knowledge.
7. **Secure Element Analysis:** Analyze the security of SAM cards used in access control systems to identify vulnerabilities or backdoor access.
8. **Cryptographic Attacks:** Perform cryptographic attacks to crack encryption keys used to secure communications between SIM cards and network operators.
9. **Forensic Analysis:** Use the SIM/SAM Extension for forensic investigations to recover deleted or hidden data from SIM cards used in criminal activities.

125KHz RFID Cloner / 13.56MHz RFID/NFC Reader/Writer

The 125KHz RFID Cloner and 13.56MHz RFID/NFC Reader/Writer is a dual-frequency device capable of cloning RFID cards and reading/writing NFC tags. It supports cloning of RFID cards based on EM4100,

HID, and AWID protocols, as well as writing to writable Chinese tags like T5577. This standalone device operates independently of a computer, making it straightforward to use. Users can read the unique ID (UID) from an original RFID card and then clone it onto a blank T5577 or similar tag. It features built-in LED lights and a buzzer indicator for status feedback during operations, and it is compatible with various RFID standards commonly used in access control and identification systems.

Attack Scenario

Red teamers can employ the 125KHz RFID Cloner / 13.56MHz RFID/NFC Reader/Writer to compromise physical security systems that rely on RFID technology. For example, attackers can clone access cards used for building entry systems, gaining unauthorized access to secured areas. By reading and writing to NFC tags, the device can also be used for malicious activities such as implanting malicious tags to trigger actions on NFC-enabled devices or systems. Its portability and ease of use make it suitable for covert operations where quick access to cloned credentials is crucial.

Red Team Attacks List

1. **RFID Card Cloning:** Clone RFID cards (EM4100, HID, AWID) to gain unauthorized access to buildings or facilities.
2. **Access Control Bypass:** Use cloned RFID cards to bypass physical access controls and enter restricted areas.
3. **NFC Tag Manipulation:** Write malicious data to NFC tags to exploit vulnerabilities in NFC-enabled systems or devices.
4. **Impersonation Attacks:** Clone RFID cards to impersonate authorized personnel and perform actions on their behalf.
5. **Physical Security Testing:** Assess the effectiveness of RFID-based security systems by testing cloned credentials against access controls.
6. **Social Engineering:** Use cloned credentials to facilitate social engineering attacks, gaining trust or access under false pretenses.
7. **Malware Delivery:** Use NFC tags to deliver malware or malicious scripts to NFC-enabled devices when scanned.
8. **Asset Tracking:** Use NFC tags for tracking purposes, embedding them in items to monitor their movement through NFC-enabled checkpoints.
9. **Data Exfiltration:** Hide stolen data on NFC tags for later retrieval or transmit sensitive information through NFC channels.

Programmable SIM USIM Card

The Programmable SIM USIM Card kit includes 10 units of blank SIM USIM cards designed for testing purposes. These cards are similar in form to those used by telecommunications operators and can be cut into various sizes: Standard SIM, Micro SIM, and Nano SIM. They are compatible with 4G LTE, WCDMA, and GSM networks, offering flexibility for testing across different cellular technologies. The cards are programmable, allowing users to write essential information such as ICCID (Integrated Circuit Card Identifier), IMSI (International Mobile Subscriber Identity), KI (Authentication Key), and OPC (Over-the-air Programming Key). This capability makes them essential tools for testing and development in the telecommunications sector.

Attack Scenario

Red teamers can utilize the Programmable SIM USIM Cards to simulate and test various attack scenarios on mobile networks. For instance, they can program these cards with IMSI numbers obtained through reconnaissance or social engineering. By inserting these SIM cards into devices, attackers can attempt to register on cellular networks with falsified credentials, bypassing authentication mechanisms or tricking networks into granting unauthorized access. Furthermore, these cards can be used to conduct man-in-the-middle attacks on mobile communications or intercept sensitive data transmitted over cellular networks.

Red Team Attacks List

1. **Impersonation Attacks:** Use programmed SIM cards to impersonate legitimate subscribers and gain unauthorized access to mobile networks.
2. **IMSI Catching:** Program SIM cards with fake IMSI numbers to collect IMSI numbers from nearby mobile devices for tracking or targeting.
3. **Registration Spoofing:** Spoof the registration process by presenting a falsified IMSI to the mobile network, bypassing authentication checks.
4. **SIM Card Cloning:** Clone legitimate SIM cards by extracting and replicating their ICCID and IMSI details onto programmable SIM cards.
5. **Network Penetration Testing:** Test the resilience of mobile network infrastructure by attempting to register programmable SIM cards with altered or unauthorized credentials.
6. **Over-the-Air Attacks:** Exploit vulnerabilities in OTA (Over-the-Air) updates by intercepting and modifying communication between SIM cards and network operators.
7. **Mobile Network Surveillance:** Monitor and intercept mobile communications by inserting programmed SIM cards into devices set to relay communications.
8. **Traffic Redirection:** Redirect mobile network traffic through a compromised SIM card to capture or manipulate data exchanged between devices and the network.
9. **Subscriber Tracking:** Use IMSI numbers programmed into SIM cards to track and identify specific mobile devices as they connect to different cellular towers.

MSR605/MSR606 Credit Card Reader Typewriter with Bluetooth, USB Magnetic Strip Card Terminal

Read	✔	Success Rate	100%
Write	✔	Decode Speed	0.1s
Bluetooth	✔	Magnetic Head	III
Work with MAC	✔	Magnetic Head Life Swipe times	1,000.000

The MSR605/MSR606 is a versatile magnetic stripe card reader/writer terminal equipped with Bluetooth and USB connectivity options. It is commonly used for reading, writing, and encoding data onto magnetic stripe cards such as credit cards, debit cards, and access control cards. The device supports both Hi-Co (high coercivity) and Lo-Co (low coercivity) magnetic cards, offering flexibility for various magnetic stripe technologies. It can be connected to a computer via USB or operated wirelessly via Bluetooth, making it convenient for both stationary and mobile applications. The MSR605/606 is often used in retail, banking, and security industries for card encoding, authentication, and data retrieval purposes.

Attack Scenario

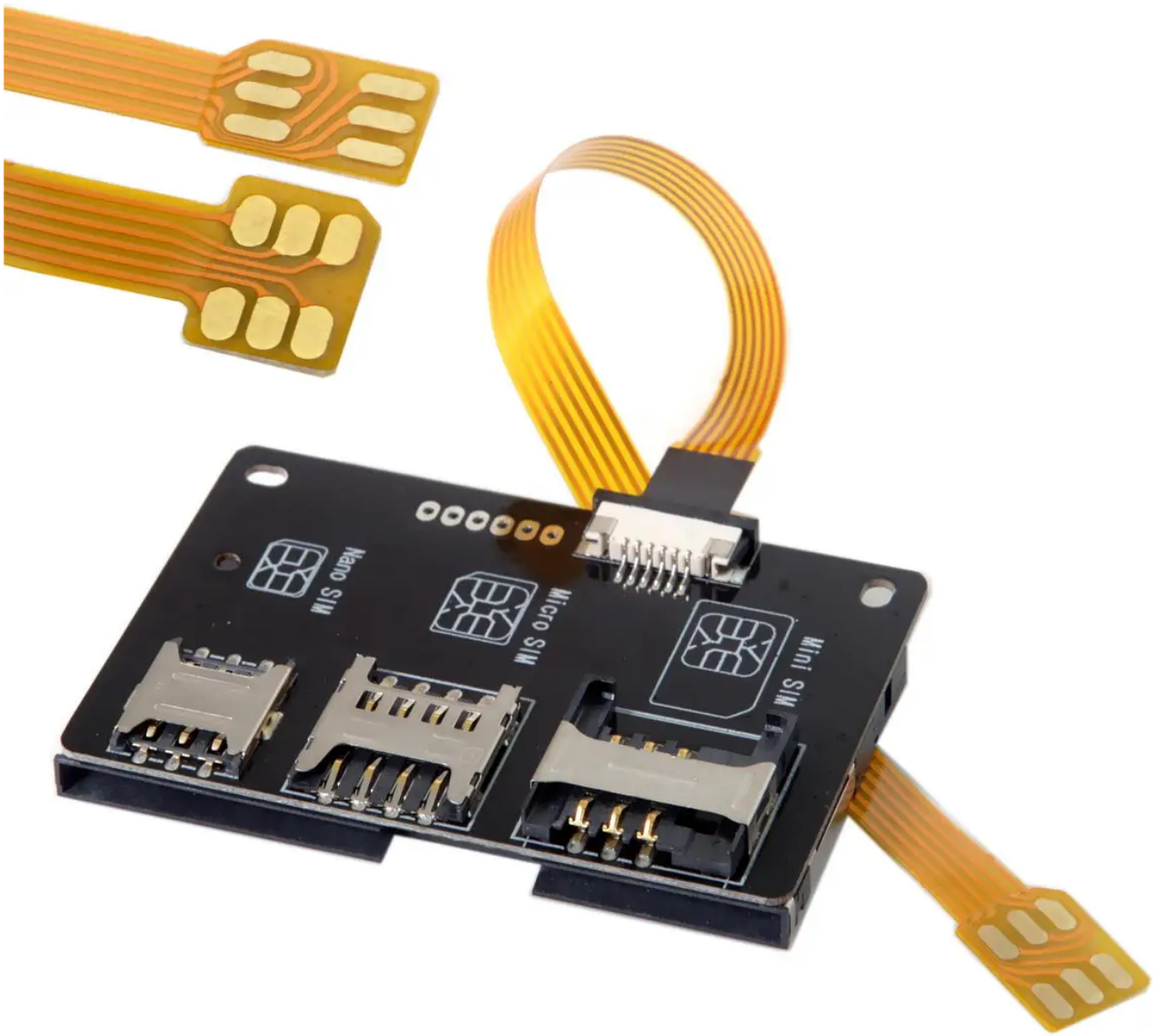
Red teamers can leverage the MSR605/MSR606 for various attacks targeting magnetic stripe cards. For instance, attackers can use the device to clone legitimate cards by reading and writing data onto blank cards. This enables unauthorized access to facilities secured by magnetic stripe access control systems or fraudulent transactions using cloned credit cards. By intercepting data from legitimate cards, attackers can

also collect sensitive information such as card numbers, expiration dates, and cardholder names, facilitating identity theft or financial fraud. The Bluetooth capability further enhances its covert use in situations requiring discreet data capture.

Red Team Attacks List

1. **Credit Card Cloning:** Clone credit cards by reading and writing data onto blank magnetic stripe cards.
2. **Access Control Bypass:** Clone access cards to gain unauthorized physical access to secured buildings or areas.
3. **Card Skimming:** Use the MSR605/606 to skim card data from unsuspecting victims at compromised terminals or ATMs.
4. **Fraudulent Transactions:** Create counterfeit credit cards for conducting fraudulent transactions at retail stores or online.
5. **Identity Theft:** Capture sensitive cardholder information, including names and card numbers, for identity theft purposes.
6. **PIN Interception:** Combine the device with additional hardware to intercept PIN codes entered at compromised terminals.
7. **Social Engineering Aid:** Use cloned cards to aid in social engineering attacks by presenting fraudulent credentials.
8. **Payment Fraud:** Initiate unauthorized payments or transfers using cloned credit card information.
9. **Cardholder Data Theft:** Steal stored cardholder data from POS (Point of Sale) systems or compromised card readers.

SIM Card Extender Kits



SIM card extender kits are versatile tools designed to extend the functionality and accessibility of SIM cards, primarily Nano SIM cards, in mobile devices and tablets. This kit includes FPC (Flexible Printed Circuit) cables and adapters that allow for the conversion and extension of Nano SIM cards to Micro SIM, Standard SIM, or Smart Card formats. The adapters facilitate easy insertion and removal of SIM cards from devices, particularly useful in scenarios where access to the SIM slot is restricted or when upgrading SIM cards in 3G/4G modems enclosed within cases. The extender kits do not support hybrid SIM slots that combine SIM cards with microSD cards simultaneously.

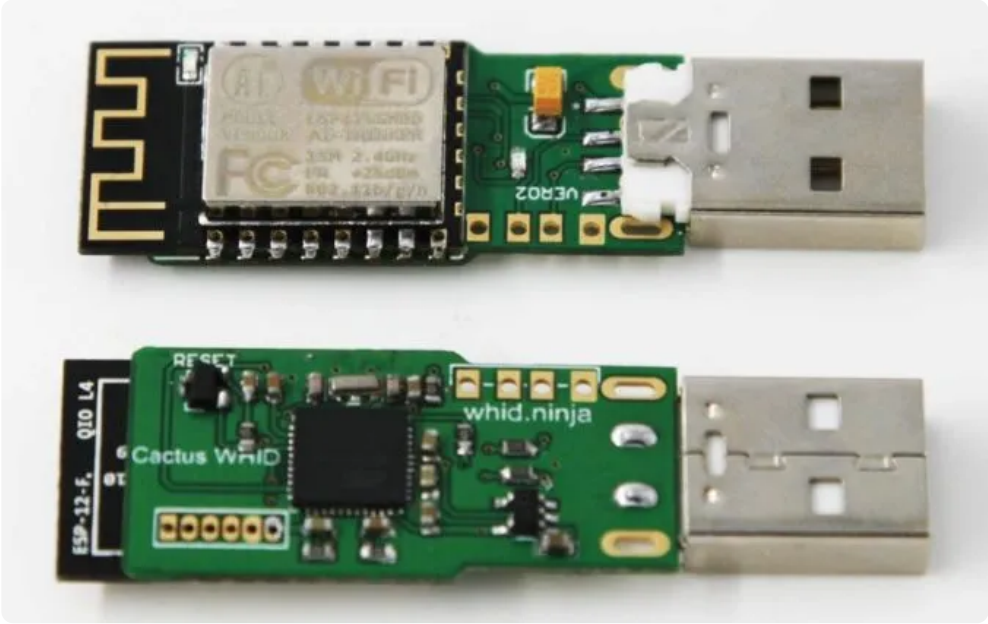
Attack Scenario

Red teamers can exploit SIM card extender kits for various reconnaissance and infiltration purposes in targeted mobile devices. By extending a Nano SIM card outside a device using the provided FPC cables and adapters, attackers can covertly access and manipulate SIM card data. This access can be leveraged to intercept SMS messages, intercept or reroute calls, and gather sensitive information such as IMSI (International Mobile Subscriber Identity) or ICCID (Integrated Circuit Card Identifier) from the SIM card. Furthermore, the extender kits can aid in testing and validating SIM card vulnerabilities, allowing red teamers to assess the security posture of mobile communications.

Red Team Attacks List

1. **SIM Card Cloning:** Use extender kits to clone Nano SIM cards by accessing and copying SIM card data.
2. **SIM Card Skimming:** Intercept communications by manipulating SIM card signals using extended adapters.
3. **SIM Card Tampering:** Modify or inject malicious data onto the SIM card through extended access.
4. **SMS Interception:** Intercept SMS messages intended for the SIM card to gather information or initiate social engineering attacks.
5. **Call Interception:** Manipulate SIM card signals to intercept or reroute calls made to the device.
6. **Identity Theft:** Gather IMSI and ICCID details from the SIM card to facilitate identity theft or fraud.
7. **Network Manipulation:** Exploit vulnerabilities in SIM card authentication to gain unauthorized access to mobile networks.
8. **SIM Card Testing:** Validate security controls by testing the resilience of SIM cards to unauthorized access or manipulation.
9. **Mobile Device Exploitation:** Use extended access to SIM cards for exploiting vulnerabilities in mobile device operating systems or applications.

Cactus WHID Injector



The Cactus WHID Injector is a specialized hardware device designed as a WiFi Human Interface Device (HID) Injector, often referred to as a "USB Rubberducky on steroids." It combines the capabilities of an Atmega 32u4 microcontroller with an ESP-12S module (ESP8266), providing both USB HID emulation and WiFi connectivity. This allows the device to emulate a USB keyboard or a serial port over WiFi, enabling remote execution of keystrokes and commands on a target machine. The WHID Injector is Arduino-friendly and equipped with features like AP (Access Point) and Client modes, TCP/IP stack, DNS support, and 4MB of flash memory for storing scripts and payloads.

Attack Scenario

Red teamers can deploy the Cactus WHID Injector in various scenarios to execute remote attacks on target machines. For example, the device can be programmed to act as a malicious HID keyboard that injects keystrokes into the target computer, executing commands to download and run malware, establish reverse shells, or exfiltrate sensitive data. In WiFi Client mode, it can connect to existing networks and interact with targets across local or remote networks, making it a versatile tool for penetration testing and security assessments.

Red Team Attacks List

1. **Keystroke Injection:** Send keystrokes to the target machine to automate commands or execute predefined scripts.
2. **Payload Delivery:** Download and execute malicious payloads from remote servers via WiFi connectivity.
3. **Reverse Shell Establishment:** Establish a reverse shell on the target machine for persistent remote access.
4. **Credential Theft:** Capture login credentials by injecting scripts that prompt users to enter sensitive information.
5. **Data Exfiltration:** Extract sensitive files or data from the target machine and transmit them over WiFi.
6. **Network Reconnaissance:** Use WiFi connectivity to scan and enumerate devices on local networks for further exploitation.
7. **Exploit Delivery:** Deliver exploit payloads via USB emulation or WiFi connection to target vulnerabilities on the host system.
8. **Social Engineering:** Execute social engineering attacks by tricking users into interacting with the device, such as plugging it into their system.
9. **Command and Control (C2) Establishment:** Use the device to establish a command and control channel for managing compromised systems remotely.
10. **Firmware Modification:** Modify device firmware to enhance capabilities or bypass security controls during operations.

O.MG FIELD KIT

The O.MG FIELD KIT is a comprehensive toolkit designed for penetration testers and security professionals, developed by the security researcher and hardware hacker known as "mg" (whom the device is named after). This kit includes hardware components such as the O.MG Cable, which resembles a regular Lightning or USB-C cable but includes a covert implant that enables remote access and execution of payloads on target devices. The kit also provides a range of accessories and tools that facilitate wireless attacks, data exfiltration, and penetration testing scenarios. It is particularly noted for its stealthy design, making it difficult to detect during security assessments.

Attack Scenario

Penetration testers and red teamers can exploit the O.MG FIELD KIT to conduct covert operations against target devices. The O.MG Cable, when connected to a target computer or mobile device, establishes a wireless connection that allows remote control and execution of commands. Attackers can leverage this capability to perform various malicious activities, including keystroke logging, capturing screenshots, exfiltrating sensitive data, and deploying additional malware or exploits onto the target system. The kit's design emphasizes stealth and usability, making it effective for scenarios where covert access is critical.

Red Team Attacks Lists

1. **Covert Access:** Use the O.MG Cable to gain covert access to target devices without arousing suspicion.
2. **Keystroke Logging:** Capture keystrokes typed on the target device to steal passwords or sensitive information.
3. **Screen Capturing:** Take screenshots of the target device's display to gather sensitive information or monitor user activity.
4. **Data Exfiltration:** Transfer stolen data from the target device to a remote server controlled by the attacker.
5. **Payload Execution:** Execute custom payloads on the target device to achieve specific objectives, such as installing backdoors or accessing privileged information.
6. **Network Reconnaissance:** Use the kit to scan and map the target network for identifying additional vulnerable devices or services.
7. **Credential Harvesting:** Extract credentials stored on the target device, including usernames, passwords, and authentication tokens.
8. **Man-in-the-Middle (MitM) Attacks:** Intercept and modify network traffic between the target device and external servers to steal sensitive data or inject malicious content.
9. **Exploitation of Vulnerabilities:** Exploit known vulnerabilities in the target device's operating system or applications to gain unauthorized access.
10. **Physical Access:** Use the kit's capabilities to extend attacks beyond network boundaries, leveraging physical access to implant the O.MG Cable discreetly.

SCREEN CRAB

The Screen Crab by Hak5 is a discreet video man-in-the-middle implant designed for capturing screenshots from HDMI devices such as computers, monitors, consoles, and televisions. Priced at $199.99, this covert inline device operates by intercepting HDMI signals between source and display devices. It enables sysadmins, penetration testers (pentesters), and security professionals to surreptitiously monitor and record on-screen activity without detection. The captured screenshots can be crucial for security audits, forensic investigations, and monitoring activities in various scenarios.

Attack Scenario

The Screen Crab is deployed between an HDMI source (e.g., a computer or gaming console) and a display device (e.g., a monitor or television). Once connected, it passively intercepts the HDMI signal and captures screenshots discreetly. This operation is transparent to both the source and display devices, ensuring that

the user remains unaware of the interception. Security professionals can use the Screen Crab to gather evidence of unauthorized activities, monitor user behavior, or assess security vulnerabilities in real-time.

Red Team Attacks Lists

1. **Stealth Monitoring:** Capture screenshots from target devices without alerting users or triggering security measures.
2. **Forensic Investigations:** Use captured screenshots as evidence for forensic analysis of security incidents or unauthorized access.
3. **Behavior Monitoring:** Monitor user activities and behaviors on devices under assessment or during penetration testing engagements.
4. **Security Audits:** Assess security posture by capturing screenshots of critical systems, applications, or sensitive data displays.
5. **Compliance Testing:** Validate compliance with security policies by documenting screen content and user interactions.
6. **Incident Response:** Aid in incident response efforts by providing visual evidence of security breaches or suspicious activities.
7. **Remote Surveillance:** Enable remote surveillance of devices and environments by capturing and transmitting screenshots to a central monitoring station.
8. **Device Vulnerability Assessment:** Identify vulnerabilities in HDMI-connected devices by analyzing captured screenshots for sensitive information exposure.

SHARK JACK

The SHARK JACK is a compact pentesting device designed for rapid network assessments and security testing. As a pocket-sized Linux computer, it executes DuckyScript™ payloads using Bash, facilitating quick deployment and execution of various attacks. Out-of-the-box, it features an ultra-fast network scanner for reconnaissance purposes. It also supports syncing with an online library to access a wide range of payloads, including those for remote access and data exfiltration. Equipped with an RGB LED for feedback and USB-C Serial connectivity on the Cable edition, the SHARK JACK combines versatility with ease of use for penetration testers and security professionals.

Attack Scenario

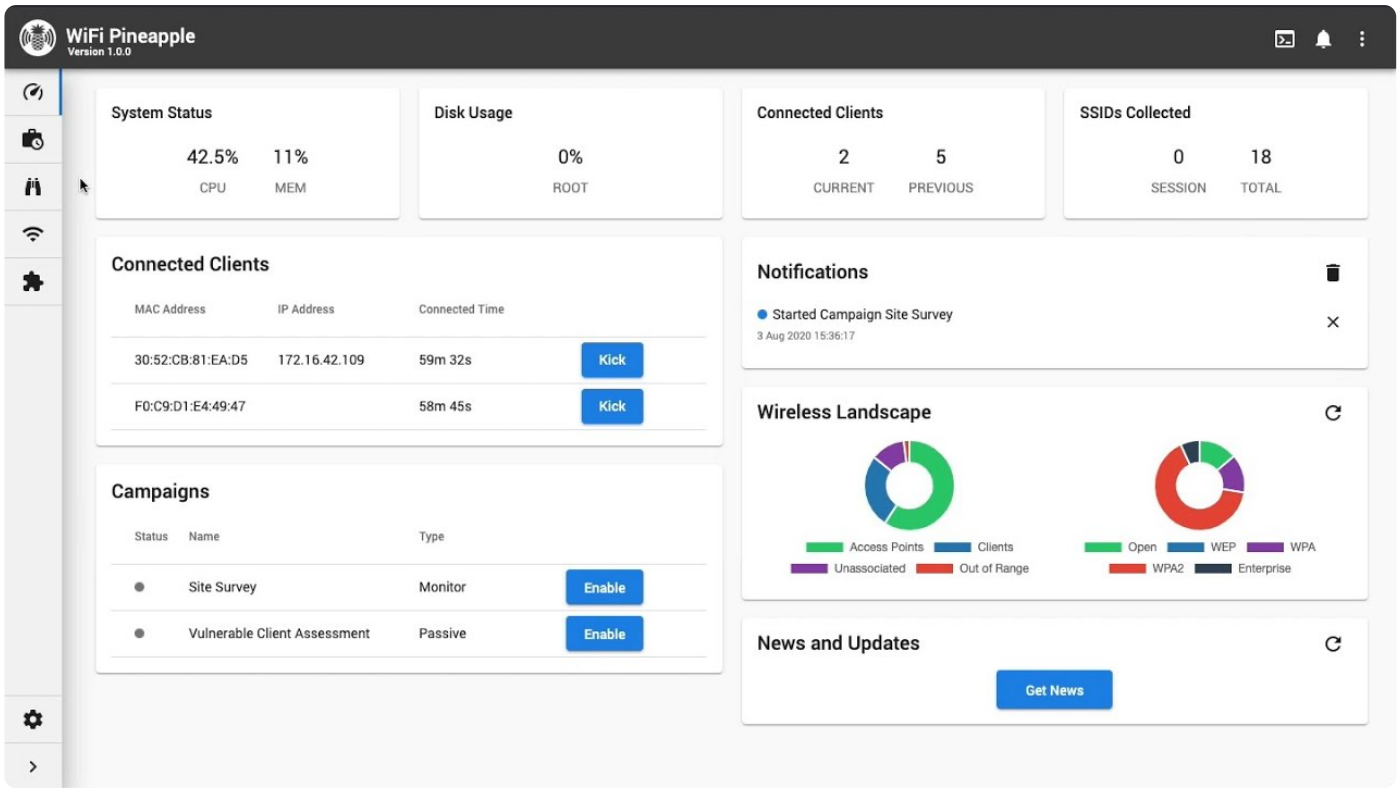
The SHARK JACK can be used in a variety of attack scenarios to assess network security:

1. **Hotplug Attack:** Connect the SHARK JACK to a target network via Ethernet or USB, leveraging its small size and inconspicuous appearance to avoid detection.
2. **Network Reconnaissance:** Activate the network scanner to quickly gather information about connected devices, open ports, and potential vulnerabilities.
3. **Payload Deployment:** Utilize pre-configured DuckyScript™ payloads to execute commands on target machines, such as remote access tools or data exfiltration commands.
4. **Man-in-the-Middle (MITM) Attacks:** Set up the SHARK JACK between a target device and the network to intercept and modify traffic, allowing for packet sniffing or injection of malicious payloads.
5. **Phishing and Social Engineering:** Craft payloads that mimic legitimate actions or websites to trick users into disclosing sensitive information.
6. **Data Exfiltration:** Use the SHARK JACK to transfer stolen data from compromised devices to an external location, bypassing traditional security controls.
7. **Wireless Network Attacks:** Exploit vulnerabilities in Wi-Fi networks using the SHARK JACK's capabilities to capture handshakes, perform deauthentication attacks, or spoof access points.

Red Team Attacks Lists

1. **Network Assessment:** Perform rapid network scans to identify vulnerabilities and weak points.
2. **Credential Harvesting:** Deploy payloads to capture login credentials and authentication tokens from compromised devices.
3. **Command Execution:** Execute commands on target machines to perform actions such as installing backdoors, escalating privileges, or manipulating files.
4. **Covert Operations:** Operate discreetly in environments by leveraging the small form factor and inconspicuous appearance of the SHARK JACK.
5. **Penetration Testing:** Conduct comprehensive security assessments by combining network reconnaissance with targeted attacks.
6. **Incident Response Simulation:** Simulate real-world attacks to test and improve incident response procedures.
7. **Security Awareness Training:** Use the SHARK JACK to demonstrate potential security risks and educate users on best practices.
8. **Physical Access Exploitation:** Exploit physical access opportunities to deploy the SHARK JACK in hidden locations for persistent monitoring or attack execution.

WIFI PINEAPPLE


WiFi Pineapple
Version 1.0.0
System Status
42.5% 11%
CPU MEM
Disk Usage
0%
ROOT
Connected Clients
2 5
CURRENT PREVIOUS
SSIDs Collected
0 18
SESSION TOTAL
Connected Clients
MAC Address IP Address Connected Time
30:52:CB:81:EA:D5 172.16.42.109 59m 32s Kick
F0:C9:D1:E4:49:47 58m 45s Kick
Campaigns
Status Name Type
Site Survey Monitor Enable
Vulnerable Client Assessment Passive Enable
Notifications
Started Campaign Site Survey
3 Aug 2020 15:36:17
Wireless Landscape
Access Points Clients
Unassociated Out of Range
Open WEP WPA
WPA2 Enterprise
News and Updates
Get News

The WiFi Pineapple® Mark VII is a versatile WiFi pentesting platform designed for red teams and security professionals. It combines robust hardware with advanced software capabilities to automate WiFi auditing and conduct sophisticated man-in-the-middle attacks. Equipped with multiple role-based radios and enterprise-grade network processors, the WiFi Pineapple Mark VII excels in capturing WPA handshakes, imitating preferred networks, and collecting actionable intelligence from target environments. Its user-friendly web interface and extensive ecosystem of apps facilitate efficient pentesting campaigns, while its compatibility with Cloud C2 enables remote access and management from anywhere.

Attack Scenario

The WiFi Pineapple Mark VII is employed in various attack scenarios to assess WiFi network security and exploit vulnerabilities:

1. **Rogue Access Point Attacks:** Use the PineAP Suite to create rogue access points that mimic legitimate networks, allowing interception of client communications and credentials.
2. **WPA/WPA Enterprise Attacks:** Capture WPA handshakes and imitate enterprise access points to gather credentials from authenticated devices.
3. **Man-in-the-Middle (MITM) Attacks:** Intercept traffic between devices and the internet, enabling eavesdropping, data manipulation, or injection of malicious payloads.
4. **Automated Pentest Campaigns:** Deploy guided campaign wizards to automate WiFi auditing, gather intelligence on connected devices, and generate custom reports.
5. **Targeted Filtering:** Utilize MAC and SSID filters to stay within the scope of engagement and minimize collateral damage during attacks.
6. **Passive Surveillance:** Monitor and collect data from all devices in the vicinity, enabling ongoing surveillance and forensic analysis.
7. **Advanced Reconnaissance:** Visualize the WiFi landscape, identify vulnerable access points, and map relationships between devices for strategic targeting.
8. **Actionable Intelligence Gathering:** Collect and analyze data to identify security weaknesses, device vulnerabilities, and potential points of exploitation.

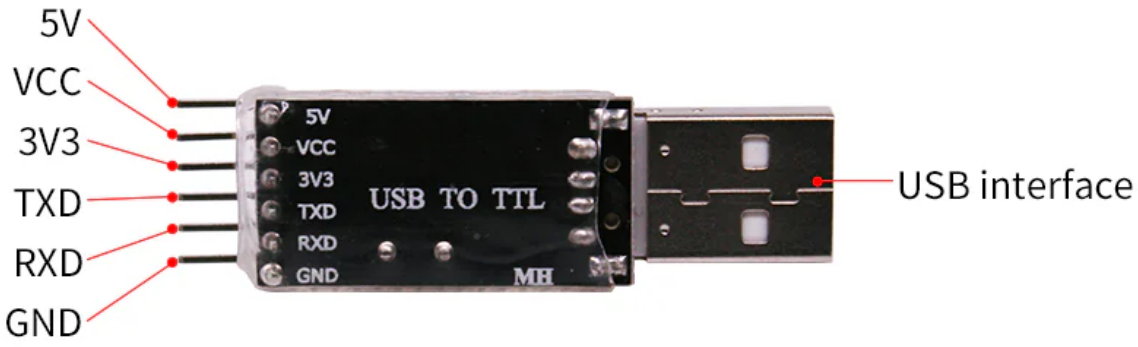
Red Team Attacks Lists

1. **WiFi Network Penetration Testing:** Conduct comprehensive assessments to identify and exploit WiFi vulnerabilities, demonstrating potential security risks.
2. **Credential Harvesting:** Capture login credentials and sensitive information transmitted over insecure WiFi networks.
3. **Data Interception:** Intercept and manipulate traffic to inject malicious payloads or gather sensitive data from connected devices.
4. **Phishing and Social Engineering:** Mimic legitimate networks to trick users into connecting to rogue access points and disclosing credentials.
5. **Wireless Network Mapping:** Map WiFi network topologies, device connections, and access point configurations for strategic attack planning.

6. **Remote Access and Control:** Manage and monitor WiFi Pineapple operations remotely using Cloud C2, enabling persistent surveillance and attack execution.

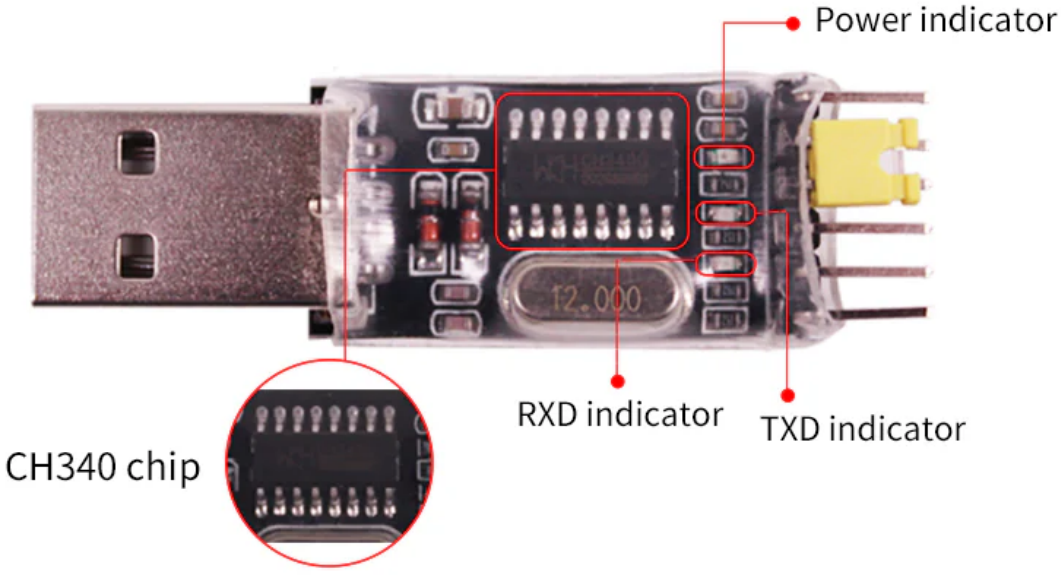
USB to TTL

Interface description



5V or 3V3 power supply can be selected by shorting circuit cap,
The voltage selection of the short-circuit cap on the 6PIN pin
Connect 5V-VCC short circuited to 3V3-TTL output
Connect 3V3-VCC short circuited to 5V-TTL output.

Hardware Distribution



A USB to TTL (Transistor-Transistor Logic) adapter is a compact electronic device used to establish communication between a computer's USB port and devices that use serial communication protocols such as UART (Universal Asynchronous Receiver/Transmitter). These adapters are commonly employed in electronics projects, debugging, and configuring embedded systems where direct serial communication with a computer is required. They typically feature a USB Type-A connector on one end and pins or wires for TTL-level serial communication on the other, allowing for easy interfacing with microcontrollers, development boards, routers, and other hardware.

Attack Scenario

The USB to TTL adapter can be utilized in various attack scenarios where direct access to and manipulation of serial communications is advantageous:

1. **Firmware Hacking:** Gain access to the serial console of devices (e.g., routers, IoT devices) to upload malicious firmware or extract sensitive information.
2. **Debugging Exploitation:** Exploit debugging interfaces exposed via serial communication to modify device behavior or extract debug logs containing sensitive information.
3. **Bootloader Manipulation:** Access and manipulate the bootloader of embedded systems or IoT devices to bypass security mechanisms, install backdoors, or modify firmware.
4. **Device Configuration Alteration:** Change device configuration settings by interacting with the serial interface, potentially disrupting operation or enabling unauthorized access.
5. **Credential Extraction:** Intercept serial communications to capture credentials, configuration data, or encryption keys transmitted in plaintext or during device initialization.

Red Team Attacks Lists

1. **Serial Console Access:** Use the USB to TTL adapter to establish a serial connection to devices with exposed UART ports, gaining access to administrative consoles or debug interfaces.
2. **Malicious Firmware Injection:** Exploit vulnerabilities in firmware update processes by injecting malicious firmware binaries through the serial interface, compromising device integrity.
3. **IoT Device Takeover:** Take control of IoT devices by exploiting insecure serial communication interfaces, enabling unauthorized access or execution of arbitrary commands.
4. **Data Interception:** Intercept and analyze serial communication traffic to capture sensitive information such as passwords, configuration details, or proprietary protocols.
5. **Reverse Engineering:** Facilitate reverse engineering efforts by extracting firmware, examining debug logs, and analyzing communication protocols via the serial interface.
6. **Exploiting Debug Features:** Exploit debug features exposed via the serial interface to identify vulnerabilities, bypass security controls, or escalate privileges on embedded systems.

USBNinja

The USBNinja is a sophisticated USB exploit framework designed for covert operations, enabling wireless remote triggering of custom payloads. Initially appearing as a standard USB cable for data transfer and charging, the USBNinja conceals its true capabilities until remotely activated. It supports multiple connector options including Micro-USB, USB Type-C, and Lightning, making it compatible with a wide range of devices. Once triggered via smartphone or a dedicated long-range antenna, the USBNinja emulates keyboard and mouse actions to execute pre-programmed payloads on the host device. This device is particularly prized for its ability to evade detection by firewalls, antivirus software, and visual inspection, making it invaluable for penetration testers, law enforcement, and government agencies.

Attack Scenario

Red teamers can utilize the USBNinja in various scenarios to execute stealthy attacks on target systems. For instance, by inserting the USBNinja into a target computer, either physically or via a compromised USB port, attackers can remotely trigger payloads that initiate malicious activities. These activities may include executing commands to download and run malware, establish unauthorized network connections, exfiltrate sensitive data, or manipulate files and settings on the compromised system. The ability to emulate keyboard and mouse inputs allows for seamless interaction with the target system, bypassing traditional security measures and enabling sophisticated social engineering attacks.

Red Team Attacks List

1. **Remote Payload Execution:** Trigger payloads remotely to execute malicious commands or scripts on the target system.
2. **Malware Deployment:** Download and run malware on the host machine to establish backdoors or steal data.
3. **Network Manipulation:** Alter network settings or establish unauthorized connections using keyboard and mouse emulation.
4. **Data Exfiltration:** Extract sensitive files or data from the target system and transmit them wirelessly to a remote location.
5. **Password Theft:** Capture login credentials by injecting commands that prompt users to enter sensitive information.
6. **System Manipulation:** Modify system configurations, delete or modify critical files, or disrupt normal operations.
7. **Persistence Establishment:** Install persistent backdoors or trojans to maintain access to the compromised system.
8. **Physical Access Mitigation:** Use the USBNinja in scenarios where physical access to the target system is limited but USB insertion is feasible.
9. **Security Bypass:** Evade detection by security software, firewalls, and visual inspection due to the device's covert nature.

GL.iNet AR150

The GL.iNet AR150 is a compact and versatile router running on the OpenWRT (LEDE) operating system, ideal for low-power consumption environments requiring Linux capabilities. Powered by a Qualcomm System-on-Chip (SoC), it features a Wi-Fi interface that supports monitor mode, enabling functionalities such as wireless scanning, Wi-Fi scanning tools, deauthentication attacks, and man-in-the-middle (MiTM) attacks. The AR150 is particularly noteworthy as it shares hardware similarities with the Hak5 Pineapple Nano but at a significantly lower cost, making it an attractive option for hackers and security professionals alike.

Attack Scenario

Red teamers can leverage the GL.iNet AR150 in various offensive scenarios to exploit vulnerabilities in wireless networks and perform targeted attacks. For instance, the device can be configured to conduct passive reconnaissance by monitoring Wi-Fi traffic and identifying connected devices. It can then launch active attacks such as deauthentication attacks to disrupt network connectivity, conduct man-in-the-middle attacks to intercept and manipulate network communications, or perform rogue access point setups to lure devices into connecting to a malicious network. The AR150's small form factor and low power consumption make it discreet and suitable for covert operations where network manipulation or reconnaissance is required.

Red Team Attacks List

1. **Wi-Fi Monitoring:** Use monitor mode to passively capture and analyze Wi-Fi traffic for reconnaissance purposes.
2. **Deauthentication Attacks:** Send deauthentication frames to disconnect devices from legitimate Wi-Fi networks, forcing them to reconnect to malicious networks.
3. **Man-in-the-Middle (MiTM) Attacks:** Intercept and manipulate network traffic between connected devices and the internet, allowing for eavesdropping or injection of malicious content.
4. **Rogue Access Point:** Set up a rogue Wi-Fi network to trick devices into connecting, enabling further exploitation or data capture.
5. **Packet Sniffing:** Capture and analyze packets transmitted over Wi-Fi networks to extract sensitive information like passwords or credentials.
6. **DNS Spoofing:** Manipulate DNS responses to redirect users to malicious websites or phishing pages.
7. **Traffic Interception:** Intercept unencrypted traffic passing through the network to capture sensitive data in transit.
8. **Network Mapping:** Use scanning tools to identify active devices and map out the network topology for targeted attacks.
9. **Exploitation of IoT Devices:** Exploit vulnerabilities in IoT devices connected to the network to gain access or pivot into more secure areas.
10. **Firmware Modification:** Customize and load alternative firmware like Pineapple firmware to enhance the device's capabilities or support specific attack vectors.

USB Logic Analyzer

The USB Logic Analyzer is an essential tool designed for debugging embedded hardware, particularly in microcontroller development environments. Compatible with Saleae Logic 2.0 software across various operating systems, it offers robust functionality for recording both analog and digital signals directly to a computer. This device supports up to 8 input channels with indicators for electrical levels, making it versatile for analyzing and measuring signals, as well as decoding various protocols. It facilitates the creation of triggers and allows for detailed analysis of protocol logic, enabling users to efficiently debug and optimize hardware designs.

Attack Scenario

Red teamers can utilize the USB Logic Analyzer in targeted attacks aimed at analyzing and exploiting vulnerabilities in embedded systems and IoT devices. For instance, the analyzer can be deployed to intercept and analyze communication protocols between IoT devices and their servers. By capturing and decoding signals, attackers can uncover sensitive data such as authentication tokens or configuration parameters. Additionally, the device can assist in reverse engineering proprietary protocols used in industrial control systems or smart home devices, enabling attackers to develop exploits or gain unauthorized access to critical infrastructure.

Red Team Attacks List

1. **Protocol Reverse Engineering:** Use the logic analyzer to capture and decode proprietary communication protocols used by IoT devices or industrial systems.
2. **Firmware Analysis:** Analyze firmware updates or device communications to identify vulnerabilities or backdoor access points.
3. **Signal Manipulation:** Modify signals to inject malicious commands or bypass authentication mechanisms in embedded systems.
4. **IoT Device Exploitation:** Exploit vulnerabilities in IoT devices by intercepting and manipulating communication signals.
5. **Data Exfiltration:** Capture sensitive data transmitted between embedded devices and external servers, such as user credentials or confidential information.
6. **Debugging and Optimization:** Assist in debugging and optimizing embedded systems by pinpointing logic errors or performance bottlenecks.
7. **Side-channel Attacks:** Perform side-channel attacks by analyzing power consumption or electromagnetic emissions to extract cryptographic keys or sensitive information.
8. **Hardware Trojans:** Detect and analyze hardware Trojans by monitoring signals for unexpected behavior or unauthorized data access.
9. **Bus Sniffing:** Sniff bus communications (e.g., I2C, SPI, UART) to eavesdrop on data exchanges between peripherals and controllers.
10. **Real-time Monitoring:** Monitor real-time data flows within embedded systems to detect and respond to anomalous activities or potential security breaches.

ZigBee Auditor

The ZigBee Auditor is a specialized tool designed for professionals involved in ZigBee network development, auditing, and cybersecurity. Equipped with an on-board antenna and utilizing a USB 2.0 high-speed interface, it operates in the 2.4 GHz frequency range compliant with FCC and CE standards. This device is essential for performing ZigBee network scanning, packet sniffing, and packet replay tasks. It is powered directly by the host computer, making it highly portable and convenient for field use. The ZigBee Auditor integrates seamlessly with EXPLIoT, an open-source framework tailored for IoT security testing and exploitation, allowing for comprehensive security assessments of ZigBee networks.

Attack Scenario

Red teamers can leverage the ZigBee Auditor to conduct targeted attacks on ZigBee-enabled devices and networks. By performing network scans, they can identify active ZigBee devices and assess their vulnerabilities. The packet sniffing capability enables attackers to intercept and analyze ZigBee communication packets, potentially revealing sensitive information such as device IDs, network configurations, or data payloads. Moreover, the packet replay functionality allows attackers to inject manipulated packets back into the network, potentially triggering unintended actions or exploiting protocol weaknesses.

Red Team Attacks List

1. **ZigBee Network Discovery:** Use the ZigBee Auditor to scan for active ZigBee networks and identify vulnerable devices.
2. **Packet Sniffing:** Intercept and analyze ZigBee communication packets to extract sensitive information or identify security weaknesses.
3. **Protocol Analysis:** Reverse engineer ZigBee communication protocols to discover vulnerabilities or develop exploits.
4. **Packet Injection:** Inject malicious packets into ZigBee networks using the packet replay feature to exploit vulnerabilities or disrupt operations.
5. **Device Identification:** Identify specific ZigBee devices within a network and gather information about their functionalities and security posture.
6. **Security Assessment:** Perform comprehensive security assessments of ZigBee networks to identify weak points and recommend mitigations.
7. **IoT Exploitation:** Exploit identified vulnerabilities in ZigBee-enabled IoT devices to gain unauthorized access or manipulate device operations.
8. **Firmware Analysis:** Analyze firmware updates or communication protocols used by ZigBee devices for potential vulnerabilities or backdoor access.
9. **Traffic Analysis:** Analyze network traffic patterns to detect anomalies or unauthorized activities within ZigBee networks.
10. **Denial-of-Service (DoS) Attacks:** Use knowledge gained from ZigBee network analysis to launch targeted DoS attacks against critical devices or services.

Resources

- https://github.com/yadox666/The-Hackers-Hardware-Toolkit
- Hak5

Conclusion

In conclusion, red team gadgets play a crucial role in modern cybersecurity by allowing organizations to proactively test and strengthen their defenses against potential cyber threats. These specialized tools provide red teams with the capability to simulate sophisticated attack scenarios, identify vulnerabilities, and assess the effectiveness of existing security measures. By leveraging gadgets like network sniffers, WiFi Pineapples, USB Rubberducky, and SIM card cloners, red teams can replicate real-world threat tactics, helping organizations to fortify their defenses and mitigate risks before they are exploited by malicious actors.

Furthermore, the insights gained from red team gadget assessments are instrumental in fostering a proactive security culture within organizations. By highlighting vulnerabilities and demonstrating the potential impact of cyber attacks, these assessments empower stakeholders to make informed decisions about resource allocation, cybersecurity investments, and incident response strategies. Ultimately, the use of red team gadgets not only enhances an organization's resilience to cyber threats but also fosters continuous improvement in security practices to safeguard sensitive data and maintain operational integrity in today's digital landscape.

HADESS

cat ~/.hadess

"Hadess" is a cybersecurity company focused on safeguarding digital assets and creating a secure digital ecosystem. Our mission involves punishing hackers and fortifying clients' defenses through innovation and expert cybersecurity services.

Website:

WWW.HADESS.IO

Email

MARKETING@HADESS.IO

To be the vanguard of cybersecurity, hadess envisions a world where digital assets are safeguarded from malicious actors. We strive to create a secure digital ecosystem, where businesses and individuals can thrive with confidence, knowing that their data is protected. Through relentless innovation and unwavering dedication, we aim to establish hadess as a symbol of trust, resilience, and retribution in the fight against cyber threats.