CRPPL: Certified Red Team Physical PenTest Leader – Quick Training

Joas Antonio

https://www.linkedin.com/in/joas-antonio-dos-santos

Redteamleaders.com

English Version

About Training

- These are slides from the quick training on Physical PenTest, based on material from a future certification launched by the Red Team Leaders project in 2023.
- My name is Joas Antonio, I am currently a Red Team Leader and I have extensive experience with numerous PenTest scenarios

https://www.linkedin.com/in/joas-antonio-dos-santos

RED TEAM LEADERS

118 05 25 40

DAYS HRS MIN SEC

Coming Soon...

About You

Name:

Job Title:

Company:

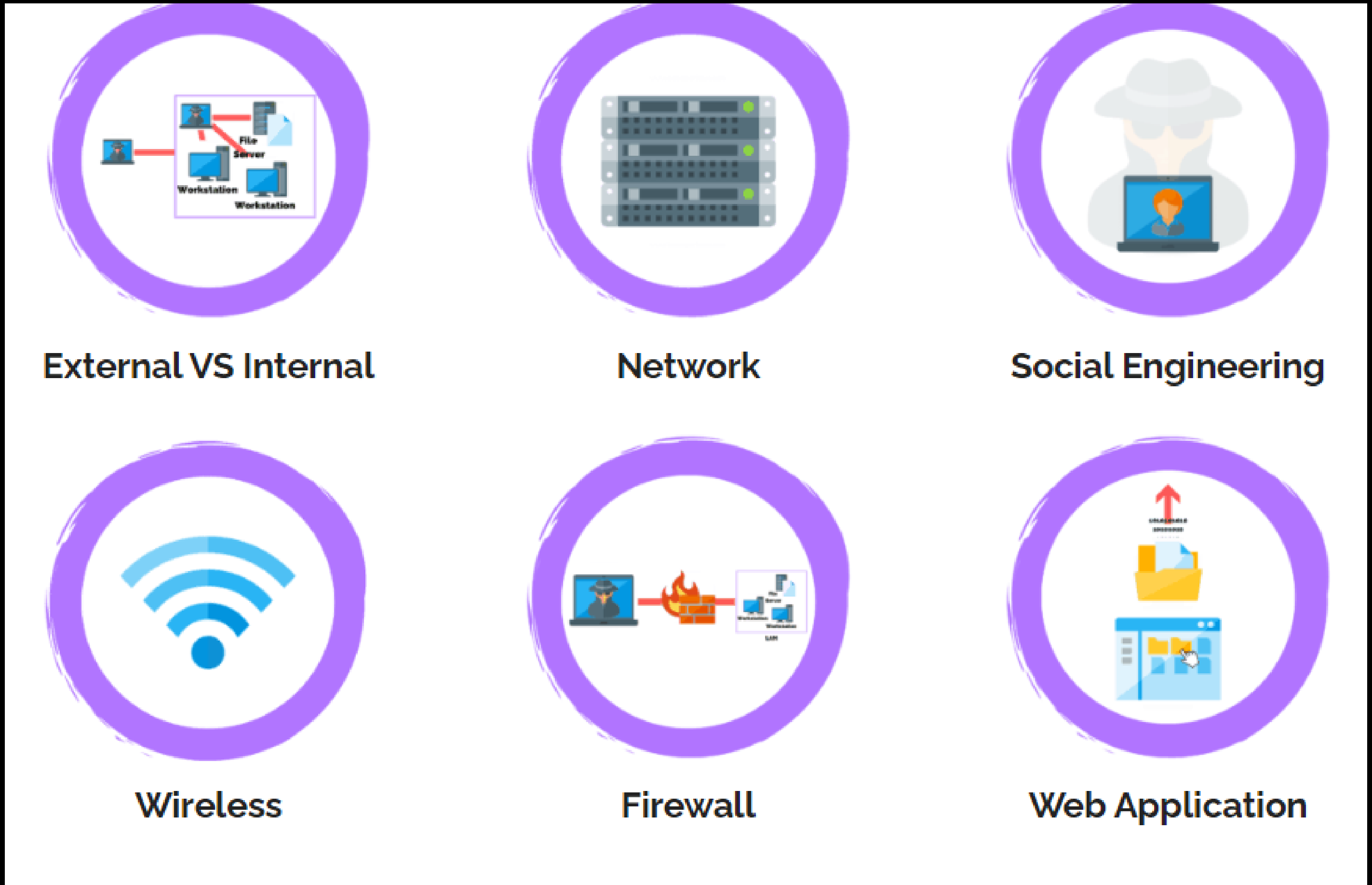
Physical PenTest Introduction

What is Physical PenTest

- A physical penetration test assesses the risk of an attacker physically breaking into your organization. Physical threats that could be simulated include bypassing door locks, stealing devices, or using social engineering to convince an employee to let them inside a server room.

- While many businesses do an excellent job of protecting their network and applications against the threat of a virtual cyber-attack, many organizations don't consider the risk associated with a possible physical attack on their locations.

Types of PenTesting



Benefits of Physical PenTest

- The primary benefit of a physical penetration test is to expose weaknesses and vulnerabilities in physical controls (locks, barriers, cameras, or sensors) so that flaws can be quickly addressed. In addition, physical penetration tests mimic real-world scenarios to demonstrate what impact a malicious actor can have on your systems.
- Physical security penetration testing, when performed properly, will strengthen your security defenses and allow you to focus on the digital side of your security. It makes no sense to throw millions of dollars on security tools if an attacker can get inside your company buildings and slip out unnoticed.

What Questions Does it Answer?

- What is the risk of someone breaking into my organization?
- Before I buy this new physical security control, is it even necessary?
- What information can an attacker gain access to if they break in (PII, Credit Cards, Employee Passwords, etc.)?
- What happens if someone gains access to my data center?
- Can an attacker slip into a conference room and take over my network?
- Will my employees challenge a stranger inside the office?

Rule of Engagement

- The Rules of Engagement, or ROE, are meant to list out the specifics of your penetration testing project to ensure that both the client and the engineers working on a project know exactly what is being testing, when its being tested, and how its being tested.
- Define the tests that will be performed on your target, defining processes and prioritizing the most important areas.

Physical PenTest - Methodology

- **Planning**

1. Gather Scoping Information

- After initiating the project, scoping/target information will be collected from the client. In the case of physical penetration testing, this information will include the addresses of target locations, compromise goals to help us focus our attacks, and information that can help us prevent issues, such as areas of the building that are off-limits and alarm instructions.

2. Review Rules of Engagement

- This process will involve a brief meeting with the client to review and acknowledge the penetration testing rules of engagement, confirm project scope and testing timeline, identify specific testing objectives, document any testing limitations or restrictions, and answer any questions related to the project. Additionally, the client will sign a “Get out of Jail” card that the test team can use to show they are authorized to be testing, should they be caught.

Physical PenTest - Methodology

- **Execution**

1. Reconnaissance

- Once the test has officially begun, a start notification will be sent to the client. The first phase will involve gathering as much information about the target location as possible. This process will start before the engineers are even on-site. They will search open-source intelligence to try to gather information to help them blend-in to the environment. This will include things like the normal attire for employees, if there are employee badges easily accessible, evaluating the various egress routes from Google Maps, trying to identify favorite restaurants of employees where a badge can be read, etc.
- Further reconnaissance will be conducted once the engineers are on-site. During this time, the engineers will identify the various ways to enter the building, conduct traffic pattern analysis, and evaluate the physical security controls present from outside the facility.

2. Threat Modeling

- For this assessment, the threat modeling phase serves to evaluate the different attack vectors that may lead to accessing the building. The types of attacks and likelihood of these threats materializing will serve to inform risk rankings/priorities and outline the attack plan going forward. In a typical physical penetration test, the goal is to identify the level of risk to an organization. As such, Triaxiom will start with the attack vector that has the least amount of risk. Once they gain access, if they remain uncaught, they will exit the building, and then try a different attack vector a few hours later. Each attack will be slightly less sophisticated until the engineer is caught. This allows the organization to quantify the level of risk they have.

Physical PenTest - Methodology

3. Post Exploitation

- After successfully gaining access to a facility, Triaxiom will continue to take actions to evaluate and demonstrate the risk. Some of the areas that will be evaluated after gaining access include:
- Network Access Controls – Can Triaxiom gain access to the network and elevate permissions?
- Clean Desk Policy – Can Triaxiom find information which could be detrimental to the company if found? This includes items such as passwords, written down credit card information, etc.
- Employee Challenges – Triaxiom will walk around the facility and see if employees will challenge a visitor they don't recognize.
- After-Hours Access – Triaxiom will attempt to remain in the facility after all employees leave for the day.
- Sensitive Area Access – Triaxiom will attempt to further their access and gain access to other sensitive areas within the facility, such as a datacenter or server room.

Physical PenTest - Methodology

- **Post-Execution**

1. Reporting

- After completing the active potion of the assessment, Triaxiom will formally document the findings. The output provided will generally include an executive-level report and a technical findings report. The executive-level report is written for management consumption and includes a high-level overview of assessment activities, scope, most critical/thematic issues discovered, overall risk scoring, organizational security strengths, and applicable pictures from the assessment. The technical findings report, on the other hand, will include all vulnerabilities listed individually, with details as to how to recreate the issue, understand the risk, recommended remediation actions, and helpful reference links.

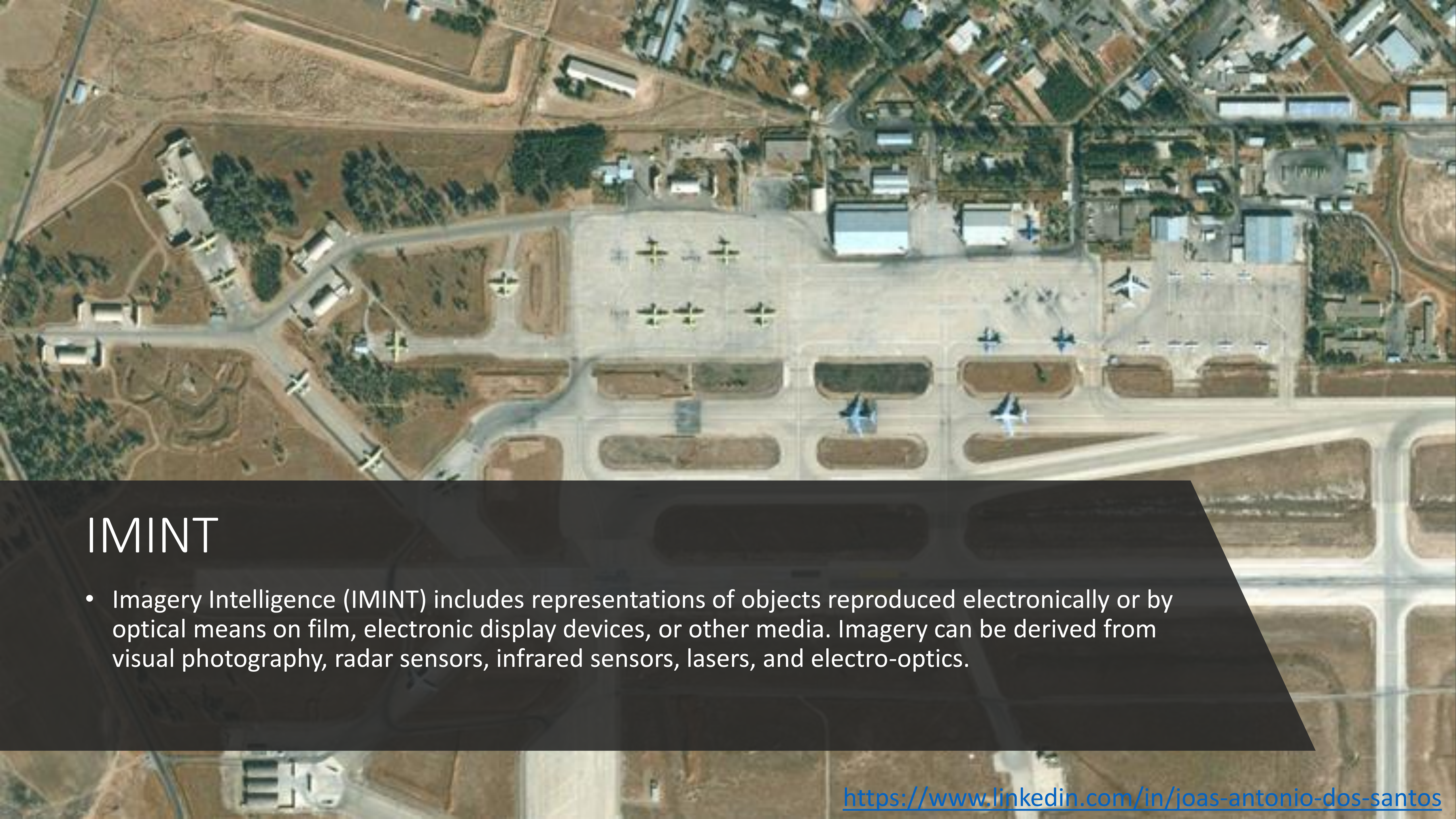
2. Quality Assurance

- All assessments go through a rigorous technical and editorial quality assurance phase. This may also include follow-ups with the client to confirm or deny environment details, as appropriate.

3. Presentation

- The final activity in any assessment and the last step in our physical penetration testing methodology is a presentation of all documentation to the client. Triaxiom will walk the client through the information provided, make any updates needed, and address questions regarding the assessment output. Following this activity, we'll provide new revisions of documentation and schedule any formal retesting, if applicable.

Information Gathering



IMINT

- Imagery Intelligence (IMINT) includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics.

https://www.linkedin.com/in/joas-antonio-dos-santos

GEOINT

- Geospatial Intelligence (GEOINT) is the analysis and visual representation of security related activities on the earth. It is produced through an integration of imagery, imagery intelligence, and geospatial information.

Resources GEOINT

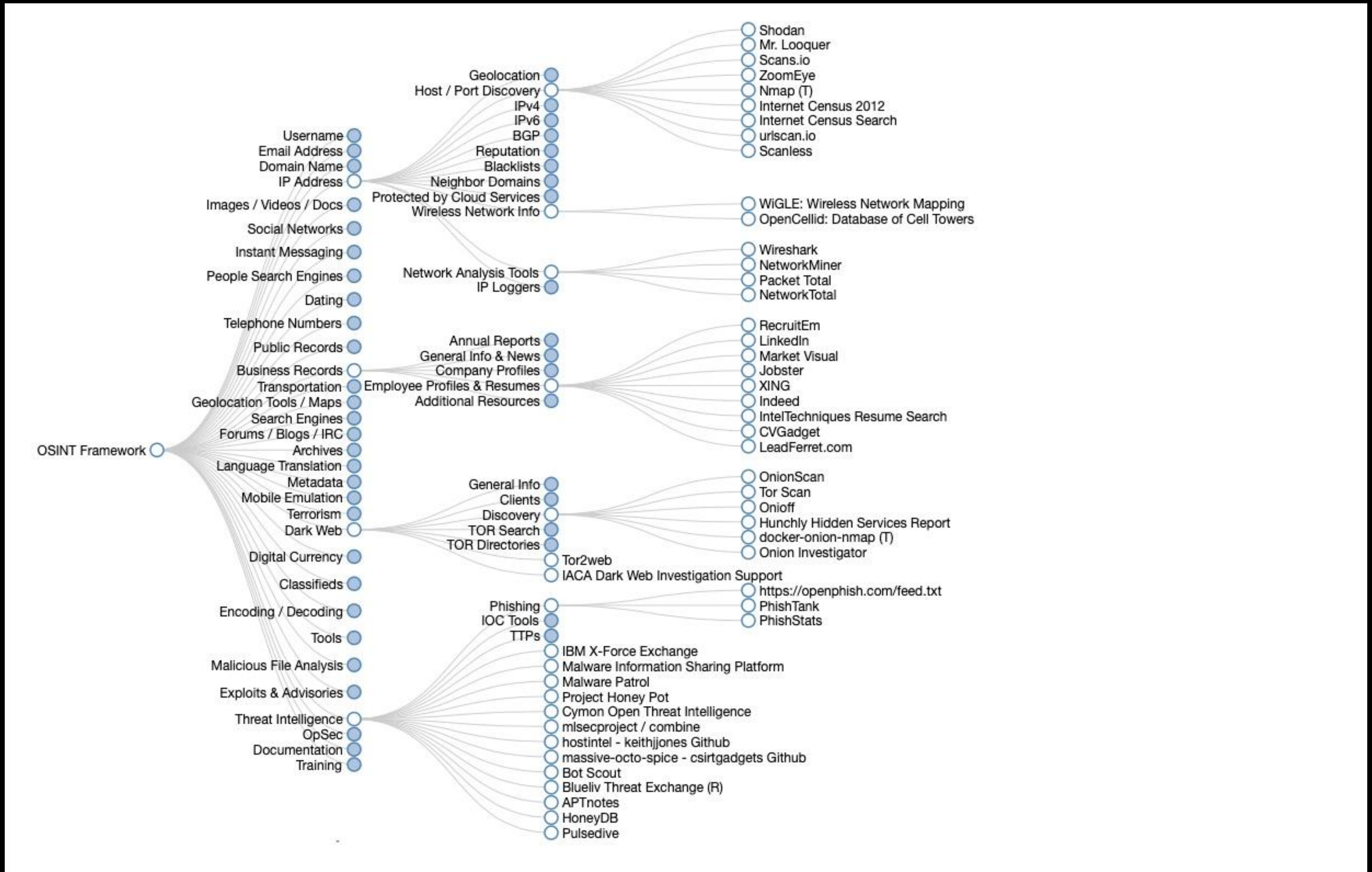
- There are many GEOINT resources used to collect geospatial data and vary widely depending on the project. Satellites, drones, uavs, airplanes, helicopters, and even blimps are used to collect geospatial data from above. GEOINT data collection from aerial platforms is generally used to capture data in large areas while sacrificing maximum resolution. Ground platforms such as cars, trucks, handhelds or backpacks are used to collect more precise data for smaller areas. Sensors attached to these platforms collect RGB (Red Green Blue), IR (Infrared), SAR (Synthetic Aperture Radar), RF (Radio Frequency), LiDAR, and even Acoustic intelligence (ACINT) data.

OSINT

- If you’ve heard the name but are wondering what it means, OSINT stands for open source intelligence, which refers to any information that can legally be gathered from free, public sources about an individual or organization. In practice, that tends to mean information found on the internet, but technically any public information falls into the category of OSINT whether it’s books or reports in a public library, articles in a newspaper or statements in a press release.

- OSINT also includes information that can be found in different types of media, too. Though we typically think of it as being text-based, information in images, videos, webinars, public speeches and conferences all fall under the term.

OSINT Framework



- OSINT Framework
  - Username
  - Email Address
  - Domain Name
  - IP Address
    - Geolocation
    - Host / Port Discovery
      - Shodan
      - Mr. Looquer
      - Scans.io
      - ZoomEye
      - Nmap (T)
      - Internet Census 2012
      - Internet Census Search
      - urlscan.io
      - Scanless
    - IPv4
    - IPv6
    - BGP
    - Reputation
    - Blacklists
    - Neighbor Domains
    - Protected by Cloud Services
    - Wireless Network Info
      - WiGLE: Wireless Network Mapping
      - OpenCellid: Database of Cell Towers
    - Network Analysis Tools
      - Wireshark
      - NetworkMiner
      - Packet Total
      - NetworkTotal
    - IP Loggers
  - Images / Videos / Docs
  - Social Networks
  - Instant Messaging
  - People Search Engines
  - Dating
  - Telephone Numbers
  - Public Records
  - Business Records
    - Annual Reports
    - General Info & News
    - Company Profiles
    - Employee Profiles & Resumes
      - RecruitEm
      - LinkedIn
      - Market Visual
      - Jobster
      - XING
      - Indeed
      - IntelTechniques Resume Search
      - CVGadget
      - LeadFerret.com
    - Additional Resources
  - Transportation
  - Geolocation Tools / Maps
  - Search Engines
  - Forums / Blogs / IRC
  - Archives
  - Language Translation
  - Metadata
  - Mobile Emulation
  - Terrorism
  - Dark Web
    - General Info
    - Clients
    - Discovery
      - OnionScan
      - Tor Scan
      - Onioff
      - Hunchly Hidden Services Report
      - docker-onion-nmap (T)
      - Onion Investigator
    - TOR Search
    - TOR Directories
    - Tor2web
    - IACA Dark Web Investigation Support
  - Digital Currency
  - Classifieds
  - Encoding / Decoding
  - Tools
  - Malicious File Analysis
  - Exploits & Advisories
  - Threat Intelligence
    - Phishing
      - https://openphish.com/feed.txt
      - PhishTank
      - PhishStats
    - IOC Tools
    - TTPs
    - IBM X-Force Exchange
    - Malware Information Sharing Platform
    - Malware Patrol
    - Project Honey Pot
    - Cymon Open Threat Intelligence
    - mlsecproject / combine
    - hostintel - keithjjones Github
    - massive-octo-spice - csirtgadgets Github
    - Bot Scout
    - Blueliv Threat Exchange (R)
    - APTnotes
    - HoneyDB
    - Pulsedive
  - OpSec
  - Documentation
  - Training

Social Engineering

What is Social Engineering?

- Social engineering is an attempt by attackers to trick humans into giving up access, credentials, bank details, or other sensitive information.
- Social engineering occurs in four stages:

1. **Preparation** — attackers collect information about victims through social media, telephone calls, email, text messages, the dark web, or other sources.
2. **Infiltration** — attackers typically approach victims by masquerading as trusted contacts or authorities, and use information gathered about the victim to gain their trust – or even to acquire access to higher-value targets with increased “value” such as system administrators, IT helpdesk members, or executives.
3. **Exploitation** — attackers “persuade” victims to give them sensitive information such as account credentials, payment account details, and other information that they can use to conduct a cyber attack. This persuasion can often be subtle, involving a link, an attachment, a website, even a social media quiz.
4. **Disengagement** — the attacker stops communicating with the victim, carries out malicious activity, and disappears.

Social Engineering: Phishing

- In a phishing attack, an attacker uses a message sent by email, social media, instant messaging clients, or SMS to obtain sensitive information from a victim or trick them into clicking a link to a malicious website.
- Phishing messages get a victim’s attention and call to action by arousing curiosity, asking for help, or invoking other emotional triggers. They often use logos, images, or text styles to spoof an organization’s identity, making it seem that the message originates from a work colleague, the victim’s bank, or another official channel. Most phishing messages use a sense of urgency, causing the victim to believe there will be negative consequences if they don’t surrender sensitive information quickly.

Types of phishing attacks:

- Email phishing — this is the traditional method of phishing, which encourages the email recipient to respond or follow up via other means. The email might include malicious links or attachments.
- Voice phishing (vishing) — a phone call, which may be from an automated messaging system or from a living person. The attacker uses the phone to obtain sensitive information from the victim or convince them to perform certain actions.
- SMS phishing (smishing) — text messages or mobile app messages that might directly request sensitive information from the victim, or contain malicious links.
- Angler phishing — an attempt by an attacker to impersonate the social media account or customer service team of a trusted company. This allows the attacker to intercept communication with brands, turn conversations into private messages, and use them for phishing attacks.
- Search engine phishing — an attempt by attackers to place fake websites at the top of search results. This might be done through paid advertising, legitimate search optimization techniques, or “black hat” techniques.
- In-session phishing — an attempt by an attacker to interfere with normal web browsing during a client session. For example, the attacker may inject a fake login popup or redirect the user to a malicious site.
- Spear phishing or “whaling” — targeted phishing to a particular individual or department based on previous reconnaissance, using any of the above techniques.

Social Engineering: Scareware

Scareware is a malware tactic used to trick victims into downloading or purchasing software and updates that are infected with malware. Most commonly, scareware attacks trick users into thinking they need to buy or install software disguised as a cybersecurity solution.

The purpose of scareware is to threaten computer users to purchase fake software or further infect their device. Scareware shows users pop-up security alerts that appear to be warnings from real antivirus companies, usually claiming that files are infected or the device is in danger. Other variants include warnings of memory limits, clean-up services for unused applications, and other hardware- or software-based updates.

If the tactic works, the victim downloads fake software or visit the site that may steal credentials or other personal information, including password hashes. In some cases, this might be bloatware with no real value, while in others it could be harmful malware. Scareware can lead to compromise of the user's device, infection of other connected devices, and theft of personal data potentially leading to identity theft.

Social Engineering: Watering Hole

A watering hole attack involves launching or downloading malicious code from a legitimate website, which is commonly visited by the targets of the attack. For example, attackers might compromise a financial industry news site, knowing that individuals who work in finance and thus represent an attractive target, are likely to visit this site. The compromised site typically installs a backdoor trojan that allows the attacker to compromise and remotely control the victim's device.

Social Engineering: Pretexting

In a pretexting attack, attackers create a fake identity and use it to manipulate their victims into providing private information. For example, attackers may pretend to be an external IT service provider, and request users’ account details and passwords to assist them with a problem. Or they might pretend to be the victim’s financial institution, asking them for confirmation of their bank account number or bank website credentials.

https://www.linkedin.com/in/joas-antonio-dos-santos

Social Engineering: Baiting

In a baiting attack, attackers provide something that victims believe to be useful. This may be a supposed software update which in fact is a malicious file, an infected USB token with a label indicating it contains valuable information, and other methods.

A quid pro quo attack is similar to baiting, but instead of promising something that will provide value to the victim, the attackers promise to perform an action that will benefit them, but requires an action from the victim in exchange. For example, an attacker may call random extensions at a company, pretending to be calling back on a technical support inquiry. When they identify an individual who actually has a support issue, they pretend to help them, but instruct them to perform actions that will compromise their machine.

Social Engineering: Tailgating

Tailgating is a physical breach social engineering technique in which unauthorized individuals track authorized individuals to gain access to secure facilities.

Tailgating is a simple social engineering-based approach that bypasses seemingly secure security mechanisms. For example, employees might hold the door for an attacker who closely follows them, allowing them to bypass authentication mechanisms.

Potential tailgaters include disgruntled ex-employees, thieves, and saboteurs, who seek to steal from or do harm to a company. Once they gain access to secured areas, they can cause business disruption, cause damage, steal data, and use the information they gathered to carry out additional attacks.

Social Engineering: Dumpster Diving

Dumpster diving (also totting, skipping, skip diving or skip salvage) is salvaging from large commercial, residential, industrial and construction containers for unused items discarded by their owners but deemed useful to the picker. It is not confined to dumpsters and skips specifically and may cover standard household waste containers, curb sides, landfills or small dumps.

Different terms are used to refer to different forms of this activity. For picking materials from the curbside trash collection, expressions such as curb shopping, trash picking or street scavenging are sometimes used. In the UK, if someone is primarily seeking recyclable metal, they are scrapping, and if they are picking the leftover food from farming left in the fields, they are gleaning.

LockPicking

What is Lockpicking

- Lock picking falls within the scope of what is called physical bypassing. A bypass is nothing more than a technical term for going around or through something by means other than normally utilized. However, bypassing typically takes advantage of a flaw or weakness in design.
- For example, we normally use a key to get through a padlock. However, if that particular model of padlock utilizes a spring-loaded bolt to hold the shackle, we may be able to very simply and quickly bypass it by sliding a thin sheet of metal between the bolt and shackle — thus releasing the shackle and unlocking the lock. This method of "shimming" is very commonly practiced among bypassers and can even be accomplished by cutting up a soda can.
- Another example would be taking a more violent approach and melting the padlock to a frothy liquid with a blowtorch.
- Regardless of the method, the goal is the same — to get through the lock without using the key.
- When it comes to physical bypassing, the sky is the limit. Your only restrictions are your imagination and innovation. Any and every lock can be bypassed, it is only a matter of how and when — there is no such thing as the perfect lock.
- However, in the vast multitude of bypasses possible, lock picking is the apple that falls furthest from the tree. Unlike any other known method, lock picking has an extreme elegance about it — being both highly subtle and strikingly artful.
- Buy your Kit: https://labs.ksec.co.uk/product-category/ksec/lockpicking/

Examples

- https://www.art-of-lockpicking.com/what-is-lock-picking/
- https://www.art-of-lockpicking.com/how-to-use-a-bump-key/
- https://www.youtube.com/watch?v=JupQ3BpKGYg
- https://www.youtube.com/watch?v=oZe7uvVmG7c
- https://www.youtube.com/watch?v=XLCO_Ev6e_4
- https://www.youtube.com/watch?v=IQDZCcdw4Z4

RFID Attacks

RFID - Risks

- RFID cards are very simple devices, which makes them reliable for everyday use. However, it also makes them an easy target for attackers looking to gain access to a facility. In this post, we’re focusing on low-power RFID cards, which are commonly used in door access systems. There are a wide variety of attacks that can be performed against RFID access systems. The majority of attacks against RFID systems can be broken into three major categories: man-in-the-middle (MITM), cloning, and brute forcing.

Man in The Middle

- An attack you may have heard about in the networking world is the MITM attack. An MITM attack is when an attacker is able to intercept and copy sensitive information between a victim and the victim's intended recipient of the information. An MITM attack against an RFID system uses a hardware device to capture and decode the RFID signal between the victim's card and a card reader. The malicious device then decodes the information and transmits it to the attacker so they can replay the code and gain access to the building. Many times, this hardware device is battery powered and simply placed on top of the legitimate card reader. When a user passes their RFID card over the reader, the attacker's device copies the signals for later use by an attacker and allows the signals to go to the reader so that a user does not become suspicious by a door suddenly seeming inaccessible.
- Another example of an MITM attack involves placing a small hardware device in line with a card reader and the controller, which is responsible for validating the credentials being read by the card reader. A controller connects to the access control server and stores a copy of valid cards in its internal storage. The controller is generally located near the doors for which it is responsible, such as above a drop ceiling. As seen in Figure 1 – ESPKey, these devices have five wire taps that connect into the wires running between the reader and the controller. The ESPKey is a mass-produced hardware device built to capture the communications across the wire and store it for later use by the attacker. These pieces of hardware are so small that, after the RFID cover is removed, they fit inside the RFID card reader housing, which obscures them from view.

Man in The Middle

- Depending on the type of RFID access control system your company uses, the system may support anti-tamper features such as using additional wires to create an electrical circuit. When the RFID reader is removed or opened, the circuit is broken. This alerts the controller that the system may have been tampered with and to shutdown the reader or take other actions. Look to make sure all the anti-tamper features of your system are in place and working. The anti-tamper controls should be tested on a regular basis along with other physical security controls.

- Another option to assist in detecting tampering is to have security cameras that focus on each door, with the RFID reader in view. Almost all security camera systems now offer motion-sensing reporting. This allows for a large amount of uneventful time to be skipped on the recording, allowing a user to quickly view any possible tampering or suspicious activity.

Clonning

- Another common technique attackers use to defeat RFID access systems is to clone (i.e. copy) a user’s RFID card without their knowledge. An attacker does not always need physical access to the RFID card to clone it. In fact, an attacker can capture the information stored on an RFID card from several feet away using off-the-shelf components and write the data to a blank compatible RFID card. Many times, these cloning devices are built using components from a large RFID reader that is used for parking garages or other areas where a user cannot get close to the card reader to scan their card.
- These low-cost cloning devices can be used by an attacker as they walk past a member of your staff on the street or in a coffee shop. Once an attacker has copied the information from the victim’s RFID card, they can clone it on to a blank RFID card for use at your facility.
- When employees are in the office, it is generally preferred that they wear their RFID card out in the open, as it sometimes displays their identification. Protecting against long-range cloning attack can be difficult, but there are a few options to mitigate this type of attack in the office:
- Separate identification details, such as photo IDs, from RFID cards. This way, an employee can wear their identification around the office and protect their RFID card inside an RFID-blocking sleeve or wallet.
- If the identification details cannot be separated from the RFID card, have employees wear their credentials above their waist, such as clipped to their lapel. This makes it more likely that an employee would notice someone who is trying to clone the employee’s card.
- If an attacker gets close to one of your employees in a public space or while they are at lunch, protecting their RFID card is significantly harder than it would be in the office, as your employees are less likely to be looking for anything out of the ordinary. The best solution for this scenario is for employees to leave their card secured off their person (e.g. in their vehicle), away from the eyes and reach of potential attackers. If an employee does not have the ability to leave their badge in a secure location, an RFID blocking sleeve should be used.

BRUTE FORCING

- Another attack you may have heard of is a brute-force attack. When attacking something like a login portal, a brute-force attack would involve the attacker submitting randomly generated credentials to the login in the hopes of finding a match to gain access to the application. This same type of attack can be used against an RFID system. An attacker can use a hardware device to submit random combinations of RFID identifiers to the access control system in the hopes that one identifier will grant them access. This attack is not often used, as it is very time consuming and generally unsuccessful without a base level of information. RFID cards many times contain a facility code or other specific identifiers that cannot be quickly guessed. If an attacker captures that data from a known-valid card, the final identifier of another employee’s RFID credentials can be brute forced with significantly fewer guesses. This could allow an attacker to leverage information obtained from one employee’s card to brute force a higher level of access.

- By adequately protecting RFID cards and readers using the best practices previously described can keep an attacker from capturing data from a valid card. If an attacker cannot obtain the facility code or other identifiers, brute forcing will be too time consuming to for the attack vector to be viable.

Tools

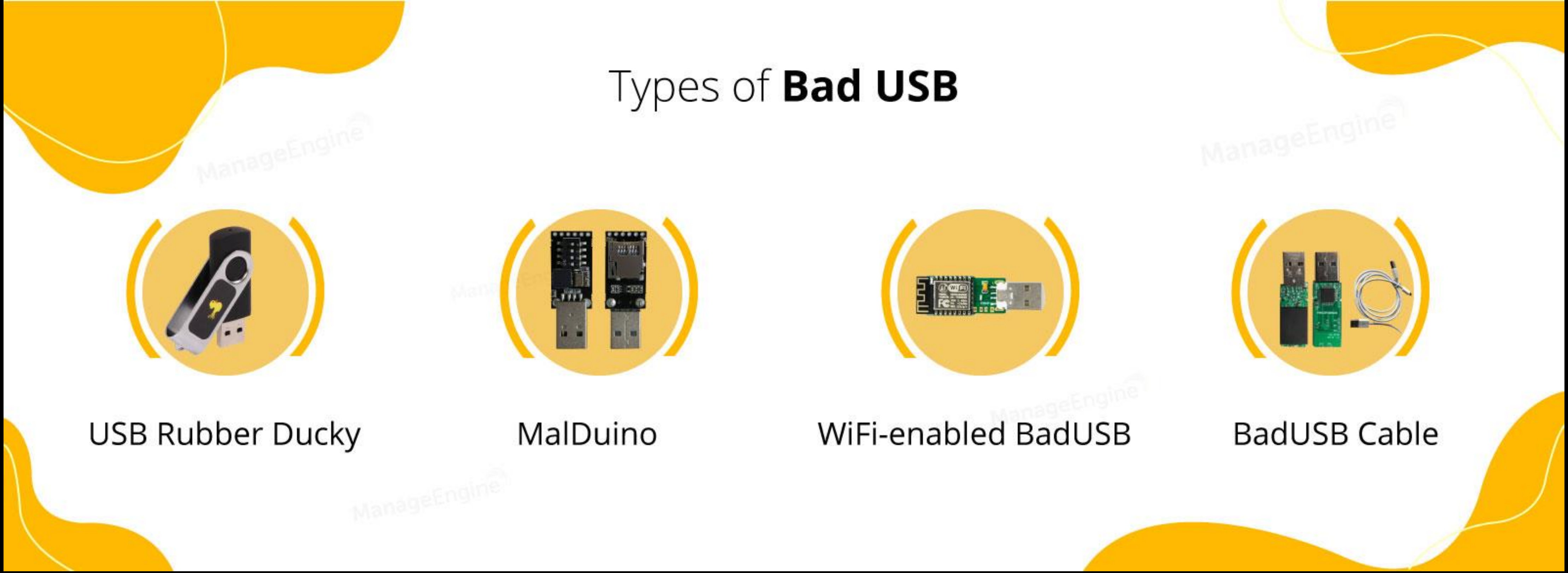
- https://lab401.com/collections/rfid-tools
- https://flipperzero.one/
- https://labs.ksec.co.uk/product-category/redteam-tools/rfid-cloners-emulators/

BadUSB

What Is

- BadUSB is a computer security attack using USB devices that are programmed with malicious software. For example, USB flash drives can contain a programmable Intel 8051 microcontroller, which can be reprogrammed, turning a USB flash drive into a malicious device

Types of BadUSB



Types of **Bad USB**

USB Rubber Ducky

MalDuino

WiFi-enabled BadUSB

BadUSB Cable

https://www.linkedin.com/in/joas-antonio-dos-santos

Digispark and Rubber Ducky

- Digispark is an ATtiny85 based microcontroller development board come with USB interface. Coding is similar to Arduino, and it use the familiar Arduino IDE for developent.
- USB Rubber ducky is an HID device that looks similar to a USB Pen drive. It may be used to inject keystroke into a system, used to hack a system, steal victims essential and credential data can inject payload to the victim’s computers. The main important thing about USB Rubber ducky is that it cannot be detected by any Anti-Virus or Firewall as it acts as an HID device.
- https://hak5.org/ and https://aliexpress.com

Malduino

- MalDuino is an arduino-powered USB device which has keyboard injection capabilities. Once plugged in, MalDuino acts as a keyboard, typing commands at superhuman speeds. What's the point? You could gain a reverse shell, change the desktop wallpaper, anything is possible. For penetration testers, hobbyists and pranksters, MalDuino will serve you well!
- https://malduino.com/

Malicious USB Cable

- The OMG Cable, which looks exactly like a standard Lightning to USB cable, was first demoed back in 2019 by security researcher MG. Since then, MG was able to work with cybersecurity vendor Hak5 to mass-produce the cables for researchers and penetration testers.
- Although users would be hard-pressed to find anything unusual about the cables from the outside, they pack some under-the-hood modifications that make them useful to hackers. An OMG cable plugged into a Mac to connect Apple's Magic Keyboard could, as an example, log passwords or anything else a user types and send that data to a remote attacker.
- https://lab401.com/, https://labs.ksec.co.uk/product-category/redteam-tools/ and https://hak5.org/

USB Ninja

- The USBNinja is a highly covert USB exploit framework allowing for wireless remote triggering of custom payloads.
- While dormant, the USBNinja functions as a regular USB Cable: Data Transfer, Recharging, etc. However, when triggered (via smartphone or dedicated long-range antenna) - it executes its preprogrammed payload on the host device.
- Emulating keyboard and mouse actions, payloads are completely customisable, and can be highly targeted.
- Undetectable by firewalls, AV software or visual inspection, the USBNinja is an ideal tool for penetration testers, police and government.
- https://usbninja.com/help/

Examples

- https://www.youtube.com/watch?v=A2JNBpUotZM
- https://null-byte.wonderhowto.com/how-to/run-usb-rubber-ducky-scripts-super-inexpensive-digispark-board-0198484/
- https://www.youtube.com/watch?v=cl3xlxGRGKU
- https://www.youtube.com/watch?v=-jL_Xz-BKBM
- https://www.youtube.com/watch?v=KQHqZQo2zG4
- https://www.youtube.com/watch?v=v_D7Ktzfq4o
- https://www.youtube.com/watch?v=UWOxzfRUwis
- https://www.youtube.com/watch?v=7x0vl6ikO5M

SDR Attacks

What is

- **Software-defined radio** (**SDR**) is a radio communication system where components that have been traditionally implemented in analog hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system.[1] While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which were once only theoretically possible.
- A basic SDR system may consist of a personal computer equipped with a sound card, or other analog-to-digital converter, preceded by some form of RF front end. Significant amounts of signal processing are handed over to the general-purpose processor, rather than being done in special-purpose hardware (electronic circuits). Such a design produces a radio which can receive and transmit widely different radio protocols (sometimes referred to as waveforms) based solely on the software used.
- Software radios have significant utility for the military and cell phone services, both of which must serve a wide variety of changing radio protocols in real time. In the long term, software-defined radios are expected by proponents like the Wireless Innovation Forum to become the dominant technology in radio communications. SDRs, along with software defined antennas are the enablers of the cognitive radio

Radio Frequency Attack

- With the advent of inexpensive radio devices such as the RTL-SDR, HackRF, LimeSDR and bladeRF, the possibility of hacking radio frequency (RF) communication and control devices has been blown wide open to anyone in the cybersecurity/infosec field. Although not commonly included in penetration tests, radio hacks should be considered as they are presently one of the most overlooked entry points to the network and systems.

Radio Frequency Attack - Methods

- Unlike traditional web based attacks, attackers try to intervene in the radio channel and then connect to the channel and exert control. Once that control is established, it can then be used to penetrate deeper within the network or system. For instance, SCADA/ICS systems often used radio communications to their remote terminal units (RTU) and other stations as physical wiring is impractical over hundreds of acres or miles (km). The attacker may first intercept and control the communication between remote terminals and then work back to the server or PLC's. In more traditional security systems, the attacker can use the interception of cellphone traffic to eavesdrop on conversations and break text-based 2FA. Intercepting pager traffic with unencrypted emails can be used for phishing and other targeted attacks.

Radio Frequency Attack - Methods

- 1. Sniffing
- The simplest attack methodology and then one most often used before the following attacks is sniffing the traffic. This includes uses an SDR device that is capable of operating at the same frequency. In this way, the attacker can study and learn the principles of the radio system and identify key instruction sin the data stream. Of course, if the data is unencrypted the attacker can also eavesdrop on the traffic.
- 2. Replay
- Many radio communications do not have a replay-proof mechanism (e.g. timestamps or randomization). In such cases, the attacker can capture and copy the transmission and then replay it to the target system. This may work on such systems as car doors, garage doors, household switches and others.

Radio Frequency Attack - Methods

- 3. Signal deception
- In some cases, the attacker can learn the critical packet structure, keys and verification method to control the target. this may include spoofing where the attacker send a fake but valid signal to the target.
- 4. Signal Hijacking and Denial of Service
- The attacker may block the target's network using a signal interference device or pulls the target on to a fake network. In this way, they can carry out attacks by hijacking upstream and downstream traffic. This might include blocking a 4G cellular network to force the target onto a 2G network where the traffic can be intercepted and eavesdropped. Hijacking can also include such devices as a femto-cell or Stingray.
- https://lab401.com/collections/sdr
- https://store.sharebrained.com/products/portapack-for-hackrf-one-kit

Examples

- https://www.youtube.com/watch?v=OVNxjCRlBgU
- https://www.youtube.com/watch?v=M2JY1_Xmokg
- https://www.youtube.com/watch?v=RnAgqGR-D-8
- https://www.youtube.com/watch?v=k8rNQ3mBZQ4&t=5s
- https://www.youtube.com/watch?v=BpRfJ15AFd0

Tailgating - Examples

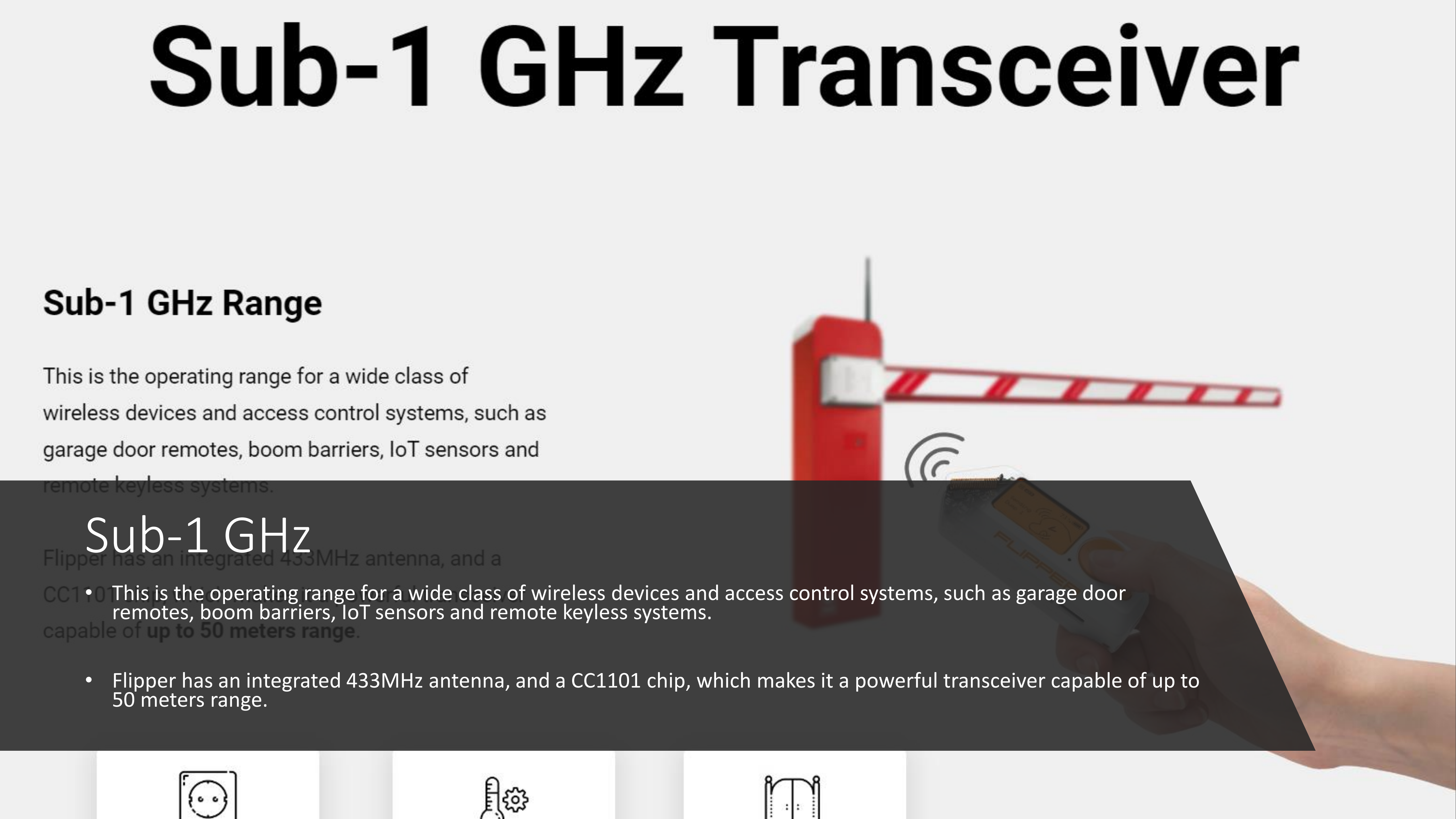
Techniques

- One of the most common tailgating methods is someone simply following someone else through a door -- usually because an employee holds open a door for the person behind them. A more sophisticated type of tailgating attack occurs when a threat actor disguises themselves as someone else - typically an authorized person with access to a particular area - to trick people to gain access to that area.
- Another instance of tailgating is when an authorized party enters an area and lets the door slowly close behind them. This leaves a small window of time when an unauthorized party can enter the premises.
- Tailgating can also happen when a third party keeps a door propped open for some reason. For instance, a painter may be working in the office lobby, so they leave the door open to get rid of paint fumes. Or an IT vendor may be troubleshooting a server or router in the server room while leaving the door to the room open. In another scenario, someone can pretend to be a delivery person and enter a building by asking an employee to "hold the door" as they bring in a package, purportedly for someone in the building or office.
- https://www.youtube.com/watch?v=nQfMKPyPWBM
- https://www.youtube.com/watch?v=1fmLds7EZXs
- https://www.youtube.com/watch?v=4eJOR4riAz0
- https://www.youtube.com/watch?v=IpWc0Rv1y8E

Flipper Zero

What Is

- Flipper Zero is a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control systems, hardware and more. It's fully open-source and customizable, so you can extend it in whatever way you like.



Sub-1 GHz Transceiver

Sub-1 GHz Range

This is the operating range for a wide class of wireless devices and access control systems, such as garage door remotes, boom barriers, IoT sensors and remote keyless systems.

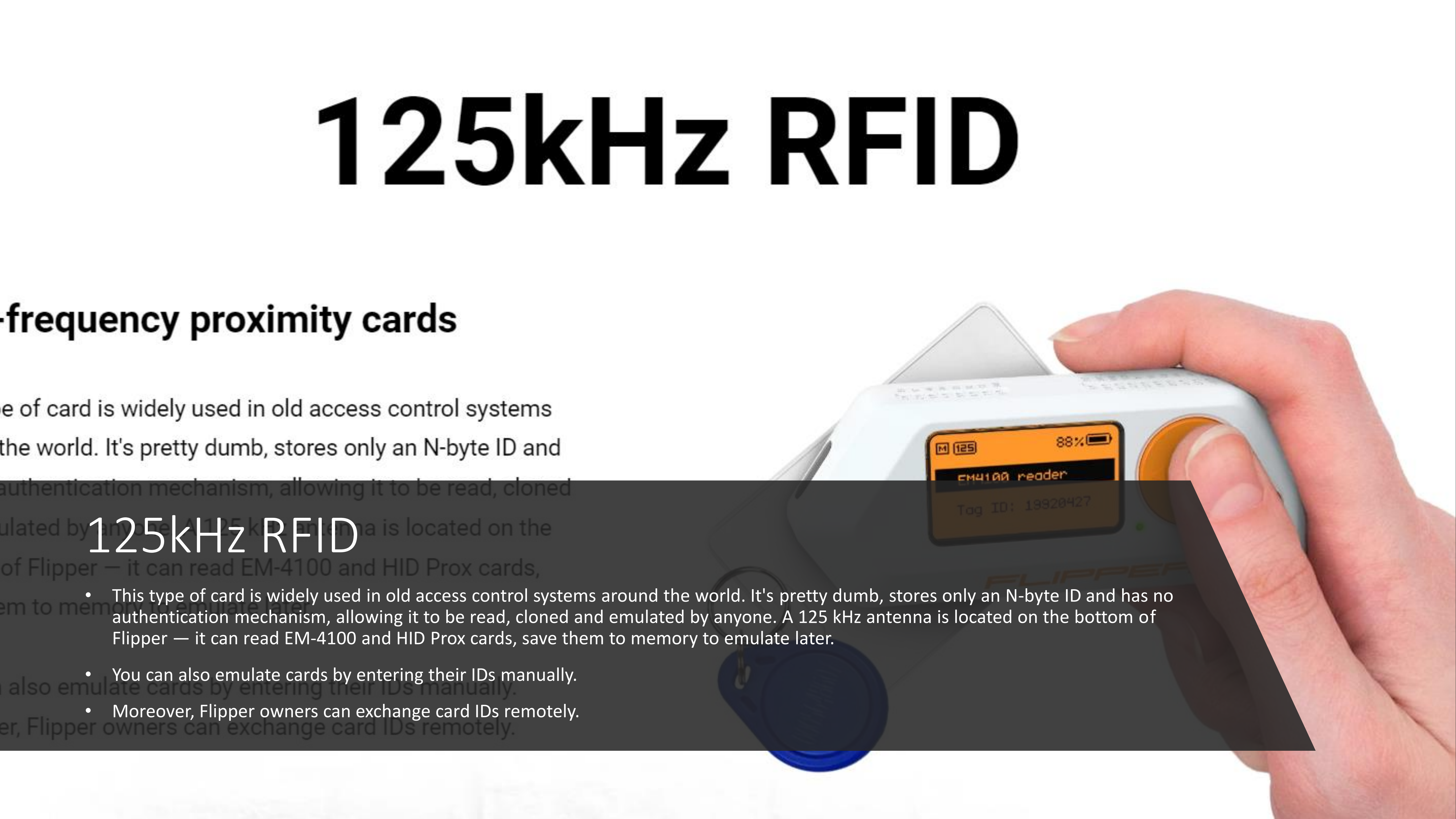
Flipper has an integrated 433MHz antenna, and a

CC1101

capable of **up to 50 meters range**.

Sub-1 GHz

- This is the operating range for a wide class of wireless devices and access control systems, such as garage door remotes, boom barriers, IoT sensors and remote keyless systems.
- Flipper has an integrated 433MHz antenna, and a CC1101 chip, which makes it a powerful transceiver capable of up to 50 meters range.



125kHz RFID

-frequency proximity cards

e of card is widely used in old access control systems the world. It's pretty dumb, stores only an N-byte ID and authentication mechanism, allowing it to be read, cloned ulated by anyone. A 125 kHz antenna is located on the of Flipper — it can read EM-4100 and HID Prox cards, em to memory to emulate later.

also emulate cards by entering their IDs manually.

er, Flipper owners can exchange card IDs remotely.

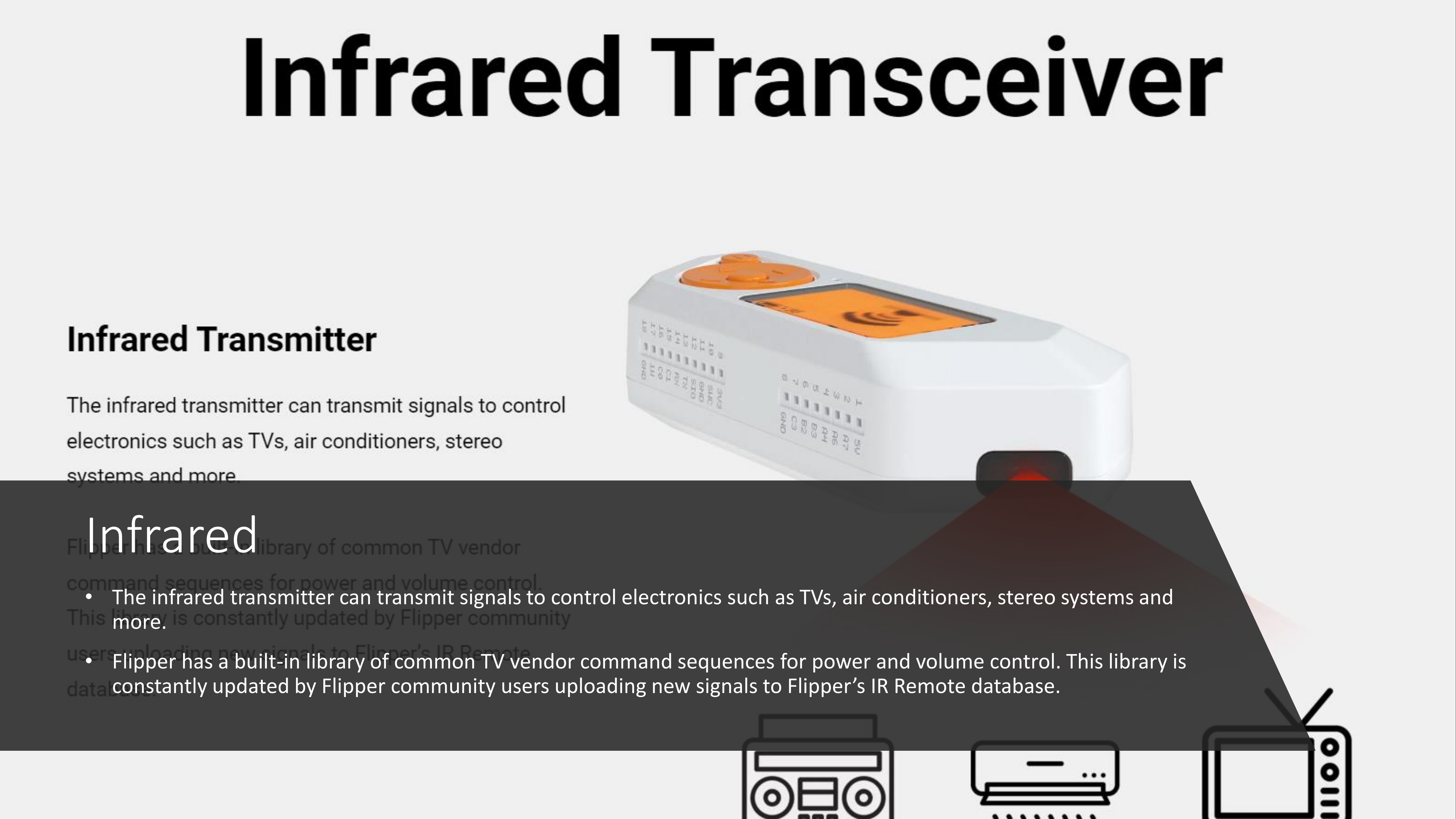
125kHz RFID

- This type of card is widely used in old access control systems around the world. It's pretty dumb, stores only an N-byte ID and has no authentication mechanism, allowing it to be read, cloned and emulated by anyone. A 125 kHz antenna is located on the bottom of Flipper — it can read EM-4100 and HID Prox cards, save them to memory to emulate later.
- You can also emulate cards by entering their IDs manually.
- Moreover, Flipper owners can exchange card IDs remotely.

NFC

NFC

- Flipper Zero has a built-in NFC module (13.56 MHz). Along with the 125kHz module, it turns Flipper into an ultimate RFID device operating in both Low Frequency (LF) and High Frequency (HF) ranges. The NFC module supports all the major standards.
- It works pretty much the same as the 125 kHz module, allowing you to interact with NFC-enabled devices — read, write and emulate HF tags.



Infrared Transceiver

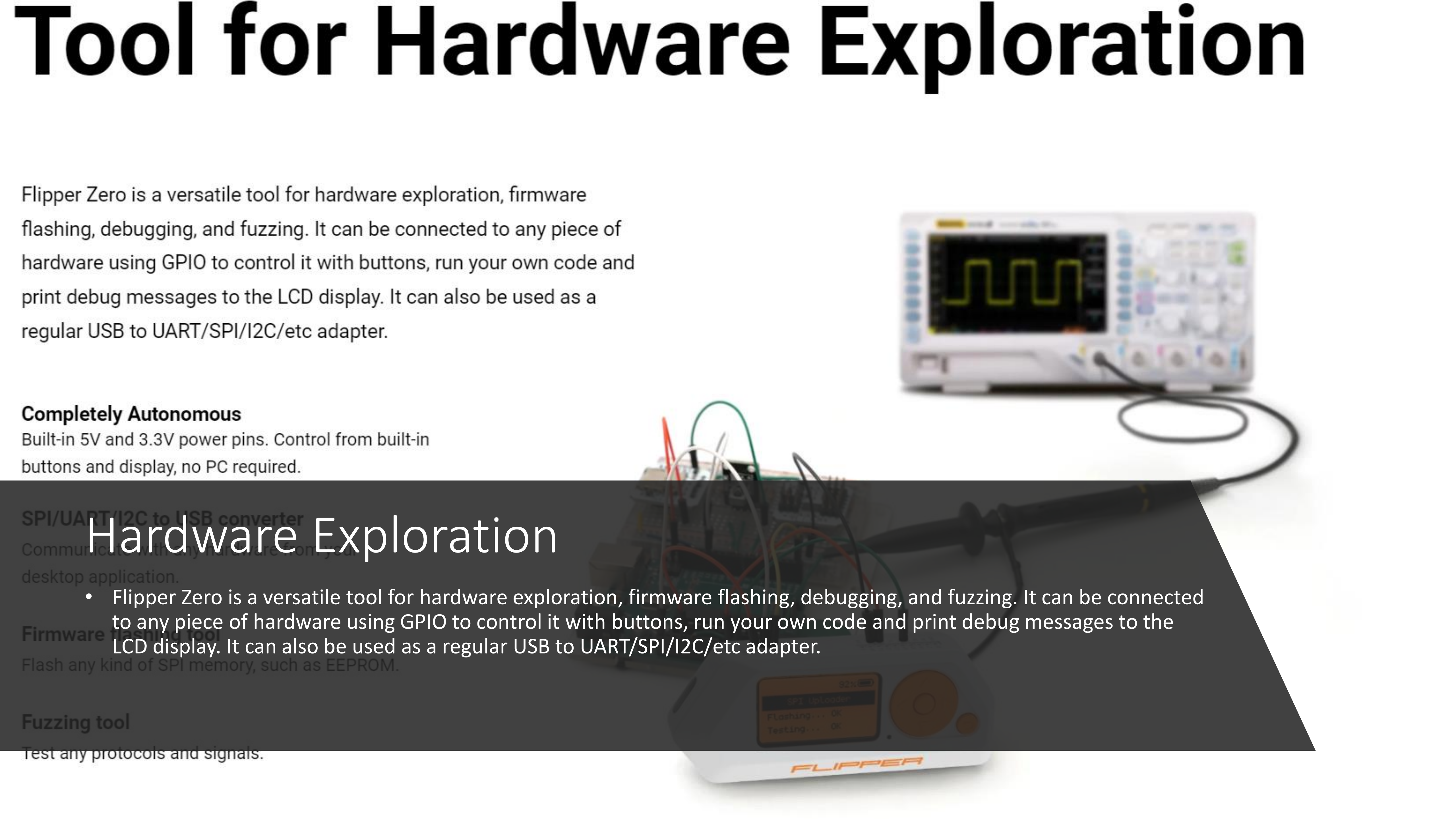
Infrared Transmitter

The infrared transmitter can transmit signals to control electronics such as TVs, air conditioners, stereo systems and more.

Flipper has a built-in library of common TV vendor command sequences for power and volume control. This library is constantly updated by Flipper community users uploading new signals to Flipper's IR Remote database.

Infrared

- The infrared transmitter can transmit signals to control electronics such as TVs, air conditioners, stereo systems and more.
- Flipper has a built-in library of common TV vendor command sequences for power and volume control. This library is constantly updated by Flipper community users uploading new signals to Flipper’s IR Remote database.



Tool for Hardware Exploration

Flipper Zero is a versatile tool for hardware exploration, firmware flashing, debugging, and fuzzing. It can be connected to any piece of hardware using GPIO to control it with buttons, run your own code and print debug messages to the LCD display. It can also be used as a regular USB to UART/SPI/I2C/etc adapter.

Completely Autonomous
Built-in 5V and 3.3V power pins. Control from built-in buttons and display, no PC required.

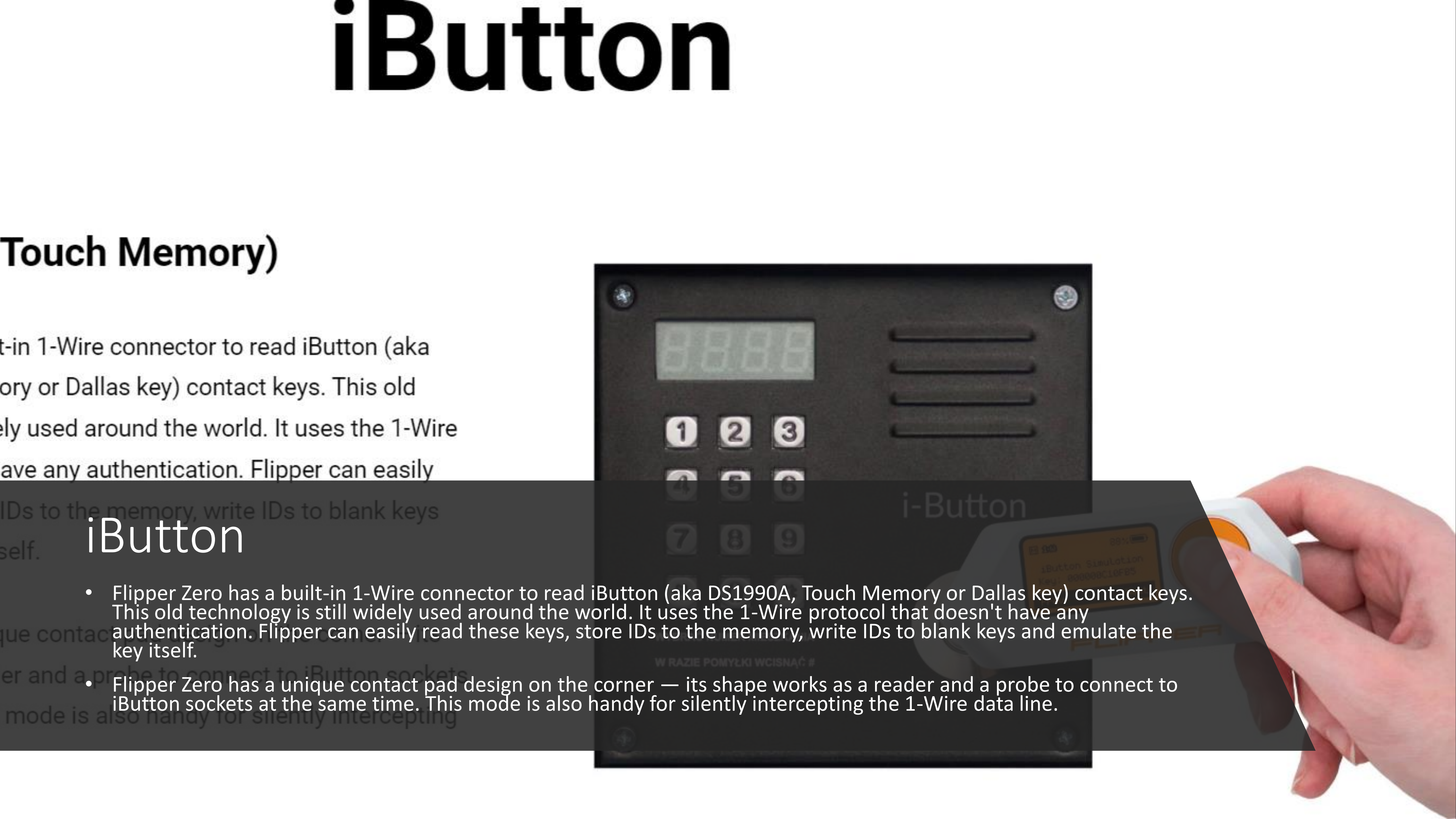
SPI/UART/I2C to USB converter
Communicate with any hardware from your desktop application.

Firmware flashing tool
Flash any kind of SPI memory, such as EEPROM.

Fuzzing tool
Test any protocols and signals.

Hardware Exploration

- Flipper Zero is a versatile tool for hardware exploration, firmware flashing, debugging, and fuzzing. It can be connected to any piece of hardware using GPIO to control it with buttons, run your own code and print debug messages to the LCD display. It can also be used as a regular USB to UART/SPI/I2C/etc adapter.



iButton

Touch Memory)

t-in 1-Wire connector to read iButton (aka
ory or Dallas key) contact keys. This old
ely used around the world. It uses the 1-Wire
ave any authentication. Flipper can easily
IDs to the memory, write IDs to blank keys
self.

que contac
er and a probe to connect to iButton sockets
mode is also handy for silently intercepting

iButton

- Flipper Zero has a built-in 1-Wire connector to read iButton (aka DS1990A, Touch Memory or Dallas key) contact keys. This old technology is still widely used around the world. It uses the 1-Wire protocol that doesn't have any authentication. Flipper can easily read these keys, store IDs to the memory, write IDs to blank keys and emulate the key itself.
- Flipper Zero has a unique contact pad design on the corner — its shape works as a reader and a probe to connect to iButton sockets at the same time. This mode is also handy for silently intercepting the 1-Wire data line.

Examples

- https://www.youtube.com/watch?v=oAq6kAFyhsI
- https://www.youtube.com/watch?v=mXjL70QKxi4
- https://www.youtube.com/watch?v=4hDG_Y39dKM
- https://www.youtube.com/watch?v=u1GDUapHdUw
- https://www.youtube.com/watch?v=S2h9hvDiA-Q
- https://www.youtube.com/watch?v=duA3eZ2fKf4
- https://www.youtube.com/watch?v=GnziFeDQ7h4

Wi-fi Attacks

Types Attack

- Evil Twin attack:
- Here the attacker sets up a fake access point with a similar name to that of a corporate AP near the company premises. When an employee unknowingly connects to this access point thinking that to be the genuine AP of the company, he/she gives away the authentication details of the original access point. The attacker, thus, is able to compromise the connection.

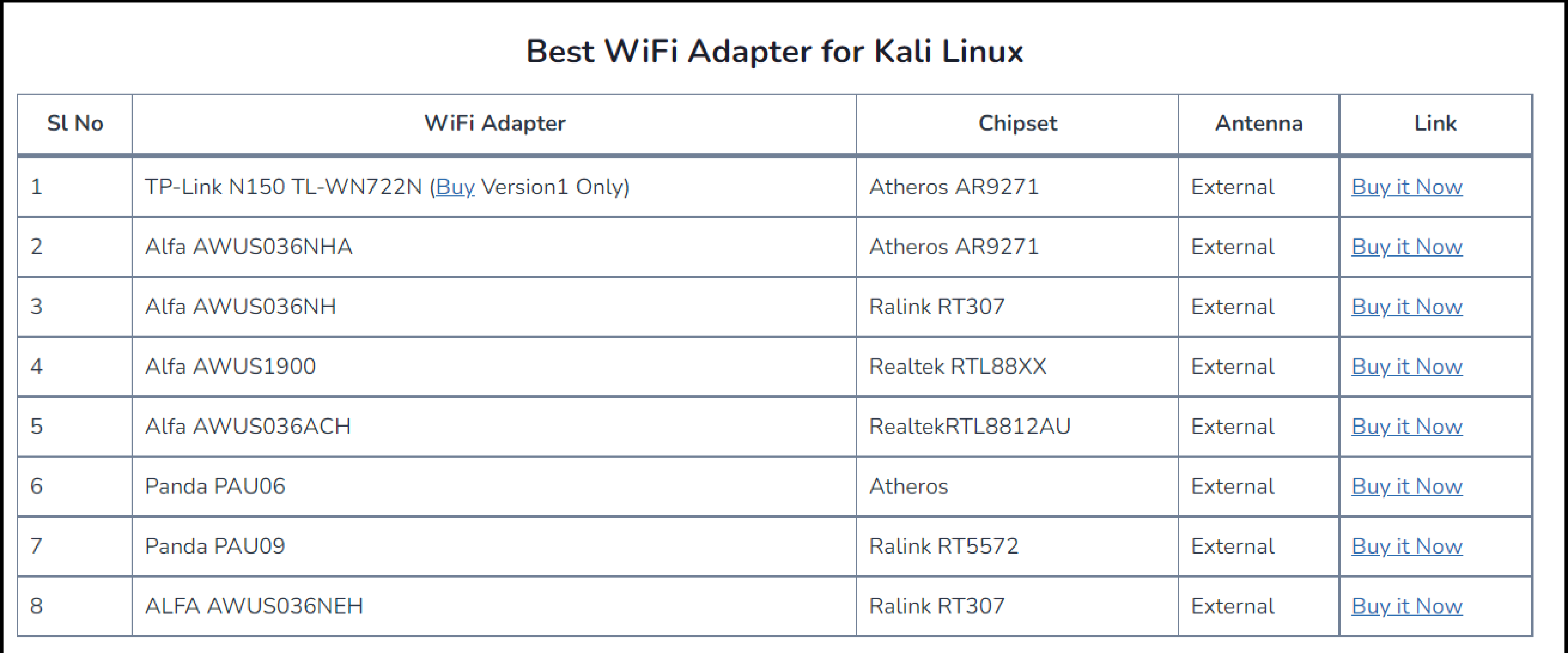
Types Attack #2

- Jamming Signals:
- An attacker can disrupt the network connection by jamming the signal, there are functioning tools for this purpose also called as creating noise.
- Misconfiguration Attacks:
- If a router is set up using the default configuration, weak credentials, weak encryption algorithms, then the attacker can easily break into the network.
- Honey spot Attack:
- An attacker can set up fake access points/hotspots with the same SSID as that of a public wi-fi AP; thus, he can set traps for the users who connect to these AP's.
- Unauthorised/Ad-Hoc connection attacks:
- An attacker can enable an AD-HOC connection in a user's system utilizing Trojan, malware, or if an employee is already using an AD-HOC connection to share the internet with peers. The attacker can compromise the connection operating in AD-HOC mode since this mode does not provide stronger encryption to the connection.

Types Attack #3

- Brute Force: WPA/WPA2 supports many types of authentication beyond pre-shared keys. aircrack-ng can ONLY crack pre-shared keys. So make sure airodump-ng shows the network as having the authentication type of PSK, otherwise, don't bother trying to crack it.
- There is another important difference between cracking WPA/WPA2 and WEP. This is the approach used to crack the WPA/WPA2 pre-shared key. Unlike WEP, where statistical methods can be used to speed up the cracking process, only plain brute force techniques can be used against WPA/WPA2. That is, because the key is not static, so collecting IVs like when cracking WEP encryption, does not speed up the attack. The only thing that does give the information to start an attack is the handshake between client and AP. Handshaking is done when the client connects to the network. Although not absolutely true, for the purposes of this tutorial, consider it true. Since the pre-shared key can be from 8 to 63 characters in length, it effectively becomes impossible to crack the pre-shared key.

Wifi Adapters



Best WiFi Adapter for Kali Linux

Sl No	WiFi Adapter	Chipset	Antenna	Link
1	TP-Link N150 TL-WN722N (Buy Version1 Only)	Atheros AR9271	External	Buy it Now
2	Alfa AWUS036NHA	Atheros AR9271	External	Buy it Now
3	Alfa AWUS036NH	Ralink RT307	External	Buy it Now
4	Alfa AWUS1900	Realtek RTL88XX	External	Buy it Now
5	Alfa AWUS036ACH	RealtekRTL8812AU	External	Buy it Now
6	Panda PAU06	Atheros	External	Buy it Now
7	Panda PAU09	Ralink RT5572	External	Buy it Now
8	ALFA AWUS036NEH	Ralink RT307	External	Buy it Now

Wifi coconut

- The WiFi Coconut by Hak5 is wireless test equipment featuring an array of 14 finely tuned 802.11 WiFi radios. It lets pentesters and IT professionals monitor and record all 2.4 GHz WiFi channels simultaneously.
- Recordings may be saved as standard packet capture (pcap) files, meaning all 2.4 GHz WiFi events may be stored and analyzed.
- There are 14 channels on the 2.4 GHz WiFi spectrum. Why packet sniff with only one radio?
- Channel hopping misses 93% of the airspace at any given time.
- What if you could monitor all channels at once, from a single USB-C device?
- Now you can. Introducing WiFi Coconut: an Open source full-spectrum WiFi sniffer that simultaneously monitors the entire 2.4 GHz airspace.
- WiFi Coconut captures standard PCAP files with its 14 finely tuned 802.11 WiFi radios, and integrates with popular tools like Kismet & Wireshark.
- https://shop.hak5.org/products/wifi-coconut

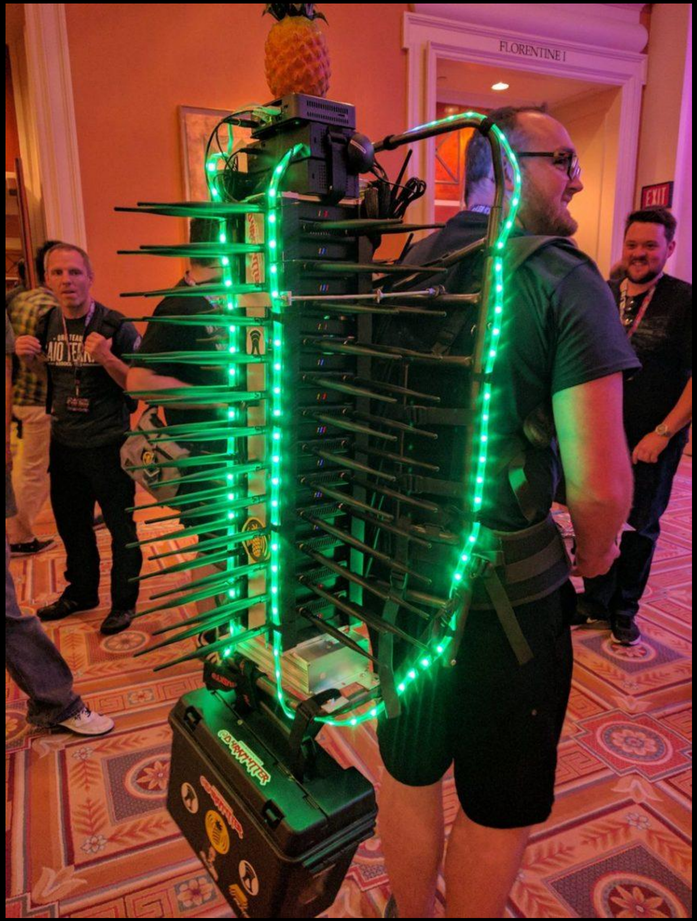
Wifi Pineapple

- Automate WiFi auditing with all new campaigns and get actionable results from vulnerability assessment reports. Command the airspace with a new interactive recon dashboard, and stay on-target and in-scope with the leading rogue access point suite for advanced man-in-the-middle attacks.
- Next-gen network processors combine with multiple role-based radios and the Hak5 patented PineAP suite to deliver impressive results. Hardened and stress tested for the most challenging environments.
- The new WiFi Pineapple Mark VII features incredible performance from a simple web interface with an expansive ecosystem of apps, automated pentest campaigns, and Cloud C2 for remote access from anywhere.
- https://shop.hak5.org/products/wifi-pineapple

ESP8266

- The main feature, the deauthentication attack, is used to disconnect devices from their WiFi network.
- No one seems to care about this huge vulnerability in the official 802.11 WiFi standard, so I took action and enabled everyone who has less than 10 USD to spare to recreate this project.
- I hope it raises more attention on the issue. In 2009 the WiFi Alliance actually fixed the problem (see 802.11w), but only a few companies implemented it into their devices and software.
- To effectively prevent a deauthentication attack, both client and access point must support the 802.11w standard with protected management frames (PMF).
- While most client devices seem to support it when the access point forces it, basically no WiFi access point has it enabled.
- https://github.com/SpacehuhnTech/esp8266_deauther

Wifi CACTUS



https://www.youtube.com/watch?v=0unUlvGEP3A

Wifi Kraken

https://www.youtube.com/watch?v=8LQYgnSx3lI

https://www.youtube.com/watch?v=nrfFyt7SRRY

Examples

- https://www.youtube.com/watch?v=vlyFOw8TzeY
- https://www.youtube.com/watch?v=WRi7CzDr61w
- https://www.youtube.com/watch?v=GIVrzoeWb3M
- https://www.youtube.com/watch?v=7v3JR4Wlw4Q
- https://www.youtube.com/watch?v=5MOsY3VNLK8

Execution Tips

Testing Execution

- When performing the physical pentest tests, always write down the details that you find interesting, whether it be security routines, number of cameras at the entrance, access controls and number of attendants
- Analyze the location geographically, mainly by restaurants and businesses that employees can attend at lunchtime, it helps a lot in a social engineering process
- Find information about the company on the internet, use OSINT for this
- Try to act as inconspicuously as possible, maybe not get a way into the building, impersonating someone or getting a job interview
- In the last case, try to use phishing techniques to catch some victim, it might come in handy in the future
- Any device that attacks wifi, bluetooth or radio frequency, use it in a safe distance

Testing Execution #2

- Use lockpicking away from security cameras, it's not cool to be recorded trying to force open a door
- Look for dark areas, whether from cameras, lack of security or any type of access control
- Rummage through the trash, maybe you'll find something interesting?

https://www.linkedin.com/in/joas-antonio-dos-santos

Report

Report Template

- A RedTeam Security Physical Physical Penetration Test Report provides detailed, actionable information to help improve physical security controls and the overall security posture of an organization. The report will include:
- Information learned during the Information Gathering and Reconnaissance phases of the project.
- Detailed steps, methods, and pretexts used during the execution of the physical penetration testing engagement
- Identification of successful and unsuccessful actions
- Evidence of security risks or mitigations observed during the engagement
- Recommendations for how to reduce risks in the future

Template:

- https://github.com/CyberSecurityUP/Red-Team-Management/tree/main/Physical%20PenTest

References

- https://www.triaxiomsecurity.com/what-is-a-physical-penetration-test/
- https://purplesec.us/physical-penetration-testing/
- https://www.triaxiomsecurity.com/our-physical-penetration-testing-methodology/
- https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/
- https://www.geoowl.com/services/geoint/
- https://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap7.htm
- https://www.encyclopedia.com/politics/encyclopedias-almanacs-transcripts-and-maps/imint-imagery-intelligence
- https://www.exabeam.com/information-security/top-8-social-engineering-techniques-and-how-to-prevent-them-2022/
- https://en.wikipedia.org/wiki/Software-defined_radio

References #2

- https://www.cybrary.it/course/physical-penetration-testing
- https://www.sans.org/course/physical-penetration-testing
- https://www.skillsoft.com/course/pentesting-for-physical-security-4cc77d58-6203-429b-bb2d-960e2f760ba3
- https://www.blackhat.com/tr-18/training/physical-penetration-testing.html
- https://drive.google.com/file/d/1wrmZ1xlJ_zeZu8PPs1p2cLVBDcN4Pi2u/view?usp=sharing