

Small Town Family Medicine Security Evaluation and Upgrade

Western Governors University

Table of Contents

Summary	3
Review of Other Work.....	6
Changes to the Project Environment.....	8
Methodology	9
Project Goals and Objectives	11
Project Timeline.....	12
Unanticipated Scope Creep.....	12
Conclusions.....	13
References.....	Error! Bookmark not defined.
Appendix A.....	15
Title of Appendix.....	Error! Bookmark not defined.
Appendix B	16
Title of Appendix.....	Error! Bookmark not defined.
Appendix C	17
Title of Appendix.....	Error! Bookmark not defined.

Summary

Small Town Family Medicine (STFM) is a small doctor's office offering general medical care to local patients. The office is owned by the sole physician, who is supported by a staff of four employees, two nurses and two front office staff. The doctor is approaching retirement age and has decided to sell the practice to a local hospital to ensure continued care for his patients after he steps away. As part of the preparation for the sale, the office hired Small Town Security Experts (STSE) to evaluate the current network for security issues and provide upgrades and remediations, particularly around the local server holding the personal health information (PHI) of the office's patients, which is protected under HIPAA. Ensuring that the PHI of the patients is secure was a critical part of the sale preparations as the hospital would not want to purchase an office that risks HIPAA violations through network insecurities. The upgrades also provided a more robust network with higher performance and reliability than the previous configuration. The original network consisted of a store-bought Linksys SOHO router with the office computers and PHI server plugged in directly. The router broadcasted two wireless networks, one for office use with access to the server and one for patient use. The guest network password was printed on a note beside the front desk, and the internal network was not hidden but was protected with a simple WPA2 password.

After performing a penetration test and vulnerability assessment on the network, STSE provided the office with a report indicating how the network was vulnerable and what remediations the team would take. The report also contained a list of maintenance the team performed on the then-current network devices and office computers, as well as which devices were to be removed or replaced, what devices and software were to be installed, and a diagram explaining how the upgraded network would be laid out and function.

The network was built using Cisco devices to ensure the reliability, performance, and support of an industry leader. A Firepower 1000 Series firewall in front of a 1000 Series Integrated Services Router now provides a secure connection into the office from the ISP, where a Catalyst 1200 Series switch segments the network into VLANs and provides switching functionality across the network. For Wi-Fi connectivity, a mesh of Business 150AX Access Points was connected to a VLAN on the switch, then used to provide three separate wireless VLANs to the office, one hidden network for wireless office laptops used by the physician and nurses to access the PHI server in exam rooms, a second for employee personal devices, and a third for patient use during their visit. All wireless networks are secured with WPA3.

The device choices and configuration provided the necessary performance and security while considering the small size of the office and managing upgrade costs.

The project was implemented in several steps over several weeks. First, the team performed a penetration test of the network and gained access to the PHI server. Given the sensitive nature of the information stored on the server, the team acquired explicit written permission from the practice and detailed rules of engagement before the test. The test simulated a realistic type of attack based on the office's physical location and layout, with the attacker in a vehicle parked in front of the building gaining access to the server by moving through the wireless network. Once the server was accessed, the test ended, and the tester generated a report describing the steps they took and the vulnerabilities they encountered with remediations.

After the test concluded, the team performed a vulnerability scan of the whole network. The scan results were combined with the pentester's report and analyzed to provide further remediations. The team also physically examined the network devices, office computers, and server to assess any maintenance needs before delivering the overall vulnerability report, a list of

remediations, and the plan for the new network layout, which included a detailed diagram and a list of new equipment the team installed in the next phase.

After obtaining approval from the practice, the team acquired the new network equipment and scheduled an installation date. The office was not able to access the network during the installation, so they closed for the day to allow the team to work. After installation, the team ensured that the network was performing as desired, performed a follow-up vulnerability scan, and repeated the penetration test to verify that the security upgrades were effective at securing the server.

Implementing the plan in this fashion ensured the team did not miss any critical vulnerabilities, the network was properly secured and returned to functionality, and the transition to the new network was as seamless as possible for the staff. The only change to the staff's routine was the day after the installation when a team member was on-site helping the staff reconnect their personal devices to the new wireless network specifically for those devices. An infographic was posted by the front desk to explain to patients how to connect to their new network. Having the network properly segmented and configured limits access to the PHI server to authorized personnel and devices and prevents potential lateral movement and access from potential outside attackers. In addition, the firewall device prevents malicious traffic from entering the network remotely. Securing the wireless networks with WPA3 prevents cracking attacks over the air like the one simulated in the penetration test. Overall, the upgraded network secured the PHI server behind multiple layers of defensive configurations.

Review of Other Work

Work 1

During installation, the team referenced the Catalyst 1200 Admin Guide many times to ensure the new switch was properly installed. The guide covers everything a network administrator might need to know to properly install, configure, and manage a Catalyst 1200 Series switch. The guide described the necessary tools and hardware to install the switch, whether in a rack, on a desktop, or even on a wall, as well as what computer software was needed to interface with the switch for configuration. Other parts of the guide of relevance to the project included the Configuration Wizards, VLAN Management, Security, and Access Control sections. The Configuration Wizards section provided a helpful wizard that allowed the team to quickly configure the three new VLANs, and the ACL Configuration Wizard helped create rules governing the traffic through the switch. Step 6 of the ACL Configuration Wizard allowed the team to whitelist the specific computers and laptops that needed access to the server by using the MAC addresses of those devices, preventing non-authorized devices from accessing the PHI server VLAN (Cisco, 2024).

Work 2

To plan for the penetration test portion of the project, the pentester read the article *The 5 Most Dangerous Wi-Fi Attacks, and How to Fight Them* on PCWorld.com. The article began by describing why attackers might target a Wi-Fi network, which boiled down to either collecting information on the network or about the network owner or using the network to mask other attacks. The article then covered five attack types: deauthentication, brute force, evil twin, router attacks, and remote attacks. Each attack type was described in three steps: how the attack works, what the hacker wants to achieve, and how to fend off the attack. For instance, according

to the article, using a deauthentication attack, “the hacker interrupts the connection between the router and a client,” then “intercepts the data traffic during the login, with which he tries to guess the Wi-Fi password” (Rau, 2023). Using this article, the team was able to craft the penetration test to simulate the most common attacks that the practice’s network would likely face and design a network secure enough to withstand them.

Work 3

A blog post on NordVPN’s website titled *WEP, WPA, WPA2, and WPA3: Differences Explained*, goes into detail about the differences between these four types of wireless security protocols. In deciding how to secure the new network, the team read over the article to ensure the most secure protocol was also suitable for the office. The article goes through each protocol one by one, explaining a bit of the history behind the protocol and then discussing, in the case of the first three, the security flaws that led to the next protocol in line to be developed as a replacement. Though WPA2 was a big step up in security compared to WEP and WPA, vulnerabilities have been discovered, leading to the development and release of WPA3. According to the article, WPA3 features stronger encryption, improved brute force attack protection, and a protocol known as the Simultaneous Authentication of Equals, or SAE (Šlekytė, 2023). This protocol helps keep passwords more secure, and the article specifically mentions that “features like this make wardriving and other hacker tactics less effective” (Šlekytė, 2023). Given that wardriving is one of the specific threats the team wanted to secure the network against, this feature was a must-have, and the team was confident that WPA3 was the solution for STFM. The article does note that device incompatibility can be an issue, as WPA3 is newer and older devices may not be compatible, but the only devices that were deemed necessary to accommodate during the upgrade were the office laptops, and they were relatively

new and compatible with WPA3. The staff was educated on this issue to explain connection issues arising from older personal devices that they or patients may have.

Changes to the Project Environment

Before the project, the network at STFM consisted of a store-bought Linksys SOHO router with the office computers and PHI server plugged in directly. The router broadcasted two wireless networks, one for office use with access to the server and one for patient use. The guest network password was printed on a note beside the front desk, and the internal network was not hidden but was protected with a simple WPA2 password.

The project replaced the Linksys router with a Cisco 1000 Series Integrated Services Router, with a Firepower 1000 Series firewall device placed between the ISP connection and the router to secure internet traffic. A Catalyst 1200 Series switch was connected to the router, then the office computers, PHI server, and one of the three Business 150AX Access Points were connected to the switch. The switch was configured to provide three separate VLANs: one for the server, one for the connected office computers, and one for the wireless network. The access point was then configured to provide wireless VLANs to the office, one hidden wireless network for wireless office laptops used by the physician and nurses to access the PHI server in exam rooms, a second for employee personal devices, and a third for patient use during their visit. The server VLAN was configured with a whitelist that allowed only the office computers and physician and nurse laptops to access the PHI server. The remaining two access points were installed across the building to provide a robust wireless mesh network, ensuring good connectivity and performance regardless of physical location in the practice. The two internal wireless networks were secured with WPA3, while the guest network was configured to

authenticate the patients against a Google or Facebook account to allow access using a feature of the access points.

Methodology

This project used a waterfall methodology. This methodology made the most sense as this was a one-time project with a straightforward endpoint. The phases of the methodology generally are as follows:

1. **Requirements:** The first phase involves gathering requirements from stakeholders and analyzing them to understand the scope and objectives of the project.
2. **Design:** Once the requirements are understood, the design phase begins. This involves creating a detailed design document that outlines the software architecture, user interface, and system components.
3. **Development:** The Development phase include implementation involves coding the software based on the design specifications. This phase also includes unit testing to ensure that each component of the software is working as expected.
4. **Testing:** In the testing phase, the software is tested as a whole to ensure that it meets the requirements and is free from defects.
5. **Deployment:** Once the software has been tested and approved, it is deployed to the production environment.
6. **Maintenance:** The final phase of the Waterfall Model is maintenance, which involves fixing any issues that arise after the software has been deployed and ensuring that it continues to meet the requirements over time. (GeeksforGeeks, 2024)

The phases of our project were as follows:

1. Requirements: our penetration test and vulnerability scans made up the bulk of our requirements phase. These informed the team of the security weaknesses our project needed to address specifically.
2. Design: for the design phase, we created the list of new network devices to be acquired and produced the remediation report and new network diagram.
3. Development: this phase was the installation date. The team installed and implemented the new network devices and configurations, including the new VLANs and wireless networks. They also configured a whitelist to allow only specific devices to access the server.
4. Testing: testing took place on the installation day to avoid any further interruption of business for the office. Tests focused on ensuring proper performance across the network and that the new security features were properly functioning.
5. Deployment: this phase took place the day after the installation date when a team member was on-site helping office staff connect devices to the new network, familiarize themselves with any relevant changes, and observing the network during an actual workday to discover any issues that were not apparent during testing.
6. Maintenance: any issues that arose during the deployment phase that the on-site team member could not resolve were addressed during maintenance, in addition to any issues that come up in the near future. The team at STSE stands by their work and will offer support when needed during a warranty window.

Project Goals and Objectives

The project's first goal was to evaluate the network's security with a penetration test in the form of an attack simulation and a full vulnerability scan of the network. The deliverables for this goal were the report detailing the network vulnerabilities and the list of remediations that the team implemented during the project, which were completed by the pentester and the team lead, respectively. The second goal of improving network security began with designing a secure network. The team delivered a diagram of the new network and a list of the new network devices that were acquired and installed to form the new network. The team then completed the second objective by acquiring and delivering the new network devices, and the third objective encompassed the actual installation, configuration, testing, and deployment of the new devices and network setup.

	Goal	Supporting objectives	Deliverables enabling the project objectives	Met/Not Met
1	Evaluated the network's security	1.a. Performed a penetration test/attack simulation	1.a.i. Vulnerability report from the pentester	Met
		1.b. Performed vulnerability scans and provided remediations	1.b.i. Vulnerability scan report	Met
			1.b.ii. List of remediations created from combined vulnerability reports	Met
2	Improved network security	2.a. Designed a secure network based on the office's needs	2.a.i. Diagram of new, secure network	Met
			2.a.ii. List of network devices to be acquired and new security configurations	Met
		2.b. Acquired new devices	2.b.i. New network devices	Met
		2.c. Installed and configured new devices	2.c.i. New network installed and configured	Met
			2.c.ii. New network tested and confirmed secure and functional	Met
			2.c.iii. Staff familiarized with changes and production functionality confirmed	Met

Project Timeline

Milestone or deliverable	Duration	Expected start date	Expected end date	Actual start date	Actual end date
Penetration test and vulnerability scan completed	1 day	1/6/2025	1/6/2025	1/6/2025	1/6/2025
Vulnerability and remediation reports, new network diagram, and list of devices for acquisition finished and delivered	1 week	1/7/2025	1/14/2025	1/7/2025	1/14/2025
New devices acquired	2 weeks	1/15/2025	1/29/2025	1/15/2025	1/29/2025
Network installation	1 day	1/30/2025	1/30/2025	1/30/2025	1/30/2025
Staff familiarization and follow-up	1 day	1/31/2025	1/31/2025	1/31/2025	1/31/2025

Luckily, the project was able to meet the projected timeline with little difficulty. The most likely source of delays was in acquiring the new network devices, but Small Town Security Experts happened to have the Cisco access points already on hand, was appropriately stocked on networking cables, and the other devices did not suffer any shipping delays, meaning the installation took place as planned.

Unanticipated Scope Creep

Overall, the project was completed smoothly and without any unforeseen issues. Given the small size of the practice, both physically and personnel-wise, as well as the relative simplicity of the practice's network needs, the project was straightforward and did not present many opportunities for scope creep. Thankfully, most of the staff was relatively young and familiar with technology, so acclimating to the new network configuration was mostly painless

and complication-free. The patient-side process of accessing the guest network did not have any significant changes for the patients as well.

Conclusions

Small Town Family Medicine needed its network security evaluated and upgraded in preparation for selling the practice to the local hospital. Our team completed the project by evaluating the network's current security status and then upgrading the network to provide a proper level of security for the stored patient information on the practice's server. As expected, the project required a single day of downtime on the part of the office for the network installation, but the upgrades provided have properly secured the server and prevented attackers from accessing patient information. The project was a success because the network is now properly segmented and protected against the attacks simulated by the team's penetration tester and major weaknesses discovered by the vulnerability scans. The team evaluated these metrics during testing after installation by repeating the attack simulation and vulnerability scans, finding that the attack was unable to gain access to the server using any of the previously attempted methods. While the team is aware that no security solution is perfect, the upgrades provided to STFM have secured the network well beyond the minimum standards of the hospital, ensuring that the state of the practice's information security will not be a hindrance in the upcoming sale.

References

- Catalyst 1200 Admin Guide*. (2024, August 21). Cisco. Retrieved February 10, 2025, from <https://www.cisco.com/c/en/us/td/docs/switches/campus-lan-switches-access/Catalyst-1200-and-1300-Switches/Admin-Guide/catalyst-1200-admin-guide.html>
- Rau, Thomas. (2023, September 25). *The 5 Most Dangerous Wi-Fi Attacks, and How to Fight Them*. PCWorld. <https://www.pcworld.com/article/2072976/attention-the-5-most-dangerous-wlan-attacks.html>
- Šlekutė, Irma. (2023, June 5). *WEP, WPA, WPA2, and WPA3: Differences Explained*. NordVPN. <https://nordvpn.com/blog/wep-vs-wpa-vs-wpa2-vs-wpa3/>
- Waterfall Model – Software Engineering*. (2024, October 18). GeeksforGeeks.org. Retrieved February 7, 2025, from <https://www.geeksforgeeks.org/waterfall-model/>

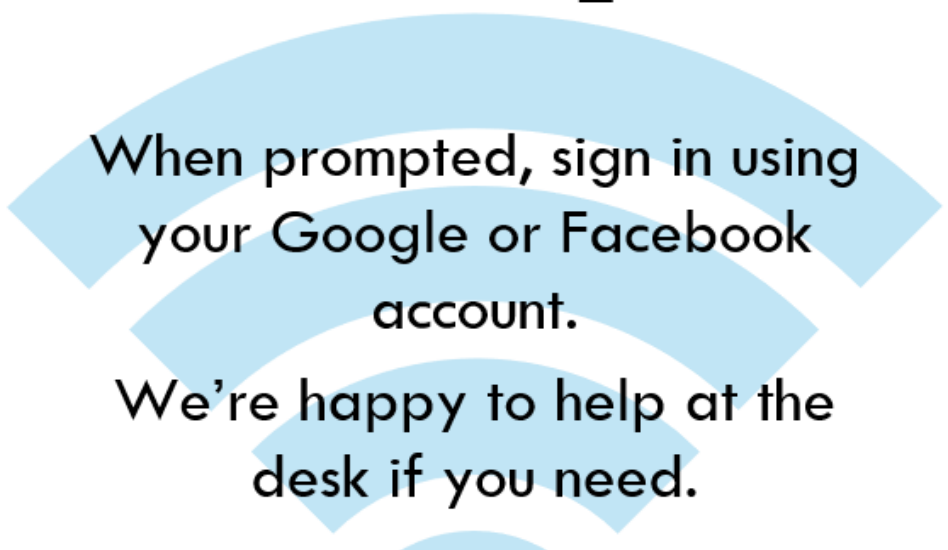
Appendix A

Patient Wireless Access Notice

This notice was placed on a placard at the front desk to instruct patients on how to access the new wireless network. Staff was shown what to expect from the login portal and how to assist patients with the login process.

Patient Wireless Access

Network: STFM_Guest



When prompted, sign in using
your Google or Facebook
account.

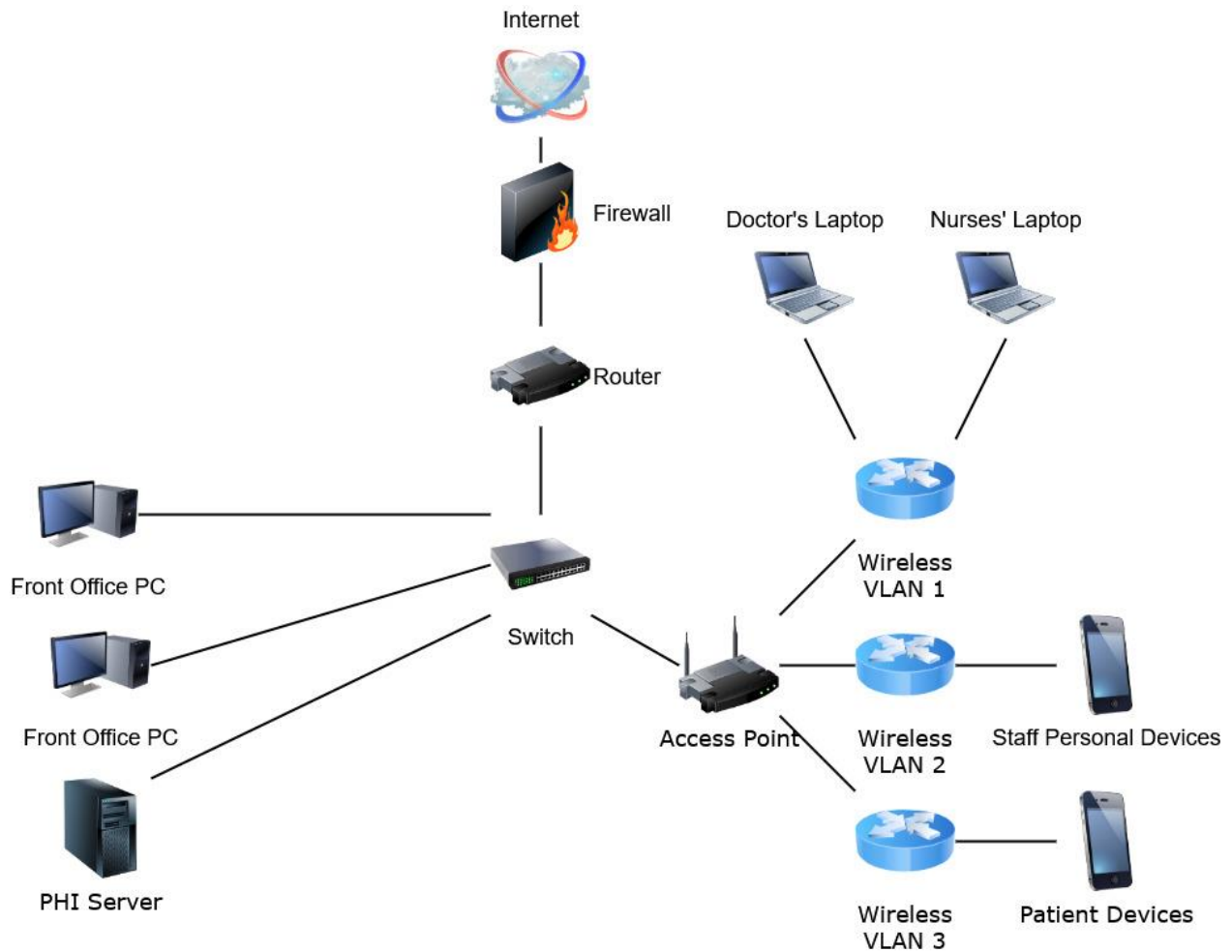
We're happy to help at the
desk if you need.

Thanks for visiting Small Town
Family Medicine!

Appendix B

New Network Diagram

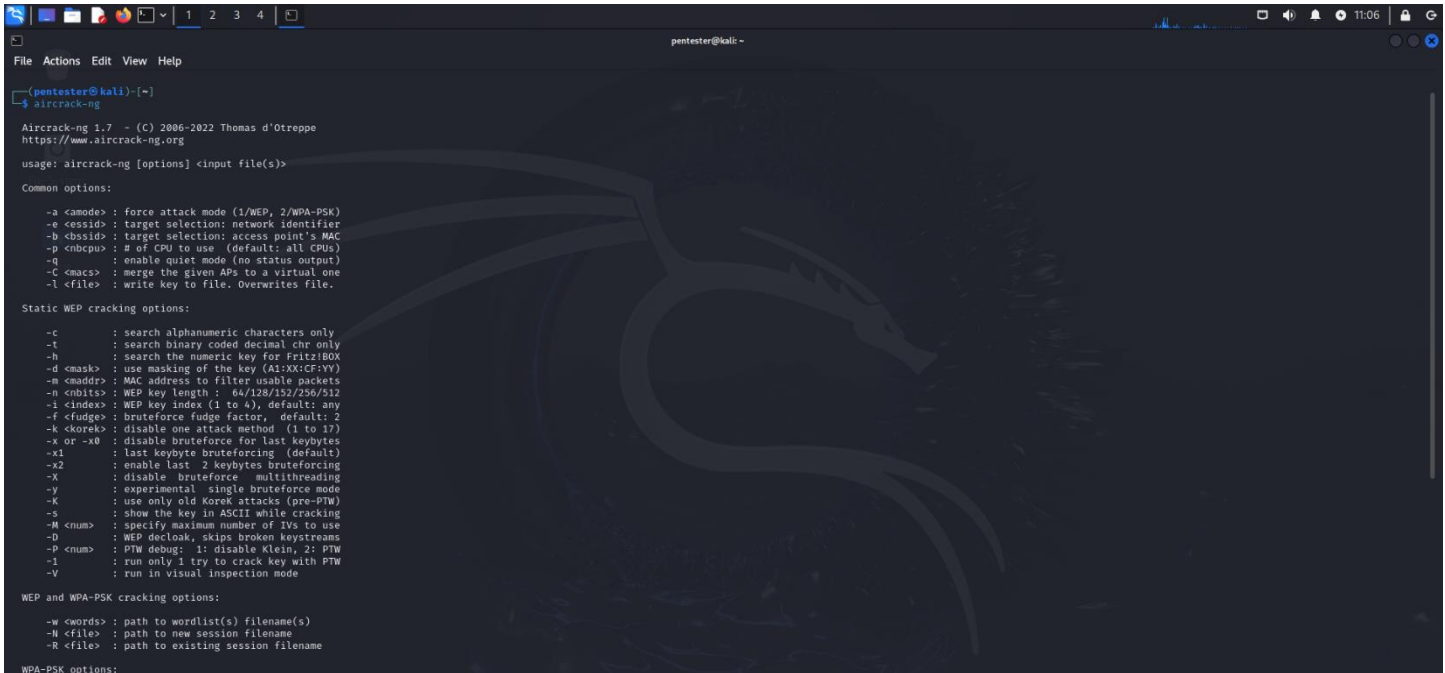
This diagram shows the logical layout of the new network and was delivered along with the list of new network devices as part of deliverable 2.a.



Appendix C

Aircrack-ng

Screenshot of the pentester starting aircrack-ng to crack the network password during the penetration test.



```
pentester@kali: ~  
$ aircrack-ng  
Aircrack-ng 1.7 - (C) 2006-2022 Thomas d'Ottreppe  
https://www.aircrack-ng.org  
usage: aircrack-ng [options] <input file(s)>  
  
Common options:  
-a <mode> : force attack mode (1/WEP, 2/WPA-PSK)  
-e <essid> : target selection: network identifier  
-b <bssid> : target selection: access point's MAC  
-p <nbcpu> : # of CPU to use (default: all CPUs)  
-q : enable quiet mode (no status output)  
-c <chars> : merge the given APS to a virtual one  
-l <file> : write key to file. Overwrites file.  
  
Static WEP cracking options:  
-c : search alphanumeric characters only  
-t : search binary coded decimal chr only  
-h : search the numeric key for Fritz!Box  
-d <mask> : use masking of the key (A1:XX:CF:IVV)  
-m <macaddr> : MAC address to filter usable packets  
-n <nbits> : WEP key length : 64/128/152/256/512  
-i <index> : WEP key index (1 to 4), default: any  
-f <fudge> : bruteforce fudge factor, default: 2  
-k <korek> : disable one attack method (1 to 17)  
-x or -x0 : disable bruteforce for last keybytes  
-x1 : last keybyte bruteforcing (default)  
-x2 : enable last 2 keybytes bruteforcing  
-X : disable bruteforce multithreading  
-y : experimental single bruteforce mode  
-K : use only old Korek attacks (pre-PTW)  
-s : show the key in ASCII while cracking  
-M <num> : specify maximum number of IVs to use  
-D : WEP decloak, skips broken keystreams  
-P <num> : PTW debug: 1: disable Klein, 2: PTW  
-l : run only 1 try to crack key with PTW  
-V : run in visual inspection mode  
  
WEP and WPA-PSK cracking options:  
-w <words> : path to wordlist(s) filename(s)  
-N <file> : path to new session filename  
-R <file> : path to existing session filename  
  
WPA-PSK options:
```