Wireless and Cyber Security Lesson Plan

Purpose: help students understand how attackers can breach wireless Internet using a router and WEP encryption.

Standards

CPP.L3A-09 Explain the principles of security by examining encryption, cryptography, and authentication techniques.

Objectives

Students will understand a brute force attack to try to find a valid username and password combination.

Students will be able to explain the importance of good practices in personal information security, using passwords, encryption, and secure transactions.

Students will explore principles of system design in security.

Students will be able to describe ethical issues that relate to computers and networks.

From https://www.techopedia.com/definition/18091/brute-force-attack

Attack 1-Wireless Router and Cain & Abel Software using AirPcap hardware

Materials: Wireless Attacks PowerPoint, wireless router (optional), AirPcap (optional), Cain & Abel software (optional)

Vocabulary: wireless router, AirPcap, Cain & Abel, WEP encryption, brute force

LINKSYS [®] by Cisco							
	Wireless-G Broadband Router wRT540L						
Setup	Setup Wireles Basic Setup	s Security Acces	Is Restrictions & Gaming	Administration Status			
Language Select your language Internet Setup	English :			Automatic Configuration - DHCP : This setting is most commonly used by Cable operators.			
Internet Connection Type	Automatic Conf	Host Name : Enter the host name provided by your ISP.					
Optional Settings (required by some ISPs)	Router Name: Host Name: Domain Name:	WRTS4GL		Domain Name : Enter the domain name provided by you ISP, More			
	MTU: Size:	Auto +		Local IP Address : This is the address of the router.			
Network Setup	- 039			Subnet Mask : This is the subnet mask of the router.			
Router IP	Local IP Address: Subnet Mask:	192 . 168 . 1 . 1 255.255.255.0 *		DHCP Server : Allows the rou to manage your IP addresses			
Network Address Server Settings (DHCP)	DHCP Server: Starting IP Address: Maximum Number	Enable Disable 192.168.1.200		Starting IP Address : The address you would like to start with. Maximum number of DHCP Users : You may limit the			
	of DHCP Users: IP Address Bance	192 168 1 100 to 149		number of addresses your rou hands out.			

The images for each of the steps is

available in the PowerPoint slide deck listed in the materials.

1.In the online router setup, begin by naming the SSID (service set identifier), which will name the router.

2. Notice the router's capabilities related to the standard's protocol.

Also important is to choose the router's channel from 1-11. Although there are 14 channels, the upper ones could possibly interfere with 2.5GHz frequencies. One, six, and eleven are the typical choices as they are spaced 22 MHz apart with a 1 MHz guard band between.

3.Routers typically offer several security modes. We are going to be using WEP for the password exploitation attack in the upcoming demo. WPA2 is currently the preferred security mode with the least vulnerability for attack. Remember earlier we said the difference between a 64 bit and a 128 bit encryption is 750,000 possibilities; this small difference exponentially increases the possibilities, thereby reducing the threat.

4.For the attack described in this presentation, we are going to unblock anonymous Internet requests to enable the packet capture. This will reinforce how important it is to make sure firewall rules are enabled as this attack would not work very well if at all if this box was checked.

5. 2.4 is the predominant frequency for wi-fi transmission due to the resilience of the signal as compared to 5GHz.

However, 5GHz offers less congestion as it is not used as much and can transmit data faster than 2.4GHz.

More about wi-fi can be found <u>https://en.wikipedia.org/wiki/IEEE_802.11</u>

6.This frequency allocation chart by the FCC will give a nice pictorial representation of how the frequencies are utilized by which sources and systems. Particularly important are the bands at 2.4 GHz and 5.0 GHz

7. Active and Passive Scanning

Passive: Beacon Frames sent from Access Point (AP) Association Request (not encrypted) or Authentication Request (encrypted) sent from computer to router Association/Authentication Response sent from router to computer

Active: Probe Frames sent from Access Point (AP) Association Request (not encrypted) or Authentication Request (encrypted) sent from computer to router Association/Authentication Response sent from router to computer

, Decoders 🔮 Network 🗐 Sniffer (Cracker 🔄 Traceroute	2 CCDU 👸 Wireless 🕼 Query		
AirPcap USB wireless capture adapter nr. 00 \\\\airpcap00				Paesive Scan
APProp Diret entire 4.11.1020 Correct shows 6 Local on durantel Si BB, 2407000 Hz, FKVTX P Option VEP Million dura finite Transmission of the finite Analysis of the finite finite finite Analysis of the finite finite finite Analysis of the finite finite finite finite Analysis of the finite finite finite finite Analysis of the finite finite finite finite finite finite Analysis of the finite finite finite finite finite finite Analysis of the finite finite finite finite finite finite finite Analysis of the finite	BSSD Last new 0 2405 CS4T3861 21/0726 0 2405 CS4T3861 21/0726 0 2405 CS4T3852 21/0726 0 2405 CS4T3852 21/0726 0 2405 CS4T3852 21/0726 0 2405 CS4T3852 21/0726 0 2405 CS4T3252 21/0726	Veles Encypted Network:	BIJ Packets Ungas WEP My 0 0 0 5 0 - 4 0 - 2 0 - 3 0 - 4 0 - 5 0 - 440 0 - 5 0 - 6 0 - 445 0 - 465 0 -	
	2.			

To actually perform the attack, install the Cain & Abel software and attach the AirPcap hardware to the computer.

- 1. Open the program Cain and Abel
- 2. Click on the tab "Wireless"
- 3. In the AirPcap USB wireless capture adapter field, select "\\\airpcap00"
- 4. Start active scanning for available SSID signals, then click "stop"
- 5. Select the target SSID, in this case the linksys, and notice the encryption is set to WEP and the channel is "6"
- 6. Set the lock on channel to the corresponding channel
- 7. Check WEP Injection to enable "ARP Request" (address resolution protocol)
- 8. For maximum speed, set the TxRate to "54" Mbps
- 9. Begin passive scan; hint, to increase the speed of the scan, right click on the list of the mac addresses and select "deauth"
- 10. After the suggested number of packets have been acquired, click "Analyze" and select the "PTW Attack" to enable the WEP attack. If you are successful, it will show the key; if not successful, continue with the scan to increase the number of packets before trying again.

Attack 2-ARDrone2

Materials and Resources FreeFlight Mobile app (available for iOS and Android)

https://github.com/felixge/node-ar-drone

In this scenario the owner is controlling the drone with a mobile device, which is used to move the drone to hover next to the attacker. The attacker decides to ground the drone with telnet, which is a remote log in. Finally the attacker runs a previously created program to control the drone.

1. Using a mobile device, connect to the drone's wireless signal. Using the Free Flight app, the owner maneuvers the drone to hover near the attacker.

2. The attacker (who is annoved by the hovering drone) makes a connection to the wireless network. Then opens the terminal and connect to the drone first testing the connection and then through telnet and drone IP address.

- 0 ping w.x.y.z
- 0 telnet w.x.y.z
- o poweroff

or

o reboot

3. The attacker can change the name of the drone and the IP address to hide declare that he's the owner. If the attacker didn't want to take control of the drone, he could just take data from the device like the image, video, or flight data or programs set on it. Another attack would be that he could inject some kind of program into the drone as well.

Then the attacker grabs the drone and begins flying it with his own device trading roles as the new owner.

4. The new attacker takes control of the drone by setting a program.

This program injects arbitrary packets to the drone in order to take the control of it. In this case the attacker is able to send its own command to the drone. We are using Node js and java script to write the program for the drone.

	240 2 260060	102 168 1 4	102 169 1 1	an deene	AR Dropp Dacket
	540 5.800909	192.100.1.4	192.108.1.1	ai_urone	AN DI DITE PACKEL
	342 3.891575	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	349 3.921727	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	356 3.954207	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	358 3.986789	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
1	360 4.018712	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
1	362 4.049094	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
1	364 4.079943	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	366 4.110863	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	368 4.149128	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	370 4.179569	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	372 4.209548	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
	374 4.239537	192.168.1.4	192.168.1.1	ar_drone	AR Drone Packet
> Eth	ernet II. Src: (hiconvE af:df:c7	(b0:c0:90:af:df:c7). Dst	: ParrotSa	91:af:d4 (90:03:b7:91:af:d4)

o vi drone.js

```
> Internet Protocol Version 4, Src: 192.168.1.4, Dst: 192.168.1.1
```

```
User Datagram Protocol, Src Port: 33812 (33812), Dst Port: 5556 (5556)
AR Drone Packet
```

```
Command: REF
```

```
Sequence Number: 13611
Control Command: 512
```

✓ Command: PCMD Sequence Number: 13612 Flag: 1 Roll: 0 (NO CHANGE) Pitch: 0 (NO CHANGE) Gaz: 1056925390 (INCREASE VERT SPEED) Yaw: 1034147594 (ROTATE RIGHT)

What's an Algorithm? David York Youtube <u>https://www.youtube.com/watch?v=6hfOvs8pY1k</u> What's an algorithm? A. A science, B. A set of instructions for solving a specific problem, C. A sequence of steps that will repeat some number of times, D. English-like syntax that resembles a programming language

If there are three people in the room, how many times does line 3 of the algorithm execute? A. 0, B. 1, C. 23 D. 6

If there are six people in the room, how many times does line 3 of the algorithm execute? A. 0, B. 1, C. 23 D. 6

Einstein's Riddle by Dan Van der Youtube https://www.youtube.com/watch?v=1rDVz_Fb6HQ

YoutubePasscode Riddle by Ganesh Pai https://www.youtube.com/watch?v=7Vd1dTBVbFg

Can you solve the temple riddle? by Dennis E. Shasha https://www.youtube.com/watch?v=nSbvlktToSY

Prisoner Hat Riddle by Alex Gendler Youtube https://www.youtube.com/watch?v=N5vJSNXPEwA