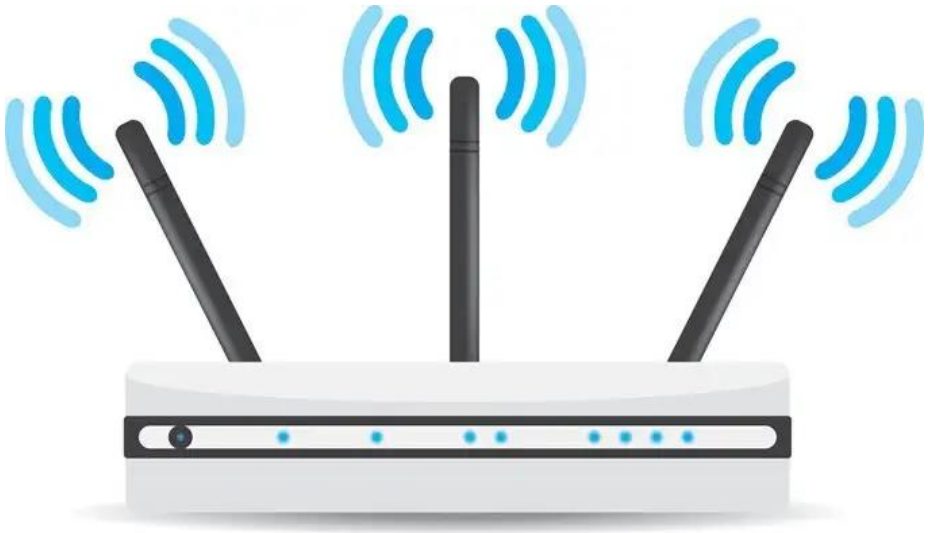
FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Wireless Attacks



FANSHAWE

Agenda

- Housekeeping notes
- Wireless Infrastructure
- Wireless Attacks
- Cracking Wireless
- Overview of Lab

FANSHAWE

Wireless Infrastructure

FANSHAWE

Wireless Networking

- Provides access to the back end wired network infrastructure without the need for a physical connection
- This is very convenient for users, but poses many challenges when it comes to security
  - People accessing wireless signals from outside the organizations physical walls
  - Rogue devices and access points providing pathways into the network
  - Unauthorized access through breaking weak implementations of wireless protocols

FANSHAWE

Wireless Components

WNIC

- Wireless Network Interface Card

AP

- Access Point

Wireless Protocols

- WEP, WPA, WPA2, WPA3, etc.

SSID and BSSID

- Service Set Identifier and Basic Service Set ID
- Identifies the WLAN and wireless device respectively

WLAN

- Wireless Local Area Network

FANSHAWE

Wireless is Accessible by Design

Utilizes open and unlicensed frequency bands

- Provides users with high availability and mobility
- Also allows attackers easy access to signals
  - Monitoring traffic
  - Interfering with traffic (DoS)

It is very hard to keep wireless traffic from leaking outside the physical boundaries of the organization

- Can use antenna positioning and tuning, but it isn't a complete solution
- There will always be some wireless leakage

FANSHAWE

Unauthorized Access

Attackers have a variety of goals when accessing the network

- Free Internet access
  - Seems somewhat harmless, but can lead to problems if they are preforming illegal activities via this connection
  - Illegal downloads, attacking other users over your connection
- Information Gathering
- Getting a foot in the door for further attacks on your network
  - Placing a wireless device in the building, with a direct connection to the wired network

FANSHAWE

Exposures & Interference

Rogue Access Points or Hotspots

- Not controlled by the organization

Fall into three main categories:

Unauthorized

- Installed by Employees

Hostile

- Installed by Attacker

Neighboring

- Seen from neighboring users

FANSHAWE

Rogue APs

Unauthorized APs

- Usually set up for convenience by uneducated users
  - For example if they are getting a weak signal from the organizations wireless network
- Often have poor, or no security measures in place
- Can provide an attacker direct access to the wired network
- Consumer APs, mobile phone or laptop hotspots, etc.

FANSHAWE

Rogue APs

Hostile APs

- Set up by an attacker with two main goals
  - Persistent backdoor access to the network
  - Tricking users into connecting so they can better monitor their traffic (MITM)

Neighboring APs

- These don't provide access to the network, but can interfere with your organizations APs
  - Could be used for DoS attacks
  - More often simply competing for the open medium

FANSHAWE

Rogue Peers

Rogue peers are devices that have a connection to the internal network and are offering it to other users

- Hotspots from mobile devices
- Ad-hoc networks via laptops

The main problem is that they are bypassing the organizations security measures

- One employee logs into the network officially
- Connection is offered to other employees and attackers, often with little or no authentication

FANSHAWE

Controls

There are a wide variety of controls that can be used to secure wireless networks

- AAA
- Encryption
- IDS and IPS
- Security Policies

FANSHAWE

AAA

As with many areas of security, AAA is a key component

Authentication:

- Validating the identity of the user
- Username, password, security token, certificates, etc.

Authorization:

- Controlling access to resources

Auditing / Accounting:

- Recording access to resources

FANSHAWE

AAA Authentication

Two main ways authentication can be done:

Local

- Doesn't scale very well
- Credentials are created and stored on the wireless device
- Access Point, Wireless LAN Controller, etc.

Authentication Server

- Credentials are created and stored on a separate server
- RADIUS: Remote Authentication Dial In User Service
- AD: Active Directory
- Cisco TACACS: Terminal Access Controller Access Control System

FANSHAWE

Encryption

Encryption provides Privacy and Integrity

- Privacy: rendering the data unreadable
- Integrity: ensuring the data wasn't tampered with

In most cases wireless local area networks (WLANs) use partial encryption

- The traffic is encrypted from the user to the access point
- In some cases, such as when a Wireless LAN Controller (WLC) is used, the traffic will be encrypted back to the WLC

FANSHAWE

IDS & IPS

IDS: Intrusion Detection System

- Looks for signatures and sends an alert

IPS: Intrusion Prevention System

- Looks for signatures and takes preventative action in addition to sending an alert
- Preventative actions
  - Dropping traffic
  - Isolating rogue APs
  - Shutting down switch ports

FANSHAWE

Policies

Defining how wireless security is going to be implemented and managed

- Installation and configuration parameters
  - Protocols, AAA, etc.
- What constitutes acceptable use (AUP)
- What training will be required of users before they are granted access

FANSHAWE

802.11 Authentication Types

802.11 is the set of IEEE standards for implementing wireless networks

There are a wide variety of authentication types used with wireless networks

- Open
- Shared
- MAC
- WEP
- WPA Personal and Enterprise
- WPA2 Personal and Enterprise
- 802.1X and EAP

FANSHAWE

802.11 Authentication Types

Open Authentication

- Choosing to use no authentication
- Hotspots

Shared Authentication

- Using a preshared key alone

MAC

- Using the 48 bit Media Access Control address to limit access
- Can be easily spoofed
- Usually implemented to prevent inadvertent access

WEP

WEP

- Wired Equivalent Privacy
  - Definitely Not
- Broken implementation of shared authentication
- Used a weak implementation of the RC4 stream cipher
- Primary problem was the use of a weak initialization vector (24-bit)
  - IV is supposed to prevent repetition of keys

FANSHAWE

WPA

Wi-Fi Protected Access

- Temporary implementation while WPA2 (802.11i) was being developed
- Developed by the Wi-Fi Alliance to replace WEP
- Can be implemented in two ways
  - WPA Personal
    - Uses a passphrase
  - WPA Enterprise
    - Uses 802.1X and EAP (Extensible Authentication Protocols)

FANSHAWE

Wi-Fi 5

- 802.11ac
- Released in 2014 to replace 802.11n
- Speeds of up to 1,300 megabits per second
  - Utilizes MU-MIMO
  - Allows for the use of more antennas

FANSHAWE

Wi-Fi 6

- 802.11ax
- Released in 2019 to replace 802.11ac
- Speeds of up to 10Gbps
- Uses broadcast sub channels to increase network capacity
- Utilizes MU-MIMO
  - Allows for the use of more antennas

FANSHAWE

802.1X & EAP

802.1X is the authentication framework

- Supplicant
  - Software installed on client device
- Authenticator
  - Access Point
- Authentication Server
  - Radius, AD, TACACS, etc.

EAP (Extensible Authentication Protocol)

- Specifies how user credentials are sent
- Variety of types of EAP can be used

FANSHAWE

EAP Methods

LEAP

- Lightweight EAP, developed by Cisco, broken

PEAP

- Protected EAP

EAP-FAST

- EAP with Flexible Authentication through Secure Tunneling

EAP-TLS

- EAP using transport layer security
- Allows for mutual authentication

FANSHAWE

Layer 2 Encryption

- Protects the connection between the client device and the Access Point
- Stops at the access point
- Traffic between the access point and the rest of the network is unencrypted
  - Devices between the AP and the endpoint of the traffic will be able to read the data

FANSHAWE

Layer 3 Encryption

- Protects the traffic from end to end
  - Client device to end point
- Devices between the endpoints can’t read the data

FANSHAWE

TKIP & AES

TKIP (Temporal Key Integrity Protocol)

- Cracked in 2008
- Operates at layer 2
- Required by WPA
- Not Allowed by WPA2

AES / CCMP

- Current Standard
- Operates at layer 2
- Optional with WPA
- Required by WPA2

FANSHAWE

Attack Terminology

WarDriving

- Driving around looking for wireless networks
- Also WarWalking, WarFlying, etc.

WarChalking

- Identifying open or easily compromised networks
- Uses a variety of symbols to relay information to other people, or for future attacks

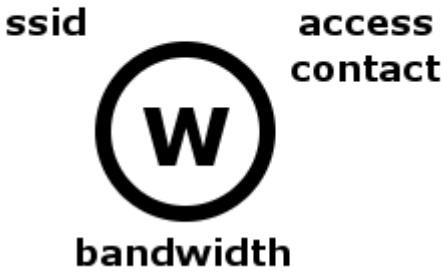
FANSHAWE

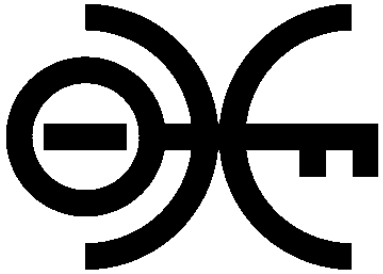
WarChalking Symbols

open node

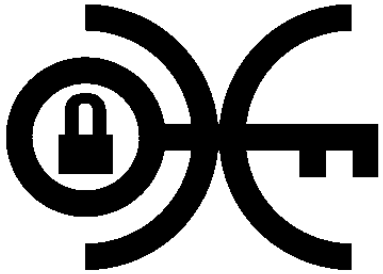
closed node

WEP node





Invisible Node



MAC Access Control

FANSHAWE

Weaknesses of Security Measures

We are going to look at a variety of security measures and the flaws with them

- SSID Hiding
- MAC Address Filtering
- Weak Authentication
- WLAN Encryption Flaws
- Attacks on the infrastructure

FANSHAWE

Hidden SSID

People often think hiding their SSID will prevent WarDrivers from finding their network

- All this does is to remove the SSID from the beacon frame the AP is sending out

If the attacker listens for a probe request and probe response from a legitimate user they will be able to see the SSID

- Many hacking tools can force this process by sending de-authentication packets

FANSHAWE

MAC Filters

The idea behind this security control is to restrict the WNICs that can connect to the AP by MAC address

- Unfortunately an attacker can sniff the network for legitimate connections to the AP in question and record their MAC
- The attacker can then simply spoof their MAC and connect, or proceed with their attack

FANSHAWE

Shared Authentication

Using a shared key such as a WEP key to authenticate client

Authentication Steps

1. Client sends authentication request
2. AP sends challenge text back
3. Client encrypts challenge text with shared key
4. Authentication succeeds or fails

Problem stems from the fact that the attacker can see the plain text challenge and the encrypted response

FANSHAWE

Shared Authentication

- With the plain text challenge and encrypted response in hand the attacker can determine the keystream
- The keystream can then be used by the attacker to encrypt future challenges from the AP
  - The key is that the attacker doesn't need to know the key, just the keystream

FANSHAWE

Infrastructure Attacks

These attacks are focused on the organization's wireless infrastructure

- Default accounts
- Default credentials
- Denial of Service Attacks
- Evil Twin
- Rogue Access Points

FANSHAWE

Defaults

Default accounts and credentials fall into the arena of security misconfigurations

- There is nothing wrong with the device, but the administrator hasn't taken the time to properly configure the device

Attackers can search the internet for these defaults

- The SSID, if left at its default will let them know what kind of device is being used
- e.g. linksys

FANSHAWE

Denial of Service Attacks

There are a wide variety of DoS attacks that can be performed on wireless networks

- De-Authentication attacks
- Dis-Association attacks
- CTS-RTS attack
  - Clear To Send Request To Send
- Signal interference attacks
  - Introducing traffic that interferes with the legitimate traffic

FANSHAWE

De-authentication Attacks

Example using **aircrack-ng** suite:

```
aireplay-ng --deauth N -c [CLIENT MAC ADDRESS] -a [AP MAC ADDRESS] wlan0mon
```

N The number of attacks… 0 represents an infinite number

-c The Client/Victim MAC address

-a The Access Point's MAC address

wlan0mon is the name of the network card in monitor mode

FANSHAWE

Evil Twin

This is an access point on the network advertising the same SSID as the legitimate access point

- Users are tricked into connecting to the malicious AP
- Leads to MITM attacks

Evil twins with MAC address spoofing are even more dangerous

- Malicious AP is very difficult to detect

FANSHAWE

WiFi Hak5 tools

https://hakshop.com

FEATURES

Leading Rogue Access Point
Patented PineAP Suite thoroughly mimics preferred networks, enabling man-in-the-middle attacks

WPA and WPA Enterprise Attacks
Capture WPA handshakes and imitate enterprise access points, capturing enterprise credentials

Precision Targeting Filters
Stay within the scope of engagement and limit collateral damage with MAC and SSID filtering

Simple Web Interface
Fast and intuitive with an emphasis on workflow and actionable intelligence – just click to attack

Cross-Platform
No software to install. Works in any modern web browser on Windows, Mac, Linux, Android, iOS

Advanced Reconnaissance
Visualize the WiFi landscape and the relationships between access points and devices

Actionable Intelligence
Identify vulnerable devices, gather intelligence on the target and direct attacks

Passive Surveillance
Monitor and collect data from all devices in the vicinity. Save and recall reports at any time

Automated Campaigns
Guided campaign wizards deliver repeatable, actionable results with custom reports

Cloud C² Enabled
Deploy with confidence. Remotely command and control the airwaves with Hak5 Cloud C²

FANSHAWE

Best Practices

For SOHOs up to medium sized businesses use WPA3-Personal with a long passphrase

- 8 to 63 characters allowed
- 16 characters is considered a good length
- Also known as Pre-Shared Key (PSK)

WPA3-Personal has two variants:

- WPA3 Only
- WPA3 Transition Mode (Uses WPA2/WPA3)

FANSHAWE

Best Practices

For larger enterprises use WPA3 Enterprise

- WPA2 – Enterprise with EAP-TLS for devices that cannot use WPA3
- Uses both client and server side certificates
- Uses 128-bit and 192-bit modes
- Used with AAA
- Current standard

FANSHAWE

Cracking Wireless

FANSHAWE

Dictionary Lists

- In their simplest form they are simply a list of text strings people often use as passwords
- To make them more useful the attacker pre-computes the password hashes for all the passwords in the list
  - Processor intensive and requires a lot of storage
- When the attacker gets hold of a list of password hashes, they simply do a reverse lookup based on the pre-computed hashes

FANSHAWE

Rainbow Tables

- More advanced than simple password list/hash matching databases
- Capable of cracking longer passwords
- The actual table only stores a selection of hashes
- Uses complex algorithms to find the password
- Requires more processing resources at the time of cracking than a simple password list/hash lookup
- Overall table is smaller

FANSHAWE

Aircrack-Ng

Attackers will often use a tool like the Aircrack-Ng suite to crack WEP and WPA Encryption

Contains a variety of tools

- airmon-ng for configuring WNIC
- airodump-ng for displaying and saving information
- aireplay-ng for capturing packets then injecting them back into the network to generate traffic
- aircrack-ng for breaking the key

FANSHAWE

John The Ripper

Free password cracking software

- Can be used in combination with Aircrack-ng
- Originally developed for UNIX systems, but works on over 15 platforms currently
- Combines a number of password crackers into one tool

Cracking WPA

Involves first capturing packets with a tool like airodump-ng, tcpdump, wireshark, etc.

- The attacker is looking for the WPA four way handshake
  - Once the attacker has the handshake they can attempt to crack the passphrase
  - You can filter for eapol frames in Wireshark
  - Extensible Authentication Protocol over LAN
- Aircrack-ng can use a dictionary attack to attempt to crack the key
  - Phrase needs to be in the dictionary
- These attacks are quite processor intensive

FANSHAWE

aircrack-ng & coWPAtty

Both tools allow us to crack WPA/WPA2-PSK

- Pre-Shared Key

Both tools require three pieces of input

- pcap file containing a WPA four way handshake
- SSID or BSSID
- dictionary file

As long as the preshared key the victim is using exists in the dictionary file, the attacker will be able to crack the password

- It can take a very long time depending on the size of the dictionary file

FANSHAWE

Pre-Calculating PMK / PSK

Used with cracking WPA/WPA2 PSK

- PSK (Pre-Shared Key)

Targets the most processor intensive process in cracking

- Calculating the pre-shared key for a given SSID and dictionary list

The passphrase still needs to be in the dictionary, but the process is much faster

- Seconds and opposed to minutes or hours

FANSHAWE

After Cracking

Attacker can perform a variety of actions after cracking the network key

Decrypting network traffic

- Airdecap-ng can be used to perform this action

Connecting to the network

- Can use a variety of tools to perform this action, such as:
  - iwconfig for WEP
  - WPA_Supplicant for WPA

FANSHAWE

coWPAtty

- Command line tool that runs on Linux systems
- Automates dictionary attacks against WPA-PSK

Has three requirements:

1) Wordlist that contains the passphrase
2) A dump file that contains the four way handshake
3) The SSID of the network

FANSHAWE

coWPAtty Options

- -f Dictionary file
- -d Hash file (genpmk)
- -r Packet capture file
- -s Network SSID
- -2 Use frames 1 and 2 or 2 and 3 for key attack
- (nonstrict mode)
- -c Check for valid 4-way frames, does not crack
- -h Print this help information and exit
- -v Print verbose information
- -V Print program version and exit

FANSHAWE

genpmk

Tool used to pre-compute hashes

- Used in cracking WPA/WPA2

Inputs

- Dictionary list
- SSID of the wireless network

Limitations

- The password needs to be in the dictionary list
- You need to pre-compute the hashes for every SSID you are doing a pentest on

FANSHAWE

genpmk Options

- -f Dictionary file
- -d Output hash file
- -s Network SSID
- -h Print this help information and exit
- -v Print verbose information
- -V Print program version and exit

FANSHAWE

Pyrit

Another tool used to create databases of pre-computed PSKs

- Used in cracking WPA/WPA2
- Exploits multi core platforms to pre-compute
  - ATI-Stream
  - Nvidia CUDA
  - OpenCL
- Very powerful tool
- More advanced than genpmk

FANSHAWE

Viewing Wireless Traffic

Monitor Mode

- Allows WNIC to capture wireless packets
- WNIC doesn't need to associate with AP

Promiscuous Mode

- Also allows WNIC to capture wireless packets
- WNIC needs to be associated with the AP
- Ignores the restriction to only process packets directed to the WNIC, instead accepts them all

FANSHAWE

Wireshark

This network traffic analyzer tool should look familiar…

Wireshark was the tool used to capture the four way handshake we will be cracking

- Avoids the need for us to set up APs in the lab
- Online students don’t have access to the APs

FANSHAWE

NetStumbler

- Windows based tool
- Active sniffer
- Variety of uses
  - WLAN detection
  - Verifying network configurations
  - Finding dead spots when doing site surveys
  - Detecting wireless interference
  - Detecting rogue access points
  - GPS Integration
  - And More

FANSHAWE

Kismet

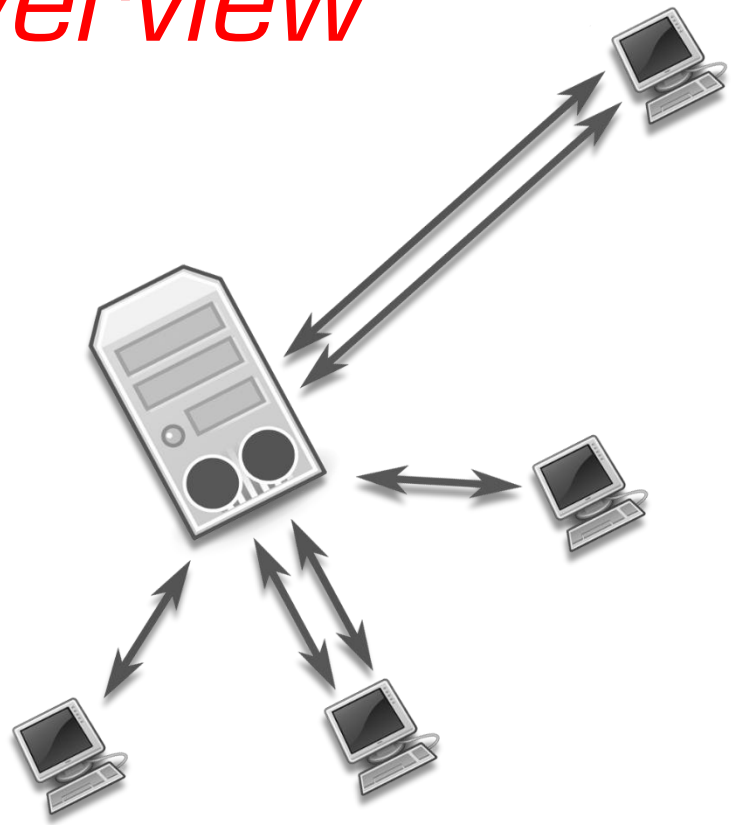
Primarily runs on Linux and Linux based systems due to hardware support

- Passive Sniffer
- Variety of uses
  - WLAN Detector
  - Packet Sniffer
  - Intrusion Detection
  - GPS Integration

https://www.kismetwireless.net/

FANSHAWE

Lab 09 Overview



FANSHAWE

Lab 09 Overview

- Dictionary Attacks
- coWPAtty
- Autoroute
- Genpmk
- Hashdump and JtR