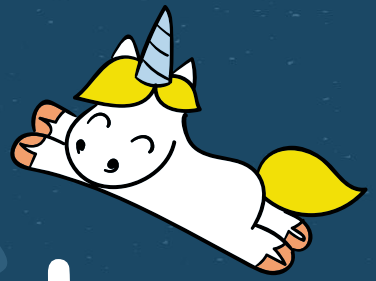




Cafe Lattes and Pixie Dust

Modern WIFI Mayhem with Wifite









Agenda

01 What's this WIFI Thing and How Does it Work?

02 Fite-ing with the Man in the Middle

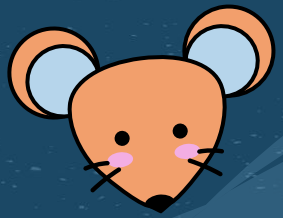
03 Pixies, Lattes, and 0 Day Unicorns

04 Lord Farquaad-ing

1

What's this WIFI Thing and How Does it Work?

"No one really understands how a network ACTUALLY works..." - Ken Pyle



WIFI = Data + Radio Waves

Devices convert data into a type that can be transferred over radio waves in a client-server relationship.

WIFI is a Layer 1 & 2 Protocol at its Core

- Layer 1: Communication among Physical Devices (does NOT have to be wired)
  - Device → Router → Modem → ISP
- Layer 2: Construction of Data Frames
  - Theses frames carry payloads (ie Network Packets)

Networked WIFI Devices communicate via Network Packets

Ethernet (802.3) Frame Format

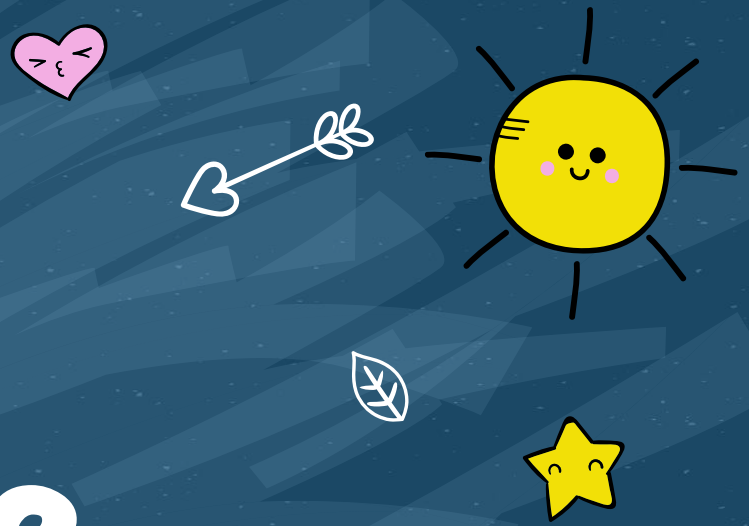
7 bytes	1 byte	6 bytes	6 bytes	2 bytes	42 to 1500 bytes	4 bytes	12 bytes
Preamble	Start of Frame Delimiter	**Destination MAC Address**	**Source MAC Address**	Type	Data (payload)	CRC	Inter-frame gap

For TCP/IP communications, the payload for a frame is a packet

WiFi (802.11) Frame Format

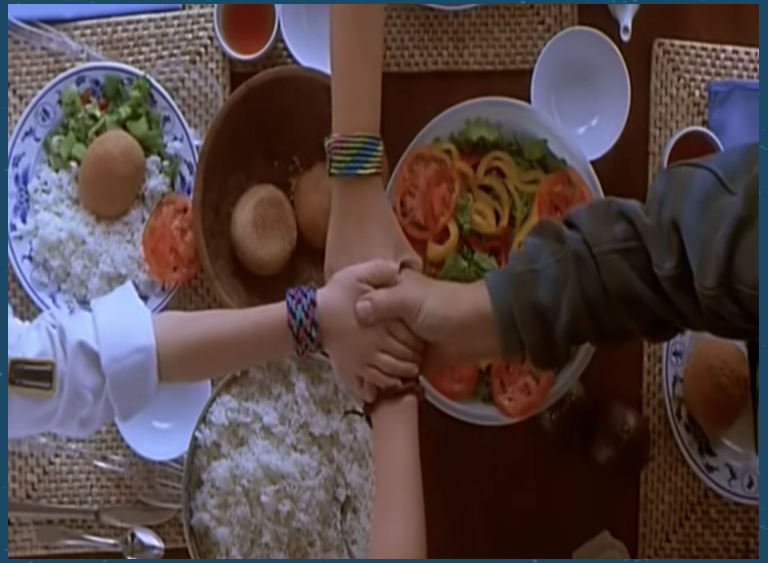
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 to 2312 bytes	4 bytes
Frame Control	Duration	MAC Address 1 (Destination)	MAC Address 2 (Source)	MAC Address 3 (Router)	Seq Control	MAC Address 4 (AP)	Data (payload)	CRC

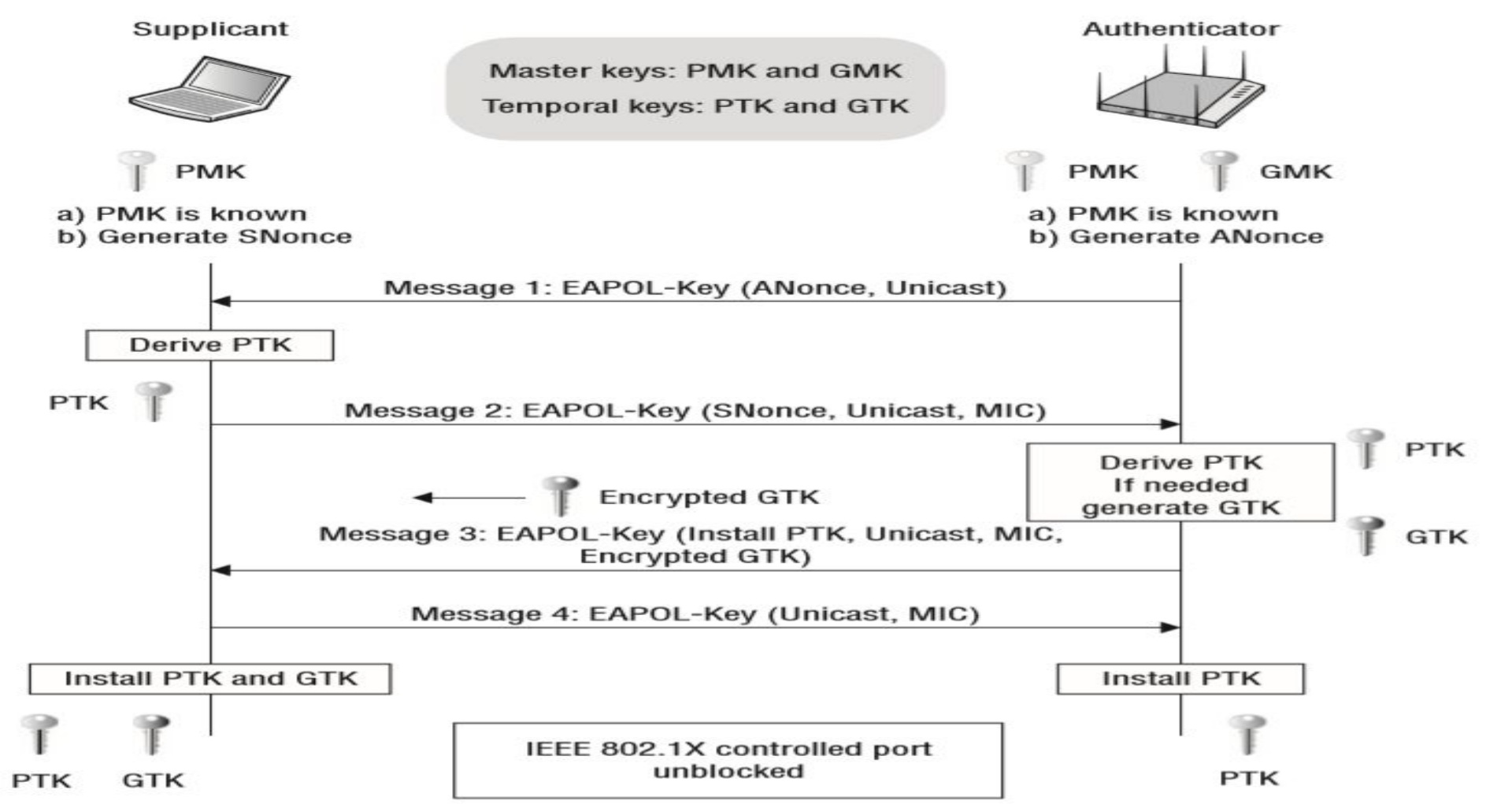
4-Way Handshake



After association, Server & Client Begin 4-Way Authentication

- Asymmetric-style encryption method
  - Both sides (router & device) generate one-time keys to authenticate messages (PTK + MIC)
  - Once authenticated, Server (router) shares public key (GTK)
  - Temporary keys are generated from Master keys stored on server (PMK & GMK)
  - Client (device) then verifies both PTK and GTK are installed and encrypted traffic sharing begins with “signed” packets.
- Keys can be stored on clients even if they’re not connected to the network at the time (Caffe Latte attack)

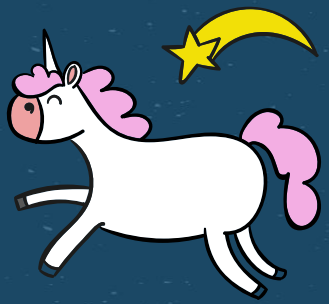


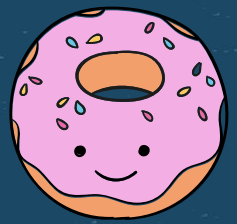

Supplicant
Authenticator
Master keys: PMK and GMK
Temporal keys: PTK and GTK
PMK
PMK
GMK
a) PMK is known
b) Generate SNonce
a) PMK is known
b) Generate ANonce
Message 1: EAPOL-Key (ANonce, Unicast)
Derive PTK
PTK
Message 2: EAPOL-Key (SNonce, Unicast, MIC)
PTK
Derive PTK
If needed
generate GTK
Encrypted GTK
GTK
Message 3: EAPOL-Key (Install PTK, Unicast, MIC,
Encrypted GTK)
Message 4: EAPOL-Key (Unicast, MIC)
Install PTK and GTK
Install PTK
PTK
GTK
IEEE 802.1X controlled port
unblocked
PTK

2

Fite-ing with the Man in the Middle

“I can feel it coming in the air tonight, Oh Lord...” - Phil Collins





WIFI is vulnerable due to its structure!

Inherent Vulnerabilities

Server-Side

Router 0 Days
Man in the Middle
Pixie Dust Attack

Key Confidentiality

PMK attack
Half-Handshake Attack

Network Packets

Packet Capture
Packet Injection

Client-Side

Deauthorization Attack
Evil Twin Attack

WIFITE

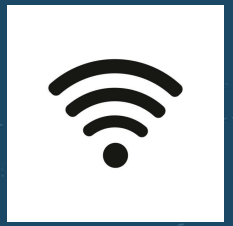
What You Need

Kali Linux

Kali comes with Wifite and many requirements built in

Wifi Adapter

No Wifi Card on VMs
Monitor Mode/Packet Injection



Tools

Hcxtools
hcxdumptools

WIFITE Progression

1. Identify/Choose Target (ranked by signal strength)
2. PMKID Attack (Server-Side Key Integrity)
3. Handshake Monitoring/Deauth Attack (Client-Side)
4. After Deauth, attempt to capture “signed” reauth packet
5. Evaluate packet capture for password hash
6. If hash found, brute force using dictionary/wordlist
    a. If full 4-way handshake, save cracked hash/exit
    b. Else, attempt half-handshake attack to verify hash









Demo

3

Pixies, Lattes, and 0 Day Unicorns

“There are very few personal problems that cannot be solved through the application of high explosives”
- Scott Adams

Evil Twin Network

Have your internet...but it's gonna cost you!

Social Engineering paired with ***WIFI attack***

- Spoof SSID trusted by victim
- Serve Internet in exchange for some action

Often paired with deauthorization attack of true SSID to "force" clients over to Evil Twin

"Some Action" could be:

- Provide attacker credentials
- Approve "Terms of Service" → Install Logic Bomb
- Download some package/file → DLL Injection, Ransomware, C2

!~WIFI ATTACKS CAN LEAD TO ENTERPRISE-LEVEL ATTACKS~!


Pixie Dust
Attack

WPS Introduced in 2006

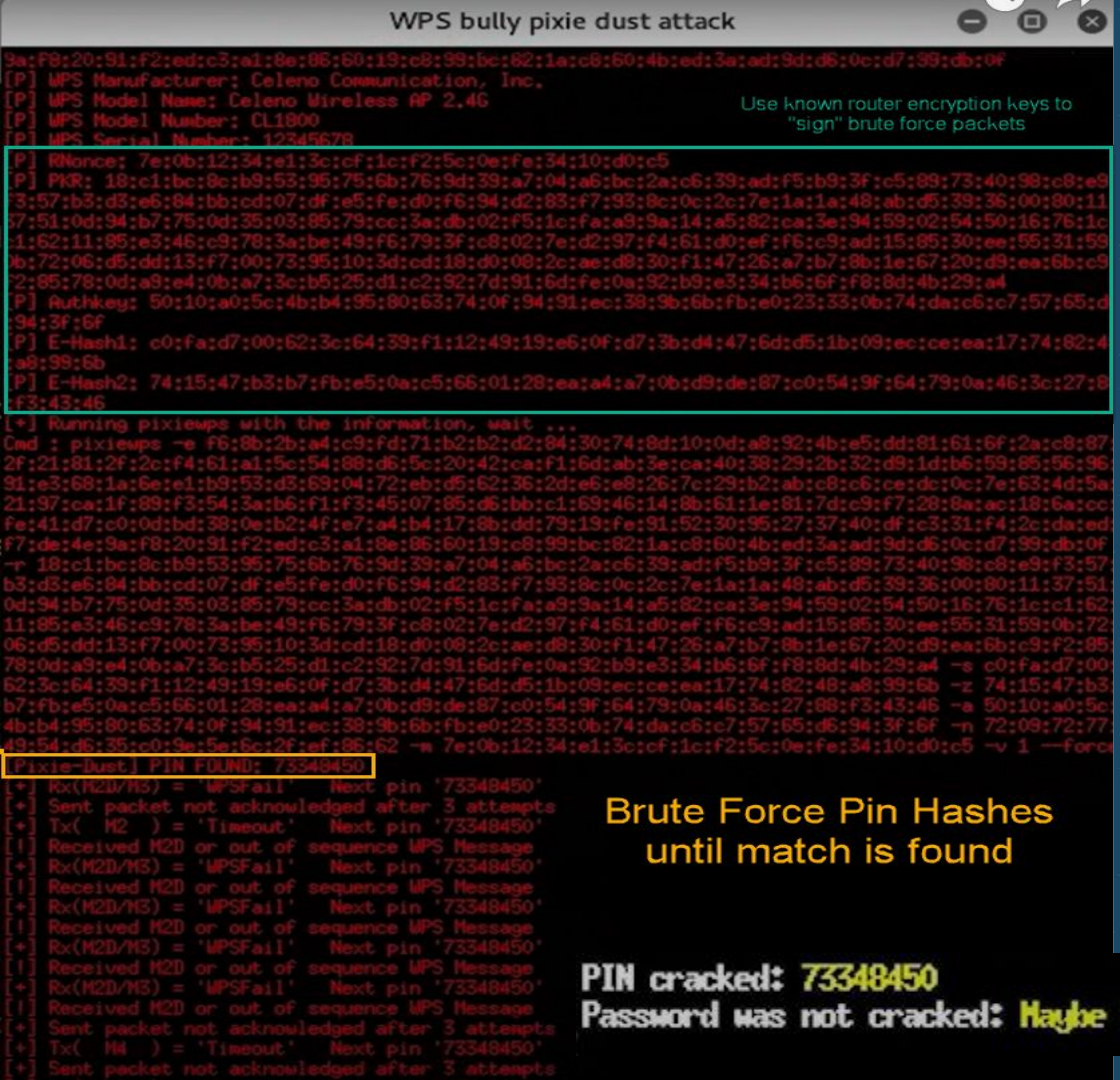
WIFI Protected Setup (WPS) allowed home users to setup home networks without remembering complex passwords

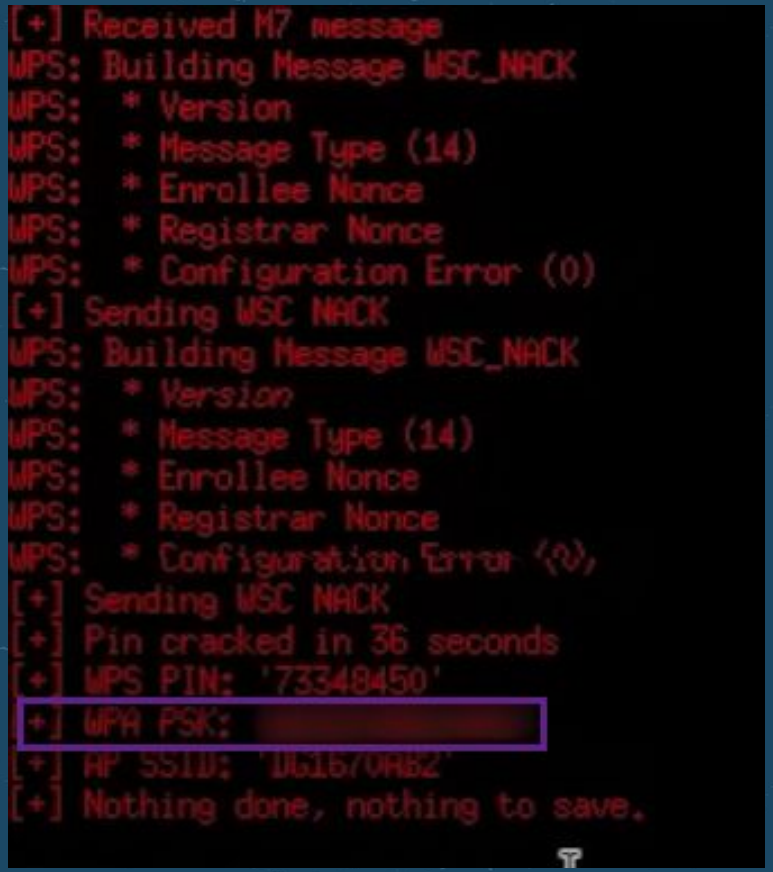
- 8 digit *standardized* PIN assigned to router
- Pixie Dusting attempts to brute force the router PIN rather than the WIFI password

Wifite has the ability to utilize two built-in programs to execute Pixie Dust attacks on vulnerable routers: *Bully* & *Reaver*

2-Step Process

- Brute Force PIN
- Use PIN to brute force WIFI Password


WPS bully pixie dust attack
[P] WPS Manufacturer: Celeno Communication, Inc.
[P] WPS Model Name: Celeno Wireless AP 2.4G
[P] WPS Model Number: CL1800
Use known router encryption keys to "sign" brute force packets
[P] RNonce: 7e:0b:12:34:e1:3c:cf:1c:f2:5c:0e:fe:34:10:d0:c5
[P] PKR: 18:c1:bc:8c:b9:53:95:75:6b:76:9d:39:a7:04:a6:bc:2a:c6:39:ad:f5:b9:3f:c5:89:73:40:98:c8:e9
[P] Authkey: 50:10:a0:5c:4b:b4:95:80:63:74:0f:94:91:ec:38:9b:6b:fb:e0:23:33:0b:74:da:c6:c7:57:65:d
[P] E-Hash1: c0:fa:d7:00:62:3c:64:39:f1:12:49:19:e6:0f:d7:3b:d4:47:6d:d5:1b:09:ec:ce:ea:17:74:82:4
[P] E-Hash2: 74:15:47:b3:b7:fb:e5:0a:c5:66:01:28:ea:a4:a7:0b:d9:de:87:c0:54:9f:64:79:0a:46:3c:27:8
[+] Running pixiewps with the information, wait ...
[Pixie-Dust] PIN FOUND: 73348450
Brute Force Pin Hashes until match is found
PIN cracked: 73348450
Password was not cracked: Maybe because bad/low signal, or PBC activated on AP



Credit Kody Kinzie, Null Byte









Cafe Latte Attack

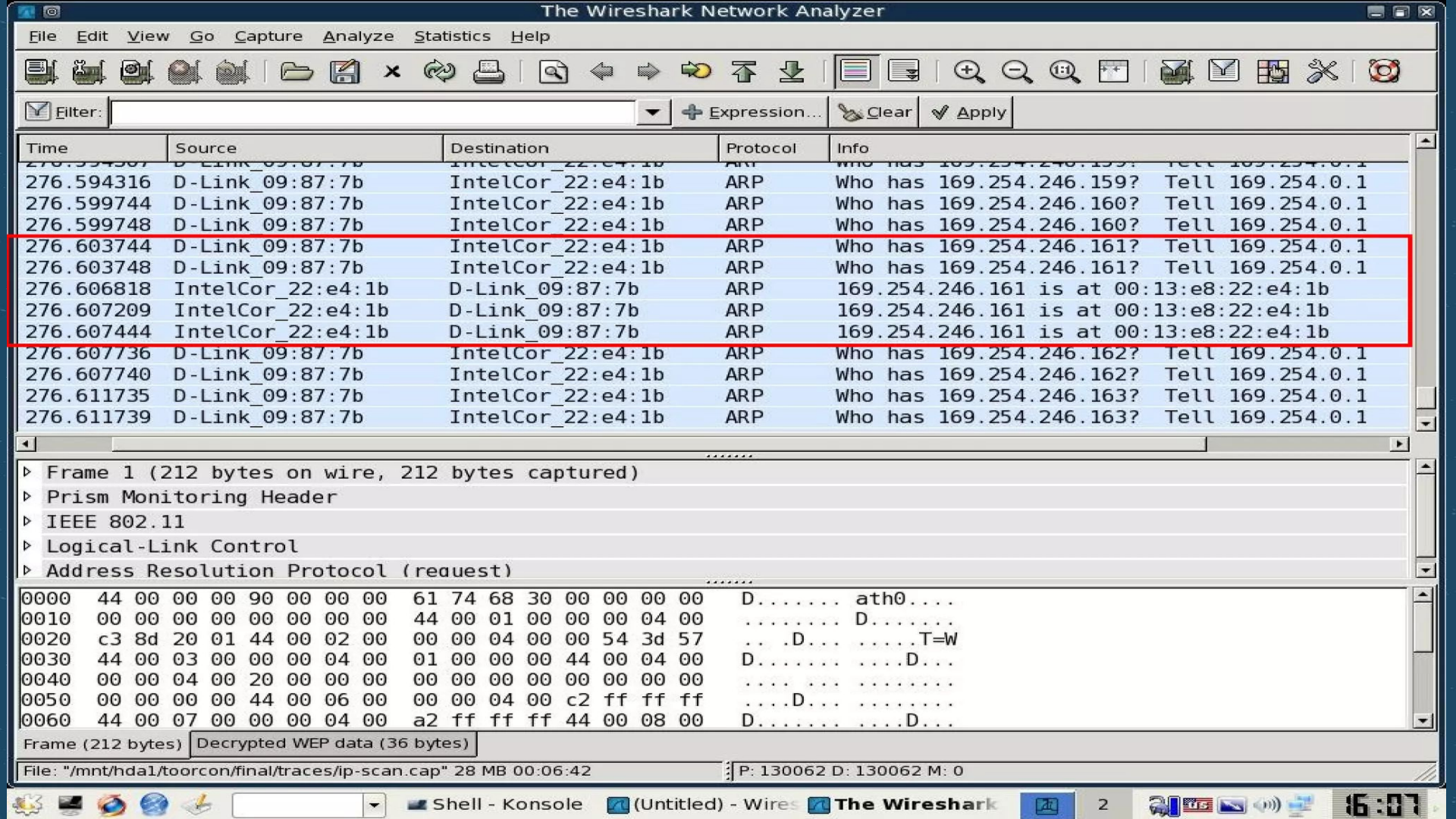
Devices are like Elephants...they don't forget!

Devices **LOVE** to associate with Networks they know! (SSID spoofing with Evil Twin Network)

Cafe Latte takes advantage of ARP packets sent between client/server after authentication (MAC/IP association) to crack WEP keys quickly

- Flip bits in captured ARP packet to send thousands of requests to client.
- Use statistical analysis to crack key from many examples of "signed" ARP packets (tens of thousands)
    - No way to determine validity of capture/replay

!~You can even do this with Wireshark~!


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
Time Source Destination Protocol Info
276.594316 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.159? Tell 169.254.0.1
276.599744 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.160? Tell 169.254.0.1
276.599748 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.160? Tell 169.254.0.1
276.603744 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
276.603748 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.161? Tell 169.254.0.1
276.606818 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
276.607209 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
276.607444 IntelCor_22:e4:1b D-Link_09:87:7b ARP 169.254.246.161 is at 00:13:e8:22:e4:1b
276.607736 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.162? Tell 169.254.0.1
276.607740 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.162? Tell 169.254.0.1
276.611735 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.163? Tell 169.254.0.1
276.611739 D-Link_09:87:7b IntelCor_22:e4:1b ARP Who has 169.254.246.163? Tell 169.254.0.1
Frame 1 (212 bytes on wire, 212 bytes captured)
Prism Monitoring Header
IEEE 802.11
Logical-Link Control
Address Resolution Protocol (request)
0000 44 00 00 00 90 00 00 00 61 74 68 30 00 00 00 00 D....... ath0....
0010 00 00 00 00 00 00 00 00 44 00 01 00 00 00 04 00 .... D.......
0020 c3 8d 20 01 44 00 02 00 00 00 04 00 00 54 3d 57 .. .D... .....T=W
0030 44 00 03 00 00 00 04 00 01 00 00 00 44 00 04 00 D....... ....D...
0040 00 00 04 00 20 00 00 00 00 00 00 00 00 00 00 00 ....
0050 00 00 00 00 44 00 06 00 00 00 04 00 c2 ff ff ff ....D... ....
0060 44 00 07 00 00 00 04 00 a2 ff ff ff 44 00 08 00 D....... ....D...
Frame (212 bytes)
Decrypted WEP data (36 bytes)
File: "/mnt/hda1/toorcon/final/traces/ip-scan.cap" 28 MB 00:06:42
P: 130062 D: 130062 M: 0
Shell - Konsole
(Untitled) - Wires
The Wireshark
2
16:07

4

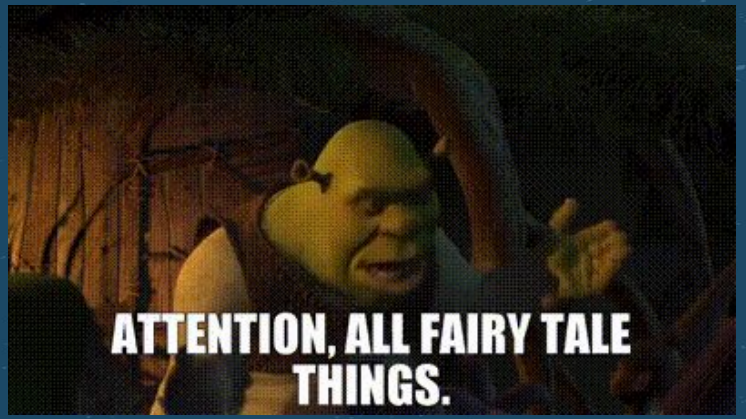
Lord Farquaad-ing

“We need to stop treating MITRE ATT&CK like a Bingo card!” - Bryson Bort, SCYTHE

Protection & Remediation

Here are some strategies to protect yourself and your WIFI devices:

1. **STRONG PASSWORDS**
2. Utilize segmented networks at home
3. Utilize latest encryption levels on routers
4. Utilize strong firewalls with MAC Address filtering
5. Do **NOT** connect to networks you do not trust!
6. Update Routers when appropriate











Questions?