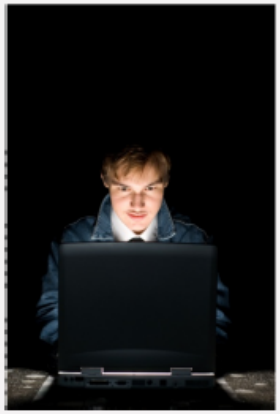
Hacking Wireless Networks

Module 15

Engineered by Hackers. Presented by Professionals.

SECURITY NEWS



October 17th 2010, Chicago, Illinois

seek4media

50% of all Wi-Fi networks capable of being hacked in 5 seconds

A study conducted recently has found that nearly 50 percent of Wi-Fi networks could be hacked. The study conducted in six cities and derived that out of 40,000 Wi-Fi network nearly 20,000 did not have passwords assigned to them.

It is estimated that nearly 82 percent of the people thought their network was secure, though the harsh reality is that nearly 25 percent of the private networks had no password. What has made the study scarier is that hackers were able to hack through secure networks.

Hackers like Jason Hart believe that today it is easy for hackers to get into another user's system and access their information, emails and social sites apart from online banking. They could also create a social identity of their own.

http://www.seek4media.com

SECURITY NEWS

October 22, 2010

SLASHGEAR
The Morning Wrap-Up
Get caught up on the news

Google Street View Car Cameras Grab Emails & Passwords

Google collected e-mails, passwords, and URLs while the company was snapping images for its Street View service, it admitted in a blog.

"In some instances, entire e-mails and URLs were captured, as well as passwords," Google's senior vice president of engineering and research, Alan Eustace, wrote in a blog post

Eustace said that "**most of the data is fragmentary**," and the company will delete the information "as soon as possible."

This collection of data, Google states, happened while **mistakingly running a piece of code from an experimental project** which ran alongside a program Google intended on using to amass data on **WiFi hotspots** to provide location-based services.

Eustace said that Google had not "**analyzed in detail the mistakenly collected data**, so they did not know for sure what the disks contained."

The company said that its director of privacy, Alma Whitten, will help "build effective privacy controls" into Google products and practices.

http://www.slashgear.com

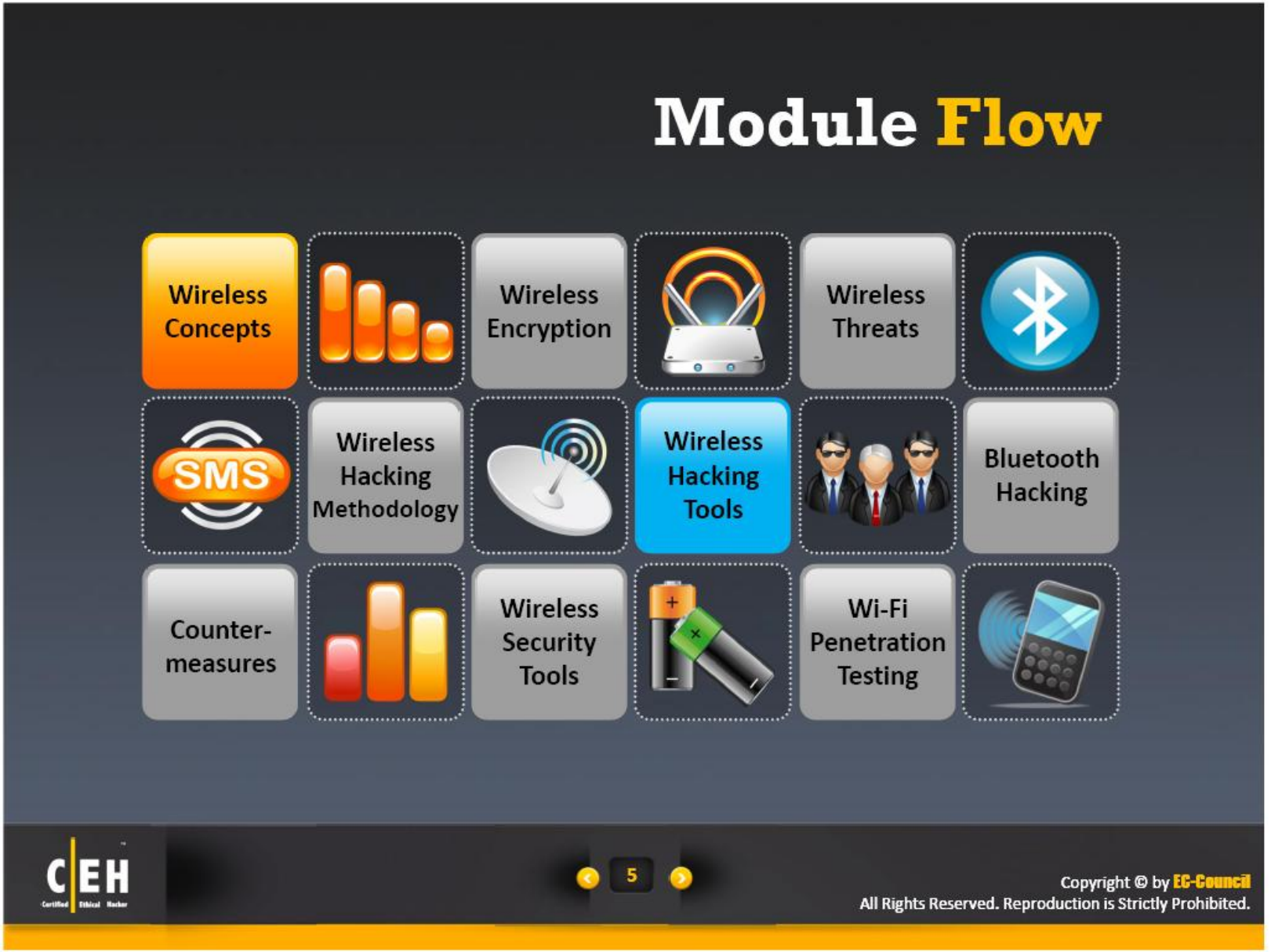
Module Objectives

- Wireless Networks
- Types of Wireless Networks
- Wi-Fi Authentication Modes
- Types of Wireless Encryption
- WEP Encryption
- What is WPA/WPA2?
- Wireless Threats

- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- How to Defend Against Bluetooth Hacking?
- How to Defend against Wireless Attacks?
- Wi-Fi Security Tools
- Wireless Penetration Testing Framework



Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
C|EH
5
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Networks

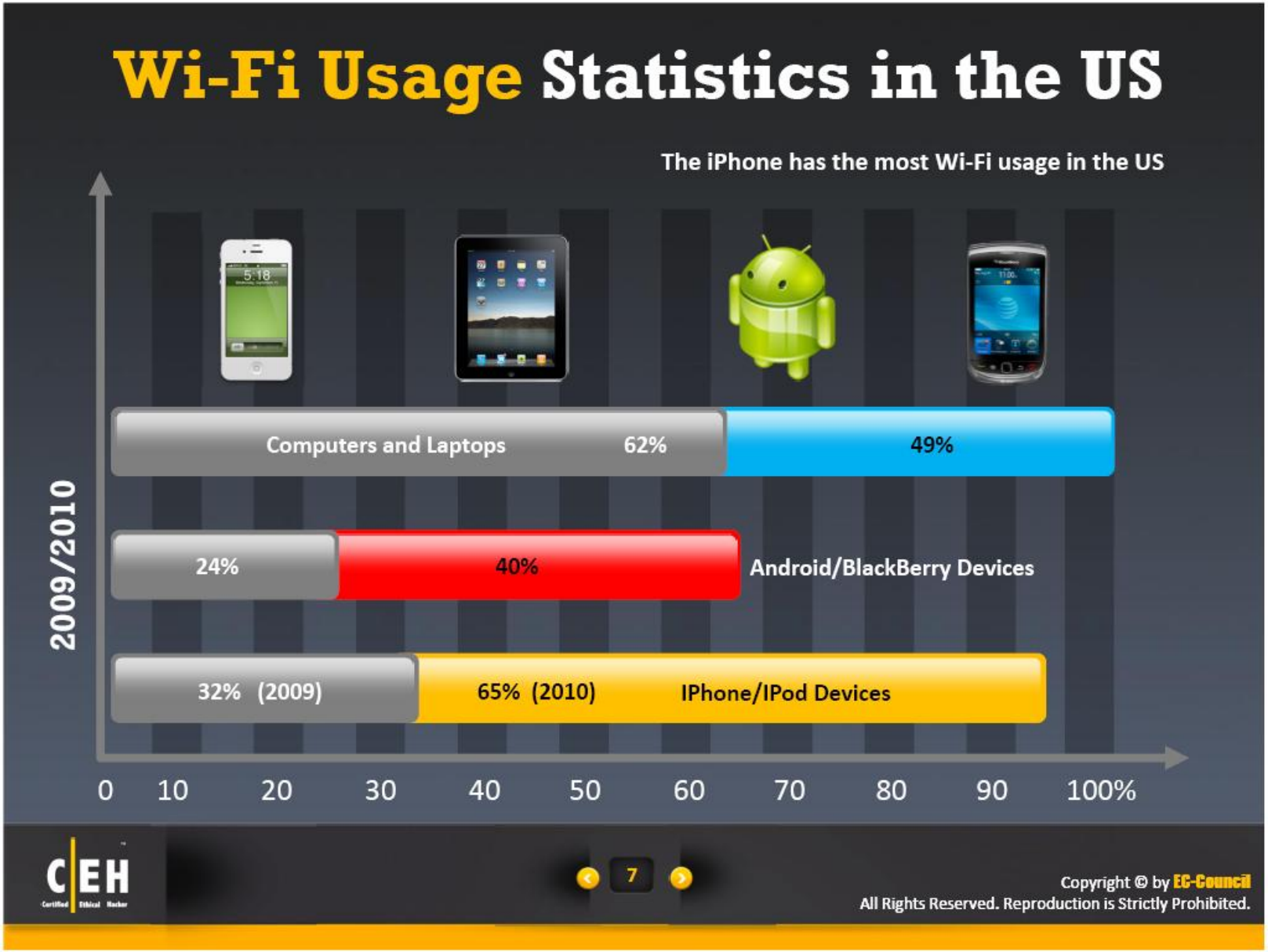
- Wi-Fi is developed on **IEEE 802.11 standards**, and it is widely used in wireless communication. It provides **wireless access** to applications and data across a radio network.
- Wi-Fi sets up numerous ways to build up a connection between the **transmitter** and the **receiver** such as DSSS, FHSS, Infrared (IR) and OFDM.

Advantages

- Installation is fast and easy and eliminates wiring through walls and ceilings
- It is easier to provide connectivity in areas where it is difficult to lay cable
- Access to the network can be from anywhere within range of an access point
- Public places like airports, libraries, schools or even coffee shops offer you constant Internet connection using Wireless LAN

Disadvantages

- Security is a big issue and may not meet expectations
- As the number of computers on the network increases, the bandwidth suffers
- Wi-Fi standards changed which results in replacing wireless cards and/or access points
- Some electronic equipment can interfere with the Wi-Fi networks


Wi-Fi Usage Statistics in the US
The iPhone has the most Wi-Fi usage in the US
2009/2010
Computers and Laptops
62%
49%
24%
40%
Android/BlackBerry Devices
32% (2009)
65% (2010)
IPhone/IPod Devices
0
10
20
30
40
50
60
70
80
90
100%
CEH
7
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

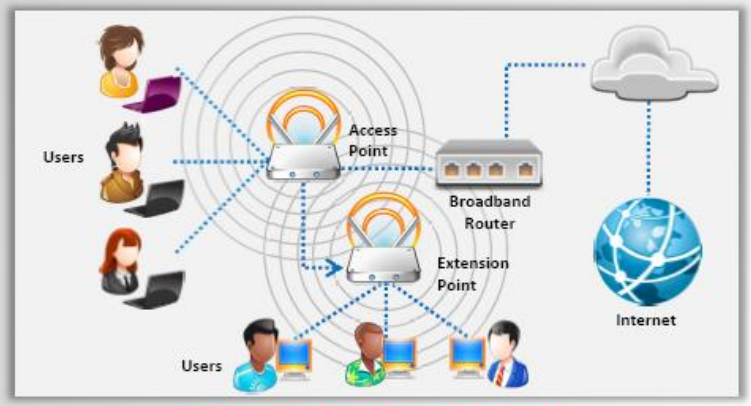
Wi-Fi Hotspots at Public Places

You will find free Wi-Fi access available in coffee shops like bookstores, offices, airport terminals, schools, hotels, communities, and other public places

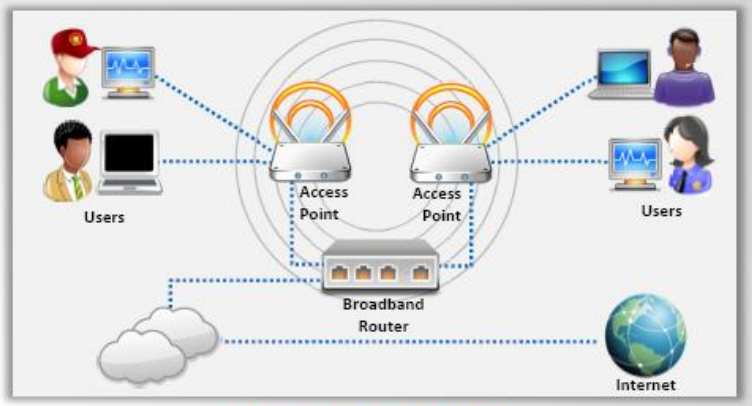
Wi-Fi Networks at Home

Wi-Fi networks at home allow you to be wherever you want with laptop, iPad, or handheld device, and not have to make holes for hide Ethernet cables

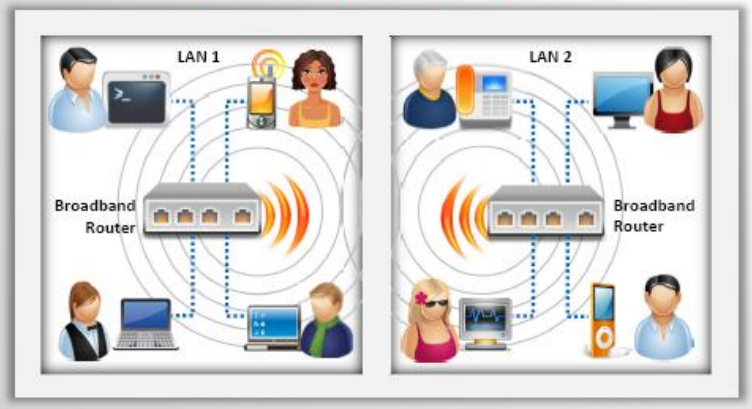
Types of Wireless Networks



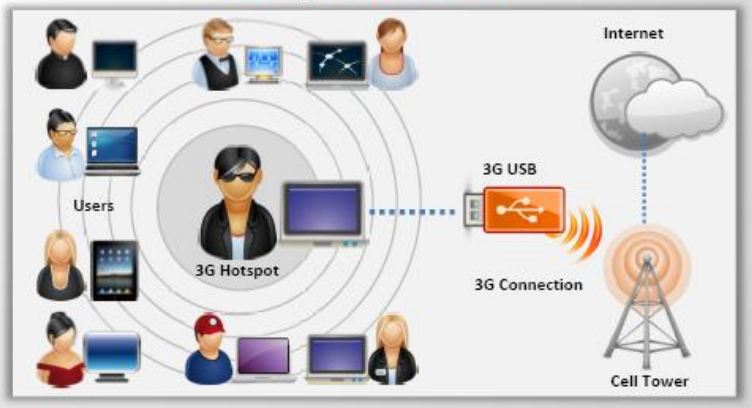
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network

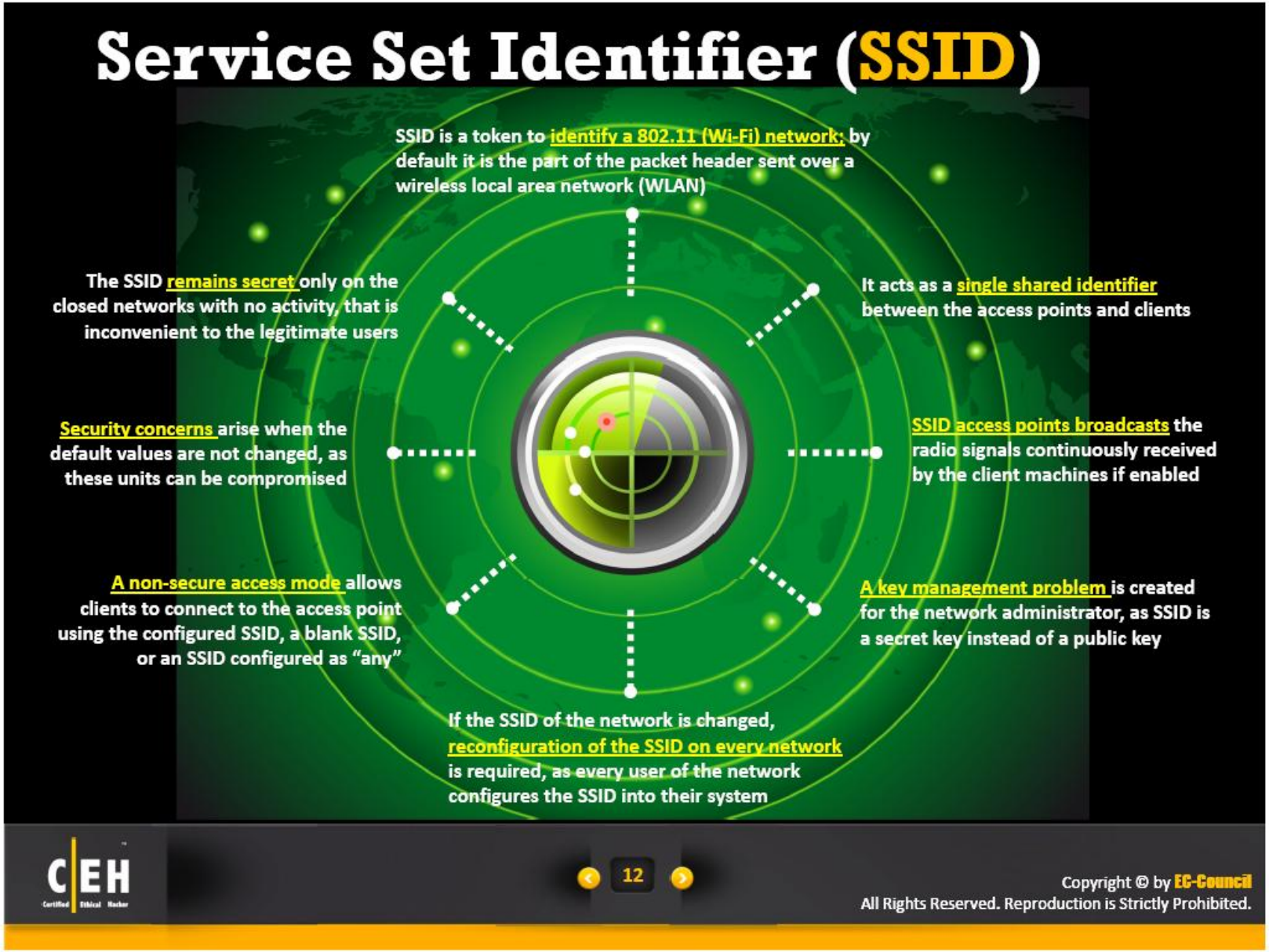


3G Hotspot

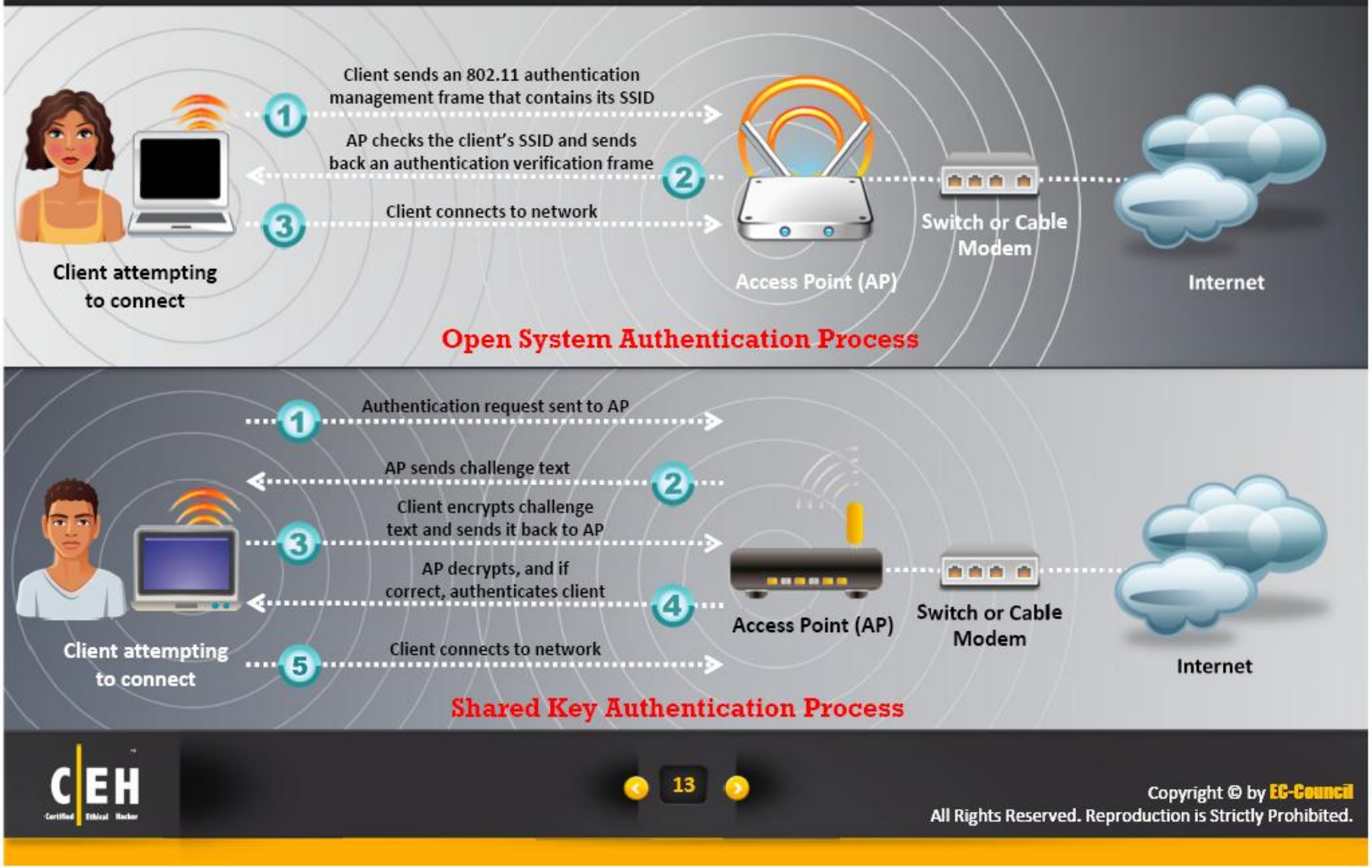
Wireless Standards

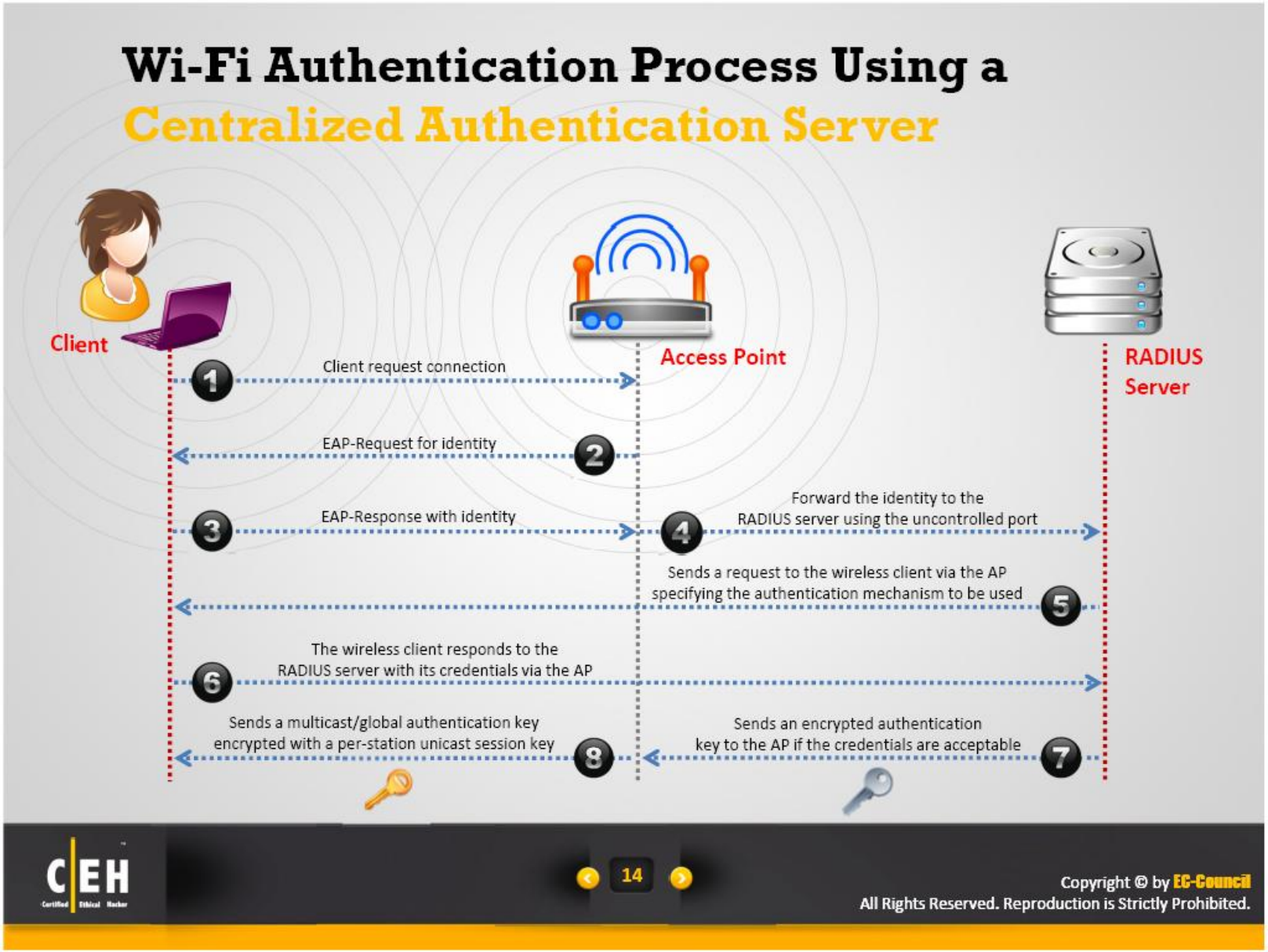
802.11a	Bandwidth up to **54 Mbps** and signals in a regulated frequency spectrum around 5 GHz
802.11b	Bandwidth up to **11 Mbps**, and uses the unregulated radio signaling frequency (2.4 GHz)
802.11g	Bandwidth up to **54 Mbps**, and it uses the 2.4 GHz frequency for greater range
802.11i	A standard for Wireless Local Area Networks (WLANs) that provides **improved encryption** for networks that use 802.11a, 802.11b and 802.11g standards
802.11n	Uses multiple input, multiple output (MIMO) technology to give Wi-Fi more speed (**over 100Mbps**) and range
802.16	A group of broadband wireless communications standards for **Metropolitan Area Networks (MANs)**
Bluetooth	Supports a very short range (~10 meters) and relatively low bandwidth (1-3 Mbps) **designed for low-power network devices** like handhelds

Service Set Identifier (SSID)

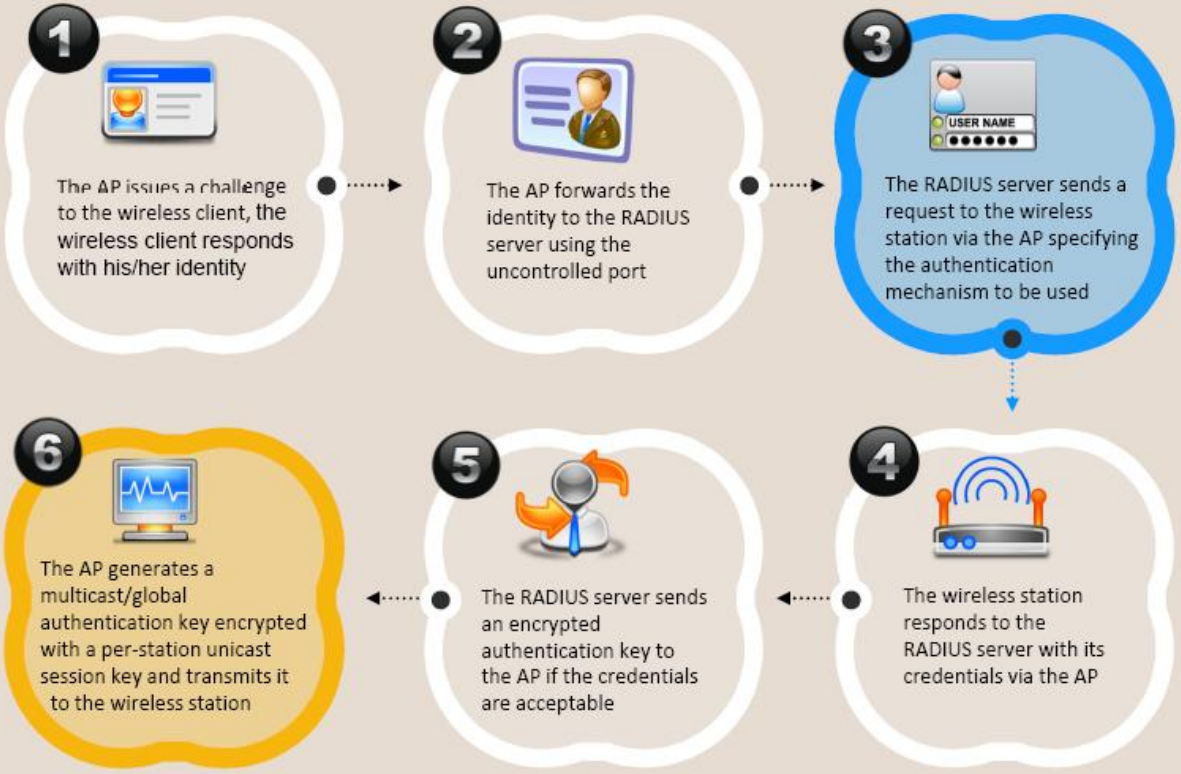


Wi-Fi Authentication Modes




Wi-Fi Authentication Process Using a
Centralized Authentication Server
Client
Access Point
RADIUS Server
1
Client request connection
2
EAP-Request for identity
3
EAP-Response with identity
4
Forward the identity to the RADIUS server using the uncontrolled port
5
Sends a request to the wireless client via the AP specifying the authentication mechanism to be used
6
The wireless client responds to the RADIUS server with its credentials via the AP
7
Sends an encrypted authentication key to the AP if the credentials are acceptable
8
Sends a multicast/global authentication key encrypted with a per-station unicast session key
CEH
14
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Authentication Process



Wireless Terminologies

GSM
Universal system used for mobile transportation for wireless network worldwide

Antenna-Directional
Used to broadcast and obtain radio waves from a single direction

Antenna-Omni-directional
Used to broadcast and obtain radio waves from all sides

WiFi Finder
Device used to find a Wi-Fi network

Association
The process of connecting a wireless device to an access point

Authentication
Process of identifying a device prior to allowing access to network resources

BSSID
The MAC address of an access point that has set up a Basic Service Set (BSS)

Wi-Fi Protected Access (WPA)
It is an advanced WLAN clients authenticating and data encryption protocol using TKIP, MIC, and AES encryption

Gigahertz
Frequency represent as billion of cycle per second

Hotspot
Places where wireless network is available for public use

Access Point
Used to connect wireless devices to a wireless network

ISM band
A range of radio frequencies that are assigned for use by unlicensed users

Bandwidth
Describes the amount of information that may be broadcasted over a connection

Wired Equivalent Privacy (WEP)
It is a WLAN clients authenticating and data encryption protocol


WarWalking
Attackers walk around with Wi-Fi enabled laptops to detect open wireless networks
WarChalking
A method used to draw symbols in public places to advertise open Wi-Fi networks
Wi-Fi Chalking
WarFlying
In this technique, attackers fly around with Wi-Fi enabled laptops to detect open wireless networks
WarDriving
Attackers drive around with Wi-Fi enabled laptops to detect open wireless networks
CEH
17
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Chalking Symbols

Free Wi-Fi

Wi-Fi with MAC filtering

Restricted Wi-Fi

Pay for Wi-Fi

Wi-Fi with WPA

Wi-Fi with multiple access controls

Wi-Fi with closed SSID

Wi-Fi Honeypot

CEH Certified Ethical Hacker

18

Wi-Fi Hotspot Finder: jiwire.com

JiWire is a Wi-Fi hotspot location directory with more than 338,271 free and paid Wi-Fi hotspots in 144 countries.

http://v4.jiwire.com

Wi-Fi Hotspot Finder: WeFi.com

Types of Wireless Antenna

Omnidirectional Antenna

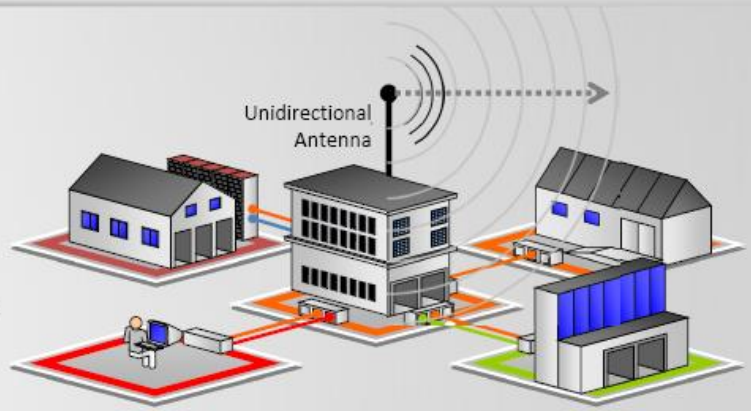
Omnidirectional antennas provide a 360 degree horizontal radiation pattern

It is used in wireless base stations

Parabolic Grid Antenna

It is based on the principle of a satellite dish but it does not have a solid backing

They can pick up Wi-Fi signals ten miles or more



Yagi Antenna

Yagi is a unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF

Dipole Antenna

Bidirectional antenna, used to support client connections rather than site-to-site applications

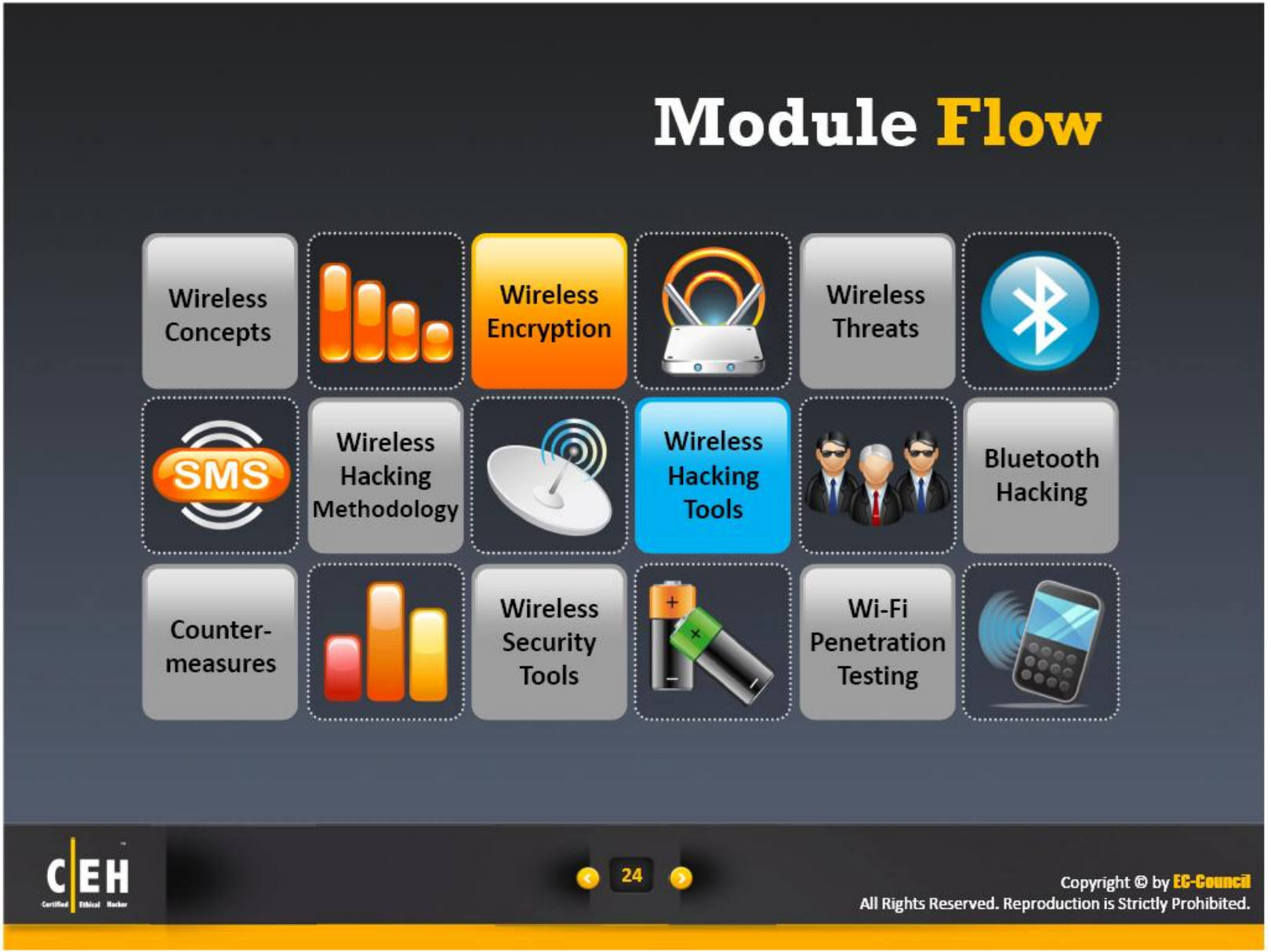
Parabolic Grid Antenna

Parabolic grid antennas enables attackers to get better signal quality resulting in more data to eavesdrop on, more bandwidth to abuse and higher power output that is essential in Layer 1 DoS and man-in-the-middle attacks

Grid parabolic antennas can pick up Wi-Fi signals from a distance of ten miles

SSID	Channel	Encryption	Authentication	Signal
Apple	2	None	Unknown	24%
My Wi-Fi	5	WEP	Unknown	40%
GSM	1	WEP	Unknown	64%
Wi-Fi Planet	6	None	Unknown	38%
Awslocal	8	None	Unknown	54%

Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
CEH
Certified Ethical Hacker
24
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Encryption

WEP

It is an old and original wireless security standard which can be cracked easily

WPA

Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security

WPA2

WPA2 uses AES (128 bit) and CCMP for wireless data encryption

WPA2 Enterprise

It integrates EAP standards with WPA encryption

TKIP

A security protocol used in WPA as a replacement for WEP

AES

It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP

EAP

Uses multiple authentication methods, such as token cards, Kerberos, certificates etc.

LEAP

It is a proprietary WLAN authentication protocol developed by Cisco

RADIUS

It is a centralized authentication and authorization management system

802.11i

It is an IEEE standard that specifies security mechanisms for 802.11 wireless networks

CCMP

CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection

WEP Encryption

What is WEP?

- **Wired Equivalent Privacy** (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions
- WEP uses **24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission

64-bit WEP uses a 40-bit key

128-bit WEP uses a 104-bit key size

256-bit WEP uses 232-bit key size

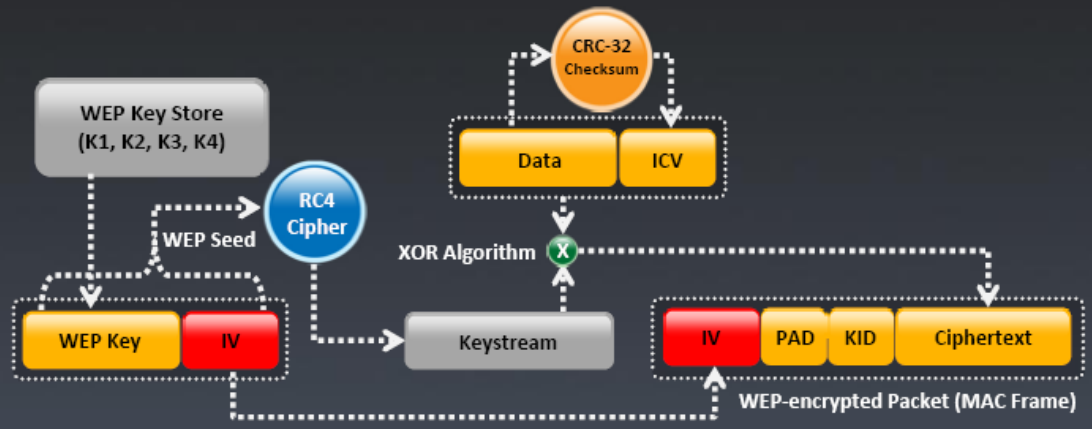
WEP Flaws

It was developed without:

- Academic or public review
- Review from cryptologists

- It has significant vulnerabilities and design flaws

How WEP Works?



1. A 32-bit Integrity Check Value (ICV) is calculated for the frame data
2. The ICV is appended to the end of the frame data
3. A 24-bit Initialization Vector (IV) is generated and appended to the WEP encryption key
4. The combination of IV and the WEP key is used as the input to RC4 algorithm to generate a key stream
5. The key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data
6. The IV is added to the encrypted data and ICV to generate a MAC frame

What is WPA?

- Wi-Fi Protected Access (WPA) is a **data encryption method** for WLANs based on 802.11 standards
- It **improves** on the authentication and encryption features of WEP (Wired Equivalent Privacy)

TKIP (Temporal Key Integrity Protocol)

- TKIP utilizes the RC4 stream cipher encryption with **128-bit** keys and 64-bit keys for authentication
- TKIP mitigates the WEP key derivation vulnerability by not reusing the same **Initialization Vector**

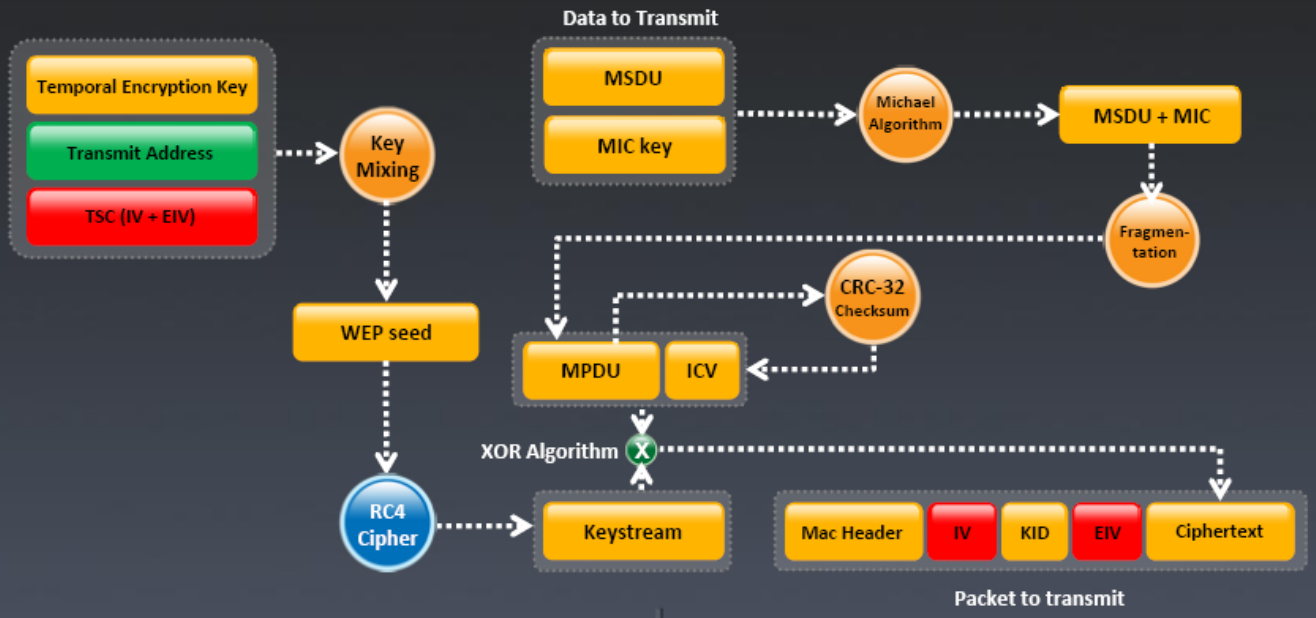
128-bit Temporal Key

- Under TKIP, the client starts with a 128-bit "temporal key" (TK) that is then **combined with the client's MAC address** and with an IV to create a key that is used to encrypt data via the RC4
- It implements a sequence counter to protect against **replay attacks**

WPA Enhances WEP

- TKIP enhances WEP by adding a **rekeying mechanism** to provide fresh encryption and integrity keys
- Temporal keys are changed for every **10,000 packets**. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse

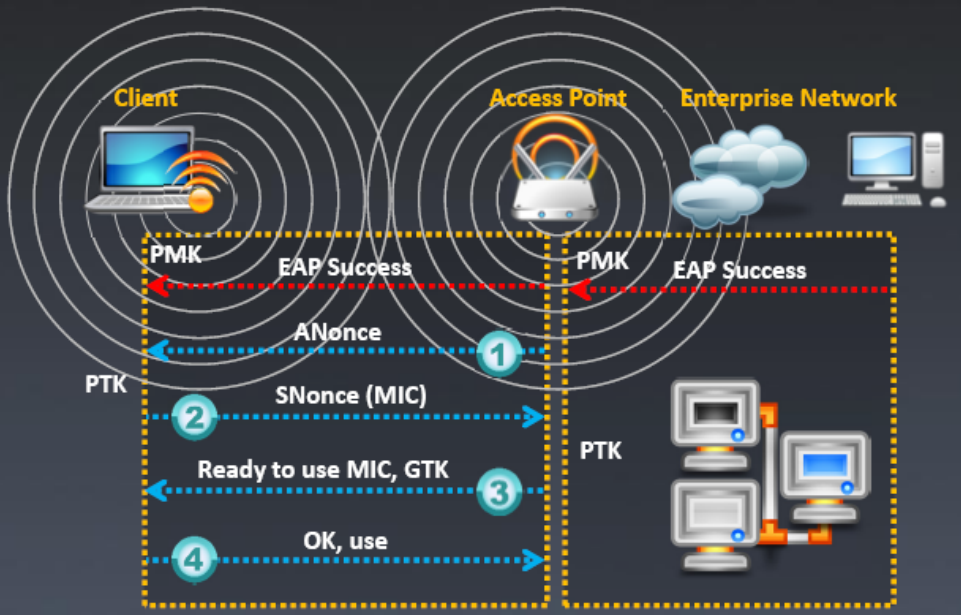
How WPA Works?



1. Temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as input to **RC4 algorithm** to generate a **Keystream**
2. MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using **Michael algorithm**
3. The combination of MSDU and MIC is fragmented to generate **MAC Protocol Data Unit (MPDU)**
4. A **32-bit Integrity Check Value (ICV)** is calculated for the MPDU
5. The combination of MPDU and ICV is bitwise **XORed with Keystream** to produce the encrypted data
6. The **IV** is added to the encrypted data to generate **MAC frame**

Temporal Keys

- In WPA and WPA2, the encryption keys (temporal keys) are derived during the **four-way handshake**
- Encryption keys are derived from the PMK that is derived during the **EAP authentication session**
- In the EAP success message, PMK is sent to the AP but is not directed to the Wi-Fi client as it has derived its own copy of the PMK

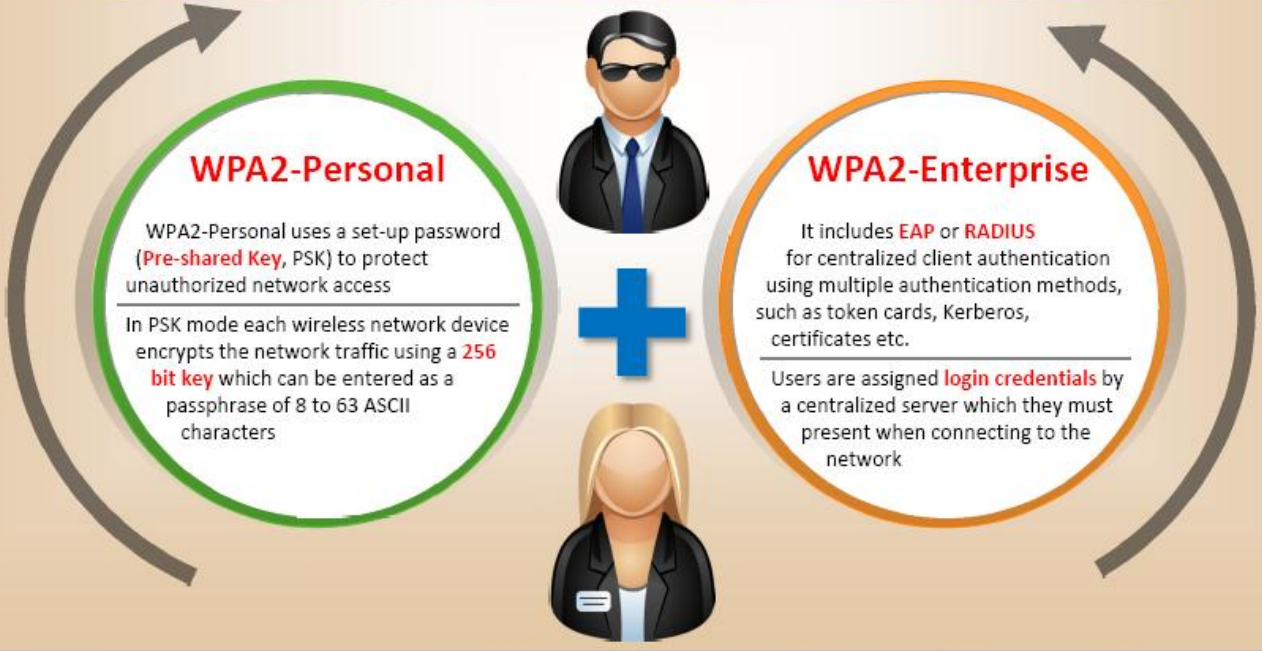


1. AP sends an ANonce to client which uses it to construct the **Pairwise Transient Key (PTK)**
2. Client respond with its own nonce-value (SNonce) to the AP together with a **Message Integrity Code (MIC)**
3. AP sends the **GTK and a sequence number** together with another MIC which is used in the next broadcast frames
4. Client confirm that the temporal keys are installed

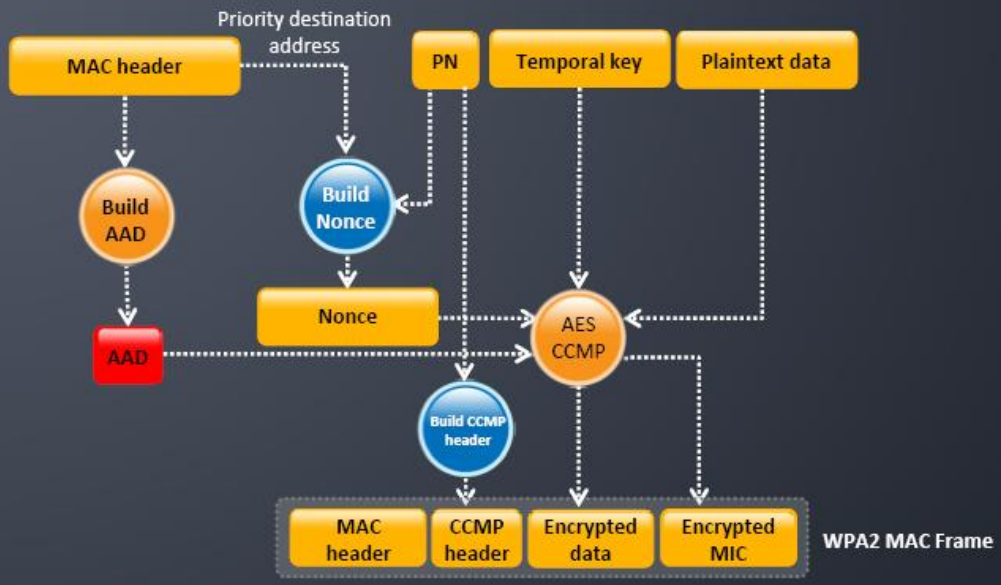
What is WPA2?

WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control

Provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm



How WPA2 Works?



In the CCMP procedure, **additional authentication data (AAD)** is taken from the MAC header and included in the **CCM encryption** process. This protects the frame against alteration of the non-encrypted portions of the frame

A **sequenced packet number (PN)** is included in the CCMP header to protect against replay attacks. The PN and portions of the MAC header are used to generate a nonce that in turn is used by the CCM encryption process

WEP vs. WPA vs. WPA2

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	AES-CCMP

WEP 	Should be replaced with more secure WPA and WPA2
WPA, WPA2 	Incorporates protection against forgery and replay attacks

WEP Issues

The IV is a 24-bit field is too small and is sent in the **cleartext** portion of a message

Identical key streams are produced with the reuse of the same IP for data protection, as the IV is short key streams are repeated within short time

Lack of centralized key management makes it difficult to change the WEP keys with any regularity

When there is IV Collision, it becomes possible to **reconstruct the RC4 keystream** based on the IV and the decrypted payload of the packet

IV is a part of the RC4 encryption key, leads to a **analytical attack** that recovers the key after intercepting and analyzing a relatively small amount of traffic

Use of RC4 was designed to be a **one-time cipher** and not intended for multiple message use

No defined method for **encryption key distribution**

Wireless adapters from the same vendor may all **generate the same IV sequence**. This enables attackers to determine the key stream and decrypt the ciphertext

Associate and disassociate messages are **not authenticated**

WEP does not provide cryptographic integrity protection. By capturing two packets an attacker can flip a bit in the encrypted stream and **modify the checksum** so that the packet is accepted

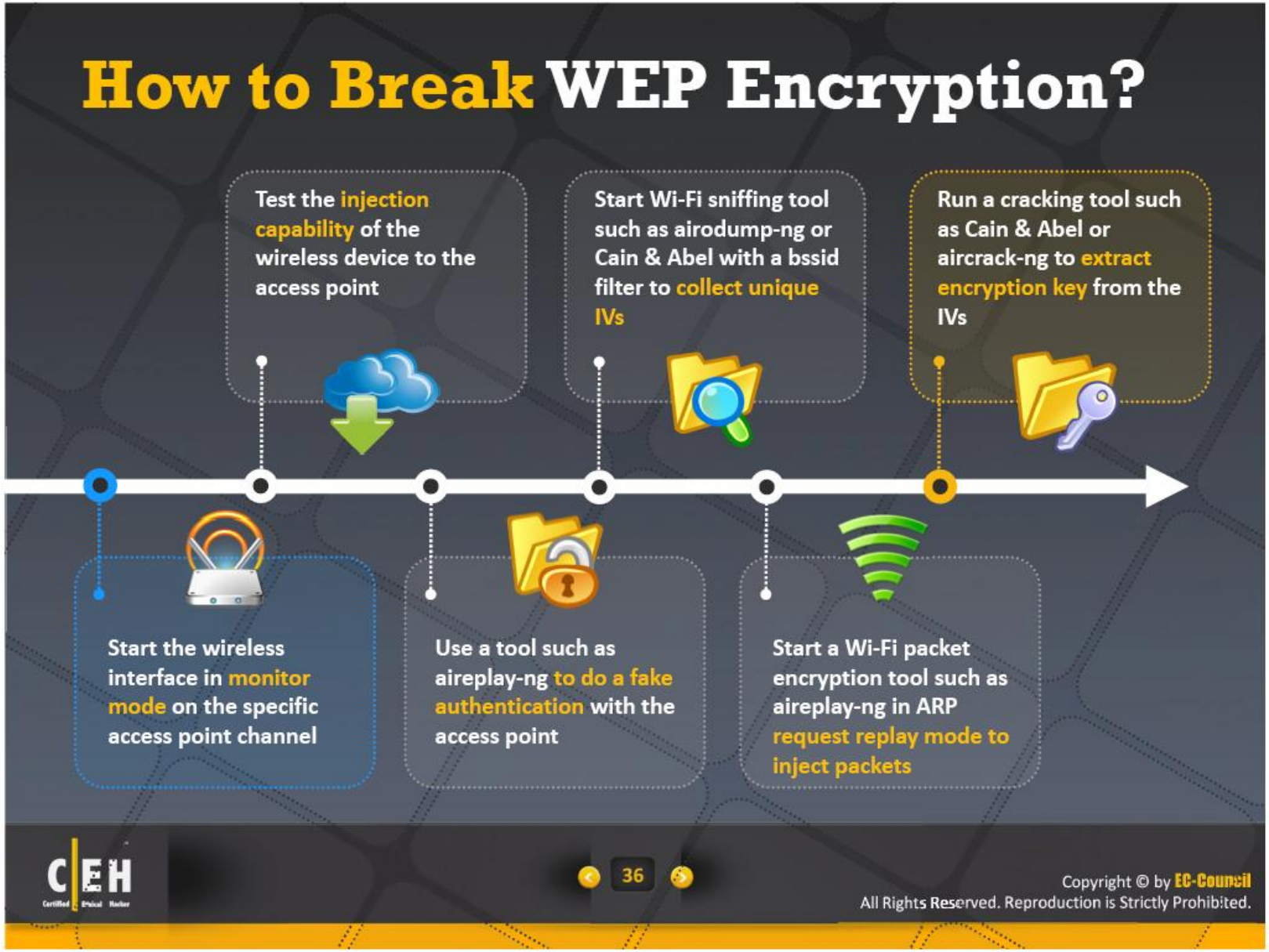
WEP is based on a password, prone to **password cracking attacks**

An attacker can construct a decryption table of the **reconstructed key stream** and can use it to decrypt the WEP Packets in real-time

Weak Initialization Vectors (IV)

In the RC4 algorithm, the Key Scheduling Algorithm (KSA) creates an IV based on the base key	The IV value is too short and not protected from reuse and no protection again message replay
A flaw in the WEP implementation of RC4 allows "weak" IVs to be generated	The way keys are constructed from the IV makes it susceptible to weak key attacks (9FMS attack)
Those weak IVs reveal information about the key bytes they were derived from	No effective detection of message tampering (message integrity)
An attacker will collect enough weak IVs to reveal bytes of the base key	It directly uses the master key and has no built-in provision to update the keys

How to Break WEP Encryption?



How to Break WPA/WPA2 Encryption?

WPA PSK

WPA PSK uses a user defined password to initialize the TKIP, which is not crackable as it is a per-packet key but the keys can be brute-forced using dictionary attacks

Offline Attack

You only have to be near the AP for a matter of seconds in order to capture the WPA/WPA2 authentication handshake, by capturing the right type of packets, you can crack WPA keys offline

Brute-Force WPA Keys

You can use tools such as aircrack, aireplay, KisMac to brute-force WPA Keys

De-authentication Attack

Force the connected client to disconnect, then capture the re-connect and authentication packet using tools such as airplay, you should be able to re-authenticate in a few seconds then attempt to Dictionary Brute Force the PMK

How to Defend Against WPA Cracking?

Passphrases

- The only way to crack WPA is to sniff the **password PMK** associated with the "handshake" authentication process, and if this password is extremely complicated, it will be **almost impossible to crack**

Passphrase Complexity

- Select a **random passphrase** that is not made up of dictionary words
- Select a complex passphrase of a **minimum of 20 characters** in length and change it at regular intervals

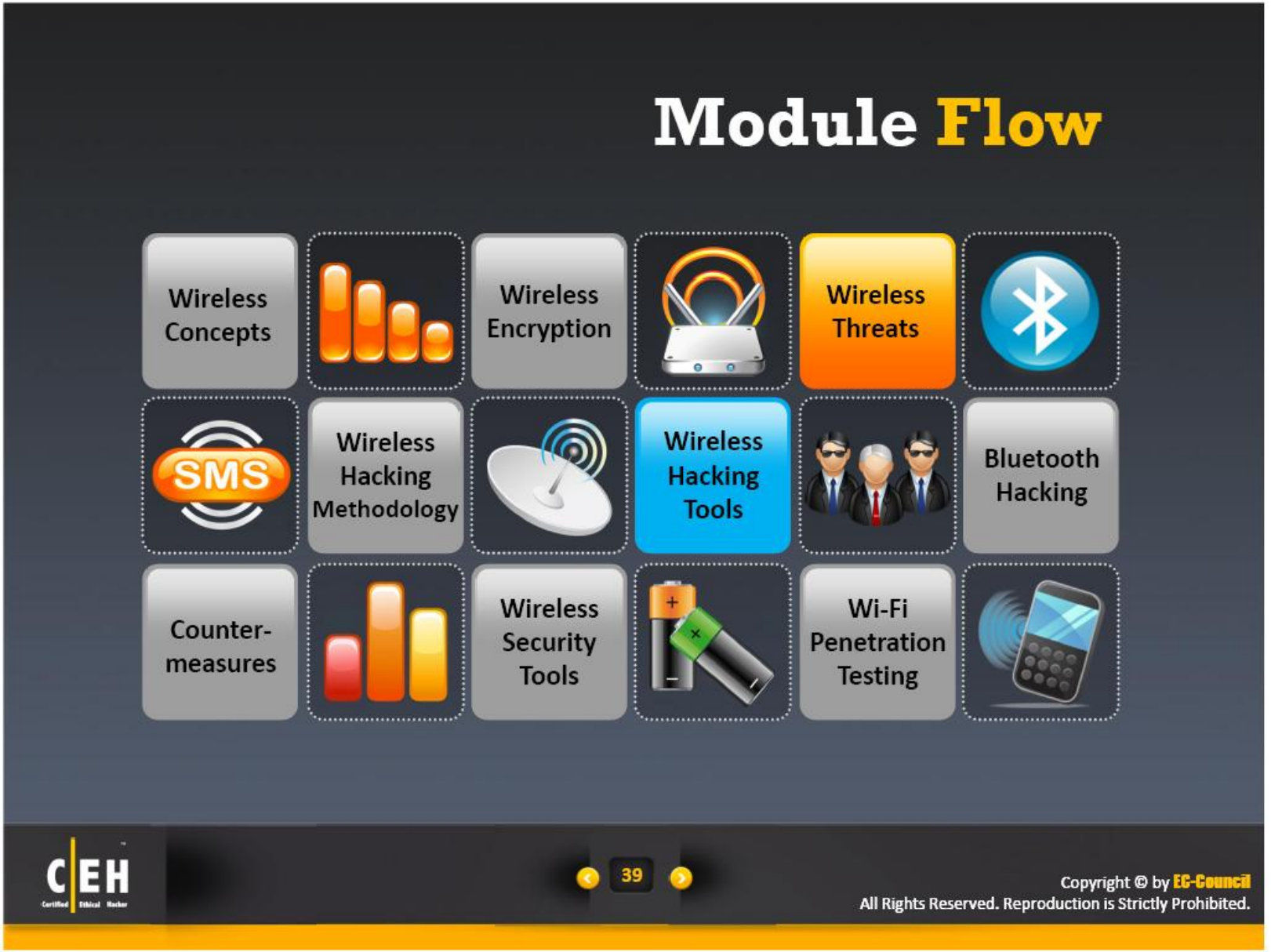
Client Settings

- Use WPA2 with **AES/CCMP encryption** only
- Properly set the client settings (e.g. validate the server, specify **server address**, don't prompt for new servers, etc.)

Additional Controls

- Use **virtual-private-network** (VPN) technology such as Remote Access VPN, Extranet VPN, Intranet VPN, etc.
- Implement a **Network Access Control** (NAC) or **Network Access Protection** (NAP) solution for additional control over end-user connectivity

Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
CEH
39
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Threats: Access Control Attacks

Wireless access control attacks aims to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls

War Driving

Rogue Access Points

MAC Spoofing

Ad Hoc Associations

AP Miscon-figuration

Client Mis-association

Unauthorized Association

Promiscuous Client

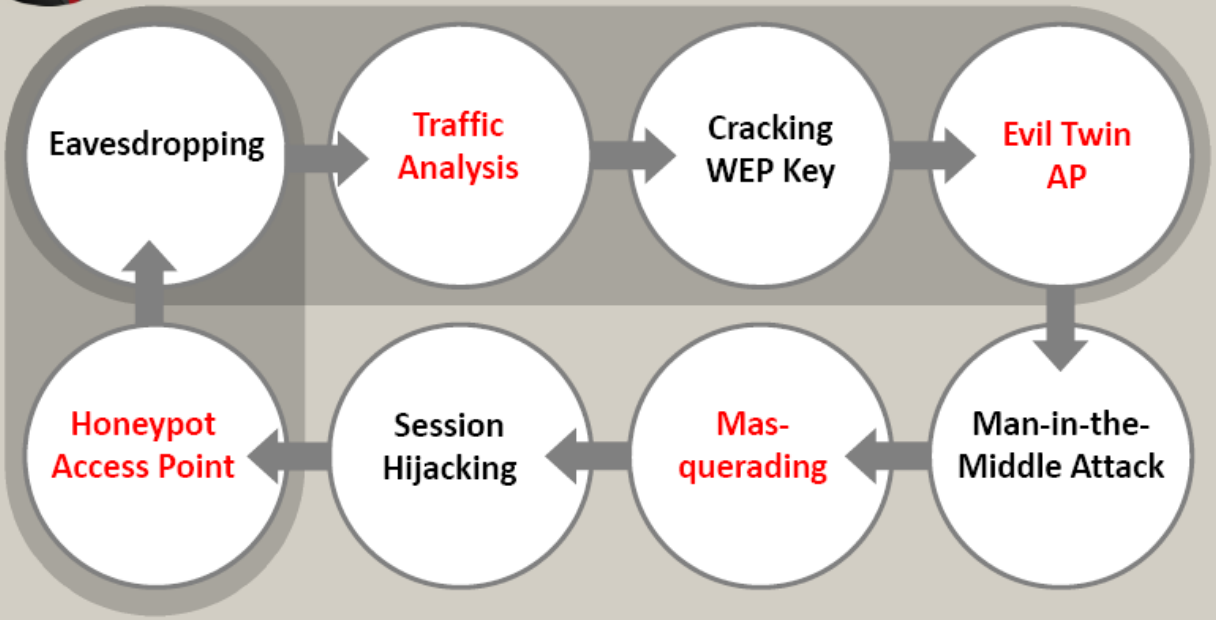
Wireless Threats: Integrity Attacks

In integrity attacks, attackers send forged control, management or data frames over a wireless network to misdirect the wireless devices in order to perform another type of attack (e.g., DoS)

- Data Frame Injection
- WEP Injection
- Data Replay
- Initialization Vector Replay Attacks
- Bit-Flipping Attacks
- Extensible AP Replay
- RADIUS Replay
- Wireless Network Viruses

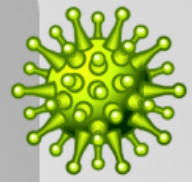
Wireless Threats: Confidentiality Attacks

These attacks attempt to **intercept confidential information sent over wireless associations**, whether sent in the clear text or encrypted by Wi-Fi protocols



Wireless Threats: Availability Attacks

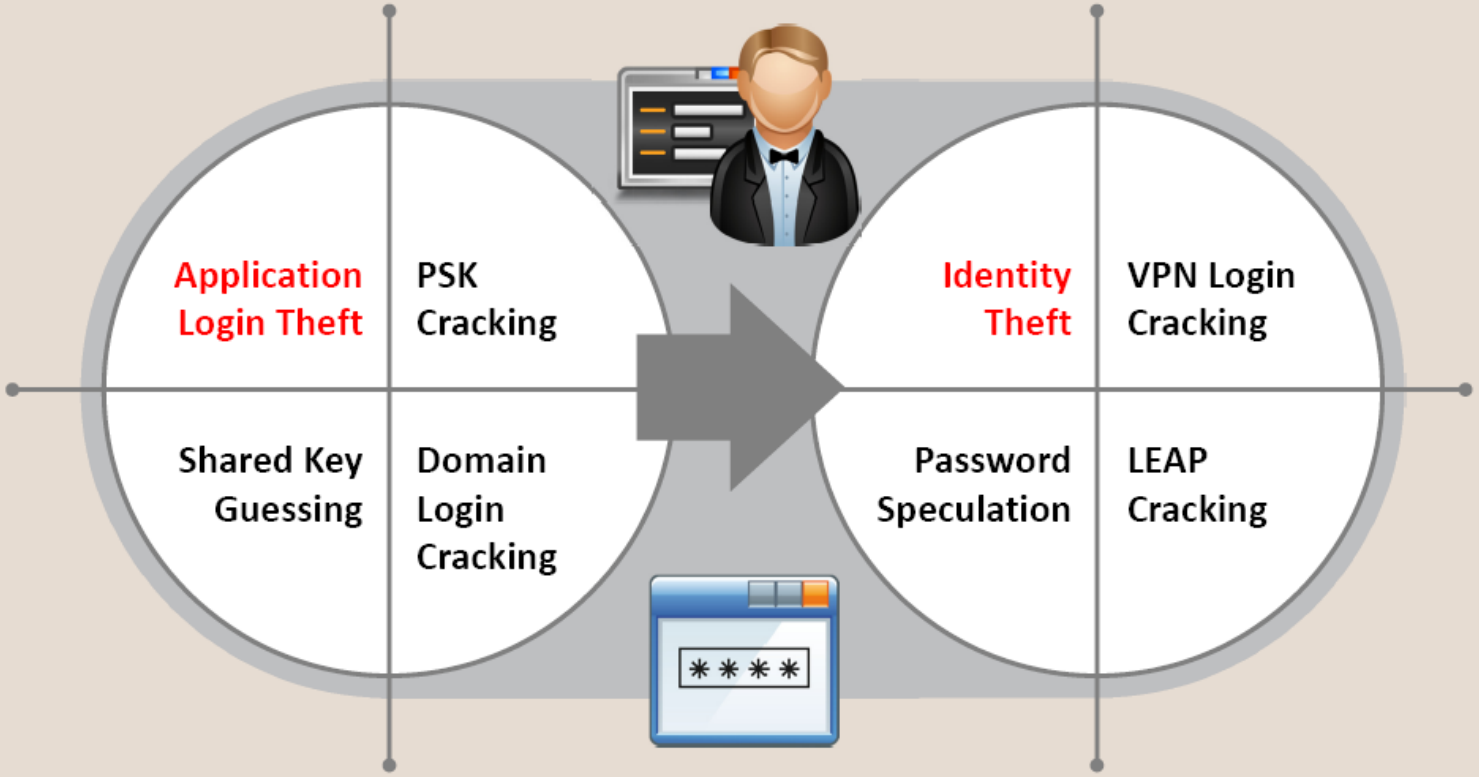
Denial of Service attacks aim to prevent legitimate users from accessing resources in a wireless network



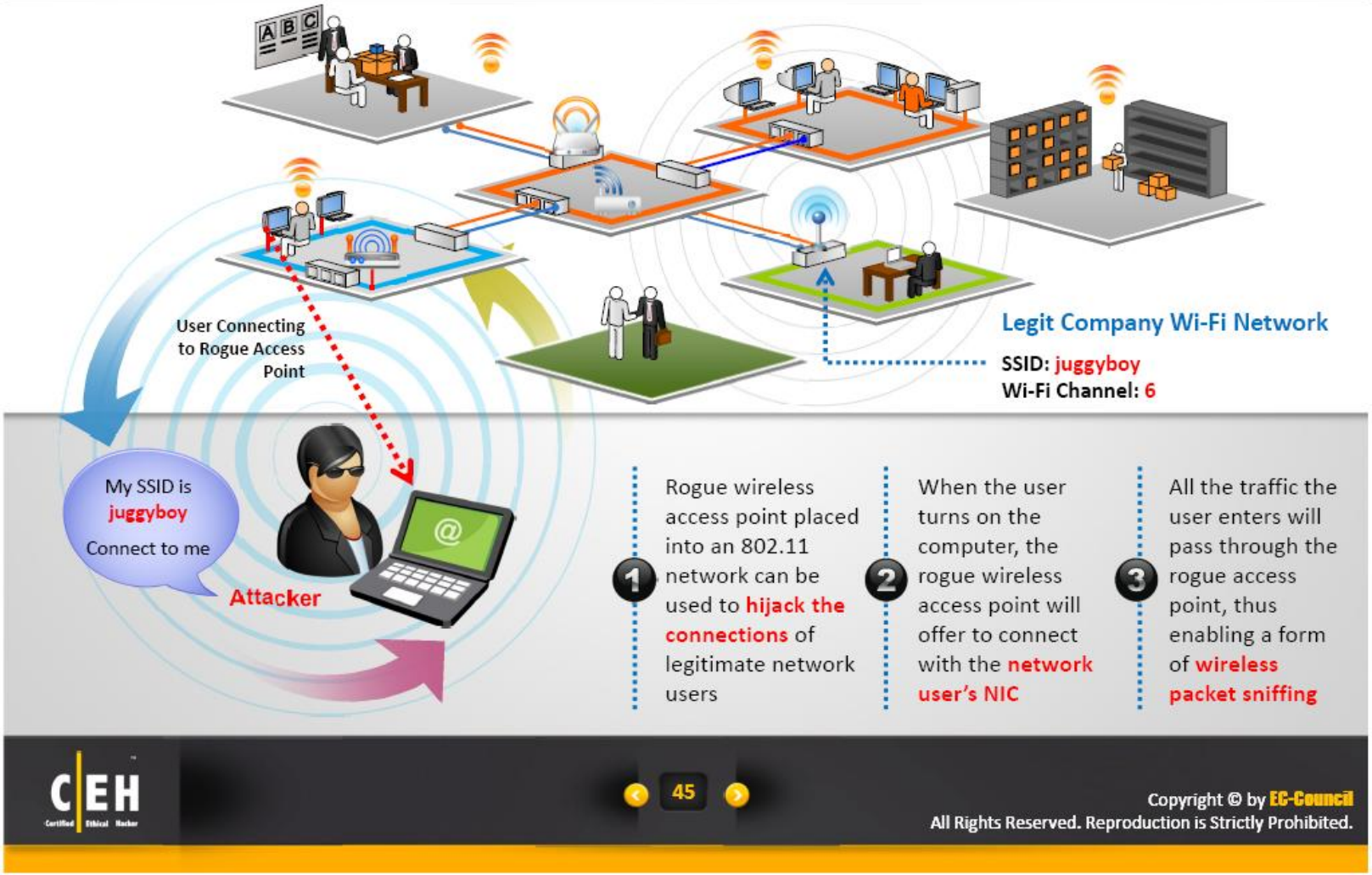
Access Point Theft	Denial of Service	Beacon Flood	Authenticate Flood
Disassociation Attacks	De-authenticate Flood	TKIP MIC Exploit	ARP Cache Poisoning Attack
EAP-Failure	Routing Attacks	Power Saving Attacks	

Wireless Threats: Authentication Attacks

The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources

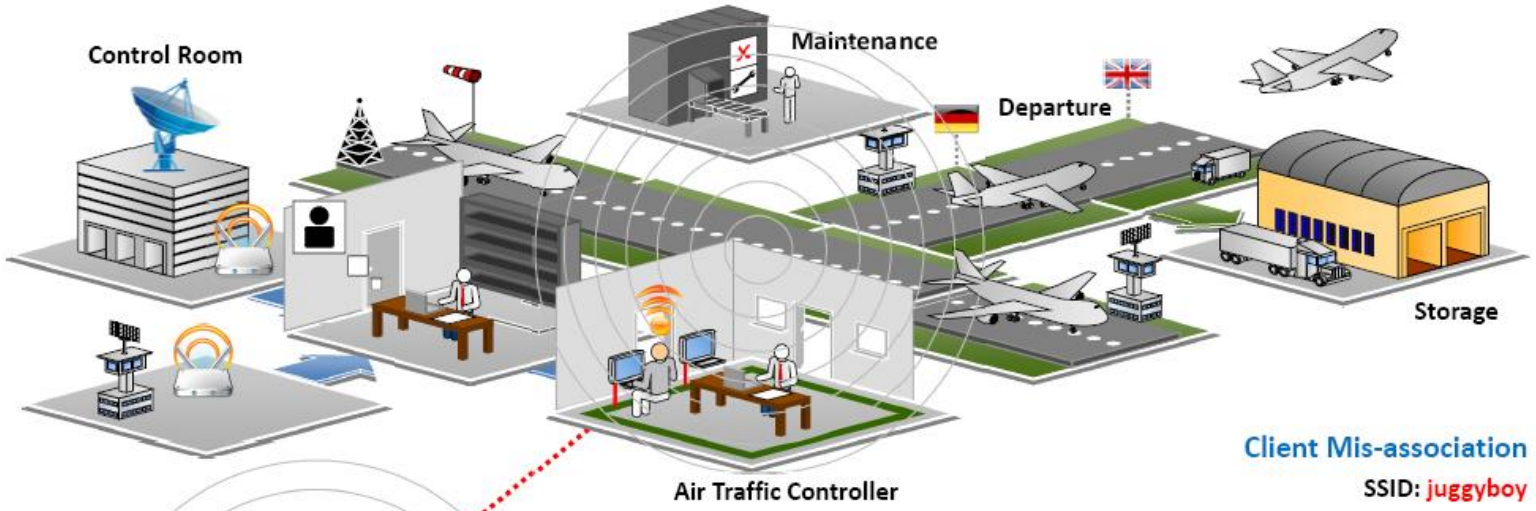


Rogue Access Point Attack



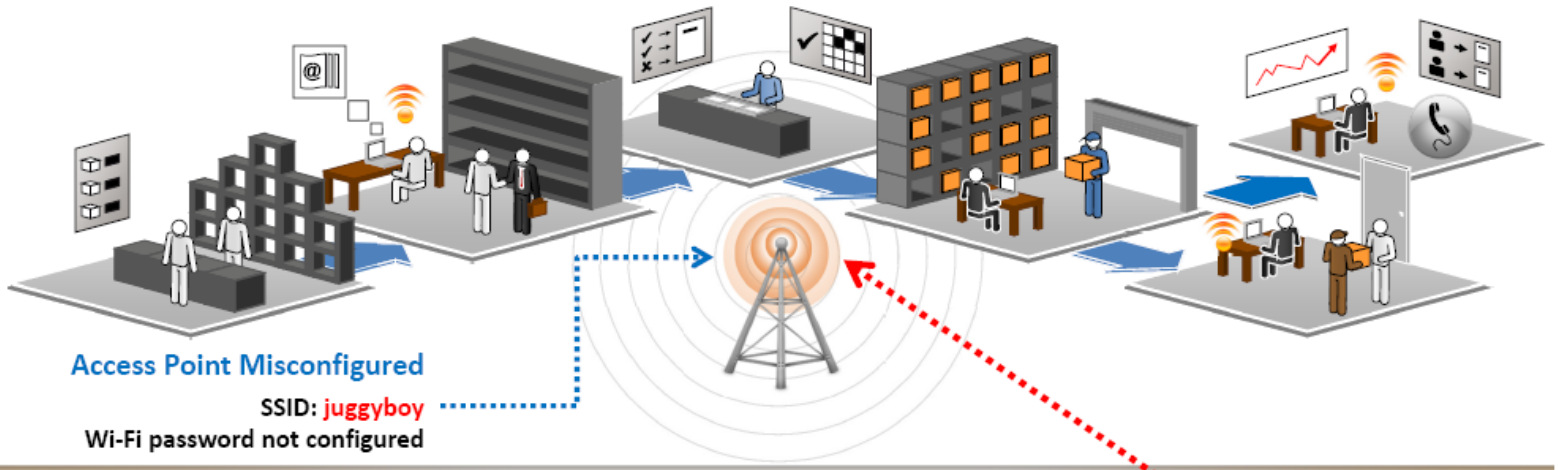
1. Rogue wireless access point placed into an 802.11 network can be used to **hijack the connections** of legitimate network users
2. When the user turns on the computer, the rogue wireless access point will offer to connect with the **network user's NIC**
3. All the traffic the user enters will pass through the rogue access point, thus enabling a form of **wireless packet sniffing**

Client Mis-association



- Attacker sets up a **rogue access point outside the corporate perimeter** and lures the employees of the organization to connect with it
- Once associated, employees may **bypass** the enterprise security policies

Misconfigured Access Point Attack



SSID Broadcast

Access points are configured to **broadcast SSIDs** to authorized users

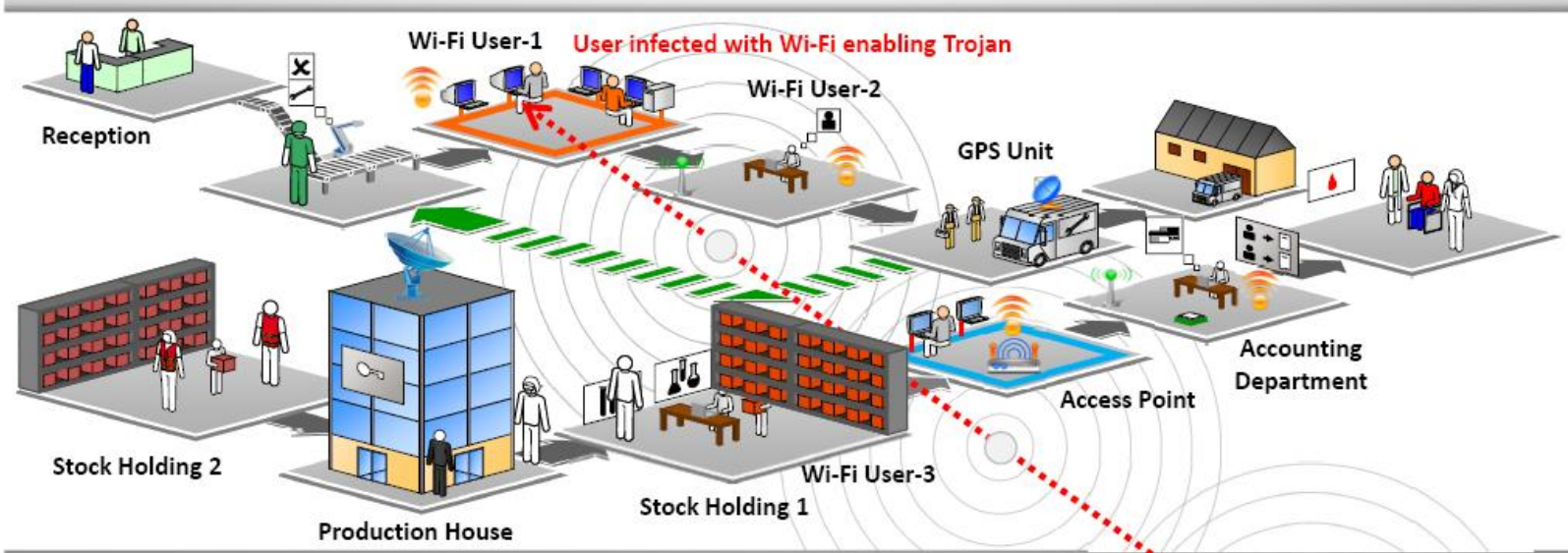
Weak Password

To verify authorized users, network administrators **incorrectly use the SSIDs as passwords**

Configuration Error

SSID broadcasting is a configuration error that assists intruders to **steal an SSID** and have the AP assume they are allowed to connect

Unauthorized Association

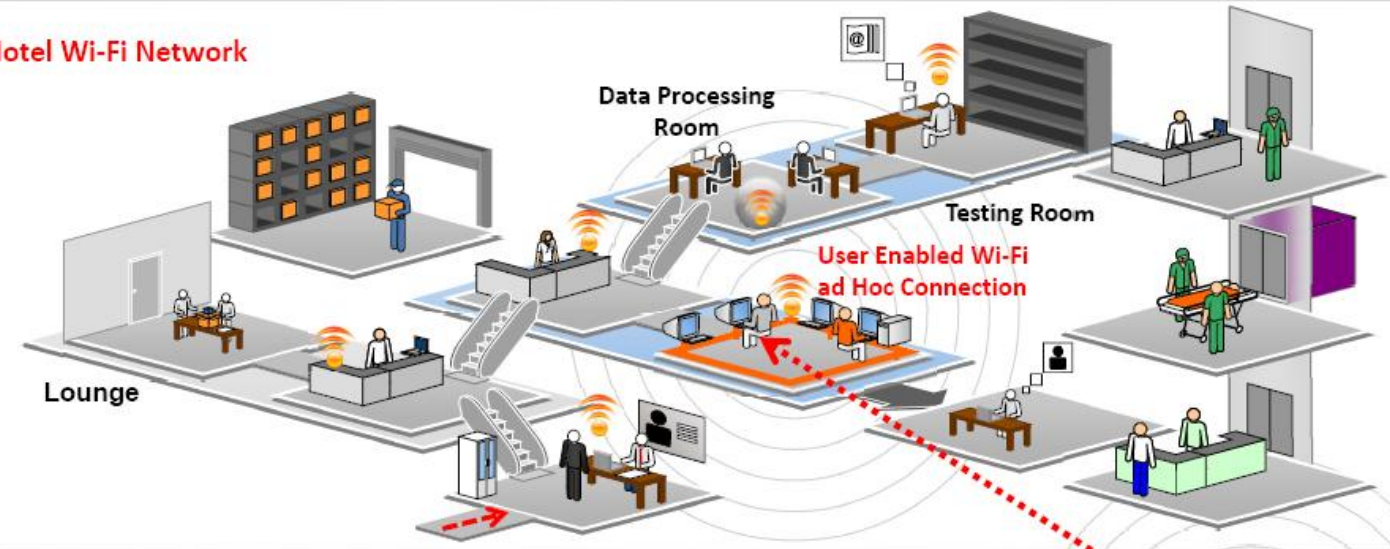


Soft access points are client cards or embedded WLAN radios in some PDAs and laptops that can be launched **inadvertently or through a virus program**

Attackers infect victim's machine and activate soft APs allowing them **unauthorized connection** to the enterprise network

Attacker connect to enterprise network through **soft APs** instead of the actual Access Points

Ad Hoc Connection Attack

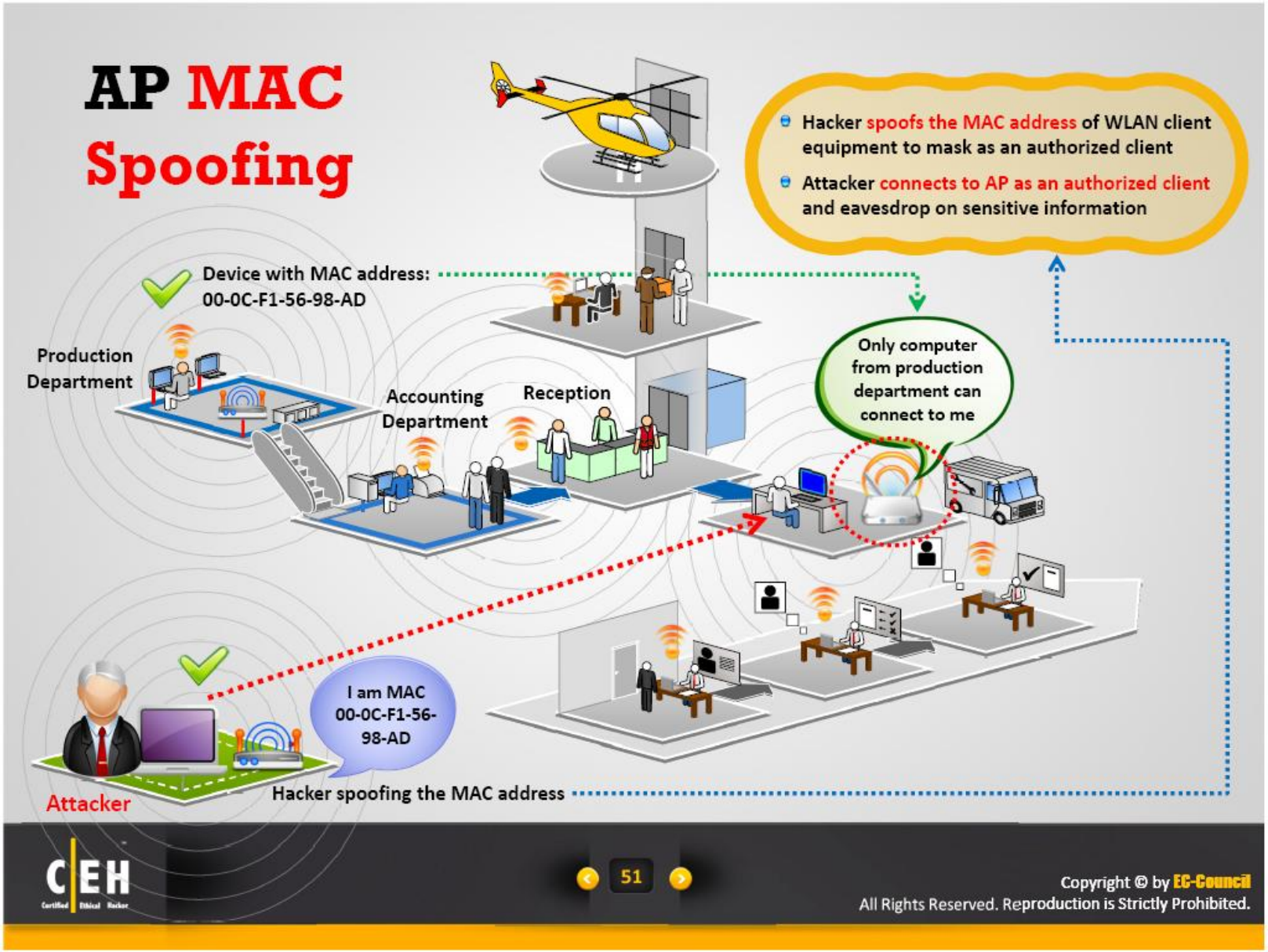


Wi–Fi clients communicate directly via **an ad hoc mode** that do not require an AP to relay packets

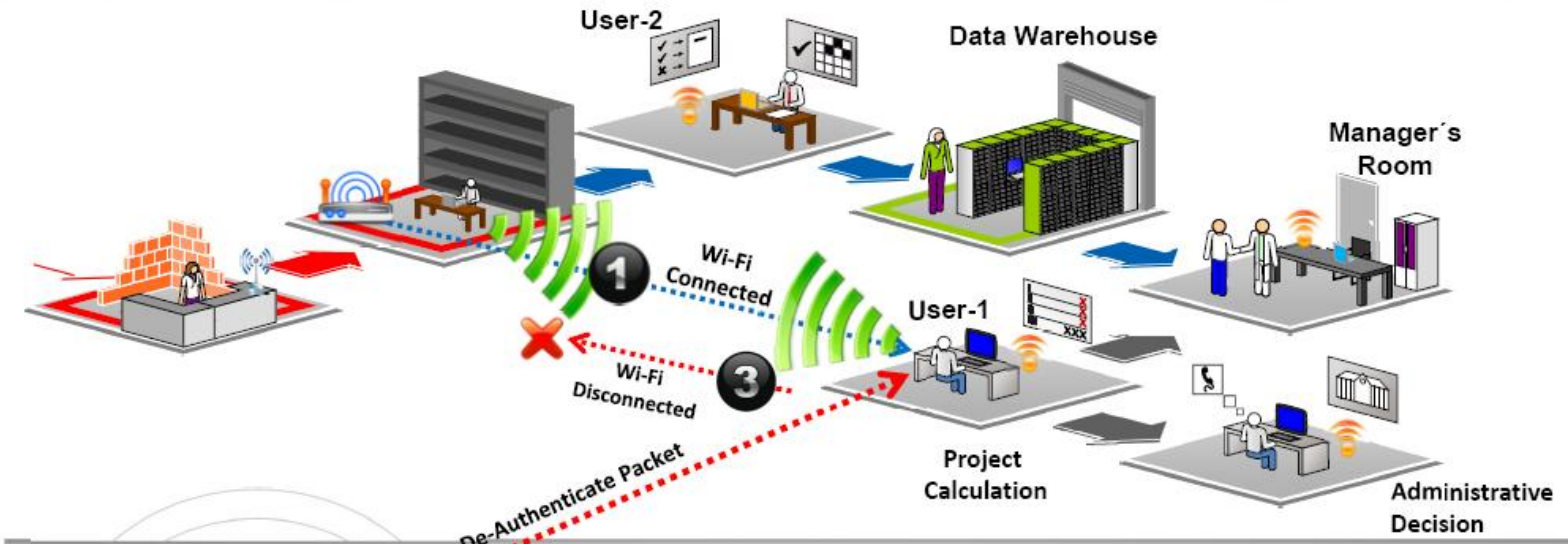
Ad hoc mode is inherently insecure and does not **provide strong authentication and encryption**

Thus attackers can easily connect to and **compromise the enterprise client operating** in ad hoc mode

HoneySpot Access Point Attack



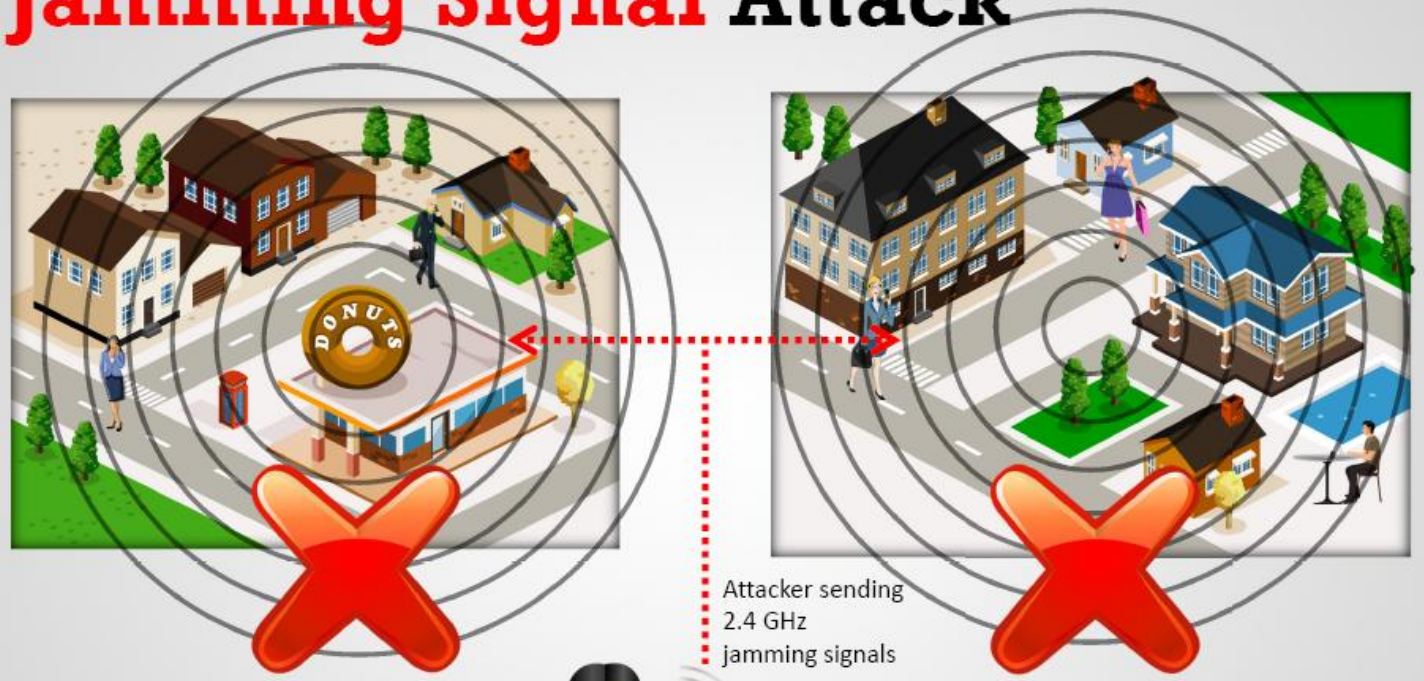
Denial-of-Service Attack



Wireless DoS attacks **disrupt network wireless connections** by sending broadcast "de–authenticate" commands

Broadcast deauthentication forces the clients to **disconnect from the AP**

Jamming Signal Attack



Attacker sending 2.4 GHz jamming signals

An attacker stakes out the area from a nearby location with a **high gain amplifier** drowning out the legitimate access point

Users simply can't get through to log in or they are **knocked off** their connections by the overpowering nearby signal

Attacker

Jamming Device

All wireless networks are prone to jamming,

The signals generated by jamming devices **appear to be an 802.11 transmission** to the devices on the wireless network, which causes them **to hold their transmissions** until the signal has subsided resulting in Denial-of-Service

Wi-Fi Jamming Devices

MGT- P6 GPS Jammer

Range : 10 ~ 20 meters
4 antennas
3G: 2110 ~ 2170MHz
Wi-Fi / Bluetooth: 2400 ~ 2485MHz

MGT- 02 Jammer

Range : 20 ~ 50 meters
4 antennas

MGT- MP200 Jammer

Range: 50 - 75m
Barrage + DDS sweep jamming 20 to 2500 MHz.
Omni-directional antennas

MGT- 03 Jammer

Range : 0 ~ 40 meters
4 antennas

MGT- P6 Wi-Fi Jammer

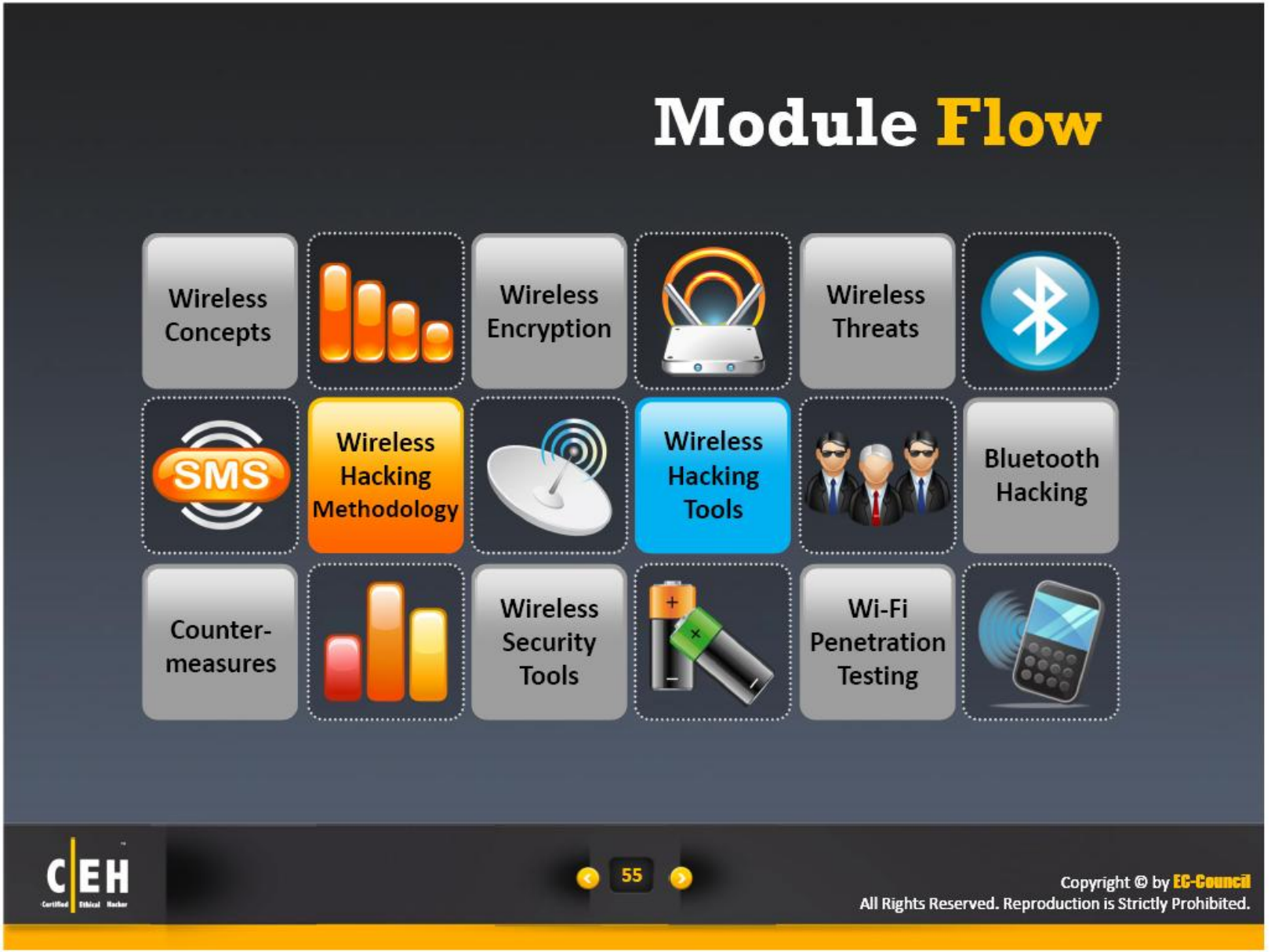
Range : 10 ~ 20 meters
iDen - CDMA - GSM: 850 ~ 960MHz
DCS - PCS: 1805 ~ 1990MHz
3G: 2110 ~ 2170MHz
Wi-Fi / Bluetooth: 2400 ~ 2485MHz
4 antennas

MGT- P3x13 Jammer

Range : 50 ~ 200 meters
3 frequency bands jammed

http://www.magnumtelecom.com

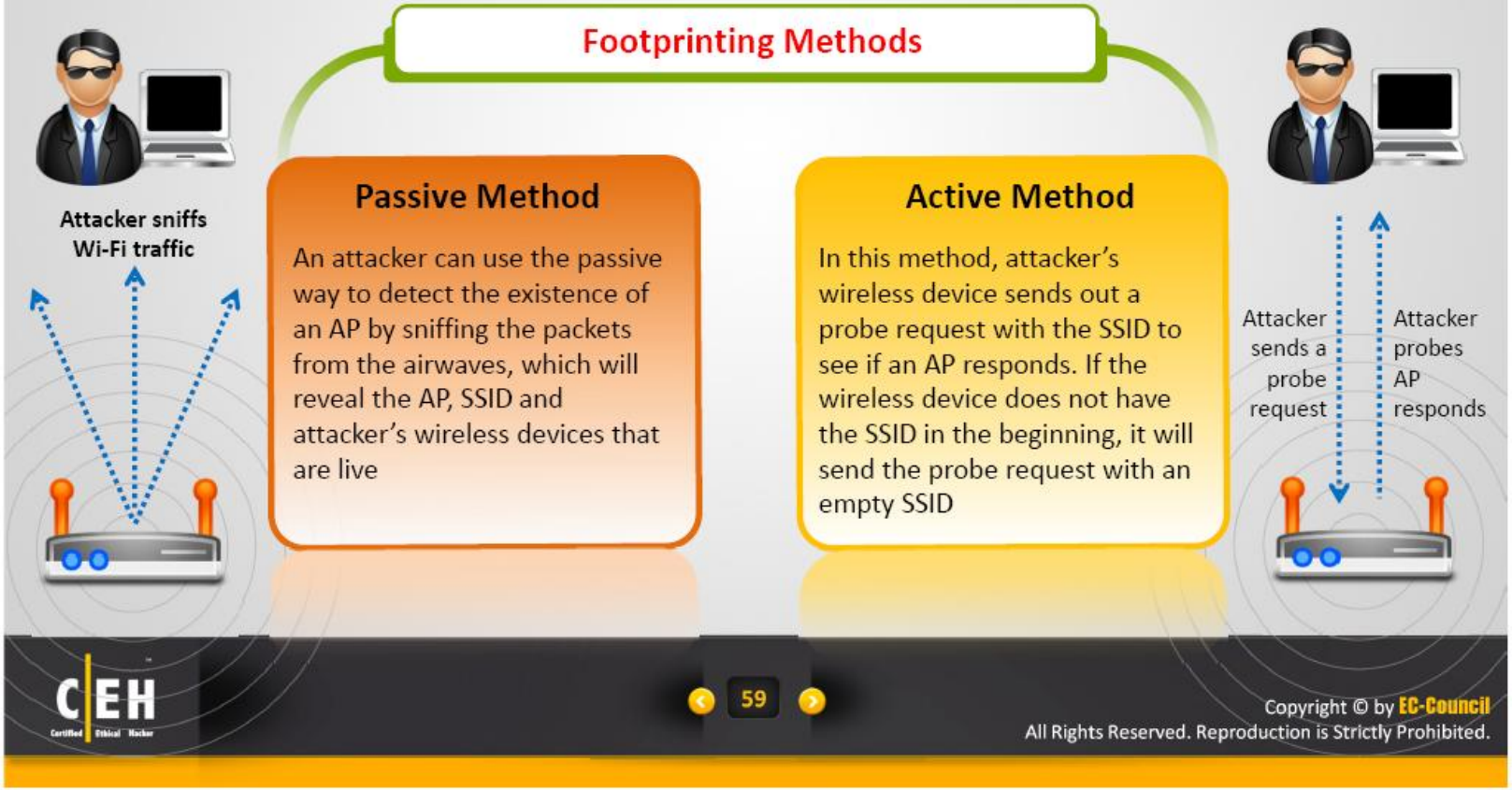
Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
CEH
55
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

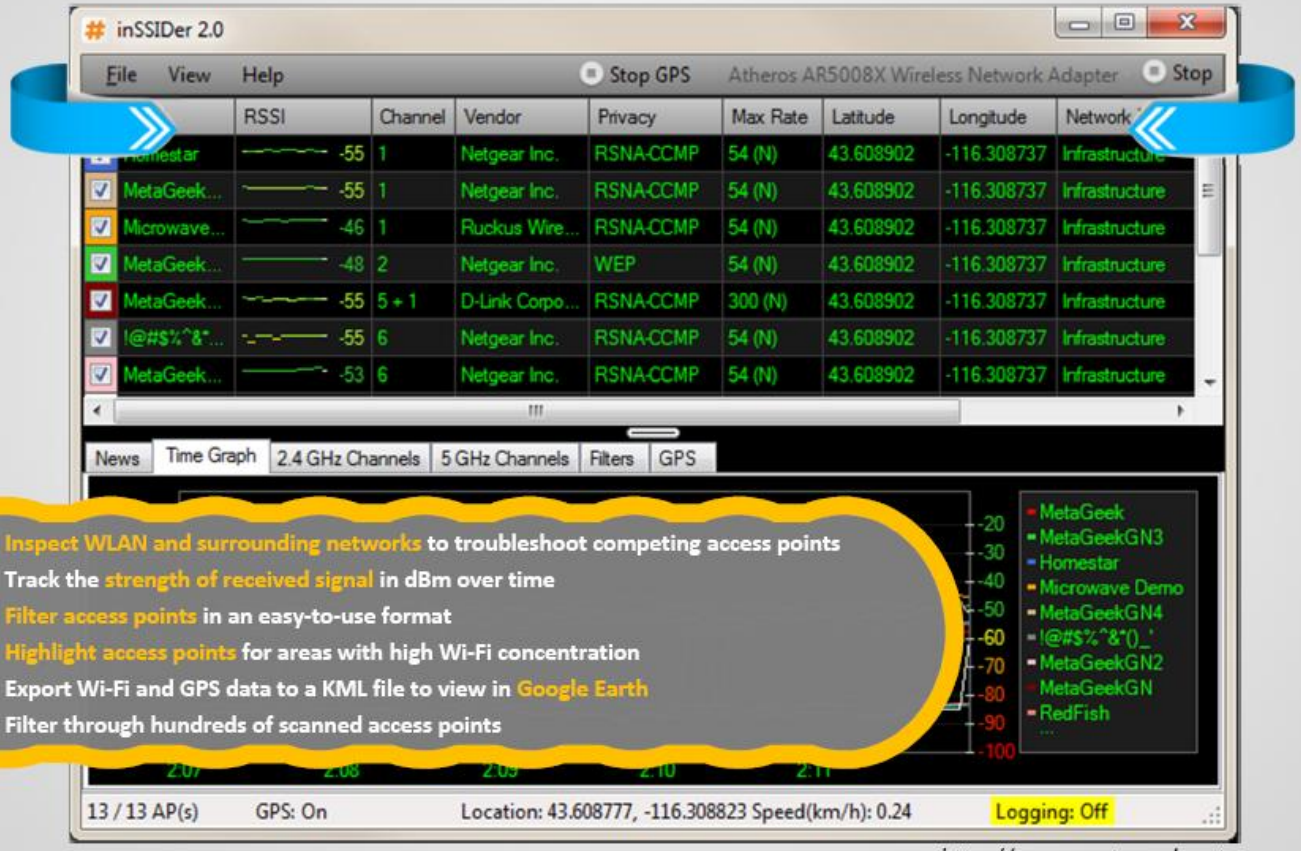
Attackers Scanning for Wi-Fi Networks

Footprint the Wireless Network

Attacking a wireless network begins **discovering** and **footprinting** the wireless network in an active or passive way



Wi-Fi Discovery Tool: inSSIDer

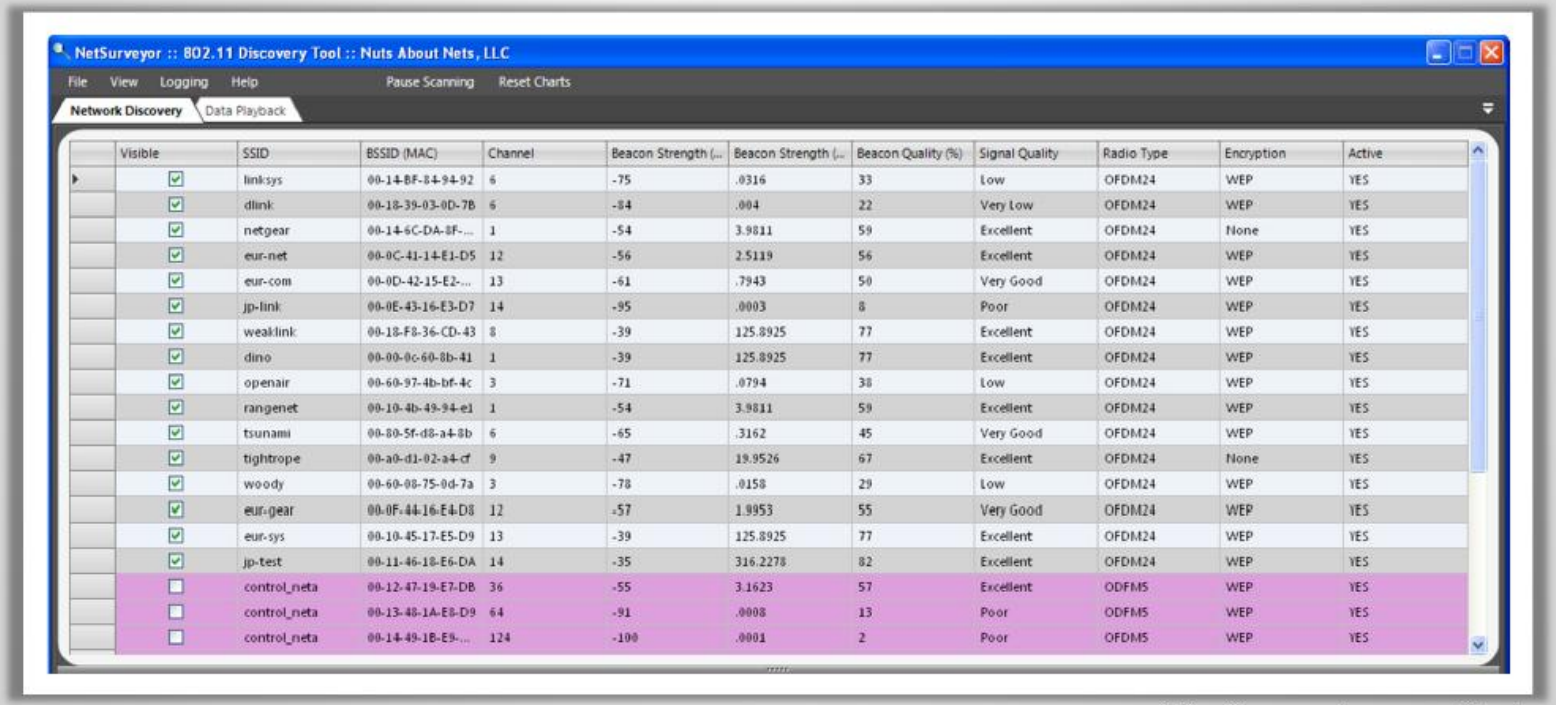


1. Inspect WLAN and surrounding networks to troubleshoot competing access points
2. Track the strength of received signal in dBm over time
3. Filter access points in an easy-to-use format
4. Highlight access points for areas with high Wi-Fi concentration
5. Export Wi-Fi and GPS data to a KML file to view in Google Earth
6. Filter through hundreds of scanned access points

http://www.metageek.net

Wi-Fi Discovery Tool: NetSurveyor

NetSurveyor is a network discovery tool used to gather information about nearby wireless access points in real time



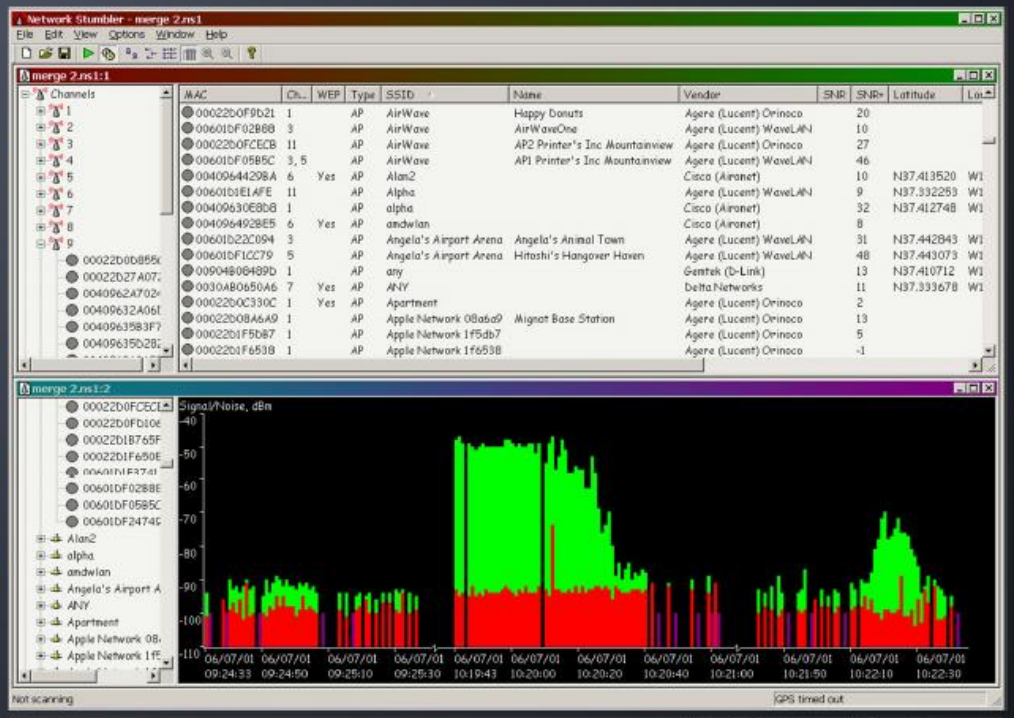
Visible	SSID	BSSID (MAC)	Channel	Beacon Strength (...	Beacon Strength (...	Beacon Quality (%)	Signal Quality	Radio Type	Encryption	Active
☑	linksys	00-14-BF-84-94-92	6	-75	.0316	33	Low	OFDM24	WEP	YES
☑	dlink	00-18-39-03-0D-7B	6	-84	.004	22	Very Low	OFDM24	WEP	YES
☑	netgear	00-14-6C-DA-8F-...	1	-54	3.9811	59	Excellent	OFDM24	None	YES
☑	eur-net	00-0C-41-14-E1-D5	12	-56	2.5119	56	Excellent	OFDM24	WEP	YES
☑	eur-com	00-0D-42-15-E2-...	13	-61	.7943	50	Very Good	OFDM24	WEP	YES
☑	jp-link	00-0E-43-16-E3-D7	14	-95	.0003	8	Poor	OFDM24	WEP	YES
☑	weaklink	00-18-F8-36-CD-43	8	-39	125.8925	77	Excellent	OFDM24	WEP	YES
☑	dino	00-00-0c-60-8b-41	1	-39	125.8925	77	Excellent	OFDM24	WEP	YES
☑	openair	00-60-97-4b-bf-4c	3	-71	.0794	38	Low	OFDM24	WEP	YES
☑	rangenet	00-10-4b-49-94-e1	1	-54	3.9811	59	Excellent	OFDM24	WEP	YES
☑	tsunami	00-80-5f-d8-a4-8b	6	-65	.3162	45	Very Good	OFDM24	WEP	YES
☑	tightrope	00-a0-d1-02-a4-cf	9	-47	19.9526	67	Excellent	OFDM24	None	YES
☑	woody	00-60-08-75-0d-7a	3	-78	.0158	29	Low	OFDM24	WEP	YES
☑	eur-gear	00-0F-44-16-E4-D8	12	-57	1.9953	55	Very Good	OFDM24	WEP	YES
☑	eur-sys	00-10-45-17-E5-D9	13	-39	125.8925	77	Excellent	OFDM24	WEP	YES
☑	jp-test	00-11-46-18-E6-DA	14	-35	316.2278	82	Excellent	OFDM24	WEP	YES
☐	control_neta	00-12-47-19-E7-DB	36	-55	3.1623	57	Excellent	ODFM5	WEP	YES
☐	control_neta	00-13-48-1A-E8-D9	64	-91	.0008	13	Poor	ODFM5	WEP	YES
☐	control_neta	00-14-49-1B-E9-...	124	-100	.0001	2	Poor	OFDM5	WEP	YES

http://www.performancewifi.net

Wi-Fi Discovery Tool: NetStumbler

Facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards

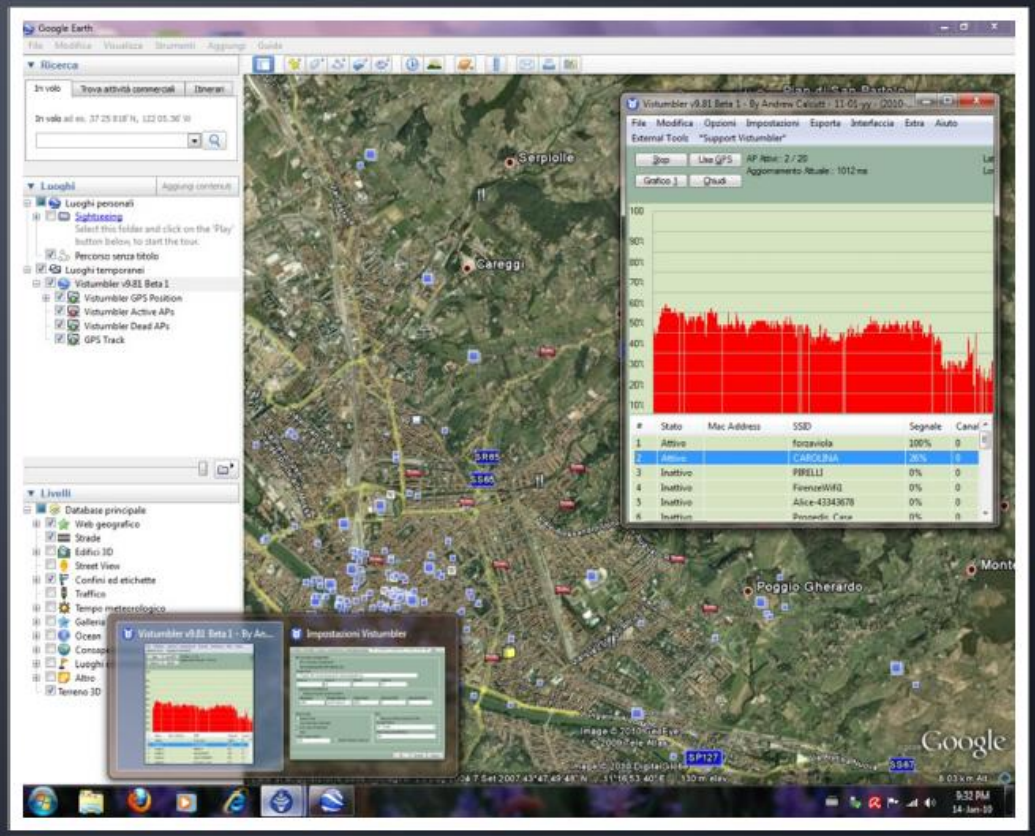
1. Wardriving
2. Verifying network configurations
3. Finding locations with poor coverage in one's WLAN
4. Detecting causes of wireless interference
5. Detecting rogue access points
6. Aiming directional antennas for long-haul WLAN links



http://www.netstumbler.com

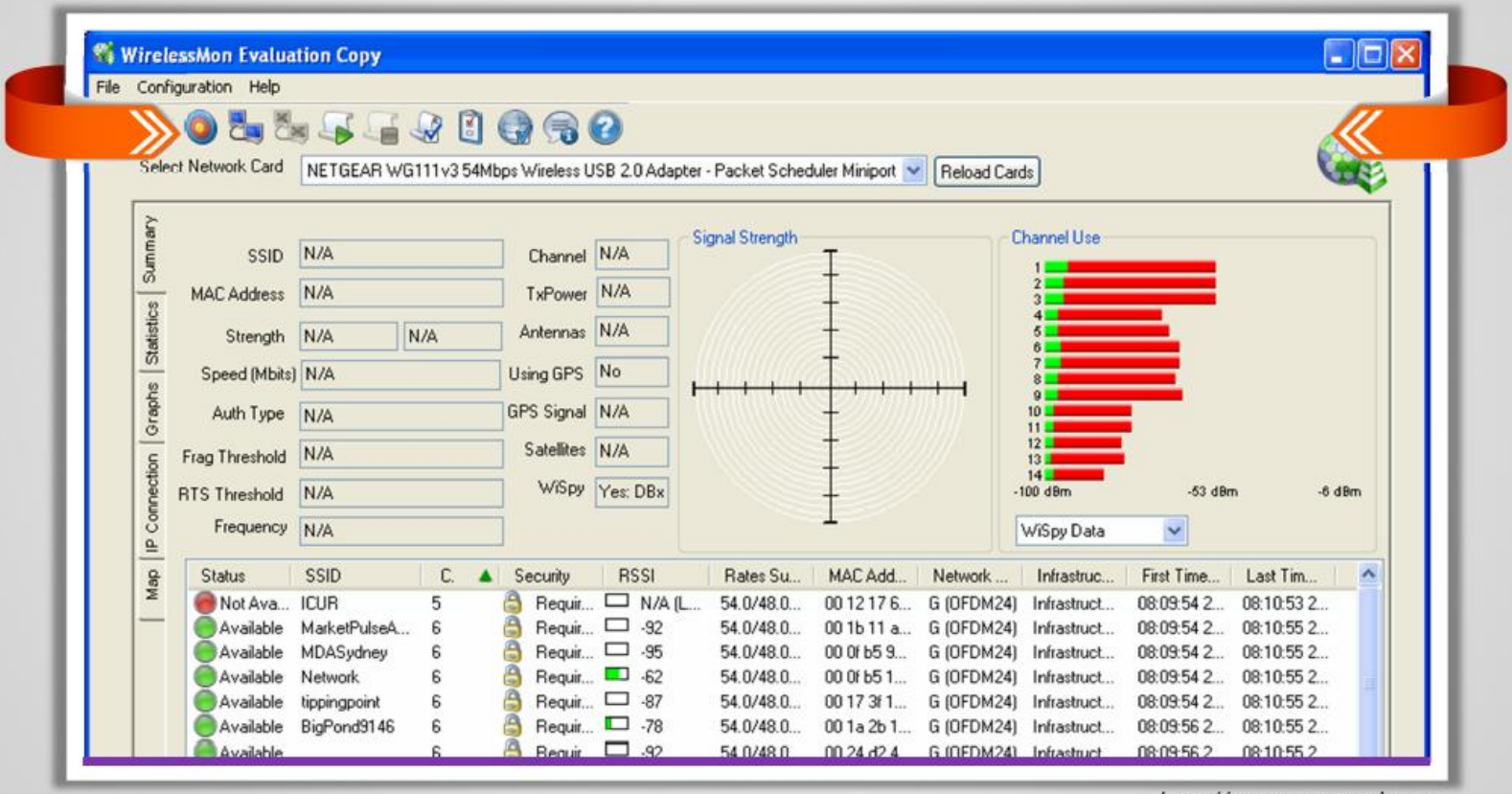
Wi-Fi Discovery Tool: Vistumbler

1. Finds wireless access points
2. Uses the Vista command 'netsh wlan show networks mode=bssid' to get wireless information
3. It supports for GPS and live Google Earth tracking



http://www.vistumbler.net

Wi-Fi Discovery Tool: WirelessMon



http://www.passmark.com

Wi-Fi Discovery Tools

WiFi Hopper
http://www.wifihopper.com

Meraki WiFi Stumbler
http://meraki.com

Wavestumbler
http://www.cqure.net

Wellenreiter
http://wellenreiter.sourceforge.net

iStumbler
http://www.istumbler.net

AirCheck Wi-Fi Tester
http://www.flukenetworks.com

WiFinder
http://www.pgmsoft.com

AirRadar 2
http://www.koingosw.com

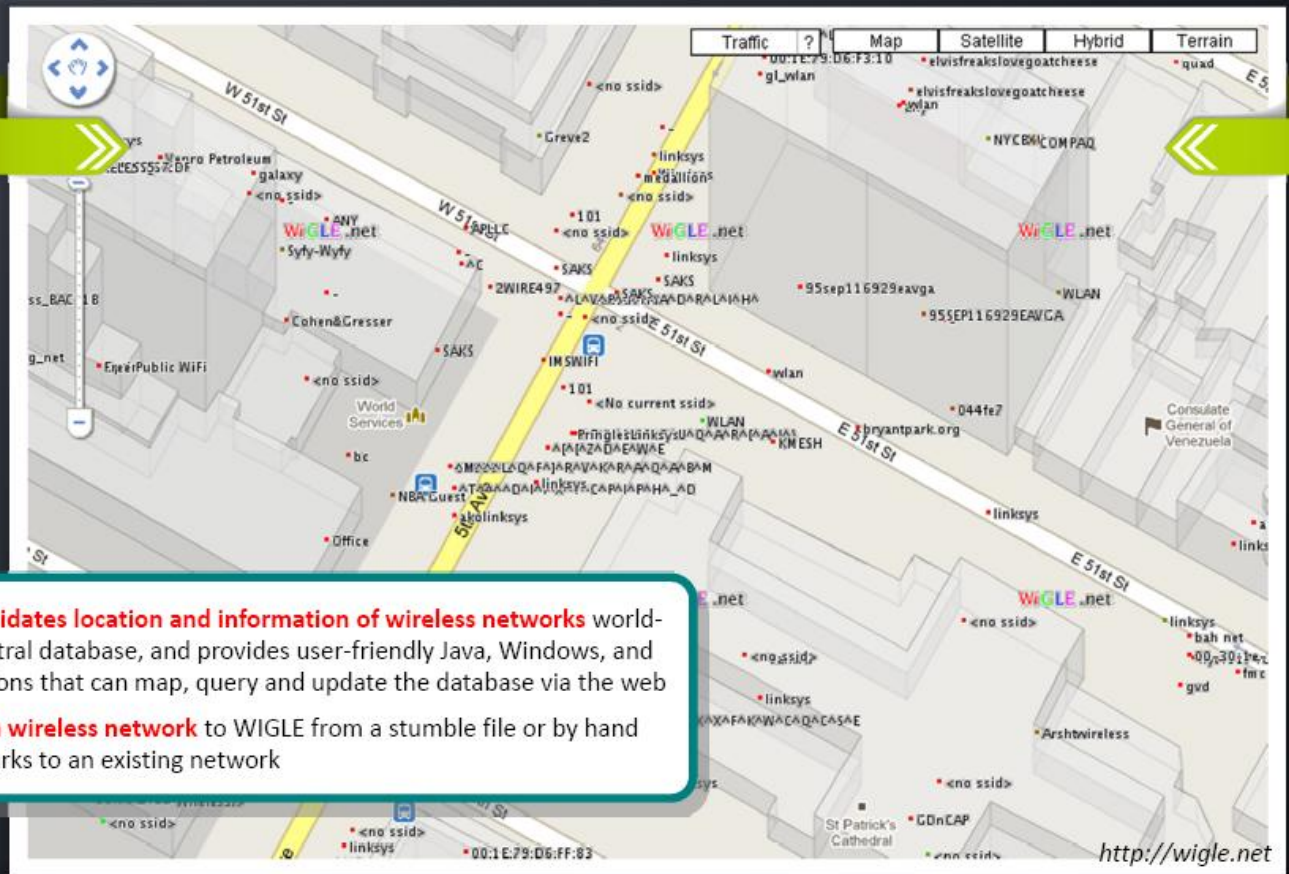
GPS Mapping

Attackers create map of discovered Wi-Fi networks and create a database with statistics collected by Wi-Fi discovery tools such as Netsurveyor, NetStumblers etc.

GPS is used to track the location of the discovered Wi-Fi networks and the coordinates uploaded to sites like WIGLE

Attackers can share this information with the hacking to community or sell it to make money

GPS Mapping Tool: WIGLE

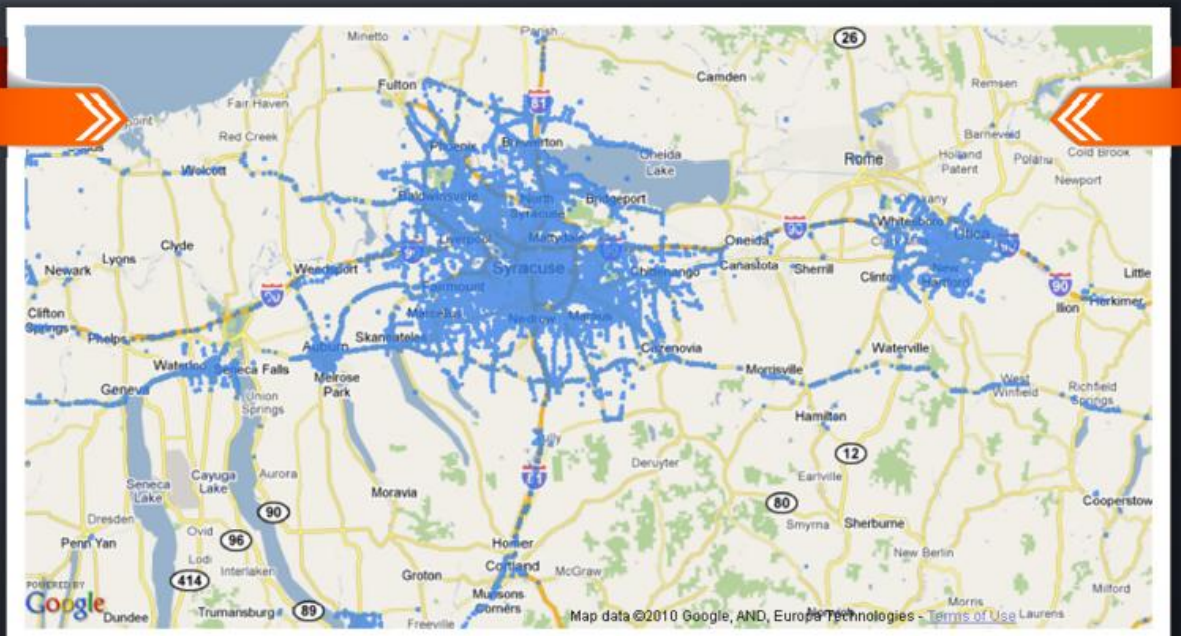


WIGLE **consolidates location and information of wireless networks** world-wide to a central database, and provides user-friendly Java, Windows, and web applications that can map, query and update the database via the web

You can **add a wireless network** to WIGLE from a stumble file or by hand and add remarks to an existing network

GPS Mapping Tool: Skyhook

Skyhook's Wi-Fi Positioning System (WPS) **determines location based** on Skyhook's massive worldwide database of known Wi-Fi access points



http://www.skyhookwireless.com

How to Discover Wi-Fi Network Using Wardriving?

STEP 1

Register with WIGLE and download map packs of your area to view the plotted access points on a geographic map

STEP 2

Connect the antenna, GPS device to the laptop via a USB serial adapter and board on a car

STEP 3

Install and launch NetStumbler and WIGLE client software and turn on the GPS device

STEP 4

Drive the car at speeds of 35 mph or below (At higher speeds, Wi-Fi antenna will not be able to detect Wi-Fi spots)

STEP 5

Capture and save the NetStumbler log files which contains GPS coordinates of the access points

STEP 6

Upload this log file to WIGLE, which will then automatically plot the points onto a map

Wireless Traffic Analysis

Identify Vulnerabilities

Wireless traffic analysis enables attackers to **identify vulnerabilities** and susceptible victims in a target wireless network

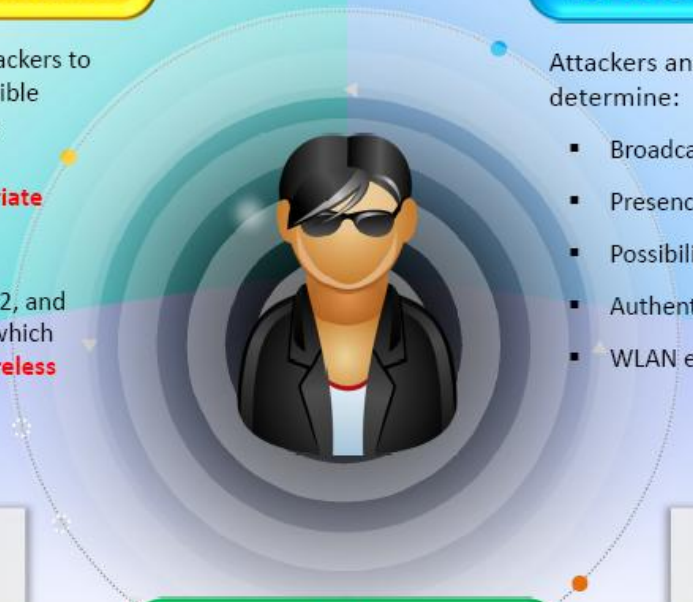
It helps in **determining the appropriate strategy** for a successful attack

Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized which makes easy to **sniff and analyze wireless packets**

Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

- Broadcasted SSID
- Presence of multiple access points
- Possibility of recovering SSIDs
- Authentication method used
- WLAN encryption algorithms



Tools

Wi-Fi packet-capture and analysis products come in a number of forms

- Wireshark/Pilot Tool
- OmniPeek Tool
- CommView Tool
- AirMagnet Wi-Fi Analyzer

Wireless Cards and Chipsets

Choosing the right Wi-Fi card is very important since tools like Aircrack-ng, KisMAC only works with selected wireless chipsets

Decide if you simply want to listen to wireless network traffic or to both listen to and **inject packets**. PCMCIA or USB

Visit **http://madwifi-project.org/wiki/Compatibility** site for compatibility

Determine the drivers required for your chipset and your operating system

Determine your Wi-Fi requirements

Learn the capabilities of a wireless card

Determine the chipset of the Wi-Fi card

Verify the chipset capabilities

Determine the drivers and patches required

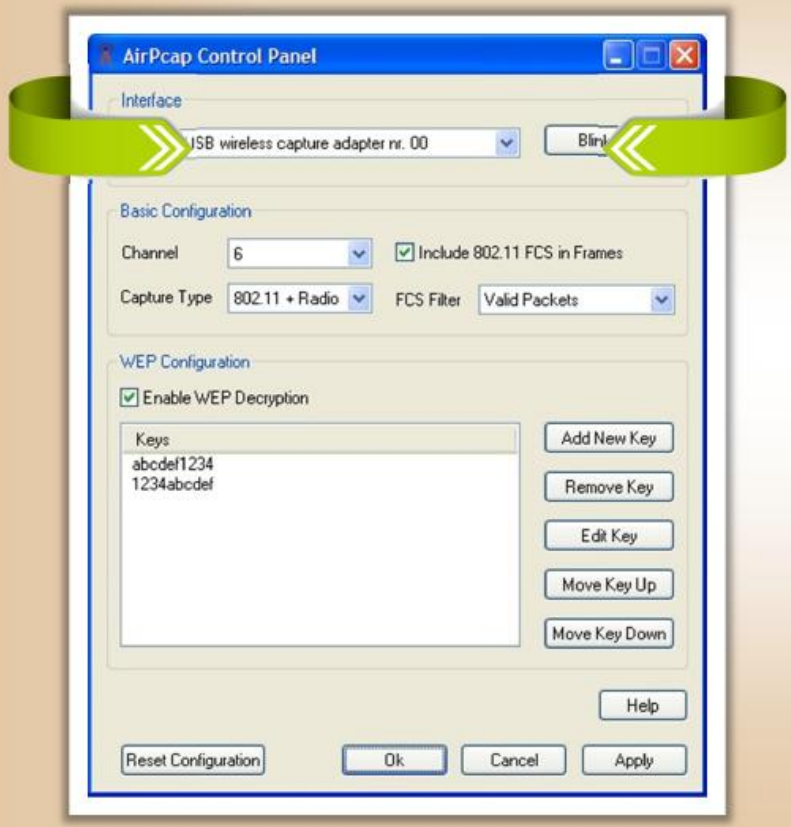
Who is the card manufacturer, version, revision, model etc.

Identify the chipset used in the card

Determine what features the chipset provides for the particular operating system that you will be using

CEH Certified Ethical Hacker

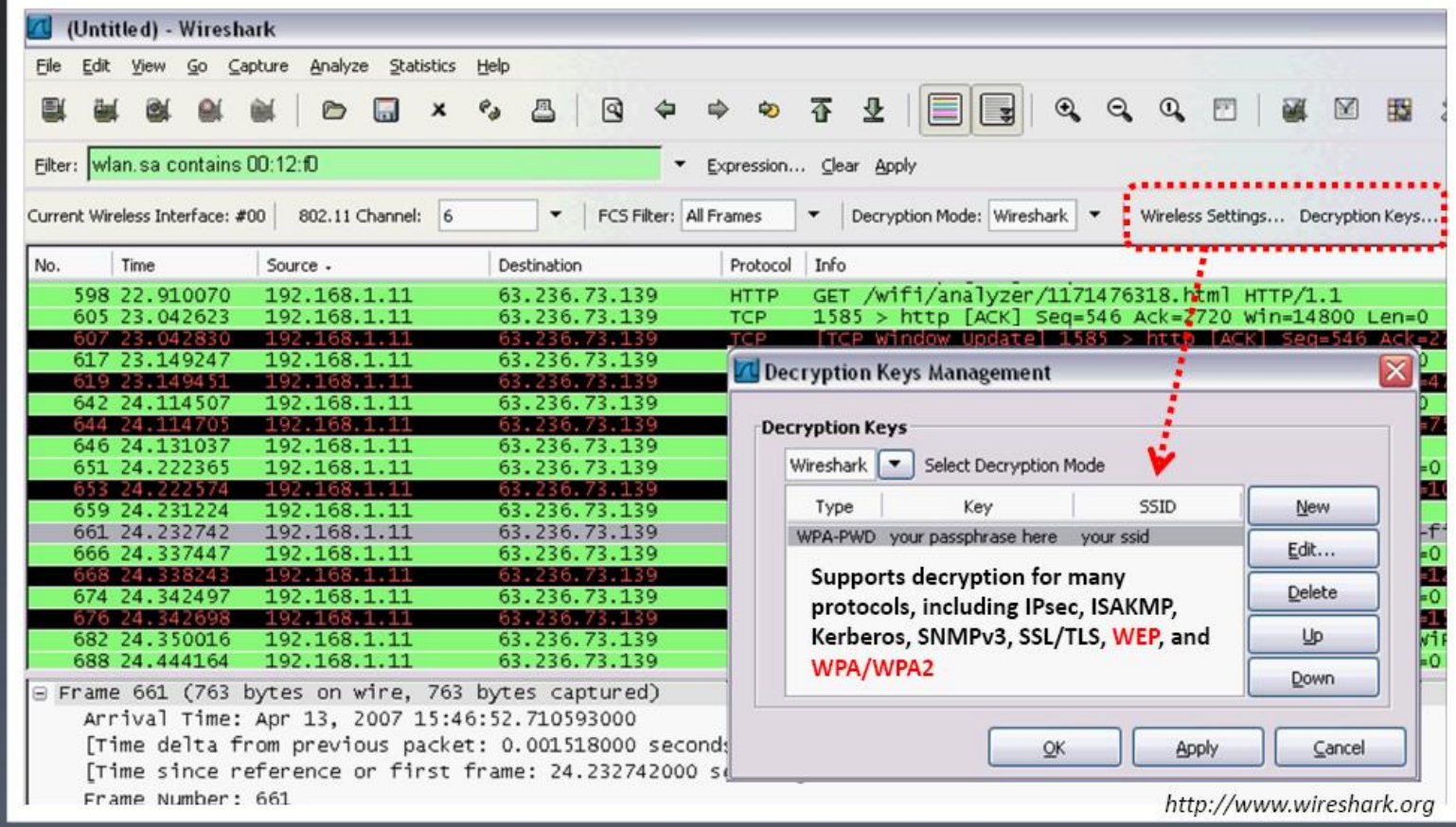
Wi-Fi USB Dongle: AirPcap



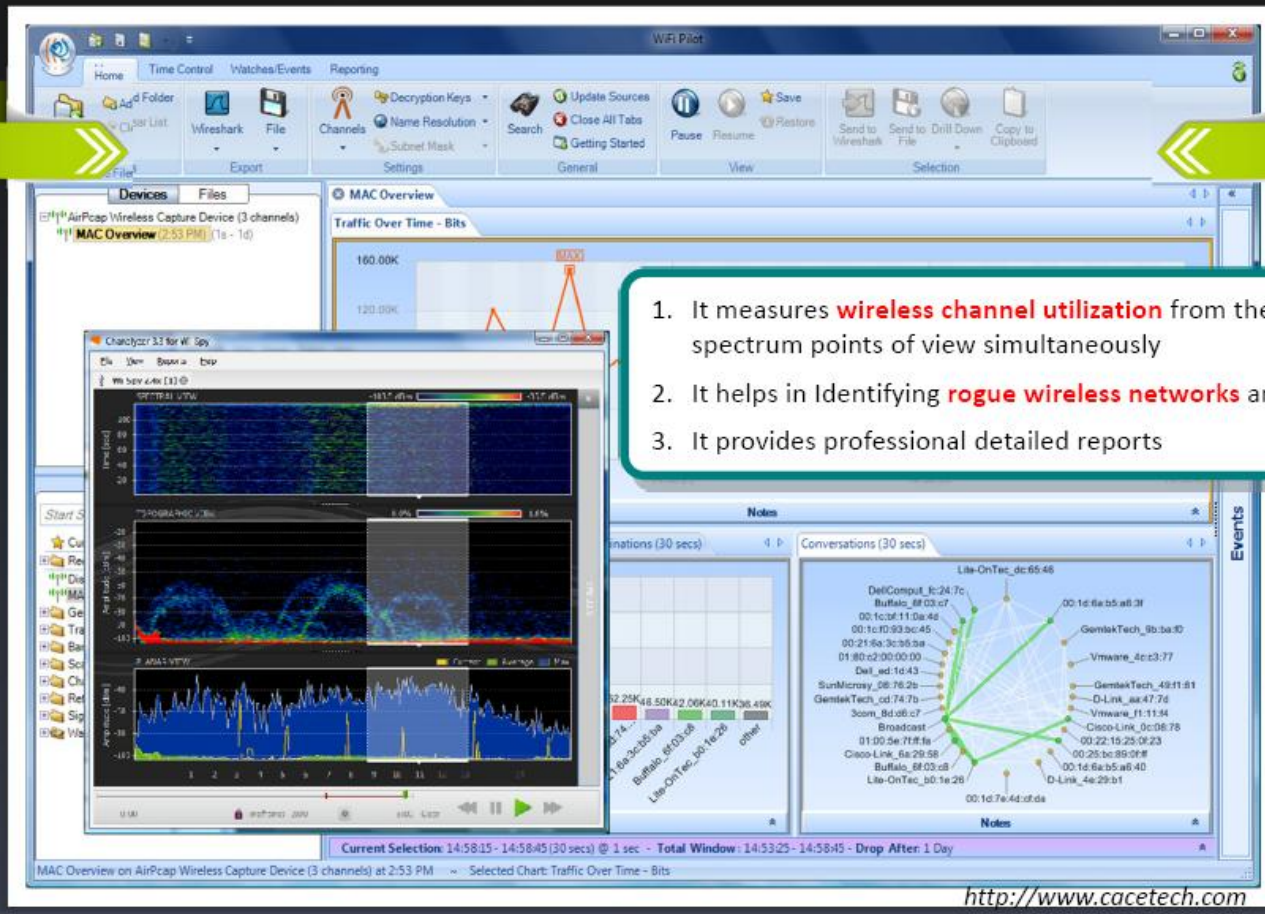
- AirPcap adapter **captures full 802.11 data, management, and control frames** that can be viewed in Wireshark for in-depth protocol dissection and analysis
- AirPcap software can be configured **to decrypt WEP/WPA-encrypted frames**
- It **provides capability** for simultaneous multi-channel capture and traffic aggregation
- It can be used for **traffic injection** that help in assessing the security of a wireless network
- AirPcap is supported in Aircrack-ng, Cain and Able, and Wireshark tools
- **AirPcapReplay**, included in the AirPcap Software Distribution, replays 802.11 network traffic that is contained in a trace file

http://www.cacetech.com

Wi-Fi Packet Sniffer: Wireshark with AirPcap



Wi-Fi Packet Sniffer: Wi-Fi Pilot



1. It measures **wireless channel utilization** from the data and spectrum points of view simultaneously
2. It helps in Identifying **rogue wireless networks** and stations
3. It provides professional detailed reports

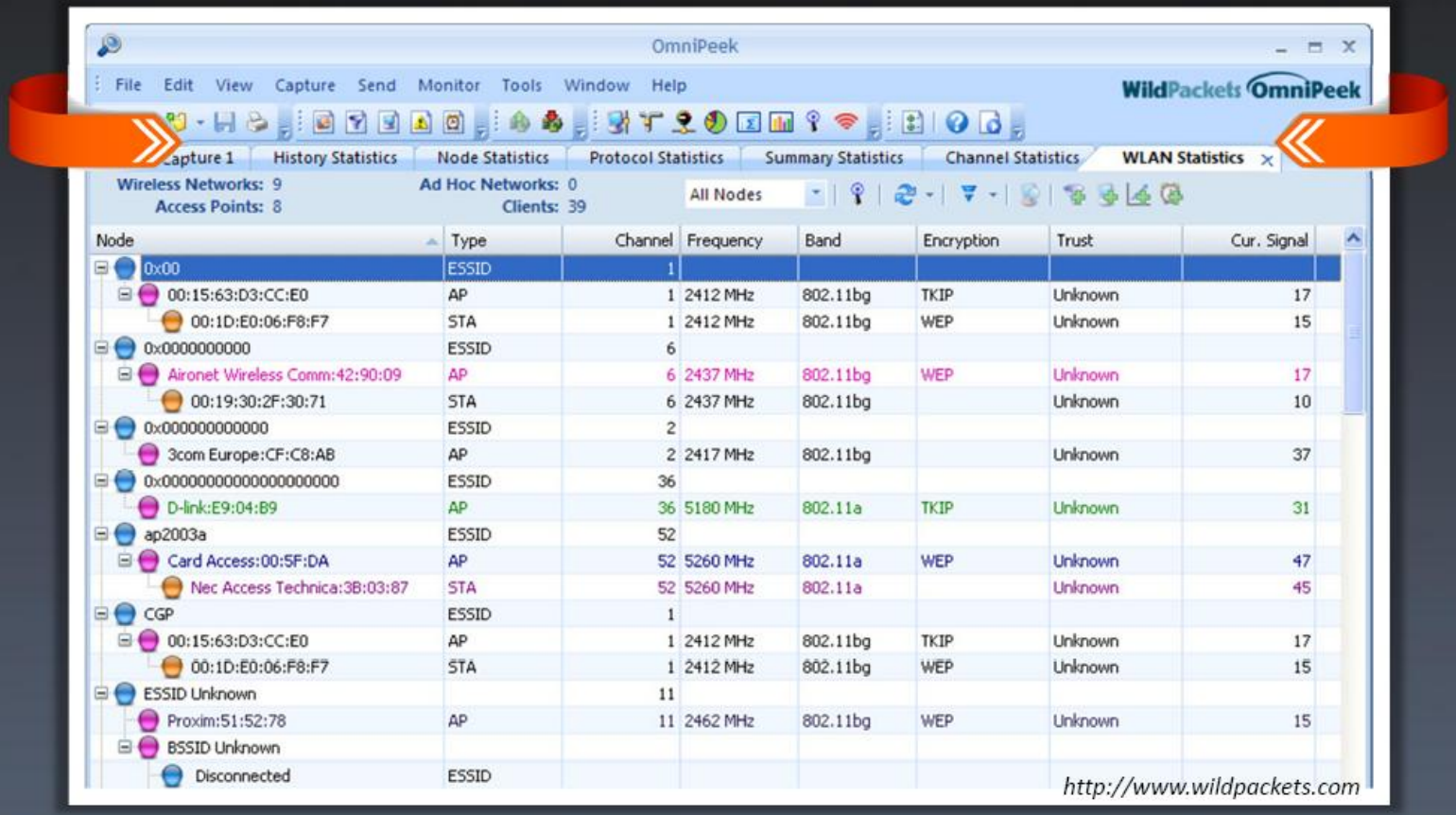
http://www.cacetech.com

Wi-Fi Packet Sniffer: OmniPeek

- OmniPeek network analyzer offers **real-time visibility and analysis** of the network traffic from a single interface, including Ethernet, 802.11a/b/g/n wireless and VoIP
- It provides a comprehensive view of all **wireless network activity** showing each wireless network, the APs comprising that network, and the users connected to each AP
- OmniPeek **provides a comprehensive network monitoring** dashboard for wireless networks, including real-time throughput, signal strength, top talkers and current activity

http://www.wildpackets.com

Wi-Fi Packet Sniffer: OmniPeek

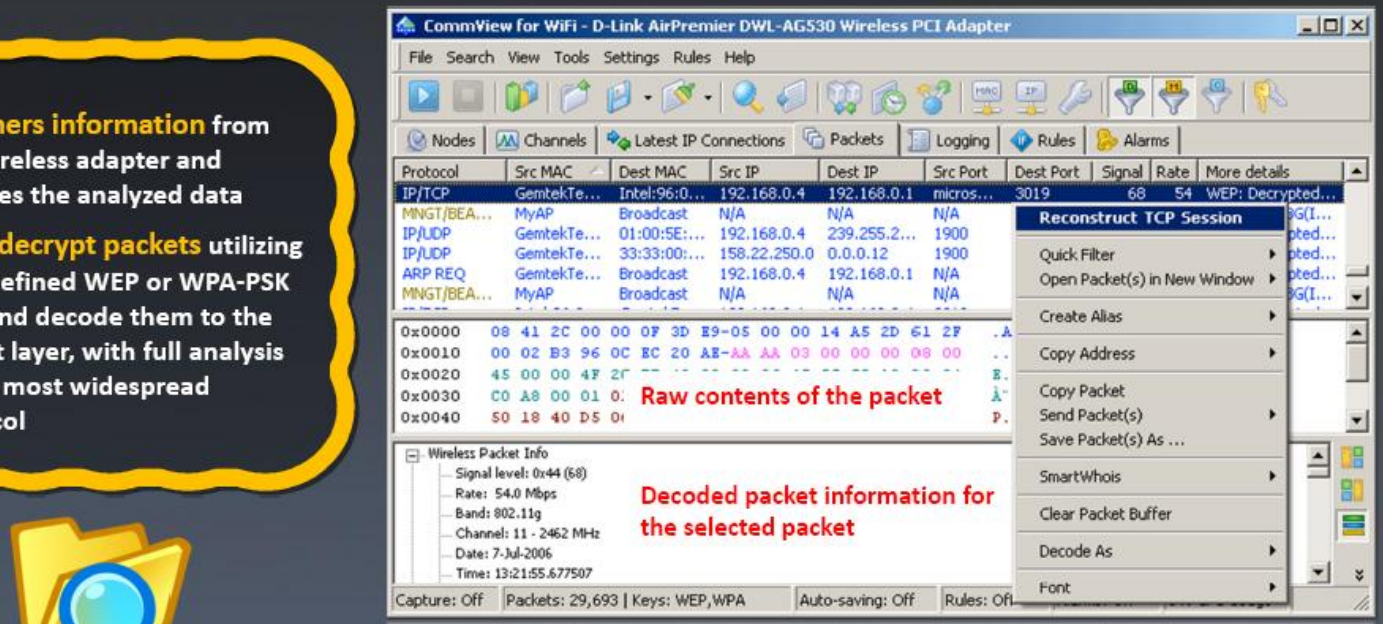


Wi-Fi Packet Sniffer: CommView for Wi-Fi

CommView for Wi-Fi is designed for capturing and analyzing network packets on wireless 802.11a/b/g/n networks

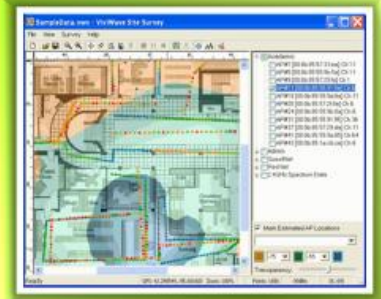
It gathers information from the wireless adapter and decodes the analyzed data

It can decrypt packets utilizing user-defined WEP or WPA-PSK keys and decode them to the lowest layer, with full analysis of the most widespread protocol



What is Spectrum Analysis?

RF spectrum analyzers examine the Wi-Fi radio transmission and measure the power (amplitude) of radio signals and RF pulses, and transform these measurements into numeric sequences



Spectrum analyzers **employ statistical analysis** to plot spectral usage, quantify "air quality," and isolate transmission sources

RF spectrum analyzers are used by RF technicians to install and maintain wireless networks, and identify **sources of interference**

Wi-Fi spectrum analysis also helps in **wireless attack detection**, including Denial of Service attacks, authentication/ encryptions attacks, network penetration attacks, etc.

Spectrum analysis tools: Wi-Spy and Chanalyzer, **AirMagnet Wi-Fi Analyzer**, WifiEagle, etc.

CEH Certified Ethical Hacker

Wireless Sniffers

ApSniff
http://www.monolith81.de

WifiScanner
http://wifiscanner.sourceforge.net

NetworkMiner
http://networkminer.sourceforge.net

Mognet
http://www.monolith81.de

Airscanner Mobile Sniffer
http://www.airscanner.com

AirTraf
http://airtraf.sourceforge.net

Observer
http://www.networkinstruments.com

Prism2Dump
http://www.dachb0den.com


Wireless Hacking Methodology
Wi-Fi Discovery
GPS Mapping
Wireless Traffic Analysis
Launch Wireless Attacks
Crack Wi-Fi Encryption
Compromise the Wi-Fi Network
The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources
CEH
Certified Ethical Hacker
82
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Aircrack-ng Suite

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

Airbase-ng
Captures WPA/WPA2 handshake and can act as an ad-hoc Access Point

Aircrack-ng
Defacto WEP and WPA/ WPA2-PSK cracking tool

Airdecap-ng
Decrypt WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets

Airdecloak-ng
Removes WEP cloaking from a pcap file

Airdriver-ng
Provides status information about the wireless drivers on your system

Airdrop-ng
This program is used for targeted, rule-based deauthentication of users

Aireplay-ng
Used for traffic generation, fake authentication, packet replay, and ARP request injection

Airgraph-ng
Creates client to AP relationship and common probe graph from airodump file

Airodump-ng
Used capture packets of raw 802.11 frames and collect WEP IVs

Airolib-ng
Store and manage essid and password lists used in WPA/ WPA2 cracking

Airserv-ng
Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection

Airmon-ng
Used to enable monitor mode on wireless interfaces from managed mode and vice versa

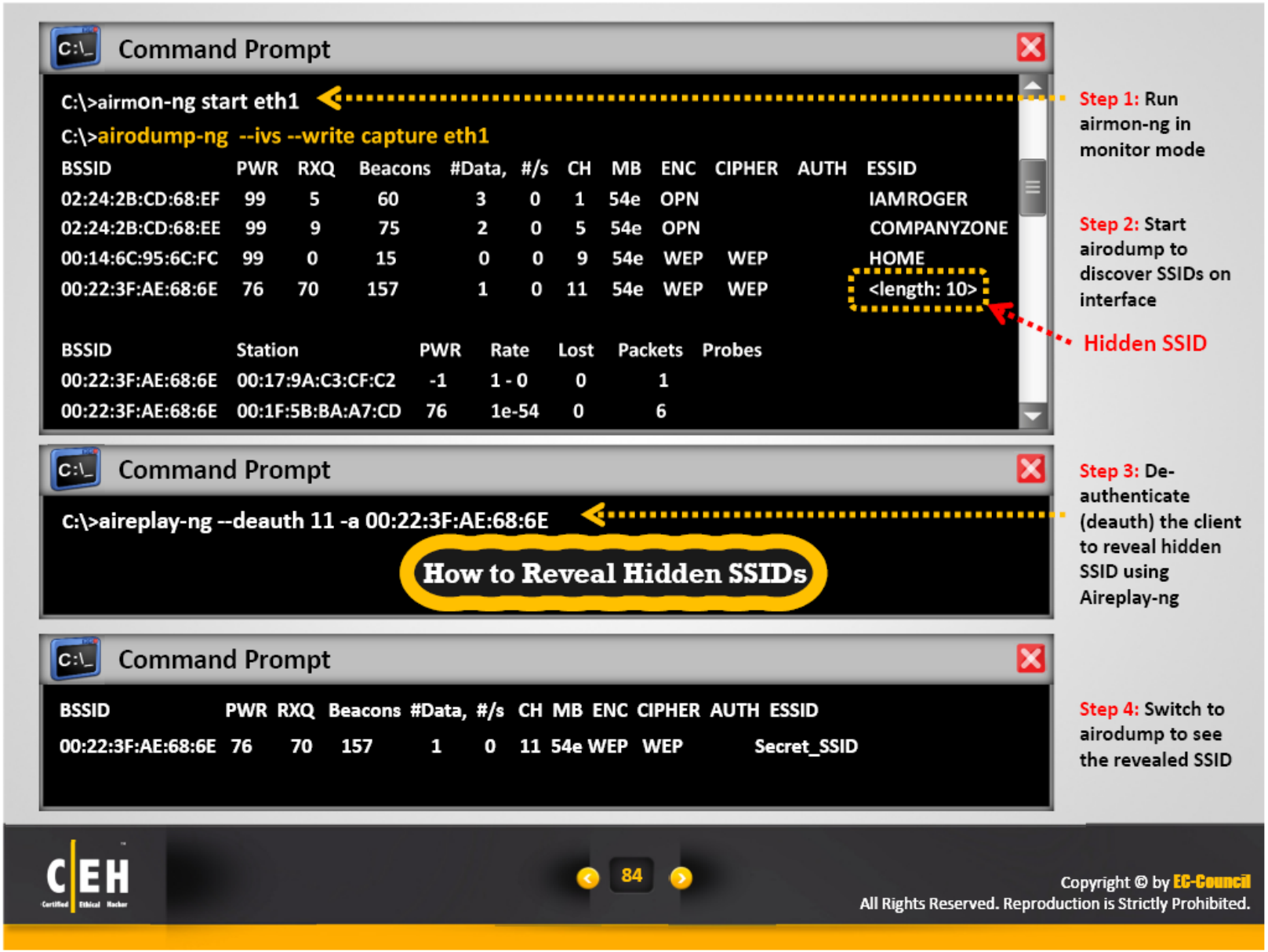
Airtun-ng
Injects frames into a WPA TKIP network with QoS, and can recover MIC key and keystram from Wi-Fi traffic

Easside-ng
Allows you to communicate via a WEP-encrypted access point (AP) without knowing the WEP key

Packetforge-ng
Used create encrypted packets that can subsequently be used for injection

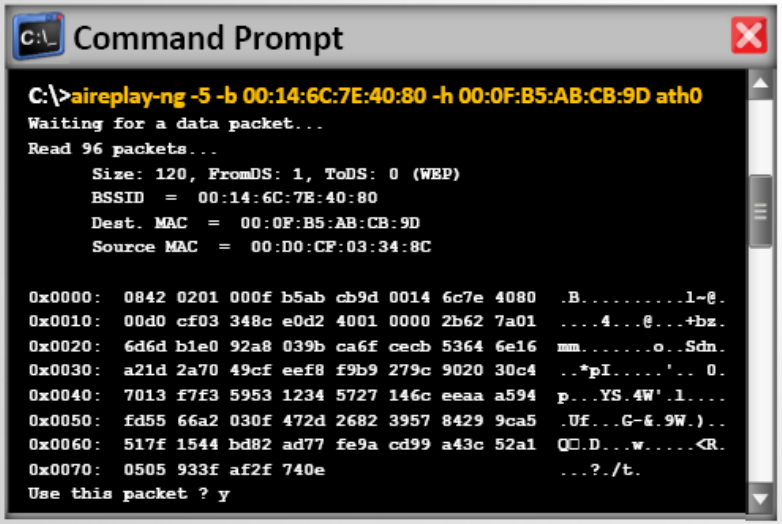
Tkiptun-ng
Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network

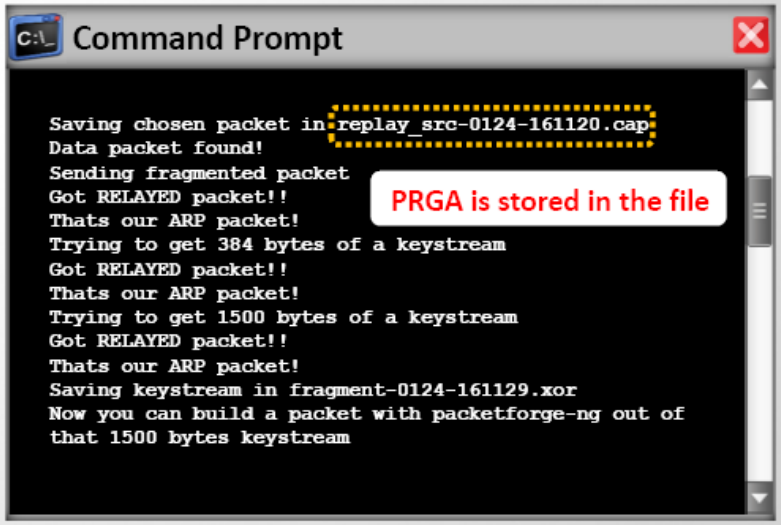
Wesside-ng
Incorporates a number of techniques to seamlessly obtain a WEP key in minutes


Command Prompt
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
02:24:2B:CD:68:EF 99 5 60 3 0 1 54e OPN IAMROGER
02:24:2B:CD:68:EE 99 9 75 2 0 5 54e OPN COMPANYZONE
00:14:6C:95:6C:FC 99 0 15 0 0 9 54e WEP WEP HOME
00:22:3F:AE:68:6E 76 70 157 1 0 11 54e WEP WEP <length: 10>
BSSID Station PWR Rate Lost Packets Probes
00:22:3F:AE:68:6E 00:17:9A:C3:CF:C2 -1 1 - 0 0 1
00:22:3F:AE:68:6E 00:1F:5B:BA:A7:CD 76 1e-54 0 6
Step 1: Run airmon-ng in monitor mode
Step 2: Start airodump to discover SSIDs on interface
Hidden SSID
Command Prompt
C:\>aireplay-ng --deauth 11 -a 00:22:3F:AE:68:6E
How to Reveal Hidden SSIDs
Step 3: De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng
Command Prompt
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:22:3F:AE:68:6E 76 70 157 1 0 11 54e WEP WEP Secret_SSID
Step 4: Switch to airodump to see the revealed SSID
C|EH
84
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack

- A fragmentation attack, when successful, can obtain **1500 bytes of PRGA** (pseudo random generation algorithm)
- This attack **does not recover** the WEP key itself, but merely obtains the PRGA
- The PRGA can then be used to generate packets with **packetforge-ng** which are in turn used for various injection attacks
- It requires at least **one data packet** to be received from the access point in order to initiate the attack

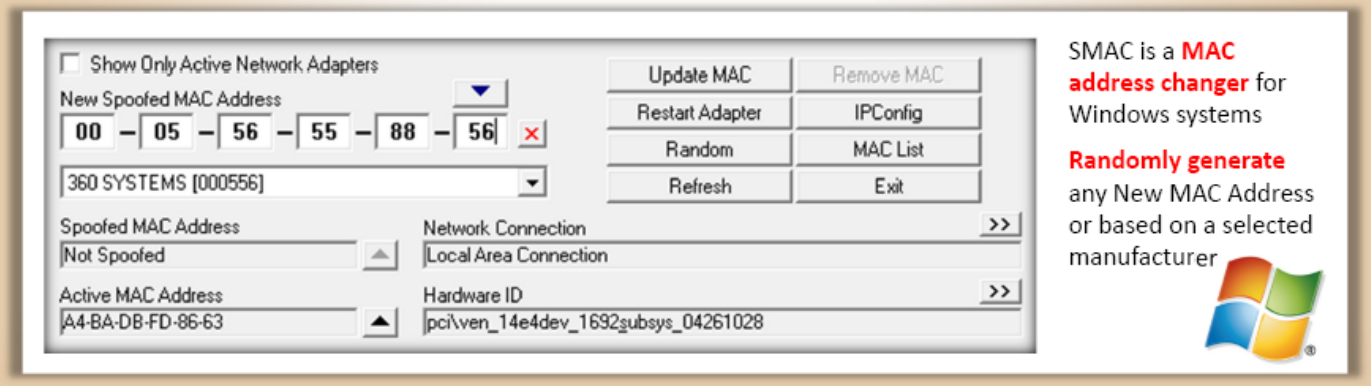




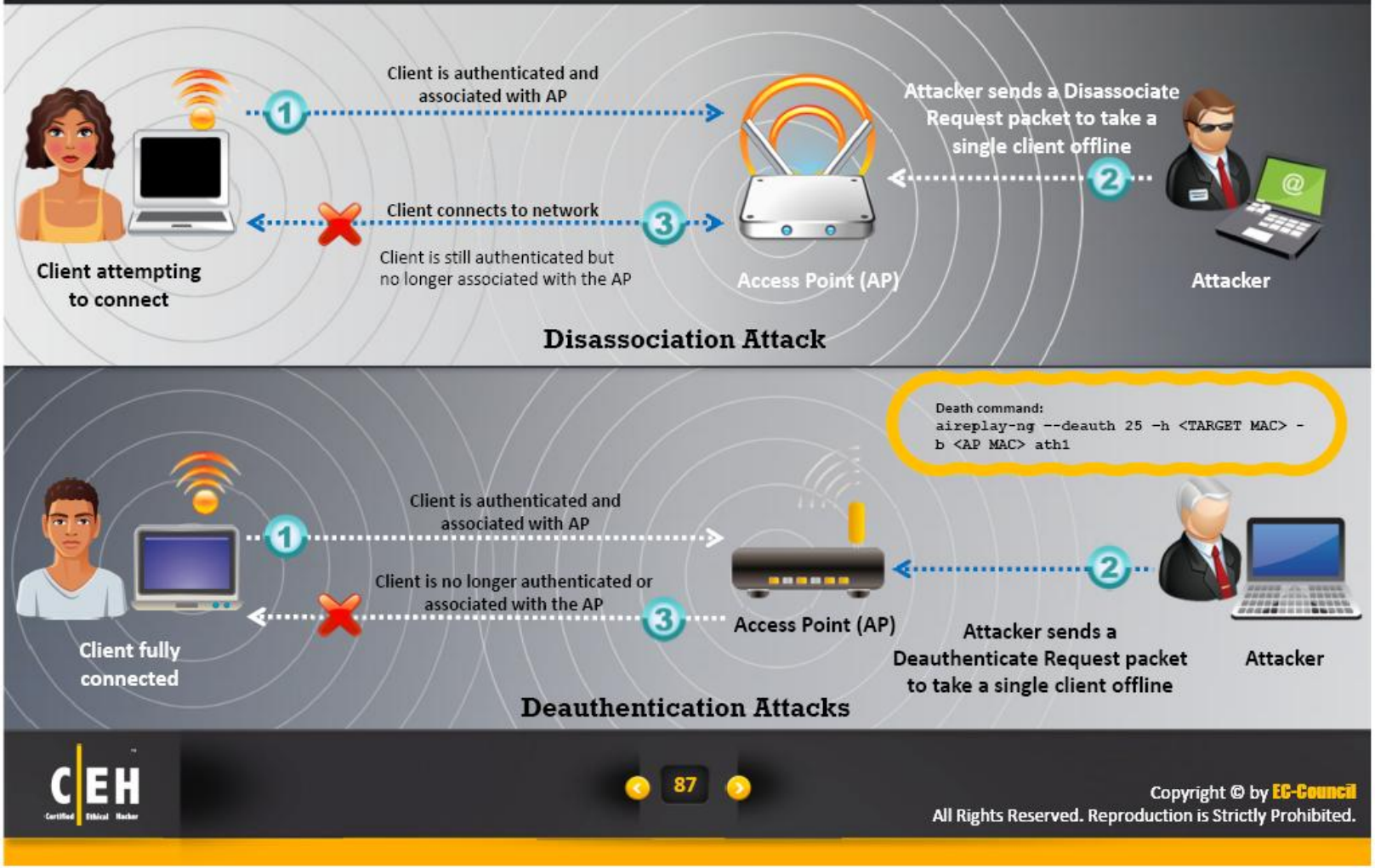
Use PRGA with packetforge-ng to generate packet(s) to be used for various **injection attacks**

How to Launch MAC Spoofing Attack?

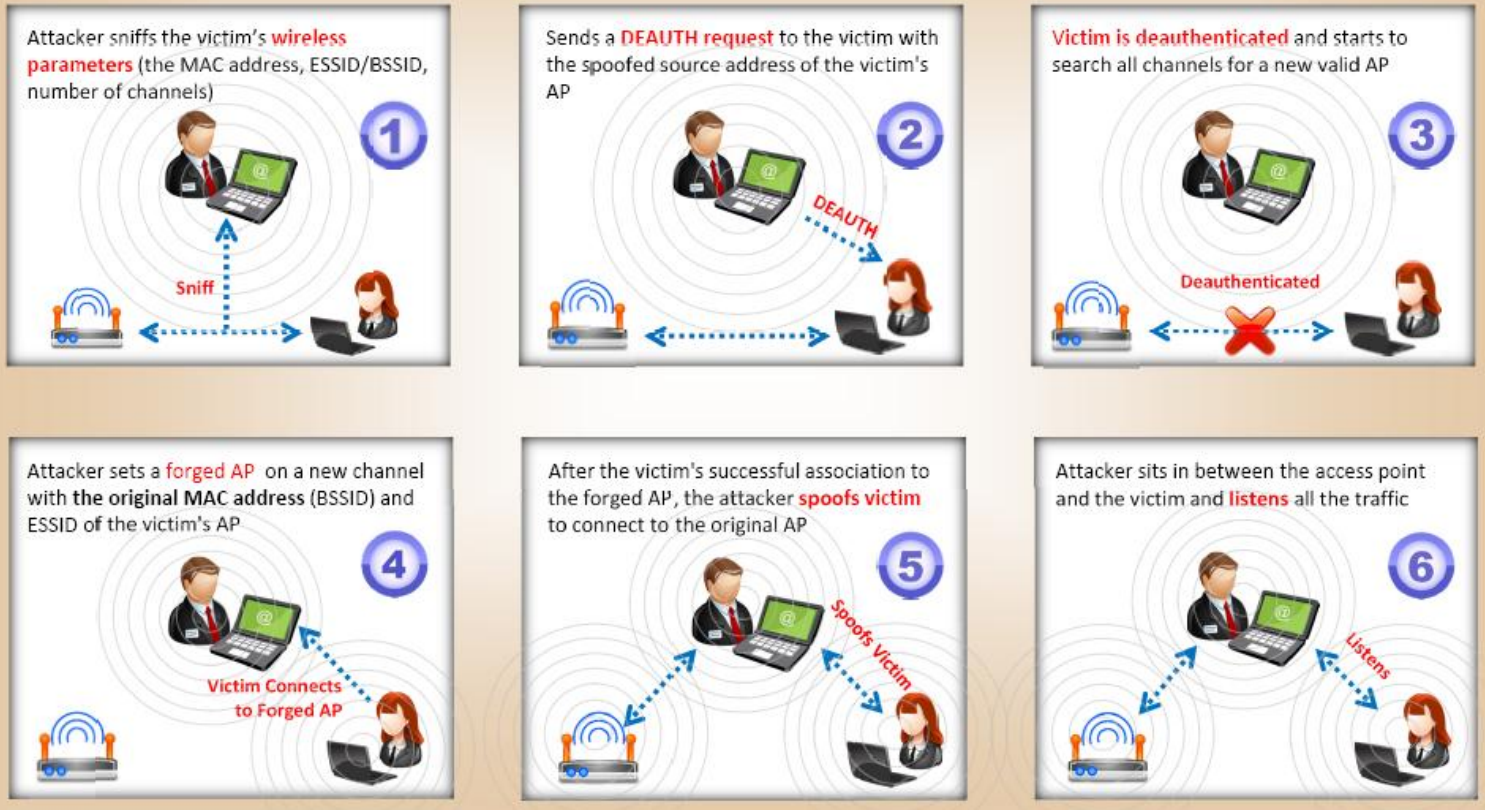
MAC spoofing attackers change the MAC address to that of an authenticated user to bypass the MAC filtering configured in an access point



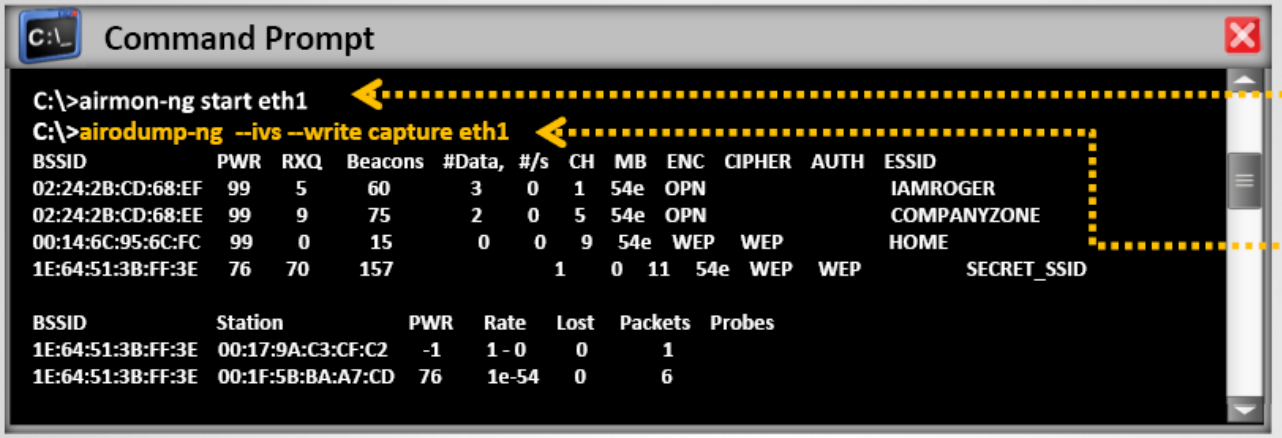
Denial of Service: Deauthentication and Disassociation Attacks



Man-in-the-Middle Attack



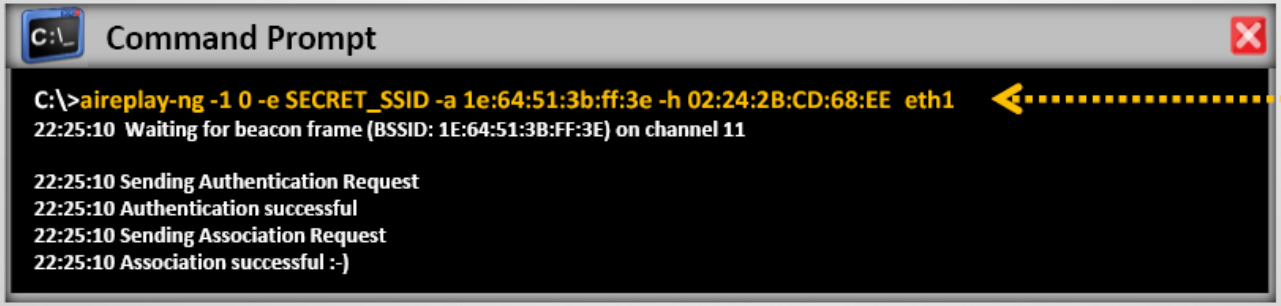
MITM Attack Using Aircrack-ng



Step 1: Run airmon-ng in monitor mode

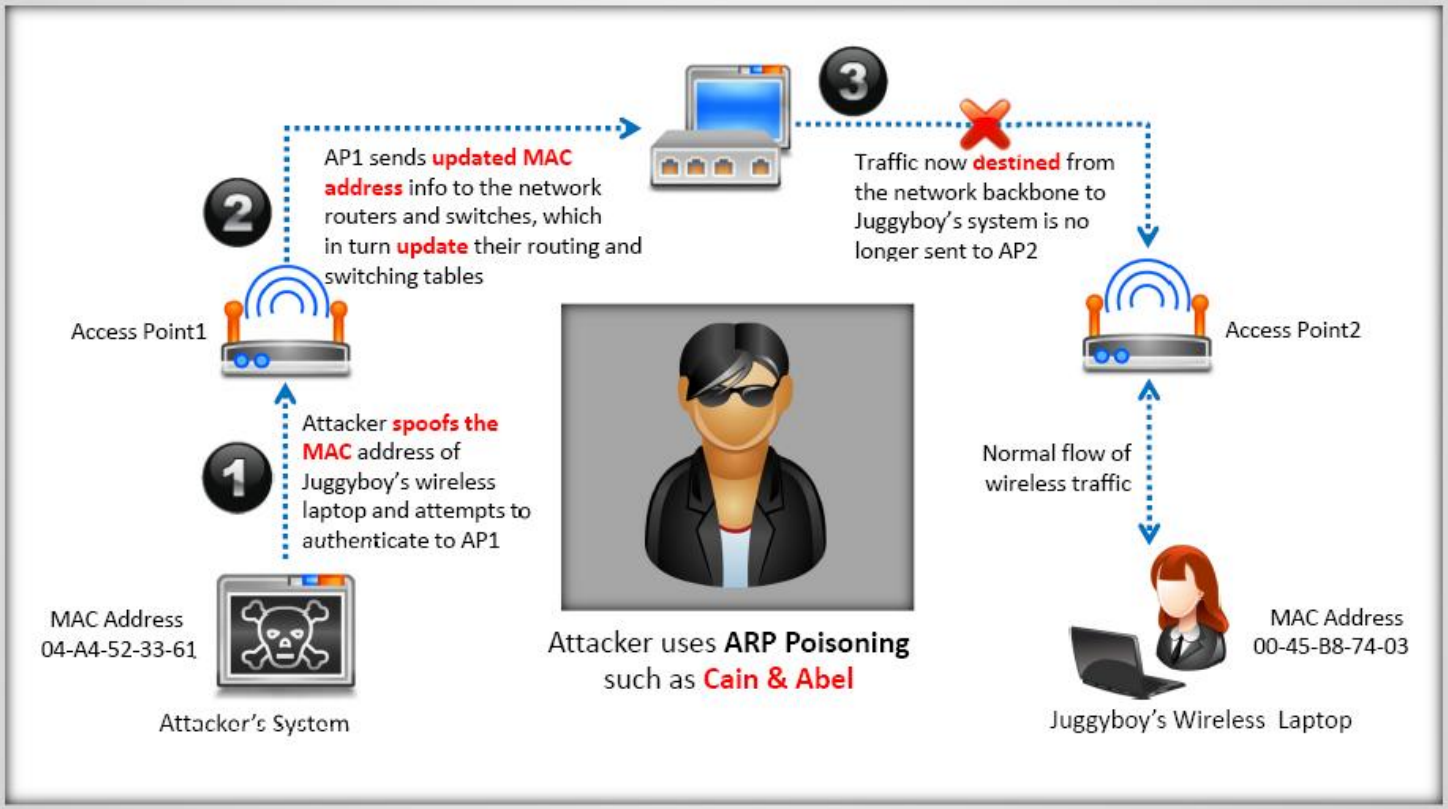
Step 2: Start airodump to discover SSIDs on interface

Step 3: De-authenticate (deauth) the client using Aireplay-ng



Step 4: Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng

Wireless ARP Poisoning Attack



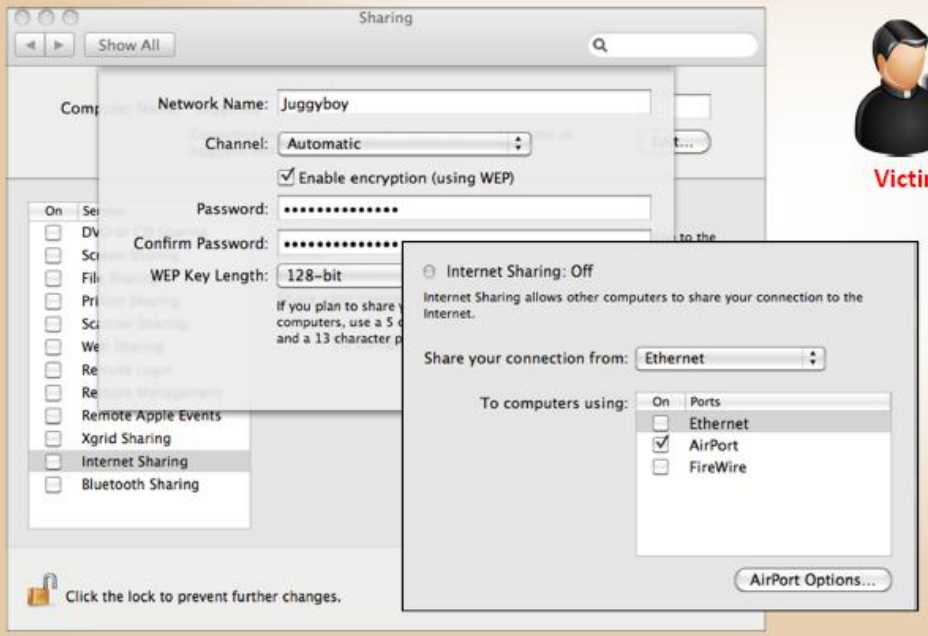
Rogue Access Point

Evil Twin

Wi-Fi is everywhere these days and so are your employees. They take their laptops to Starbucks, to FedEx Office, and to the airport. How do you keep the company data safe?

How to Set Up a Fake Hotspot (Evil Twin)?

1. You will need a laptop with Internet connectivity (3G or wired connection) and a mini access point
2. Enable Internet Connection Sharing in Windows 7 or Internet Sharing in Mac OS X
3. Broadcast your Wi-Fi connection and run a sniffer program to capture passwords



A user tries to log in and finds two access points. One is legitimate, while the other is an identical fake (evil twin). Victim picks one, if it's the fake, the hacker gets login information and access to the computer. In the meantime, the user goes nowhere. He or she probably thinks it was just a login attempt that randomly failed.

How to Crack WEP Using Aircrack?

1. `C:\>airmon-ng start eth1`

STEP 1: Monitor wireless traffic With `airmon-ng`

2. `C:\>airodump-ng --ivs --write capture eth1`

STEP 2: Collect wireless traffic data with `airodump-ng`

3. `C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1`

STEP 3: Associate your wireless card with the AP you are accessing with aireplay-ng

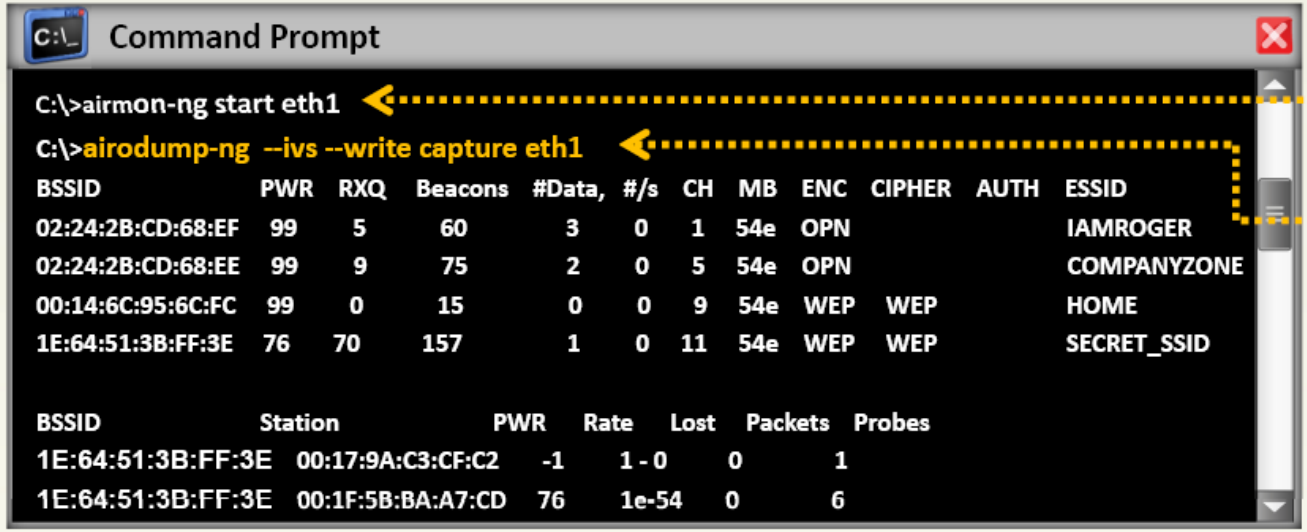
4. `C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1`

STEP 4: Start packet injection with aireplay-ng

5. `C:\>aircrack-ng -s capture.ivs`

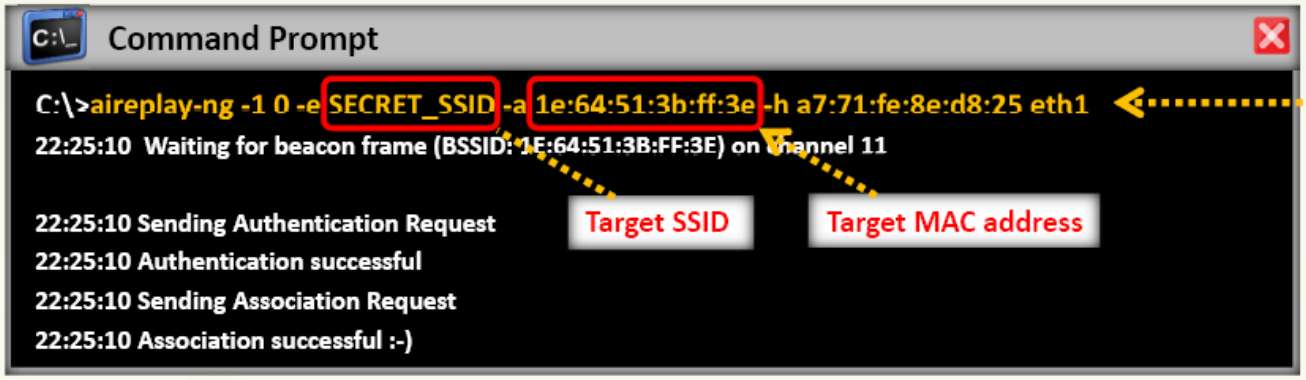
STEP 5: Decrypt the WEP Key with aircrack-ng

How to Crack WEP Using Aircrack? Screenshot 1/2



Step 1: Run airmon-ng in monitor mode

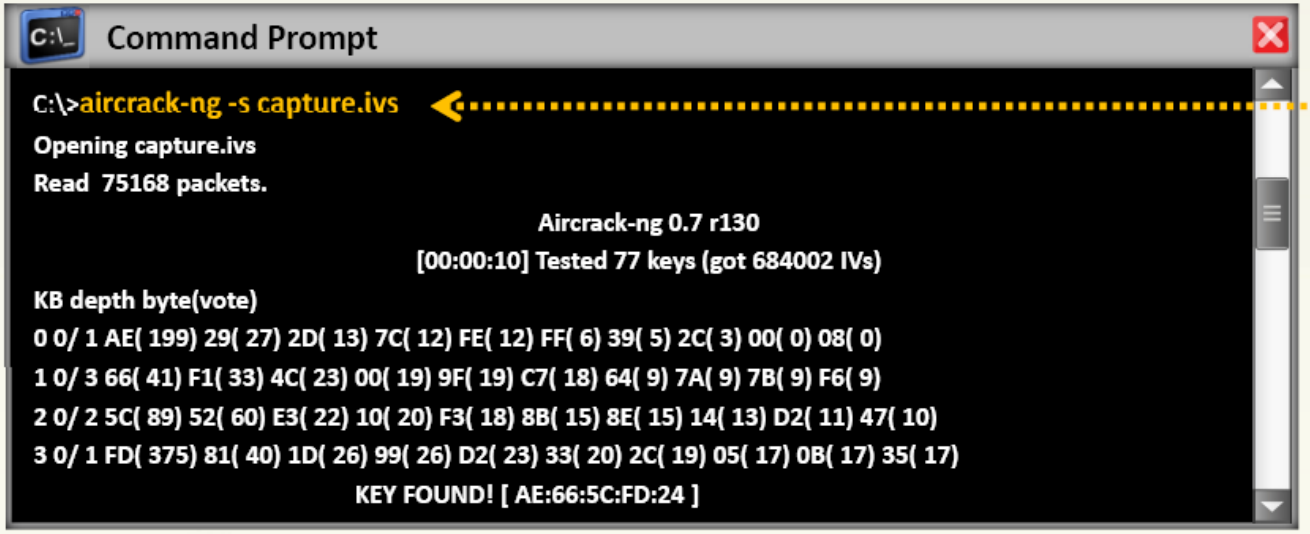
Step 2: Start airodump to discover SSIDs on interface and keep it running. Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.



Step 3: Associate your wireless card with target access point

How to Crack WEP Using Aircrack? Screenshot 2/2

Step 4: Inject packet using aireplay-ng to generate traffic on target access point



Step 5: Wait for airodump-ng to capture more than 50,000 IVs Crack WEP key using aircrack-ng.

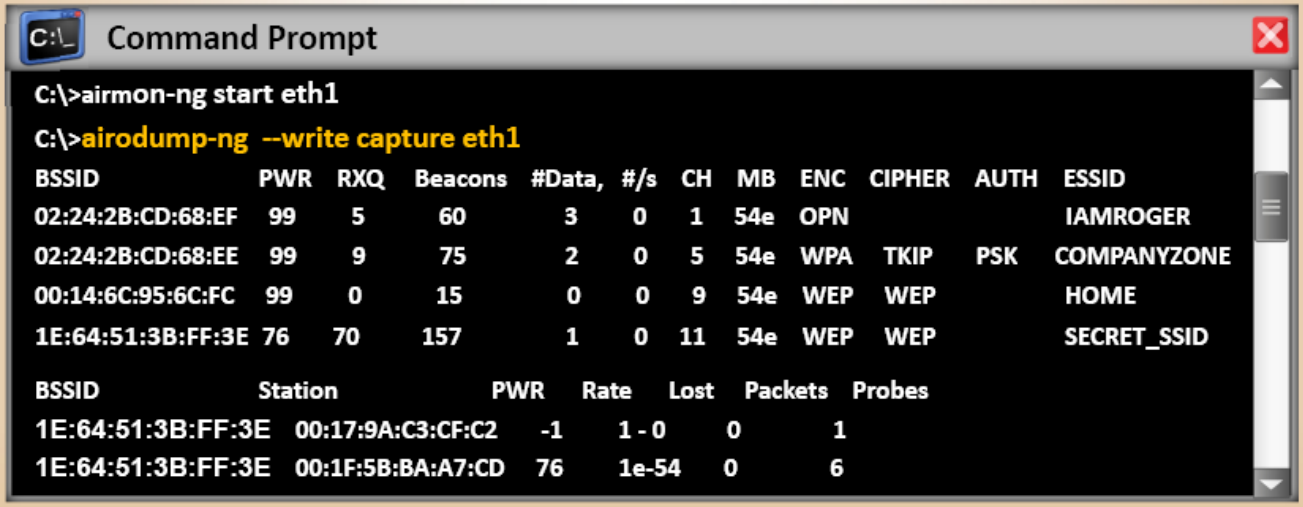
How to Crack WPA-PSK Using Aircrack?

Step 1: Monitor wireless traffic with **airmon-ng**

```
C:\>airmon-ng start eth1
```

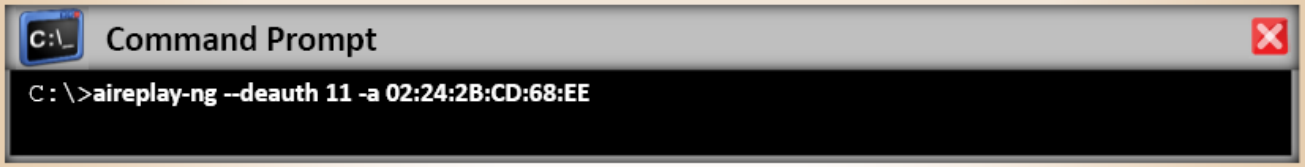
Step 2: Collect wireless traffic data with **airodump-ng**

```
C:\>airodump-ng  --write
capture eth1r
```



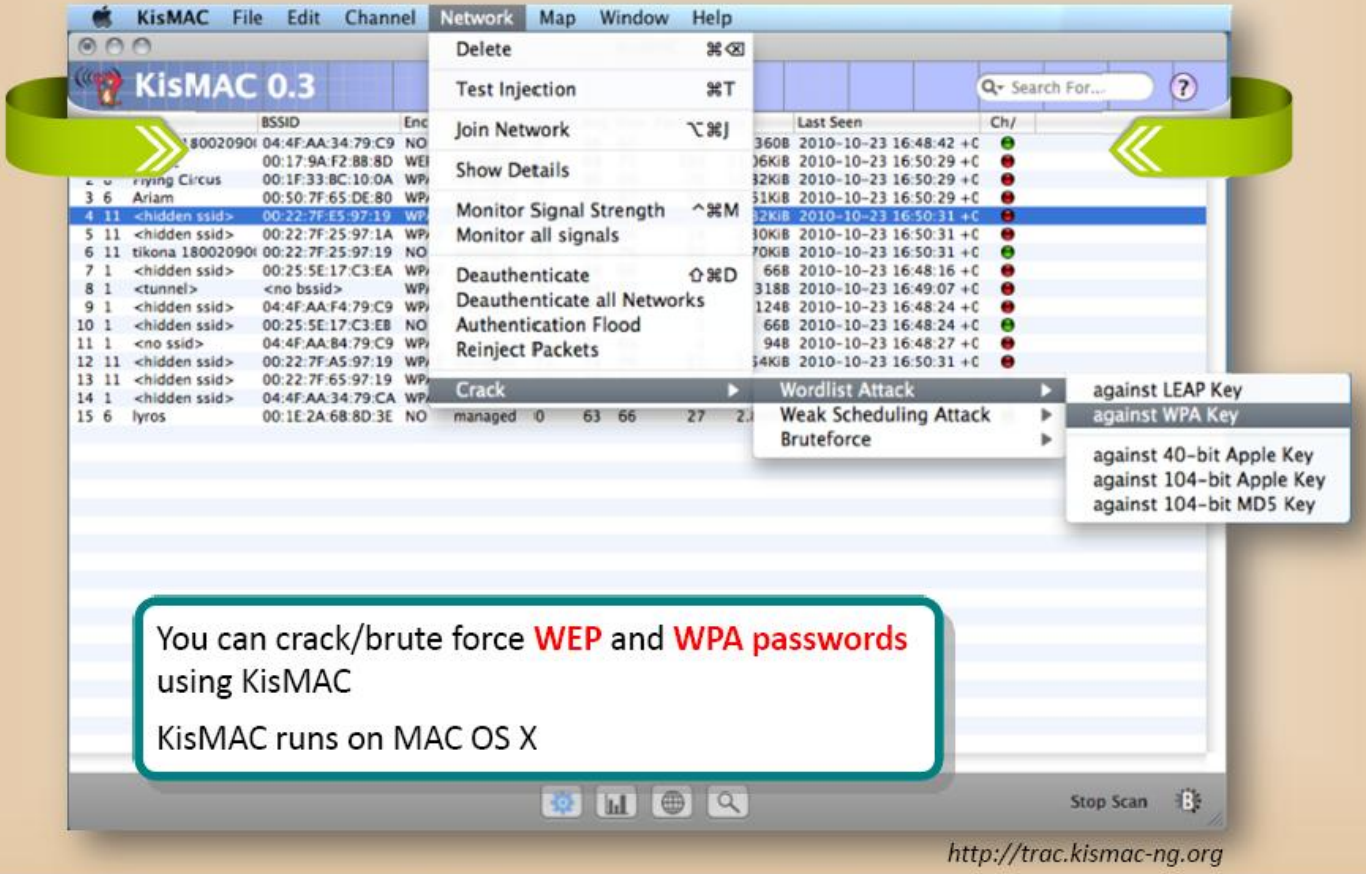
How to Crack WPA-PSK Using Aircrack?

Step 3: De-authenticate (deauth) the client using Aireplay-ng. The client will try to authenticate with AP which will lead to airodump capturing an authentication packet (WPA handshake)



Step 4: Run the capture file through aircrack-ng

WPA Cracking Tool: KisMAC

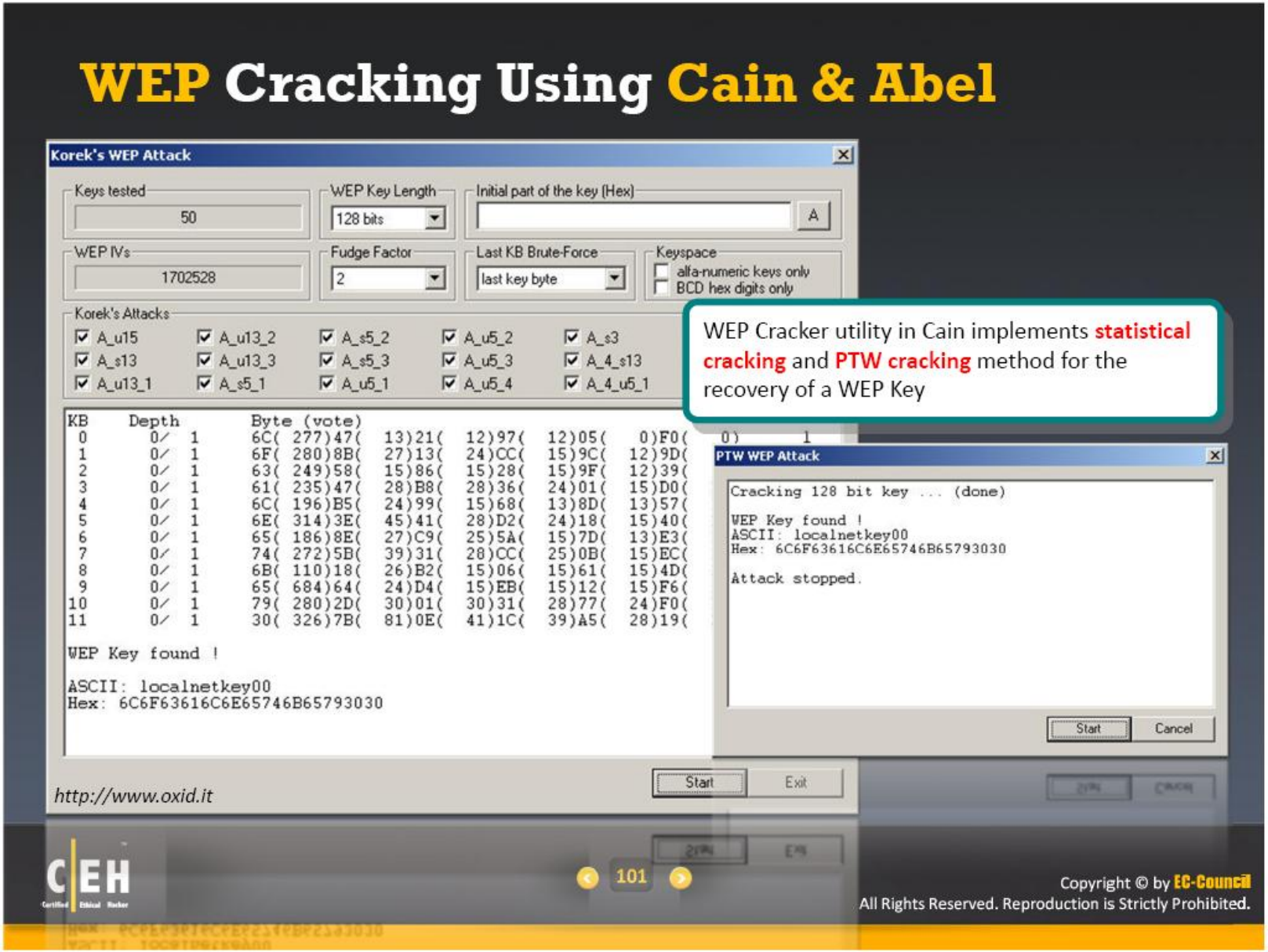


You can crack/brute force **WEP** and **WPA passwords** using KisMAC

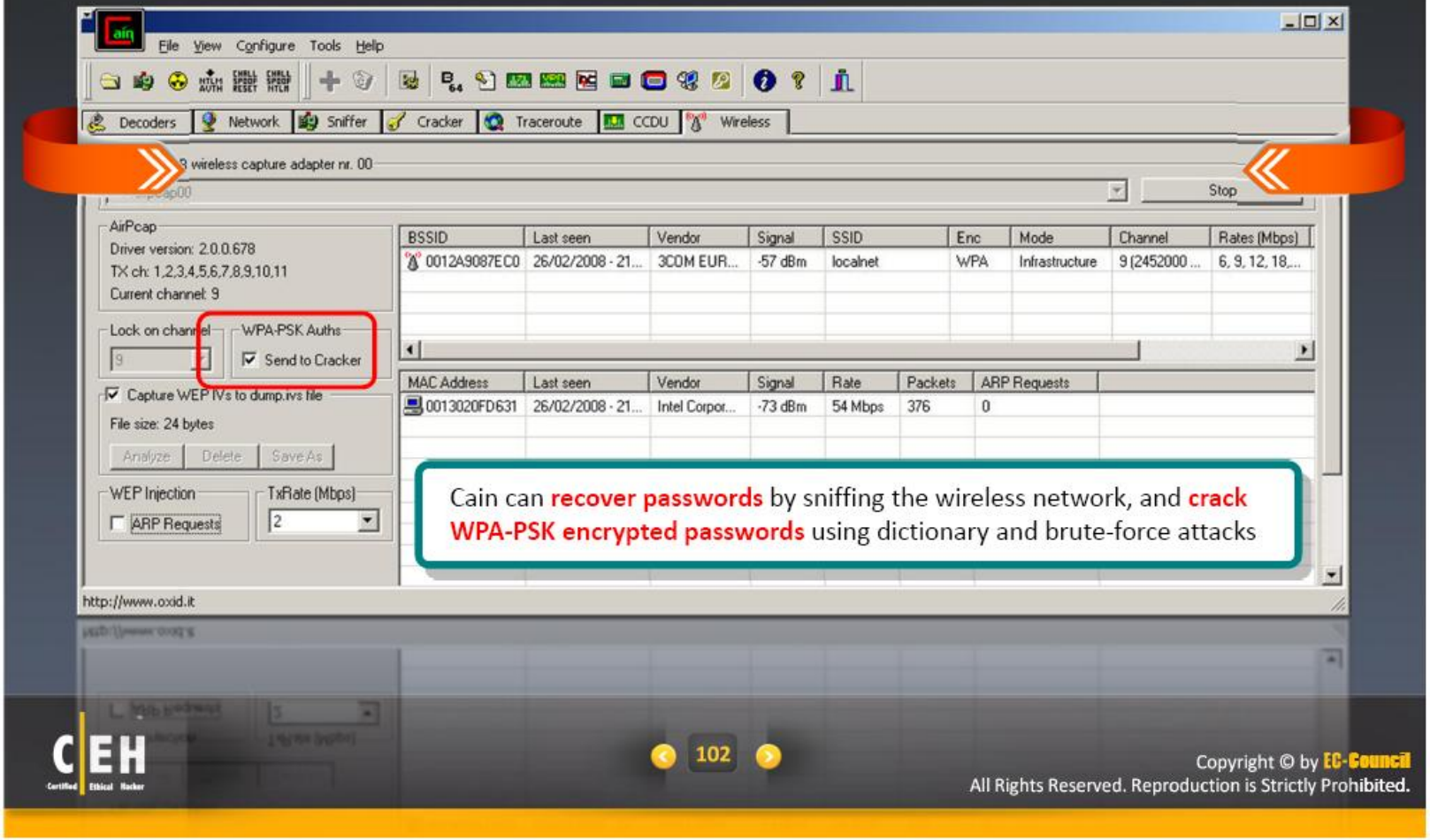
KisMAC runs on MAC OS X

http://trac.kismac-ng.org

WEP Cracking Using Cain & Abel

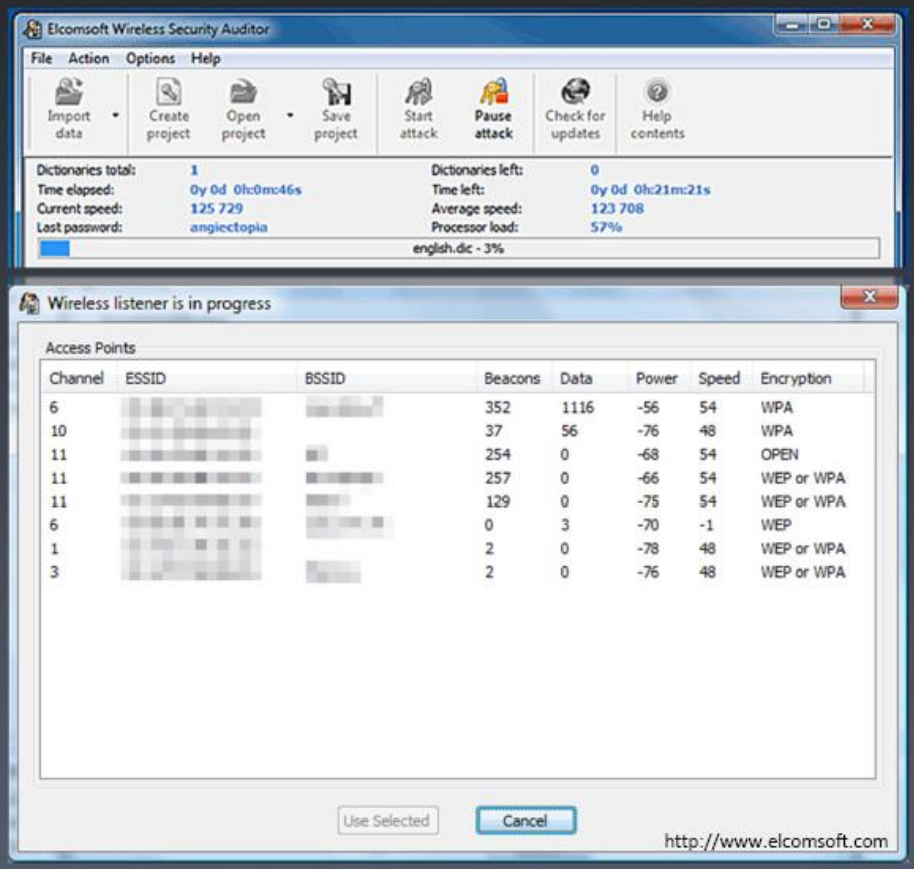


WPA Brute Forcing Using Cain & Abel



WPA Cracking Tool: Elcomsoft Wireless Security Auditor

- Elcomsoft Wireless Security Auditor allows network administrators to audit accessible wireless networks
- It comes with a built-in wireless network sniffer (with AirPcap adapters)
- It tests the strength of WPA/WPA2-PSK passwords protecting your wireless network



WEP/WPA Cracking Tools

jc-wepcracker
http://www.802.11mercenary.net

dwepcrack
http://www.dachb0den.com

WepAttack
http://wepattack.sourceforge.net

Airoway
http://www.xoroz.com

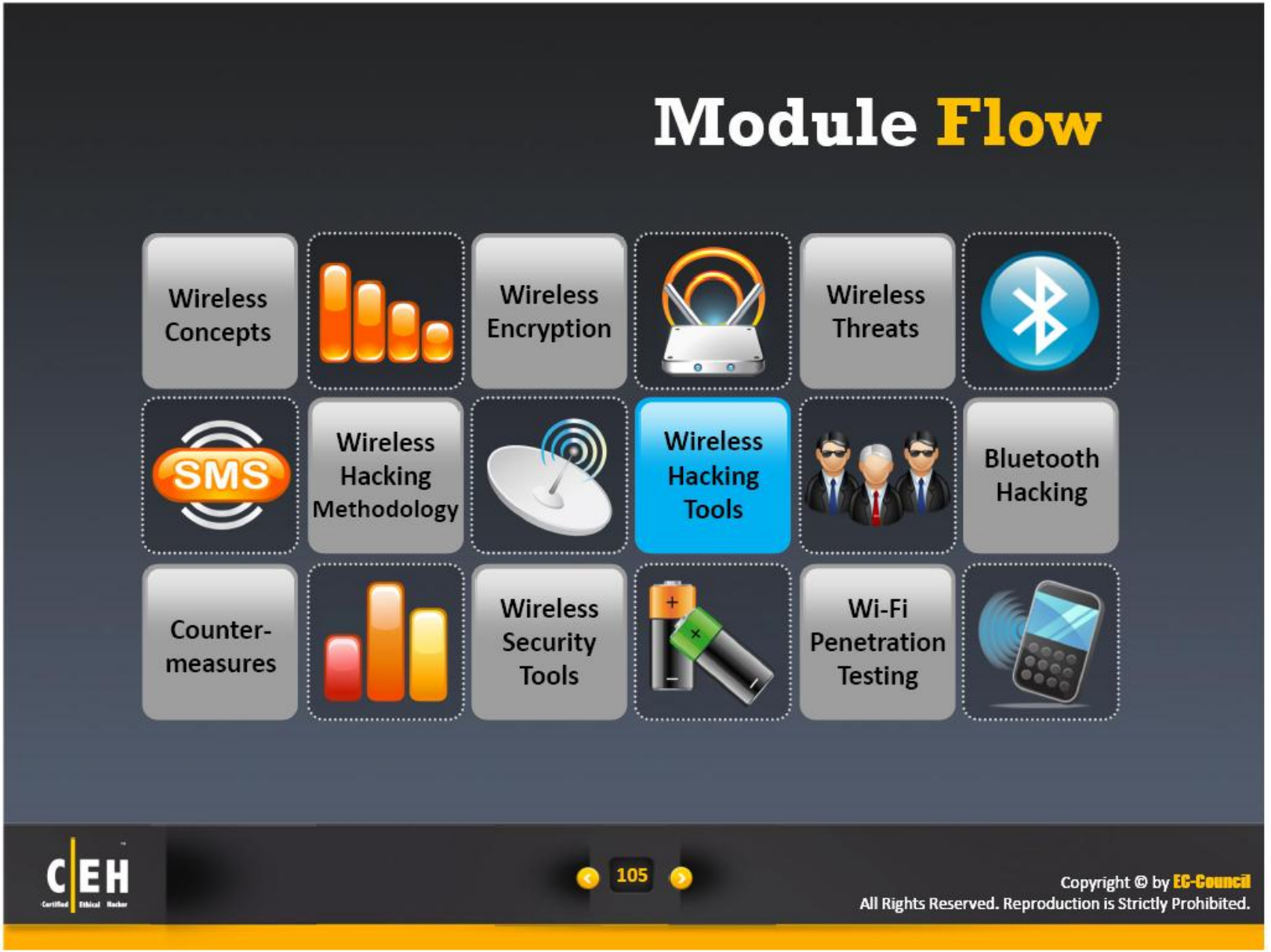
Wesside-ng
http://www.aircrack-ng.org

WEPCrack
http://wepcrack.sourceforge.net

chopchop
http://www.netstumbler.org

WepDecrypt
http://wepdecrypt.sourceforge.net

Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
CEH
105
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Sniffer: Kismet

- It is an 802.11 Layer2 wireless network detector, sniffer, and intrusion detection system
- Identifies networks by passively collecting packets
- Detects hidden networks and presence of nonbeaconing networks via data traffic

http://www.kismetwireless.net

Wardriving Tools

Aerosol
http://www.stolenshoes.net

StumbVerter
http://mikepuchol.com

Airbase
http://www.802.11mercenary.net

MiniStumbler
http://www.stumbler.net

ApSniff
http://www.monolith81.de

Driftnet
http://www.ex-parrot.com

WiFiFoFum
http://wifihopper.com

WarLinux
http://sourceforge.net

RF Monitoring Tools

NetworkManager
http://projects.gnome.org

KWaveControl
http://korinoco.sourceforge.net

KWiFiManager
http://kwifimanager.sourceforge.net

aphunter
http://www.math.ucla.edu

NetworkControl
http://www.arachnoid.com

Qwireless
http://www.uv-ac.de

KOrinoco
http://korinoco.sourceforge.net

WMIinfo
http://zevv.nl

Wi-Fi Connection Manager Tools

Aironet Wireless LAN
http://www.cisco.com

Intel PROSet
http://www.intel.com

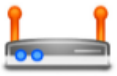
Boingo
http://www.boingo.com

Odyssey Access Client
http://www.juniper.net

HandyWi
http://www.handywi.com

Wireless Zero Config
http://technet.microsoft.com

Mobile Connect
http://www3.ipass.com



QuickLink Mobile
http://www.smithmicro.com

Wi-Fi Traffic Analyzer Tools

Aruba Spectrum Analyzer
http://www.arubanetworks.com

Network Observer
http://www.networkinstruments.com

AirMagnet Handheld Analyzer
http://www.airmagnet.com

Ufasoft Snif
http://www.ufasoft.com

OptiView Network Analyzer
http://www.flukenetworks.com

vxSniffer
http://www.cam.com

Network Packet Analyzer
http://www.javvin.com

Network Assistant
http://www.flukenetworks.com

Wi-Fi Raw Packet Capturing Tools

PCAGizmo
http://pcausa.com

WirelessNetView
http://www.nirsoft.net

Pirni Sniffer
http://code.google.com

Tcpdump
http://www.tcpdump.org

Airview
http://airview.sourceforge.net

Wi-Fi Spectrum Analyzing Tools

Cisco Spectrum Expert
http://www.cisco.com

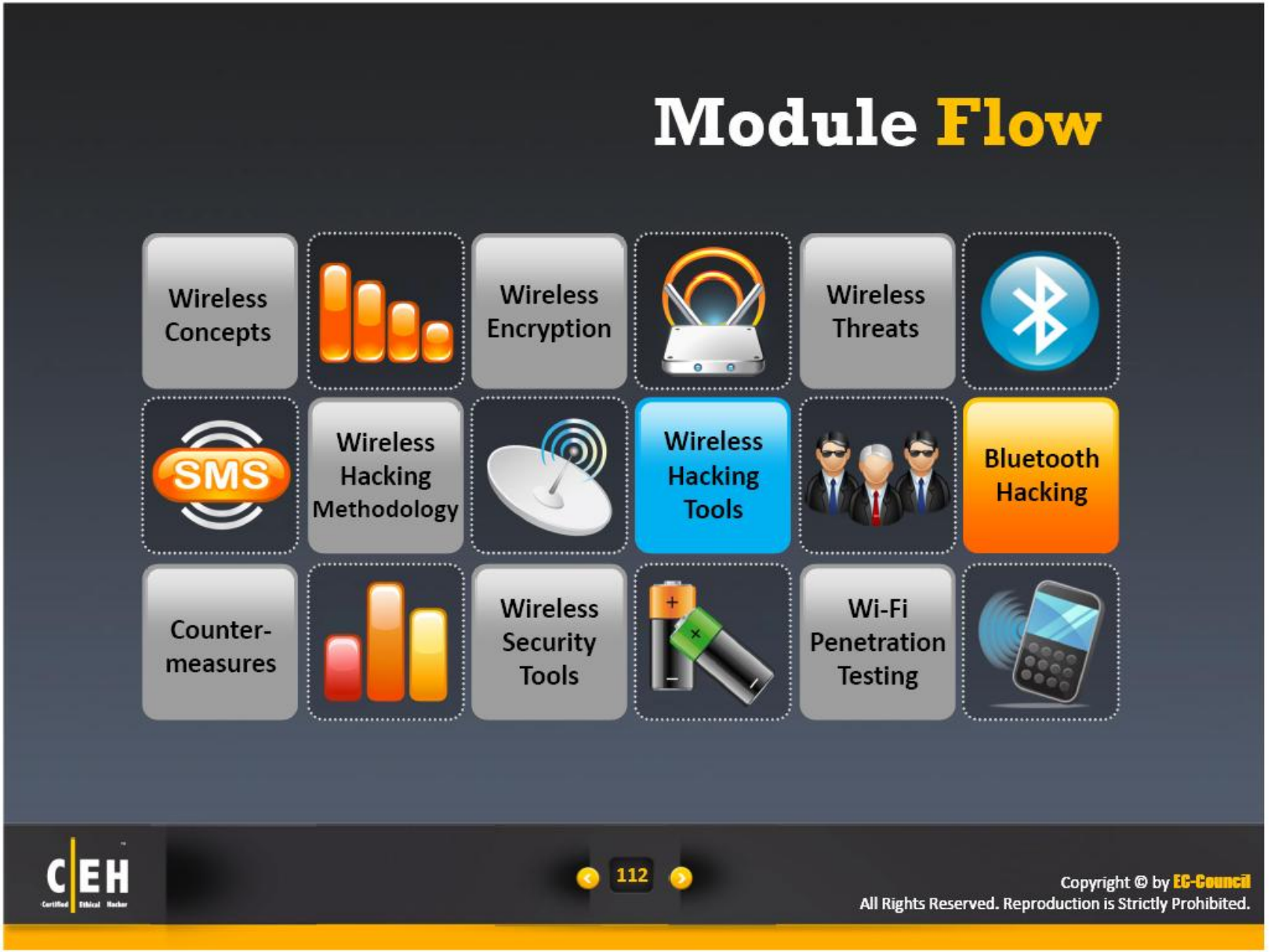
AirMedic
http://www.airmagnet.com

WifiSleuth
http://www.nutsaboutnets.com

BumbleBee
http://www.bvsystems.com

Wi-Spy
http://www.metageek.net

Module Flow

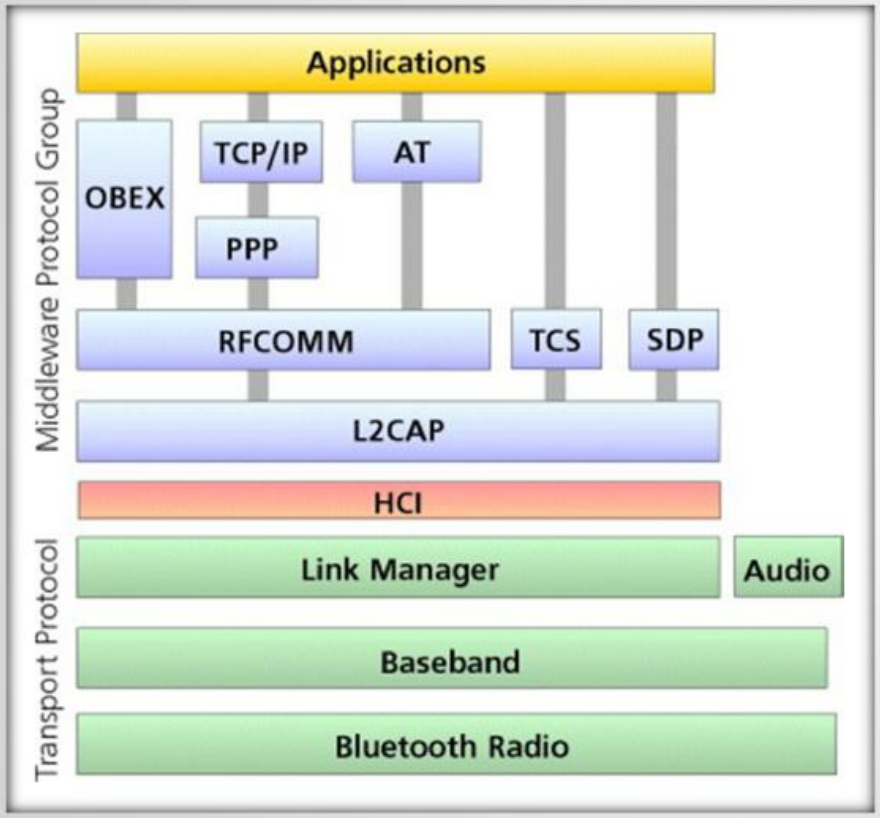

Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
C|EH
Certified Ethical Hacker
112
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking

Bluetooth hacking refers to **exploitation of Bluetooth stack implementation vulnerabilities** to compromise sensitive data in Bluetooth-enabled devices and networks

Bluetooth enabled electronic devices connect and communicate wirelessly through **short-range, ad hoc networks** known as piconets

Bluetooth Stack



Bluetooth modes

Discoverable modes

1. **Discoverable:** Sends inquiry responses to all inquiries
2. **Limited discoverable:** Visible for a certain period of time
3. **Non-discoverable:** Never answers an inquiry scan

Pairing modes

1. **Non-pairable mode:** Rejects every pairing request
2. **Pairable mode:** Will pair upon request

Bluetooth Threats

Leaking calendars and address books
Attacker can steal user's personal information and can use it for malicious purposes

Bugging devices
Attacker could instruct the user to make a phone call to other phones without any user interaction. They could even record the user's conversation

Sending SMS messages
Terrorists could send false bomb threats to airlines using the phones of legitimate users

Causing financial losses
Hackers could send many MMS messages with an international user's phone, resulting in a high phone bill

Remote control
Hackers can remotely control a phone to make phone calls or connect to the Internet

Social engineering
Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information

Malicious code
Mobile phone worms can exploit a Bluetooth connection to replicate and spread itself

Protocol vulnerabilities
Attackers exploit Bluetooth parings and communication protocols to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.

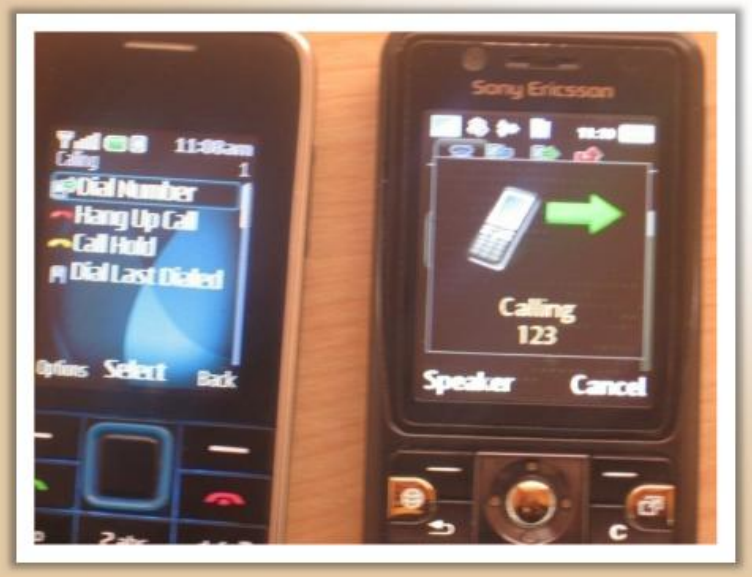
How to BlueJack a Victim?

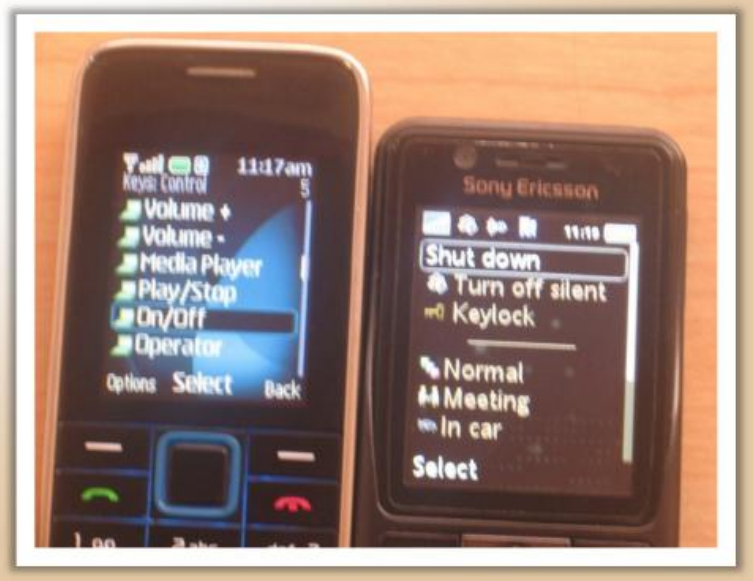
STEP 1	STEP 2	STEP 3	STEP 4
Select an area with plenty of mobile users, like a café, shopping center, etc.	Create a new contact on your phone address book	Save the new contact with the name text and without the telephone number	Choose one phone from the list discovered by Bluetooth and send the contact
Go to contacts in your address book (You can delete this contact entry later)	Enter the message into the name field Ex: "Would you like to go on a date with me?"	Choose "send via Bluetooth". These searches for any Bluetooth device within range	You will get the message "card sent" and then listen for the SMS message tone of your victim's phone

BlueJacking is a new term used to define the activity of sending anonymous messages to other Bluetooth-equipped devices via the OBEX protocol

Bluetooth Hacking Tool: Super Bluetooth Hack

- A Bluetooth Trojan when infected allows the attacker to **control and read information** from victim phone
- Uses **Bluetooth AT commands** to access/hack other Bluetooth-enabled phones
- Once infected, it **enables attackers to read** messages and contacts, change profile, manipulate ringtone, restart or switch off the phone, restore factory settings and make calls from a victim's phone

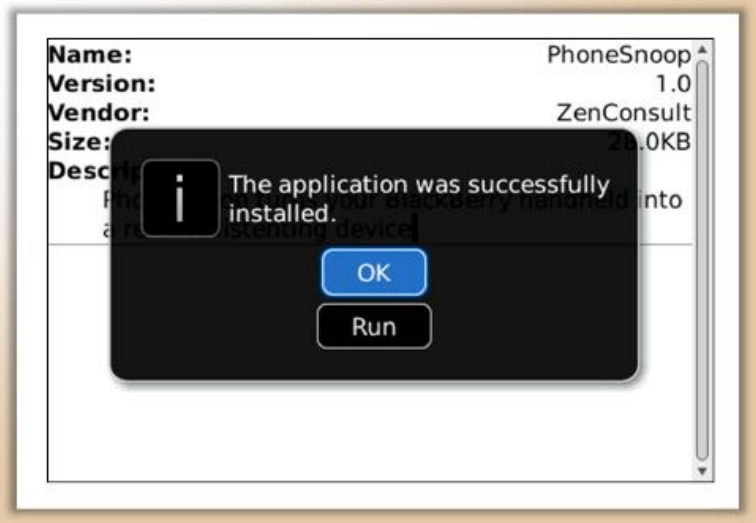




Bluetooth Hacking Tool: PhoneSnoop

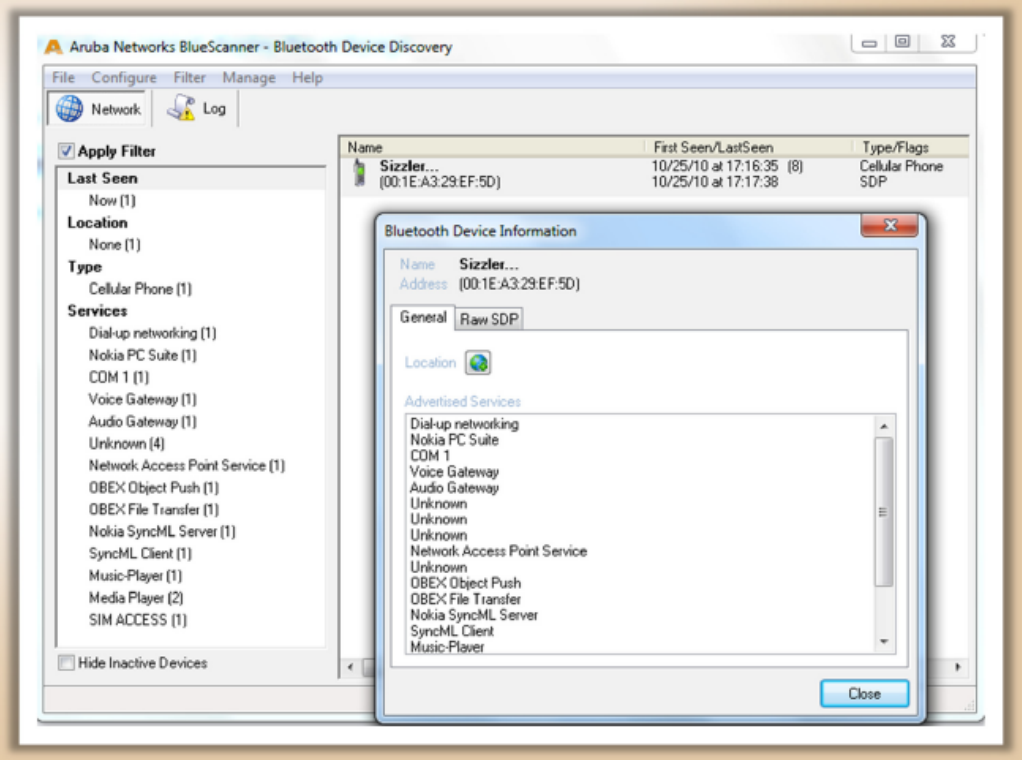
PhoneSnoop is **BlackBerry spyware** that enables an attacker to **remotely activate** the microphone of a BlackBerry handheld and listen to sounds near or around it, PhoneSnoop is a component of Bugs - a proof-of-concept spyware toolkit

It exists **solely to demonstrate** the capabilities of a BlackBerry handheld when used to conduct surveillance on an individual. It is purely a proof-of-concept application and does not possess the stealth or spyware features that could make it malicious



Bluetooth Hacking Tool: BlueScanner

- A **Bluetooth device discovery** and vulnerability assessment tool for Windows
- Discover **Bluetooth devices type** (phone, computer, keyboard, PDA, etc.), and the services that are advertised by the devices
- **Records all information** that can be gathered from the device, without attempting to authenticating with the remote device



Bluetooth Hacking Tools

BTBrowser
http://www.benhui.net

Bluediving
http://bluediving.sourceforge.net

BH Bluejack
http://www.bluejackingtools.com

BTCrack
http://www.nruns.com

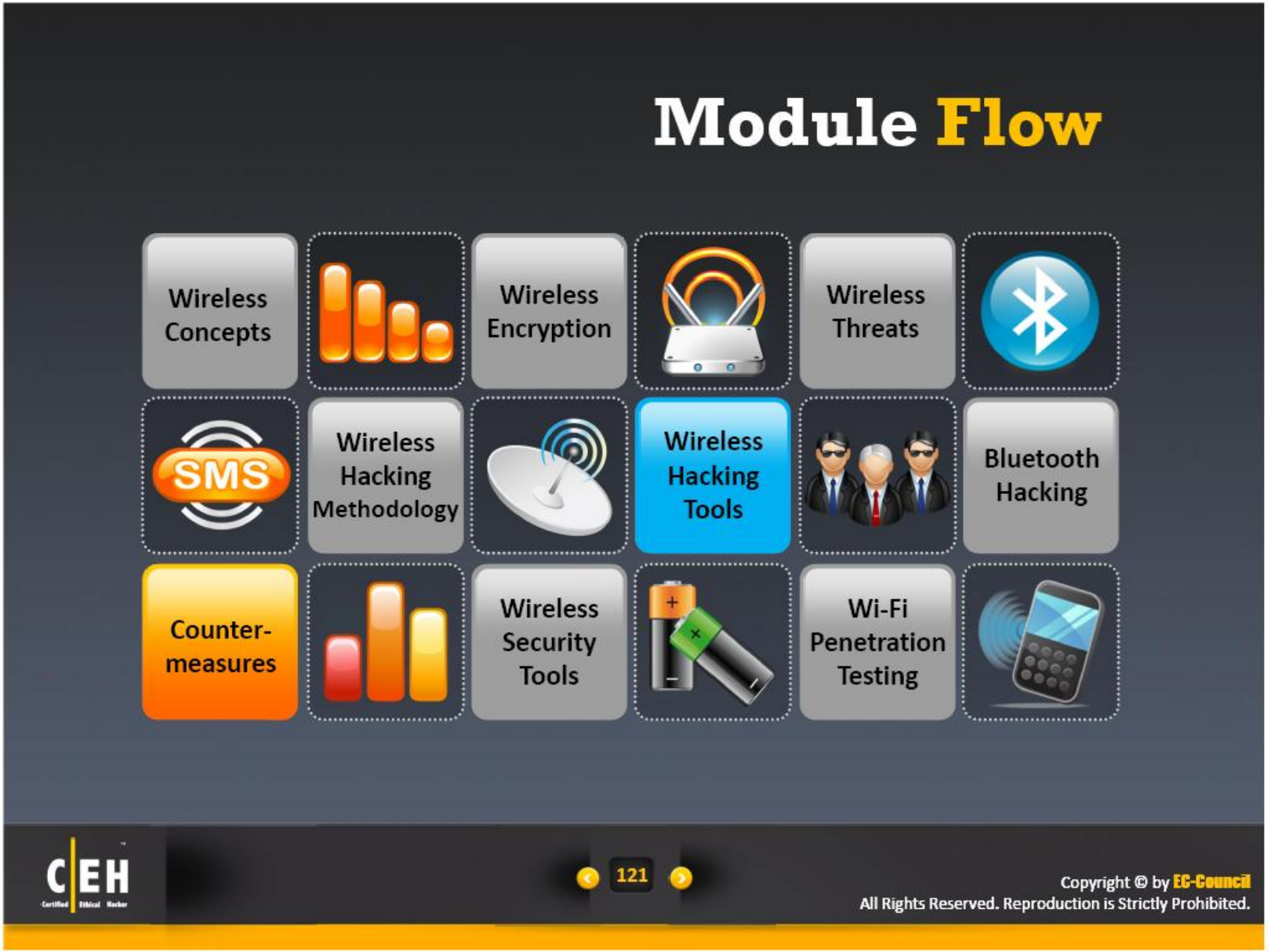
Bluesnarfer
http://www.securiteam.com

Blooover
http://trifinite.org

BTCrawler
http://www.silentservices.de

BTScanner
http://www.pentest.co.uk

Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
CEH
Certified Ethical Hacker
121
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against Bluetooth Hacking?

Use non-regular patterns as PIN keys while pairing a device. Use those key combinations which are non-sequential on the keypad

Keep BT in the **disabled state**, enable it only when needed and disable immediately after the intended task is completed

Always **enable encryption** when establishing BT connection to your PC

Keep the device in **non-discoverable (hidden) mode**

Keep a **check of all paired devices** in the past from time to time and delete any paired device which you are not sure about

DO NOT accept any **unknown and unexpected request** for pairing your device

How to Detect and Block Rogue AP?

Detecting Rogue AP

- **RF scanning**

  Re-purposed access points that do only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area

- **AP scanning**

  Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its MIBS and web interface

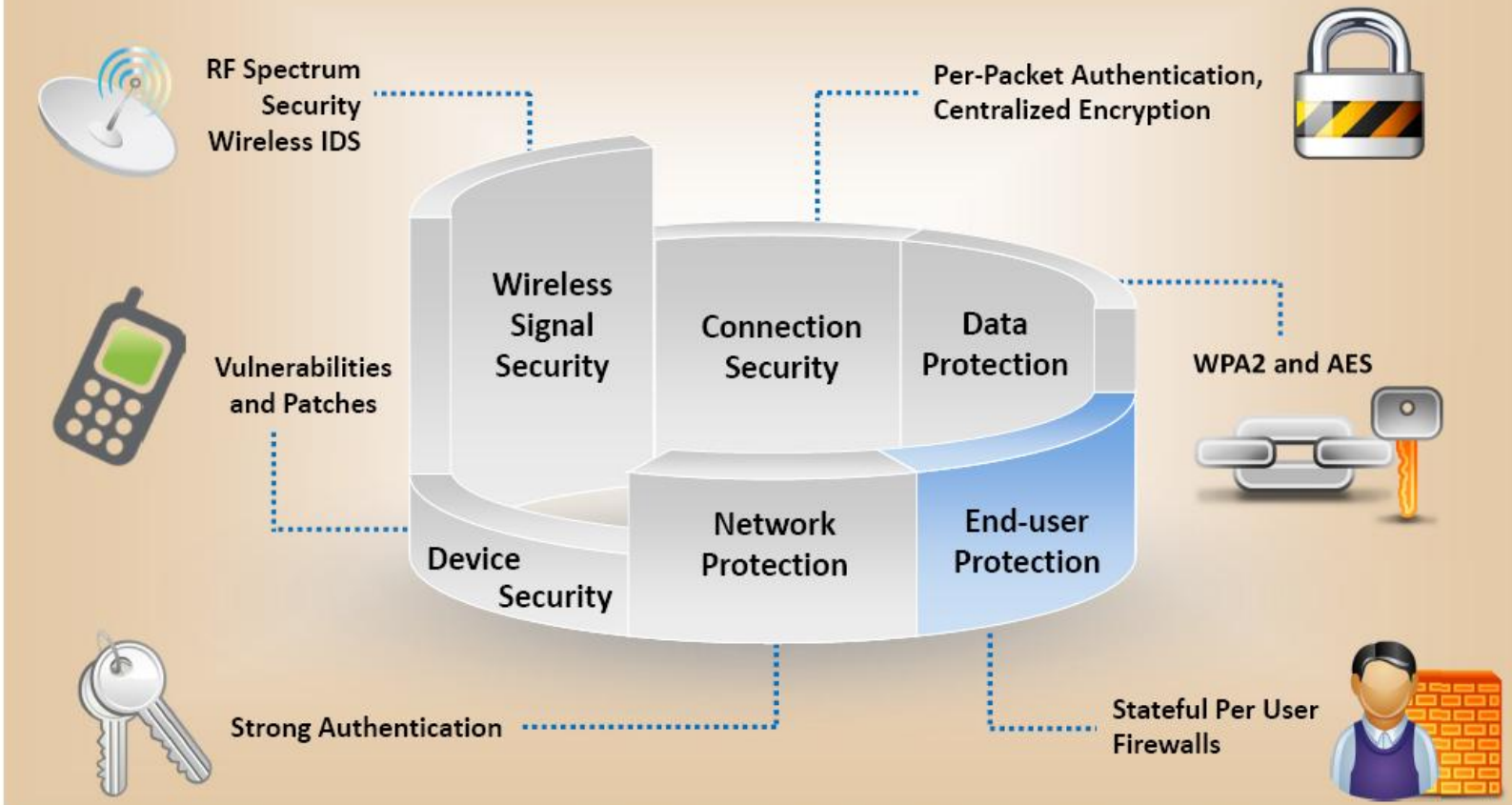
- **Using wired side inputs**

  Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, CDP (Cisco discovery protocol) using multiple protocols

Blocking Rogue AP

- Deny wireless service to new clients by launching a denial-of-service attack (DoS) on the rogue AP
- Block the switch port to which AP is connected or manually locate the AP and pull it physically off the LAN

Wireless Security Layers



How to Defend Against Wireless Attacks?

Wi-Fi Configuration Best Practices

- ✓ Change the default SSID after WLAN configuration
- ✓ Set the router access password and enable firewall protection
- ✗ Disable SSID broadcasts
- ✗ Disable remote router login and wireless administration
- ✓ Enable MAC Address filtering on your access point or router
- ✓ Enable encryption on access point and change passphrase often

How to Defend Against Wireless Attacks?

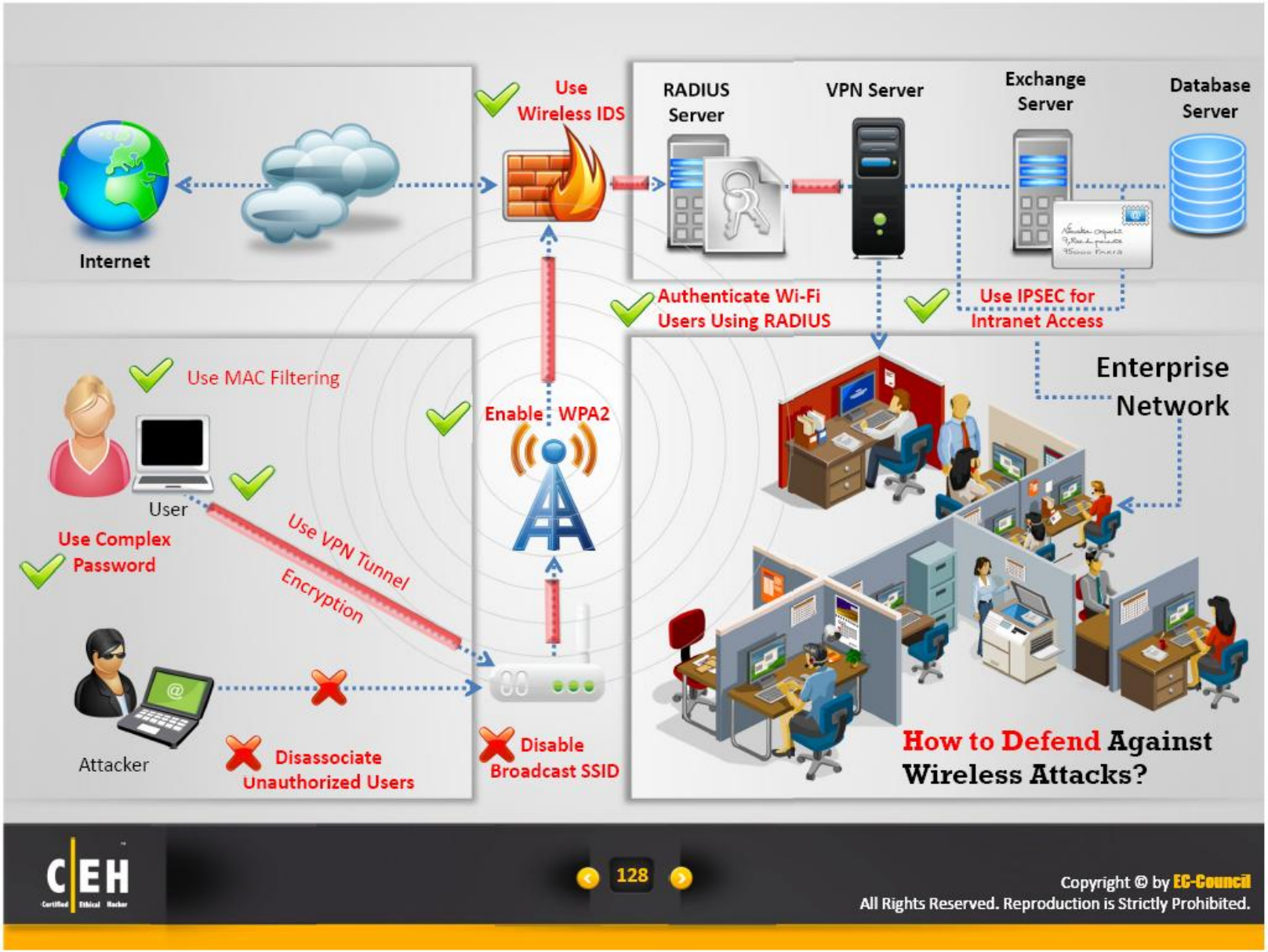
SSID Settings: Best Practices

- Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone
- Do not use your SSID, company name, network name, or any easy to guess string in passphrases
- Place a firewall or packet filter in between the AP and the corporate Intranet
- Limit the strength of the wireless network so it cannot be detected outside the bounds of your organization
- Check the wireless devices for configuration or setup problems regularly
- Implement a different technique for encrypting traffic, such as IPSEC over wireless

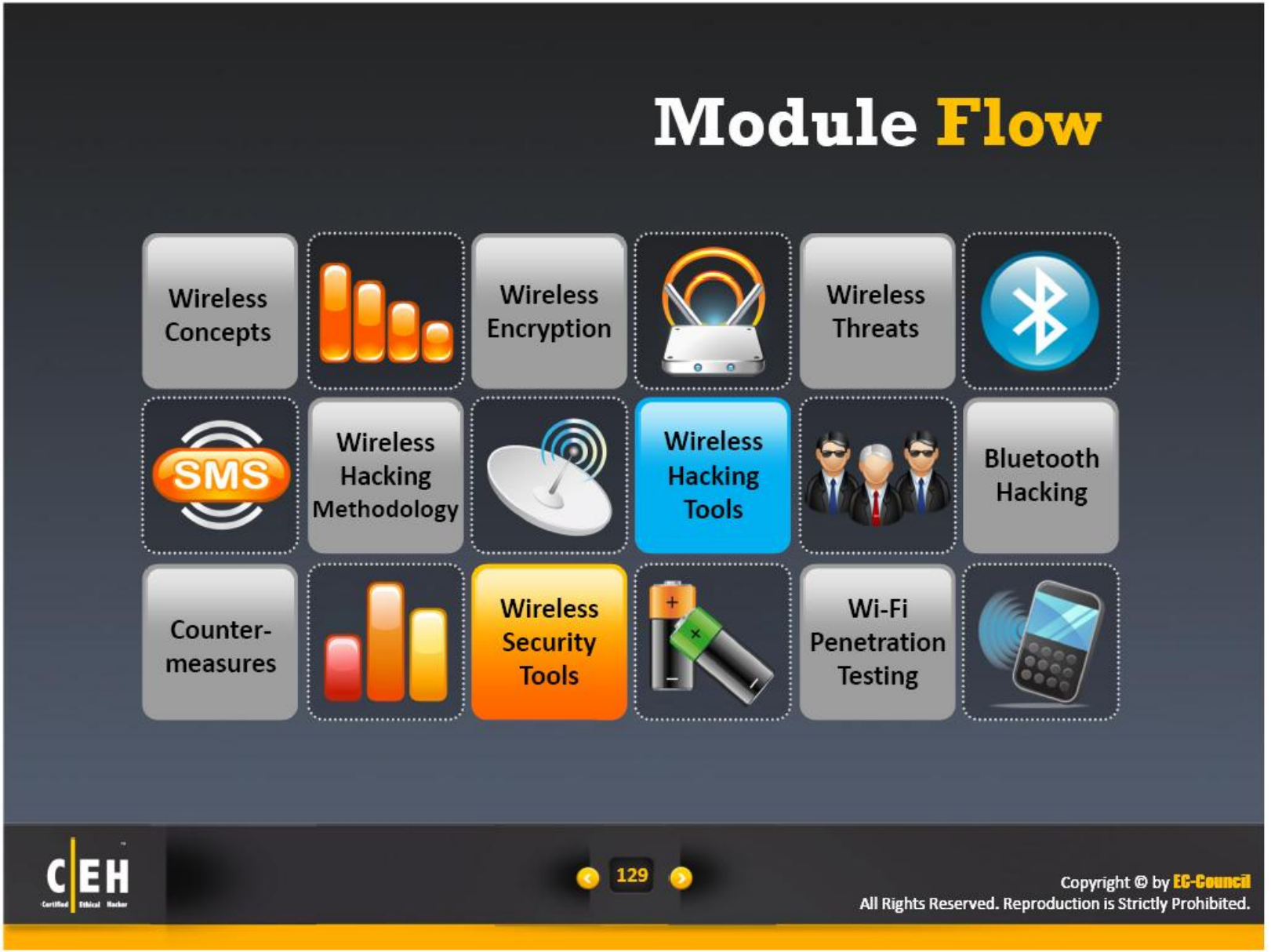
How to Defend Against Wireless Attacks?

Wi-Fi Authentication Best Practices

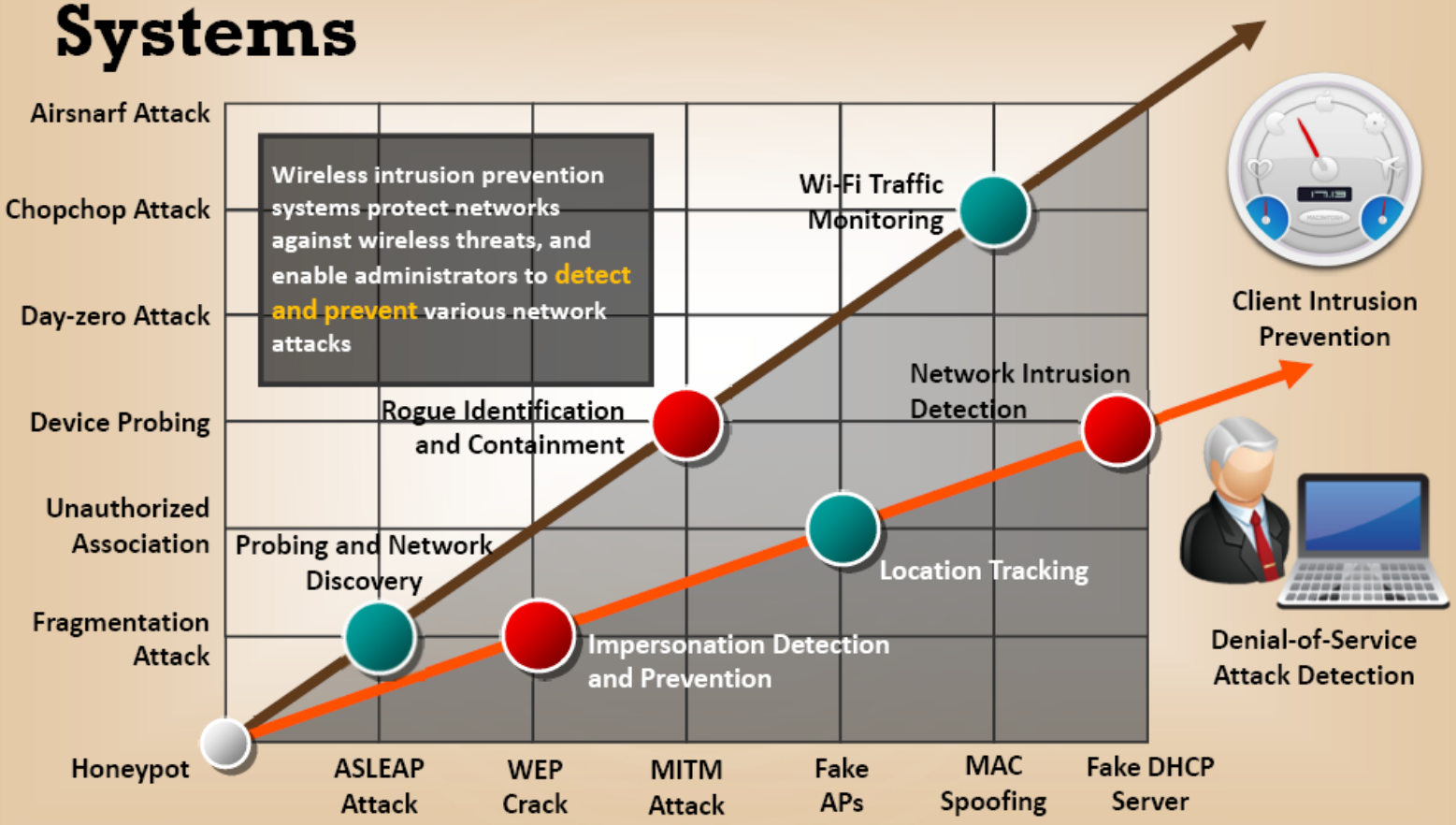
- Choose Wi-Fi Protected Access (WPA) instead of WEP
- Implement WPA2 Enterprise wherever possible
- Disable the network when not required
- Place wireless access points in a secured location
- Keep drivers on all wireless equipment updated
- Use a centralized server for authentication


Internet
Use Wireless IDS
RADIUS Server
VPN Server
Exchange Server
Database Server
Authenticate Wi-Fi Users Using RADIUS
Use IPSEC for Intranet Access
Enterprise Network
Use MAC Filtering
Enable WPA2
User
Use Complex Password
Use VPN Tunnel
Encryption
Attacker
Disassociate Unauthorized Users
Disable Broadcast SSID
How to Defend Against Wireless Attacks?
CEH
128
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

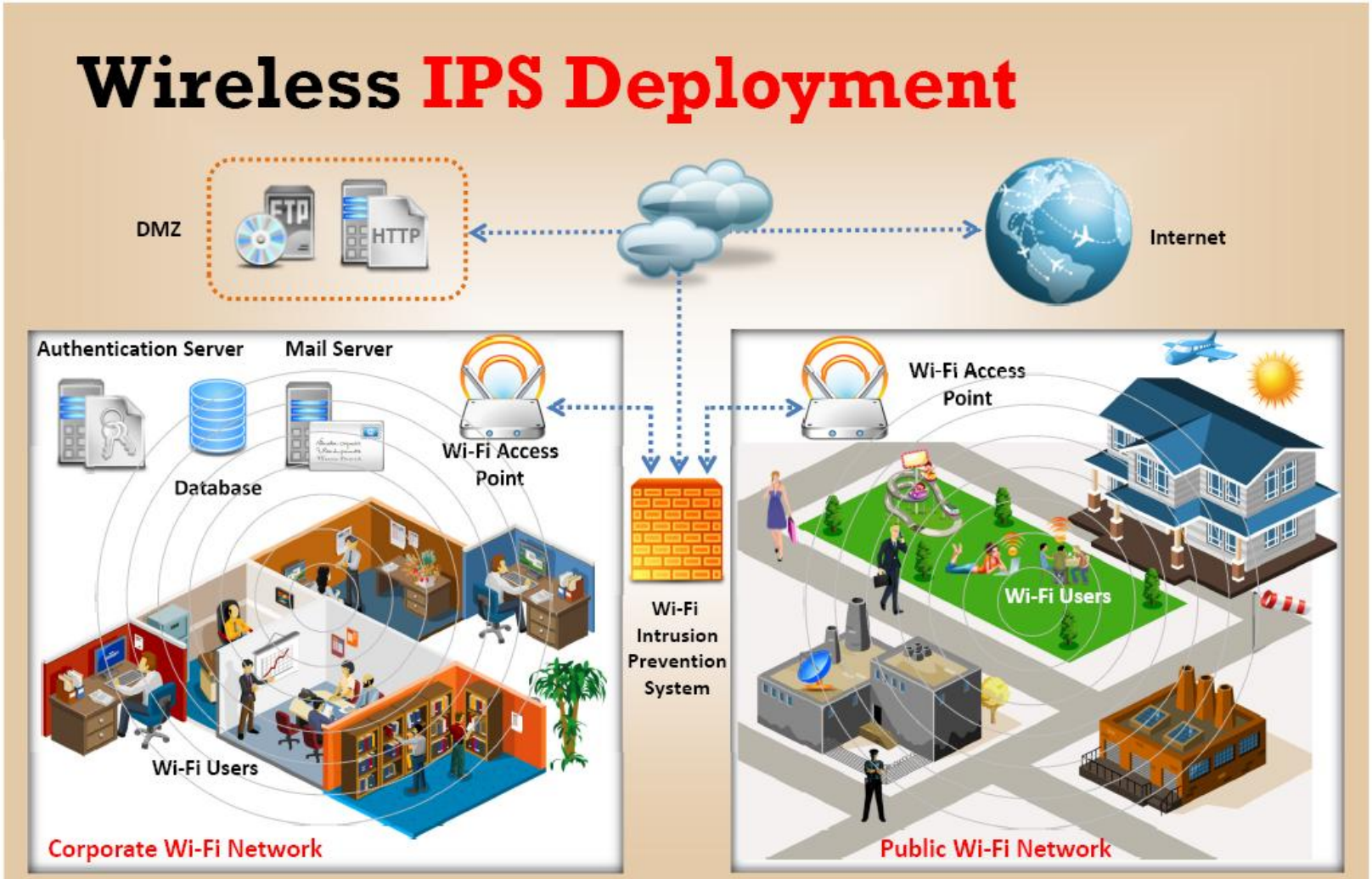
Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
C|EH
Certified Ethical Hacker
129
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Intrusion Prevention Systems

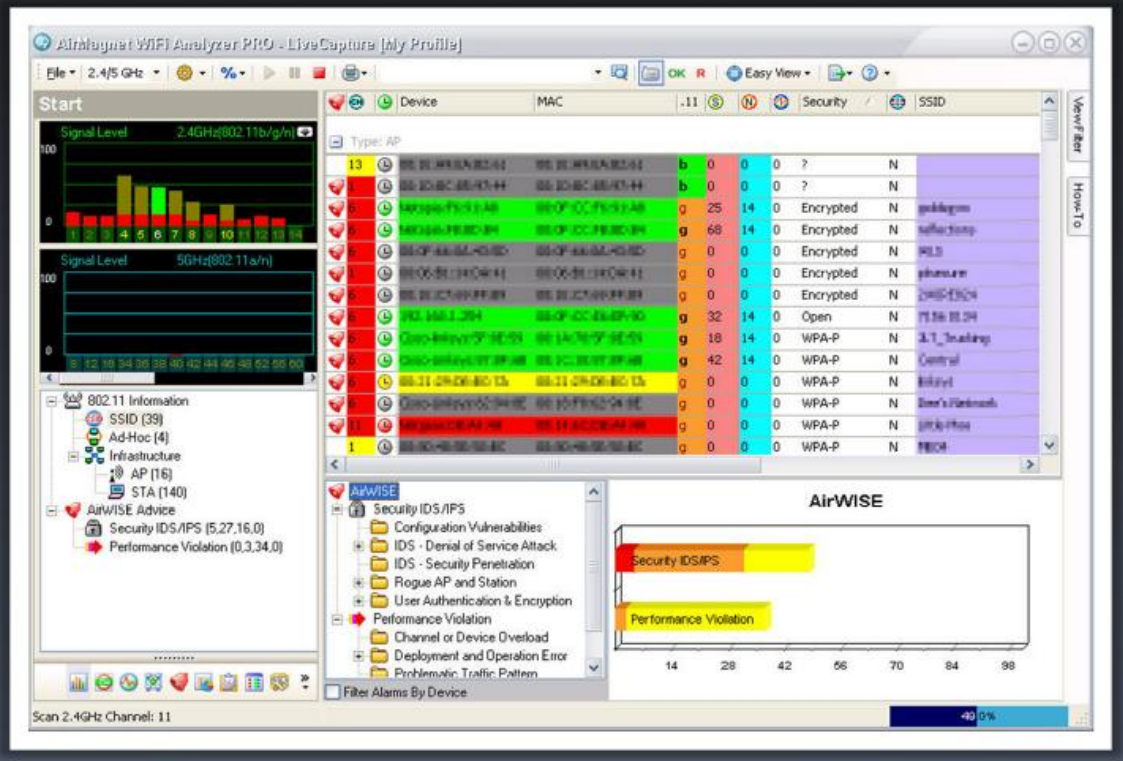


Wireless IPS Deployment



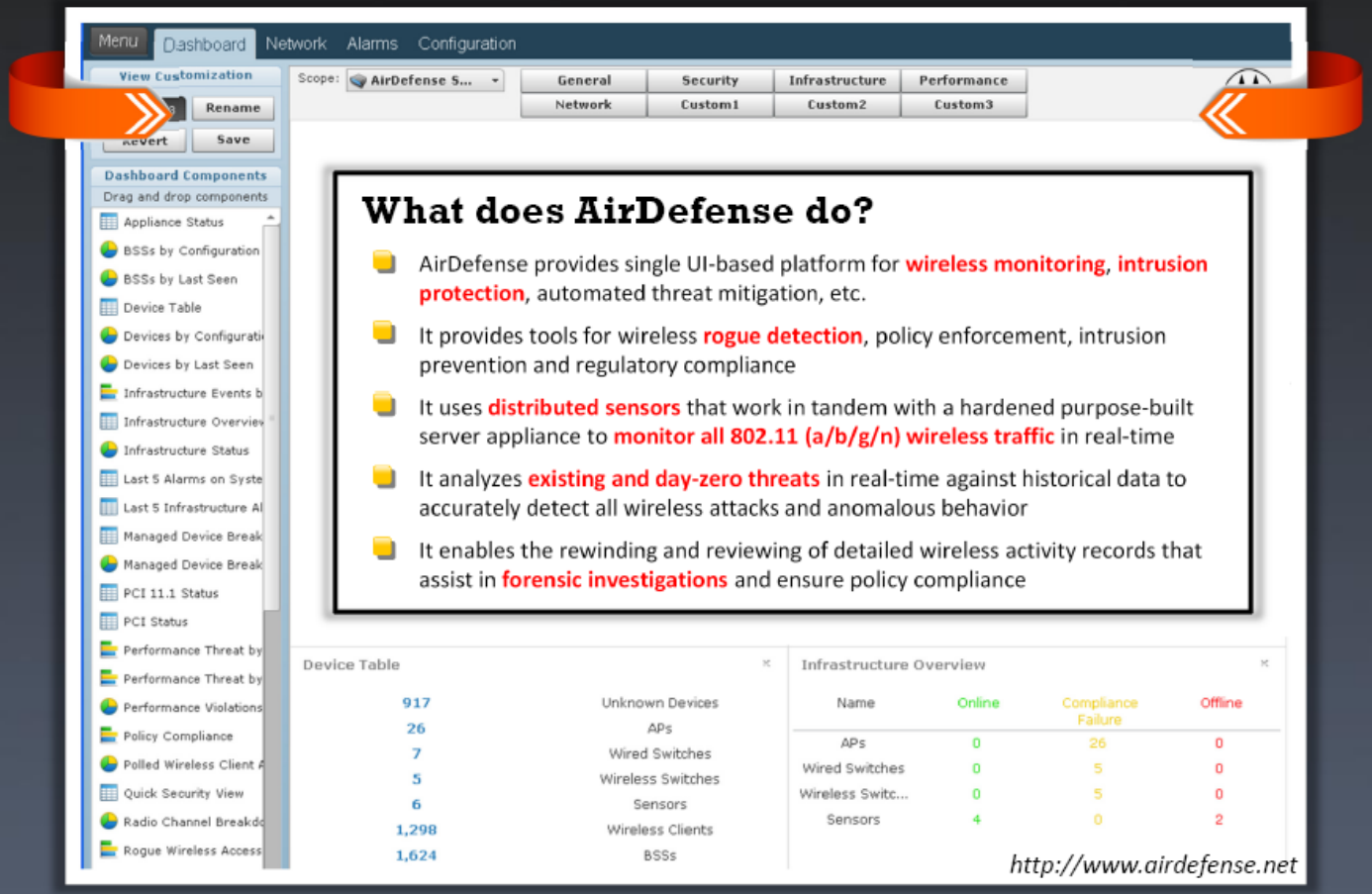
Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer

- It is a Wi-Fi networks auditing and troubleshooting tool
- Automatically detects security threats and other wireless network vulnerabilities
- It detects Wi-Fi attacks such as Denial of Service attacks, authentication/ encryptions attacks, network penetration attacks, etc.
- It can locate unauthorized (rogue) devices or any policy violator

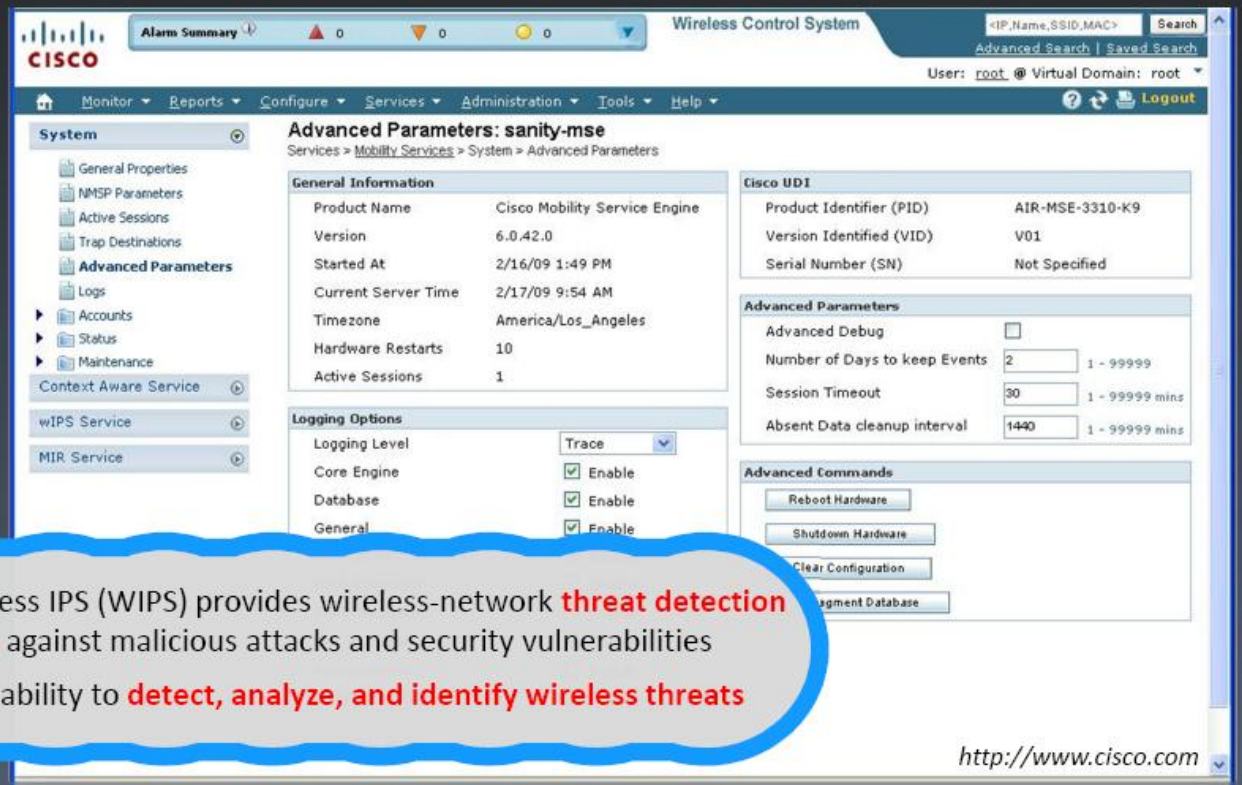


http://www.airmagnet.com

Wi-Fi Security Auditing Tool: AirDefense



Wi-Fi Security Auditing Tool: Adaptive Wireless IPS



Adaptive Wireless IPS (WIPS) provides wireless-network **threat detection and mitigation** against malicious attacks and security vulnerabilities

It provides the ability to **detect, analyze, and identify wireless threats**

Wi-Fi Security Auditing Tool: Aruba RFProtect WIPS

Integrated wireless **intrusion detection** and prevention

Automatic threat mitigation for centrally evaluating forensic data, and actively containing rogues and locking down device configuration

Automated compliance reporting to meet policy mandates for PCI, HIPAA, DoD 8100.2, and GBLA with automated report distribution that is tailored to specific audit requirements

CEH Certified Ethical Hacker

Wi-Fi Intrusion Prevention System

SonicWALL Wireless Networking
http://www.sonicwall.com

Network Box IDP
http://www.network-box.com

TippingPoint IPS
http://h10163.www1.hp.com

3Com AirProtect
http://www.3com.com

Newbury RF Firewall
http://www.newburynetworks.com

AirMobile Server
http://www.airmobile.se

SpectraGuard Enterprise
http://www.airtightnetworks.com

WLS Manager
http://www.airpatrolcorp.com

Wi-Fi Predictive Planning Tools

AirMagnet Planner
http://www.airmagnet.com

Networks RingMaster
http://www.trapezenetworks.com

Control System Planning Tool
http://www.cisco.com

Spot Predictive Site Survey
http://www.connect802.com

SpectraGuard Planner
http://www.airtightnetworks.com

Site Survey Professional
http://www.ekahau.com

LAN Planner
http://www.motorola.com

Wi-Fi Planner
http://www2.aerohive.com

Wi-Fi Vulnerability Scanning Tools

Karma
http://theta44.org

FastTrack
http://www.thepentest.com

Zenmap
http://nmap.org

WiFiDEnum
http://labs.arubanetworks.com

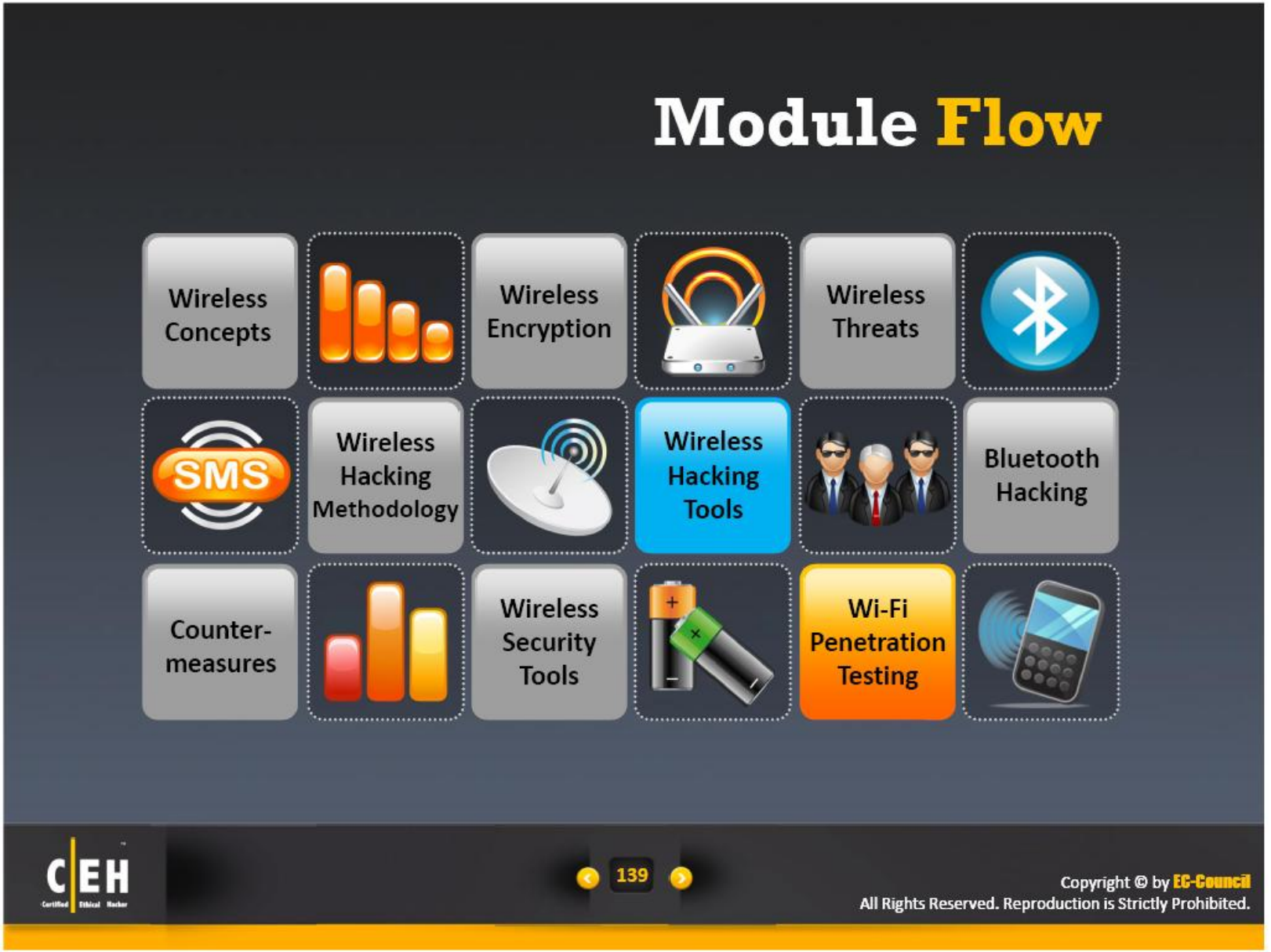
Nessus
http://www.nessus.org

WiFiZoo
http://community.corest.com

OSWA
http://securitystartshere.org

Security Assessment Toolkit
http://www.hotlabs.org

Module Flow


Wireless Concepts
Wireless Encryption
Wireless Threats
SMS
Wireless Hacking Methodology
Wireless Hacking Tools
Bluetooth Hacking
Counter-measures
Wireless Security Tools
Wi-Fi Penetration Testing
CEH
Certified Ethical Hacker
139
Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Penetration Testing

- The process of actively **evaluating information security measures** implemented in a wireless network to analyze design weaknesses, technical flaws and vulnerabilities
- The results are delivered comprehensively in a report to executive, management, and technical audiences

Threat Assessment

Identify the wireless threats facing an organization's information assets

Upgrading Infrastructure

Change or upgrade existing infrastructure of software, hardware, or network design

Risk Prevention and Response

Provide comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation

Security Control Auditing

To test and validate the efficiency of wireless security protections and controls

Data Theft Detection

Find streams of sensitive data by sniffing the traffic

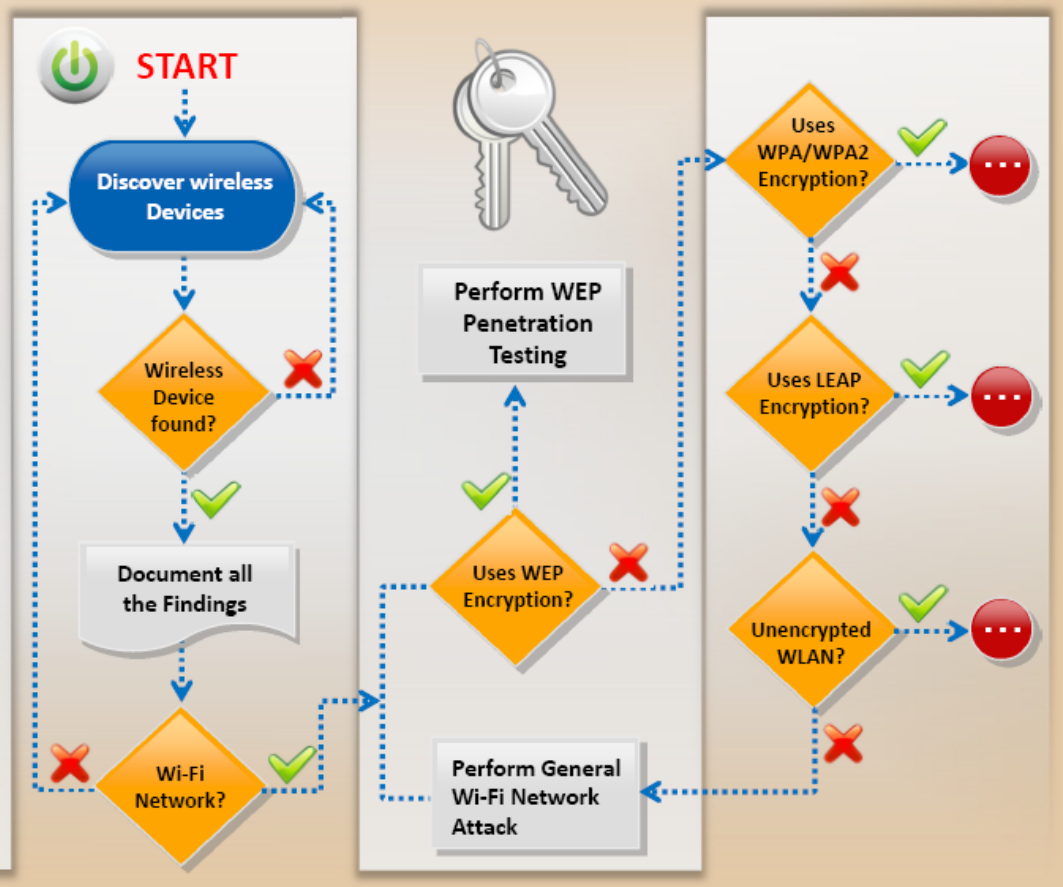
Information System Management

Collect information on security protocols, network strength and connected devices

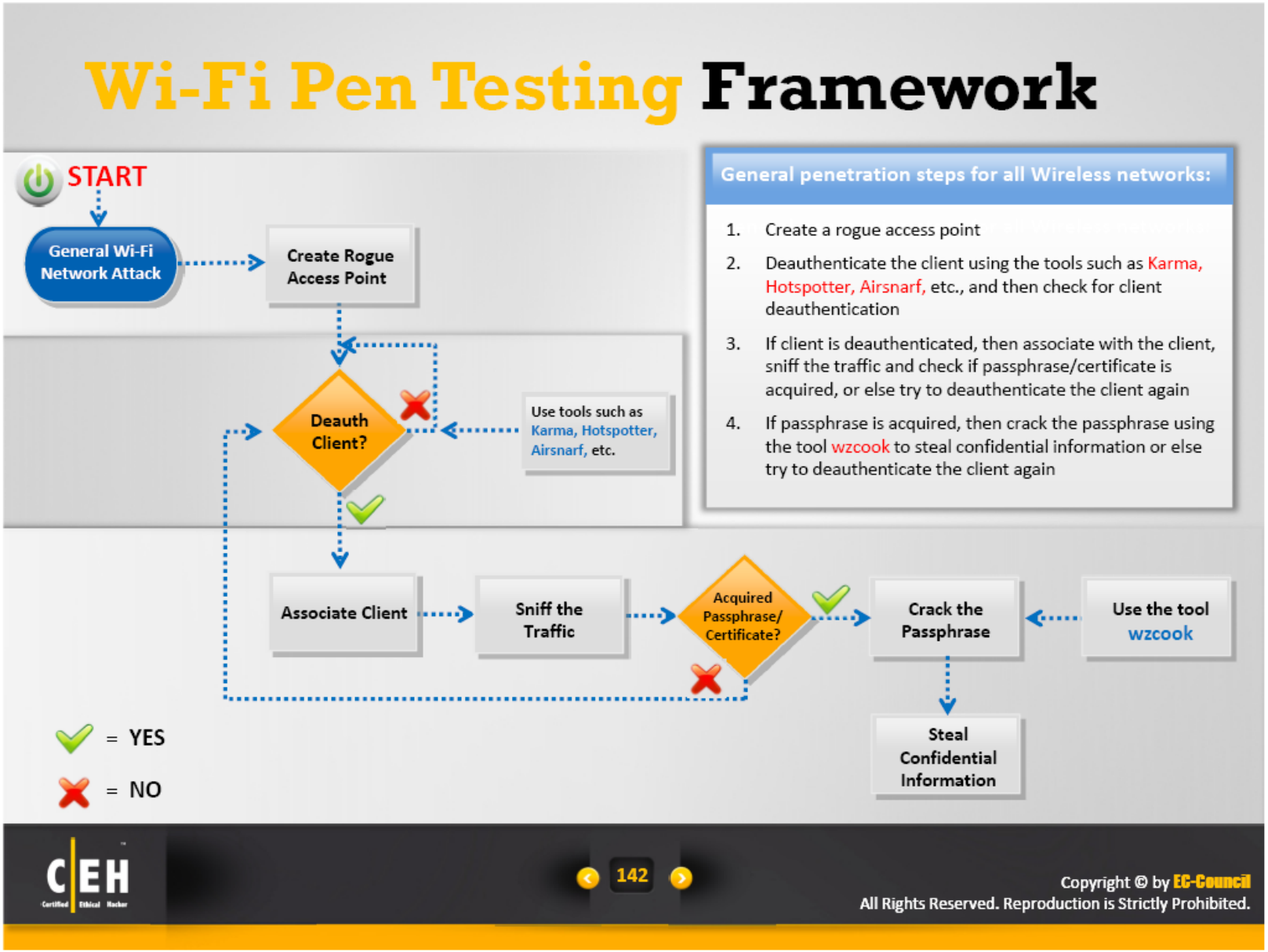
Wireless Penetration Testing Framework

Wireless Pen Testing Framework

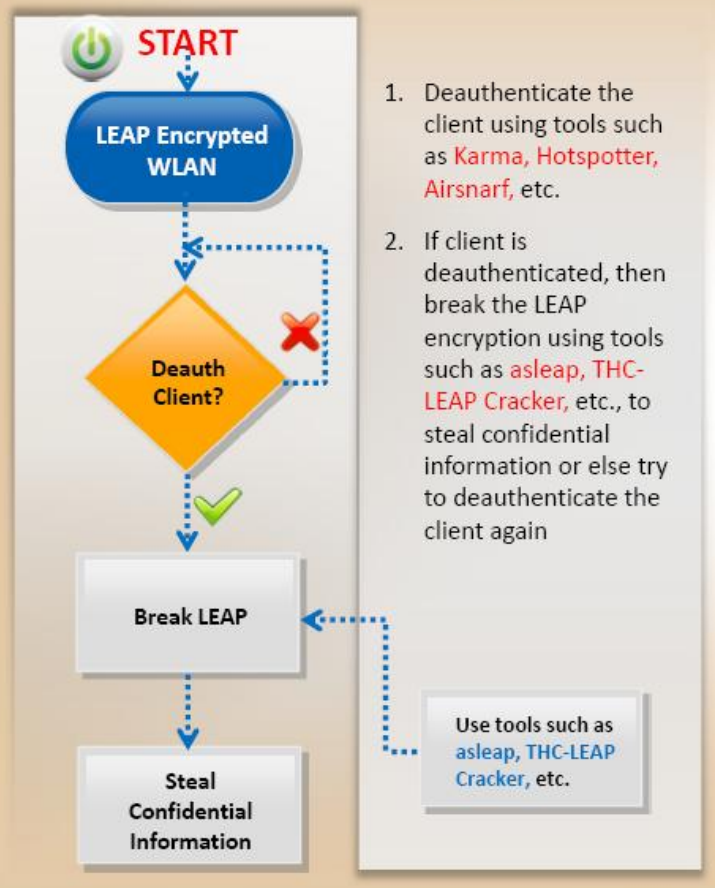
1. Discover wireless devices
2. If wireless device is found, document all the findings
3. If the wireless device found is using Wi-Fi network, then perform general Wi-Fi network attack and check if it uses WEP encryption
4. If WLAN uses WEP encryption, then perform WEP encryption pen testing or else check if it uses WPA/WPA2 encryption
5. If WLAN uses WPA/WPA2 encryption, then perform WPA/WPA2 encryption pen testing or else check if it uses LEAP encryption
6. If WLAN uses LEAP encryption, then perform LEAP encryption pen testing or else check if WLAN is unencrypted
7. If WLAN is unencrypted, then perform unencrypted WLAN pen testing or else perform general Wi-Fi network attack



Wi-Fi Pen Testing Framework

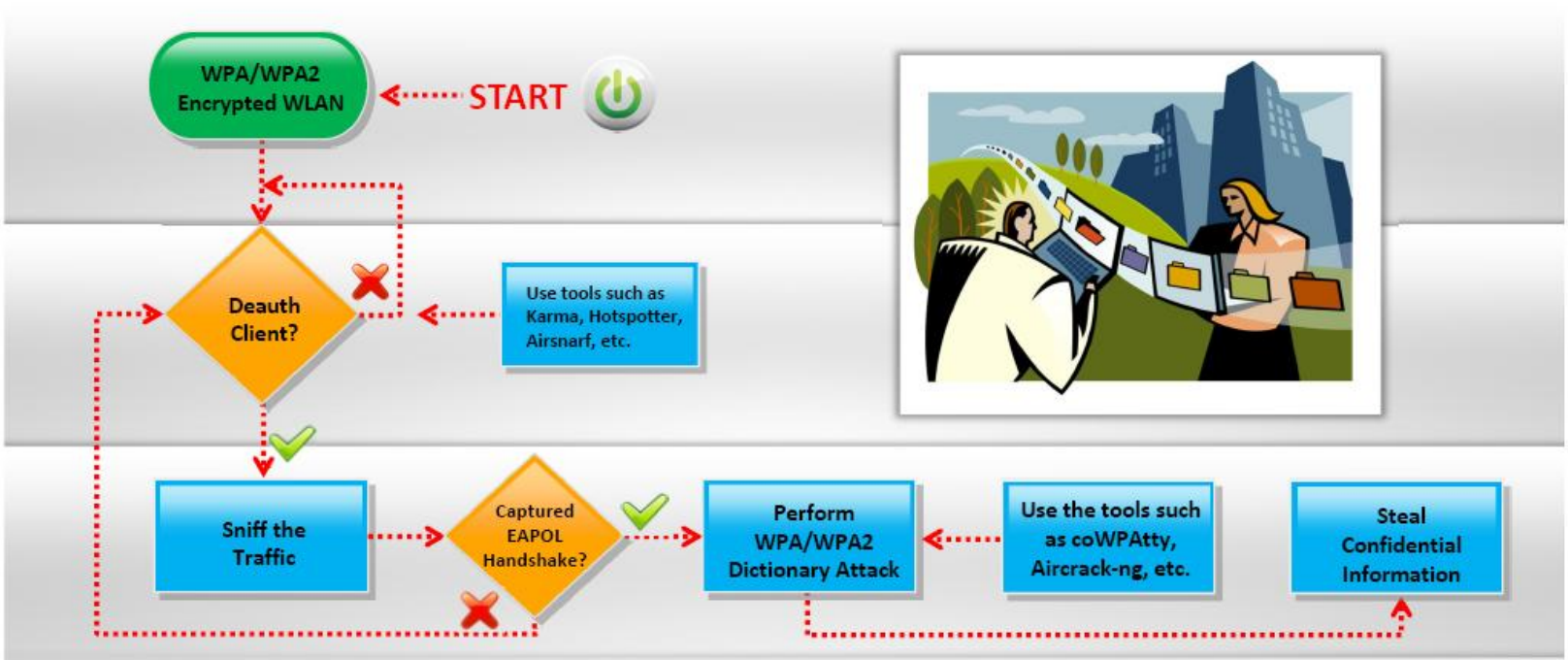


Pen Testing LEAP Encrypted WLAN



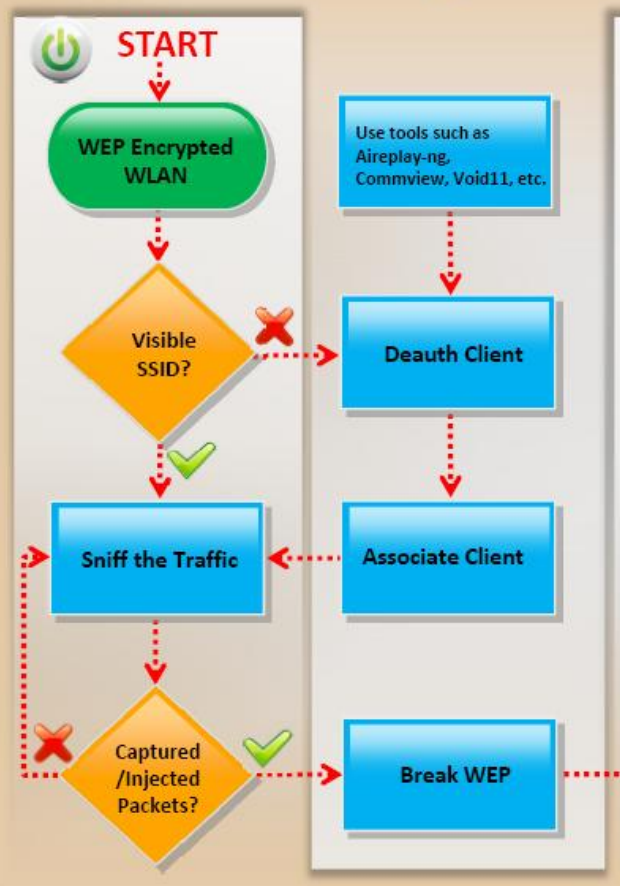
1. Deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.
2. If client is deauthenticated, then break the LEAP encryption using tools such as asleap, THC-LEAP Cracker, etc., to steal confidential information or else try to deauthenticate the client again

Pen Testing WPA/WPA2 Encrypted WLAN



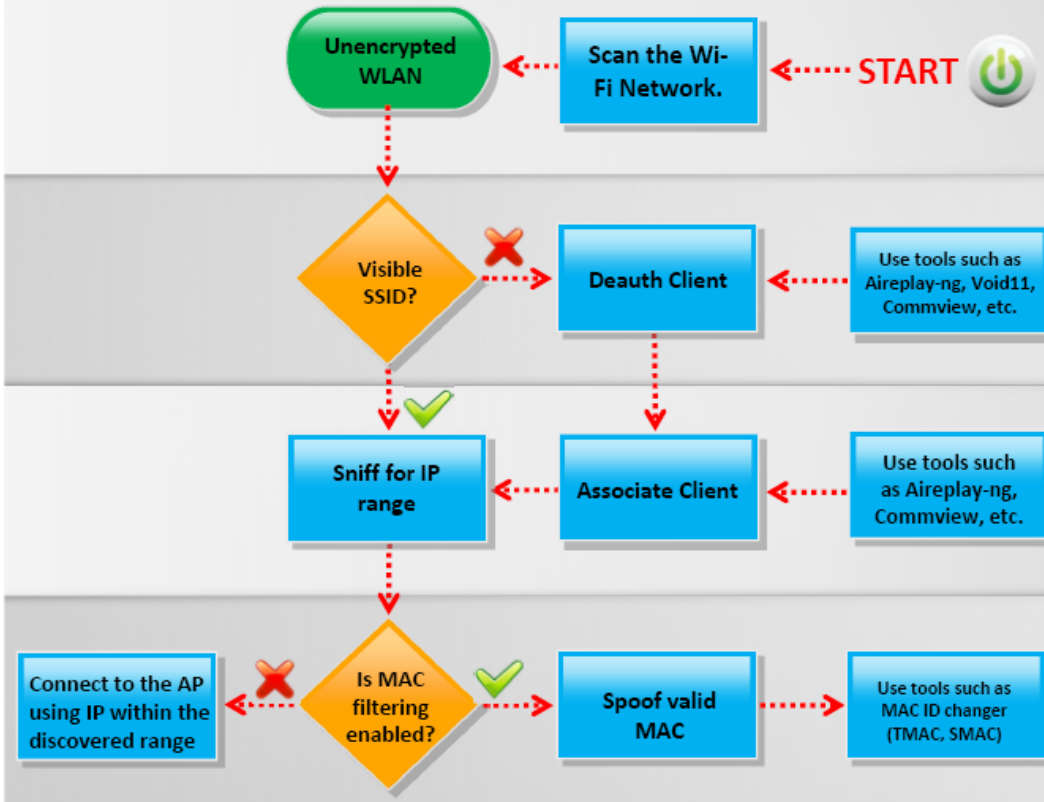
1. Deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.
2. If client is deauthenticated, sniff the traffic and then check the status of capturing EAPOL handshake or else try to deauthenticate the client again
3. If EAPOL handshake is captured, then perform WPA/WPA2 dictionary attack using tools such as coWPAtty, Aircrack-ng, etc. to steal confidential information or else try to deauthenticate the client again

Pen Testing WEP Encrypted WLAN



1. check if the SSID is visible or hidden
2. If SSID is visible, sniff the traffic and then check the status of packet capturing
3. If the packets are captured/injected, then break the WEP key using tools such as Aircrack-ng, Airsnort, WEPcrack, etc., or else sniff the traffic again.
4. If SSID is hidden, then deauthenticate the client using tools such as Aireplay-ng, Commview, Void11, etc., associate the client and then follow the procedure of visible SSID

Pen Testing Unencrypted WLAN



1. Check if the SSID is visible or hidden
2. If SSID is visible, sniff for IP range and then check the status of MAC filtering
3. If MAC filtering is enabled, spoof valid MAC using tools such as SMAC or connect to the AP using IP within the discovered range
4. If SSID is hidden, discover the SSID using tools such as Aireplay-ng, and follow the procedure of visible SSID

Module Summary

- IEEE 802.11 standards based Wi-Fi networks are widely used for communication and data transfer across a radio network
- A Wi-Fi infrastructure generally consists of hardware components such as wireless routers and APs, antennas, relay towers and authentication servers, and software components such as encryption algorithms, key management and distribution mechanisms
- Most widely used wireless encryption mechanisms include WEP, WPA and WPA2, of which, WPA2 is considered most secure
- WEP uses 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission
- WPA uses TKIP which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit keys for authentication whereas WPA2 encrypts the network traffic using a 256 bit key with AES encryption
- WEP is vulnerable to various analytical attack that recovers the key due to its weak IVs whereas WPA is vulnerable to password brute forcing attacks
- Wi-Fi networks are vulnerable to various access control, integrity, confidentiality, availability and authentication attacks
- Wi-Fi attack countermeasures include configuration best practices, SSID settings best practices, authentication best practices and wireless IDS systems

Quotes

"We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology."

- **Carl Sagan**,
An American Astronomer
and Popular Science Writer