

Smart Intern Long Term Virtual Internship

**An Internship Report submitted in partial fulfilment of the requirements for the award of degree
of**

BACHELOR OF TECHNOLOGY

In

Computer Science and Engineering

Submitted by:

Kurella Sai Priyanka 20NR1A0557

Koyya Sonia Prathyusha 21NR1A0512



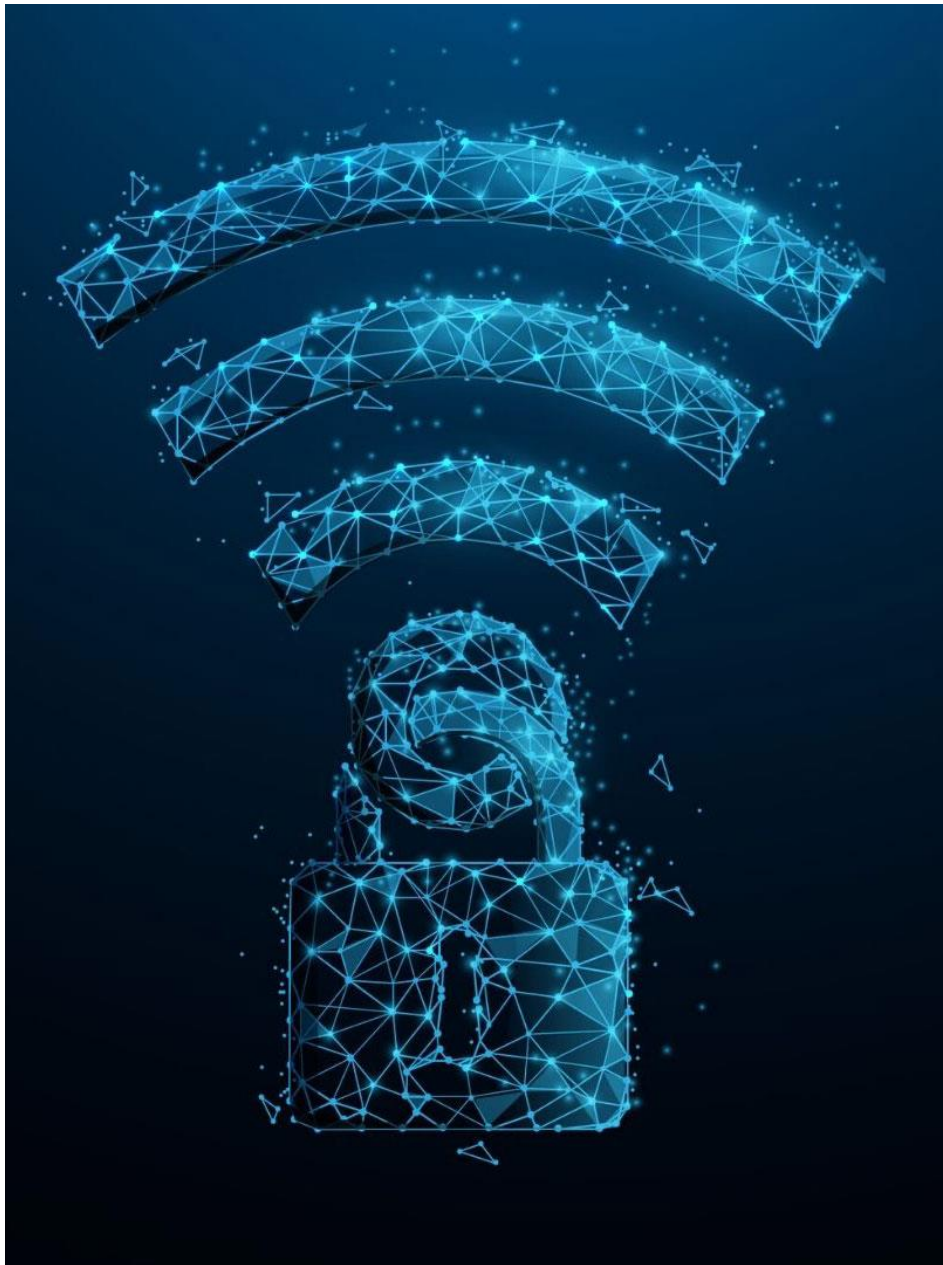
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BABA INSTITUTE OF TECHNOLOGY AND SCIENCES

Approved by AICTE, permanently affiliated to JNTUGV & Accredited by NAAC

p.m.palem, Madhurawada, Vishakhapatnam, Andhra Pradesh

Wireless Network Security Assessment



Introduction

Wireless networks have become an integral part of modern business operations, offering convenience, flexibility, and increased productivity. However, the convenience of wireless connectivity also brings inherent security risks that organizations must address to safeguard their sensitive data and critical assets. A wireless network security assessment is a systematic evaluation of the security measures and vulnerabilities within an organization's wireless infrastructure.

The primary objective of a wireless network security assessment is to identify potential weaknesses in the wireless network that could be exploited by malicious actors. This assessment encompasses a range of techniques and methodologies aimed at uncovering vulnerabilities related to network architecture, protocols, access points, encryption, authentication mechanisms, and overall network management.

By conducting a wireless network security assessment, organizations gain valuable insights into the effectiveness of their current security measures and their ability to protect against unauthorized access, data breaches, and cyber threats. The assessment helps organizations make informed decisions about enhancing their wireless network security and implementing measures to mitigate risks.

Key Components of a Wireless Network Security Assessment:

1. Network Architecture Review: Evaluating the design and layout of the wireless network to ensure secure segmentation and proper isolation of critical assets.
2. Access Point Analysis: Identifying vulnerabilities in wireless access points, including default or weak credentials, outdated firmware, and misconfigurations.
3. Encryption and Authentication Assessment: Examining the encryption protocols and authentication mechanisms in use to ensure they meet current security standards.
4. Rogue Device Detection: Detecting unauthorized or rogue access points and devices that could provide unauthorized entry points.
5. Intrusion Detection and Prevention: Assessing the network's ability to detect and respond to unauthorized or malicious activities.
6. User Awareness and Training: Evaluating the level of user awareness and understanding of wireless security best practices and potential threats.

Executive Summary

Objective:

The objective of a wireless network refers to the overarching goal or purpose for which the network is designed and deployed. It outlines what the network aims to achieve in terms of functionality, performance, and benefits. The objectives of a wireless network can vary depending on the context, industry, and organization, but here are some common objectives:

- 1. Connectivity:** The primary objective of most wireless networks is to provide seamless and reliable connectivity. Users should be able to access resources and communicate with each other efficiently, regardless of their physical location within the network coverage area.
- 2. Mobility:** Wireless networks enable users to stay connected while on the move. The objective is to allow users to access network services and data from different locations without being tied to a specific physical connection point.
- 3. Flexibility:** Wireless networks provide flexibility in setting up and rearranging network components. This is particularly useful in environments where physical cabling may be challenging or impractical.
- 4. Scalability:** Wireless networks should be designed to accommodate an increasing number of devices and users as the organization grows. The objective is to maintain performance and quality of service even as the network load increases.
- 5. Cost-Efficiency:** In some cases, wireless networks can be more cost-effective to deploy and maintain compared to traditional wired networks. The objective here is to achieve connectivity without incurring excessive infrastructure costs.
- 6. User Experience:** The objective is to provide a seamless and satisfying user experience with fast and reliable connections. This is especially important in consumer-oriented environments like cafes, hotels, and public spaces.
- 7. Remote Access:** Wireless networks enable remote access to resources, allowing users to connect to the corporate network from outside the office. The objective is to enable secure remote work and access to resources.

Methodology:

The assessment followed a comprehensive methodology that included a combination of active and passive techniques. It encompassed a thorough examination of the organization's wireless architecture, protocols, access points, authentication mechanisms, encryption methods, and monitoring capabilities. Both internal and external wireless networks were assessed to ensure a holistic view of the organization's wireless security landscape.

Key Findings:

1. **Weak Authentication Mechanisms:** Several wireless access points were found to be using weak or default authentication credentials, making them vulnerable to unauthorized access.
2. **Outdated Firmware and Patches:** A significant number of access points were running outdated firmware versions, lacking crucial security patches that could mitigate known vulnerabilities.
3. **Rogue Access Points:** Multiple rogue access points were detected within the network perimeter, potentially providing a point of entry for malicious actors.
4. **Insufficient Encryption:** Some wireless communication was observed to use weak encryption protocols, putting sensitive data at risk of interception and unauthorized access.
5. **Lack of Intrusion Detection:** The organization's wireless network lacked a robust intrusion detection system, making it difficult to promptly identify and respond to security breaches.

Recommendations:

1. **Authentication Enhancement:** Implement strong, unique passwords for all wireless access points and enforce regular password updates. Consider implementing multi-factor authentication for heightened security.
2. **Firmware and Patch Management:** Establish a routine process for monitoring and applying firmware updates and security patches to all wireless devices. Consider automation to streamline this process and ensure timely updates.
3. **Rogue Access Point Monitoring:** Deploy a wireless intrusion detection and prevention system to continuously monitor for rogue access points and unauthorized devices. This will help prevent unauthorized access and enhance network visibility.
4. **Encryption Strengthening:** Upgrade to the latest encryption protocols (e.g., WPA3) to ensure robust protection of wireless communications. Disable outdated and vulnerable encryption standards (e.g., WEP).
5. **Intrusion Detection Implementation:** Invest in a dedicated intrusion detection system for wireless networks that provides real-time alerts and forensic analysis of security incidents.

Overview

A wireless network security assessment is a systematic and thorough evaluation of the security aspects of an organization's wireless network infrastructure. It involves analyzing various components, protocols, and practices to identify vulnerabilities, weaknesses, and potential threats that could compromise the confidentiality, integrity, and availability of data and resources. The goal of a wireless network security assessment is to ensure that the wireless network is well-protected against unauthorized access, data breaches, and cyberattacks.

Key Aspects of a Wireless Network Security Assessment:

- 1. Network Architecture Analysis:** Reviewing the design and layout of the wireless network to assess its segmentation, access points, and overall topology. This step ensures that the network is properly organized to prevent unauthorized access and data leakage.
- 2. Access Point Examination:** Evaluating the security configuration of wireless access points, including authentication mechanisms, encryption protocols, and proper management. This helps identify vulnerabilities that could be exploited by attackers seeking to gain unauthorized entry.
- 3. Encryption and Authentication Assessment:** Analyzing the effectiveness of encryption methods and authentication mechanisms in use, such as WPA2/WPA3 and strong password policies. This ensures that wireless communications are adequately protected against eavesdropping and unauthorized access.
- 4. Rogue Device Detection:** Identifying unauthorized or rogue access points and devices within the wireless network that could serve as potential entry points for attackers. Detecting and mitigating these rogue devices helps maintain the network's integrity.
- 5. Intrusion Detection and Prevention:** Reviewing the network's ability to detect and respond to unusual or suspicious activities, such as unauthorized attempts to connect, brute-force attacks, or data exfiltration.
- 6. User Awareness and Training Evaluation:** Reviewing the level of awareness and understanding among users about wireless security best practices, potential risks, and the importance of adhering to security policies.

Benefits of Wireless Network Security Assessment:

Wireless network security offers a range of benefits that contribute to protecting sensitive information, maintaining network integrity, and ensuring a safe and productive environment for users. Some of the key benefits of wireless network security include:

- 1. Data Protection:** Implementing wireless network security measures, such as encryption protocols like WPA3, helps safeguard data transmitted over the network. This prevents unauthorized interception and eavesdropping on sensitive information.
- 2. Access Control:** Security mechanisms like strong authentication methods (e.g., WPA2-Enterprise) enable controlled access to the wireless network. Only authorized users with valid credentials can connect, reducing the risk of unauthorized access.
- 3. Prevention of Unauthorized Access:** Effective security measures prevent unauthorized users from connecting to the network and potentially compromising its resources. This helps maintain the confidentiality and availability of network services.
- 4. Mitigation of Rogue Devices:** Wireless network security tools can detect and mitigate the presence of rogue devices—unauthorized access points or clients that can introduce security vulnerabilities or perform malicious activities.
- 5. Network Availability:** By preventing unauthorized access and reducing the risk of attacks, wireless network security contributes to maintaining network availability and preventing disruptions that could impact business operations.
- 8. Secure Remote Access:** Organizations can offer secure remote access to employees, allowing them to work from outside the office environment without compromising the security of the network and sensitive data.
- 9. Confidentiality:** Wireless security measures ensure that sensitive business information remains confidential and is not exposed to unauthorized individuals.
- 10. Secure Guest Access:** Organizations can provide guest access to their networks while isolating guest traffic from internal resources. This enables guest connectivity without jeopardizing the security of the main network.

In summary, wireless network security is crucial for maintaining the confidentiality, integrity, and availability of network resources. It provides protection against a wide range of threats and vulnerabilities, offering peace of mind for users and organizations alike.

Detail Report

Information Gathering:

Information gathering is a crucial phase in the cybersecurity and assessment process. It involves collecting relevant data and intelligence about a target system, network, or organization to understand its vulnerabilities and potential attack surfaces. Here are different aspects of information gathering:

1. Email Footprint Analysis:

Email footprint analysis is a process that involves examining the digital trail left by an individual or organization through their email communications. This analysis can provide valuable insights into various aspects, such as communication patterns, relationships, and potential security vulnerabilities. Email footprint analysis is to gain a comprehensive understanding of an entity's email-related activities, which can include communication patterns, contact relationships, potential security risks, and data leakage.

2. DNS Information Gathering:

DNS (Domain Name System) information gathering is a process used to collect valuable data about domain names, IP addresses, and their associated infrastructure. This information is important for various purposes, including cybersecurity, network management, and digital forensics. DNS information gathering is to retrieve, analyze, and interpret DNS-related data to gain insights into the target domain's infrastructure, services, and potential vulnerabilities.

3. WHOIS Information Gathering:

WHOIS information gathering involves accessing and analyzing the WHOIS database to retrieve valuable information about domain registrations, including details about the registrant, domain creation and expiration dates, contact information, and more. This process is essential for various purposes, such as domain ownership verification, cybersecurity, brand protection, and legal investigations.

4. Information Gathering for Social Engineering Attacks:

Information gathering is a crucial phase in the planning of social engineering attacks, which involve manipulating individuals into divulging confidential information, taking certain actions, or compromising security. Effective information gathering provides attackers with the insights they need to craft convincing and targeted attacks. Information gathering for social engineering attacks is to collect relevant details about the target individuals, organizations, or systems in order to create a credible and successful social engineering attack.

5. Information Gathering for Physical Security Assessments:

Information gathering for physical security assessments involves collecting relevant data and insights to assess the vulnerabilities, strengths, and risks associated with an organization's physical security measures. This process helps identify potential weaknesses in physical security systems, access control, and facility protection. Information gathering for physical security assessments is to comprehensively understand an organization's physical security posture, identify vulnerabilities, and develop recommendations to enhance security measures.

6. Emerging Trends and Technologies in Information Gathering:

Emerging trends and technologies are significantly shaping the landscape of information gathering across various domains, from cybersecurity to marketing and beyond. These trends leverage advancements in data collection, analysis, and automation to gather insights and make informed decisions.

1)Email Footprint Analysis:

Email footprint analysis refers to the process of examining and evaluating an individual or organization's digital trail left through their email communications. It involves collecting, analyzing, and interpreting various metadata and content from emails to gain insights into patterns, behaviour, and relationships. This analysis can be used for various purposes, such as cybersecurity investigations, digital forensics, marketing research, and more.

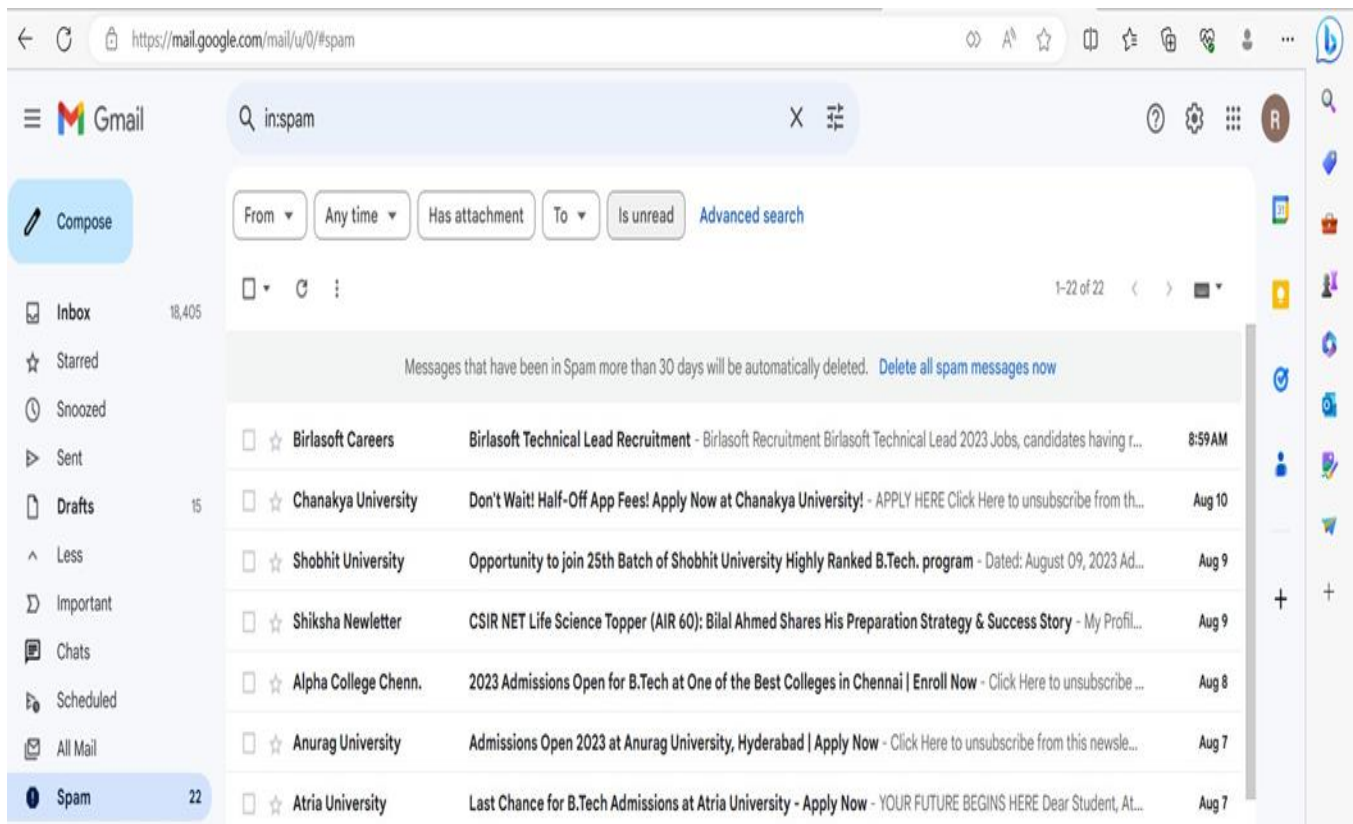
Here are some aspects typically considered in email footprint analysis:

1. **Email Headers:** Analyzing email headers can reveal valuable information such as the sender's IP address, email client, server paths, and timestamps. This information can help in identifying potential sources of phishing attacks or email spoofing.
2. **Sender and Recipient Analysis:** Studying the frequency and volume of email exchanges between different senders and recipients can provide insights into communication patterns and relationships. It can also help identify key contacts or suspicious interactions.
3. **Content Analysis:** Examining the content of emails can offer information about topics of interest, potential risks, or even sensitive information leaks. Natural language processing techniques can be used to extract relevant data from email content.
4. **Attachment Analysis:** Checking attachments for malware or suspicious files can be an essential part of email footprint analysis, especially in cybersecurity investigations.
5. **Timestamps and Time Zones:** Analyzing the timestamps and time zones of emails can help establish the location of email senders or uncover anomalies in communication patterns.
6. **Email Forwarding and BCC Analysis:** Tracking email forwarding and BCC (blind carbon copy) recipients can be crucial in understanding how information is disseminated within or outside an organization.
7. **Email Volume and Traffic Patterns:** Monitoring the volume and frequency of incoming and outgoing emails over time can help detect abnormal activity or potential email-based attacks.
8. **Email Authentication Records:** Analyzing SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) records can help verify the legitimacy of emails and identify spoofed or fraudulent messages.
9. **Geolocation Data:** If available, geolocation data associated with email communications can provide additional context, especially in cases of suspicious or malicious activity.

PROCESS FOR EMAIL FOOTPRINTING ANALYSIS:

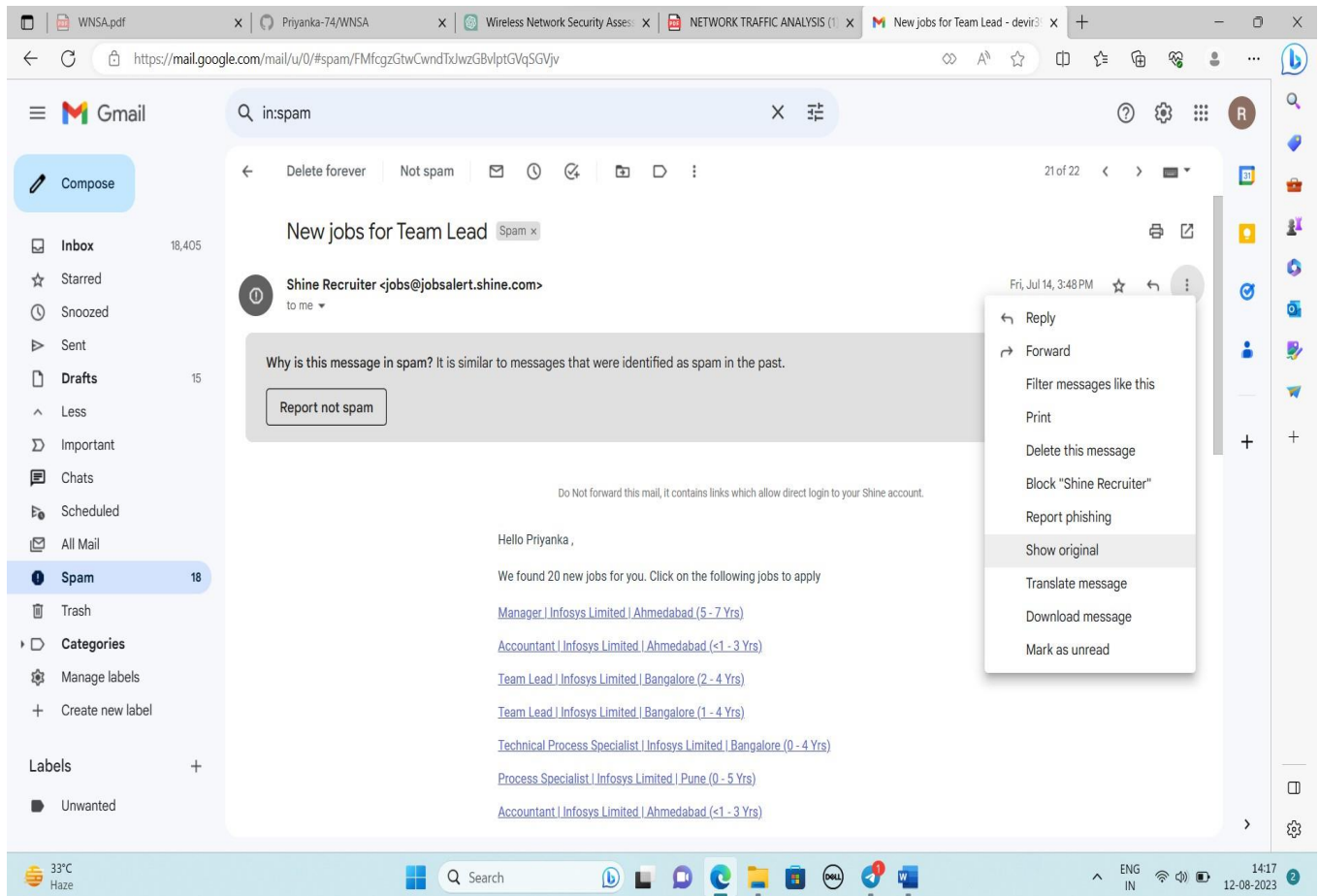
Step-1 :

- Open your Gmail ,GO through the spam mails box and open it .
- In spam folder where you can find many spam mails .
- TO perform an foot printing ,open any spam mail which you want perform.



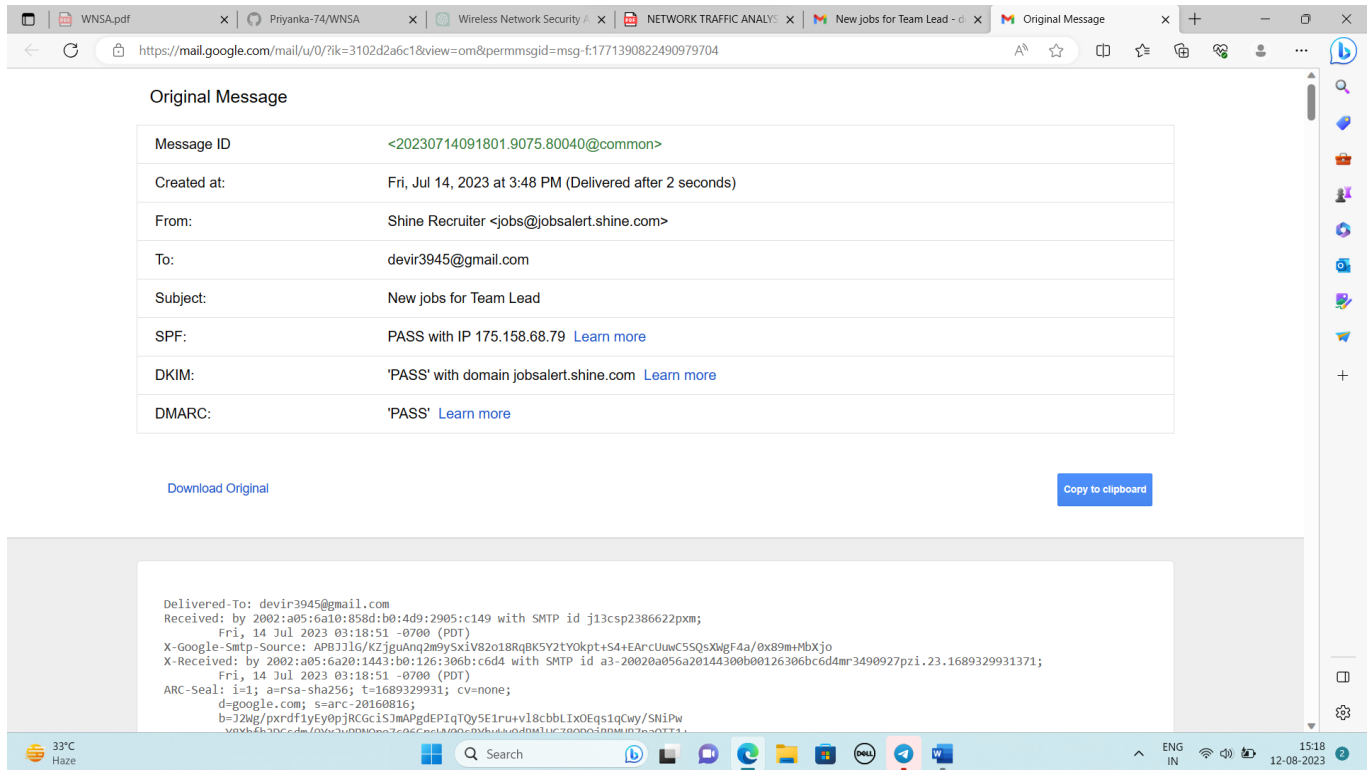
Step-2:

- Now , select the spam mail to perform email footprint analysis.
- In spam mail you'll find show original.



Step-3:

- Now click on the show original therefore you'll redirect to new tab.
- You'll find some code type below the original message in that you have to find "receive form"



- After finding receive form you'll find IP address over there copy it.

Step-4:

- Open another new tab and search for whois IP lookup and open the first result of your search paste the IP address over there.

The screenshot displays the Whois website interface. The browser's address bar shows the URL <https://www.whois.com/whois/shine.com>. The website header includes the Whois logo and a search bar with the text "Enter Domain or IP" and a "WHOIS" button. Below the header, a navigation menu lists various services: DOMAINS, WEBSITE, CLOUD, HOSTING, SERVERS, EMAIL, SECURITY, WHOIS, SUPPORT, LOGIN, and a shopping cart icon. The main content area displays the domain information for "shine.com", which was updated 8 days ago. The domain information is organized into two sections: "Domain Information" and "Registrant Contact".

Domain Information	
Domain:	shine.com
Registrar:	Network Solutions, LLC
Registered On:	1995-09-15
Expires On:	2024-01-18
Updated On:	2021-12-01
Status:	clientTransferProhibited
Name Servers:	a1-232.akam.net a16-67.akam.net a18-64.akam.net a20-65.akam.net a7-66.akam.net a9-67.akam.net

Registrant Contact	
Name:	HT Media Limited
Organization:	HT Media Limited

On the right side of the domain information, there is a section titled "Interested in similar domains?" which lists several domains with "Buy Now" buttons: seyine.com, chchine.com, happyshinecreative.com, theshineclothing.com, shineclothing.net, and shinefitness.net. Below this list, there is a red banner for ".space" domains, showing a sale price of \$0.88 (down from \$24.88).

- In above you'll find the Ip address range from 172.82.221.71
- And also, the mail is form MS-820.

By this you'll find the information through email footprint analysis.

2)DNS INFORMATION GATHERING:

Passive mode

- DNS Enumeration
- OSINT

Offensive mode

- spider websites Tools
- recon-ng
- dnsrecon
- the Harvester

DNS (Domain Name System) information gathering is a process used to collect valuable data about domain names, IP addresses, and their associated infrastructure. This information is important for various purposes, including cybersecurity, network management, and digital forensics.

Methods:

DNS Queries: Using tools like nslookup, dig, or online DNS lookup services to query DNS servers and retrieve information about domain names and records.

Zone Transfers: Zone transfers can provide a comprehensive list of DNS records for a domain. However, not all DNS servers allow zone transfers due to security concerns.

Web-Based Tools: Various online tools provide easy-to-use interfaces for querying DNS information, analyzing DNS records, and mapping domain relationships.

WHOIS Lookup: WHOIS databases provide information about domain registrants, contact details, and registration dates.

Passive DNS: Passive DNS databases maintain historical DNS data, allowing analysis of changes and trends over time

Smartinternz x Altoro Mutual x Temp Mail - Disposable x Whois testfire.net x Network Tools: DNS,JP, x DNS Lookup x DNS records for akamai x start of authority - Goo x +

https://www.nslookup.io/domains/testfire.net/dns-records/ 90%

Kali Linux x Kali Tools x Kali Docs x Kali Forums x Kali NetHunter x Exploit-DB x Google Hacking DB x OffSec

DNS course for developers — \$90 off during the pre-sale

Learning Browser extension API

DNS records for testfire.net

Cloudflare Google DNS OpenDNS Authoritative Local DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
65.61.137.117	24h

AAAA records

No AAAA records found.

CNAME record

No CNAME record found.

TXT records

SPF record

This record is valid for 30m.

Pass if the email sender's IP is in the MX records (with CIDR /24 for IPv4) of testfire.net.	mx/24
Or else, mark the email as fail.	-all

Smartinternz x Altoro Mutual x Temp Mail - Disposable x Whois testfire.net x Network Tools: DNS,JP, x DNS Lookup x DNS records for akamai x start of authority - Goo x +

Smartinternz x Altoro Mutual x Temp Mail - Disposable x Whois testfire.net x Network Tools: DNS,JP, x DNS Lookup x DNS records for akamai x start of authority - Goo x +

https://www.nslookup.io/domains/testfire.net/dns-records/ 90%

Kali Linux x Kali Tools x Kali Docs x Kali Forums x Kali NetHunter x Exploit-DB x Google Hacking DB x OffSec

Cloudflare Google DNS OpenDNS Authoritative Local DNS

NS records

Name server	Revalidate in
usw2.akam.net.	24h
eur2.akam.net.	24h
ns1-99.akam.net.	24h
usc3.akam.net.	24h
asia3.akam.net.	24h
usc2.akam.net.	24h
ns1-206.akam.net.	24h
eur5.akam.net.	24h

MX records

No mail servers found.

Other records

SOA

SOA data	Revalidate in
Start of authority	asia3.akam.net.
Email	hostmaster@akamai.com
Serial	1366025607
Refresh	12h
Retry	2h
Expire	168h
Negative cache TTL	24h

3)WHOIS INFORMATION GATHERING:

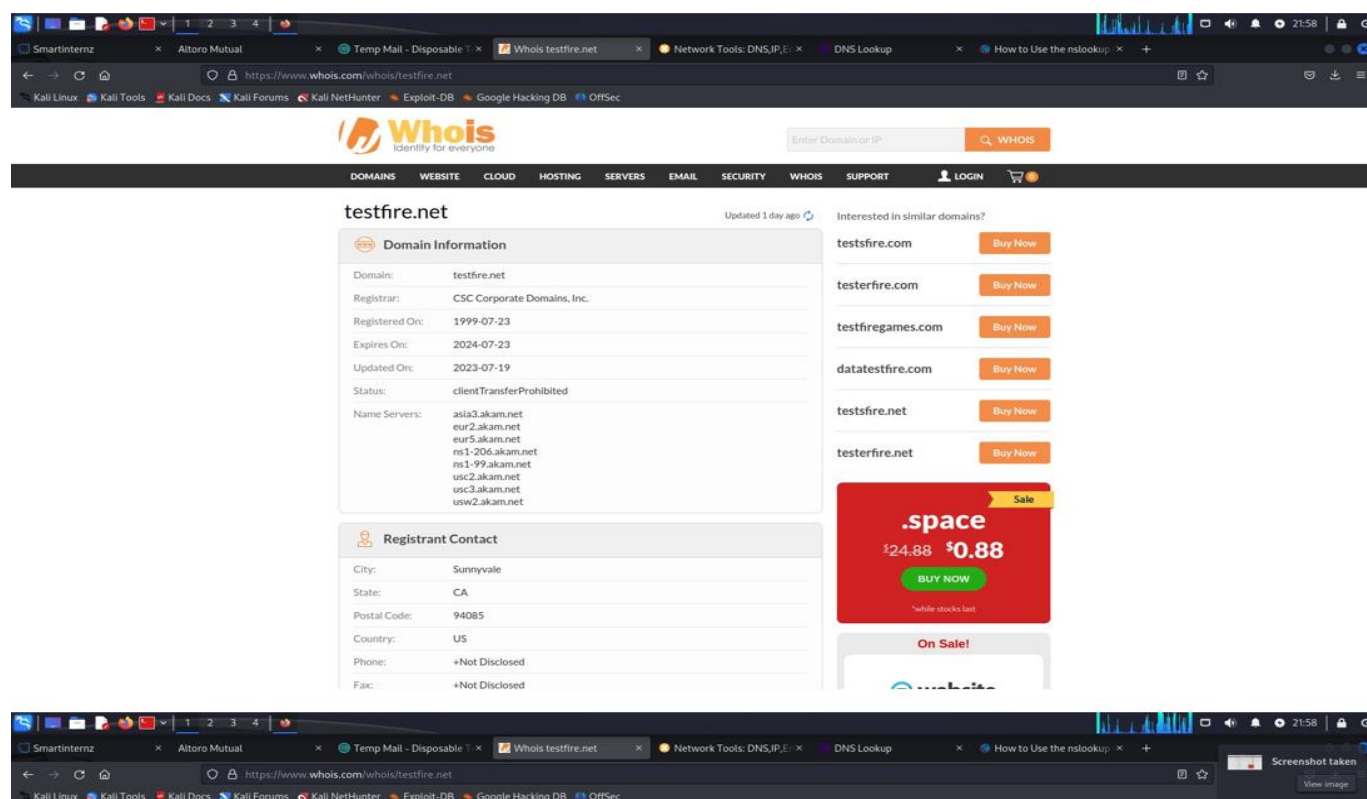
WHOIS information gathering involves accessing and analyzing the WHOIS database to retrieve valuable information about domain registrations, including details about the registrant, domain creation and expiration dates, contact information, and more. This process is essential for various purposes, such as domain ownership verification, cybersecurity, brand protection, and legal investigations.

Methods:

WHOIS Lookups: Using WHOIS lookup tools, online services, or command-line utilities, you can query the WHOIS database to retrieve information about a specific domain.

WHOIS Databases: Various online platforms and official registrar websites offer WHOIS lookup services, enabling you to input a domain name and receive relevant information.

Automated Tools: Some tools offer automated bulk WHOIS queries, allowing you to gather information about multiple domain names simultaneously.



SmartInternz x Altoro Mutual x Temp Mail - Disposable T x Whois testfire.net x Network Tools: DNS,IP,E x DNS Lookup x How to Use the nslookup x +

← → ↻ 🔍 https://www.whois.com/whois/testfire.net

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Registrant Contact

City: Sunnyvale
State: CA
Postal Code: 94085
Country: US
Phone: +Not Disclosed
Fax: +Not Disclosed

Administrative Contact

City: Sunnyvale
State: CA
Postal Code: 94085
Country: US
Phone: +Not Disclosed
Fax: +Not Disclosed

Technical Contact

City: Sunnyvale
State: CA
Postal Code: 94085
Country: US
Phone: +Not Disclosed
Fax: +Not Disclosed

.space
\$24.88 **\$0.88**
BUY NOW
*while stocks last


On Sale!
.xyz
XYZ @ \$2.88 ~~\$13.88~~

Introducing
WORDPRESS HOSTING
\$3.58 /mo
VIEW MORE

SmartInternz x Altoro Mutual x Temp Mail - Disposable T x Whois testfire.net x Network Tools: DNS,IP,E x DNS Lookup x How to Use the nslookup x +

← → ↻ 🔍 https://www.whois.com/whois/testfire.net

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Identity for everyone

DOMAINS WEBSITE CLOUD HOSTING SERVERS EMAIL SECURITY WHOIS SUPPORT LOGIN

testfire.net

Updated 1 day ago

Domain Information

Domain: testfire.net
Registrar: CSC Corporate Domains, Inc.
Registered On: 1999-07-23
Expires On: 2024-07-23
Updated On: 2023-07-19
Status: clientTransferProhibited
Name Servers: asia3.akam.net, eur2.akam.net, eur5.akam.net, ns1-206.akam.net, ns1-99.akam.net, usc2.akam.net, usc3.akam.net, usw2.akam.net

Registrant Contact

City: Sunnyvale
State: CA
Postal Code: 94085
Country: US
Phone: +Not Disclosed
Fax: +Not Disclosed

Interested in similar domains?

testsfire.com BUY NOW

testerfire.com BUY NOW

testfiregames.com BUY NOW

datatestfire.com BUY NOW

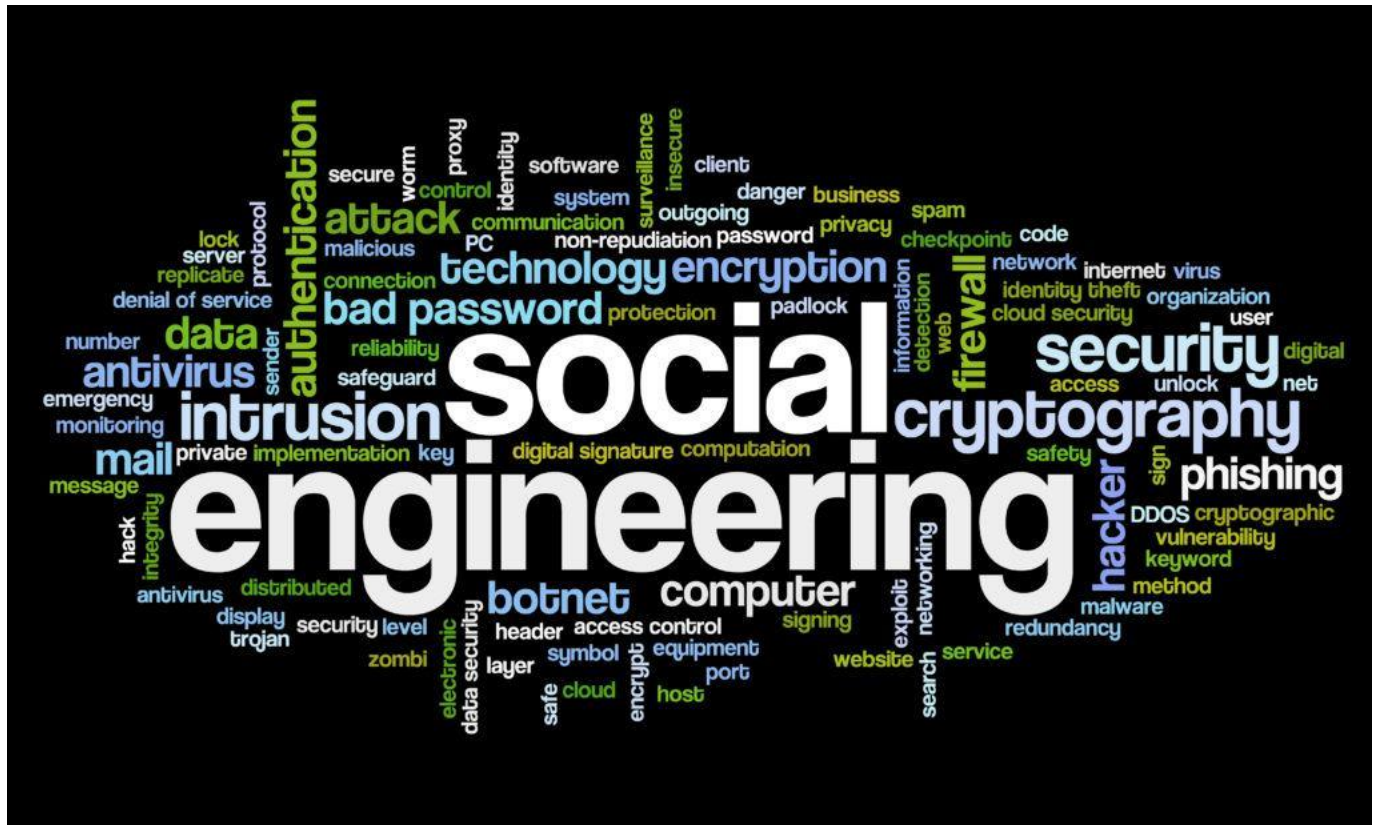
testsfire.net BUY NOW

testerfire.net BUY NOW

.space
\$24.88 **\$0.88**
BUY NOW
*while stocks last

On Sale!

4)Information Gathering for Social Engineering Attacks:



Step-1:

- Open the kali Linux
- Open the terminal
- Enter the command setoolkit



The screenshot shows a terminal window with a menu bar (File, Actions, Edit, View, Help) and a title bar (root@virtual: ~). The prompt is (root@virtual)-[~]. The command # setoolkit has been entered.

Step-2:

```

root@virtual: /home/virtual
File Actions Edit View Help

..#####..#####..#####
##.....##.....##.....
##.....##.....##.....
..#####..#####..#####
##.....##.....##.....
##.....##.....##.....
..#####..#####..#####
[—] The Social-Engineer Toolkit (SET) [—]
[—] Created by: David Kennedy (ReL1K) [—]
      Version: 8.0.3
      Codename: 'Maverick'
[—] Follow us on Twitter: @TrustedSec [—]
[—] Follow me on Twitter: @HackingDave [—]
[—] Homepage: https://www.trustedsec.com [—]
Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

```

```

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1

```

- Select from the menu of social engineering attack.

Step-3:

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules

99) Return back to the main menu.

set> 2
```

- Select from the menu in which you want to perform.

Step-4:

```
root@virtual: /home/virtual
File Actions Edit View Help

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks
in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a met
asploit based payload. Uses a customized java applet created by Thomas Werth
to deliver the payload.

The Metasploit Browser Exploit method will utilize select Metasploit browser
exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that
has a username and password field and harvest all the information posted to t
he website.

The TabNabbing method will wait for a user to move to a different tab, then r
efresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This met
hod utilizes iframe replacements to make the highlighted URL link to appear l
egitimate however when clicked a window pops up then is replaced with the mal
icious link. You can edit the link replacement settings in the set_config if
its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web att
```

```
root@virtual: /home/virtual
File Actions Edit View Help
efresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3
```

- Select from the menu in which you want to perform.

Step-5:

```
set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

- Select from the menu in which you want to perform.

5)Information Gathering for Physical Security Assessments:

Information gathering is a crucial step in conducting physical security assessments. It involves collecting open-source intelligence, such as pictures, maps, and company information, on the target organization. It also helps to identify the methods of entry, such as doors, locks, and windows, and the post-exploitation actions, such as accessing sensitive data or installing backdoors². Information gathering tools can include online databases, social media platforms, satellite imagery, and physical reconnaissance.

Information gathering for physical security assessments involves the systematic collection and analysis of data to assess the security measures, vulnerabilities, and risks associated with a physical location or facility. This process helps organizations identify potential weaknesses in their physical security infrastructure and develop strategies to mitigate them. The goal is to enhance the overall security posture and protect assets, personnel, and sensitive information from threats.

Key steps involved in information gathering for physical security assessments include:

Site Visits and Surveys: Physical security experts visit the facility to gather first-hand information about its layout, access points, entry and exit routes, security personnel deployment, existing security measures (e.g., access control systems, alarms, cameras), and potential vulnerabilities.

Blueprint and Floor Plan Analysis: Reviewing architectural blueprints and floor plans helps identify critical areas, potential escape routes, access points, utility locations, and areas prone to risks (e.g., windows, ventilation systems).

Interviews and Questionnaires: Engaging with relevant personnel, such as security staff, employees, and management, through interviews and questionnaires provides insights into security policies, procedures, incident history, and observations about security vulnerabilities.

Threat and Risk Assessment: Evaluating potential threats (e.g., theft, vandalism, sabotage, terrorism) and associated risks helps prioritize security measures. This may involve assessing the likelihood and impact of various threats and their potential consequences.

Asset Identification: Identifying and categorizing valuable assets (e.g., equipment, data, intellectual property) assists in understanding what needs protection and where security measures should be focused.

Security Technology Assessment: Reviewing the effectiveness and coverage of existing security technologies (e.g., surveillance cameras, access control systems, alarms) helps determine if they align with security objectives.

Physical Environment Analysis: Examining the surrounding environment (e.g., neighbouring properties, natural barriers) can reveal potential security vulnerabilities and opportunities to enhance physical security.

Threat Intelligence: Gathering information from open sources, law enforcement, and security agencies can provide insights into recent criminal activity or threats in the area.

Social Engineering Assessment: Assessing the susceptibility of employees to social engineering attacks (e.g., tailgating, impersonation) helps identify potential weaknesses in personnel security awareness.

Budget and Resource Considerations: Evaluating the available budget and resources helps ensure that proposed security enhancements are feasible and practical.

After gathering this information, organizations can develop a comprehensive physical security plan that outlines recommended improvements, enhancements, and countermeasures to address identified vulnerabilities and risks. This plan should prioritize actions based on potential impact, feasibility, and cost-effectiveness. Regular assessments and updates to the physical security plan are essential to adapt to changing threats and maintain a strong security posture.

Planning the Assessment

- Who will conduct the assessment?
 - Third party involvement
 - Team members
- What is the scope?
 - Process and controls
 - Security awareness- Is the team challenged for ID?
 - Removal of confidential customer information
 - Steal laptop, proprietary information
 - Social engineering included?
- Target selection
 - Regional location, size of facility, dates (schedule well in advance)

Physical Security Assessments

6)Emerging Trends and Technologies in Information Gathering:

The IT industry is always active and on the go. Whatever your interests are, the virtual world has something for you. Here are the top emerging trends in information technology unfolding with their brief encapsulation.

1. Artificial Intelligence and Machine Learning:

Artificial Intelligence (AI) and Machine Language (ML) have been unquestionably one of the latest advancements. Consequently, its market will reach \$267 billion by 2027. Today you can find AI and ML in every field, from finance and healthcare to manufacturing and retail. The robust AI and ML pair aims to improve, automate, and process time-sensitive data with minimal human interference requirements.

2. Advanced Analytics:

Advanced or predictive analytics generate a predictive model for specific Applications, like marketing. It combines Artificial Intelligence and statistical techniques to anticipate outcomes. You can evaluate historical data, identify patterns, and observe trends to determine potential future events before they happen.

3.Open-Source Intelligence (OSINT):

OSINT involves gathering information from publicly available sources, such as social media, news articles, forums, and websites. OSINT tools and techniques are continually evolving to better aggregate and analyze data from these sources, aiding in threat assessment and risk management.

4.Geospatial Intelligence (GEOINT):

GEOINT integrates geographic information systems (GIS) with various data sources, such as satellite imagery and sensor networks. This enables organizations to analyze and visualize spatial data, aiding in areas like disaster response, urban planning, and security assessments.

5.Internet of Things (IoT):

The proliferation of IoT devices provides a wealth of data that can be collected and analysed for various purposes, including monitoring and managing physical assets, environmental conditions, and infrastructure.

6.Drones and Unmanned Aerial Vehicles (UAVs):

Drones equipped with cameras, sensors, and other data collection tools are used for aerial surveillance, mapping, and data gathering in areas that might be difficult or dangerous for humans to access.

7.Virtual Reality (VR) and Augmented Reality (AR):

VR and AR technologies offer new ways to visualize and interact with data. In information gathering, they can be used for immersive training, virtual walkthroughs, and data visualization.

8.Blockchain Technology:

Blockchain's decentralized and tamper-proof nature can enhance the security and reliability of information gathered and shared within a network. It can be particularly useful in ensuring the integrity of data in supply chains and transactions.

9.Quantum Computing:

While still in its infancy, quantum computing has the potential to revolutionize data processing and analysis by solving complex problems much faster than traditional computers. This could have significant implications for information gathering and analysis.

10.Biometric and Facial Recognition:

Advances in biometric technology and facial recognition systems are being used for identity verification, access control, and security monitoring.

11.Social Media Analytics:

As social media continues to play a significant role in communication, sentiment analysis and social media monitoring tools help organizations gauge public opinion, track trends, and identify potential security threats.

12.Automated Threat Intelligence:

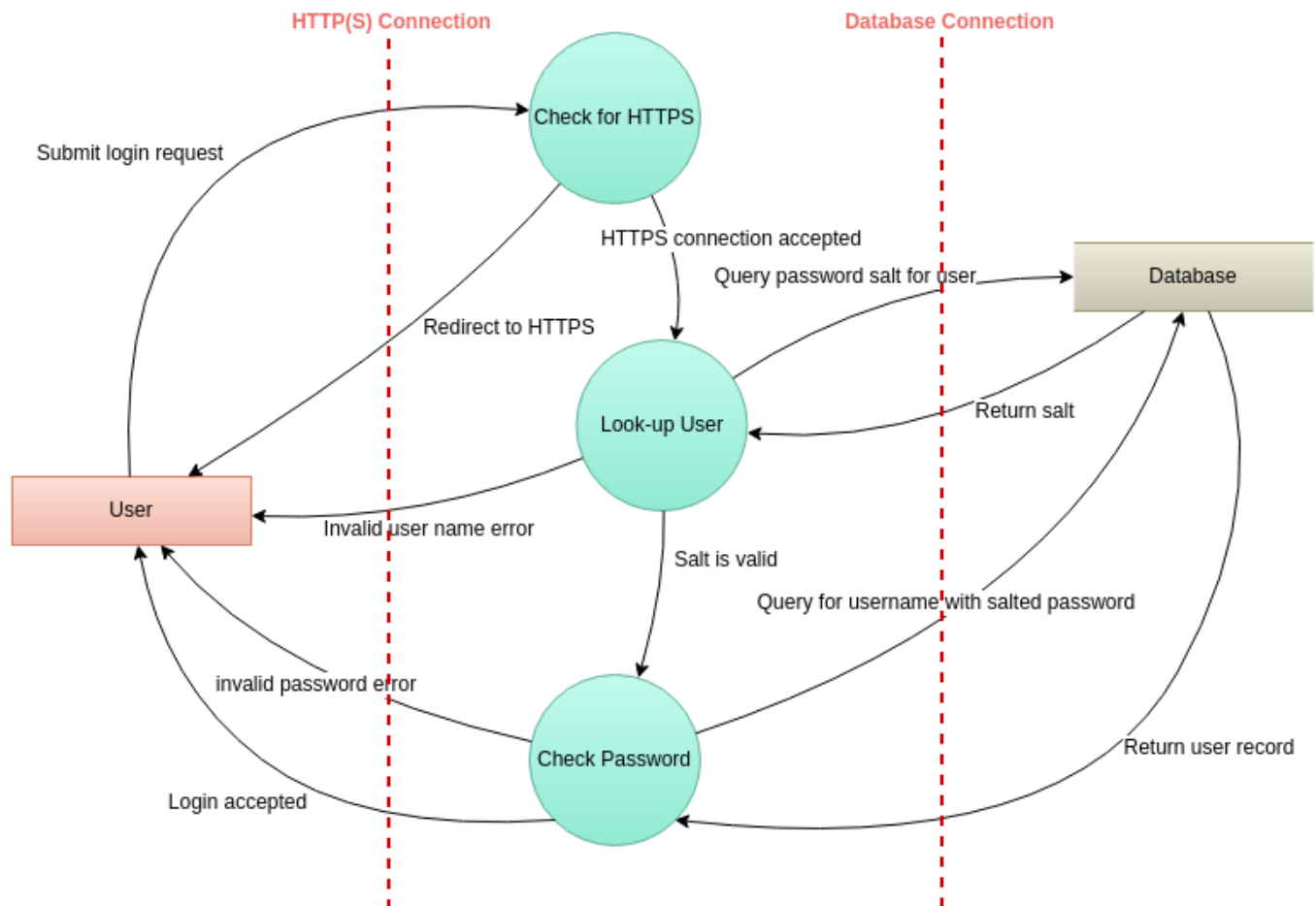
Automation tools are increasingly used to gather, analyze, and disseminate threat intelligence, helping organizations respond more effectively to emerging security risks.

Remember that while these trends and technologies offer exciting possibilities for information gathering, they also raise ethical, privacy, and security considerations that need to be carefully addressed. Organizations must adopt these technologies responsibly and ensure compliance with relevant regulations and standards.

Threat Modelling:

Threat modelling is a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified and enumerated, and countermeasures prioritized. It works to identify, communicate, and understand threats and mitigations within the context of protecting something of value. It is a planned activity for identifying and assessing application threats and vulnerabilities.

Identify potential threats and risks that the wireless network may face. Consider factors such as unauthorized access, eavesdropping, data interception, and rogue devices.



Threat modelling is a structured approach used to identify and prioritize potential threats to a system, application, or network. It involves systematically analyzing and documenting potential vulnerabilities, attack vectors, and risks in order to make informed decisions about security controls and mitigation strategies. Threat modelling helps organizations proactively identify and address security concerns before they can be exploited by malicious actors. Here's an overview of the threat modelling process:

1.Scope Definition:

Clearly define the scope of the threat modelling exercise. Identify the system, application, or network that you want to assess for security threats. Understand the system's components, boundaries, and interactions.

2.Asset Identification:

Identify and enumerate the valuable assets within the system. This could include sensitive data, user credentials, hardware components, software modules, and more.

3.Identify Threats:

Brainstorm and list potential threats that could exploit vulnerabilities in the system. Consider both internal and external threats, such as unauthorized access, data breaches, denial-of-service attacks, and social engineering.

4.Vulnerability Analysis:

Analyze the system's components to identify vulnerabilities that could be exploited by the identified threats. Evaluate weaknesses in design, configuration, authentication mechanisms, and other aspects of the system.

5.Attack Surface Analysis:

Determine the potential entry points or attack vectors that an adversary could use to exploit vulnerabilities. This could involve analyzing interfaces, APIs, communication channels, and user interactions.

6.Risk Assessment:

Evaluate the potential impact and likelihood of each identified threat. Assign a risk score or rating to each threat based on its potential consequences and the likelihood of it occurring.

7.Mitigation Strategies:

Develop and prioritize mitigation strategies to address the identified threats. Consider security controls, countermeasures, and best practices that can reduce the likelihood or impact of each threat.

8.Security Control Implementation:

Implement the selected security controls and mitigation strategies to reduce the identified risks. This could involve implementing access controls, encryption, monitoring systems, intrusion detection mechanisms, and more.

9.Validation and Testing:

Test the effectiveness of the implemented security controls through various methods, such as penetration testing, vulnerability scanning, and code review. Verify that the mitigation strategies adequately address the identified threats.

10.Documentation:

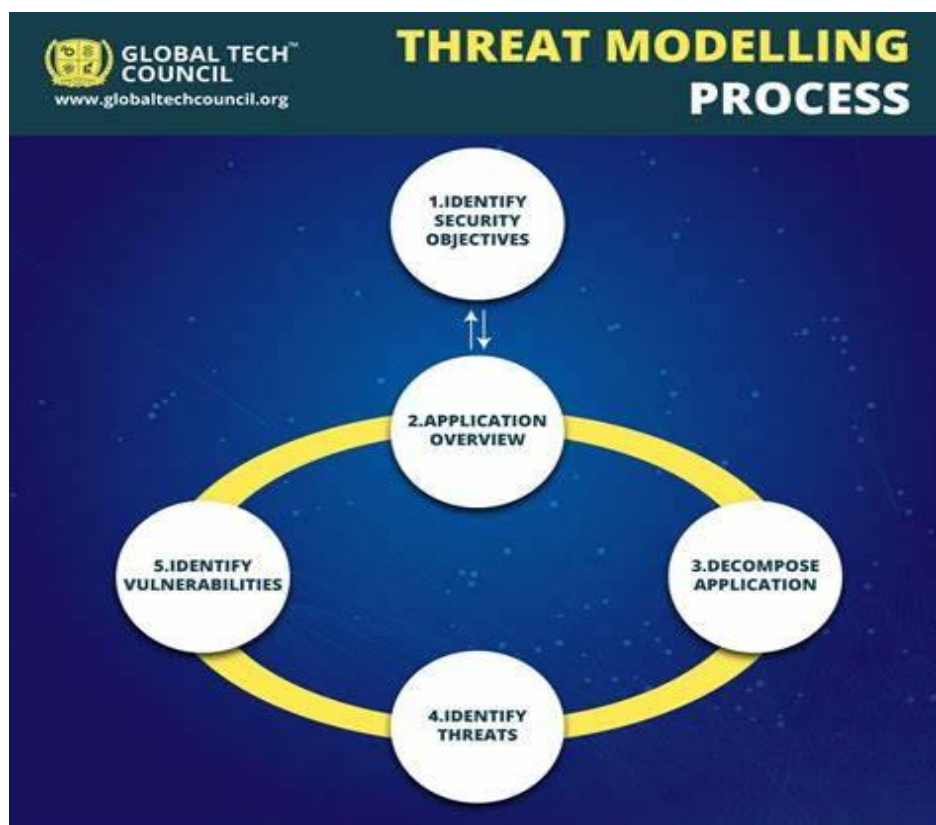
Document the threat modelling process, including the identified threats, vulnerabilities, risks, and the corresponding mitigation measures. This documentation serves as a reference for future assessments and provides transparency for stakeholders.

11.Iterative Process:

Threat modelling is an ongoing process. As the system evolves, new threats may emerge, and existing threats may change in significance. Regularly revisit and update the threat model to ensure it remains relevant and effective.

12.Training and Awareness:

Educate relevant stakeholders, including developers, administrators, and users, about the threat model and the security practices in place. Raise awareness about potential threats and best practices to mitigate them.



Vulnerability Assessment:

Certainly, a vulnerability assessment is a crucial part of a wireless network security assessment project. It involves systematically identifying and evaluating potential weaknesses and vulnerabilities within your organization's wireless network infrastructure. Here's a detailed overview of the vulnerability assessment process:

Vulnerability Assessment for Wireless Network Security:

1. **Preparation:**

- Define the scope of the vulnerability assessment, including which systems, devices, and components will be evaluated.
- Gather information about the wireless network's architecture, hardware, software, and configurations.
- Identify key stakeholders and establish communication channels for reporting findings.

2. **Vulnerability Identification:**

- Use automated vulnerability scanning tools to identify potential security flaws, misconfigurations, and weaknesses.
- Scan wireless access points, routers, switches, and other network components.
- Detect vulnerabilities in authentication mechanisms, encryption protocols, and wireless communication.

3. **Vulnerability Analysis:**

- Assess the severity and potential impact of each identified vulnerability.
- Prioritize vulnerabilities based on factors such as exploitability, potential data exposure, and network impact.

4. **Risk Assessment:**

- Estimate the risk associated with each vulnerability by considering factors like likelihood of exploitation and potential consequences.
- Categorize vulnerabilities into low, medium, and high-risk levels.

5. **Verification and Validation:**

- Manually verify critical vulnerabilities to confirm their presence and potential impact.
- Ensure that false positives and false negatives are minimized through manual assessment.

6. **Impact Analysis:**

- Assess the potential impact of exploiting vulnerabilities on the confidentiality, integrity, and availability of the wireless network and associated data.
- Consider potential scenarios involving data breaches, unauthorized access, and network disruption.

7. ****Recommendations:****

- Offer actionable recommendations to address each identified vulnerability.
 - Provide guidance on how to apply patches, reconfigure settings, or implement additional security controls.
- Prioritize recommendations based on risk severity and potential impact.

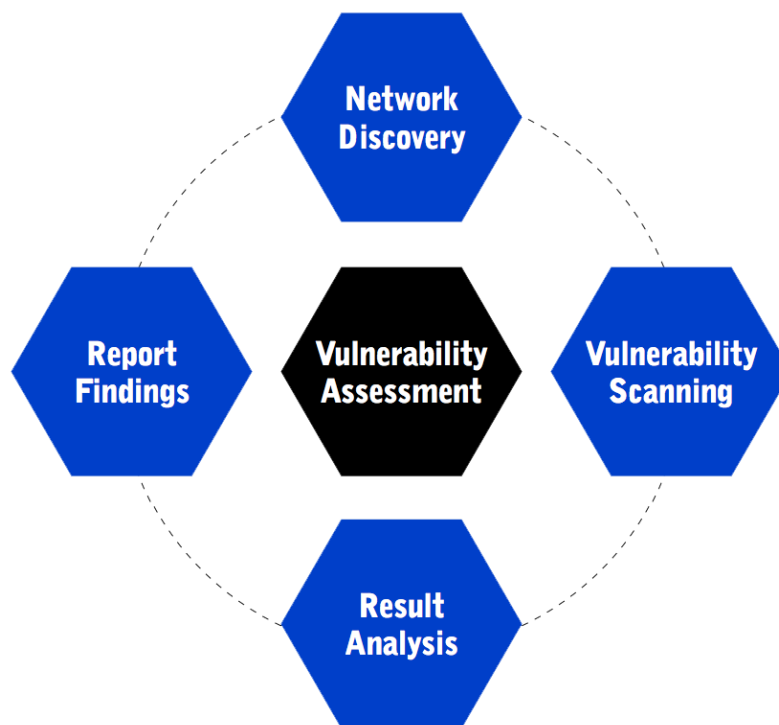
8. ****Remediation Planning:****

- Collaborate with relevant teams to plan and schedule the implementation of recommended fixes and security measures.
- Establish a timeline for addressing vulnerabilities based on risk assessment and available resources.

9. ****Continuous Monitoring:****

- Implement continuous monitoring mechanisms to detect and mitigate new vulnerabilities as they arise.
- Regularly conduct follow-up vulnerability assessments to ensure that security measures are effective and up to date.

A well-executed vulnerability assessment helps organizations proactively identify and address security weaknesses in their wireless network infrastructure. By systematically evaluating vulnerabilities and taking appropriate remediation actions, organizations can enhance the overall security posture of their wireless networks and reduce the risk of potential breaches or cyberattacks.



Step 1:

- [illegible]

Step 2:

- ```

File Edit View Bookmarks Plugins Settings Help
 ▢ New Tab ▢ Split View ▾

TX packets 67319 bytes 7390270 (7.0 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(john@john) [-]
nmap 192.168.55.104
Starting Nmap 7.94 (https://nmap.org) at 2023-07-31 17:24:15
Nmap scan report for 192.168.55.104
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.55.104 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

(john@john) [-]
$ nmap 192.168.55.104,0/24
Starting Nmap 7.94 (https://nmap.org) at 2023-07-31 17:25:15
Failed to resolve '192.168.55.104'
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.35 seconds

(john@john) [-]
$ nmap 192.168.55.0/24
Starting Nmap 7.94 (https://nmap.org) at 2023-07-31 17:26:15
Nmap scan report for 192.168.55.1
Host is up (0.027s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp open telnet
25/tcp open domain
80/tcp open http
161/tcp filtered snmp
5555/tcp filtered freeciv

Nmap scan report for 192.168.55.101
Host is up (0.0046s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT STATE SERVICE
524/tcp open atp
9999/tcp open abyss

Nmap scan report for 192.168.55.103
Host is up (0.00015s latency).
All 1000 scanned ports on 192.168.55.103 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.55.104
Host is up (0.000082s latency).
All 1000 scanned ports on 192.168.55.104 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (4 hosts up) scanned in 6.33 seconds

(john@john) [-]

```



Step :3

- Enter the command “ nmap –script vuln IP address ”

```
80/tcp open http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-slowloris-check:
| VULNERABLE:
| Slowloris DOS attack
| State: LIKELY VULNERABLE
| IDs: CVE:CVE-2007-6750
| Slowloris tries to keep many connections to the target web server open and hold
| them open as long as possible. It accomplishes this by opening connections to
| the target web server and sending a partial request. By doing so, it starves
| the http server's resources causing Denial Of Service.
|
| Disclosure date: 2009-09-17
| References:
| http://ha.ckers.org/slowloris/
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp open https
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 1395.11 seconds
```

- IDs: CVE: CVE-2007-6750

Step 4:

- Search for vulnerability of CVE-2007-6750

| Name                          | Description                                                                                                                                                                                                                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CVE-2007-6750</a> | The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.16. |

BACK TO TOP

| Assigning CNA       |                                                                                                                                                                                                                                                               |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MITRE Corporation   |                                                                                                                                                                                                                                                               |
| Date Record Created |                                                                                                                                                                                                                                                               |
| 20111227            | Disclaimer: The <a href="#">record creation date</a> may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE. |
| Phase (Legacy)      |                                                                                                                                                                                                                                                               |
| Assigned (20111227) |                                                                                                                                                                                                                                                               |

## **Assigning CWE codes to each vulnerability:**

1. SQL Injection (SQLi): CWE-89
2. Cross-Site Scripting (XSS): CWE-7949
3. Cross-Site Request Forgery (CSRF): CWE-352
4. Remote Code Execution (RCE): CWE-94
5. Server-Side Request Forgery (SSRF): CWE-918
6. XML External Entity (XXE) Injection: CWE-611
7. Local File Inclusion (LFI)\*\*: CWE-22
8. Remote File Inclusion (RFI): CWE-98
9. Insecure Direct Object References (IDOR): CWE-639
10. Buffer Overflow: CWE-120
11. Missing Security Updates/Patches: CWE-937
12. Insecure Authentication: CWE-287
13. Insecure Communication: CWE-319
14. Insecure Deserialization: CWE-502
15. Weak Passwords: CWE-521
16. Information Disclosure: CWE-200
17. Security Misconfigurations: CWE-815
18. Zero-Day Vulnerabilities: CWE-937 (Similar to missing security updates, as zero-day vulnerabilities are unknown and unpatched.

## **Authentication and Encryption Evaluation:**

Authentication and encryption are crucial aspects of wireless network security. Evaluating the effectiveness of these mechanisms is an essential step in ensuring the confidentiality and integrity of data transmitted over the network. Here's a detailed overview of the authentication and encryption evaluation process:

### **Authentication and Encryption Evaluation for Wireless Network Security:**

#### **1. \*\*Authentication Mechanisms:\*\***

- Review the various authentication methods in use, such as WPA2, WPA3, EAP, and captive portal.
- Assess the strength of authentication credentials and password policies.
- Identify any instances of default or weak credentials that could be exploited by attackers.

#### **2. \*\*Encryption Protocols:\*\***

- Evaluate the encryption protocols employed, such as WEP, WPA2, and WPA3.
- Determine whether the latest encryption standards are in use (e.g., transitioning from WPA2 to WPA3).
- Identify any instances of outdated or deprecated encryption protocols that pose security risks.

#### **3. \*\*Key Management:\*\***

- Examine the methods used for key distribution and management in the wireless network.
- Assess the frequency of key rotation and the process for updating encryption keys.

#### **4. \*\*Wireless SSID Configuration:\*\***

- Review the SSID (Service Set Identifier) configurations for broadcast and visibility.
- Determine whether hidden SSIDs are being used and assess the security implications.

#### **5. \*\*Authentication Factors:\*\***

- Analyze the use of multi-factor authentication (MFA) to enhance security.
- Evaluate the implementation of MFA using factors like passwords, tokens, or biometrics.

#### **6. \*\*Certificate Management:\*\***

- Assess the use of digital certificates for authentication and encryption purposes.
- Verify the validity and expiration of certificates used in the wireless network.

## **7. \*\*Guest Network Access:\*\***

- Evaluate the security measures in place for guest or public network access.
- Ensure that guest networks are isolated from internal resources and properly secured.

## **8. \*\*Vulnerability Analysis:\*\***

- Perform vulnerability assessments and penetration testing on authentication and encryption mechanisms.
- Test for potential weaknesses, such as brute-force attacks, dictionary attacks, or vulnerabilities in the encryption protocols.

## **9. \*\*Compliance and Standards:\*\***

- Ensure that authentication and encryption practices comply with industry standards (e.g., PCI DSS, HIPAA) and best practices.
- Review whether security configurations align with recommended guidelines from security organizations.

## **10. \*\*Documentation and Reporting:\*\***

- Document the findings related to authentication and encryption mechanisms, including strengths and weaknesses.
- Include detailed recommendations for improving authentication and encryption security.

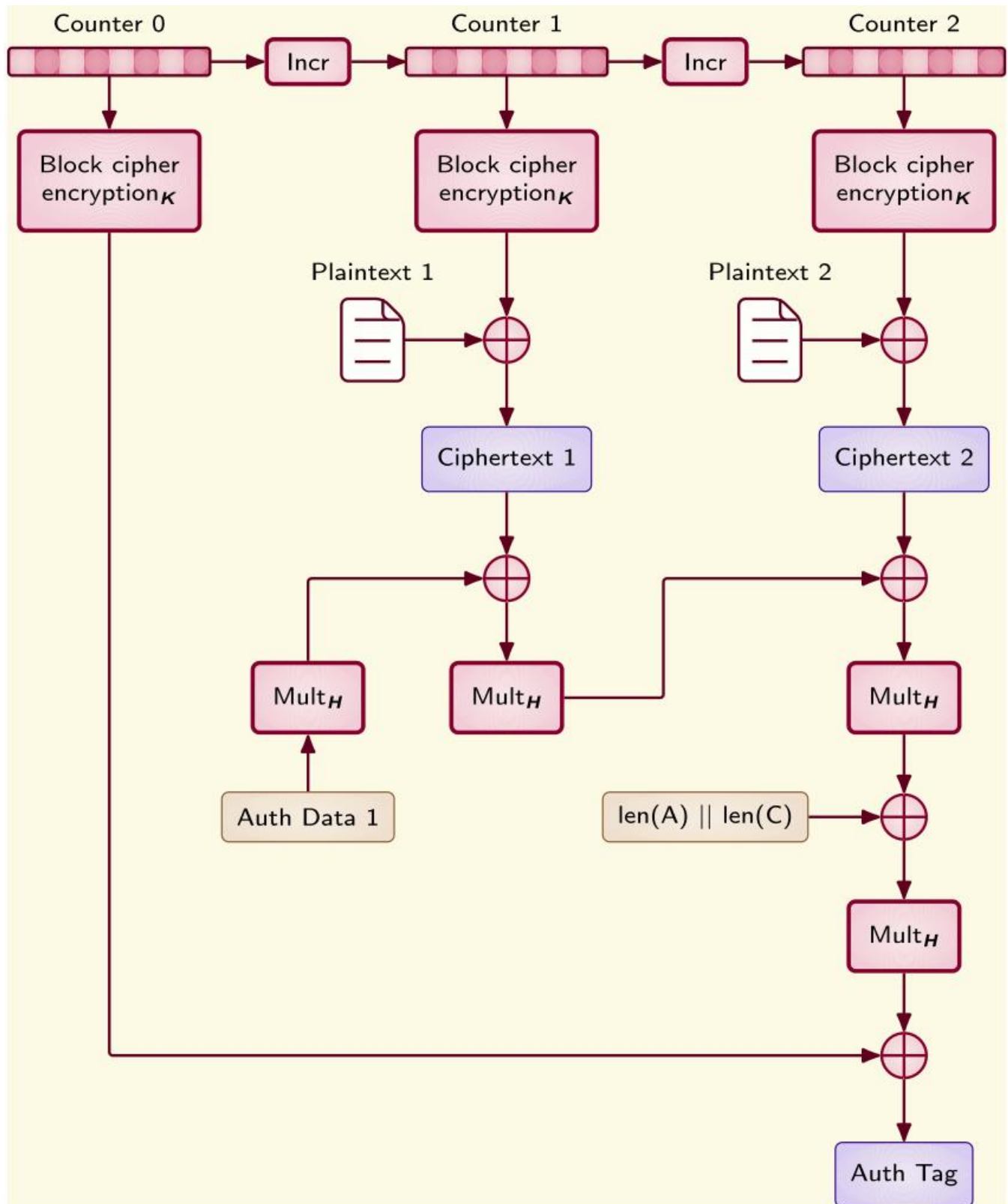
## **11. \*\*Recommendations and Remediation:\*\***

- Provide actionable recommendations for enhancing authentication and encryption security.
- Suggest measures such as upgrading to stronger encryption protocols, enforcing MFA, and regularly updating authentication credentials.

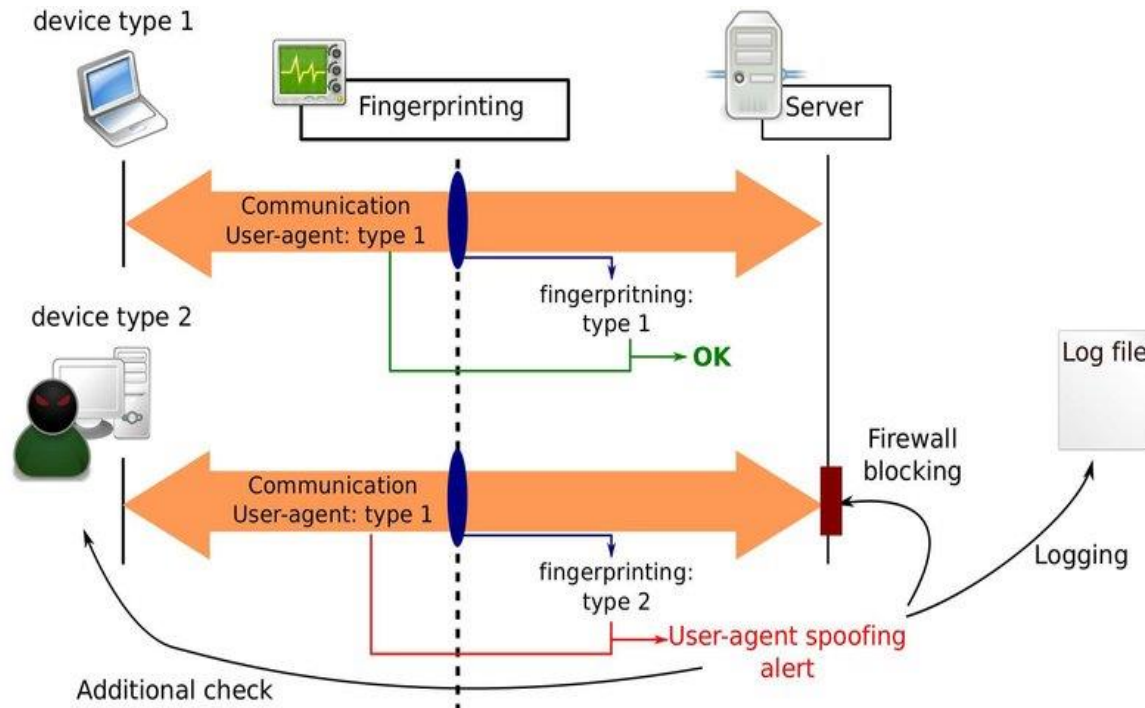
## **12. \*\*Implementation and Follow-Up:\*\***

- Collaborate with relevant teams to implement recommended changes and enhancements.
- Monitor the implementation to ensure that authentication and encryption improvements are successfully applied.

By evaluating authentication and encryption mechanisms within your wireless network, you can identify vulnerabilities and weaknesses that could potentially be exploited by attackers. Strengthening these aspects of network security helps safeguard sensitive data and communications, ensuring that only authorized users can access and transmit information within the network.



## Rogue Device Detection:



Detecting and mitigating rogue devices is a critical component of wireless network security. Rogue devices can pose serious security risks by providing unauthorized access points for attackers or introducing vulnerabilities into the network. Here's an overview of the rogue device detection process:

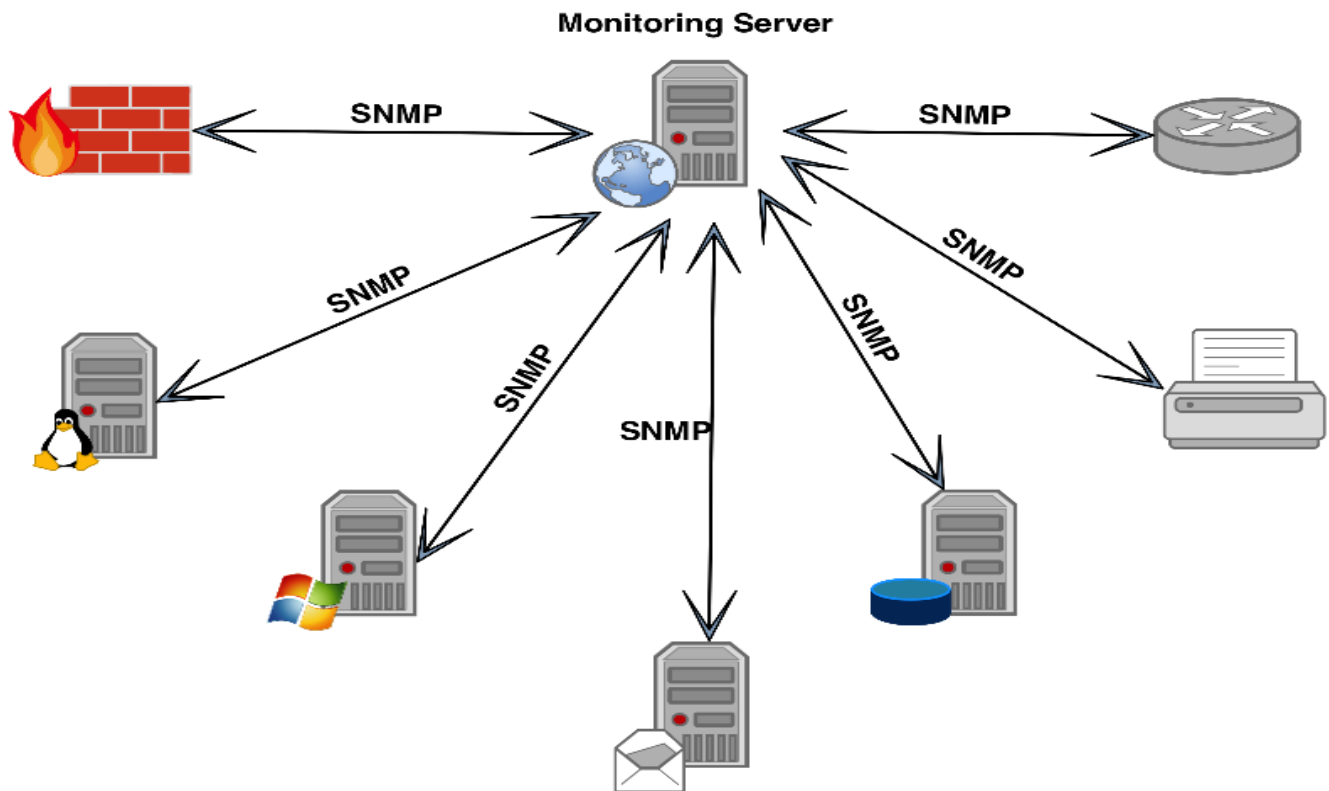
### **Rogue Device Detection for Wireless Network Security:**

#### **1. \*\*Network Monitoring and Analysis:\*\***

- Implement network monitoring tools to continuously monitor wireless traffic and access points.
- Collect data on connected devices, MAC addresses, signal strength, and traffic patterns.

Network monitoring systems include software and hardware tools that can track various aspects of a network and its operation, such as traffic, bandwidth utilization, and uptime. These systems can detect devices and other elements that comprise or touch the network, as well as provide status updates.

Network administrators rely on network monitoring systems to help them quickly detect device or connection failures or issues such as traffic bottlenecks that limit data flow. The ability to detect issues extends to parts of the network traditionally beyond their demarcation boundaries. These systems can alert administrators to issues by email or text and deliver reports using network analytics.

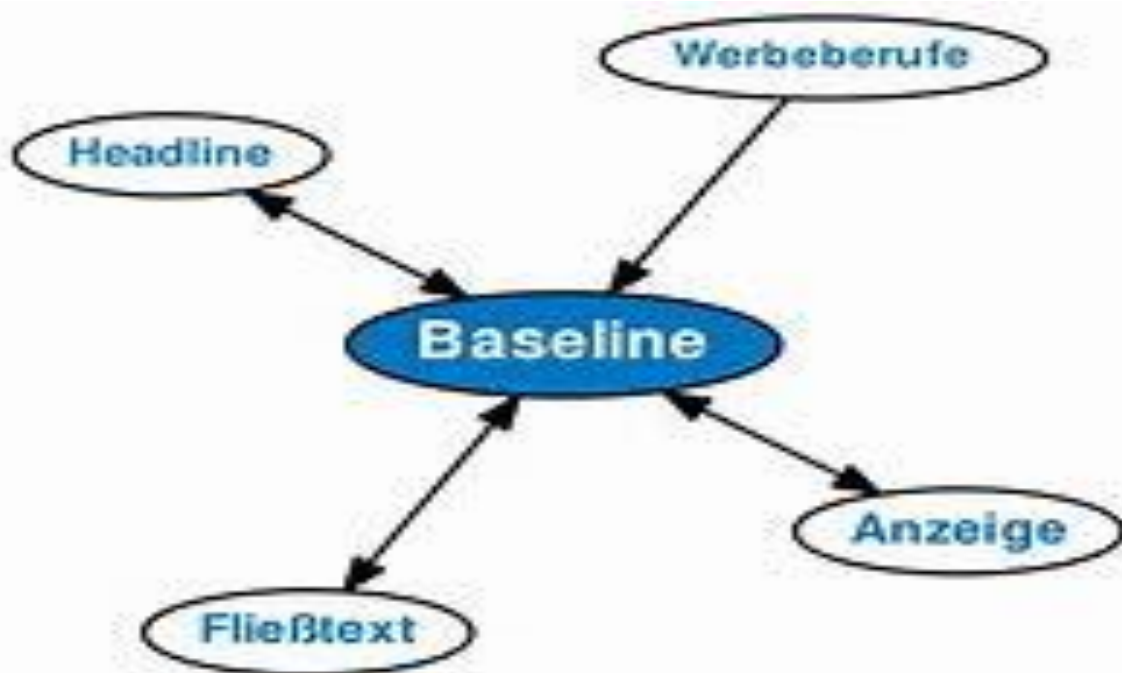


## 2. **\*\*Baseline Establishment:\*\***

- Establish a baseline of normal device behaviour and network activity.
- Monitor and analyze patterns to detect deviations that could indicate the presence of rogue devices.

A baseline may be established for the singular purpose of marking an approved configuration item, e.g., a project plan that has been signed off for execution. Associating multiple configuration items to such a baseline indicates those items as also being approved. Baselines may also be used to mark milestones.

Baselines themselves are valued not only to identify the notable state of work product(s) but also provide historical views of how work product elements have progressed together over time. When a fixed baseline is retrieved, the state of the work product(s) in that subset share the same significance in their history of changes; this allows project leaders to compare the relative progress of single parts of a project to the project as a whole, which allows project leaders to identify individual items that lag or lead in progress toward better functionality or performance. For this reason, baseline identification, monitoring, and retrieval are critical to the success of configuration management, and ultimately, project quality.



Quelle: <https://wirtschaftslexikon.gabler.de/definition/baseline-2766>

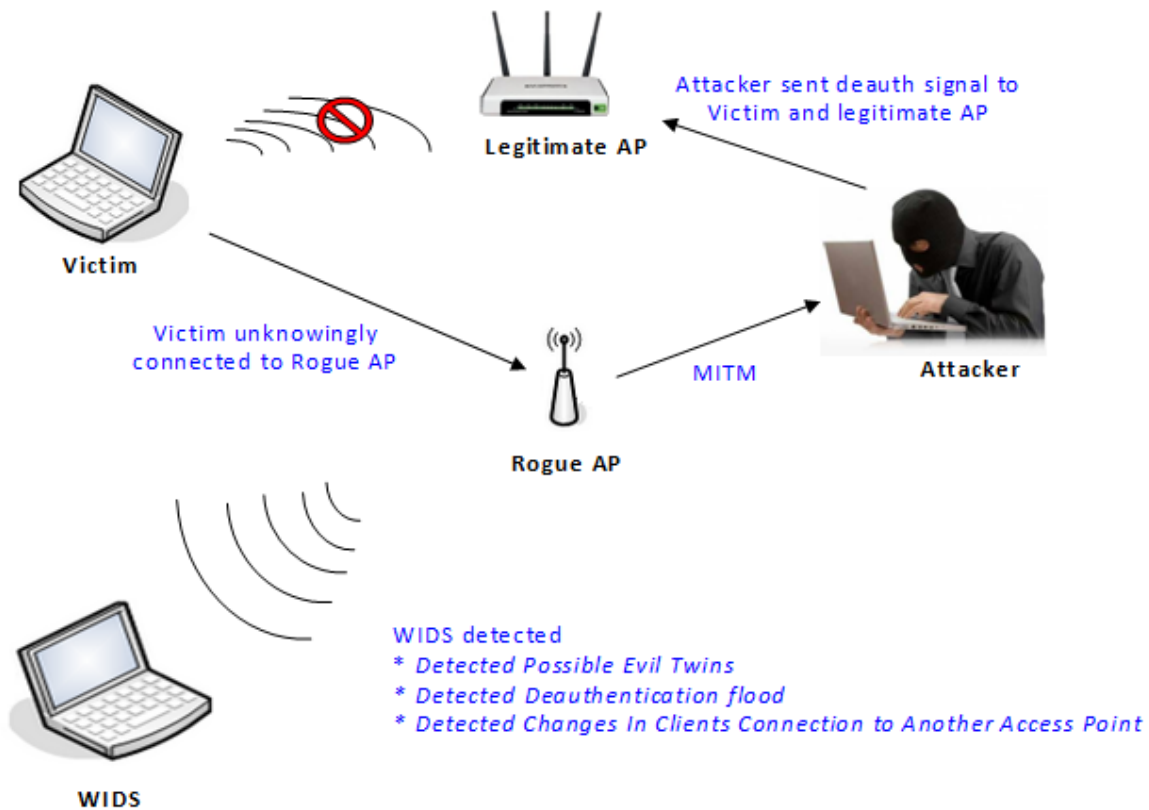
### 3. **\*\*Wireless Intrusion Detection Systems (WIDS):\*\***

- Deploy a wireless intrusion detection system (WIDS) to actively scan for unauthorized devices.
- Configure WIDS to detect and alert on anomalies, unusual behaviour, or unauthorized access points.

A wireless intrusion detection system (WIDS) monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools. The system monitors the radio spectrum used by wireless LANs, and immediately alerts a systems administrator whenever a rogue access point is detected. Conventionally it is achieved by comparing the MAC address of the participating wireless devices.

Rogue devices can spoof MAC address of an authorized network device as their own. New research uses fingerprinting approach to weed out devices with spoofed MAC addresses. The idea is to compare the unique signatures exhibited by the signals emitted by each wireless device against the known signatures of pre-authorized, known wireless devices.



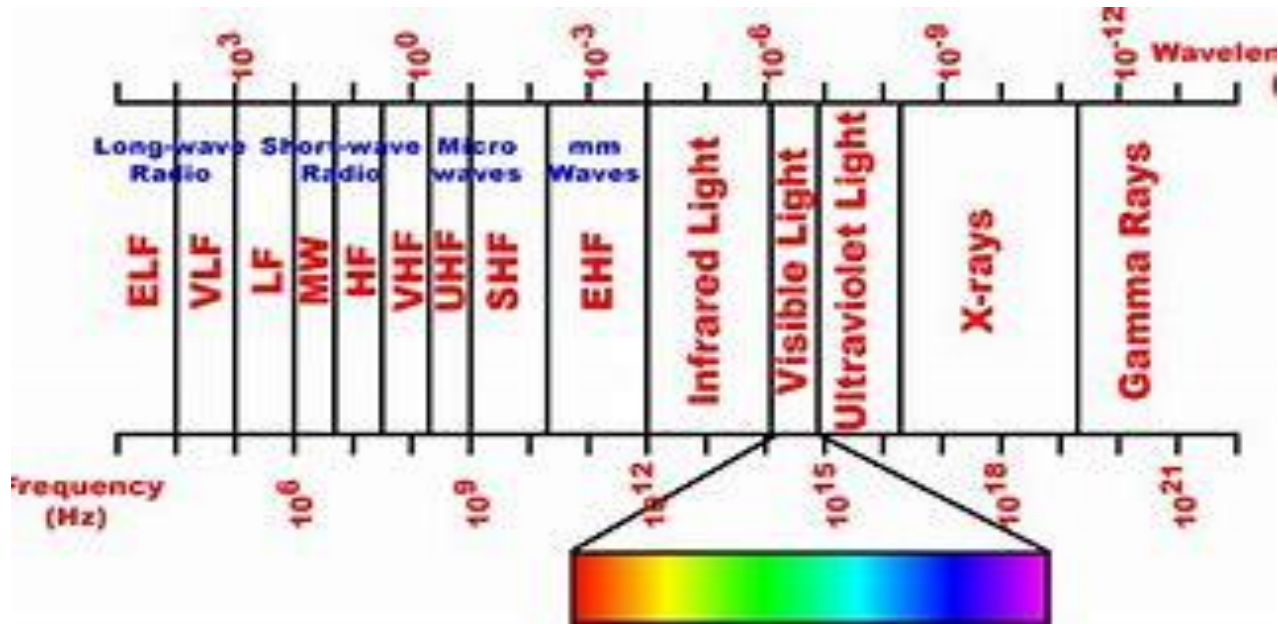


#### 4. **\*\*Radio Frequency (RF) Scanning:\*\***

- Perform regular RF scanning to identify nearby wireless networks and devices.
- Detect any unauthorized or unknown access points operating within the organization's vicinity.

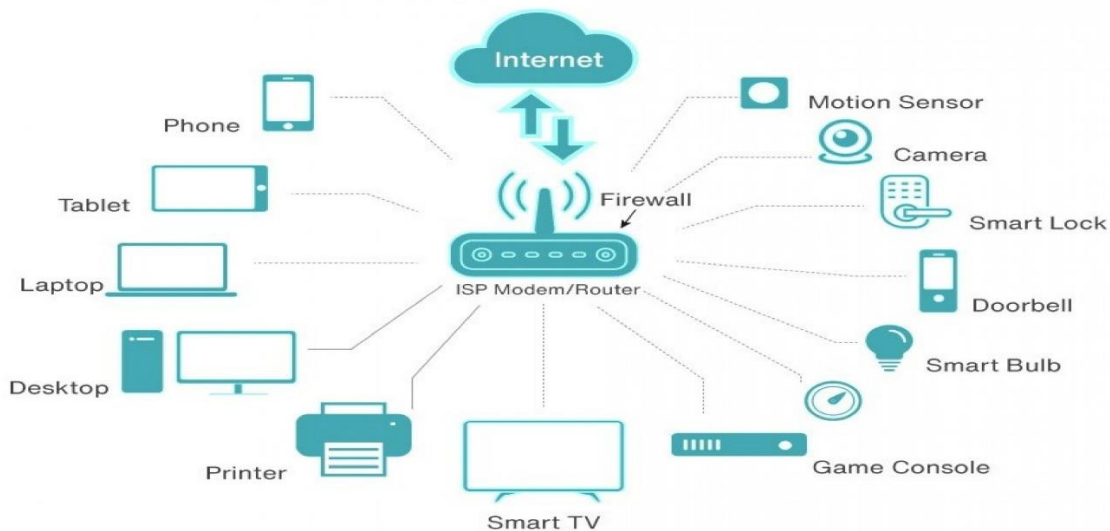
Radio frequency (RF) is the oscillation rate of an alternating electric current or voltage or of a magnetic, electric or electromagnetic field or mechanical system in the frequency range from around 20 kHz to around 300 GHz. This is roughly between the upper limit of audio frequencies and the lower limit of infrared frequencies. These are the frequencies at which energy from an oscillating current can radiate off a conductor into space as radio waves, so they are used in radio technology, among other uses. Different sources specify different upper and lower bounds for the frequency range.

A traditional spectrum analyser searches for signals within a spectral bandwidth and provides snapshots of the signal in the frequency or modulation domain. However, this is often not enough information to confidently describe the dynamic nature of modern RF signals.



## 5. \*\*Network Segmentation and Isolation:\*\*

Network isolation and segmentation are techniques used to improve network performance and security. They involve dividing a computer network into smaller parts called VLANs (virtual local area networks) or subnetworks. Segmentation creates isolation and determines if two endpoints should access each other. It lessens the attack surface, obstructing lateral movement, and isolates attacks before they spread<sup>1</sup>. Segmentation is an effective way of detecting and containing adversary movements.



## 6. \*\*MAC Address Monitoring:\*\*

- Maintain a whitelist of approved MAC addresses for authorized devices.
- Monitor for any MAC addresses not on the whitelist and investigate anomalies.

In today's networks, MAC addresses more than just uniquely identify network devices and enable network communications. They are essential for helping network protocols to properly function, and for core network devices to dynamically allocate and manage IPs. MAC address scanning enables you to gain in-depth insights into the network architecture and the associated network devices in your organization.

Tracking your network devices with an effective MAC address scanner assists you with network maintenance and effectively monitoring the devices connecting to your network. A MAC IP scanner also enables you to enhance network security by identifying malicious devices using their MAC addresses, and blocking their access to your network.

```
Command Prompt
Windows IP Configuration

Host Name : TestPC1-HP
Primary Dns Suffix :
Node Type : Hybrid
IP Routing Enabled. :
WINS Proxy Enabled. :

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . :
Description : Realtek PCIe GBE Family Controller
Physical Address. : E0-69-95-DA-67-EC
DHCP Enabled. : Yes
Autoconfiguration Enabled : Yes
Link-local IPv6 Address : fe80::5935:6361:ba6d:875%2(Preferred)
IPv4 Address. : 10.138.236.138(Preferred)
Subnet Mask : 255.255.255.0
Lease Obtained. : Monday, November 2, 2015 4:52:22 PM
Lease Expires : Wednesday, November 4, 2015 9:31:51 AM
Default Gateway : 10.138.236.71
DHCP Server : 10.138.236.71
DHCPv6 IAID : 283142549
```

### 13. **\*\*User Awareness and Training:\*\***

- Educate users about the risks of connecting unauthorized devices to the network.
- Encourage users to report any suspicious or unknown devices to the IT/security team.

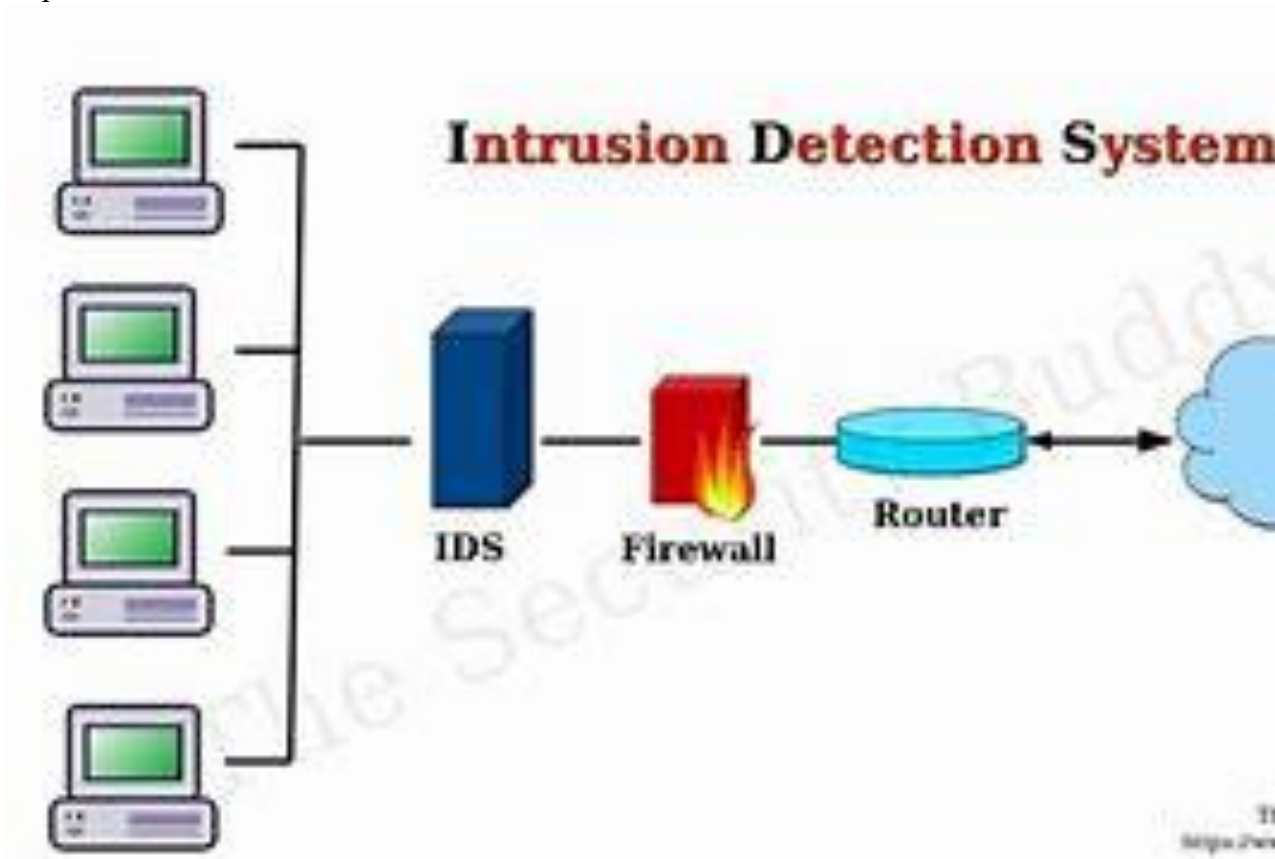
User awareness training is an education activity whose aim is to teach employees about cybersecurity. It provides cybersecurity training and education for employees, so they have the information they need to avoid the many dangers that lurk online, including malware, phishing, man-in-the-middle attacks, eavesdropping attacks, and others. The importance of user awareness and cybersecurity training for employees has increased exponentially in the last decade because employees now face a much broader range of cyber threats than ever before, many of which, such as ransomware, are capable of inflicting massive damage to the entire organization. User awareness training is typically performed as a comprehensive security awareness program that educates employees about a multitude of cybersecurity-related topics. It may involve mock attack simulations to test and reinforce good behaviour, and it can either take place online or in person.





## **Intrusion Detection Testing:**

Intrusion detection testing is a crucial aspect of wireless network security assessment, aimed at evaluating the effectiveness of your network's intrusion detection and prevention mechanisms. It involves simulating various attack scenarios to determine how well your network can detect and respond to unauthorized activities.



### **Intrusion Detection Testing for Wireless Network Security:**

#### **1. \*\*Preparation:\*\***

- Define the scope of intrusion detection testing, including the specific attack scenarios to be simulated.
- Identify the types of attacks to be tested, such as unauthorized access attempts, data exfiltration, and denial of service (DoS) attacks.

#### **2. \*\*Test Environment Setup:\*\***

- Create a controlled testing environment that mirrors the organization's wireless network architecture.
- Set up test access points, devices, and servers to simulate real-world network traffic and interactions.

### 3. **\*\*Attack Scenario Simulation:\*\***

- Simulate various attack scenarios to test the intrusion detection and prevention systems.
- Examples of attack scenarios include brute-force password attacks, unauthorized device connections, and suspicious traffic patterns.

### 4. **\*\*Data Collection and Analysis:\*\***

- Monitor network traffic and system logs during the attack simulations.
- Collect data on alerts triggered, response times, and effectiveness of intrusion detection mechanisms.

### 5. **\*\*False Positive and Negative Assessment:\*\***

- Analyze the accuracy of intrusion detection alerts by assessing false positives (legitimate activities mistaken for attacks) and false negatives (undetected attacks).
- Adjust detection thresholds and configurations based on the analysis.

### 6. **\*\*Anomaly Detection Testing:\*\***

- Test the intrusion detection system's ability to detect abnormal behaviour or deviations from established patterns.
- Simulate traffic patterns that may indicate a breach, such as unusual data transfers or communication with unauthorized devices.

### 7. **\*\*Evasion Techniques Testing:\*\***

- Test the system's resilience against evasion techniques that attackers may use to bypass detection.
- Explore methods to evade detection, such as fragmented packets, encryption, and protocol manipulation.

### 8. **\*\*Incident Response Simulation:\*\***

- Simulate the response process to detected attacks or anomalies.
- Evaluate the organization's ability to investigate, contain, and mitigate the impact of a detected intrusion.


### 9. **\*\*Reporting:\*\***

- Prepare a comprehensive report detailing the results of intrusion detection testing.
- Include information about attack scenarios, detection rates, false positives/negatives, and overall system performance.

### 10. **\*\*Recommendations and Remediation:\*\***

- Provide actionable recommendations for improving the intrusion detection and prevention mechanisms based on testing outcomes.
- Suggest adjustments to configurations, rules, or monitoring thresholds.

diff


 Copy code

- Provide actionable recommendations for improving the intrusion detection
- Suggest adjustments to configurations, rules, or monitoring thresholds.

#### 11. **\*\*Validation and Follow-Up:\*\***

- Validate the implementation of recommended changes and adjustments.
- Conduct follow-up testing to ensure that intrusion detection mechanisms have been effectively enhanced.

diff


 Copy code

- Validate the implementation of recommended changes and adjustments.
- Conduct follow-up testing to ensure that intrusion detection mechanisms

#### 12. **\*\*Continuous Improvement:\*\***

- Incorporate lessons learned from intrusion detection testing into ongoing security practices.
- Continuously refine and update intrusion detection systems to adapt to evolving threats.

vbnet

 Copy code

- Incorporate lessons learned from intrusion detection testing into ongoing
- Continuously refine and update intrusion detection systems to adapt to evo

By conducting intrusion detection testing, organizations can identify vulnerabilities and gaps in their intrusion detection and prevention systems. This process helps enhance the network's ability to detect and respond to unauthorized activities, contributing to a more resilient and secure wireless network environment.

## **User Awareness and Training Assessment:**

User awareness and training assessment is a critical component of a wireless network security assessment project. It focuses on evaluating how well users understand security best practices, potential risks, and their role in maintaining a secure wireless network environment. Here's an overview of the user awareness and training assessment process:

### **User Awareness and Training Assessment for Wireless Network Security:**

#### **1. Objective Definition:**

- Clearly define the goals and objectives of the user awareness and training assessment.
- Determine the key areas of wireless network security that users need to be aware of, such as password hygiene, device security, and social engineering risks.

#### **2. Training Program Evaluation:**

- Review existing user training programs and materials related to wireless network security.
- Assess the content, format, and delivery methods of training materials.

#### **3. User Interaction Analysis:**

- Observe and analyze how users interact with the wireless network on a daily basis.
- Identify common practices, habits, and potential security gaps.

#### **4. User Interviews and Surveys:**

- Conduct interviews or surveys with a sample of users to gauge their understanding of wireless security.
- Ask questions about password management, device usage, and their knowledge of potential threats.

#### **5. Simulated Phishing Tests:**

- Perform simulated phishing tests to evaluate users' susceptibility to social engineering attacks.
- Measure the percentage of users who click on suspicious links or provide sensitive information.

#### **6. Assessment of User Responses:**

- Analyze user responses to simulated security incidents or scenarios.
- Evaluate how well users recognize and respond to potential security threats.



## 7. User Behaviour Monitoring:

- Use monitoring tools to track user behaviour on the wireless network.
- Identify any patterns of behaviour that may indicate security lapses.
- 

## 8. Security Awareness Workshops:


- Organize workshops or training sessions to educate users about wireless network security best practices.
- Provide interactive sessions on topics such as password security, secure Wi-Fi usage, and identifying phishing attempts.

## 9. Assessment Metrics and Metrics:

- Define metrics to measure the effectiveness of user awareness and training efforts.
- Establish benchmarks for improved user behaviour and security awareness.

## 10. Documentation and Reporting:


diff

 Copy code

- Document findings related to user awareness and training assessment.
- Include observations, survey results, user responses, and outcomes of simu

## 11. Recommendations and Remediation:

CSS

 Copy code

- Provide actionable recommendations to improve user awareness and training
- Suggest enhancements to training materials, communication strategies, and

## 12. Implementation and Follow-Up:

sql

Copy code

- Collaborate with relevant teams to implement recommended changes to user awareness and training programs based on findings.
- Monitor the implementation and track improvements in user behavior and security posture.

## 13. Continuous Improvement:

sql

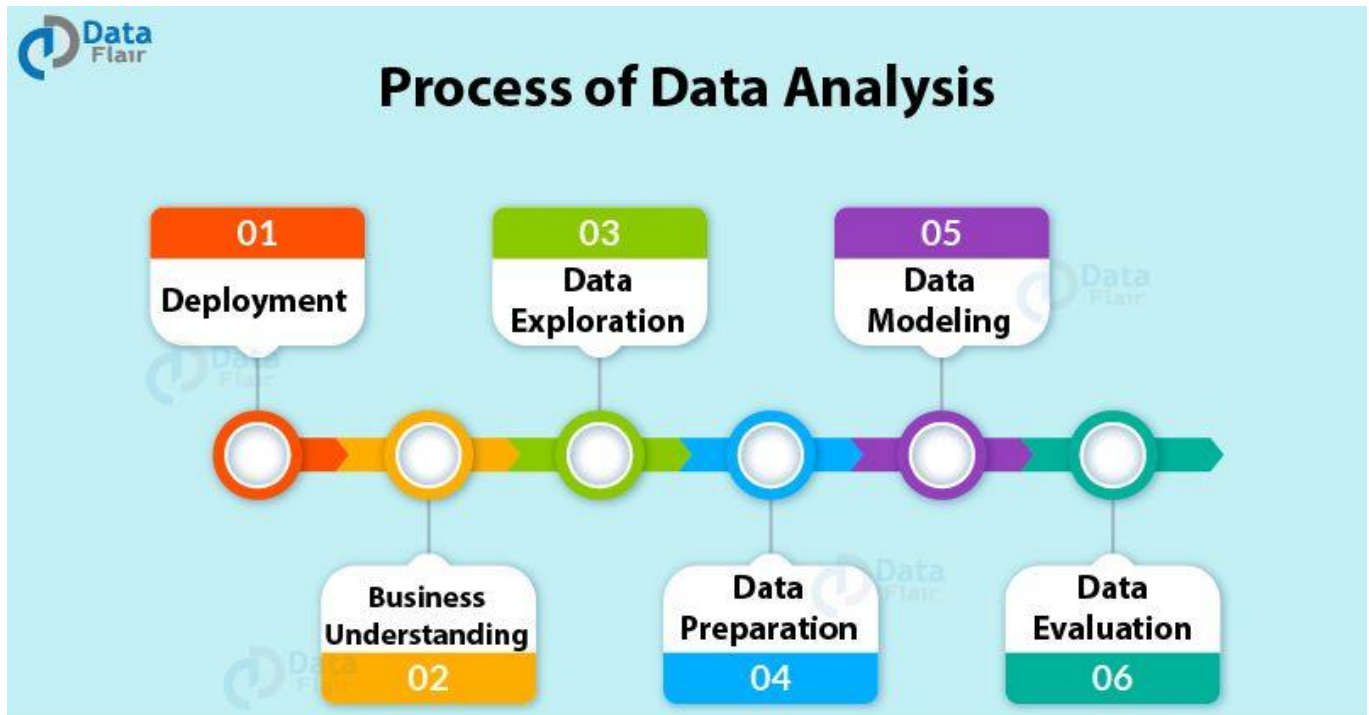
Copy code

- Continuously refine and update user awareness and training programs based on findings and changing threats.
- Regularly assess and reinforce user understanding of wireless network security risks and best practices.



## **Data Analysis and Reporting:**

Data analysis and reporting are essential components of a wireless network security assessment project. Proper analysis of collected data and the creation of comprehensive reports help communicate findings, vulnerabilities, and recommendations to stakeholders.



## **Data Analysis and Reporting for Wireless Network Security Assessment:**

### **1. \*\*Data Collection Review:\*\***

- Compile and review all collected data from various assessment activities, including vulnerability scans, intrusion tests, user surveys, and more.
- Ensure data accuracy, completeness, and relevance to the assessment objectives.

### **2. \*\*Data Organization and Preparation:\*\***

- Organize collected data into structured formats, databases, or spreadsheets for easier analysis.
- Cleanse and pre-process data to remove inconsistencies, duplicates, and irrelevant information.

### **3. \*\*Data Analysis:\*\***

- Apply data analysis techniques to identify patterns, trends, and correlations within the collected data.

- Use statistical methods and visualization tools to gain insights into the security posture of the wireless network.

#### **4. \*\*Vulnerability Prioritization:\*\***

- Prioritize identified vulnerabilities based on severity, potential impact, and risk to the organization.
- Assign risk scores or levels to vulnerabilities to guide the focus of remediation efforts.

#### **5. \*\*Incident and Anomaly Detection Analysis:\*\***

- Analyze data related to detected incidents, anomalies, and intrusion attempts.
- Evaluate the effectiveness of intrusion detection systems and response mechanisms.

#### **6. \*\*User Behaviour Assessment:\*\***

- Review data related to user behaviour, interactions, and responses to security incidents or simulated tests.
- Identify patterns of risky behaviour, compliance with security practices, and areas for user education.

#### **7. \*\*Simulation Results Examination:\*\***

- Analyze the outcomes of simulated attacks, such as phishing tests or intrusion attempts.
- Assess user responses, system alerts, and security controls' effectiveness in mitigating threats.

#### **8. \*\*Contextual Analysis:\*\***

- Provide context to the data by considering the organization's network architecture, policies, and industry standards.
- Interpret data findings in the context of potential business impacts and consequences.

#### **9. \*\*Report Generation:\*\***

- Prepare a detailed report summarizing the assessment process, methodologies, and objectives.
- Present key findings, vulnerabilities, strengths, weaknesses, and actionable recommendations.

#### **10. \*\*Visualizations and Graphics:\*\***

- Use charts, graphs, and visual representations to communicate complex data in a clear and understandable manner.
- Visualizations can help stakeholders quickly grasp the assessment outcomes and focus areas.

#### **11. \*\*Executive Summary:\*\***

- Create an executive summary section that provides a high-level overview of the assessment's key findings, risks, and recommended actions.
- Summarize the potential impact of identified vulnerabilities on the organization.

12. **\*\*Recommendations and Mitigation Strategies:\*\***

- Include detailed recommendations for addressing identified vulnerabilities and improving the wireless network's security posture.
- Prioritize recommendations based on risk assessment and potential impact.

13. **\*\*Documentation and Evidence:\*\***

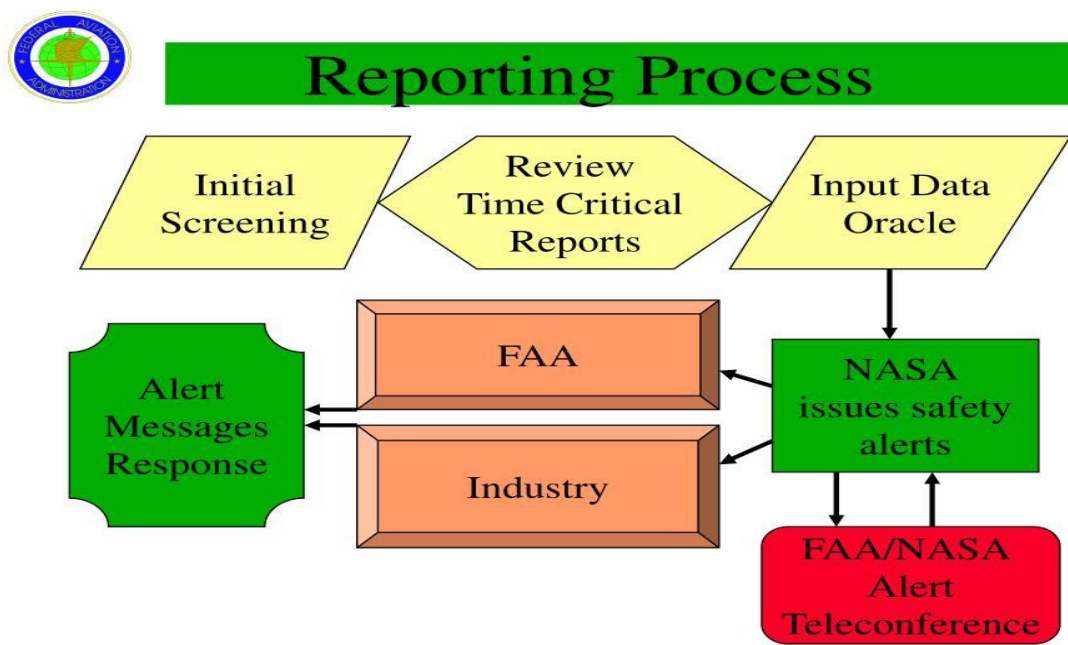
- Include supporting evidence, screenshots, logs, and other documentation to validate assessment findings.
- Ensure that the report is well-documented and transparent in its approach.

14. **\*\*Presentation to Stakeholders:\*\***

- Present the assessment report to key stakeholders, including IT teams, management, and security personnel.
- Clearly communicate the assessment results, implications, and recommended steps for improvement.

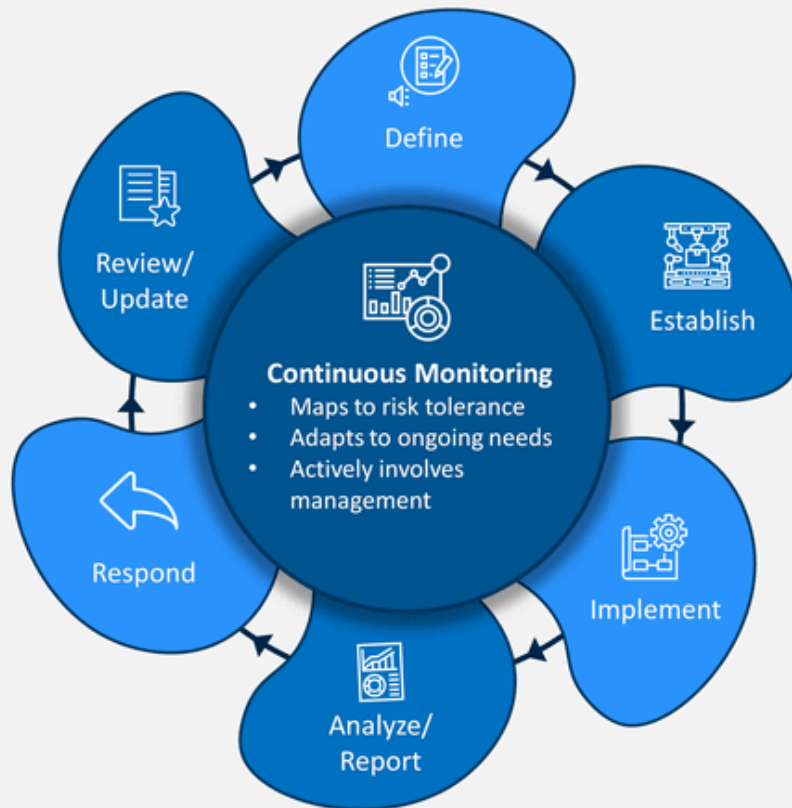
15. **\*\*Distribution and Archiving:\*\***

- Distribute the final assessment report to relevant parties.
- Archive the report and associated data for future reference and comparison in subsequent assessments.



## **Continuous Monitoring:**

Continuous monitoring is a crucial practice in maintaining the security of your wireless network beyond a one-time assessment. It involves ongoing surveillance, analysis, and response to security events and potential threats.



## **Continuous Monitoring for Wireless Network Security:**

### **1. Real-Time Event Detection:**

- Implement intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic in real time.
- Detect and alert on suspicious activities, unauthorized access attempts, and other security events.

## **2. Log Collection and Analysis:**

- Collect and analyze logs from network devices, access points, authentication servers, and other relevant components.
- Monitor for anomalies, unauthorized changes, and signs of potential compromise.

## **3. Vulnerability Scanning and Assessment:**

- Regularly conduct vulnerability scans to identify new weaknesses and potential vulnerabilities in the network.
- Prioritize and address vulnerabilities based on risk levels.

## **4. Patch and Update Management:**

- Stay updated with the latest security patches, firmware updates, and software releases for network devices.
- Implement timely patches to address known vulnerabilities and improve security.

## **5. Threat Intelligence Integration:**

- Integrate threat intelligence feeds to stay informed about emerging threats and attack patterns.
- Use threat intelligence data to enhance detection and response capabilities.

## **6. Behavioural Analysis:**

- Monitor user and device behaviour for deviations from established patterns.
- Detect anomalies that may indicate unauthorized access or compromised devices.

## **7. User and Device Management:**

- Regularly review and manage user accounts, access rights, and device registrations.
- Remove or disable inactive or unauthorized accounts and devices.

## **8. Incident Response and Remediation:**


- Develop and maintain an incident response plan that outlines roles, responsibilities, and procedures in case of a security breach.
- Respond promptly to security incidents, investigate breaches, and take appropriate remediation actions.

## 9. Regular Security Audits:

- Conduct periodic security audits to assess the effectiveness of security controls and policies.
- Review configurations, access controls, and encryption settings.

## 10. Security Awareness Training:


CSS

 Copy code

- Provide ongoing security awareness training to educate users about evolving threats.
- Foster a culture of security-conscious behavior among employees.

## 11. Penetration Testing:


vbnet

 Copy code

- Periodically perform penetration testing to assess the network's resilience.
- Validate the effectiveness of security measures and identify potential weaknesses.

## 12. Documentation and Reporting:


diff

 Copy code

- Document and maintain records of monitoring activities, incidents, and response actions.
- Generate regular security status reports for management and stakeholders.

## 13. Continuous Improvement:

diff

 Copy code

- Continuously analyze monitoring results and incident data to identify areas for improvement.
- Update security policies, procedures, and controls based on lessons learned.



## **Conclusion**

In conclusion, a thorough wireless network security assessment is an indispensable endeavour for any organization aiming to safeguard its sensitive information, maintain operational integrity, and ensure the confidentiality of data exchanged over wireless networks. By systematically evaluating various facets of network security, vulnerabilities, and user practices, an effective assessment provides valuable insights and actionable recommendations to enhance the overall security posture.

Through meticulous vulnerability assessments, organizations can identify and prioritize potential weaknesses within their wireless network infrastructure. By scrutinizing authentication and encryption mechanisms, they can fortify access controls and data protection protocols. Rogue device detection mechanisms aid in thwarting unauthorized access points, while intrusion detection testing ensures an organization's ability to swiftly detect and counteract potential breaches.

Furthermore, user awareness and training assessments play a pivotal role in cultivating a security-conscious culture, empowering users to recognize risks and contribute to a resilient network environment. Ongoing monitoring and analysis, combined with continuous improvement strategies, provide the tools needed to respond to evolving threats and swiftly address emerging vulnerabilities.

The culmination of these efforts is a comprehensive report that not only encapsulates findings and vulnerabilities but also presents a strategic roadmap for bolstering wireless network security. This report serves as a valuable resource for decision-makers, enabling them to allocate resources effectively, implement necessary changes, and align security practices with regulatory requirements and industry standards.

Ultimately, a wireless network security assessment is not merely a one-time undertaking; rather, it is an ongoing commitment to adapt, evolve, and continuously enhance security measures. By embracing these principles and consistently prioritizing the protection of wireless networks, organizations can proactively safeguard their digital assets and contribute to a safer, more resilient technological landscape.