WIRELESS NETWORK SECURITY ASSESSMENT (NIST 800-48)

DISCLAIMER

This document does not promote or encourage any Illegal activities, all content provided in this document is meant for education, research purposes. The document is not transformative in nature, it is used for teaching purpose.

Copyright Disclaimer Under Section 107 of the Copyright Act 1976, allowance is made for "fair use" for purposes such as criticism, commenting, news reporting, teaching, scholarship, and research. Fair use is a use permitted by copyright statute that might otherwise be infringing. Non-profit, educational or personal use tips the balance in favor of fair use.

The document is created with the intention of educating others in a motivational/inspirational form. Do not try to use the scripts/code/methods if it is not legal in your country.

I Do not take any responsibility for anything you do using this document, Use at your own risk.

TABLE OF CONTENTS

INTRODUCTION TO WIRELESS SECURITY

Highlight the key threats associated with Wireless Security and risk associated with it.

WIRELESS SECURITY CHECKLIST

Presenting Wireless security checklist based upon the international standard of **NIST 800-48**

WIRELESS HEATMAP PRECAUTIONARY MEASURES

Designing a Heatmap for wireless network to secure organization from physical, environmental threats.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

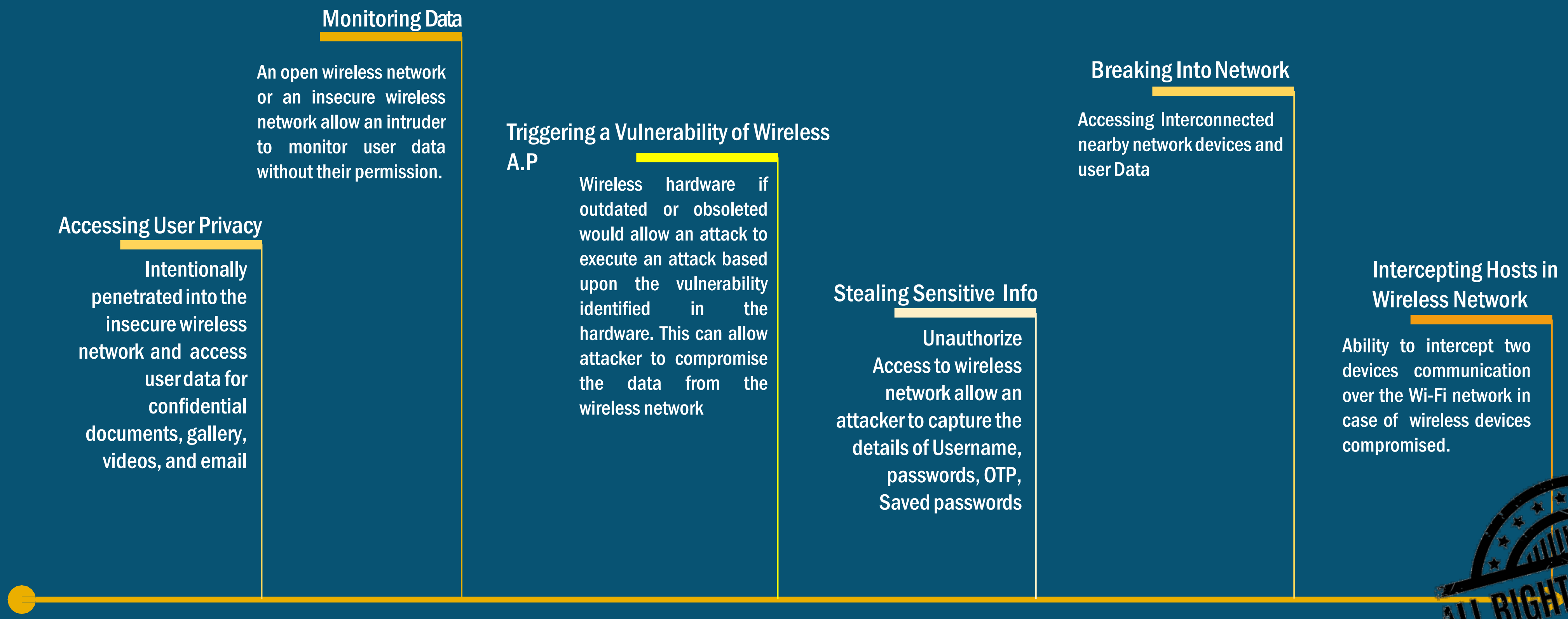
INTRODUCTION TO WIRELESS SECURITY

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

INTRODUCTION TO WIRELESS SECURITY

Wireless Security assessment emphasis for the prevention of unauthorized access to the individual / organization system(s), Cameras, Network devices, Network Printers, Network Scanner, cell phones etc.

DAMAGES



Accessing User Privacy

Intentionally penetrated into the insecure wireless network and access user data for confidential documents, gallery, videos, and email

Monitoring Data

An open wireless network or an insecure wireless network allow an intruder to monitor user data without their permission.

Triggering a Vulnerability of Wireless A.P

Wireless hardware if outdated or obsoleted would allow an attack to execute an attack based upon the vulnerability identified in the hardware. This can allow attacker to compromise the data from the wireless network

Stealing Sensitive Info

Unauthorize Access to wireless network allow an attacker to capture the details of Username, passwords, OTP, Saved passwords

Breaking Into Network

Accessing Interconnected nearby network devices and user Data

Intercepting Hosts in Wireless Network

Ability to intercept two devices communication over the Wi-Fi network in case of wireless devices compromised.

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

WIRELESS SECURITY CHECKLIST (NIST 800-48)

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

WIRELESS SECURITY CHECKLIST (NIST 800-48)

Ubaid Jafri

WIRELESS SECURITY ASSESSMENT - CHECKLIST

NIST 800 - 48 (Wireless Security Checklist)

S.No	Mandatory Requirements	Currently in Place	Will Be Implemented	Remarks
1	Security policy that addresses the use of Wireless technology, including IEEE 802.11x technologies			
2	Comprehensive Security assessments performed at regular and random intervals (Including validating the rouge WAPs do not exist in the IEEE 802.11x WLAN) to fully understand the wireless network security posture			
3	Default shared keys replaced every 90 Days			
4	Administrator WAP password changed every 90 days or post compromise.			
5	Network Users trained in the risk associated with wireless technology			
6	complete inventory of all WAPs and IEEE 802.11x wireless devices connected.			
7	WAPs maintained in secured areas to prevent unauthorized physical access and user manipulation			
8	When disposing of WAPs no longer required, WAP configuration settings cleared to prevent disclosure of network configuration, keys, passwords etc.			
9	if the WAP supports logging, logging turned on and logs reviewed on a regular on a regular basis.			
10	Default SSID* and default IP Address changed in the WAP.			

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

WIRELESS SECURITY CHECKLIST (NIST 800-48) – CONT'D..

WIRELESS SECURITY ASSESSMENT - CHECKLIST				
NIST 800 - 48 (Wireless Security Checklist)				
S.No	**Mandatory Requirements**	**Currently in Place**	**Will Be Implemented**	**Remarks**
11	SSID* character string validated to establish that it does not reflect the trustee's name.			
12	All in secure and nonessential management protocols on the WAPs disabled			
13	All Security features of the WLAN product, including the cryptographic authentication and the strongest encryption algorithm available (WPA2 or better), enabled			
14	Encryption is used and the encryption key size at a minimum of 256 bits.			
15	All WAPs meet the requirements of trustee's internal network security			
16	"AD HOC Mode" for IEEE 802.11 disabled.			
17	User authentication mechanisms enabled for the management interfaces of the WAP.			
18	MAC Filtering enabled and in use.			
19	Anti-Virus software installed and latest anti-virus definations maintained on all wireless clients.			
20	SSL/TLS used for Web-based management of WAPs			

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

WIRELESS SECURITY CHECKLIST (NIST 800-48) – CONT'D..

WIRELESS SECURITY ASSESSMENT - CHECKLIST				
NIST 800 - 48 (Wireless Security Checklist)				
S.No	**Mandatory Requirements**	**Currently in Place**	**Will Be Implemented**	**Remarks**
21	if using SNMP agent, SNMPv3 or equivalent cryptographically protected protocol used to enhance the security of WAP traffic management.			
22	Personal firewall software installed on all wireless clients.			
23	Software patches and upgrades fully tested and deployed on a regular basis			
24	Security practice on deploying a wireless technology is fully understood			

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

WIRELESS HEATMAP

PRECAUTIONARY MEASURES

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

WIRELESS HEATMAP

PRECAUTIONARY MEASURES

While designing & implementing wireless network following are the key list of activities which are required from security poi nt of view in order to secure Wi-Fi from external threats.

1. Wireless Network Signal must be transmitted within the organization vicinity;

2. Wireless Network Channel must not be overlapped with other A.P this could create interference in the signal strength;

3. Wireless A.P must not be installed in an open area in the organization;

4. Unused port of wireless A.P must be physically tapped so no other user could allow to connect A.P with a physical cable;

5. The placement of A.P must be at least 120 meters before or after from an existing one;

6. The A.P must be disabled to broadcast any AD-Hoc network

7. The SSID of wireless A.P must be same in all over the organization

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.

THANK YOU

Note: The information posted in this document is for Research & Educational purpose only, illegal use of this document may violate the security law varies upon the country. Do not try this for offensive purpose.