TITLE OF THE PROJECT

Wireless Network Security Assessment

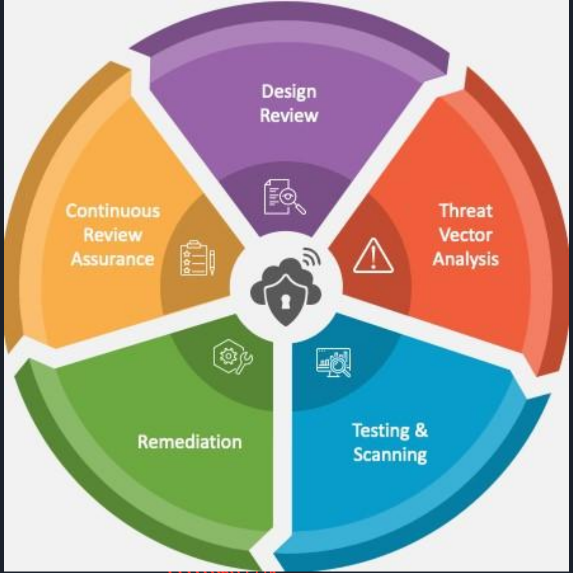
TEAM MEMBERS:

Mocherla Percy
Pirati Alekhya
Ilapuram Sailaja
Gogula Pavani

Team Lead:
Chinnam Ananda Kumari

OBJECTIVE OF THE PROJECT

This presentation provides an overview of wireless network security assessment and demonstrates how to perform a simple assessment using the 'scapy' library in Python.Wireless security assessment helps identify vulnerabilities and security risks in the wireless network. Our Security Consultants test for different vulnerabilities and perform different test cases to identify vulnerabilities in the wireless network.



Introduction to wireless network security assessment :

A Wireless Security Assessment will Identify all your access points and assess their vulnerability. Check the strength of your encryption security and user authentication. Test the efficacy of your data segregation.When you use a wireless network it enables your physical security controls to be bypassed and access gain to your systems. This can be through overlooked access points, such as a smaller office site, which is nevertheless connected to your servers, or an attacker sitting outside your office with a laptop or holed up in a nearby building with a powerful antenna. A Wireless Security Test will alert you to their presence, or potential presence.

Protecting Wireless Networks – Best Practices

a) Update router firmware: It is recommended to update the firmware of the router whenever an update is released. Updating the firmware will minimize the risk of getting hacked as it will remove most of the vulnerabilities.

b) Make use of Strong Passwords: A strong password is at least eight characters long and includes a mix of upper- and lower-case letters, numbers, and symbols. It is recommended to change the passwords frequently.

c) Using MAC Filtering:By allowing only devices with specific MAC addresses to connect to the network, you can prevent unauthorized access. MAC filtering can be implemented by accessing the wireless router's configuration page and adding the MAC addresses of devices that are allowed to connect to the network

d) Enable WPA3 Security: It is recommended to make use of WPA3 encryption as it provides stronger protection than WPA2

Wireless Encryption Types:

a) Wired Equivalent Privacy (WEP) : The main issue with WEP is that while sending data from our computer, it only utilises one static key.

b) Wi-Fi Protected Setup (WPS): WPS is a built-in feature of many routers that makes it easier to connect Wi-Fi-enabled devices to a secure wireless network.

c) Wi-Fi Protected Access (WPA): WPA improves upon the security feature of WEP by using Extensible Authentication Protocol (EAP) to secure network access.

d) Wi-Fi Protected Access Version 2 (WPA2): Only users with your network password can access the data broadcast or received over your wireless network thanks to WPA2.

e) Wi-Fi Protected Access Version 3 (WPA3): The newest security encryption, the WPA3 Protocol, is rising in popularity. WPA3 provides excellent security and hinders illegal access.

HOW TO DISCOVER CRITICAL WIRELESS NETWORK SECURITY VULNERABILITIES IN AN OPTIMIZED BUDGET ?

1. Evaluating Vulnerabilities: Wireless penetration testing can provide information on exploitable threats by enabling you to perform an audit. You can identify the most critical threats for an organization and prevent attacks before they actually happen.
2. Setting Regulations and Policies: Wireless penetration testing helps organizations address security threats by settings rules or policies to protect their employees. Making sure that the sales department only has access to the sales information is key.

CONCLUSION :

In a world where malicious intruders are always probing networks in search of weaknesses to exploit, you cannot afford to ignore any vulnerability, misconfiguration, or weak security control in your network eco-system. The security problem is further compounded by the increased use of remote access to networks via wireless technologies which have opened more opportunities for malicious intruders.

Thank you for your time and attention 🙂