happiest minds

WIRELESS SECURITY

Assessment Methodology

Happiest People . Happiest Customers

Contents

1 Executive Summary

Owing to the outburst of wireless networks around the world and how organizations of almost all sizes have been evolving to fit them into their operational architecture, the need to assess the degree of security of the same has been on a constant surge. With the innate infinite potential of the wireless world to deploy itself through the length and breadth of organizations, it has become more of a responsibility than a choice for their IT teams to run a relentless assessment on the wireless vulnerability on a regular basis. That being said, what is Wireless Security Assessment? This whitepaper intends to shed light on the same, and on the rational methodologies that make up for a holistic assessment framework in detail.

2 Introduction - What is Wireless Security Assessment?

Wireless Security Assessment is a counterpart of the broader concept of 'Security Assessment' - which takes care of the security of an enterprise in a holistic sense of word by performing evaluations such as Extended Internet Footprint Assessment, Source Code Review, Infrastructure Assessment, Application Assessment and SCADA Assessment. What grants Wireless Security Assessment the spotlight of our attention is the increasing ease of its deployment through the addition of rogue Access Points (AP) by anybody from an amateur user to the administrator. In all, Wireless Security Assessment aims at setting up a security baseline, checking compliance, gathering film-ware versions for all equipments, determining maximum distance that wireless traffic can be received, discovering unauthorized access points, verifying if unencrypted traffic is traversing the wireless network and ensuring that weak forms of WEP are not in use. To understand Wireless Security Assessment in its actual depth, let's look at the two types of methodologies that are available: 1. Manual Assessment Methodology & 2. Automated Assessment Methodologies.

2.1 Manual Assessment Methodology:

The Manual Assessment Methodology, otherwise known as Ad-hoc Assessment, is a voluntary security evaluation that happens in a moment of time. The Manual Assessment Methodology employs the type of typical tools most people looking for an open AP are aware of these tools can be anything from NetStumbler & WiFiFoFum to Airsnort & Airmagnet. The Manual Assessment Methodology comes to play when the current operating status of a wireless environment is to be checked. It's also used to evaluate if the Automated Assessment Methodology is functional. What makes Manual Assessment Methodology a tad tactical is its infrequency of evaluation and its limitation to examine security only at a given point in time. For instance, there may might as well be a rogue AP installed the next day after the assessment and the system may not trigger it until the next manual evaluation. Therefore, to think that an annual Manual Assessment is ideal for an organization may not entirely work on its absolute benefit.

2.2 Automated Assessment Methodology:

An Automated Assessment Methodology is an on-going intuitive security interface that alerts the wireless environment should there be any discrepancies in the same, be it: changes, additions or any sort of suspicious activity. Considering the threat an insecure wireless device can pose to its environment, it's best to think of the Automated Assessment Methodology to be an imperative. However, networks such as Wi-Fi hotspots needn't necessarily have an Automated Assessment process, for the reason that they are by nature open and also because they are principally used only for internet access. The agenda of an Automated Assessment Methodology is to alert the personnel of questionable security discrepancies that occur in the network as and when they are happening in real-time.

3 Performing the Assessment Methodologies:

Both Assessment Methodologies, Manual & Automated, have their place and say in governing the security architecture of a wireless network. While one takes care of an instant evaluation, the other looks after an on-the-go assessment of networks. An intelligent security ecosystem has the right cohesion of both ideas in place. Be that as they may, let's look at how we can practically perform both of these assessment methodologies.

3.1 Performing Manual Assessment Methodology:

There are both, commercial and free tools at disposal to perform a Manual Assessment. While the free tools trigger the most obvious vulnerabilities that surface in a network, the commercial ones have the ability to meticulously trace the insecurities in more detail than just revealing open AP. In that gravity of things, commercial tools prove more viable for a Manual Assessment as compared to free tools. Airmagnet for instance is a commercial tool that can perform 802.11 a, b or g on Windows XP and print out detailed assessment reports. It also has a function that lets you track an open AP using a 'find' tool. Airsnort on the other hand is a free tool which is designed to crack the WEP keys, although WEP by itself is quite inadequate, unless it's layered with VPN for instance. Airsnort detects way more insecurities as compared to say, NetStumbler or MiniStumbler, but then again it comes with a cost of not having the capability to generate reports. To sum it up, an ideal method to process Manual Assessment is to let the commercial tools take charge of down-to-the-it reporting and have the free tools spot the obvious insecurities after that.

3.2 Performing an Automated Assessment Methodology:

The Automated Assessment is best performed by employing standalone solutions that have sensors which enable coverage for your entire network. Some also have IDS security functionalities that are compatible with switches, access points and authentication solutions, those together notify all wireless users should there be vulnerabilities. To top it up, Automated Assessment Methodology also can be performed by holding health checkups through a quarantine network to minimize threats from viruses, bugs and worms. The sensors in the standalone solutions let the Automated Assessment take the cake, mostly because it protects the networks from focused attacks or accidental damage. Let's look at these more in detail.

3.2.1 Intrusion Detection (ID):

Intrusion Detection is a software application that examines enterprise networks and activities for questionable violations to generate detailed reports. While there may be different types of Intrusion Detection such as network-based and host-based, the primary agenda of them all is to identify suspicious traffic in the network. The goal of Intrusion Detection is to recognize incidents, log in data about them and finally to report attempts. That being said, organizations today use Intrusion Detection to identify security policies, record existing threats and also deter personnel from violating these security policies. To put the finger on the word, Intrusion Detection with the aid of client-based software, sensors, APs and wireless switches actively monitor wireless irregularities, ensuring Automated Assessment runs as vigilant as possible.

3.2.2 Quarantine:

Quarantine is a system health-checkup that is a given a run to minimize the proliferation of malware between peers on the network, to consequently enhance its bandwidth. Quarantine surfaces out of the fact that an alarming number of naive users not adhering to corporate guidelines while updating their systems, which consequently expose vulnerabilities in the architecture, inviting insecurities of all kinds. Quarantine ensures it becomes imperative for networks to scrutinize systems and become absolutely compliant before permitting them to classified resources.

4 Attacks

To comprehend Wireless Security Assessment in its entirety, it's best we understand the nature of the potential attacks there can ever be, which can range from Access Control to Confidentiality to Authentication.

4.1 Wireless Access Control Attacks:

Wireless Access Control Attacks aims to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. The attacks can take place through anything from war-driving, rouge access points, MAC spoofing, ad-hoc associations, AP/Client misconfigurations, unauthorized association and Promiscuous clients.

4.2 Wireless Integrity Attacks:

In integrity attacks, the attackers send forged control, data and management frames over the wireless network to misdirect the wireless devices in order to perform DOS attack. This can happen through a range of spectrums such as Data Frame Injections, WEP Injections, Data Replay, Vector Replay Attacks, Bit-Flipping Attacks, AP Replay Attacks, Radius Replay and Wireless Network Viruses.

4.3 Wireless Confidentiality Attacks:

Confidentiality attacks attempts to intercept confidential information sent over the wireless associations, whether sent in clear text or encrypted by Wi-Fi protocols. This can be caused through Eavesdropping, Session Hijacking, Honey-pot AP, Masquerading, Evil Twin AP, Cracking WEP Key or Traffic Analysis.

4.4 Wireless Availability Attacks:

Wireless Availability Attacks aim to prevent legitimate users from accessing resources in a wireless network via AP Theft, Beacon Flood, Authentication Flood, TKIP MIC exploitation, De-authenticate Flood, Routing Attacks ARP Cache Positioning and Power Saving Attacks.

4.5 Wireless Authentication Attacks:

The objective of Wireless Authentication Attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc to gain unauthorized access to network resources which can happen over a course of time through Application Login Theft, PSK Cracking, Shared Key Guessing, Domain Login Cracking, Identity Theft, VPN Login Cracking, LEAP Cracking and Password Speculation.

5 Best Practices

The possible best practices to counter the attacks range over from tackling Wi-Fi Configurations, SSID Settings and Wi-Fi Authentications.

5.1 Wi-Fi configuration best practices

- Change the default SSID after WLAN configuration
- Set the router access password and enable firewall protection
- Enable MAC address filtering on the AP or router
- Enable encryption on router and change passphrase often

5.2 SSID settings best practices

- Use SSID cloaking to keep certain default wireless messages from broadcasting ID to everyone
- Place a firewall or packet filter in between the AP and the corporate internet
- Check the wireless devices for configuration or setup problems regularly
- Implement a different technique for encrypting the traffic, such as IPSEC over wireless

5.3 Wi-Fi Authentication best practices

- Choose WPA instead of WEP
- Implement WPA2 Enterprise wherever possible
- Place wireless access points in a secured location
- Keep drivers on all wireless devices updated
- Use a centralized server for authentication

6 Conclusion

Wireless Security Assessment Methodologies, be it Manual or Automated, involves 5 steps. The first is the discovery of APs, identification of targets to be made a part of the assessment and triggering the traffic leaked outside the set boundaries. The second step deals with inspecting access control, identifying vulnerabilities already on board and determining security settings. The third involves investigation of additional encryption architecture. The fourth step basically is enabling user, device and manual authentication and the final one, assessing the physical location of APs. The primary goal of Wireless Security Assessment is to monitor networks and alert personnel of any unchartered irregularities in its traffic, whichever type of assessment one chooses to adopt.

Author

Karthik Palanisamy

Technical Security Assessment Professional with 4 plus years of consulting experience in network & web application vulnerability assessment and penetration testing, thick client security, database security, mobile application security, SAP application penetration testing, source code audit, configuration review of devices and security architecture review (Applications and Infra-structures).Currently holding a position with Happiest Minds Technologies to deliver technical security assessment and penetration testing services covering application security, infrastructures security, mobile application security and source code review.

About Happiest Minds

Happiest Minds has a sharp focus on enabling Digital Transformation for customers by delivering a Smart, Secure and Connected experience through disruptive technologies: mobility, big data analytics, security, cloud computing, social computing, M2M/IoT, unified communications, etc. Enterprises are embracing these technologies to implement Omni-channel strategies, manage structured & unstructured data and make real time decisions based on actionable insights, while ensuring security for data and infrastructure. Happiest Minds also offers high degree of skills, IPs and domain expertise across a set of focused areas that include IT Services, Product Engineering Services, Infrastructure Management, Security, Testing and Consulting.

Headquartered in Bangalore, India, Happiest Minds has operations in the US, UK, Singapore and Australia. It secured a $52.5 million Series-A funding led by Canaan Partners, Intel Capital and Ashok Soota.

E-mail: Business@happiestminds.com

Visit us: www.happiestminds.com

Follow us on