Analyzing Wireless Network Attacks using Offensive Security Tools

[1]May Aye Chan Aung, [2]Khin Phyo Thant
[1]*Network Security Lab, University of Computer Studies, Mandalay*
[2]*Department of Information Technology and System Maintenance*
University of Computer Studies, Mandalay
mayayechanaung@gmail.com, khinphyothantucsy@gmail.com

Abstract **– Wireless network attacks have greatly increased in the past few years. Now, it is time for attackers to intercept secure web connection over the internet. With the passage of time, attackers are getting smarter and smarter. They can now even intercept secure web connections with the help of proxy tools and digital certificates. While it is equally important to stay wireless networks, every wireless clients should know how hackers attack wireless networks and how to prevent these networks. The objective of this paper is to gain a better understanding of different wireless network attacks and the basic strategy adopted by hackers for list of wireless network attacks. This paper highlight different types of wireless network attacks, various tools or methods commonly used by attackers, technical terms associated with each type of attack and how a computer user can detect such attacks.**

I. Introduction

Due to the open nature of wireless networks, it makes adversaries to launch different types of attacks. Hence wireless network communication remains a challenging and critical issue. Wireless networks are being used in many commercial and military applications to collect real time data and event driven data. Wireless Networks consists of large number of nodes interconnected to each other, are becoming a viable solution to many applications like domestic, commercial, and military applications. Wireless networks collects and sends the data from the areas even where ordinary networks are unreachable for various environmental and strategic reasons.

The most promising concepts of wireless networking are auto-configurable and self-organizing. And it provides an adaptable and flexible wireless connectivity to the mobile users. The same notion can be used for different classes of wireless technologies such as wireless local area network (WLAN), wireless personal area network(WPAN), and wireless metropolitan network (WMAN). Wireless mesh networks [5] are expected to resolve the limitations and improve the performance of ad-hoc networks, like WLANs (Wireless Local area Network), WPANs (Wireless Personal Area Network), and WMANs (Wireless Metropolitan Area Network).

Now a day's many laptops are coming with pre-installed networks cards. The ability to enter into a network while moving has a great benefit. However, there are many security issues with the wireless networking. As the security techniques becoming old, it becomes easy to crack. To overcome this, the network administrators or the users must stay up-to-date on any new risks that arise.

The remaining of the paper is organized as follows: Types of wireless network attacks is provided in next section. Offensive security tools is briefly described in section 3. The final conclusion is drawn in section 4.

II. Types of Wireless Network Attacks

There are different types of attacks that exist for wireless networks. Many of these attacks can be mitigated through using the latest techniques and best practice. And, the minimum security measure should be taken to overcome the wireless attacks, such as proper authentication, finding rough access points, best encryption techniques etc. Major attacks are Access control

attacks, integrity attacks, confidentiality attacks authentication attacks and availability attacks. There are tools available to prevent these attacks. Many of these tools can be found in the BackTrack and Kali Auditor Security Collection.

Access control attacks are used to penetrate a wireless network by bypassing the access control measures.

Integrity attacks send forged control, management or data frames over wireless to mislead the recipient or facilitate another type of attack (e.g., DoS).

Confidentiality attacks attempt to intercept private information sent over wireless associations, whether sent in the clear or encrypted by 802.11 or higher layer protocols.

In Authentication attacks, intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services.

Availability attacks impede delivery of wireless services to legitimate users, either by denying them access to WLAN resources or by crippling those resources.

In this section, a brief description of types of attacks along with their name and various tools and methods used is shown in each table.

III. Offensive Security Tools

Cyber security professionals have borrowed a term originally used by the military during training. The teams are divided into a blue team having defensive functions and a red team having offensive tasks. In terms of cyber security, the blue team is monitoring the systems trying to detect them while the red team is performing a penetration test. Red team has several stages and usually begins with reconnaissance and gradually flows into exploitation of identified vulnerabilities. However, at each stage of the engagement, the penetration testers might get detected, usually by unintentionally rising an alert into the Intrusion Detection System or Intrusion Prevention System (IDS or IPS) under the Blue team‘s control.

Offensive security tools are used by security professionals for testing and demonstrating security weakness. Well-known can common tools are Metasploit Framework, Ettercap , sslstrip, evilgrade, Social Engineering Toolkit, sqlmap, aircrack-ng, oclHashcat, ncrack , Cain and Abel.

IV. Conclusion

Wireless networks are more vulnerable to security threats, due to the computation and power limitations. Wireless networks attacks have become a very common security issue when it comes to networks. This paper has ben highlight different types of wireless network attacks, various tools or methods commonly used by attackers, technical terms associated with each type of attack and how a computer user can detect such attacks.

References

[1] http://www.acunetix.com/websitesecurity/authentication.htm

[2] http://www.tech faq.com/network-attacks.html

[3] http://www.wirelessnetworktools.com/

[4] http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks

[5] Ian F. Akyildiz, Xudong Wang and Weilin Wang, “wireless mesh networks: a survey,” Computer Networks, vol. 47, pp. 445-487, Jan.2005.

Table1. Access Control Attacks

Type of Attacks	Description	Method and Tools
War Diving	Discovering wireless LANs by listening to beacons or sending probe requests, thereby providing launch point for further attacks.	Airmon-ng, DStumbler, KisMAC, MacStumbler, NetStumbler, Wellenreiter, WiFiFoFum
Rouge Access Points	Installing an unsecured AP inside firewall, creating open backdoor into trusted network.	Any hardware or software AP
Ad Hoc Associations	Connecting directly to an unsecured station to circumvent AP security or to attack station.	Any wireless card or USB adapter
MAC Spoofing	Reconfiguring an attacker's MAC address to pose as an authorized AP or station.	MacChanger, SirMACsAlot, SMAC, Wellenreiter, wicontrol
802.1x RADIUS Cracking	Recovering RADIUS secret by brute force from 802.1X access request, for use by evil twin AP.	Packet capture tool on LAN or network path between AP and RADIUS server

Table 2. Integrity Attacks

Type of Attacks	Description	Method and Tools
802.11 Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + Injection Tools
802.1X EAP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless Capture + Injection Tools between station and AP
802.1X RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay.	Ethernet Capture + Injection Tools between AP and authentication server

Table 3. Confidentiality Attacks

Type of Attacks	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ettercap, Kismet, Wireshark, commercial analyzers
WEP Key Cracking	Capturing data to recover a WEP key using passive or active methods.	Aircrack-ng, airoway, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab, wesside

Evil Twin AP	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.	cqureAP, D-Link G200, HermesAP, Rogue Squadron, WifiBSD
AP Phishing	Running a phony portal or Web server on an evil twin AP to "phish" for user logins, credit card numbers.	Airpwn, Airsnarf, Hotspotter, Karma, RGlueAP
Man in the Middle	Running traditional man-in-the-middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap-NG, sshmitm

Table 4. Authentication Attacks

Type of Attacks	Description	Method and Tools
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed, vendor default or cracked WEP keys.	WEP Cracking Tools
PSK Cracking	Recovering a WPA/WPA2 PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, genpmk, KisMAC, wpa_crack
Application Login Theft	Capturing user credentials (e.g., e-mail address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain
VPN Login Cracking	Recovering user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)
802.1X Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Capture Tools
802.1X Password Guessing	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password Dictionary
802.1X LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker
802.1X EAP Downgrade	Forcing an 802.1X server to offer a weaker type of authentication using forged EAP-Response/Nak packets.	File2air, libradiate

Table 5. Availability Attacks

Type of Attacks	Description	Method and Tools
AP Theft	Physically removing an AP from a public space.	"Five finger discount"
Queensland DoS	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmit
802.11 Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.	FakeAP
802.11 Associate / Authenticate Flood	Sending forged Authenticates or Associates from random MACs to fill a target AP's association table.	FATA-Jack, Macfld
802.11 TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject, LORCON
802.11 Deauthenticate Flood	Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an AP.	Aireplay, Airforge, MDK, void11, commercial WIPS
802.1X EAP-Start Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.	QACafe, File2air, libradiate
802.1X EAP-Failure	Observing a valid 802.1X EAP exchange, and then sending the station a forged EAP-Failure message.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Sending a malformed 802.1X EAP Identity response known to cause some APs to crash.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Sending EAP type-specific messages with bad length fields to try to crash an AP or RADIUS server.	QACafe, File2air, libradiate