MARYMOUNT UNIVERSITY

Assignment: IT557; Monitoring, Auditing, and Penetration Testing
Assigned: Nov. 10, 2018
Instructor: Professor Ali Bicak
Student Name: George Boakye

LAB REPORT FILE (LAB8)

SECTION 3

Part 1

Risks of using public Wi-Fi

Wi-Fi users are at risk from hackers since same features that make free Wi-Fi access desirable for consumers also attract hackers. The features are that it requires no authentication to establish a network connection, creating amazing opportunities for unlimited access to hackers in unsecured devices on the same network. Fortunately, there are safeguards against them.

Hackers can access every piece of information such as business network security credentials, emails, and credit card information sent over the internet when hackers position themselves between the Wi-Fi user and the access point (AP) and this could include information as understood to be encrypted. In this manner, the Wi-Fi user doesn't directly communicate via the AP but through the attacker before the packets requested or sent is relayed.

Malware distribution over public Wi-Fi networks is another risk to be considered when connecting to such free APs. Sharing files across a network is an easy means for an attacker to plant infected software on user's computer. Sometimes, a pop-up window may appear during the connection process offering a software upgrade. Clicking such window directly installs malware over the network (Office of the CIO n.d.; Dolly 2018; Kaspersky, n.d.)

Using public Wi-Fi in a more secure fashion

Using VPN: Virtual private network (VPN) connection is a must when connecting to company networks through unsecured connections such as Wi-Fi hotspot. VPN shields browsing activity from prying eyes on public Wi-Fi or unsecured networks. Data that passes through VPN connections is strongly encrypted to the point that an attacker positioning himself between the user and the AP may find difficult to access and interpret. Although VPN implementation is expensive, the additional security is well worth its implementation. Since most hackers are after an easy target, they'll likely discard stolen information rather than put it through a lengthy decryption process.

Turning off file sharing: File sharing must be turned off when connecting to public Wi-Fi. Sharing can be turned off from the system preferences or Control Panel, depending on OS, or let Windows turn it off by choosing the "Public" option the first time connecting to a new, unsecured network. These simple and easy steps could help mitigate massive amounts of data theft both at home and at work.

Using SSL Connections: Enabling the "Always Use HTTPS" option on websites visited frequently could help institute some security measures in the absence of VPN session. Most websites that require an account or credentials have the "HTTPS" implemented somewhere in its settings. A connection over HTTPS may help protect some information from the view of the attacker especially when the decryption process of such information is expensive for the hacker to pursue. For instance, username and password for some portals may be the same as a person's bank or corporate network credentials and sending these credentials in an unencrypted manner may land in the hands of a smart attacker.

Available options when on personal travel

Autoconnect must be disabled and Keeping Wi-Fi off when not needed: Wi-Fi hardware in wireless ability electronic devices still transmit data between networks within range even when there's no active connection. Keeping Wi-Fi turned off when not in need especially saves on battery life and avoids passive transmission of data.

Investing in an unlimited mobile data plan: Investing in an unlimited data plan not only eliminates accessing insecure Wi-Fi networks, it gives the opportunity to use personal mobile devices to create personal internet "hotspot" for connecting other devices. Individuals mostly connect to public Wi-Fi networks just to save excess charges on phone bills. Exercising such extra care can help shield individuals from getting hacked.

Staying protected: Having the mind of a security professional in mind also goes great length to mitigate Wi-Fi security issues. Buying and installing personal robust internet security solution on devices could be the way forward. These solutions can constantly run a malware scan on files and will always scan new files as they are downloaded.

Part 2

Part 2: A

The following are some plain wordlist dictionaries compatible with aircrack-ng and used to brute force WPA/WPA2 wireless networks: *.lst, .txt, .cap, .ivs*

Again, aircrack-ng comes with a small dictionary called password.lst. The file is located in the 'test' directory of the source files.

Word list for aircrack-ng can be downloaded from https://www.wirelesshack.org/wpa-wpa2-word-list-dictionaries.html

Part 2: B

Based on Section 2, Step 2, the command aircrack-ng -w wordlist.txt /WLAN/wordlist/WLAN/Capture-01.cap was used to crack 'Silentvalor' network. However, the downloaded dictionary file and the "Capture-01.cap" file were in the same WLAN directory although the "Capture-01.cap" file was in a sub-directory within the WLAN directory hence the full path /WLAN/wordlist/WLAN/Capture-01.cap specified.

Therefore, if both files had just been in same directory without any sub-directory (E.g. wordlist), the command to execute the cracking would've been: "aircrack-ng Capture-01.cap -w wordlist.txt"

Part 3
WLAN SECURITY IMPLEMENTATION PLAN

Summary

From the lab, it was discovered that the attacker manipulated 'Silentvalor' network with aircrack-ng suite. airmon-ng command tool was used to enable the monitor mode on the WLAN interfaces. The airodump-ng tool enabled packet capturing of 802.11 frames which enabled the collection of WEP initialization vectors and later used in cracking the network.

aireplay-ng tool provided the ability to inject frames that generated traffic and later used to crack the WEP and WPA-PSK keys. The command enabled the attacker to gain handshake data and as a result obtained fake authentication. The ability was made when the BSSID was obtained after the command was executed. After such commands were ran, it was easy for the attacker to authenticate with the passphrase "darkobsidian" and even obtained IP address (172.100.40.111) on 'Silentvalor' network with BSSID/MAC 04:A1:51:2C:DD:F5. This was an exploited vulnerability based on lack of encryption.

Critical risks, threats, and vulnerabilities on the WLAN

Implementing proper and strong security measures on WLAN networks to avoid improper and unauthorized accesses is strongly encouraged.

With respect to the 'Silentvalor' WLAN network, failing to implement encryption on the network exposed the risk and vulnerability seen during the lab section and the subsequent threat of attacker cracking the network to obtain the passphrase and network information such as BSSID and exploiting the network to obtaining a valid IP address.

More risks and threats are regularly evolving and associated with the evolution of wireless connection. Some risks and threats in WLAN networks include;

Authorized users frequently share PSK with others to be able to access the network. This activity posses a great challenge when an attacker gets a hint of such credentials.

In business or organization networks, an employee could plug in a wireless AP to the network or even enable the hotspot service from his workstation that could enable unauthorized user to access the network from a distance. This could possibly allow unauthorized user access to some internal systems that should have been restricted to internal users only.

Some businesses and users also broadcast SSIDs either intentionally or unintentionally. This gives attackers an idea of who owns the WLAN network and to tailor their attack directly to the infrastructure. Setting SSID as for instance 'muwireless' without proper authentication procedures such as supplicant's username, passwords, MAC, and so on makes it simply easy for attackers to connect and in the event of havoc, it becomes difficult tracking down perpetrators.

Some WLAN networks are implemented with no encryption mechanisms and even those that are encrypted usually use weak encryption such as WEP.

Assessment of the overall security of Silenttvalor WLAN

The ‘Silentvalor’ WLAN was simply weak and vulnerable to exploitation due to it lacking encryption and passphrase information. Weak encryption used made information to be displayed in unencrypted form.

Security recommendations

Encouraging encryption in WLAN infrastructure can help mitigate the protocol capturing mechanism when aircrack-ng suite is executed on WLAN networks. ‘Silentvalor’ needed encryption to be enabled for all the data payload within IP packets. WPA2 was released as an advanced wireless LAN encryption method, Silentvalor should have been encrypted with such, as it operated 802.11.

References

Dolly, J. (2018, January 09). *Why you should never, ever connect to public WiFi*. Retrieved from CSO: https://www.csoonline.com/article/3246984/wi-fi/why-you-should-never-ever-connect-to-public-wifi.html

Kaspersky. (n.d.). *How to Avoid Public WiFi Security Risks*. Retrieved from Kaspersky: https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Office of the CIO. (n.d.). *Information Security Awareness Program: Public Wi-Fi Security Risks*. Retrieved from Government of the Northwest Territories: https://www.fin.gov.nt.ca/sites/fin/files/public_wifi_security_risks.pdf