Lab Report 18

1. Assessment Sheet
2. **What functions do these WLAN applications and tools perform on WLANs: airmon-ng, airodump-ng, aircrack-ng, and aireplay-ng?**

Airmon-ng: this tool is used to enable monitor mode of a wireless interface.

Airodump-ng: this is used to capture the wireless frames.

Aircrack-ng: for cracking wireless password through analysis the captured wireless frames.

Airreplay-ng: it used to send the wireless data frames which might be used in a DoS attack.

1. **Why is it critical to use encryption techniques on a wireless LAN? Which encryption method is best for use on a WLAN (WEP, WPA, WPA2)?**

If we don’t encrypt our data on a wireless connection, the data is quite easily be captured by tools like Wireshark and airodump. And, this is every dangerous, especially when we use the connection to login our confidential information. The best encryption method is WPA2 which is harder to crack – taking more time and more complex. And other two are not secure and easily be cracked.

1. **What security countermeasures can you enable on your wireless access point as part of a layered security solution for WLAN implementations?**

So, first we need to isolate the access point within a secure physical location, and then, we need to implement firewall or IPS on these devices which help us stop some attacks.

1. **Why is it so important for organizations, including homeowners, to properly secure their wireless network**

If we don’t secure our wireless network properly, our data would be compromised. For individual, their banking information or identification information will be breached through wireless connection. And, for company, their assets would be compromised if not secure wireless properly.

1. **What risks, threats, and vulnerabilities are prominent with WLAN infrastructures?**

Due to the vulnerability of WLAN protocols, it was easy to be attacked through DoS or DDoS manner. And, also, in most situations, WLAN’s passwords are open to public, at least several people. So, the information transmitted on the wireless is not secure any more.

1. **What is the risk of logging onto access points in airports or other public places?**

Most parts of these public access points are not encrypted properly, so if we connect to it, we have likely to be attacked by hackers which our data would be hijacked by attackers.

1. **Why is it important to have a wireless access policy and to conduct regular site surveys and audits?**

Because the wireless configuration is so easy for every person and the encryption method are not perfect although it has been enhanced a lot. The penetrating tools of airmon-ng are free available. As a result, if we want to protect our wireless environment, we need to periodically check the logs in order to see whether there are abnormal things happen.

1. **What is a risk of using your mobile cell phone or external WLAN as a WiFi connection point**

In an organization, if we allow our staff to use WLAN arbitrarily, we could not monitor it effectively, which means that the user of WLAN can bypass the security setting of LAN. The more serious thing is that through WLAN connection, which is using the company’s network, it was easily be attacked by hackers who wants to compromise the data of the company through this unsafe connection.

1. Challenge Questions

**Description:**

1. Report Screenshot
2. Steps of crack the WPA key

In the cracking process, we need use several tools of Kali linux and these tools help us to crack the password of Wireless connection. The process of cracking is list as follows:

1. Create a folder to store captured data

In this step we create a folder to store the capture result of airodum-ng .

1. Airmon-ng start wlan0

This tools help us to make a wireless interface into monitor mode, in most case it create a monitor for a specified interface. In this case we created a monitor named wlan0

1. Ifconfig

By using this command, we want to make sure the Airmon-ng works properly.

1. Aireplay-ng -0 5 –a MAC –h MAC –ignore-negative-on mon0

With the help of Aireplay-ng, we can send certain signal frames to the wireless network which can cause DoS attack. In this case, we perform deauthentication attack by specify “0” and fragmentation attack by specify “5”. And, the –a switch specifies access point MAC address and the –h switch specifies source MAC address.

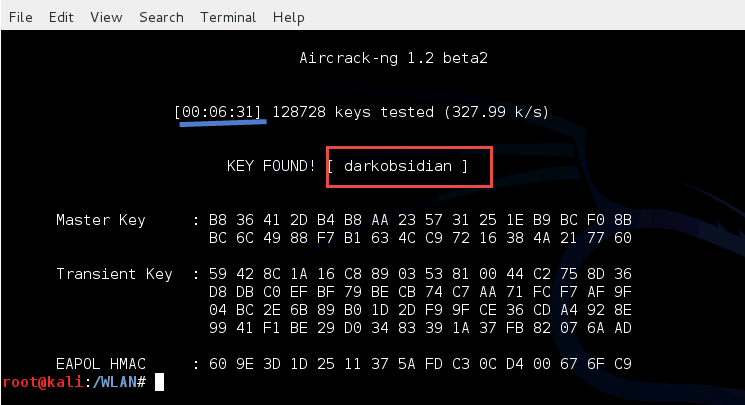
1. Airodump-ng –channel 11 –bssid target mac –write Cpature mon0

By using this tool, we could capture the raw 802.11 frames. In this case we capture specific channel 11 by using “-channel” switch. And we use “–bssid” switch to filter the specific access points which meet the filter expression.

1. Aircrack-ng –w wordlist Capture mon0

This tool helps us to crack the password of wireless network through the analysis the captured 802.11 frames. In this case, we use “-w” switch to specify a password dictionary which can extremely save a lot of time.

1. Cracked WLAN password and the time costs



Time spend: 00:06:31

1. Draft a WLAN Security Implementation plan

In my security Implementation plan, I want draw attentions to the following areas:

* Physical Security
* User authentication
* Access controls
* Access point management
* Logging and auditing

1. Physical Security

As we all know that wireless devices are quite easily be configured by who doesn’t have proficient experience in IT technology, so we should not allow unauthorized people to get close to the wireless devices in order to prevent physical theft. In practice, we should keep wireless devices in a secured room which only authorized people can get in. Besides, every time if a person want go to that area, they should be logged on the system.

1. User authentication

The default secure measures supported by WLAN cannot distinguish the user and they only can identify wireless devices or stations. So, in order to make it more secure, we should add user-level authentication on WLAN which means that if a user wants to use the network to access sensitive data or company’s intranet, he/she must be verified with their identity and secure tokens in order to make sure the authentication.

1. Access controls

We should restrict that only authorized wireless station can connect to the WLAN instead of any devices. Furthermore, the access point should refuse those unencrypted network traffic which helps us to prevent the attacks and if the hackers want do attacks, they should first get the shared secret between real user and real access point.

1. Access point management

Any unnecessary services and ports should be removed or shutting down within an access point. We should also disable the access privilege to WLAN key distribution program. For instance, we only allow administrator to come in and manage the access point.

1. Logging and auditing

Any unauthorized activities including login event, network traffic and so on should be exactly recorded in a security place. And, all these logs should be read-only to anyone expect the process which writes these logs.

Reference:

1. LIM, K. H. (2003). *Security Guidelines for Wireless LAN Implementation.* SANS Institute.

1. Other additional supporting text/image content