Ethical Hacking

Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

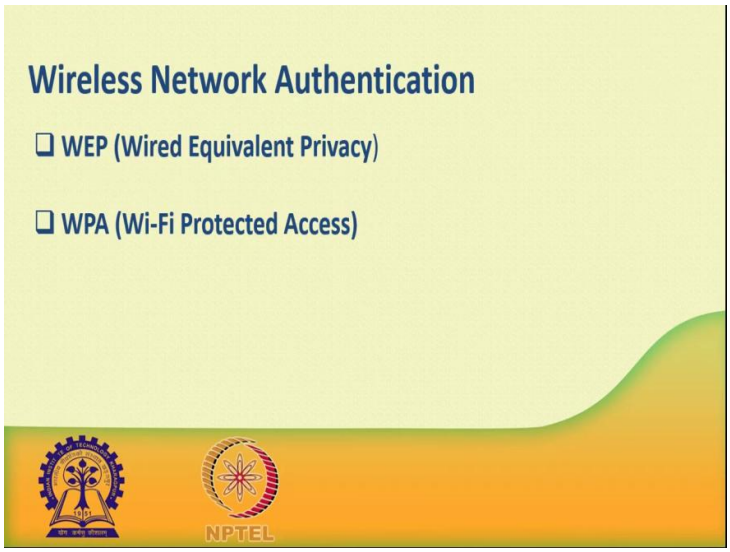
Lecture - 44
Wifi Hacking

In this session, we will discuss about Wifi Hacking. Wireless network are accessible to anyone within the router's transmission radius. This makes them vulnerable to attacks. Hotspots are available in public place such as Airports, Restaurant, Park, etc. In this session we will introduce you two common techniques used to exploit weaknesses in wireless network security implementations. We will also look at some of the countermeasure you can put in place to protect against such attacks.

A wireless network is a network that uses radio app to link computers and other devices together. The implementation is done at the layer 1 that is in physical layer of OSI model. Now, how to access a wireless network? You will need a wireless network enabled devices such as a laptop, tablet, smartphone etc. We will also need to be within the transmission radius of a wireless network access point. Most devices will provide you with the list of available network. If the network is not password protected, then you just have to click on connect. If it is password protected then you will need the password to gain access.

Since, the network is easily accessible to everyone with the wireless network enabled device. Most networks are password protected.

(Refer Slide Time: 02:20)



Now, let us look at some of the most commonly used authentication technique WEP, Wired Equivalent Privacy. It was developed for $IEEE$ 802.11 double n standards. Its goal was to provide the privacy equivalent to that provided by wired networks. WEP, work by encrypting the data being transmitted over the network to keep it safe from eavesdropping.

WEP authentication, open system authentication, these methods grant access to station authentication requested based on the configured access policy. Shared key authentication, this method sends to a an encrypted challenge to the station requesting access, the station in brief the challenge with it is key then responds. If, the encrypted challenge matches the access point value, then access is granted.

Now, what are the weaknesses of WEP encryption? WEP has significant design flaws and vulnerabilities. The integrity of the packet is checked using cyclic redundancy check, CRC 32. CRC 32 integrity check can be compromised by capturing at least 2 packets. The bits in the encrypted stream and the checksum can be modified by the attacker so that the packet is accepted by the authentication system. This leads to unauthorized access to the network.

WEP use the RC4 encryption algorithm to create stream cyphers. The stream cypher input is made up of an initial value IV and a secret the length of the initial value is 24

bits long while the secrete key can either be forty bits or 104 bits long. The total length of both the initial value and secret can either be 64 bits or 128 bits long.

The lower possible value of the secret key, make it easy to crack with initial values combinations. We do not encrypt sufficiently, this makes them vulnerable to attack. WEP is based on password. This makes it vulnerable to dictionary attack. Key management is poorly implemented. Changing keys especially on large network is challenging. WEP does not provide a centralized key management system.

The initial value can be reduced. Because of this security flaw, WEP has been deprecated in favour of WPA. WPA stands for Wi-Fi Protected Access. It is a security protocol developed by the Wi-Fi alliance in response to the weakness found in WEP. It is used to encrypt data on 802.11 W length. It uses higher initial values 48 bit instead of at 24 bits as WEP uses. It uses temporal key to encrypt. And, there are some weaknesses for WPA. The collision avoidance implementation can be broken. It is vulnerable to denial of service attack. Pre shares key uses passphrase, wake passphrase are vulnerable to dictionary attack.

Now, the question is that how to crack wireless networks? The first we will discuss about WEP cracking. Cracking is the process of exploiting security weakness in wireless network and gaining unauthorized access. WEP cracking refers to exploit on networks that use WEP to implement security controls. There are basically two types of cracks namely, passive cracking. This type of cracking has no effect on the network traffic until the WEP security has been trapped, it is difficult to detect.

Active cracking, this type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking, it is more effective compared to passive cracking. Now, there are different WEP cracking tools are there, air crack, WEP crack, qismat, web tech, crypt all these tools are available for WEP cracking.

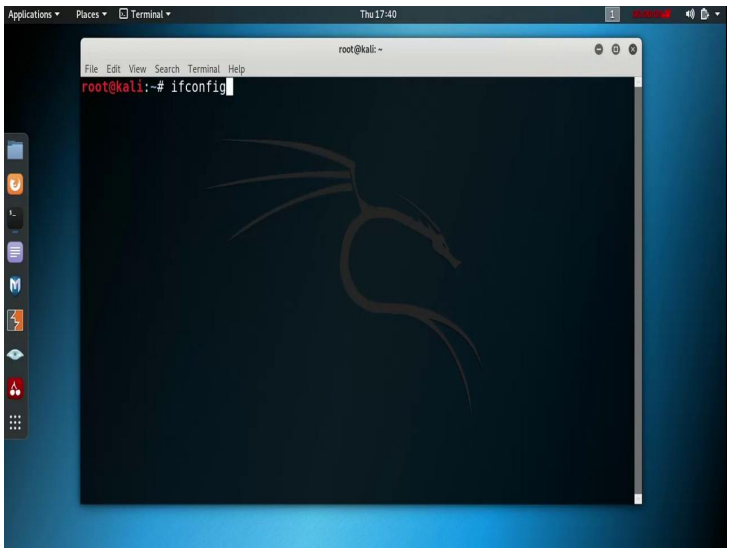
Now, we will discuss about WPA cracking. WPA users are 256 pre shared key or passphrase for authentications. Short pass phrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords. There are several tools are used for WPA cracking, cow patty, kaneabel. There are few attacks are there for WPA shipping. This involves intercepting packets as they are transmitted over a network. The captured data can then be decoded using the tools such as air crack, kaneabel etc.

Man in the middle attack, this involves eavesdropping on a network and capturing sensitive information.

Denial of service attack, the main intent of this attack is to deny legitimate users network resource. Many cracking tools can be used to perform this type of attack. It is possible to crack that WEP or WPA keys used to gain access to a wireless network. Doing so, required software and hardware resources and patience. The success of such attack can also depend on how active and inactive the uses of the target network are.

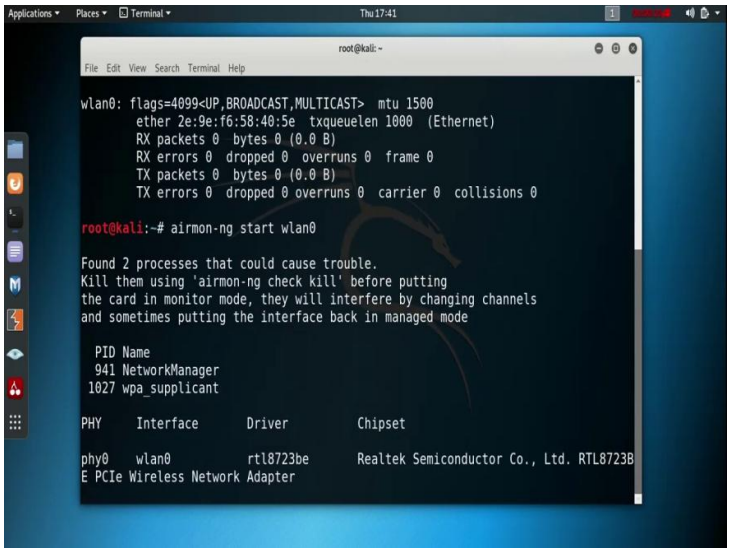
Now, the most important part is how to secure wireless network in minimizing wireless network attack. An organization can attack some policies. Number 1, changing default password that come with a hardware. Number 2, enabling the authentication mechanism, number 3, access to the network can be restricted by following only registered mac address. Number 4, use of strong WEP and WPA PSK keys, a combination of symbol number and characters, reduced the strength of the key in cracking using dictionary and book forced attack. Number 5, firewall software can also help to reduce un priced access thank you.

(Refer Slide Time: 10:52)



Now, I will show you how to hack a Wi-Fi? So, first check the interface name of the NIC card.

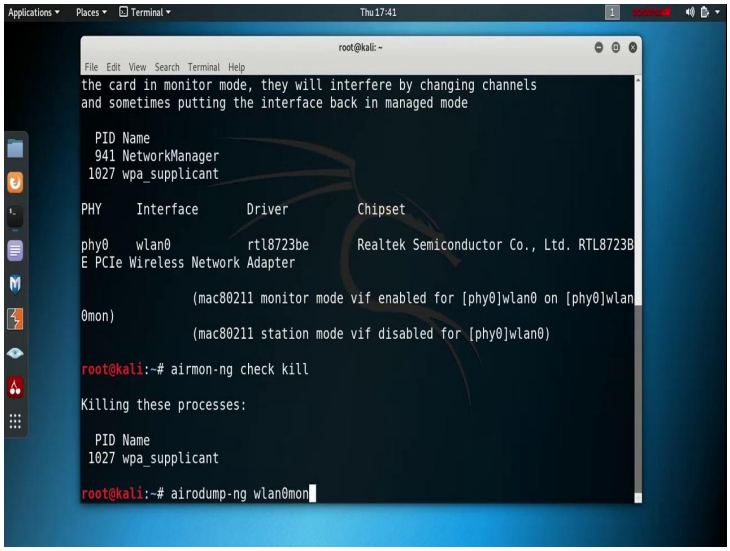
(Refer Slide Time: 10:57)



So, use the command $ifconfig$ and see the interface name is $wlan0$. Now, we need to place our nic card into monitor mode to monitor all the Wi-Fi around us. So, the command is $airmon-ng\ start\ wlan0$ here $wlan0$ is the interface main.

Now, see we are already on the monitor mode and name of the monitor mode is $wlan0mon$ and some process is also running. So, now, we need to kill all the running processes.

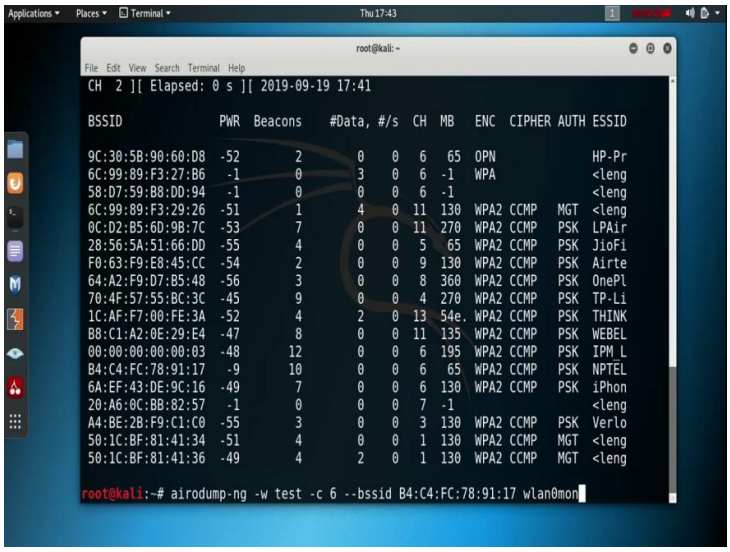
(Refer Slide Time: 11:43)



So, we use the command $airmon - ng\ check\ kill$ to kill all the running processes. So, it is killing these processes.

Now, took down all the information about the Wi-Fi around us. We need to use the command $airodump - ng\ wlan0mon$, where $wlan0mon$ is the name of the interface. And, now see it is successfully able to dump all the information about all the Wi-Fi around us

(Refer Slide Time: 12:26)

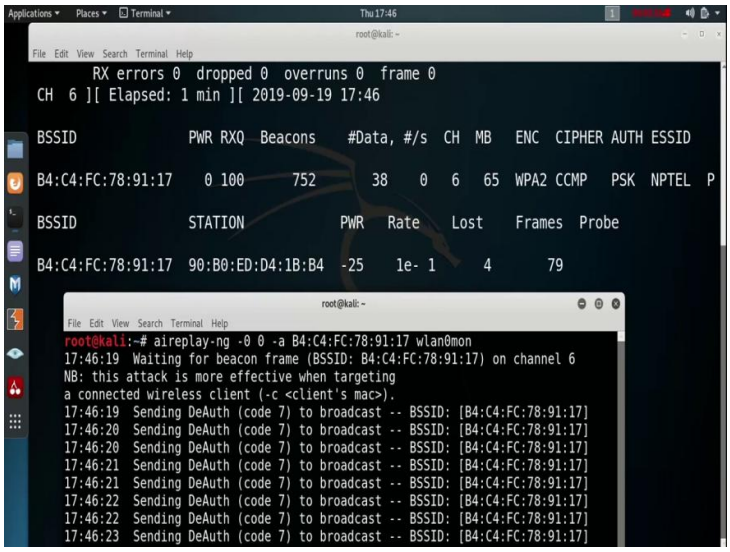


And, this is our target Wi-Fi, NPTEL Wi-Fi. And, see it is showing BSS ID; that means, the mac address of the router and then power. Power represents the strength of the Wi-Fi, which value is absolute value is smaller. It indicate the maximum power and the channel is also important.

Like our radio wireless has multiple channels so that various communications strings do not interfere with each other. The 802.11 standard allow us for channel ranging from 1 to 14, in the US the FCC regulates wireless communication and devices for use in the states are only enable to use channel 1 through 11. Europe use channel 1 through 13 and Japan 1 to 14, and other nations may also use the full range. And, see corresponding encryption and cypher is also there. So, it is WPA to encryption. Now, to dump the Wi-Fi password, we need to use the command $airodum - ng - file\_name$.

So, here we specify the file name is $test$, then $-c$ specify the channel. The Wi-Fi is running over channel 6, then $--bssid$, mac address of the router. So, it specify the mac address of the router. So, put the mac address of our target Wi-Fi means target router, then provide the monitor mode name which we on previously $wlan0mon$.

(Refer Slide Time: 15:31)

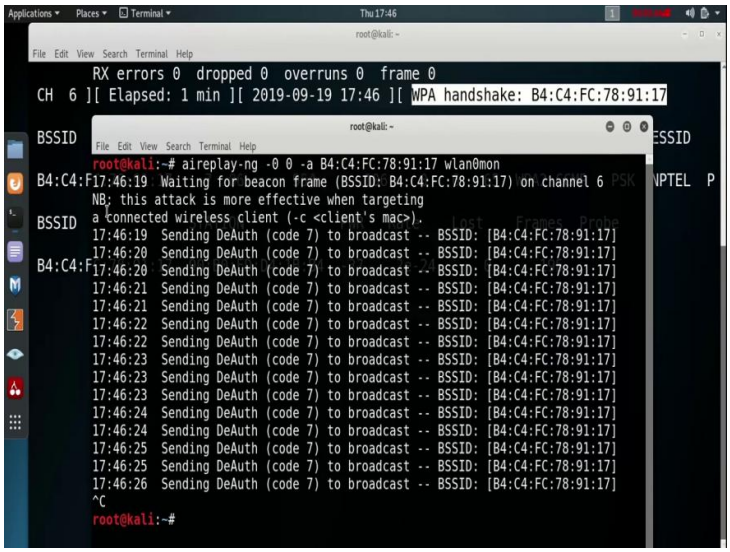


And, now see it is basically showing the details of that particular router. So, BSSID is showing here and it also showing all the connected station with that particular router. So, here only one station is connected and the corresponding mac address is also there.

Now, the thing is that in WPA or WPA 2 encryption, the router sends the password at the time of the connection establishment. So, once a station is already connected. So, we never got, we never get the password. So, now, our aim is to disconnect at least one station from that particular router. As a result it try to reconnect automatically. So, at that time we will we will capture the data packet as well as the authentication key. So, now, open a new terminal and send that the authentication packet to the connected station of that particular router.

So, the command is $aireplay-ng\ -0\ 0-a\ mac\_address\ the\_monitor\_mode$ ($wlan0mon$). It send the authentication packet and as a result. See we got the WPA handshake that means, we got the key.

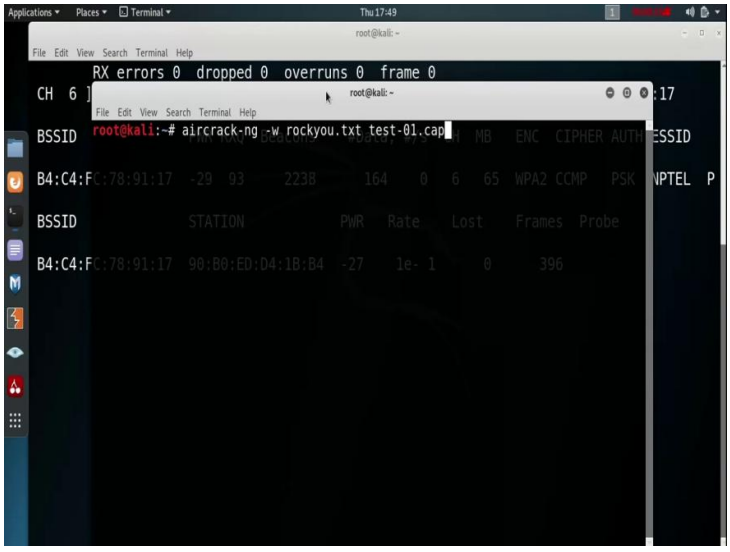
(Refer Slide Time: 18:03)



But, the thing is that key is encrypted and this encryption is using a hash algorithm; that means, we are able to encrypt it, but decryption is not possible.

So, in that case we use the dictionary method or rainbow table method to decrypt the password. So, here we use a very common dictionary $rockyou.txt$ to break the password of the Wi-Fi.

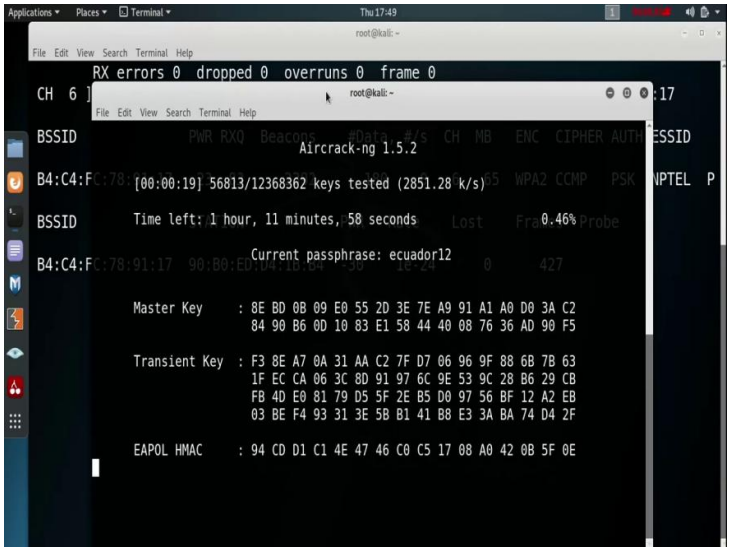
(Refer Slide Time: 18:47)



So, the command is $aircrack\ -ng$, so use the tool $aircrack-ng\ -w$, then specify the dictionary name which is $rockyou.txt$ and then the filename where we stored the password. So, we basically used the name $test$.

So, it create $test-01.cap5$.

(Refer Slide Time: 19:16)

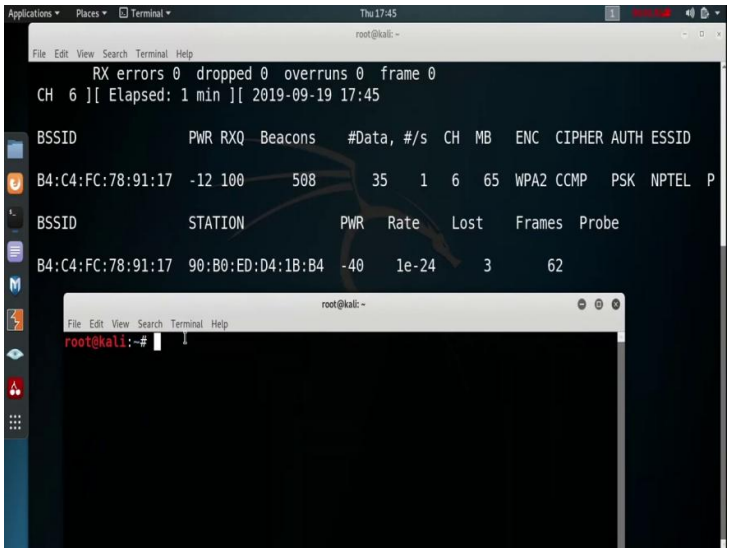


And, it is start the decryption. Once it finds out the password in the dictionary, it able to detect it and successfully got the password. So, you got the password and the password is $NPTEL@2019$. Now, two things is very important. Number 1, if there is no station is connected with that particular router, then no station is disconnected and we never got the password.

Either we need some station to connect it with that particular Wi-Fi; that means, router otherwise at that time when you monitor the password it needs to connect any particular system. And, number 2, this thing is not possible using the virtual machine. If, you use a virtual machine, then you need to use a separate NIC card which is directly connected with the virtual machine.

So, either install kali linux into your main machine or run a live kali linux or use a usb NIC card which is directly connected in the virtual machine.

(Refer Slide Time: 23:25)



Thank you.