EX NO: 4	KISMET
DATE: 22/08/2023	

AIM: To install and see the working of Kismet to find and monitor nearby WIFI.

PROCEDURE:

Step 1- Install Kismet

To install Kismet on Kali Linux, we'll first clone the git repository with the command below.

git clone https://www.kismetwireless.net/git/kismet.git

Depending on which OS you're using, Kismet may not need any dependencies. But to ensure Kismet runs correctly', we should install Kismet's slightly lengthy list of dependencies. These are needed because Kismet deals with detecting, decoding, logging, and sorting lots of wireless data while controlling a wireless card, which requires several libraries to be installed. Y ou can do this by running the following in a terminal window.

sudo apt-get install build-essential git libmicrohttpd-dev zlib1g-dev libnl-3-dev libnl-genl-3-dev libcap-dev libpcap-dev libncurses5-dev libnm-dev libdw-dev libsqlite3-dev

Next, navigate to the Kismet directory we created using cd, and configure he installation.

cd kismet

./configure

This will configure the installation for your particular OS distribution. When that process is complete, create the installation with:

make

When this is complete, we'll run the resulting file to complete the installation with the suidinstall option. This is important because Kismet is directly taking in signals and writing data to your computer. It is a terrible idea to do this as a root user because if any of that data is malicious, it could be executed as root.

When unprivileged users need to accomplish tasks that require privileges, like controlling the wireless network adapter, Linux lets us give privileges to programs instead of users so we don't have to make everyone, including malware, root.

To mitigate [giving root access], Kismet uses separate processes to control the network interfaces and capture packets. These capture programs are much smaller than Kismet itself and do minimal (or no) processing on the contents of the packets they receive

Run the following to complete the SUID installation

sudo make suidinstall

After Kismet is installed, add yourself to the Kismet group to be able to capture packets as a non-root user. Be sure to replace "YourUsername" with your actual username.

sudo usermod -a -G kismet YourUsername

Step 2- Put Your Wireless Card in Monitor Mode

Attach your wireless network card to your computer, and if needed, attach it to the virtual machine using the "USB" settings. To find your card, you can use the ip a or ifconfig commands. Your card should be named something like "wlan1" or "wlan0."

Once you have the name of your card, you can put the card in monitor mode by running the command below.

sudo airmon-ng start YourCardName

This will put YourCardName (be sure to replace with your actual card's name) in monitor mode Your card will be renamed to add a "mon" at the end of the name of the

card. So, if it was named "wlan0" before, it will now be named "wlan0mon This change lets us immediately identify that a card is in wireless monitor mode.

We will use this new name for the card to launch Kismet.

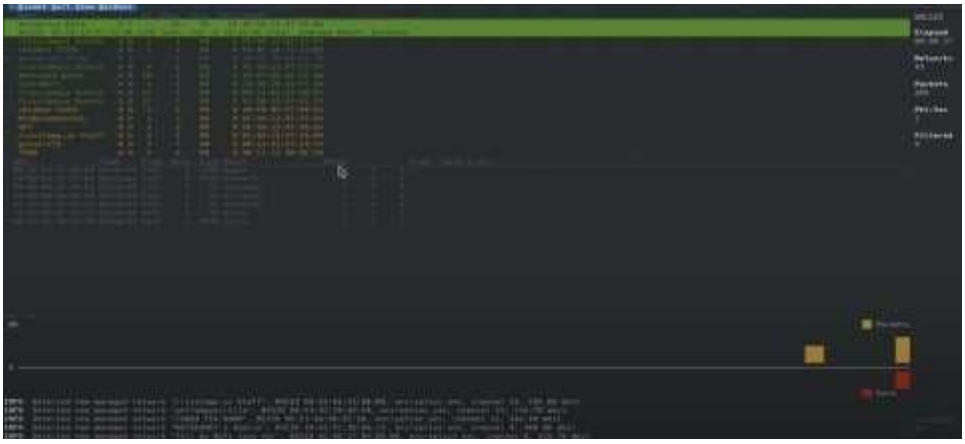
Step 3-Launch Kismet

Starting Kismet is simple. To start as a non-root user, you can simply type the following.

kismet -c YourCardNameMon

Step 4-Persistent Network Surveillance

Once we start Kismet, we should see a list of all the Wi-Fi devices we can detect nearby. The number of devices detected will vary depending on if you're scanning 2.4 GHz, 5 GHz, or both. If you have the ability to add an antenna to your wireless network adapter, a higher gain (or directional) antenna can extend your range and the number of devices detected.



Upon highlighting a network, the first thing we'll notice is the list of wireless clients appears in the main window. These are clients that are associated with the network.

To learn more about a specific network's clients, you can, after highlighting the client window,we can see more information about each client in real time. If you have a network that you want to monitor persistently, it's a good idea to note

the channel number. Since Kismet is exploring all channels by hopping through them, you will miss all transmissions on one channel while Kismet is scanning another. This packet fragmentation can cause you to lose data, so once you identify the network you wish to watch, you should switch from "scanning" to persistently monitoring one channel. This will allow you to capture all activity on the channel

To do this, click on "Kismet" in the top-left corner, and then click on "Config Channel”

In the configuration window, select "Lock," and then enter the number of the channel you wantto monitor.

Step5-Watch for Patterns & Explore Around You

Human behavior will have an effect on the wireless signals around you, and Kismet can let you watch these normally perceivable changes in the wireless environment. It doesn't matter that these networks are encrypted because the relationships between them and plaintext portions of packets are more than enough. By watching the type of traffic flowing across networks, we can take a step beyond simply seeing what is around us and instead begin to learn how thesenetworks are used and by whom.

In particular, Kismet has an "Alerts" section in the menu under "Windows" that will warn you of any suspicious wireless behavior. This can detect things like networks switching channels, deauth packets, networks spoofing other networks, and APs that are rapidly switching names. Our writers accidentally turned on

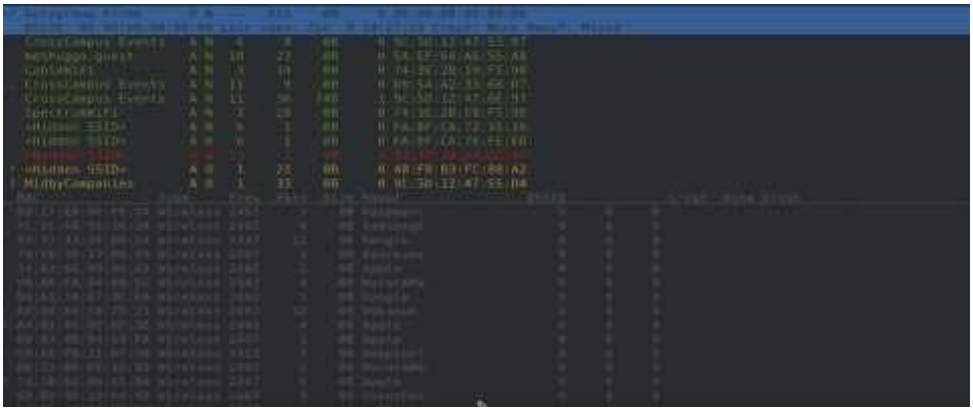
a Hak5 Wi-Fi_ Pineapple while monitoring with Kismet and nearly had a panic attack when a torrent of incredibly serious sounding alert messages started cascading down our screen detecting what was obviously targeted Wi-Fi hacking.

STEP 6-Hiding Your Activity from Cheap & Easy Wireless Surveillance Earlier, I mentioned that Wi-Fi can be detected nearly a mile away using a directional Wi-Fi antenna. These signals are so strong that they are a backup for GPS navigation for the military via NAVSOP (Navigation via Signals of Opportunity). If the military can fly planes by the light of your Wi-Fi network, maybe it's time to consider if you need it turned to the very highest setting. which it almost definitely is right now., in order to just get Wi-Fi in your house or business. Most people have logged into their router exactly once and never change any of the settings beyond the required ones. While the instructions_are different _for _each brand of router, nearly every brand will have a power setting. You can turn this down. Way down. Manufacturers jack it all the way up by default so that you don't complain about the signal strength. If you don't have trouble with your Wi-Fi range, reduce it so it only covers the area you need. Anything you want kept secret should be hard-wired, plain and simple. If you can't block the signals from going out of your house and being picked up by a sensitive antenna, don't put those signals out in the first place. If you have to, you can use Kismet to test the range of when someone can pick up data from your network.

Hiding Your Devices from the Kismet List

For client devices, including smartphones, turn off the Wi-Fi setting whenever you don't need it. Your Wi-Fi card can be used to track you anywhere, not just at home or work. This is true even while you are not connected to Wi-Fi. Devices that rely on Wi-Fi to function you can't do much about. Smartphone manufacturers try to randomize the MAC address that your phone advertises while walking around, but this goes out the window as soon as the phone tries to associate with a network it thinks it knows. This is super easy to do to a crowd of people, which means it doesn't stand up to a real attack. Don't believe me? If you change your phone's

mobile hotspot to "Google Starbucks,"" nearly every smartphone nearby will connect to you and reveal its true MAC address, allowing you to track it.



RESULTS: Thus the kismet is installed and worked successfully.