Detecting Rogue Access Points using Kismet

B R Chandavarkar*, Thejdeep Gudivada†, Shiva Sagar B‡ and Siddartha L K§
Department of Computer Science and Engineering,
National Institute of Technology Karnataka
Mangalore, India - 575025
Email: *brc.nitk@gmail.com, †tejdeepg@gmail.com, ‡shivasagarboraiah@gmail.com, §siddu244@gmail.com

***Abstract*—As large scale organisations tend to expand their wired network infrastructure with the help of access points, increase in the threat to the security of the organisation also occurs. One of the main concerns is that of Rogue Access Points (RAP). In this paper, we discuss about detecting such access points using a Network Sniffing and Intrusion Detection tool called as Kismet**

***Keywords*—Access Points, Network Security, Infrastructure.**

I. Introduction

Nowadays, a major concern for network administrators is the presence of unauthorized access points in the network of the organization. The intruder who is setting up the AP can either be external to the organization or internal to it. Although we can circumvent external intruders from installing Rogue Access Points by using various intrusion detection software, detecting an internal intruder is hard. Also, Rogue Access Points set up by internal intruders are increasing at an alarming rate considering the fact that setting up an AP is as easy as configuring your system to act as a router. The major problem with Rogue Access Points is that they set up a backdoor to the organisation's network thus putting all the sensitive data owned by the organisation at risk. A previously unknown AP may turn out to be an unauthorized AP installed by an employee or may be a malicious AP set to gather information

II. Types of Rogue Access Points

There are a wide range of permutations and combinations of devices which can act as an RAP :

- *Bridging Access Points* — On sub-networks coinciding with or different from wired interface address
- *NAT Access Points* — With or without MAC cloning
- *Soft Access Points* — which can be configured on the wireless interface of a system or using USB dongles.
- Access Points with open wireless links

Soft Access Points is the easiest and the most economical way of setting up an RAP, hence the alarming increase, resulting in almost 20% of the Access Points in an organisation to be unauthorised.

III. Detecting a Rogue Access Point

There are a couple of ways by which a RAP can be detected and suitable action be taken. Moving to a WLAN infrastructure begin with a site survey where planning tools are used to create a floor plan and installing a new AP will involve thinking into overlap between two Access Points, geographical barriers, interference and a many more factors. At the same time, rogue discovery is also done. A baseline list of all untrusted Access Points consisting of their MAC address, approximate location is considered. This can be easily done using Network stumblers, scanning both bands of 802.11 as the intruder rogue may be operating at any frequency. Below is an example of a Rogue Surveillance system :

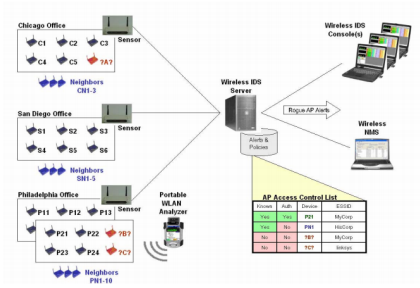

Fig. 1: Example of a Rogue Surveillance System

In general, to generate alerts caused due to Rogue Access Points the systems rely on the Access Control List (ACL) . And the ACL entries can be configured to differentiate between :

- *Known or Authorized Devices* — These are Access Points in your WLAN and the stations are permitted to use them
- *Known or Unauthorized Devices* — Access Points and Stations operating in and near your facility that are not part of your WLAN
- *Unknown or Unauthorized Devices* — Newly discovered Access Points that require investigation and some immediate action to be taken. It is safe to assume that this is a intruder AP or a station. Upon encountering these, Rogue Alerts are issued to the wireless Network Management System and subsequent action is taken. Rogue blocking methods basically fall into two categories :
  - *Wired* — This method involves disabling the LAN switch port closest to the Rogue Access Point's Ethernet attachment point. Similarly, using Firewalls and other filters may also be alternate methods but blocking the closest Ethernet link is the most effective method. We can determine if a rogue is connected to the wired Ethernet network by letting a Wireless Intrusion Detection System send periodic SNMP requests to switches thereby querying all the devices which are connected to the Ethernet matching the retrieved list of addresses with that of the rogue devices.

- *Wireless* — There are two major methods by which Rogue blocking can be done with a wireless AP. The first method employs sending of 802.11 Deauthenticate Control Frames. Essentially, new associations and data transmission will be halted until the flood ends. Another methods jams the channel used by the Rogue Access Point by generating RF noise at that particular frequency. This method is generally not preferred as it affects the nearby Access Points too.

IV. Kismet — Installation and Configuration

Kismet is a 802.11 wireless network detector, sniffer and Intrusion Detection System. Kismet works with any wireless Netowrk Interface Card which supports raw monitoring and can sniff any form of 802.11x traffic.

- Installing Kismet on Linux
  - Download the tar.xz compressed binary source from http://www.kismetwireless.net/download.shtml
  - Decompress the archive and *cd* into it
  - Install all the required dependencies by executing the following command in the terminal — *sudo apt-get install libpcre3-dev libnl-dev libnl-genl-3-dev build-essential libncurses-dev libpcap-dev*
  - Run *./configure* in the terminal
  - Next, run *make* in the terminal
  - As a last step, run *sudo make suidinstall* so that super user permissions are given to Kismet
- Configure Kismet
  - Open */usr/local/etc/kismet.conf* in the text editor of your choice
  - Change *ncsource* if an explicit Network Interface Card is available
  - Change *enablesource* according the above point

```
# See the README for full information on the new source format
# ncsource=interface:options
# for example:
 ncsource=wlan1
# ncsource=wlfi0:type=madwifi
# ncsource=wlan0:name=intel,hop=false,channel=11

# Comma-separated list of sources to enable.  This is only needed if you defined
# multiple sources and only want to enable some of them.  By default, all defined
# sources are enabled.
# For example, if sources with name=prismsource and name=ciscosource are defined,
# and you only want to enable those two:
#enablesources=prismsource,ciscosource
```

Fig. 2: The modified configuration file

  - Change the adapter mode using the following command — *sudo ifconfig wlan1 down — sudo ifconfig wlan1 mode monitor — sudo ifconfig wlan1 up*. If you are unable to set your wireless interface mode to *monitor* you can install Aircrack-ng by executing *sudo apt-get install aircrack-ng* and then running *airmon-ng start ¡interface¿*. This will change the mode of the interface to *monitor*
  - Execute *kismet* and then choose to *Automatically start Kismet server*

```
INFO: Opened pcapdump log file 'Kismet-20141119-12-54-39-1.pcapdump'
INFO: Opened netxml log file 'Kismet-20141119-12-54-39-1.netxml'
INFO: Opened nettxt log file 'Kismet-20141119-12-54-39-1.nettxt'
INFO: Opened gpsxml log file 'Kismet-20141119-12-54-39-1.gpsxml'
INFO: Opened alert log file 'Kismet-20141119-12-54-39-1.alert'
INFO: Kismet starting to gather packets
INFO: Kismet server accepted connection from 127.0.0.1
```

Fig. 3: Kismet server in action

  - The Packet source needs to be set capture all the packages between the interface. Kismet usually captures data at 802.3 layer which requires changing the mode of network interfaces.

V. Creating a Rogue Access Point

Before we actually get into detecting a Rogue Access Point, it would make sense to create once and conclude our results using Kismet. We will be using Aircrack-ng tool and creating a Rogue Access Point using airbase-ng. Execute the following commands in a Linux terminal :

- *airmon-ng start wlan0* — This is used to start a wireless interface in monitor mode. Monitor mode allows a computer to monitor all traffic received from a wireless network.
- *airbase-ng -e RAP -c 11 -v mon0* — This command starts a new Access Point with the name of RAP on channel 11. Keep this process running, perform subsequent commands on a new terminal.
- *ifconfig at0 up* — This is used to bring up the interface at0.
- *ifconfig at0 10.0.0.254 netmask 255.255.255.0*
- *route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.254*
- *nano /etc/dhcp3/dhcpd.conf* and paste the following DHCP configurations:

```
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 10.0.0.0 netmask 255.255.255.0
option subnet-mask 255.255.255.0;
option broadcast-address 10.0.0.255;
option routers 10.0.0.254;
option domain-name-servers 8.8.8.8;
range 10.0.0.1 10.0.0.140;
```

- *iptables –flush*
- *iptables –table nat –flush*
- *iptables –delete-chain*
- *iptables –table nat –delete-chain*
- *iptables -P FORWARD ACCEPT*
- *iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE*
- *echo > '/var/lib/dhcp3/dhcpd.leases'*
- *ln -s /var/run/dhcp3server/dhcpd.pid /var/run/dhcpd.pid*
- *dhcpd3 -d -f -cf /etc/dhcp3/dhcpd.conf at0*
- *echo '1' > /proc/sys/net/ipv4/ip_forward*

VI. Detecting a Rogue Access Point

Kismet has all of the features that you'd expect from a normal packet filter, but it also has many features that were specifically designed for wireless networks. The software is also designed to decode WEP packets on the fly as those packets are captured. Similarly, people who install a rogue access point with malicious intent sometimes try to hide the access point's SSID. Kismet can fight back against this technique because it supports SSID decloaking.
Detection of a Rogue Access Point consists of two phases —

discovery of the existence of such an access point followed by the determination of its location. Detecting a rogues existence can be accomplished with different tools and techniques. Wireless sniffing tools, such as AirMagnet or NetStumbler, can be executed on laptops or handhelds capturing information about access points within their range. Any signal detected can be compared to a list of authorized access points via its MAC address, vendor name, or security configurations. The wireless sniffing software will only detect signals within the range of the device it is running on. The monitoring device(s) may be mobile and moved around the facility on a regular basis looking for rogue signals. This may not be practical in a large facility, or one that is not easily navigated. It is also not effective against an intermittent signal that is not present at the time of monitoring. A variation of the mobile sniffer approach is to run wireless monitoring software on distributed machines on the network and have them report back suspicious signals to a centralized monitoring server. Kismet, has the capability to operate in this fashion with ”drone remotes”. This eliminates the need for mobile monitoring, but will only detect signals within the range of the fixed location monitors.

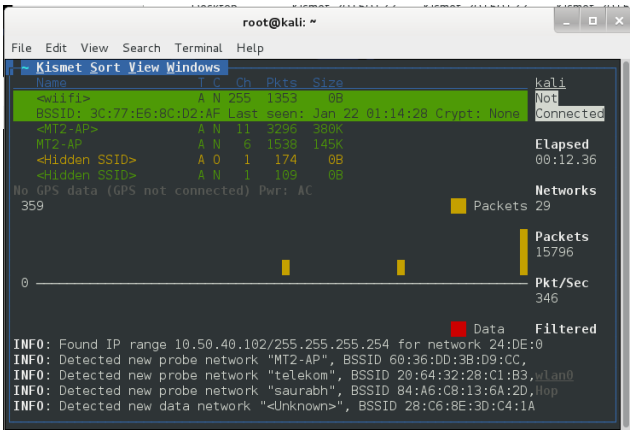

Fig. 4: Kismet showing the Rouge AP along with others

Kismet uses a laptop PC or a handheld device with a wireless NIC to scan the airwaves for wireless traffic. Kismet can detect multiple packet sources simultaneously and can even use multiple wireless NICs simultaneously to multiplex the capture process. As it scans the airwaves, it uses channel hopping to detect wireless devices operating on any available frequency. There's a limit to this detection, however. Current versions of Kismet are limited to detecting only 802.11b wireless devices. Kismet might be able to detect an 802.11g device since it's backward-compatible with 802.11b, but you can forget about using Kismet to detect the less popular 802.11a networks unless you happen to find a Kismet-compatible 802.11a NIC.

As Kismet detects devices, it plots the device's location on a map. The mapping feature is enabled by using an optional GPS card. As wireless devices are being detected, identifying information is also logged. For example, the SSID is recorded, as is the device's manufacturer. Kismet can also alert you to any device that's using weak encryption and any access point that's using a default configuration (which is obviously a huge security risk).

To complete the mapping, you must walk around your office with the wireless device that's running Kismet and let Kismet see what it can detect. While mapping the location of each detected device, Kismet can draw circles on the map to indicate each device's range. Kismet can even guess what signals will be available in unscanned areas of your building, although it's better to scan the entire building if possible.

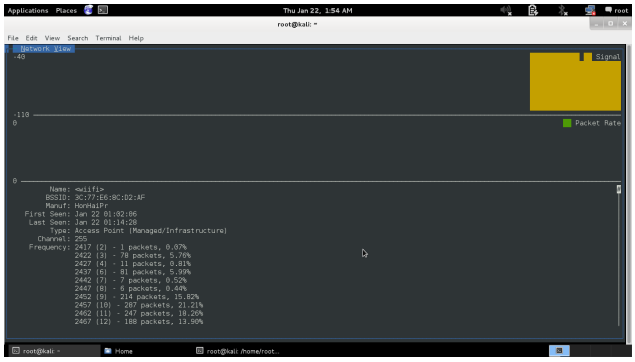

Fig. 5: Kismet showing details of detected Rouge AP

Once you've completed a wireless scan, it's important to analyze the data that you've collected to look for any potential security problems or any wireless devices that don't belong. If the scan appears to be normal, you can use the scan results as a baseline for future scans. If you're ever unsure of a wireless device that's detected during a scan, you can compare the scan results to your baseline scan to see if the detected device is friend or foe.

VII. Conclusion

Various Types of Rogue Access Points can be a threat to the security of the network. Kismet Interface helps in tracking all the those points that causes security issues to the network. We are also able to analyse the signal strength of different networks and keep track the best access point.

References

[1] S. Shetty, Min Song and Liran Ma, *Rogue Access Point Detection by Analyzing Network Traffic Characteristics*, MILCOM, 2007.

[2] V.S.S. Sriram, G. Sahoo and K.K. Agrawal, *Detecting and eliminating Rogue Access Points in IEEE-802.11 WLAN - a multi-agent sourcing Methodology*, IACC, 2010.

[3] S. Nikbakhsh, A.B.A. Manaf, M. Zamani and M. Janbeglou, *A Novel Approach for Rogue Access Point Detection on the Client-Side*, WAINA, 2012.