**Hardware based Intrusion Detection System**

**A Project Synopsis**

**Presented At**

**Maharaja Surajmal Institute of Technology**



By

Amit Sharma

Atif Ahmed

Nishant Kumar

**Project Guide: Prof. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# Abstract

Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization. Sometimes, legacy or operational constraints do not even allow the definition of a fully secure information system. Therefore, intrusion detection systems have the task of monitoring the usage of such systems to detect any apparition of insecure states. They detect attempts and active misuse either by legitimate users of the information systems or by external parties to abuse their privileges or exploit security vulnerabilities.

# Introduction

IDS arms any business against attacks by continuously monitoring network activity, ensuring all activity is normal. If IDS detects malicious activity it responds immediately by destroying the attacker's access and shutting down the attack. IDS reads network traffic and looks for patterns of attacks or signatures, if a signature is identified, IDS sends an alert to the Management Console and a response is immediately deployed.

The reason of developing this tool was the following:

* IDS(s) are difficult to setup
* Costs are high
* Rules implemented on the IDS can clash with services

# Objective

Main objective of this tool is to create a portable hardware based IDS which can be installed easily without any technical knowledge. Thus, empowering the common user and protecting them against the attack vectors.

DHCP

Dynamic Host Configuration Protocol (**DHCP**) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. It enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

STEPS TO CONFIGURE DHCP SERVER

**STEP 1:**

* Apt-get update

(This Linux command updates softwares)

* Apt-get install dnsmasq

(This command installs dnsmasq tool. dnsmasq provides DNS & DHCP services).

**Step 2:**

By convention, most DHCP servers have static IP address as first address in their network space. So, first make DHCP server Raspberry Pi have static IP.

To configure this we must edit the network interface file

* Sudo nano /etc/network/interfaces

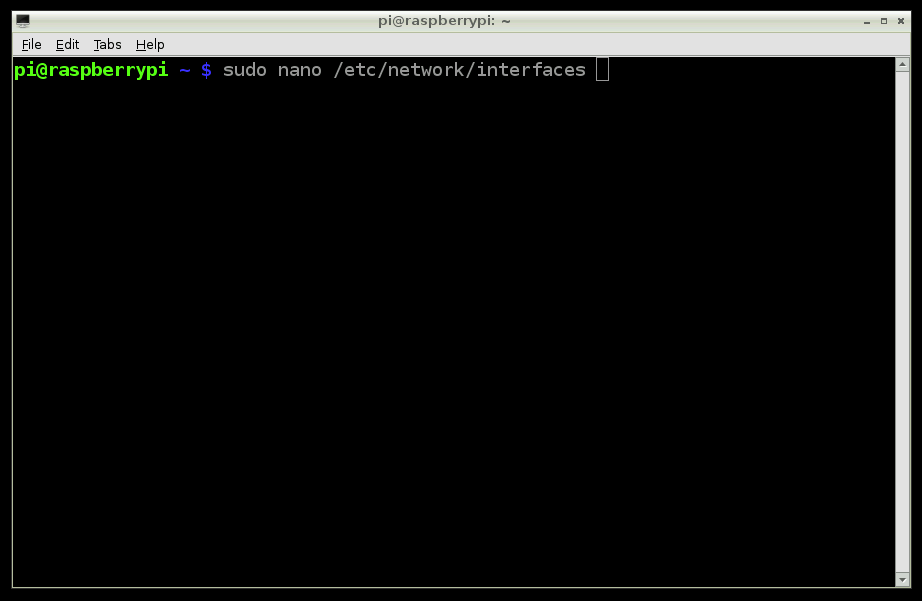


Figure 1: Opening the interfaces file

* Find and comment the line “iface eth0 inet dhcp
* Add your staic ip & netmask details

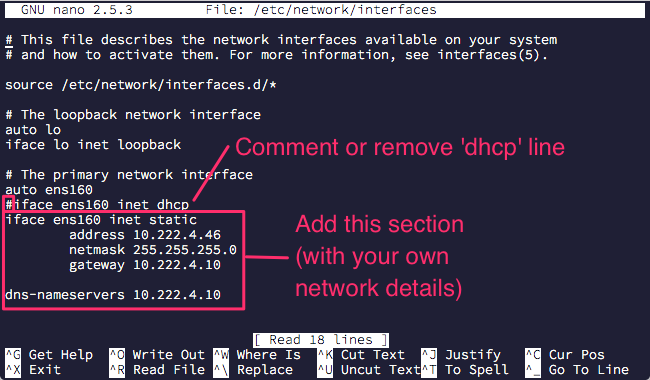


Figure 2: Editing the interfaces file

-sudo services networking restart

(This command restarts the networking services for changes to take effect).

Now we need to configure the DHCP server software, dnsmasq, that was installed earlier.

We are going to explicitly specify a configuration file for the dnsmasq service, so let’s first make a backup of the default config file and then save ours in its place.

-Now add the interface and dhcp range in the config file to be edited as:

interface=eth0

dhcp-range=192.168.0.2,192.168.0.254,255.255.255.0,12h

(The first line tells dnsmasq to listen for DHCP requests on the Ethernet port of the Pi. The second line specifies the range of IP addresses that can be given out; and the 12h at the end of the line specifies the lease time).

-Press Ctrl+O then Enter to save followed by Ctrl+X to quit nano.

The DHCP service is now active and listening for requests from client host computers.

# Creating a Wi-Fi Hotspot in Raspberry Pi

**STEP 1:**

Install the necessary software by

* Sudo apt-get install hostapd udhcp

**STEP 2:**

Configure the DHCP by editing the file /etc/udhcp.conf like this

start 192.168.42.2 # This is the range of IPs that the hostspot will give to client devices.

end 192.168.42.20

interface wlan0 # The device uDHCP listens on.

remaining yes

opt dns 8.8.8.8 4.2.2.2 # The DNS servers client devices will use.

opt subnet 255.255.255.0

opt router 192.168.42.1 # The Pi's IP address on wlan0 which we will set up shortly.

opt lease 864000 # 10 day DHCP lease time in seconds

**STEP 3:**

Give the Pi a static IP address with the following command:

* Sudo ifconfig wlan 192.168.42.1

 Replace the line "iface wlan0 inet dhcp" to:

* Iface wlan inet static

Address 192.168.42.1

Netmask 255.255.255.0

Configure HostAPD.To create a WPA-secred network, edit the file /etc/hostapd/hostapd.conf as

interface=wlan0

driver=nl80211

ssid=My\_AP

hw\_mode=g

channel=6

macaddr\_acl=0

auth\_algs=1

ignore\_broadcast\_ssid=0

wpa=2

wpa\_passphrase=My\_Passphrase

wpa\_key\_mgmt=WPA-PSK

#wpa\_pairwise=TKIP

rsn\_pairwise=CCMP

**STEP 4:**

Configure the NAT (Network Address Translation). NAT is a technique that allows several devices to use a single connection to the internet. First, enable IP forwarding in the kernel:

* sudo sh –c “echo 1 > /proc/sys/net/ipv4/ip\_forward”

To enable NAT in the kernel, run the following commands:

* sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
* sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT
* sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT

**STEP 4:**

Run the services by entering the following commands:

* sudo service hostapd start
* sudo service udhcpd start

# Conclusion

There are limited number of available IDS specially as a hardware which is cheap and easy to deploy. Most ofthem require an expert supervision while setting up the rules. And due to the above-mentioned reasons home users are still in a vulnerable state where and attacker can exploit the network. The tool which we are developing resolves all the issues which are suggested in the document