**ROYAL THUNDERS**

**TITLE**

Various attacks and mitigation techniques to cure against network threats.

**ABSTRACT**

In this Hackathon, we will be presenting packet inspection techniques with platforms compatibility in the context of emerging Internet technologies. It examines and explores the capabilities of content-based traffic analyzer for software defined networks. Network monitoring is a challenging and demanding task that is a vital part of a Network Administrators job and is very important for security point of view. Network Administrators are constantly striving to maintain smooth operation of their networks. But then to minimize human intervention and for intelligence purpose, approach have been taken so that system will work intelligently, without human intervention.

**DESIGN ARCHITECTURE**

A protocol is usually detected by a protocol decoder which is defined in terms of protocol/port, IP address (e.g. traffic from/to specific networks), and protocol attributes. The nDPI library inherits the same design of OpenDPI. Library code is used for implementing general functions, and protocol dissection is implemented in plugins which is showed in the below figure. All the library code is now fully re-entrant, meaning that applications based on nDPI do not need to use locks or synchronisation techniques. All the library initialisation is performed once at startup. nDPI expects that the library caller has already divided the packet in flows i.e dissector division in such a way that it gives a sober look and feel as shown in below figure. The protocol dissectors are registered with attributes such as the default protocol and port. This means for instance that the HTTP dissector specified the default TCP/80, and the DNS dissector TCP and UDP on port 53.

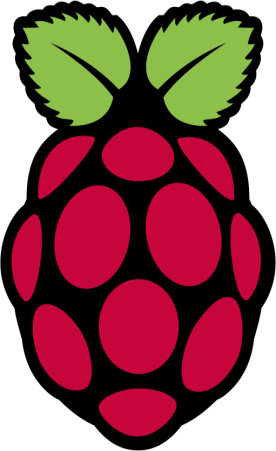
The protocol recognition lifecycle for a new flow as follows:

• nDPI decodes the layer 3 and layer 4 of the packet.

• In case there is a dissector registered for the packet protocol/port, that dissector is tried first.

• In case of no match, all the registered dissectors for the packet protocol (i.e. in case of a UDP packet, all UDP dissectors are tried, but no non-UDP dissector is considered) are tried. Hence, improving the processing and saving CPU time.

• Protocol detection ends as soon as a dissector matches. A typical question of nDPI users, is how many packets we need to detect the application protocol, or to decided that a given flow is unknown. In our experience we have learnt that the answer depends on the protocol. For most UDP-based protocols such as DNS, NetFlow or SNMP one packet is enough to make this decision. Unfortunately there are other UDP protocols such as BitTorrent whose signature might require up to 8 packets in order to be detected. This leads us to the rule of thumb that in nDPI at most 8 packets per direction are enough to make a decision.



Detected protocols:

ICMP packets: 8 bytes: 592 flows: 1

SSH packets: 3 bytes: 248 flows: 1

DHCPV6 packets: 1 bytes: 173 flows: 1

xt\_ndpi.ko

(Kernel Object)

Packet Dispatcher

DNS Dissector

ICMP Dissector

OSPF/BGP Dissector

HTTP/HTTPS Dissector

TCP/UDP Dissector

Hardware Kernel Space User Space Output

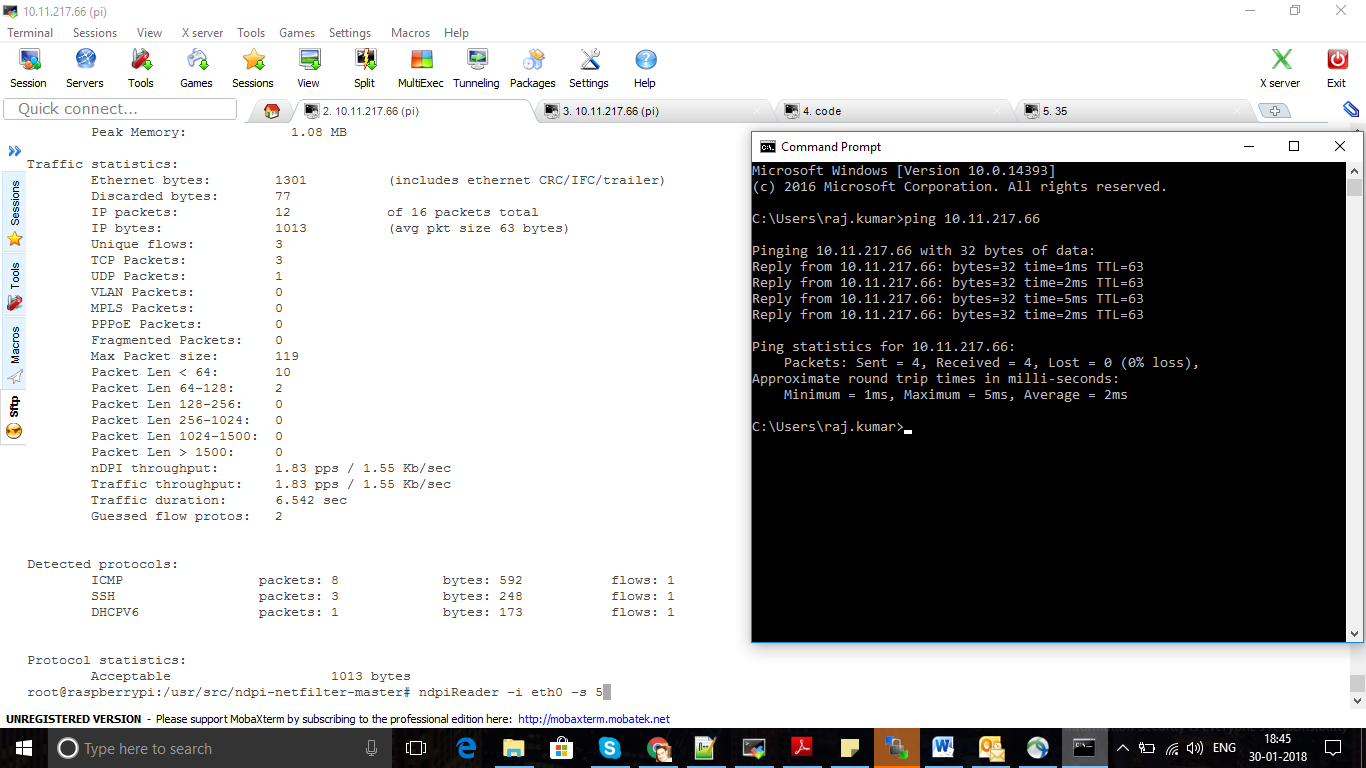
**SOLUTION APPROACH:**

Threat detection will get happen based on combined decision of dissectors and application, It will maintain statistics which will conclude to determine the attack. So, basically It will detect the upcoming threat on our networking devices and for preventive measure, currently handling the resources so that kernel resources won’t get wasted.

**Expected Output**

* Accept under DPI-action.
* Flows under DPI-action.

**SAMPLE OUTPUT :**



**Note :** Live dashboard development is in process, once done we will be able to show everything live on Raspberry Pi IP via GUI.

**BUSINESS IMPACT**

* **Losing confidential information** : “The Call is Coming from Inside the House!” .

In today’s increasingly litigious and highly competitive workplace, confidentiality is important for number of reasons :

* Failure to properly secure and protect confidential business information can lead to the loss of business/clients.
* In the wrong hands, confidential information can be misused to commit illegal activity (e.g., fraud or discrimination), which can in turn result in costly lawsuits for the employer. Many states have laws protecting the confidentiality of certain information in the workplace. The disclosure of sensitive employee and management information can lead to a loss of employee trust, confidence and loyalty. This will almost always result in a loss of productivity.
* **Slam on Company’s Performance** : DOS attack.
* Company’s performance will get hamper and loss of customer trust which in turns gives bad/less business from client side.
* **L2 Switching/L3 Routing/Securities Impact** : Talking about Cisco and Garrettcom products, we have a good future if we go further in packet inspection line. Our problem statement can turns GarrettCom - A Belden Brand into king of networking devices, which in turn will give Incedo a healthy business.