New IPS Based On Modified Forks Of Wireshark And Snort Merged Into A Single Product.

MINT 709: Capstone Project Report

ARJUN JOSHI

Supervisor: Mr. Lenonard Rogers



ABSTRACT

Intrusion prevention has become an extremely important feature of the Defense-in-Depth strategy. The intention of this project is to build the Linux-based open source system which functions as an IPS based on a merger/rewrite of Wireshark and Snort with IP Geolocation built in. This system should work like a wire in the network without causing much delay. Wireshark will capture and analyze every packet. It will generate basic reports for further analysis. I express my cavernous sense of obligation and gratitude to my supervisor Mr. Leonard Rogers for his genuine guidance and constant encouragement throughout this project work. I am highly obliged as my honourable supervisor has devoted his valuable time and shared his expertise knowledge.

I pay my profound gratefulness to Dr. Michael Macgregor for giving me an opportunity to carry out the project work. I must thank him for sparing his valuable time from his busy schedule.

I extend my sincere thanks to Mr. Shahnawaz Mir for providing me such an opportunity to do my project work.

I also wish to express my heartfelt appreciation to my friends, colleagues and many who have rendered their support for the successful completion of the project, both explicitly and implicitly.

ARJUN JOSHI

Abstract	Ι
Acknowledgement	II
List Of Figures	IV
List Of Tables	V
1. INTRODUCTION	1
1.1 Description of the problem	1
1.2 Organization of Report	2
2. COMPONENTS	3
2.1 Linux-Open Source	3
2.2 Ubuntu	3
2.3 Virtualbox/Virtuallization	3
2.4 Intrusion Prevention System (IPS) and SNORT	4
2.5 Wireshark	5
2.6 IPTABLES FIREWALL	6
2.6.1 TTL Target	6
2.6.2 Proxy ARP	7
3. Test Procedure	8
3.1 Network Diagram	8
3.2 Configuration Script	8
4. RESULTS	11
5. CONCLUSION	19
REFERENCES	20

LIST OF FIGURES

No	Title	Page
1.1.1	Project Block Diagram	1
1.1.2	System as a Wire	1
3.1.1	Network Diagram	8
4.1	SELinux Disabled	11
4.2	Ping from VBOX1 to VBOX3	11
4.3	Mirror packet on VBOX4 Management Interface	12
4.4	TCPDUMP and Wireshark capture at VBOX3	13
4.5	TCPDUMP and Wireshark capture at VBOX4	14
4.6	GEOIP Reports Generation	15
4.7.1	Hping3 for Generation of flood traffic	16
4.7.2	Top Talkers	16
4.7.3	Packet Counts by Protocols	17
4.7.4	Packet Length Statistics	17
4.7.5	Packet Length Statistics by Protocol	18

LIST OF TABLES

 No.
 Title
 Page

 2.6.1.1
 TTL target
 6

INTRODUCTION

This Chapter explains description of the problem with a Project Block Diagram. Organization of report is also carried out in section 1.2.

1.1 Description of the problem

This is a multi-phase project with several phases. I have dealt with the initial phase problem: "Interface modification and packet collection/replication"

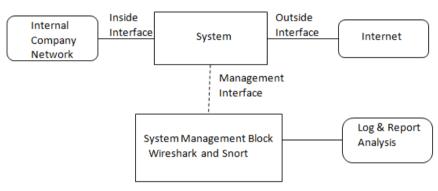


Figure 1.1.1: Project Block Diagram



Figure 1.1.2: System as a Wire

This initial phase is to create a Linux operating system that can monitor and record information of all traffic passing through two of its interfaces. One of the main functions in this new system is to pass packets between the inside and outside interfaces without causing delay between the interfaces. Figure 1.1.1 Shows block diagram of Project. In other words, as far as the packet is concerned it is just traveling on the wire without crossing any interfaces as shown in above Figure 1.1.2. To do this, it means that the packet's hop count is not decremented as it passes between interfaces.

While this does bend/violate some of the rules around the standards of the TCP/IP, the reasons for doing this is to prevent the IPS from being easily detected, and to ensure that trace backs of the communications stream are not seen as going through an additional hop. Also, the inside and outside interfaces do not require an IP Address to function nor do they use their own MAC address.

In the initial phase, they are simply passing traffic back and forth to each other and to the third interface. This means that any inbound traffic received at either the inside or outside interfaces are fully passed to their counterpart and the management interface while ensuring that any data that would normally be changed while going through a hop is not changed and that the packets integrity is maintained.

The management interface does have an IP Address defined and is where the IPS (Wireshark/Snort) solutions are built. As the traffic is replicated to this interface, the Wireshark function (Phase One) is used to capture and analyze every packet. This includes checking the packet's IP Geolocation address from the Geolocation database.

Traffic analysis such as Top 10 or Top 100 talkers on the network can be tracked. Traffic types can also be tracked to better manage QOS loads, allowing for better and even automated traffic shaping, based on the weighting, type and network load of protocols travelling on the network.

1.2 Organization of Report

This report consists of 5 chapters in total. The framework for the report is described as follows:

Chapter 1 provides a brief introduction about initial phase of this project with explanation of project diagram. Components of this project are described in the Chapter 2. Chapter 3 discusses the Test Procedure including network diagram and configuration script which fulfills the initial phase requirement. Result of this project is discussed in Chapter 4. Finally Chapter 5 gives the conclusive remarks of work.

COMPONENTS

In this chapter components are described. It gives the basic description and idea of every tool used in this project.

2.1 Linux-Open Source

Linux is the widely-used open source operating system. As an operating system, Linux is software that resides below all of the other software on a computer, receiving requests from those programs and relaying these requests to the computer's hardware. Ref. [1]

2.2 Ubuntu

Ubuntu is basically a debian-based Linux OS. Ubuntu Touch edition is used for personal computers, Smartphone and tablets. Ubuntu server edition runs network servers. I have used Ubuntu version 14.04.1 for this project. Ref. [2]

2.3 Virtual box/Virtualization

It is a kind of hypervisor used to run an OS in a special environment, which is called a virtual machine. There is continuous development & additional features are implemented inside virtual box. It contains a GUI interface (Qt), as well as headless and command-line tools (SDL) to control and run virtual machines. I have used Virtual Box Version 5.1.4. Ref. [3, 4]

There are 8 different virtual PCI Ethernet cards in VM. For each such card, there is an option to select

- 1. The hardware which will be virtualized
- 2. The mode of virtualization that the virtual card can be operating in with respect to physical networking hardware on the host.

Networking Modes

Networking adapters can be separately configured to work in one of the following modes:

Network Address Translation (NAT)

This mode is used to surf the Web, view e-mail and download files. The "NAT network" is a new NAT scheme introduced in Virtual Box 4.3.

Not attached

This mode indicates network card exists but is not connected, as if no Ethernet cable is plugged into the card.

Bridged networking

There is a direct connection between virtual Box and the installed network cards. Virtual Box exchanges network packets directly, bypassing host OS network stack.

Internal networking

Various kind of software-based network can be created through this mode which is visible to selected virtual machines.

Host-only networking

It creates a separate network that contains the host and a set of VMs, without the need of host's physical network interface. A separate virtual network interface is created on top of the host that provides connection among VMs and the host.

Generic networking

This mode shares the same generic network interface. It allows the user to pick up a driver that can be included with Virtual Box or be distributed in another extension pack.

2.4 Intrusion Prevention System and SNORT

IPS is a threat prevention technology which verifies network traffic flows to discover and forestall vulnerability exploits. Vulnerability exploits occur within the kind of malicious inputs to a target application or service that attackers use to interrupt and gain management of an application or machine. After successful exploit, the aggressor will disable the target application (resulting in a denial-of-service state), or will probably gain access to all or any rights and permissions available to the compromised application.

Intrusion prevention systems track network traffic for malicious activity. The important functions of intrusion prevention systems are to spot malicious activity, log info concerning this activity, report it and block or stop it. Ref. [5]

Categorization

Intrusion prevention systems may be categorized into four totally different types:

- 1. **Host-based intrusion prevention system**: It tracks one host for malicious activity by analyzing events occurring inside particular host using an installed software package.
- 2. Wireless intrusion prevention systems: It tracks a wireless network for malicious traffic as per the behavior of wireless networking protocols.

- 3. **Network-based intrusion prevention system**: It tracks the complete network for malicious traffic by checking protocol activity.
- 4. **Network behavior analysis**: It examines network traffic to spot threats that generate uncommon traffic flows, like distributed denial of service (DDoS) attacks, certain varieties of malware and policy violations.

Detection Techniques

There are three detection techniques for intrusion prevention systems: stateful protocol analysis, statistical anomaly-based, and signature-based Ref. [5]

- 1. **Stateful Protocol Analysis based**: It identifies deviations of protocol states. It compares observed events with respect to "predetermine profiles of normally accepted definitions of benign activity.
- 2. Statistical anomaly-based: It monitors network traffic and based on traffic compares against an established baseline. What is "normal" for that network will be identified by the baseline.
- 3. **Signature-Based**: It monitors packets within the Network and compares it with pre-determined and pre-configured attack patterns known as signatures.

Snort:

It is an open source and free network detection system and prevention system which was created by Martin Roesch in 1998. It has the capability to perform live traffic analysis and packet logging on IP networks.

It performs content searching, matching and protocol analysis. The program may also be accustomed to notice probes, attacks, including common gateway interface, operating system fingerprinting attempts, server message block probes, stealth port scans, and buffer overflows.

There are three basic modes of configuration for snort: packet logger, sniffer and network intrusion detection. The program will log packet to the disk in packet logger mode. The program will read and display network packets on the console in sniffer mode. The program will monitor and analyze network traffic with respect to rule defined by the user in intrusion detection mode. Ref. [6]

2.5 Wireshark

It is an open source and free packet analyzer. It is normally used for network analysis, troubleshooting, education and software & communications protocol development. It is using pcap to capture packets. It also has a terminal based version called TShark. User can see all traffic visible on interface using promiscuous mode. Wireless network interface controllers can also be kept into monitor mode. Ref. [7]

2.6 IPTABLES Firewall

Most of Linux distributions contain IPtables which is a standard firewall. It works by matching every packet that crosses the networking interface against a group of rules to come to a decision what to try and do.

There are several choices to determine which packets match a particular rule. You can match the source or destination address or port, the packet protocol type, the interface that is being used, etc.

When the outlined pattern matches, the action that takes place is named a **target**. A target is often being a final policy decision for the packet, like drop, or accept. It can also be move the packet to a distinct chain for process, or just log the encounter.

These rules are organized into teams referred to as **chains**. A chain could be a set of rules that a packet is checked against consecutively. Once the packet matches one of the rules, it executes the associated task and isn't checked against the rest of rules in the chain. Iptables can also keep track of connections.

There are three main chains. They are:

- **INPUT**: It controls all packets that are addressed to your server.
- **OUTPUT**: It keeps rules for traffic created by your server.
- **FORWARD**: It deals with traffic destined for different servers that are not created on your server. This chain is normally a way to configure your server to route requests to different machines. Ref. [8]

2.6.1 TTL Target

It modifies the Time To Live field in IP header. The **TTL** target is applied within the mangle table. There are 3 ways to define TTL Target as defined in the table below: Ref. [9]

1	ttl-set
Ex	iptables -t mangle -A PREROUTING -i eth0(interface) -j TTLttl-set 64
Detail	Thettl-set option specifies the TTL target which TTL value to keep on the packet in question.
2	ttl-dec
Ex	iptables -t mangle -A PREROUTING -i eth0 (interface) -j TTLttl-dec 1
Details	The ttl-dec option specifies the TTL target to decrement Time To Live value by the amount specified after the ttl-dec option.

Table 2.6.1.1 TTL target

	Ex, if the TTL for an incoming packet was 53 & we had setttl-dec 3, the packet would leave host with a TTL value of 49.
3	ttl-inc
Ex	iptables -t mangle -A PREROUTING -i eth0 (interface) -j TTLttl-inc 1
Detail	Thettl-inc option specifies the TTL target to increment Time To Live value with the value specified to thettl-inc option. Ex, A packet entering with a TTL of 53 would leave the host with TTL 56, if we have specifiedttl-inc 4.

2.6.2 Proxy ARP

A network switch is a kind of bridge with many ports. Proxy ARP can publish ARP entries on 1 interface for machines on 2nd interface. Here, machines on one network segment can reach machines on other segment via intermediary machine. Ref. [10]

Example:

Enable IP forwarding: echo 1 > /proc/sys/net/ipv4/ip_forward Proxy ARP: echo 1 > /proc/sys/net/ipv4/conf/eth0 (interface)/proxy_arp echo 1 > /proc/sys/net/ipv4/conf/eth1 (interface)/proxy_arp

TEST PROCEDURE

This Chapter gives a detailed description about how testing is carried out for this Project. Section 3.1 shows network diagram, while section 3.2 describes configuration script.

3.1 Network Diagram

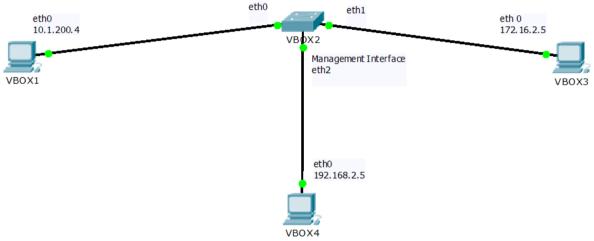


Figure 3.1.1: Network Diagram

- As per the diagram, I am successfully able to ping VBOX3 from VBOX1
- TTL value is also not affecting after changes in VBOX2 so VBOX 2 is behaving as a wire
- I am also able to mirror VBOX1 ---> VBOX3 traffic on VBOX4 which will act as a management box
- IP address has been removed from the interfaces of VBOX2. There is only MAC addresses assigned on interfaces for VBOX2.

3.2 Configuration Script

Part 1: IP assignment on interface

VBOX1: Ifconfig eth0 10.1.200.4 netmask 255.255.255.0 VBOX3: Ifconfig eth0 172.16.2.5 netmask 255.255.255.0 VBOX4: Ifconfig eth0 192.168.2.5 netmask 255.255.255.0

Part 2: Static Route Assignment on every VBOX

VBOX1: IP route add 172.16.2.0/24 dev eth0 VBOX2: IP route add 172.16.2.0/24 dev eth1 IP route add 10.1.200.0/24 dev eth0 IP route add 192.168.2.0/24 dev eth2 VBOX3: IP route add 10.1.200.0/24 dev eth0

Part 3: Forward interface traffic via VBOX2 and Proxy ARP configuration

VBOX2: Sysctl -w net.ipv4.ip_forward=1 Iptables -A FORWARD -i eth0 -j ACCEPT echo 1 > /proc/sys/net/ipv4/conf/eth0/proxy_arp echo 1 > /proc/sys/net/ipv4/conf/eth1/proxy_arp echo 1 > /proc/sys/net/ipv4/conf/eth2/proxy_arp

Part 4: VBOX2 Act as a Wire/Hop count unaffected by VBOX2

VBOX2: Iptables –t mangle –A PREROUTING –i eth0 –j TTL --ttl-inc 1 Iptables –t mangle –A PREROUTING –i eth1 –j TTL --ttl-inc 1

Part 5: Mirror Traffic to VBOX4 Management Interface

Iptables -t mangles -A PREROUTING -j TEE --gateway 192.168.2.5

Following commands are used for Permanent configuration:

VBOX1: gedit /etc/network/interfaces auto eth0 iface eth0 inet static address 10.1.200.4 netmask 255.255.255.0 up route add -net 10.1.200.0/24 dev eth0 up route add -net 172.16.2.0/24 dev eth0 VBOX3: gedit /etc/network/interfaces auto eth0 iface eth0 inet static address 172.16.2.5 netmask 255.255.0

up route add -net 10.1.200.0/24 dev eth0 up route add -net 172.16.2.0/24 dev eth0 VBOX4: gedit /etc/network/interfaces auto eth0 iface eth0 inet static address 192.168.2.5 netmask 255.255.255.0 up route add -net 192.168.2.0/24 dev eth0

VBOX2: gedit /etc/network/interfaces

auto eth0 iface eth0 inet manual up ifconfig eth0 up

auto eth1 iface eth1 inet manual up ifconfig eth1 up

auto eth2 iface eth2 inet manual up ifconfig eth0 up

up route add -net 10.1.200.0/24 dev eth0 up route add -net 172.16.2.0/24 dev eth1 up route add -net 192.168.2.0/24 dev eth2

gedit /etc/sysctl.conf net.ipv4.ip_forward=1 net.ipv4.conf.eth0.proxy_arp=1 net.ipv4.conf.eth1.proxy_arp=1 net.ipv4.conf.eth2.proxy_arp=1

sudo apt-get install iptables-persistent sudo /etc/init.d/iptables-persistent save sudo /etc/init.d/iptables-persistent reload

RESULTS

This chapter shows the snapshots taken for VBOX1 \rightarrow VBOX3 Ping with highlighting TTL Value. It also shows wireshark report generation which is captured on VBOX4

1. SELinux Disabled



Figure 4.1: SELinux Disabled

2 Ping from VBOX1 to VBOX3

Before and after changes in IPTABLE forwarding.

Vbox1 [Running]	
😑 🗣 File Edit View Search Terminal Help 🛛 🛨 🖪 📼 🗐 3:31 PM	₩
arjun@arjun-VirtualBox:~\$ ping 172.16.2.5	
O PING 172.16.2.5 (172.16.2.5) 56(84) bytes of data.	
64 bytes from 172.16.2.5: icmp_seq=1 ttl=63 time=0.718 ms	
64 bytes from 172.16.2.5: icmp_seq=2 ttl=63 time=0.554 ms	
64 bytes from 172.16.2.5: icmp_seq=3 ttl=63 time=0.880 ms	
64 bytes from 172.16.2.5: icmp_seq=4 ttl=63 time=0.534 ms	
64 bytes from 172.16.2.5: icmp_seq=5 ttl=63 time=0.858 ms	
64 bytes from 172.16.2.5: icmp_seq=6 ttl=63 time=0.880 ms	
172.16.2.5 ping statistics	
6 packets transmitted, 6 received, 0% packet loss, time 4998	ms
<pre>arjun@arjun-VirtualBox:~\$ ping 172.16.2.5 PING 172.16.2.5 (172.16.2.5) 56(84) bytes of data.</pre>	
64 bytes from 172.16.2.5: icmp_seq=1 ttl=64 time=0.605 ms	
64 bytes from 172.16.2.5: icmp_seq=2 ttl=64 time=0.611 ms	
64 bytes from 172.16.2.5: icmp_seq=3 ttl=64 time=0.586 ms	
64 bytes from 172.16.2.5: icmp_seq=4 ttl=64 time=0.708 ms	
64 bytes from 172.16.2.5: icmp_seq=5 ttl=64 time=0.597 ms	
64 bytes from 172.16.2.5: icmp_seq=6 ttl=64 time=0.620 ms	
<u>~</u> ^c	
172.16.2.5 ping statistics	
6 packets transmitted, 6 received, 0% packet loss, time 4998	ms
Tt min/avg/max/mdev = 0.5 <u>8</u> 6/0.621/0.708/0.042 ms	
arjun@arjun-VirtualBox:~\$	
🛛 💿 💿 💭 🎾 🚍 🖳 😳 🐼 💌 Lef	t ೫

Figure 4.2: Ping from VBOX1 to VBOX3

...

3. Packet from VBOX1 to VBOX2 mirror on VBOX4 Management Interface

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help64 bytes from 172.16.2.5: icmp_seq=3 ttl=64 time=0.699 ms 64 bytes from 172.16.2.5: icmp_seq=4 ttl=64 time=0.699 ms 64 bytes from 172.16.2.5: icmp_seq=6 ttl=64 time=0.699 ms 64 bytes from 172.16.2.5: icmp_seq=6 ttl=64 time=0.698 ms 64 bytes from 172.16.2.5: icmp_seq=7 ttl=64 time=0.698 ms 64 bytes from 172.16.2.5: icmp_seq=8 ttl=64 time=0.1980 ms 64 bytes from 172.16.2.5: icmp_seq=9 ttl=64 time=0.918 ms 64 bytes from 172.16.2.5: icmp_seq=10 ttl=64 time=0.916 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.916 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.916 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.918 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.688 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.688 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.614 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.614 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.698 ms 64 bytes from 172.16.2.5: icmp_seq=12 ttl=64 time=0.688 ms 64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.580 ms <th>Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from m 👣 🖬</th> <th>📧 🕪) 2:16 PM 🔱</th> <th>arjun@arjun-VirtualBox: ~</th> <th>🏚 🖪 💌 📢) 3:38 PM</th>	Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from m 👣 🖬	📧 🕪) 2:16 PM 🔱	arjun@arjun-VirtualBox: ~	🏚 🖪 💌 📢) 3:38 PM
Filter:icmpNo.TimeSourceDestinatiorProtocol LengthInfe64bytesfrom 172.16.2.5:icmp_seq=8ttl=64time=0.91664bytesfrom 172.16.2.5:icmp_seq=18ttl=6464bytesfrom 172.16.2.5:icmp_seq=11ttl=6464bytesfrom 172.16.2.5:icmp_seq=12ttl=6464bytesfrom 172.16.2.5:icmp_seq=12ttl=6464bytesfrom 172.16.2.5:icmp_seq=12ttl=6464bytesfrom 172.16.2.5:icmp_seq=12ttl=6464bytesfrom 172.16.2.5:icmp_seq=13ttl=6464bytesfrom 172.16.2.5:icmp_seq=1364bytesfrom 172.16.2.5:icmp_seq=1664bytesfrom 172.16.2.5:icmp_seq=1664bytesfrom 172.16.2.5:icmp_seq=1664bytesfrom 172.16.2.5:icmp_seq=1664bytesfrom 172.16.2.5:icmp_seq=1764bytesfrom 172.16.2.5:icmp_seq=1864bytesfrom 172.16.2.5:icmp_seq=1864bytesfrom 172.16.2.5:icmp_seq=2464bytesfrom 172.16.2.5:icmp_seq=2464bytesfrom 172.16.2.5:icmp_seq=2464bytesfrom 172.16.2.5:icmp_seq=2464bytesfrom 172.16.2.5:icmp_seq=2464bytesfrom 172.16.2.5:icmp_seq=2664 <td< th=""><th>d a c c c c c c c c c</th><th>ny Tools Internals Help</th><th>64 bytes from 172.16.2.5: 64 bytes from 172.16.2.5:</th><th>icmp_seq=4 ttl=64 time=0.609 ms icmp_seq=5 ttl=64 time=0.605 ms</th></td<>	d a c c c c c c c c c	ny Tools Internals Help	64 bytes from 172.16.2.5: 64 bytes from 172.16.2.5:	icmp_seq=4 ttl=64 time=0.609 ms icmp_seq=5 ttl=64 time=0.605 ms
No. 11me Source Destination Protocol Lengt Inter 64 bytes from 172.16.2.5: tcmp_seq=10 ttl=64 time=0.954 ns 64 bytes from 172.16.2.5: tcmp_seq=11 ttl=64 time=0.668 ns 64 bytes from 172.16.2.5: tcmp_seq=13 ttl=64 time=0.688 ns 64 bytes from 172.16.2.5: tcmp_seq=13 ttl=64 time=0.618 ns 64 bytes from 172.16.2.5: tcmp_seq=14 ttl=64 time=0.688 ns 64 bytes from 172.16.2.5: tcmp_seq=16 ttl=64 time=0.614 ns 64 bytes from 172.16.2.5: tcmp_seq=17 ttl=64 time=0.614 ns 64 bytes from 172.16.2.5: tcmp_seq=17 ttl=64 time=0.614 ns 64 bytes from 172.16.2.5: tcmp_seq=18 ttl=64 time=0.614 ns 64 bytes from 172.16.2.5: tcmp_seq=210 ttl=64 time=0.629 ns 64 bytes from 172.16.2.5: tcmp_seq=210 ttl=64 time=0.629 ns 64 byte			64 bytes from 172.16.2.5:	icmp_seq=7 ttl=64 time=0.890 ms
64 bytes from 172.16.2.5: icmp_seq=12 ttl=64 time=0.668 ms 64 bytes from 172.16.2.5: icmp_seq=13 ttl=64 time=0.583 ms 64 bytes from 172.16.2.5: icmp_seq=14 ttl=64 time=0.583 ms 64 bytes from 172.16.2.5: icmp_seq=14 ttl=64 time=0.614 ms 64 bytes from 172.16.2.5: icmp_seq=16 ttl=64 time=0.614 ms 64 bytes from 172.16.2.5: icmp_seq=17 ttl=64 time=0.614 ms 64 bytes from 172.16.2.5: icmp_seq=17 ttl=64 time=0.614 ms 64 bytes from 172.16.2.5: icmp_seq=17 ttl=64 time=0.639 ms 64 bytes from 172.16.2.5: icmp_seq=18 ttl=64 time=0.435 ms 64 bytes from 172.16.2.5: icmp_seq=18 ttl=64 time=0.435 ms 64 bytes from 172.16.2.5: icmp_seq=28 ttl=64 time=0.435 ms 64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.435 ms 64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.598 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.598 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.598 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.546 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.548 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.548 ms 64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.548 ms <td>No. Time Source Destination</td> <td>Protocol Length Infc</td> <td>64 bytes from 172.16.2.5: 64 bytes from 172.16.2.5:</td> <td>icmp_seq=9 ttl=64 time=6.74 ms icmp_seq=10 ttl=64 time=0.916 ms</td>	No. Time Source Destination	Protocol Length Infc	64 bytes from 172.16.2.5: 64 bytes from 172.16.2.5:	icmp_seq=9 ttl=64 time=6.74 ms icmp_seq=10 ttl=64 time=0.916 ms
Image: Second	_		64 bytes from 172.16.2.5:	icmp_seq=12 ttl=64 time=0.668 ms
64 bytes from 172.16.2.5: icmp_seq=17 ttl=64 time=0.514 ms 64 bytes from 172.16.2.5: icmp_seq=18 ttl=64 time=0.569 ms 64 bytes from 172.16.2.5: icmp_seq=20 ttl=64 time=0.944 ms 64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.988 ms 64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.988 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.988 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.863 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.863 ms 64 bytes from 172.16.2.5: icmp_seq=23 ttl=64 time=0.863 ms 64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.888 ms 64 bytes from 172.16.2.5: icmp_seq=26 ttl=64 time=0.888 ms <td></td> <td></td> <td>64 bytes from 172.16.2.5: 5 64 bytes from 172.16.2.5: 5</td> <td>icmp_seq=14 ttl=64 time=0.890 ms icmp_seq=15 ttl=64 time=1.30 ms</td>			64 bytes from 172.16.2.5: 5 64 bytes from 172.16.2.5: 5	icmp_seq=14 ttl=64 time=0.890 ms icmp_seq=15 ttl=64 time=1.30 ms
64 bytes from 172.16.2.5: icmp_seq=19 ttl=64 time=0.435 ms 64 bytes from 172.16.2.5: icmp_seq=20 ttl=64 time=0.944 ms 64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.888 ms 64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.863 ms 64 bytes from 172.16.2.5: icmp_seq=23 ttl=64 time=0.863 ms 64 bytes from 172.16.2.5: icmp_seq=24 ttl=64 time=0.868 ms 64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.868 ms 64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.888 ms 64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.888 ms			64 bytes from 172.16.2.5:	icmp_seq=17 ttl=64 time=0.514 ms
64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.598 ms 64 bytes from 172.16.2.5: icmp_seq=23 ttl=64 time=0.863 ms 64 bytes from 172.16.2.5: icmp_seq=24 ttl=64 time=0.865 ms 64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.885 ms 64 bytes from 172.16.2.5: icmp_seq=26 ttl=64 time=0.885 ms			64 bytes from 172 16 2 5.	icmp_seq=20 ttl=64 time=0.944 ms
64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.885 ms 64 bytes from 172.16.2.5: icmp_seq=26 ttl=64 time=0.580 ms			64 bytes from 172.16.2.5:	icmp_seq=22 ttl=64 time=0.598 ms
etho: etho: etho:		1	64 bytes from 172.16.2.5:	icmp_seq=25 ttl=64 time=0.885 ms
🖸 🗇 💭 🥔 🚍 🗮 🔟 🔇 🖲 Left 🕱	🛃 eth0: <live capture="" in="" progress=""> N Profile:</live>		a. 64 bytes from 172.16.2.5: 9	

Before Executing Part5 Script of chapter 3

Vbox1 [Running]

After Executing Part 5 Script of chapter 3

🕘 😑 🕒 Vbox4 [Running]	Vbox1 (Running)
Capturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 🗉 👣 📧 🜒 2:53 PM 🛟	arjun@arjun-VirtualBox: ~ 👣 🖬 🖦 🕪 🕬 4:14 PM
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help	
	64 bytes from 172.16.2.5: icmp_seq=5 ttl=64 time=1.16 ms 64 bytes from 172.16.2.5: icmp seq=6 ttl=64 time=0.713 ms
	64 bytes from 172.16.2.5: tcmp_seq=0 ttt=64 ttme=0.783 ms
Filter: icmp • •	64 bytes from 172.16.2.5: icmp_seq=8 ttl=64 time=1.05 ms
No. Time Source Destination Protocol Length Infc	64 bytes from 172.16.2.5: icmp_seq=9 ttl=64 time=1.06 ms
1 0.00000000 10.1.200.10 172.16.2.5 ICMP 98 Echo	64 bytes from 172.16.2.5: icmp_seq=10 ttl=64 time=0.883 ms 64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.812 ms
2 0.000456000 172.16.2.5 172.16.2.4 ICMP 98 Echo	64 bytes from 172.16.2.5: icmp_seq=11 ttl=64 time=0.812 ms 64 bytes from 172.16.2.5: icmp_seq=12 ttl=64 time=1.21 ms
3 1.000262000 10.1.200.10 172.16.2.5 ICMP 98 Echo	64 bytes from 172.16.2.5: icmp_seq=12 ttl=64 time=1.18 ms
4 1.000855000 172.16.2.5 172.16.2.4 ICMP 98 Echo	64 bytes from 172.16.2.5: icmp_seq=14 ttl=64 time=1.08 ms
5 2.002156000 10.1.200.10 172.16.2.5 ICMP 98 Echo	64 bytes from 172.16.2.5: icmp_seq=15 ttl=64 time=0.683 ms
6 2.002972000 172.16.2.5 172.16.2.4 ICMP 98 Echo	64 bytes from 172.16.2.5: icmp_seq=16 ttl=64 time=0.832 ms
Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on .	64 bytes from 172.16.2.5: icmp_seq=17 ttl=64 time=0.909 ms 64 bytes from 172.16.2.5: icmp seq=18 ttl=64 time=1.86 ms
Ethernet II, Src: CadmusCo 31:e1:5f (08:00:27:31:e1:5f), Dst: CadmusCo	
▶ Internet Protocol Version 4, Src: 10.1.200.10 (10.1.200.10), Dst: 172.	64 bytes from 172.16.2.5: icmp seq=20 ttl=64 time=1.27 ms
▶ Internet Control Message Protocol	64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.838 ms
	64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.826 ms
0000 08 00 27 1b ca 09 08 00 27 31 e1 5f 08 00 45 00' '1.	Terminal 172.16.2.5: icmp_seq=23 ttl=64 time=0.975 ms Terminal 172.16.2.5: icmp_seq=24 ttl=64 time=0.925 ms
0010 00 54 20 7a 40 00 41 01 99 0e 0a 01 c8 0a ac 10 .T z@.A	64 bytes from 172.16.2.5: tcmp_seq=24 ttl=64 ttme=0.925 ms
0020 02 05 08 00 c4 88 11 c2 00 0b 49 65 1a 58 c9 e9	64 bytes from 172.16.2.5: icmp_scq=26 ttl=64 time=0.875 ms
	64 bytes from 172.16.2.5: icmp_seq=27 ttl=64 time=0.740 ms
💭 🕅 eth0: <live capture="" in="" progress=""> 🛛 Profile: Default</live>	
🛛 💿 🥥 💷 🗮 🛄 🔇 💌 Left ¥	🖸 🔗 🗐 🌽 🔛 🖉 🔛 🖉 🔛 Left

Figure 4.3: Mirror packet on VBOX4 Management Interface

4. TCPDUMP and wireshark capture at VBOX3

- VBOX1 is Pinging to VBOX3.
- I run below command on VBOX3 to capture traffic via TCPDUMP tcpdump –i eth0 icmp
- From the capture it does not show any IP address of VBOX2. So VBOX2 behaves as a wire.

Vbox1 [Running]	Vbox3 [Running]
minal have the Auto capture keyboard option turned on. This will cause the Virtual Machine to	📲 Terminal 🚺 🖬 ា 🕬 12:1:
Continue /	🖉 🥘 💿 root@arjun-VirtualBox: /home/arjun
Search your computer and online sources =12 ttl=64 time=1.32 ms	00:12:04.115453 IP 172.16.2.5 > 10.1.200.4: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=13 ttl=64 time=1.25 ms	2487, seq 27, length 64
64 bytes from 172.16.2.5: icmp_seq=14 ttl=64 time=0.757 ms	00:12:05.115216 IP 10.1.200.4 > 172.16.2.5: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=15 ttl=64 time=0.909 ms	id 2487, seq 28, length 64
64 bytes from 172.16.2.5: icmp_seq=16 ttl=64 time=0.830 ms	00:12:05.115254 IP 172.16.2.5 > 10.1.200.4: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=17 ttl=64 time=0.753 ms	2487, seq 28, length 64
64 bytes from 172.16.2.5: icmp_seq=18 ttl=64 time=1.16 ms	00:12:06.117510 IP 10.1.200.4 > 172.16.2.5: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=19 ttl=64 time=1.11 ms 64 bytes from 172.16.2.5: icmp_seq=20 ttl=64 time=0.850 ms	id 2487, seq 29, length 64
64 bytes from 172.16.2.5: icmp_seq=21 ttl=64 time=0.743 ms	00:12:06.117608 IP 172.16.2.5 > 10.1.200.4: ICMP echo re 2487, seq 29, length 64
64 bytes from 172.16.2.5: icmp_seq=22 ttl=64 time=0.841 ms	00:12:07.119631 IP 10.1.200.4 > 172.16.2.5: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=23 ttl=64 time=0.906 ms	id 2407 and 20 Janath 64
64 bytes from 172.16.2.5: icmp_seq=24 ttl=64 time=0.785 ms	00:12:07.119670 IP 172.16.2.5 > 10.1.200.4: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=25 ttl=64 time=0.833 ms	2487, seq 30, length 64
64 bytes from 172.16.2.5: icmp_seq=26 ttl=64 time=0.848 ms	00:12:08.121429 IP 10.1.200.4 > 172.16.2.5: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=27 ttl=64 time=0.878 ms 64 bytes from 172.16.2.5: icmp_seq=28 ttl=64 time=0.897 ms	2487, seq 31, length 64
64 bytes from 172.16.2.5: icmp_seq=20 ttl=64 time=0.897 Ms	00:12:08.121465 IP 172.16.2.5 > 10.1.200.4: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=30 ttl=64 time=1.30 ms	2487, seq 31, length 64 2487, seq 31, length 64
64 bytes from 172.16.2.5: icmp_seq=31 ttl=64 time=0.881 ms	id 2487, seq 32, length 64
64 bytes from 172.16.2.5: icmp_seq=32 ttl=64 time=0.795 ms	00:12:09.120430 IP 172.16.2.5 > 10.1.200.4: ICMP echo re
64 bytes from 172.16.2.5: icmp_seq=33 ttl=64 time=0.738 ms	2487, seq 32, length 64
🛐 💿 🗐 🥟 💻 🚝 🛄 🚳 🖲 Left ೫	S 🖸 🖶 🗮 🖉 🕼 🖉
Vbox1 [Running]	Vbox3 [Running]
inal 1 En (%) (4)) 7:58 PM (
ve the Auto capture keyboard option turned on. This will cause the Virtual Machine to	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 🛙 👣 🗈 📧 🐠 12:14 AM
ve the Auto capture keyboard option turned on. This will cause the Virtual Machine to	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1] f. En 📧 40) 12:14 AM
Auto capture keyboard option turned on. This will cause the Virtual Machine to contribution Virtual Box: Thome for the Virtual Machine to Search your computer and online sources 1=127 ttl=64 time=1.01 ms 64 bytes from 172.16.2.5: icmp_seq=128 ttl=64 time=0.756 ms	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1] 1 [m] 🗈 40) 12:14 AN File Edit View Go Capture Analyze Statistics Telephony Tools Internals () () () () () () () () () () () () () (
All Control of the second option turned on. This will cause the Virtual Machine to 40, 758 PM Control of the second former of the secon	apturing from eth0 (Wireshark 1.10.6 (v1.10.6 from 1 i iii iii iii iii iii iii iii iii ii
the Auto capture keyboard option turned on. This will cause the Virtual Machine to the Auto capture keyboard option turned on. This will cause the Virtual Machine to the automation virtual Box former Automation Search your computer and online sources 1=127 ttl=64 time=1.01 ms 64 bytes from 172.16.2.5: tcmp_seq=128 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: tcmp_seq=120 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: tcmp_seq=120 ttl=64 time=0.788 ms	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1] En E v1) 12:14AA File Edit View Go Capture Analyze Statistics Telephony Tools Internals © © 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
All the Auto capture keyboard option turned on. This will cause the Virtual Machine to 40, 7758 Provided and the Control of the Auto capture keyboard option turned for turned f	apturing from eth0 (Wireshark 1.10.6 (v1.10.6 from t i i i i i i i i i i i i i i i i i i
All the Auto capture keyboard option turned on. This will cause the Virtual Machine to 40, 7258 PM C control of the Auto Capture Keyboard option turned on the Auto Search your computer and online sources _=127 ttl=64 time=1.01 ms 64 bytes from 172.16.2.5: icmp_seq=128 ttl=64 time=0.756 ms 64 bytes from 172.16.2.5: icmp_seq=129 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.05 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.897 ms	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from t i i i i i i i i i i i i i i i i i i
the Auto capture keyboard option turned on. This will cause the Virtual Machine to the Auto capture keyboard option turned for this will cause the Virtual Machine to Control of the Automation Virtual Boor The Automation Search your computer and online sources 1=127 ttl=64 time=1.01 ms 64 bytes from 172.16.2.5: icmp_seq=128 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.05 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.05 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.887 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.887 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.887 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.897 ms 85 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from t i i i i i i i 2:14 AN File Edit View Go Capture Analyze Statistics Telephony Tools Internals i i i i i i i i i i i i i i i i i i i
All the Auto capture keyboard option turned on. This will cause the Virtual Machine to 40, 7258 PM C control of the Machine Sources 1 = 127 ttl=64 time=1.01 ms 64 bytes from 172.16.2.5: icmp_seq=128 ttl=64 time=0.756 ms 64 bytes from 172.16.2.5: icmp_seq=120 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.05 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.05 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.897 ms	apturing from eth0 (Wireshark 1.10.6 (v1.10.6 from t i i w i) 12:14 AM File Edit View Go Capture Analyze Statistics Telephony Tools Internals © O I I I I I I I I I I I I I I I I I I
A bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.98 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.05 ms 64 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=1.05 ms 64 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.06 ms 64 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.16 ms	apturing from eth0 (Wireshark 1.10.6 (v1.10.6 from t i i i i i i i i i i i i i i i i i i
A the Auto capture keyboard option turned on. This will cause the Virtual Machine to the Auto capture keyboard option turned on. This will cause the Virtual Machine to the Control of the Automatic terms and the Automatic	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1 Image: Second
A the Auto capture keyboard option turned on. This will cause the Virtual Machine to Search your computer and online sources =127 ttl=64 time=0. 756 ms 64 bytes from 172.16.2.5: tcmp_seq=128 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: tcmp_seq=130 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: tcmp_seq=131 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: tcmp_seq=131 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: tcmp_seq=131 ttl=64 time=0.813 ms 64 bytes from 172.16.2.5: tcmp_seq=135 ttl=64 time=0.613 ms 64 bytes from 172.16.2.5: tcmp_seq=135 ttl=64 time=0.613 ms 64 bytes from 172.16.2.5: tcmp_seq=135 ttl=64 time=0.748 ms 64 bytes from 172.16.2.5: tcmp_seq=138 ttl=64 time=0.748 ms	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from t] Image: Statistics Telephony Tools Internals File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Statistics Telephony Tool
the Auto capture keyboard option turned on. This will cause the Vital Machine to 40, 758 mg of the automation Virtual Boor The William Machine to 40, 758 mg of the automation Virtual Boor The Machine to 40, 758 mg of the automation Virtual Boor The Machine to 40, 758 mg of the automation Virtual Boor The Machine to 40, 758 mg of the automation Virtual Boor The Machine to 40, 758 mg of the automation Virtual Boor The Machine to 40, 758 mg of the automation Virtual Boor The Machine to 40, 758 mg of the automation Virtual Boor The Machine to 40, 758 mg of the automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the Automation Virtual Boor The Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation Virtual Machine to 40, 758 mg of the Automation	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from t] Image: Statistics Telephony Tools Internals File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Statistics Telephony Tool
A the set of the set o	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from t] Image: Statistics Telephony Tools Internals File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Superstand Statistics Telephony Tools Internals Image: Superstand Statistics Telephony Tools Internals Image: Superstand Statistics Telephony Tools Internals Image: Superstand Statistics Time Image: Superstand Statistics Statistics Image: Superstand Statistics Time Image: Superstand Statistics Image: Superstand Statistics Image: Superstand Statistics Time Image: Superstand Statistics Image: Superstand Statistics Image: Superstand Statistic
We the Auto capture keyboard option turned on. This will cause the Virtual Machine to Search your computer and online sources =127 ttl=64 time=0. The sources	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1 a m w)) 12:14 AM File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Second Statistics Telephony Tools Internals Image: Second Statistics Telephony Tools Internals Image: Second Statistics Telephony Tools Internals Image: Second Statistics Time Image: Second Statistics Second Statistics Image: Second Statistics Time Image: Second Statistics Image: Second Statistics Image: Second Statistics <t< td=""></t<>
Auto capture keyboard option turned on. This will cause the Virtual Machine to 400 758 per Search your computer and online sources =127 ttl=64 time=0.101 ms 64 bytes from 172.16.2.5: icmp_seq=128 ttl=64 time=0.756 ms 64 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.98 ms 64 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.831 ms 64 bytes from 172.16.2.5: icmp_seq=135 ttl=64 time=0.683 ms 64 bytes from 172.16.2.5: icmp_seq=136 ttl=64 time=0.748 ms 64 bytes from 172.16.2.5: icmp_seq=139 ttl=64 time=0.779 ms 64 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=0.779 ms 64 bytes from 172.16.2.5: icmp_seq=140 ttl=64 time=0.782 ms 64 bytes from 172.16.2.5: icmp_seq=140 ttl=64 time=0.894 ms	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from t] Image: Statistics Telephony Tools Internals File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals<
Auto capture keyboard option turned on. This will cause the Virtual Machine to Search your computer and online sources = 127 ttl=64 time=0. 756 ms 64 bytes from 172.16.2.5: tcmp_seq=128 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: tcmp_seq=130 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: tcmp_seq=131 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: tcmp_seq=131 ttl=64 time=1.08 ms 64 bytes from 172.16.2.5: tcmp_seq=131 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: tcmp_seq=133 ttl=64 time=0.183 ms 64 bytes from 172.16.2.5: tcmp_seq=135 ttl=64 time=0.613 ms 64 bytes from 172.16.2.5: tcmp_seq=135 ttl=64 time=0.613 ms 64 bytes from 172.16.2.5: tcmp_seq=135 ttl=64 time=0.613 ms 64 bytes from 172.16.2.5: tcmp_seq=135 ttl=64 time=0.778 ms 64 bytes from 172.16.2.5: tcmp_seq=138 ttl=64 time=0.779 ms 64 bytes from 172.16.2.5: tcmp_seq=138 ttl=64 time=0.779 ms 64 bytes from 172.16.2.5: tcmp_seq=148 ttl=64 time=0.779 ms 64 bytes from 172.16.2.5: tcmp_seq=148 ttl=64 time=0.779 ms 64 bytes from 172.16.2.5: tcmp_seq=148 ttl=64 time=0.894 ms	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from t] Image: Statistics Telephony Tools Internals File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals<
The Auto capture keyboard option turned on. This will cause the Virtual Machine to 20 758 as a constrained of the Auto capture keyboard option turned on. This will cause the Virtual Machine to 20 757 ms of a bytes from 172.16.2.5: icmp_seq=128 ttl=64 time=0.757 ms of a bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.08 ms of a bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.08 ms of a bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.897 ms of a bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.897 ms of a bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.897 ms of a bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.813 ms of a bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.813 ms of a bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.939 ms of a bytes from 172.16.2.5: icmp_seq=143 ttl=64 time=0.797 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.894 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.894 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.635 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.635 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.894 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.635 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.635 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.100 ms of a bytes from 172.16.2.5: icmp_seq=141 ttl=64	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1 a m w) 12:14 AM File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Second Statistics Telephony Tools Internals Image:
A bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.683 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.757 ms 64 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.897 ms 64 bytes from 172.16.2.5: icmp_seq=133 ttl=64 time=0.683 ms 64 bytes from 172.16.2.5: icmp_seq=134 ttl=64 time=0.683 ms 64 bytes from 172.16.2.5: icmp_seq=135 ttl=64 time=0.779 ms 64 bytes from 172.16.2.5: icmp_seq=138 ttl=64 time=0.788 ms 64 bytes from 172.16.2.5: icmp_seq=138 ttl=64 time=0.778 ms 64 bytes from 172.16.2.5: icmp_seq=134 ttl=64 time=0.788 ms 64 bytes from 172.16.2.5: icmp_seq=134 ttl=64 time=0.788 ms 64 bytes from 172.16.2.5: icmp_seq=148 ttl=64 time=0.788 ms 64 bytes from 172.16.2.5: icmp_seq=144 ttl=64 time=0.788 ms 64 bytes from 172.16.2.5: icmp_seq=145 ttl=64 time=0.788 ms 64 bytes from 172.16.2.5: icmp_seq=146 ttl=64 time=0.788 ms 64 byte	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1 a m w)) 12:14 AM File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Second Statisting Telephony Tools Internals
A the Auto capture keyboard option turned on. This will cause the Vitual Machine to 40. 7258 and 72588 and 725888 and 72588 and 725888 and	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1] Image: Statistics Telephony Tools Internals File Edit View Go Capture Analyze Statistics Telephony Tools Internals File Edit View Go Capture Analyze Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics Telephony Tools Internals Image: Statistics
The beta duto capture keyboard option turned on. This will cause the Vital Machine to the control of the second se	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1 Image: Solution of the soluti
The Auto capture keyboard option turned on. This will cause the Virtual Machine to 2007 258 as a constrained on the sources 1=127 ttl=64 time=1.01 ms of 4 bytes from 172.16.2.5: icmp_seq=128 ttl=64 time=0.757 ms of 4 bytes from 172.16.2.5: icmp_seq=130 ttl=64 time=1.08 ms of 4 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=1.08 ms of 4 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.08 ms of 4 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.08 ms of 4 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.08 ms of 4 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=1.08 ms of 4 bytes from 172.16.2.5: icmp_seq=132 ttl=64 time=0.897 ms of 4 bytes from 172.16.2.5: icmp_seq=135 ttl=64 time=0.813 ms of 4 bytes from 172.16.2.5: icmp_seq=137 ttl=64 time=0.798 ms of 4 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.798 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.788 ms of 4 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.788 ms of 4 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.788 ms of 4 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.788 ms of 4 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.788 ms of 4 bytes from 172.16.2.5: icmp_seq=131 ttl=64 time=0.788 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.788 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.884 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.887 ms of 4 bytes from 172.16.2.5: icmp_seq=141 ttl=64 time=0.887 ms of 4 bytes from 172.16.2.5: icmp_seq=141 t	apturing from eth0 [Wireshark 1.10.6 (v1.10.6 from 1 Image: Solution of the soluti

Figure 4.4: TCPDUMP and Wireshark capture at VBOX3

5. TCPDUMP and wireshark capture at VBOX4

- VBOX1 is Pinging to VBOX3.
- I run below command on VBOX4 to capture traffic via TCPDUMP tcpdump –i eth0 icmp
- VBOX4 is behaving as a Management Interface

	Vbox1 [Running]		Vbox4 (Running	1
You have the Auto capture keyboard	arch Terminal Help	(intual Machine to	rminal	tu En 📧 ◄)) 10:36 PM 🔱
root@arju	n-VirtualBox: /home/arjun		🖳 🔞 🖨 🗊 root@arjun-VirtualBox: /home/a	ariun
64 bytes from 172	2.16.2.5: icmp_seq=359	ttl=64 time=0.765 ms	22:36:15.394452 IP 172.16.2.5 > 1	
	2.16.2.5: icmp_seq=360		2487, seq 374, length 64	
	2.16.2.5: icmp_seq=361 2.16.2.5: icmp_seq=362		22:36:16.394877 IP 10.1.200.4 > 1	72.16.2.5: ICMP echo request,
	2.16.2.5: icmp_seq=363		id 2487, seq 375, length 64 22:36:16.395179 IP 172.16.2.5 > 1	a 1 200 4: TCMP acho rooly id
	2.16.2.5: icmp_seq=364		2487, seg 375, length 64	0.1.200.4. ICHP echo repty, to
	2.16.2.5: icmp_seq=365		22:36:17.395196 IP 10.1.200.4 > 1	72.16.2.5: ICMP echo request,
	2.16.2.5: icmp_seq=366 2.16.2.5: icmp_seq=367		🗾 id 2487, seq 376, length 64	
	2.16.2.5: icmp_seq=368		22:36:17.395604 IP 172.16.2.5 > 1 2487, seq 376, length 64	0.1.200.4: ICMP echo reply, id
64 bytes from 172	2.16.2.5: icmp_seq=369	ttl=64 time=0.668 ms	22:36:18.396406 IP 10.1.200.4 > 1	72.16.2.5: ICMP echo request.
	2.16.2.5: icmp_seq=370		id 2487, seq 377, length 64	
	2.16.2.5: icmp_seq=371 2.16.2.5: icmp_seq=372		22:36:18.396776 IP 172.16.2.5 > 1	0.1.200.4: ICMP echo reply, id
	2.16.2.5: icmp_seq=373		2487, seq 377, length 64 22:36:19.395346 IP 10.1.200.4 > 1	72 16 2 5; TCMP acho coquest
	2.16.2.5: icmp_seq=374		id 2487, seq 378, length 64	rz.io.z.s. ichr echo request,
	2.16.2.5: icmp_seq=375		22:36:19.395997 IP 172.16.2.5 > 1	0.1.200.4: ICMP echo reply, id
	2.16.2.5: icmp_seq=376 2.16.2.5: icmp_seq=377		2487, seq 378, length 64	
	2.16.2.5: icmp_seq=378		22:36:20.394420 IP 10.1.200.4 > 1 id 2487, seg 379, length 64	72.16.2.5: ICMP echo request,
	2.16.2.5: icmp_seq=379		22:36:20.394790 IP 172.16.2.5 > 1	0.1.200.4: ICMP echo reply. id
64 bytes from 172	2.16.2.5: icmp_seq=380	ttl=64 time=0.804 ms	2487, seq 379, length 64	
			a	
	S 6) 🗐 🥟 📖 💻 🔐 🔘 🔇 🖲 Left ೫		🔉 🗇 🗐 🤌 📰 🗮 🔐 🔯 🖲 Left #
	Vbox1 [Running]		Vbox4 [Running]	
Terminal		tr En (*) () 8:01 PM	Vbox4 [Running]	1 En III (10:35 PM 化
Terminal You have the Auto capture keyboard	option turned on. This will cause the Vi	irtual Machine to		↓ En 画 40)10:35 PM 袋
You have the Auto capture keyboard	option turned on. This will cause the Vi	irtual Machine to	■ File Edit View Go Capture Analyze Statis	
You have the Auto capture keyboard		ttl=64 time=0.924 ms		
Vou have the Auto capture keyboard You have the Auto capture keyboard Search your comput 64 bytes from 172 64 bytes from 172	option turned on. This will cause the Vi n-Victual Box (home failun ter and online sources ==298 2.16.2.5: tcmp_seq=299 2.16.2.5: tcmp_seq=300	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=1.22 ms	File Edit View Go Capture Analyze Statis	
Vou have the Auto capture keyboard read and the Auto capture keyboard Search your compute 64 bytes from 172 64 bytes from 172 64 bytes from 172	cotion turned on. This will cause the Vi a Vintual East Thome A durn ter and online sources 1=298 2.16.2.5: tcmp_seq=299 2.16.2.5: tcmp_seq=300 2.16.2.5: tcmp_seq=301	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=1.22 ms ttl=64 time=0.831 ms	File Edit View Go Capture Analyze Statis	tics Telephony Tools Internals Help
You have the Auto capture keyboard root madue Search your comput 64 bytes from 172 64 bytes from 172 64 bytes from 172 64 bytes from 172	option turned on. This will cause the Vi n-Victual Box (home failun ter and online sources ==298 2.16.2.5: tcmp_seq=299 2.16.2.5: tcmp_seq=300	11 CA CONTRACTOR 10 CONTRACTOR	File Edit View Go Capture Analyze Statis	tics Telephony Tools Internals Help C Q S F F F F F F F F F F F F F F F F F F
You have the Auto capture keyboard Control of the Auto capture keyboard Search your comput 64 bytes from 172 64 bytes from 172 65 bytes from 172 66 bytes from 172 66 bytes from 172 67 bytes from 172 68 bytes from	cption turned on. This will cause the Vi review of the sources 1=298 2.16.2.5: tcmp_seq=299 2.16.2.5: tcmp_seq=300 2.16.2.5: tcmp_seq=301 2.16.2.5: tcmp_seq=301 2.16.2.5: tcmp_seq=303 2.16.2.5: tcmp_seq=304	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=1.22 ms ttl=64 time=0.831 ms ttl=64 time=0.847 ms ttl=64 time=0.997 ms ttl=64 time=0.687 ms	File Edit View Go Capture Analyze Statis Image: Statistic Statistin Statisti Statist Statistic Statistic Statistic Statistic Statis	tics Telephony Tools Internals Help C Q S S S S S S S S S S S S S S S S S S
You have the Auto capture keyboard recordination Search your comput 64 bytes from 177 64 bytes from 177	cotion turned on. This will cause the Vi a Virtual Box: /home & fun ter and online sources _=298 2.16.2.5: icmp_seq=309 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.847 ms ttl=64 time=0.987 ms ttl=64 time=0.687 ms ttl=64 time=0.785 ms	File Edit View Go Capture Analyze Statis Image: Statis Image: Statis Image: Statis <thimage: statis<="" th=""> Ima</thimage:>	tics Telephony Tools Internals Help C Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q Q
You have the Auto capture keyboard root madue Search your comput 64 bytes from 172 64 bytes from 172	option turned on. This will cause the VI a Virtual Box: /home / argun ter and online sources298 2.16.2.5: icmp_seq=309 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=306	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.847 ms ttl=64 time=0.887 ms ttl=64 time=0.687 ms ttl=64 time=0.785 ms ttl=64 time=0.785 ms ttl=64 time=0.610 ms	File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis Filter: Image: Capture Analyze S	tics Telephony Tools Internals Help C Q S S S S S S S S S S S S S S S S S S
You have the Auto capture keyboard Search your compute 64 bytes from 172 64 bytes from 172	cotion turned on. This will cause the Vi a Virtual Box: /home & fun ter and online sources _=298 2.16.2.5: icmp_seq=309 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.22 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.785 ms ttl=64 time=0.610 ms ttl=64 time=0.610 ms	File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis Filter: Image: Capture Analyze Statis Filter: image: Capture Analyze Statis Filter: image: Capture Analyze Statis No. Time Source De 100 27.007631006 172.16.2.5 10 101 28.00732006 10.1.200.4 17 103 29.009222006 10.1.200.4 17 104 29.009526006 172.16.2.5 10	tics Telephony Tools Internals Help C Q Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 1.200.4 ICMP 98 Echo 1.200.4 ICMP 98 Echo
You have the Auto capture keyboard record and the Search your comput 64 bytes from 177 64 bytes from 177	cption turned on. This will cause the Vi revint unit flow: Thome & rjun ter and online sources _=298 2.16.2.5: tcmp_seq=299 2.16.2.5: tcmp_seq=300 2.16.2.5: tcmp_seq=301 2.16.2.5: tcmp_seq=303 2.16.2.5: tcmp_seq=304 2.16.2.5: tcmp_seq=304 2.16.2.5: tcmp_seq=306 2.16.2.5: tcmp_seq=306 2.16.2.5: tcmp_seq=307	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.847 ms ttl=64 time=0.687 ms ttl=64 time=0.610 ms ttl=64 time=0.610 ms ttl=64 time=0.909 ms ttl=64 time=0.877 ms	File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis Filter: Image: Capture Analyze Statis Filter: image: Capture Analyze Statis Filter: image: Capture Analyze Statis No. Time Source De 100 27.007631006 172.16.2.5 10 101 28.00732006 10.1.200.4 17 103 29.009222006 10.1.200.4 17 104 29.009526006 172.16.2.5 10	tics Telephony Tools Internals Help C Q A A A A A A A A A A A A A A A A A A
You have the Auto capture keyboard read manual Search your comput 64 bytes from 172 64 bytes from 172	cption turned on. This will cause the Vi revirtual flax: Thome S right ter and online sources _=298 2.16.2.5: 1cmp_seq=299 2.16.2.5: 1cmp_seq=300 2.16.2.5: 1cmp_seq=301 2.16.2.5: 1cmp_seq=303 2.16.2.5: 1cmp_seq=304 2.16.2.5: 1cmp_seq=304 2.16.2.5: 1cmp_seq=306 2.16.2.5: 1cmp_seq=307 2.16.2.5: 1cmp_seq=307 2.16.2.5: 1cmp_seq=309 2.16.2.5: 1cmp_seq=309 2.16.2.5: 1cmp_seq=309	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.22 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.997 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.010 ms ttl=64 time=0.909 ms ttl=64 time=0.877 ms ttl=64 time=0.877 ms ttl=64 time=0.877 ms ttl=64 time=0.718 ms	File Edit View Go Capture Analyze Statis Image: Statis	tics Telephony Tools Internals Help C Q Q Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo
Terminal You have the Auto capture keyboard Search your compute 64 bytes from 172	cption turned on. This will cause the VI nevintual floar. Thom to Arjun ter and online sources _=298 2.16.2.5: icmp_seq=209 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=307 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.610 ms ttl=64 time=0.909 ms ttl=64 time=0.909 ms ttl=64 time=0.977 ms ttl=64 time=0.937 ms	File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis Filter: icmp No. Time Source De Io0 27.007631006 172.16.2.5 10 128.007832006 10.1.200.4 17 Io2 28.008577006 172.16.2.5 10 1329.009522006 10.1.200.4 17 Io3 29.009522006 10.1.200.4 17 104 29.009526000 172.16.2.5 10 Frame 1: 98 bytes on wire (784 bits), Ethernet II, Src: CadmusCo_31:e1:5f (0)	tics Telephony Tools Internals Help C Q Q Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo
Terminal You have the Auto capture keyboard Coordination Search your comput 64 bytes from 172 6	cotion turned on. This will cause the Vi a Virtual Box: /home & rjun ter and online sources _=298 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=307 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=309 2.16.2.5: icmp_seq=309 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=3112 2.16.2.5: icmp_seq=312	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.610 ms ttl=64 time=0.610 ms ttl=64 time=0.979 ms ttl=64 time=0.977 ms ttl=64 time=0.977 ms ttl=64 time=0.977 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms	File Edit View Go Capture Analyze Statis File Edit View Go Capture Analyze Statis File Capture Analyze Statis Filter: Ime Source De Filter: Ime Source De 100 27.067631006 172.16.2.5 10 101 28.007832006 10.1.200.4 17 102 28.008577006 172.16.2.5 10 103 29.009526006 172.16.2.5 10 103 29.009526006 172.16.2.5 10 103 30.008023006 10.1.200.4 17 Image: Frame 1: 98 bytes on wire (784 bits), Frame 1: 98 bytes on wire (784 bits), Internet Protocol Version 4, Src: 10. Src: 10. 10 10.15 floater	tics Telephony Tools Internals Help C Q Q Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo
Terminal You have the Auto capture keyboard reor madue Get bytes 64 bytes 64 <t< td=""><td>cption turned on. This will cause the VI nevintual floar. Thom to Arjun ter and online sources _=298 2.16.2.5: icmp_seq=209 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=307 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311</td><td>ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.897 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.718 ms ttl=64 time=0.971 ms ttl=64 time=0.971 ms ttl=64 time=0.973 ms ttl=64 time=0.973 ms ttl=64 time=0.973 ms ttl=64 time=0.973 ms</td><td>File Edit View Go Capture Analyze Statis Image: Statis</td><td>tics Telephony Tools Internals Help C Q Q Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo</td></t<>	cption turned on. This will cause the VI nevintual floar. Thom to Arjun ter and online sources _=298 2.16.2.5: icmp_seq=209 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=307 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.897 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.718 ms ttl=64 time=0.971 ms ttl=64 time=0.971 ms ttl=64 time=0.973 ms ttl=64 time=0.973 ms ttl=64 time=0.973 ms ttl=64 time=0.973 ms	File Edit View Go Capture Analyze Statis Image: Statis	tics Telephony Tools Internals Help C Q Q Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo
Terminal You have the Auto capture keyboard Coordination Search your comput 64 bytes from 172 64 bytes from 172 <td>cotion turned on. This will cause the Vi a Virtual Box: /home & fun ter and online sources _=298 2.16.2.5: icmp_seq=209 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=306 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=313 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=315 2.</td> <td>ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.837 ms ttl=64 time=0.687 ms ttl=64 time=0.610 ms ttl=64 time=0.610 ms ttl=64 time=0.999 ms ttl=64 time=0.917 ms ttl=64 time=0.718 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=1.23 ms ttl=64 time=1.32 ms ttl=64 time=0.378 ms</td> <td>File Edit View Go Capture Analyze Statis Image: Statistic Statistis Statistis Statiste Statistic Statistic Statistic Statistic Stat</td> <td>tics Telephony Tools Internals Help C Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo 1.200.4 (10.1.200.4), Dst: 172.16</td>	cotion turned on. This will cause the Vi a Virtual Box: /home & fun ter and online sources _=298 2.16.2.5: icmp_seq=209 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=306 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=313 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=315 2.	ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.837 ms ttl=64 time=0.687 ms ttl=64 time=0.610 ms ttl=64 time=0.610 ms ttl=64 time=0.999 ms ttl=64 time=0.917 ms ttl=64 time=0.718 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=1.23 ms ttl=64 time=1.32 ms ttl=64 time=0.378 ms	File Edit View Go Capture Analyze Statis Image: Statistic Statistis Statistis Statiste Statistic Statistic Statistic Statistic Stat	tics Telephony Tools Internals Help C Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo 1.200.4 (10.1.200.4), Dst: 172.16
Terminal You have the Auto capture keyboard root madue Get bytes Get bytes<	cption turned on. This will cause the Vi review of the comparent of the co	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.997 ms ttl=64 time=0.987 ms ttl=64 time=0.687 ms ttl=64 time=0.089 ms ttl=64 time=0.910 ms ttl=64 time=0.918 ms ttl=64 time=0.946 ms ttl=64 time=1.32 ms ttl=64 time=1.32 ms ttl=64 time=0.788 ms ttl=64 time=0.788 ms ttl=64 time=0.788 ms	File Edit View Go Capture Analyze Statis Image: Statistic Statistis Statiste Statiste Statistic Statistic Statistic Statistic Stati	tics Telephony Tools Internals Help C Q Q A stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo 1.200.4 (10.1.200.4), Dst: 172.16 1.5f 08 00 45 00
Terminal You have the Auto capture keyboard Search your compute 64 bytes from 177	cption turned on. This will cause the Vi nevintual flow: Thome Argun ter and online sources _=298 2.16.2.5: icmp_seq=209 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=303 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=313 2.16.2.5: icmp_seq=314 2.16.2.5: icmp_seq=314 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=314 2.16.2.5: icmp_seq=315	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.2831 ms ttl=64 time=0.831 ms ttl=64 time=0.847 ms ttl=64 time=0.997 ms ttl=64 time=0.687 ms ttl=64 time=0.610 ms ttl=64 time=0.909 ms ttl=64 time=0.918 ms ttl=64 time=0.918 ms ttl=64 time=0.937 ms ttl=64 time=0.938 ms ttl=64 time=1.32 ms ttl=64 time=0.788 ms ttl=64 time=0.788 ms ttl=64 time=0.788 ms	File Edit View Go Capture Analyze Statis Image: Statistic State Image: State Ima	tics Telephony Tools Internals Help C Q Q Q stinatior Protocol Length Infc 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 1.200.4 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 2.16.2.5 ICMP 98 Echo 98 bytes captured (784 bits) on 98:00:27:31:e1:5f), Dst: CadmusCo 1.200.4 (10.1.200.4), Dst: 172.16 1.5f 08 00 45 00''1. a 01 c8 04 ac 10'1.
Vau have the Auto capture keyboard Yau have the Auto capture keyboard Capture the Auto capture the Auto captur	cption turned on. This will cause the Vi review of the comparent of the co	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.837 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.999 ms ttl=64 time=0.999 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.938 ms ttl=64 time=0.788 ms ttl=64 time=0.788 ms ttl=64 time=0.760 ms	File Edit View Go Capture Analyze Statis Image: Statistic Statistis Statiste Statiste Statistic Statistic Statistic Statistic Stati	tics Telephony Tools Internals Help C Q Image: Constraint of the second sec
Search your compute 64 bytes from 177	cption turned on. This will cause the VI a VI than Hone: A run ter and online sources _=298 2.16.2.5: icmp_seq=299 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=312 2.16.2.5: icmp_seq=313 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=316	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.837 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.999 ms ttl=64 time=0.999 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.938 ms ttl=64 time=0.788 ms ttl=64 time=0.788 ms ttl=64 time=0.760 ms	File Edit View Go Capture Analyze Statis Io 2 28.00857000 172.16.2.5 Io 2 28.00857000 172.16.2.5 Io 2 28.00852000 172.16.2.5 Forme 1: 98 bytes on wire (784 bits), Fthernet II, Src: CadmusCo 31:e1:5f (Finternet Protocol Version 4, Src: 10. Internet Control Message Protocol 00010 00 54 95 at 40 00 41 01 23 ea 00 00020 02 05 08 00 4d c9 09 57 01 21 6d	tics Telephony Tools Internals Help C Q Image: Constraint of the second sec
You have the Auto capture keyboard root made 64 bytes from 172 64 bytes from 172	cption turned on. This will cause the VI a Virtual Box: Thome Argun ter and online sources _=298 2.16.2.5: icmp_seq=299 2.16.2.5: icmp_seq=300 2.16.2.5: icmp_seq=301 2.16.2.5: icmp_seq=302 2.16.2.5: icmp_seq=304 2.16.2.5: icmp_seq=305 2.16.2.5: icmp_seq=306 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=308 2.16.2.5: icmp_seq=310 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=311 2.16.2.5: icmp_seq=313 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=314 2.16.2.5: icmp_seq=315 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=316 2.16.2.5: icmp_seq=318 2.16.2.5: icmp_seq=318 2.16.2.5: icmp_seq=319	ttl=64 time=0.924 ms ttl=64 time=0.924 ms ttl=64 time=0.773 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.831 ms ttl=64 time=0.837 ms ttl=64 time=0.687 ms ttl=64 time=0.687 ms ttl=64 time=0.999 ms ttl=64 time=0.999 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.937 ms ttl=64 time=0.938 ms ttl=64 time=0.788 ms ttl=64 time=0.788 ms ttl=64 time=0.760 ms	File Edit View Go Capture Analyze Statis Image: Statistic Statistis Statisting Statiste Statistic Statistic Statistic Statistic Sta	tics Telephony Tools Internals Help C Q Image: Constraint of the second sec

Figure 4.5: TCPDUMP and Wireshark capture at VBOX4

6. GEOIP Reports Generation

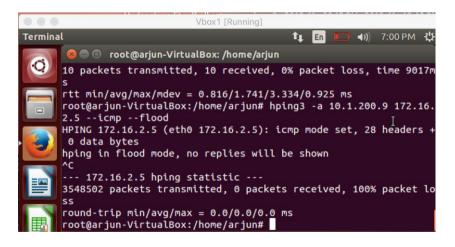
I uploaded GEOIP database on wireshark and surf the webpage. It is showing location of city, country, latitude, and longitude with all listed public IP address.

		Et	hernet · 10	IPv4 · 21	IPv6 · 8	TCP · 22	UDP · 37						*
ddress 🔺 Packets	Bytes		ackets $A \rightarrow B$		s A → B	Packets B → A		ytes B → A		Country	AS Number		
4.244.4.23		7197		5	4330		3			Canada	AS6327 Shav	and	
4.244.4.56	120	86 k		71	77 k		49			Canada	AS6327 Shav	- 17	
4.244.4.59	2	120		1	66		1			Canada	AS6327 Shav		
54.69.181.174	2	163		1	97		1			United States			. ~ /
04.25.31.35	25	5932		10	4695		15			United States			1 3
64.100.78.103	1.20	1090		5	370		10			India	AS4758 Nati		2
72.217.4.97		4402		3	2853		3			United States			
72.217.4.238	1000	4402		3	2853		3			United States			
72.217.6.3	-	4402		3	2853		3			United States			
72.217.6.110	14	6873		7	2688		7		4185	United States	AS15169 God	3	
73.194.74.188	1	54		0	0		1			United States	AS15169 Goc	N	
92.168.0.1		1295		6	834		6			_	-	- That	
92.168.0.11	258	143 k		125	31 k		133		111 k				164.100.78.10
209.85.200.189	2	137		1	72		1			United States			City: Bangalore,
216.58.192.163		4402		3	2853		3			United States			Country: India
216.58.192.174		4522		4	2919		4			United States			Packets: 15
216.58.192.238		4328		3	2853		2			United States			Bytes: 1090
216.58.216.69	2	120		1	66		1			United States			AS Number: -
216.58.216.78		6189		6	3617		5			United States	AS15169 Goc		
224.0.0.251	3	246		0	0		3		246		-		
239.255.255.250	4	864		0	0		4		864	-	-		
							-				-		

Figure 4.6: GEOIP Reports Generation

7. Basic Reports Generation

I used Hping3 for Generation of flood traffic from VBOX1 to VBOX3. Wireshark running within VBOX4 is capturing traffic.



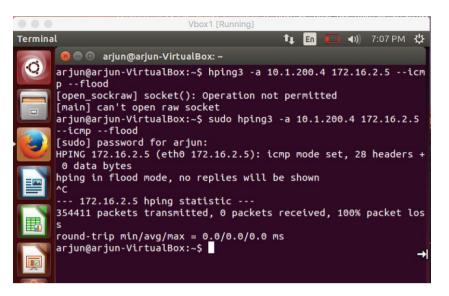


Figure 4.7.1: Hping3 for Generation of flood traffic

Top Talkers (Listed by Size of Bytes)

					Vbox4 [F	Running]	
Vireshark File Edit View Go E C A Filter: No. Time 990827 60.6415	Ethernet: 2	points: eth0 Fibre Chann	el FDDI	IPv4: 3 IPv6 I	IPX JXTA I	NCP RSVP Si 14 Endpoints	CTP TCP Tok
990828 60.6411 990829 60.6411 990830 60.6411 990830 60.6421 990833 60.6421 990833 60.6421 990835 60.6421 990835 60.6421 990835 60.6421 990835 60.6421 990835 60.6421 990835 60.6421 910835 60.6421 91085 60.64210	Address 172.16.2.5 10.1.200.4 10.1.200.9	647 899	Bytes • 59 449 860 38 873 940 20 575 920	152 555	9 153 300	495 344	29 720 640 -
0000 08 00 27 0010 00 1c 11 0020 c8 04 00 0030 00 00 00	♥ Name res	Copy	Limit to dis	play filter			

Figure 4.7.2: Top Talkers

Packet counts by Protocols (As only Ping is used, it shows ICMP traffic)

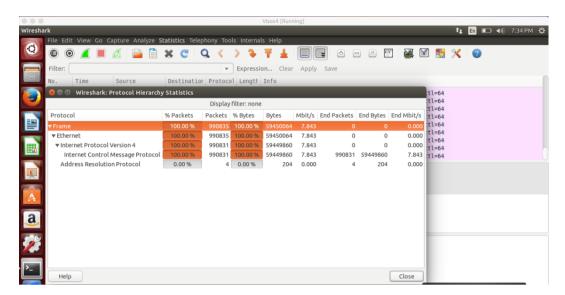


Figure 4.7.3: Packet Counts by Protocols

Packet Length Statistics

00		0		atistics Telep	2 (> 2	Ŧ			Ð		(1)
Filter:						Expressi	0.0	Clear	Apply	Save	_	_
	me	Sourc	e	Destinatior				cicui	OPPU	5046		
990828 60 990829 60 990830 60	.641974000 .641976000 .641977000 .641978000 .641978000	172.1 172.1 172.1	6.2.5 6.2.5 6.2.5	10.1.200.4 10.1.200.4 10.1.200.4 10.1.200.4 10.1.200.4	ICMP ICMP ICMP ICMP ICMP CMP	60 60	Echo Echo	(ping) (ping)	reply reply reply Packet Lo	engths Star		seq=2
Topic / Iter ▼ Packet Le			Rate (ms)	Percent	CMP CMP CMP	Filter:		Cance	l Cr	eate Stat	9,	seq=2 seq=2 seq=2
0-19	(0.000000	0.00%	aptured	(480 bi	ts) o	n inter	face 0			
20-39	C)	0.000000	0.00%						8:00:27:f	a:2a	:b4)
40-79	9	990835	16.339039	100.00%	2.10.2.	b), DSL:	10.1	.200.4	(10.1.20	10.4)		
80-159	c)	0.000000	0.00%								
160-319	C)	0.000000	0.00%								
320-639	c	8	0.000000	0.00%								
640-127			0.000000	0.00%								
1280-25			0.000000	0.00%	15 00			F				
2560-51			0.000000	0.00%	la 01							
5120-42	94967295 0)	0.000000	0.00%	10 00	i						

Figure 4.7.4: Packet Length Statistics

Packet Length Statistics by Protocol

	•	ا 🖌 🔇			×C	2 <	> 3	Ŧ	▲		Ð		1 ++
	Filter:					*	Expressi	on	Clear	Apply	Save		
2	No.	Time	Sourc	e	Destinatior	Protocol	Length	Info					
	990828 990829 990836	8 60.64197 9 60.64197 9 60.64197	4006 172.1 6006 172.1 7006 172.1 8006 172.1	6.2.5 6.2.5 6.2.5	10.1.200.4 10.1.200.4 10.1.200.4 10.1.200.4	ICMP ICMP ICMP ICMP ICMP CMP	60 60	Echo Echo Wire		reply id=0x2609, reply id=0x2609, Packet Lengths Sta			seq=2543
	Topic/	/ Item	Count	Rate (ms)	Percent	CMP CMP CMP	Filter:	icm	Cance		eate Stal) 9,] 9,	seq=267 seq=269 seq=272
	1280 2560	9 9 59 -319	0 0 0 0 0	0.000000 0.000000 16.338973 0.000000 0.000000 0.000000 0.000000 0.000000	0.00% 0.00% 100.00% 0.00% 0.00% 0.00% 0.00% 0.00% 0.00%	:a1:f0)	(480 bit , Dst: Ca 5), Dst: 	admus 10.1	Co_fa:2 .200.4	a:b4 (0)		fa:2a	:b4)

Figure 4.7.5: Packet Length Statistics by Protocol

CHAPTER 5

CONCLUSION

I modified Linux operating system to capture traffic passing through two of its interfaces. As per the results packet is just travelling on the wire without crossing any interfaces because hop count is not changing. Intermediate VBOX2 is not detectable because of these changes.

Packets are also transferred on management interface, where the IPS (wireshark/snort) solution will be built as the next stage of Project for future scope.

Website Link:

- 1. https://opensource.com/resources/what-is-linux
- 2. https://en.wikipedia.org/wiki/Ubuntu_(operating_system)
- 3. https://www.virtualbox.org/manual/ch06.html
- 4. https://www.virtualbox.org/manual/ch01.html#idm26
- 5. https://en.wikipedia.org/wiki/Intrusion_detection_system
- 6. https://en.wikipedia.org/wiki/Snort_(software)
- 7. https://en.wikipedia.org/wiki/Wireshark
- 8. https://www.digitalocean.com/community/tutorials/how-the-iptables-firewall-works
- 9. http://www.linuxtopia.org/Linux_Firewall_iptables/x4799.html
- 10. https://www.tummy.com/articles/networking-basics-how-arp-works/
- 11. https://help.ubuntu.com/community/IptablesHowTo
- 12. https://help.ubuntu.com/community/VirtualBox/Networking
- 13. http://blogging.dragon.org.uk/setup-a-test-networking-lab-with-virtualbox/
- 14. http://myogyisg.blogspot.ca/2012/01/linux-iptables-routing-snatmasquerade.html
- 15. http://tlug.ss.narkive.com/mrfX145J/setting-up-virtual-box-to-snat-dnat
- 16. https://forums.virtualbox.org/viewtopic.php?f=7&t=37133
- 17. http://serverfault.com/questions/284056/simulated-nat-traversal-on-virtual-box
- 18. http://servertopic.com/topic/A9Rp-simulated-nat-traversal-on-virtual-box
- 19. http://unix.stackexchange.com/questions/74663/virtualbox-nat-host-onlyadapter
- 20. https://www.tolaris.com/2009/03/05/using-host-networking-and-nat-with-virtualbox/
- 21. http://linux-training.be/networking/ch13.html
- 22. https://gtalug.org/pipermail/legacy/2010-January/048633.html
- 23. https://community.oracle.com/docs/DOC-890092
- 24. http://www.howopensource.com/2011/06/how-to-use-virtualbox-in-terminalcommandline/

- 25. http://linuxpitstop.com/install-and-use-command-line-tool-vboxmanage-onubuntu-16-04/
- 26. https://www.unixmen.com/install-ubuntu-14-04-3-lts-virtualbox/
- 27. https://technology.amis.nl/2014/01/27/a-short-guide-to-networking-in-virtualbox-with-oracle-linux-inside/
- 28. https://openmaniak.com/tcpdump.php
- 29. http://networkengineering.stackexchange.com/questions/10530/ping-betweendifferent-subnet-across-a-link
- 30. http://archive.openflow.org/wk/index.php/OpenFlow_Tutorial
- 31. https://blog.wireshark.org/2010/02/running-wireshark-as-you/

Books:

- 32. Charles M. Kozierok, The TCP/IP Guide, Version 3.0, 2005
- 33. Laura chappell, Wireshark 101 Essential Skills for Network Analysis, 2013.

Video Link:

- 34. https://www.youtube.com/watch?v=WXhpSRaae7w
- 35. https://www.youtube.com/watch?v=1PsTYAd6MiI
- 36. https://www.youtube.com/watch?v=ZD0-LOCKpO4
- 37. https://www.youtube.com/watch?v=XKfhOQWrUVw
- 38. https://www.youtube.com/watch?v=ZtCWXdtIKE0
- 39. https://www.youtube.com/watch?v=Vf2S-XeZoEQ
- 40. https://www.youtube.com/watch?v=D08catMKcRg
- 41. https://www.youtube.com/results?search_query=wireshark+IO+graphs
- 42. https://www.youtube.com/watch?v=hrExIIJYJho