

# Objective

You will install and learn to use a packet capture and analysis tools.

Systems Administrators are often called upon to troubleshoot systems that usually rely on a network, but that network traffic is rarely observable at an application level. Wireshark and other tools like it allow us to see what is happening at a packet level (OSI layer 3/4) and frame level (OSI level 2). And the interface offers quite effective filters to reduce "noise", allowing a sysadmin to focus more clearly on the protocols and sequences being investigated.

This is a powerful tool. And as you have no doubt heard, with great power comes great responsibility. When sniffing the traffic on a network, you are likely to see at least some unencrypted traffic which may contain passwords or other privileged information. In a perfect world, such information would not be leaked by applications, but we all know that this world is not perfect. Never misuse the information that you see. Always protect the privacy of your peers and clients.

When using tools such as tcpdump or Wireshark, be mindful of what you do and for your own sake, document everything that you do. You never know when you will be required to produce that documentation for legal purposes.

系统管理员经常被要求对通常依赖于网络的系统进行故障排除，但在应用程序级别很少可以观察到网络流量。Wireshark和其他类似的工具允许我们查看数据包级别（OSI第3/4层）和帧级别（OSI第2层）发生的情况。该接口提供了相当有效的过滤器来减少“噪音”，允许系统管理员更清楚地关注正在调查的协议和序列。

这是一个强大的工具。正如你们毫无疑问听到的，强大的力量带来巨大的责任。当嗅探网络上的流量时，您可能会看到至少一些未加密的流量，其中可能包含密码或其他特权信息。在一个完美的世界里，这些信息不会被应用程序泄露，但我们都知道这个世界并不完美。不要误用你看到的信息。始终保护同事和客户的隐私。

当使用诸如tcpdump或Wireshark之类的工具时，请注意您所做的事情，并且为了您自己的利益，记录您所做的一切。您永远不知道出于法律目的何时需要出示该文件。

So be sensible and ethical, but particularly when using tcpdump or Wireshark.

1. **Set time zone from CLI (command-line interface)**

Check the current time on the *server*:

date

weird

You may find that the current time on the server is a UTC time. Display the time zone file:

more /etc/timezone



You may find that your time zone is Etc/UTC, which is a special area for the universal coordinated time (zone). The time zone is name using Area/Location in the IANA-timezones-database.

Find out the available time zone in Asia:

timedatectl list-timezones | grep Asia | more

按q退出

The closest time zone in the database to Nanjing is Asia/Shanghai. Use the following command to set the time zone:

sudo timedatectl set-timezone Asia/Shanghai

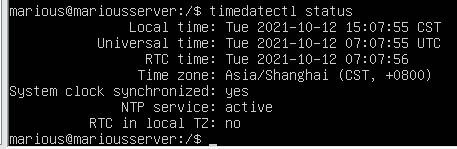
Display the time zone file and check the current time again.



The current time zone should be Asia/Shanghai and the time should be an AEST time now.

You can also use the timedatectl command to query the system clock and its settings:

timedatectl status



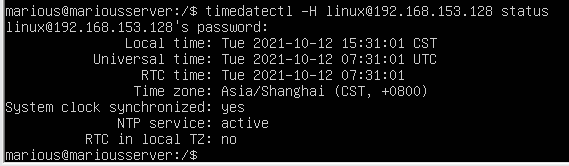
You can use the timedatectl command to query a remote system. Find out your *desktop* IP address (How?) and issue the following command to confirm the time zone of the desktop VM to have been set to Asia/Shanghai.

192.168.153.128

timedatectl -H abc123@*desktopIP* status

tips：需安装openssh-server，缺的依赖人家要安什么就安什么，然后开启22号端口

desktopIP前面要加desktop的用户名



Restart the cron to allow it to pick up the time zone change:

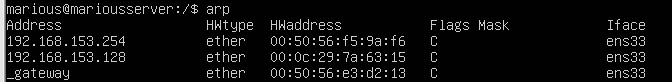
sudo service cron restart



1. **Capture packets using tcpdump from CLI**

First let's inspect the ARP cache using the following command on the *server*:

arp



Find out your desktop IP address and remove it from the ARP cache:

sudo arp -d *desktopIP*

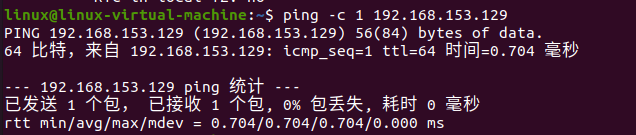
Capture 4 either ICMP or ARP packets using tcpdump command:

sudo tcpdump -c 4 "icmp or arp"



On the *desktop*, open a terminal program and issue the following command:

ping -c 1 *serverIP*



On the *server*, you can see ARP request/reply packets and ICMP request/reply packets, which is the protocol the

ping utility uses.



Record the server's MAC address from the packet captured. 00:50:56:e3:d2:13

1. **Packet capture and analysis with Wireshark**

Install Wireshark on the *desktop*

*sudo apt-get install wireshark*

Start the Ubuntu Software by clicking at the icon on the dock at the left of the screen. Search for wireshark.

Install Wireshark (with 5 stars) and accept all defaults. Start Wireshark from CLI

Now start up the Wireshark as a superuser. (Once a user has been authenticated, a time stamp is updated and the user may then use sudo without a password for a short period of time. The "&" at the end of this command is to push the process to the "background" of that terminal window. For your purposes, this just means that your terminal is usable for other things now while Wireshark is still running.)

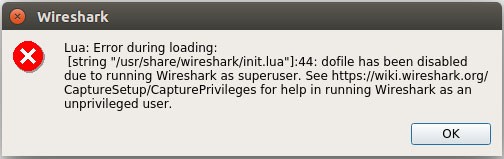
现在以超级用户身份启动Wireshark。（一旦用户通过身份验证，将更新时间戳，然后用户可以在短时间内不使用密码使用sudo。此命令末尾的“&amp;”将进程推到“后台”对于您的目的，这只是意味着您的终端可以在Wireshark仍在运行时用于其他用途。）

In the terminal, issue the following commands:

sudo ls

sudo wireshark &

The GUI should load up…欢迎使用wireshark



If you receive a message as shown,

You may press OK to ignore it or do the following to fix it.

sudo gedit /usr/share/wireshark/init.lua

Then make the following change and save.

"disable\_lua = false" to "disable\_lua = true"

Then select the Ethernet interface of the VM, likely to be enp0s3, by double-clicking to start capturing. Note the sections of the GUI:

* + Menu Bar
  + Main Toolbar
  + Filter Toolbar
  + Packet List pane, showing one line for every packet you capture
  + Packet Details pane, showing a decoded breakdown of the selected packet
  + Packet Bytes pane, showing the raw content of the packet
  + Status bar

These will make more sense once you have run a capture.

Capture packets

On the *server*, try this:

ping -c 2 192.168.153.128

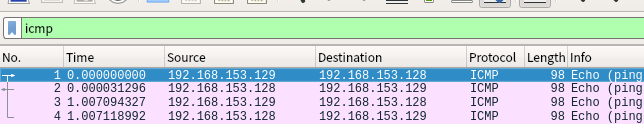
发俩包

(How to find out your desktop VM's IP?) ifconfig

On the *desktop*, point your browser to [www.baidu.com](http://www.baidu.com/) Then, stop the capture and save the capture to a file. Analyse packets

Now let's analyse the packet capture.

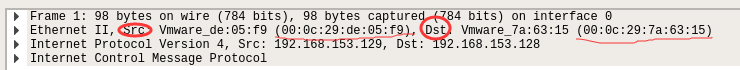
1. Filter the results down to just ICMP – in the filter toolbar, simply by typing icmp and <Enter>



Select one of the ping request packet (noting that it comes from your source IP address). Record the packet number (leftmost column). 选择一个ping请求包（注意它来自您的源IP地址(server）。记录数据包编号（最左边的列）。

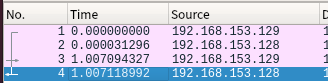
Now in the Packet Details pane, you may drill down into ever deeper levels via the triangles on the left. Find your source MAC address and the destination MAC address. (Note them down for your teacher)

现在在“数据包详细信息”窗格中，您可以通过左侧的三角形深入到更深的层次。查找源MAC地址和目标MAC地址。



Then select the corresponding ping reply packet (it should be next recorded packet to the request packet). Dig

in the Packet Details pane for the Internet Control Message Protocol and dig out the response time of that ping. (Note it down for your teacher). 然后选择相应的ping应答包（它应该是请求包的下一个记录包）。挖掘在Internet控制消息协议的数据包详细信息窗格中，找出该ping的响应时间。



1. Filter the results down to DNS (remove the previous keyword and type dns and <Enter> Select the DNS response packet.

Find out the IP address of the host [www.baidu.com](http://www.baidu.com/) from the answer. (Note it down for your teacher).



What are all of the protocols that Wireshark allows us to inspect?

From the menu bar: Analyze -> Enabled Protocols

(This is also the answer to ‘what protocol is XYZ that showed up in my capture?’) Analyse packets from a Wireshark Capture file

We are unable to cover very much in a lab. You are strongly recommended that you spend some time to learn to use

Wireshark effectively.

You can find more information at wiki.wireshark.org.

# Submission and mark

For full marks today, show your teacher

1. /etc/timezone file on the server;



1. the server's MAC address from the packet captured by tcpdump on the server;
2. MAC addresses of the source and destination, response time of ping from the packets with Wireshark;
3. IP address of [www.baidu.com](http://www.baidu.com/) from the packet with Wireshark;

6 marks for all 4 items above;

3 mark for any 2-3 items above; 0 mark for 1 or less items above.

You should be ready to answer any questions to demonstrate that all work is done by yourself otherwise you may receive 0 mark.