# 5CS031 Network Security

# Workshop 3: Password Retrieval

**Student Name:\_\_\_\_\_\_Loucas Xiourouppa\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Student Number:\_\_\_\_2007307\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**This is an assessed workshop. You will need to complete the workshop tasks, answer the questions and then submit the Word file, complete with your screenshots and answers, before the deadline posted on the workshops submission page, on Canvas.**

**The tools and techniques used in this workshop are purely for legitimate password retrieval, and it should be understood that the University accepts no responsibility for any person who uses them anything other than this. To do so may well be viewed as committing a serious offence.**

**Scenario**

In this workshop you will be creating several users on a Linux server, each with differing complexities of passwords. The encrypted passwords are stored in a file called shadow on the Linux server A copy of this file will be obtained and then a password retrieval tool will be applied to the Linux password file to reveal the passwords,

**Prepare the environment**

**It is recommended that you use a Windows VM to perform this exercise. There is a Security Windows 7 VM in the “resources” on Canvas that can be used for this exercise but any other available to you will be fine.**

1. Start VMware Player
2. Start the Virtual Machine called Security Windows 7.
3. You **will** need to download these tools into your **VMware Security Windows 7** virtual machine:
   1. **Winscp-5.11.3-Setup.exe** is a secure FTP client – this is needed to copy the password shadow file off the Linux server to Windows 7. You can find the file in the Resources on Canvas if you need it.
   2. **John the Ripper** - download it from the Canvas.

**VMware Linux Server**

1. You will need to setup and configure your own personalised Linux Server virtual machine for this exercise.
2. From the Resources in Canvas, download the file called “LinuxServer.zip”. Right-click on this file and extract the zip file into a folder, and then rename the folder to “LinuxServer1234567”. Change the numbers to your own student ID.
3. Change the Virtual machine name from “LinuxServer” to “LinuxServer1234567”. Use your own Student ID for the numbers.
4. Start the virtual machine and if you are prompted with the question “Did you move this virtual machine, or did you copy it?”, select **“I moved it”** and click OK.
5. The workstation's anti-virus program may popup and ask if you allow this program. You will have to click "Allow".

Click inside the VMware Linux Server window.

Login with

Username: root

Password: password

Enter the command below and press enter:

**ifconfig**

Copy down the value for the IP address (**inet**) for eth0 below:

192.168.92.137

**Part 1 – Cracking the passwords**

1. Create 3 different user accounts in the Linux Server and create a password for each user
2. Make sure that you create 2 accounts with simple English words passwords and 1 account with a more difficult password with numbers. **Do not use your actual student password**! Fill in the following table:

| Username | Password |
| --- | --- |
| loucas | 123 |
| alex | 123 |
| LXT | 123456 |

**Copy the shadow file to your Security Windows 7**

1. In the Security Windows 7, run **Winscp-5.11.3-Setup.exe** to install **WinSCP.** Once it has installed and enter the following parameters to connect to your Linux Server:

File Protocol: **FTP**

Host name: {***your LinuxServer IP address***}

User name: **root**

Password : **password**

1. Navigate in the right hand pane to the **/etc** directory and copy the **shadow** file to “My Documents” in the Security Windows 7.

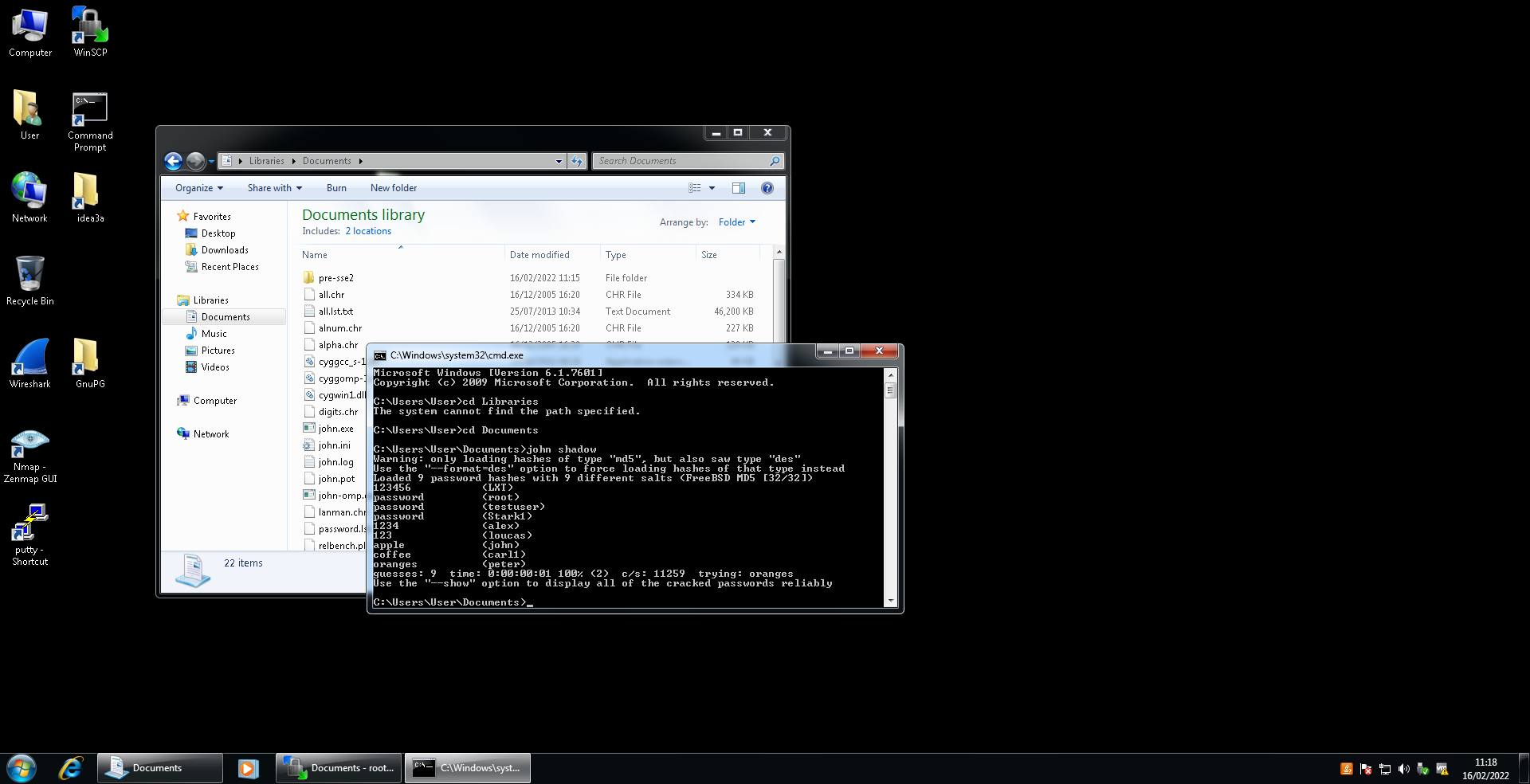
**Use John The Ripper to retrieve the passwords**

1. If “John the Ripper” is not already present on the Security Windows 7 desktop, copy the “john the ripper” zip file to the Windows 7 desktop, then extract the files.
2. Navigate to the “**john179/run**” directory, highlight all the files there and copy them into the “My Documents” folder.
3. Open up a command prompt window and navigate to the “My Documents” directory, then execute John The Ripper on the shadow file:

**john shadow**

1. This will then recover the passwords. Take a note of the approximate time it takes to recover each password. If it does not complete in 15 minutes, then press “Ctrl-C” to end the program.
2. Save a screenshot of your results and paste it below:

[Screenshot]



**Server based use of John The Ripper**

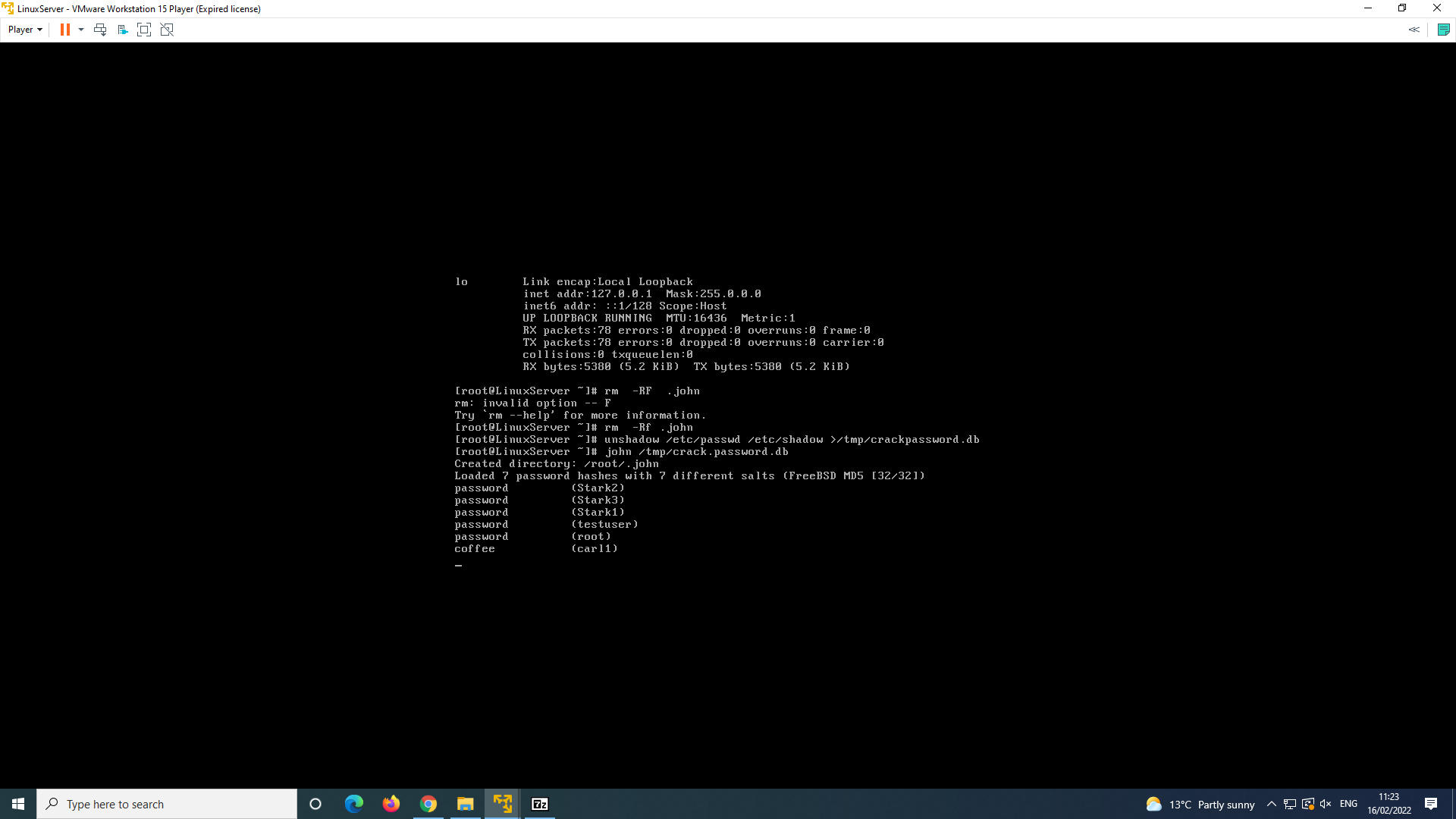
1. Log in to your Linux Server as "root" with the password of "password".  
   1. Clear any previous runs of John The Ripper by running the following command:  
        
      **rm -Rf .john**
2. Combine the password and shadow password files on the Unix server by executing the following command on the Unix server:

**unshadow /etc/passwd /etc/shadow > /tmp/crack.password.db**

* 1. Now crack the passwords on the system by using John The Ripper:  
       
     **john /tmp/crack.password.db**

1. Now, this will probably run for a very long time, if any of the passwords are complicated. So if it runs for more than 15 minutes, press “Ctrl - C” to stop it. Save a screenshot of the usernames and passwords on the Linux server below:

[Screenshot]

**Part 2 – Sniffing for Passwords**

**Scenario**

You will be using a packet sniffer to examine the contents of packets sent from one computer to another. We will be using 3 virtual machines – Security Windows (Attacker), LinuxServer(Victim) and Windows 7 Victim (Victim) to create the traffic. Traffic will be generated between the different machines.

**Preparing the VMware Windows 7 Victim Environment**

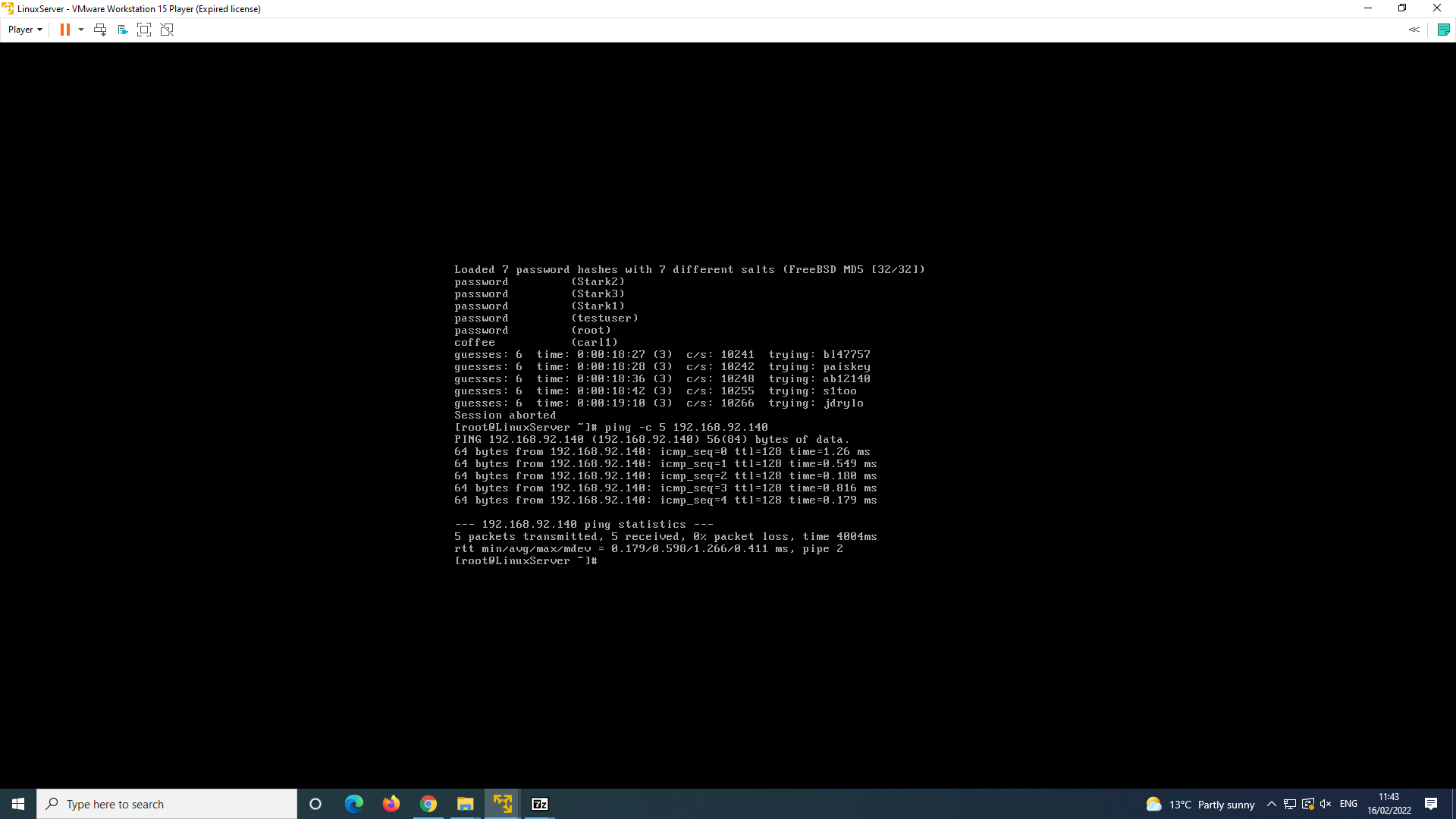
1. Download Windows 7 Victim VM from Canvas and start it
2. Get the value for the IP address below:  
     
   [Windows7 Victim IP address]
3. 192.168.92.140

**Check network connectivity**

Now check that you have network connectivity between the virtual machines. In the Windows 7 Victim, Security Windows 7 and Linux Server machines, use the command prompt window and the ping command to ping the other two machines’ IP addresses. For example:

**ping 192.168.123.123** *(use your own IP addresses here)*  
  
In Linux the **ping** command will send an endless stream of packets until told to stop. Search the internet to find out how you can set the number of packets that the ping command will send to 5 packets only, and also how to stop a running ping command.

[Your Answer Here]



**Wireshark**

On the Security Windows 7 desktop open up Wireshark and select **Capture>Interfaces**, and from the Pop up click on start button for your IP address. Various panes will fill with information regarding traffic.

Examine the headings on these and try to understand what they relate to. Use a ping command between the other two VMs and see the records in Wireshark relating to these.

Click on a record and see the contents of the packet in the lower pane. Now we only want to gather traffic from the Windows 7 Victim, so we need to filter the traffic. In the Wireshark GUI, there is a dialogue box to set filters.

Use the Help function in Wireshark, as well as the documentation at

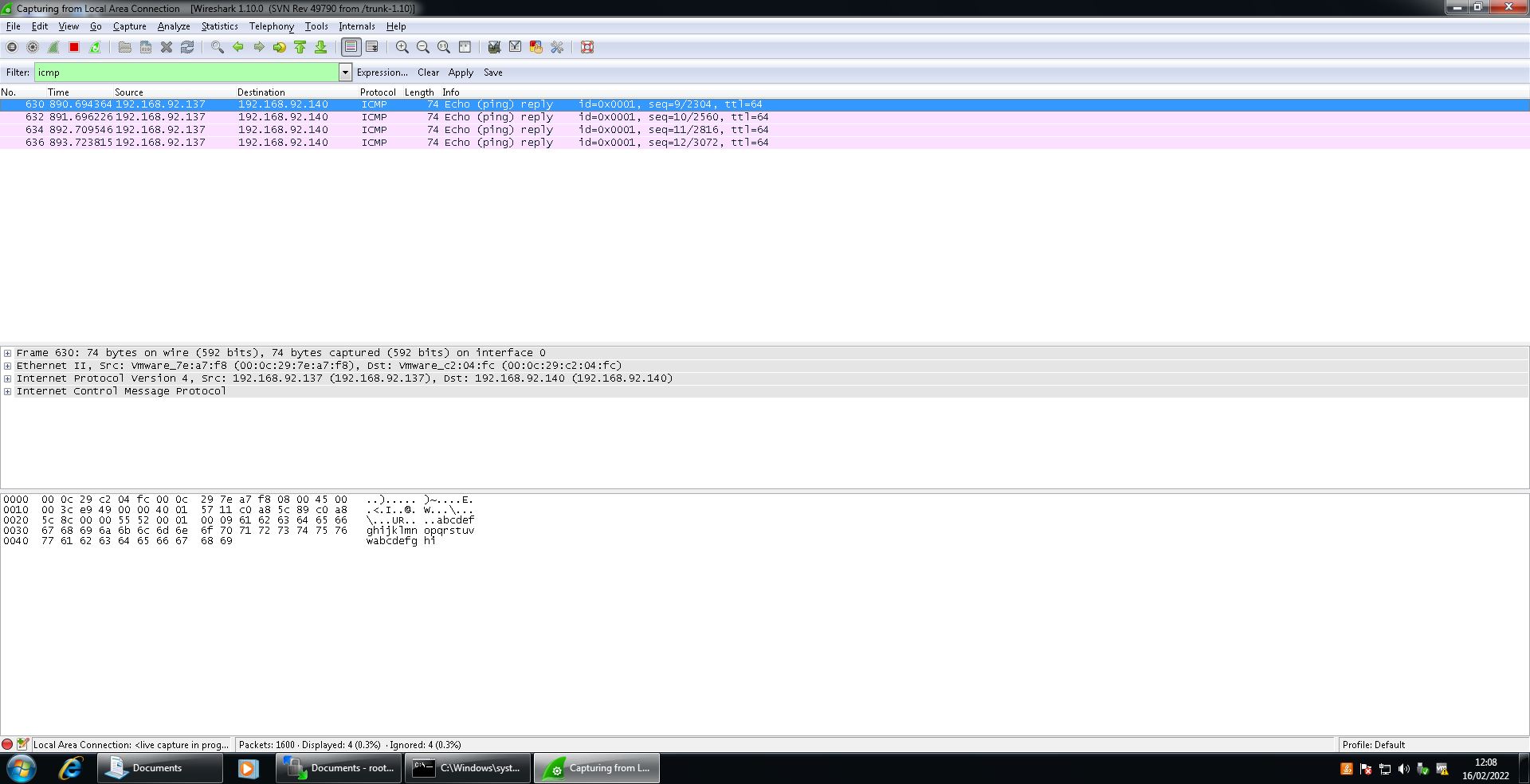
<http://wiki.wireshark.org/DisplayFilters>

to find out how to use the correct syntax to filter traffic only from the Windows 7 Victim machine.

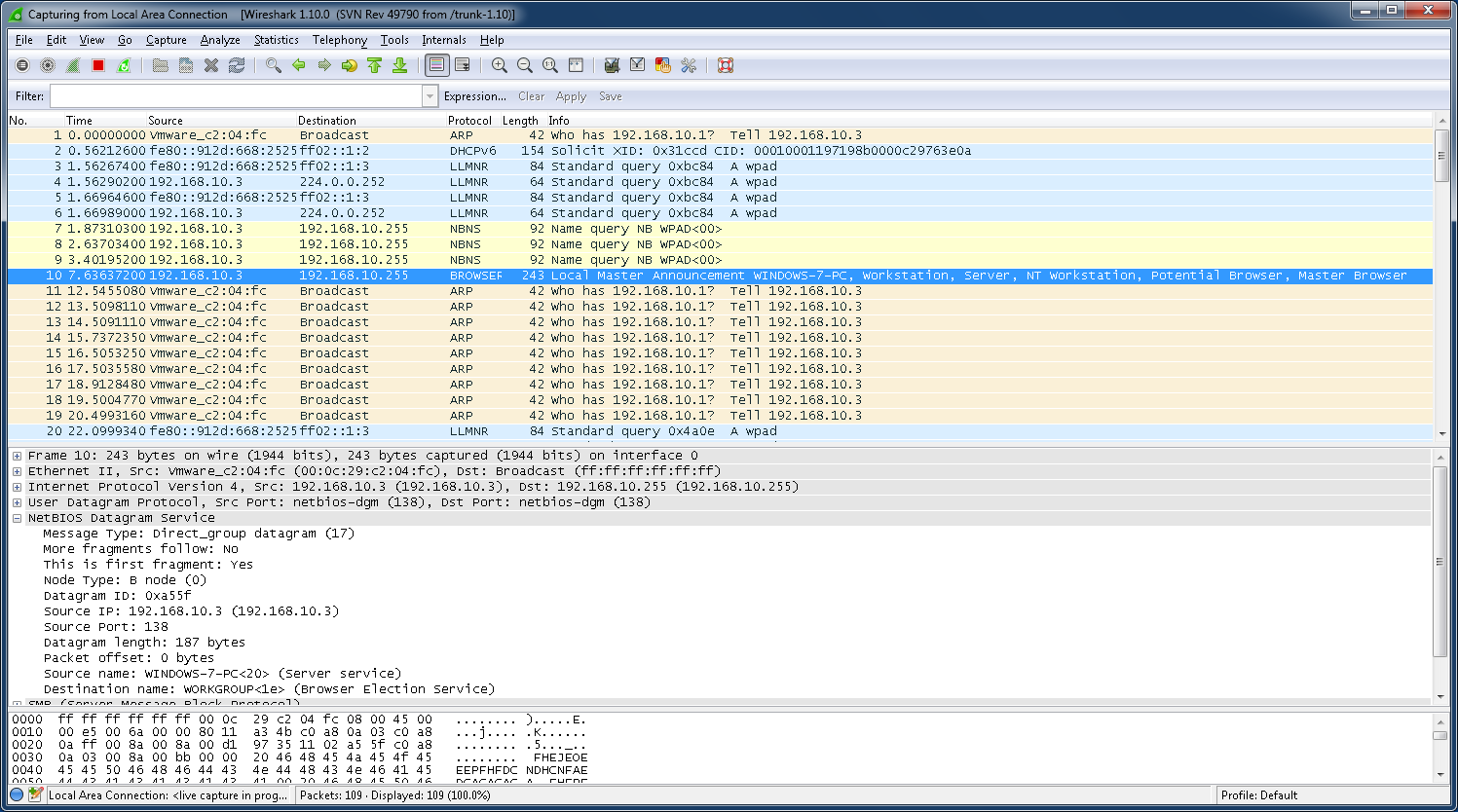
**Traffic to create and examine**

1. Ping between Windows 7 Victim and LinuxServer – use a Wireshark filter to display only the echo reply from the Linux. When you have set up the filter correctly and are displaying only the echo replies from the Linux, capture the screen and paste it in the space below:

[screen capture here]



1. Using a web browser on Windows 7 Victim connect to the Linux Server's Webmin web application. The URL for this is <http://192.168.xxx.xxx:10000>. Substitute the 192.168.xxx.xxx with the IP address for your Linux Server. For example, if your Linux Server’s IP address is 192.168.123.234, then point your web browser in Windows7 Victim to <http://192.168.123.234:10000> .
2. Login to the Webmin web application. The username is “root” and password is “password”.
3. Use Wireshark to search through the packets gathered to find the packet with the password and username. When you are successful, capture the screen and paste it below:



1. To FTP from the Windows 7 Victim VM to the server we first must create a simple text file. Open notepad and create a text file with your name and student ID in it, and save it to the C: drive in Windows 7 Victim.
2. Set Wireshark to gather packets from Windows 7 Victim. Open a command window and start an FTP session to transfer the file to the server.

**ftp 192.168.123.34** *(use your own LinuxServer IP here)*

**User : testuser**

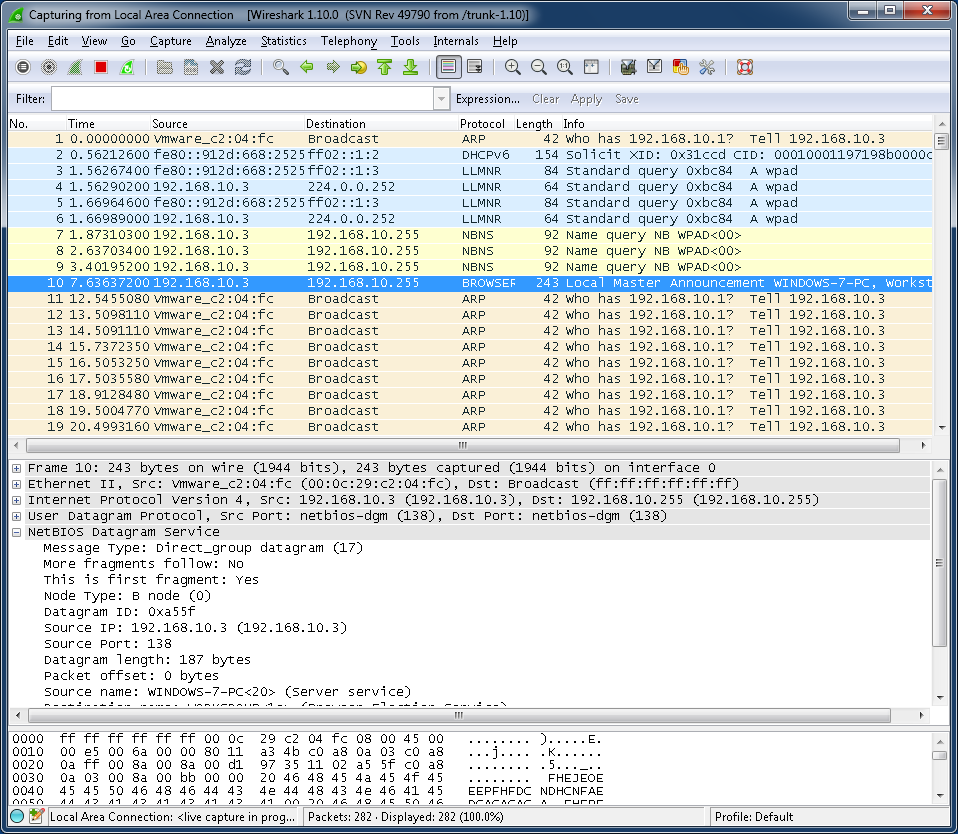
**Password : password**

**put myname.txt**

**quit**

1. Now examine the packets in Wireshark. When you can see the contents of your file, capture the screen and paste it below:

[screen capture here]



1. When you have finished, shutdown the Linux Server with the following command:  
     
   **shutdown -h now**

**Workshop Questions**

**Do some research online and** answer to the following questions/topics:

1. Appraise 3 popular password cracking tools.  
     
   Crackstation

Password Cracker

Brutus Password cracker

1. What are the top 5 most popular passwords? What are your thoughts on them?  
     
   top 5 most popular passwords are:

123456

123456789

picture1

password

1111111

These passwords are weak and will take less than a second to hack the accounts with these passwords.

1. What is “multi-factor authentication”? Can this be compromised?  
     
   This is an electronic authentication in which a user is granted access to a website or an application after they present pieces of evidence to the authentication mechanism. Although its hard to compromise it because it needs data from the user to grant access, they are frustrating to set up and sometimes it can be inconsistent

1. What is “Biometric authentication” and what are its limitations?   
     
   Biometric authentication is a security process which relies on a person's unique biological identity. For example it can be fingerprints, facial, voice and iris(eyes). To this day they are not as safe as pin codes to use. They can be easily spoofed by sensors and let any user get access. They can cost a lot of money to set up too. For example a woman's iphone in Asia would scan her sister and grant access to the phone.
2. Name 3 other popular network traffic sniffing tools. How would you protect your web browsing activities against network sniffing tools?

3 popular sniffing tools are:

SolarWinds Network Performance Monitor, Paessler PRTG Network Monitor and ManageEngine Netflow Analyzer

These sniffing tools can analyse traffic by type so if you see shady packets entering your network, you could stop an attack faster. These packet sniffers can also improve bandwidth by finding “fault performance”. These can also highlight unusual spikes in traffic which someone can see that and dig deeper.