### COS30015 IT Security

### Lab 8 – Modified by Faizal

Comparing Security between Telnet and SSH. Using **Kali** and **Metasploitable 2**.

Ref.: <https://www.youtube.com/watch?v=bZNc7sHt_BY>

**Requirements:**

1. **Kali Linux** – Network setting as **Host-only adapter**
2. **Metasploitable 2** - Network setting as **Host-only adapter** – Install it in your VirtualBox.

**Instruction:** Fill-in the blank while you are doing the steps.

On VirtualBox, start Kali then Metasploitable 2 one after another.

Fill-in IP addresses:

|  |  |
| --- | --- |
| Kali IP (client) | 192.168.56.103 |
| Metasploitable 2 IP (server) | 192.168.56.102 |

Start from now on, be aware of your Kali and Metasploitable IP address. Follow the steps based on your IP addresses.

**Lab 8 Part 1:**

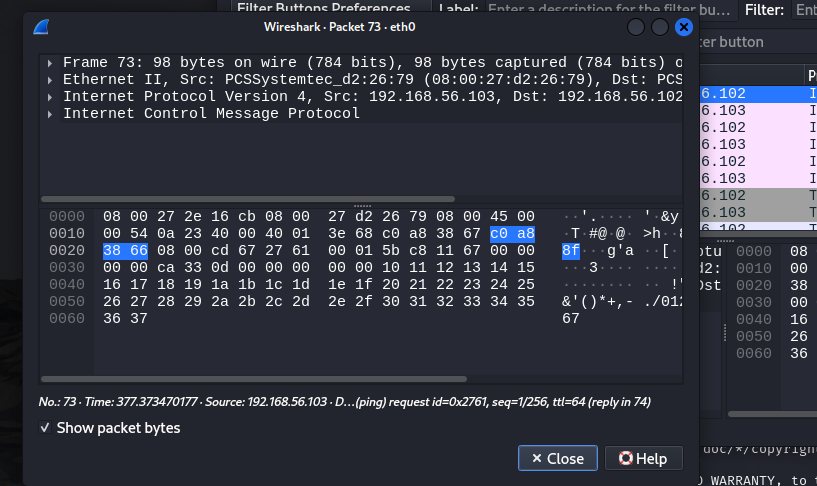
1. During the Metasploitable 2 start up, login as follows:

* Login: msfadmin
* Password: msfadmin

1. What is the best way to know that your Kali would be able to connect to Metasploitable?

|  |
| --- |
| Use ping to each other |

1. Execute Wireshark on your Kali Linux VM. Set filter so that your Wireshark only shows results of network traffic between Kali and Metasploitable 2.
2. Sample Filter:



1. On Kali open terminal to start the telnet command below. (**Note** the IP address is the Metasploitable VM)

**telnet 192.168.100.105** (Enter)

1. Login telnet from Kali using Metasploitable password.
2. Check the **Wireshark** output:

Once you have login to the Metasploitable, on Wireshark Stop the packet capturing. This is to avoid busy results.

Search for the first Packet labelled with **TELNET**.

Right-click on this packet, then choose **Follow** > **TCP Stream**

Provide screen capture of the Wireshark output here:

|  |
| --- |
|  |

1. Can you see the exposed Login and Password done with connecting to Metasploitable via Telnet?

|  |
| --- |
| yes |

**List down 2 important information shown in Packet captured at No. 7 above:**

|  |
| --- |
| 1. Source kali ip and destination ip metaspoitable 2 address 2. Source and destination port number. Source port no. 56092(on kali-client) destination port no.23(on metaspoitable2 telnet server) 3. And other ip packet info. -ack,seq,num etc |

1. On Kali – Wireshark, restart packet capturing. Got to Kali terminal with msfadmin prompt since your are still connecting to Metasploitable (server)
2. On Kali terminal try to run commands:
   1. Enter: ls – you can see vulnerable directory
   2. Enter: cd vulnerable – to go inside vulnerable directory
   3. Enter: ls -alh – to view all files/directories with access right.
3. Stop Wireshark capturing.
4. Observe the recent Telnet traffic. Open – Follow – TCP Stream again.
5. What can you see in the packets?

|  |
| --- |
|  |

1. Close the TCP Stream view and Start Wireshark capturing again. Don’t save any results.
2. On Kali terminal, with msfadmin account still connecting to Metasploitable, enter: exit. This makes the telnet session terminated. Obeserve the Wireshark results for the terminating session.

|  |  |
| --- | --- |
| What is the telnet port number open at Metasploitable? | 23 |
| What is the client port number (Kali session) shown? | 56092 |

Now, we are going to compare connection done via Telnet above, with SSH below.

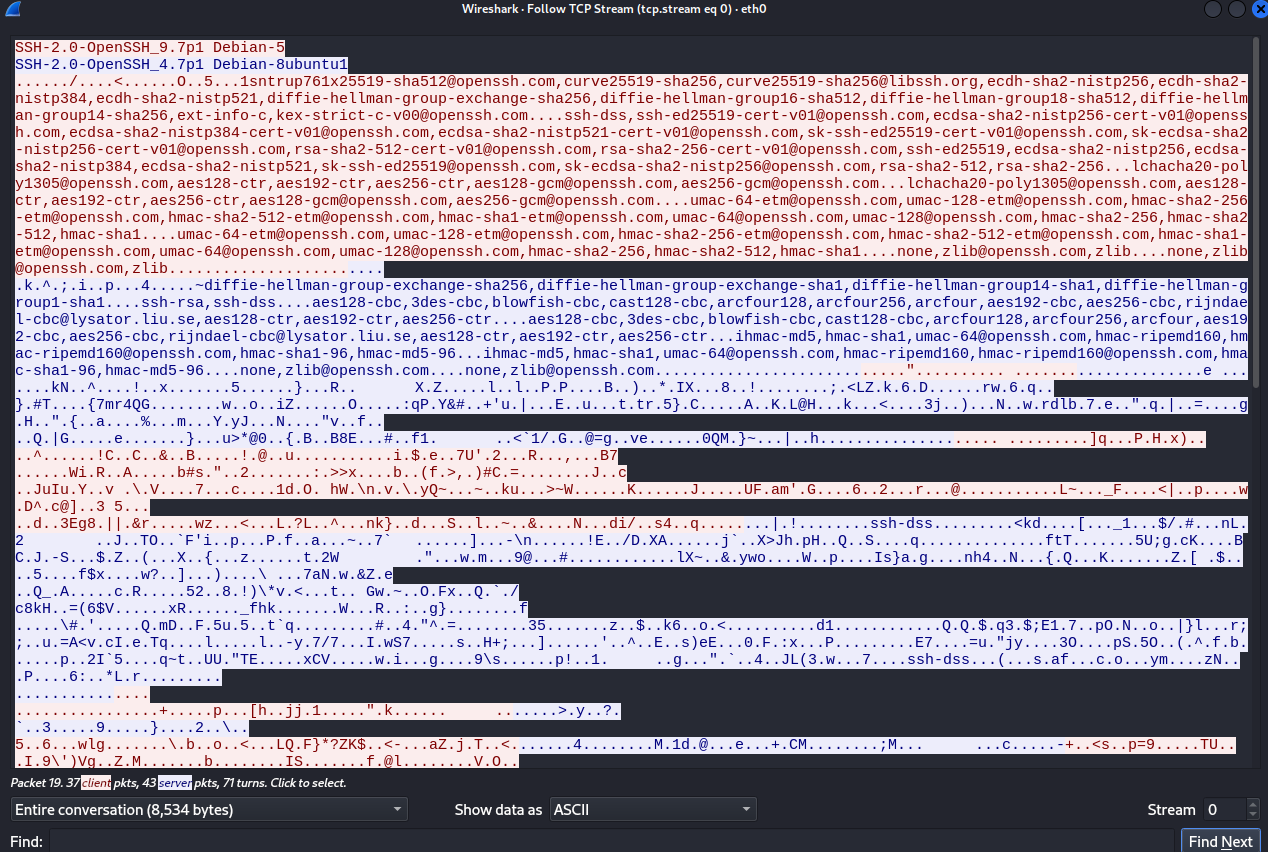
1. Let’s try this again connecting Kali with Metasploitable via SSH. Remember to ensure Wireshark still running at the back to capture SSH session.

On Kali Terminal enter:

ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.100.105 (Metasploitable IP)

password: msfadmin

1. Once you have login, go to Wireshark and stop capturing. Observe all packets involving Kali and Metasploitable and answer all the questions below:



|  |
| --- |
| 1. What is the version of the SSH and running on what operating system?   **Client:**  **Server:** |
|  |
| 1. Search for SSH packet result labelled as Key Exchange. What key exchange technique in used? |
|  |
| 1. List down 3 different Hashing techniques available to be use for the session: |
|  |
| 1. What is the Port Number of Metasploitable SSH server? |
| 1. What is the Client (Kali) Port Number given during this SSH session? |

1. On Wireshark results above, starting from Packet labelled as “Server: Key Exchange Init”, **list down all the SSH packet** labels/info in the table below:

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Source IP | Destination IP |  |
| 1. | 192.168.100.105 | 192.168.100.101 | Server: Key Exchange Init |
| 2. | 192.168.100.101 | 192.168.100.105 | Client: Key Exchange Init |
| 3. |  |  |  |
| 4. |  |  |  |
| 5. |  |  |  |
| 6. |  |  |  |
| 7. |  |  |  |
| 8. | 192.168.100.105  &  192.168.100.101 | 192.168.100.101  &  192.168.100.105 | All packets are labelled as “Server or Client: Encrypted Packet” |

1. With all the SSH packets above, can you read any information other than Protocol session?

|  |
| --- |
|  |

1. And because of that, you should not use Telnet to connect to server anymore. Use SSH connection since all packets are encrypted.
2. Using your Windows Host OS, search on Google conceptual diagram on how SSH works. Attach the diagram below:

**Note**: The diagram should show session negotiation between SSH Client with SSH Server and what are the purpose of the packet traffics.

|  |
| --- |
| EP124: How does SSH work? - ByteByteGo Newsletter |

**Lab 8 Part 2:**

**Before we continue, stop Wireshark. Close/Shutdown Metasploitable and Kali.**

**Part 2-a: Public / Private key Crypto using RSA simulator**

1. Go to the following URL on your Windows Host OS.

<http://www.cs.pitt.edu/~kirk/cs1501/notes/rsademo/>

and read the page.

1. At the bottom of the page are links to three Java-script powered applications which:
2. Generate asymmetric key pairs for PGP.
3. Encrypt a character using one key.
4. Decrypt a character using the other key.
5. Use the applications to:

Generate keys for a message (use 5 and 7)

encode a four-letter word (eg. 'aced').

decode the encrypted numbers to retrieve the word.

**Note: do one letter at a time. Refresh the browser (F5) if it doesn't recalculate.**

**P = \_\_5\_\_\_**

**Q = \_\_7\_\_\_\_**

**D (decrypt) = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**E (encrypt)= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**N (shared key)= \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PHI = \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Original word: \_\_a c e d\_\_\_\_\_**

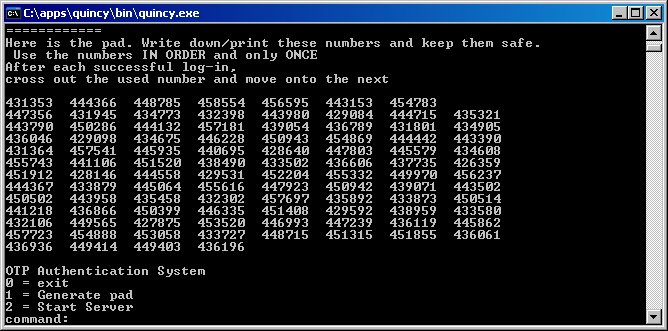
**Encoded message: \_\_\_\_\_\_\_**

**Decoded message: \_\_\_\_\_\_\_\_\_\_\_\_**

**Part 2-b: One-time pads (Optional) – Do this at home:**

Before you continue this One-time pad, preferable you use Windows 7 Basic that we have created in our VirtualBox in previous lab session. Set the **Windows 7 Basic to use NAT Network setting.**

1. Since you use NAT for this Windows 7 VM, you can browse the Internet.
2. On Canvas, download the ***OTP.zip*** file to your desktop PC. A One-Time Pad is an authentication system which defeats packet sniffing and keyloggers (replay attacks).
3. Unzip and run the program (otp4.exe)
4. Type 1 to generate a pad.
5. Type in the first 6 digits of your student number (your user name)
6. Take a screen shot of the numbers displayed. Paste it into a Word doc or image file. This is your one-time pad.



1. Type 2 to start the authentication server.
2. Type in your user name (number) and passcode (the first number on the pad). It will work only once.
3. Log out (exit) and try logging in again. This time, you must use the second number.
4. Try shutting down the server (Ctrl + C) - it stores a hash of your most recently used passcode each time you log in successfully.
5. Run the program again. Start the server. It will pick up where it left off. If you want, look at the source code to see how it works.

*End of Lab*