NSR/AS Lab 5 – Public Key Cryptography – Dylan Rodwell – 105341089

Dylan Rodwell

(105341089)

105341089@student.swin.edu.au

# **Abstract**

This lab session used MATLAB to break a cypher text (c) encrypted with a simple RSA public key system. By exploiting the key’s small modulus size (n), it demonstrates how the algorithm can be compromised by factoring n into it’s secret prime components (p, q). These components can then be used to calculate Euler’s totient (x = φ(n)), and use it to brute force the private exponent (d), such that (d\*e) mod x == 1. MATLAB was used to create a script that automates this process and decrypts the message. The routine *decryptString.m* was used to decrypt the message. It’s “decryptString” function takes n, d, and c in as parameters and outputs the decrypted cypher (c) in plain text.

*-Key words: RSA, cryptography, public key*

# **Introduction to VPNs**

**What is a VPN?**

Article [1] states that a Virtual Private Network (VPN) “is an encrypted connection that secures data transmission between devices over the internet”. This is used to encrypt the data traffic and securely transfer data between devices.

**VPN Capabilities and Vulnerabilities**

The capabilities of VPNs include:

***Secure encryption***. To access the data on the VPN, a device needs an encryption key. This security feature prevents unauthorised access to your data while using a VPN, even when on a public network.

**Data transfer**. VPNs can also be used to transfer data via a secure connection. The encrypted connection stops people without the encryption key from accessing the data being transferred, making it suitable for transferring sensitive information.

**Remote Access**. The VPN tunnelling can also be used to remotely connect to devices via a secure connection where the traffic is encrypted. This is very useful for securely remotely logging on to a company network from home when working from home.

**How VPNs can be used to implement organisational security policy**

VPNs do help enforce organisational security policies in various ways. These include:

**Data confidentiality Policies**. By using VPNs to encrypt all communications and data traffic, it ensures that all traffic stays secure even when travelling through public networks. This keeps the data confidential and compliant with data protection policies like HIPAA and GDPR.

**Access control**. Access control can be used with VPNs as well, by using authenticated VPN connections. This allows organisations to apply role-based access control. This prevents users from accessing sensitive or confidential information that they shouldn’t have access to via the VPN connection.

**Auditing**. VPN servers can log information about connections, which helps admins of the network to monitor connections for suspicious activity and aid in investigations.

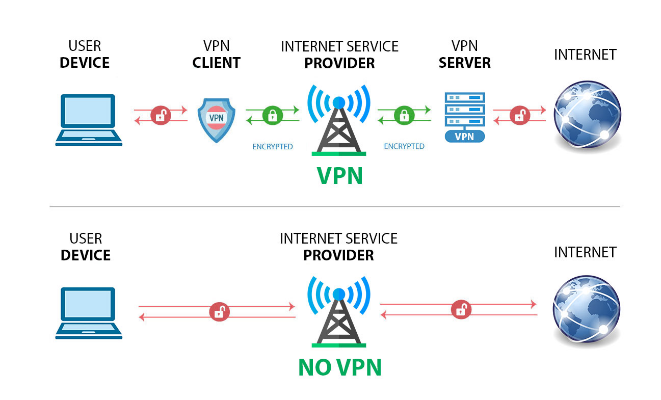


Figure 1. [4]. example diagram of VPN use in a business.

# **OpenVPN Behaviour**

**Host Configuration**

The first step in this lab is to check the ip addresses on the virtual machines by using the command “ifconfig”.

(ifconfig photo for VM1 was lost)

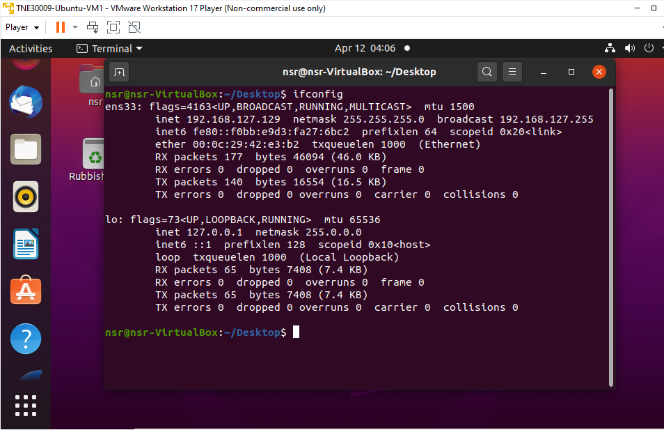


Figure 2. ifconfig used on VM2.

|  |  |
| --- | --- |
| VM1 | 192.168.127.128 255.255.255.0 |
| VM2 | 192.168.127.129 255.255.255.0 |

By running this command on both VMs, the addresses have been identified as:

To demonstrate connectivity between the two VMs, VM2 was pinged from VM1.

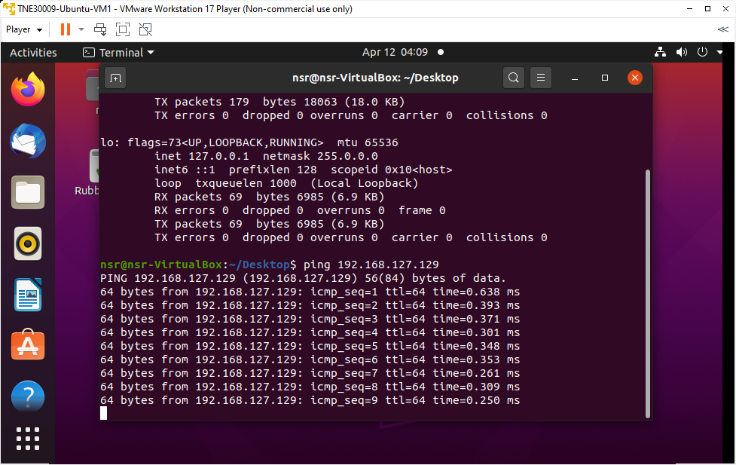


Figure 3. pinging VM2 from VM1.

**Generate Shared Password**

The next step in the lab is to generate a new key that will be used as the password.

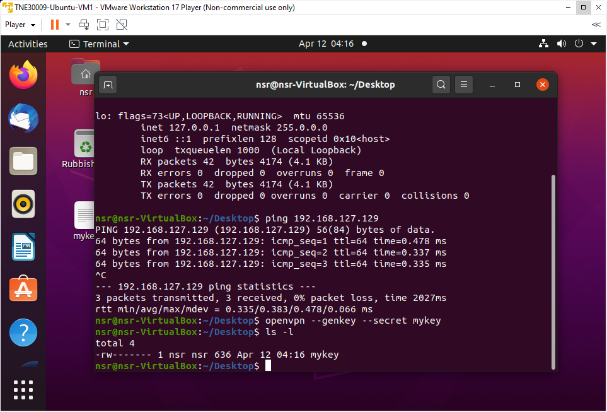


Figure 4. generate shared password on VM1.

Now to examine the key using the cat command.

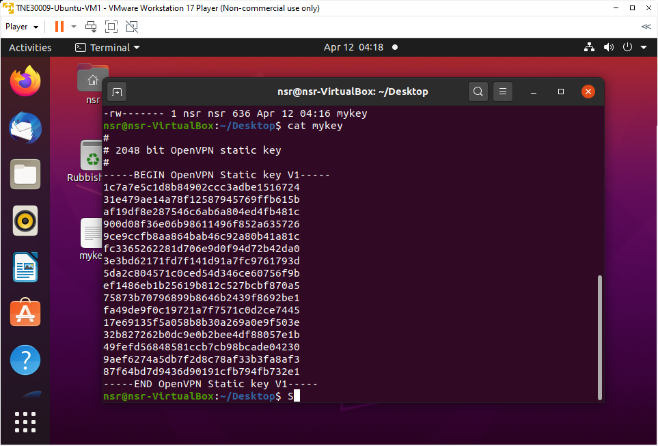


Figure 5. examine OpenVPN key on VM1.

**Transfer Shared Key To Other Machine**

The next task is to install openssh on each of the machines.

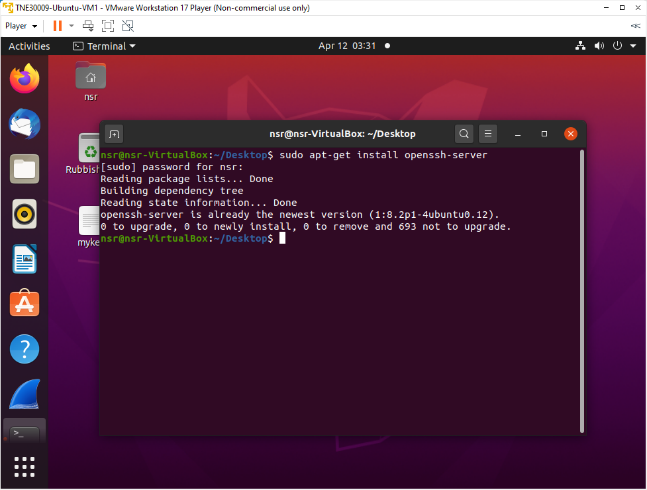


Figure 6. install openssh onto VM1.

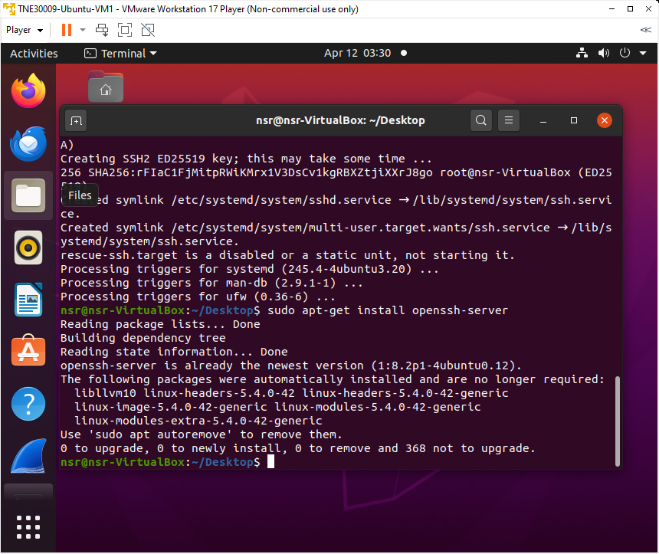


Figure 7. install openssh onto VM2.

Now the key is going to be sent to VM2 via ssh.

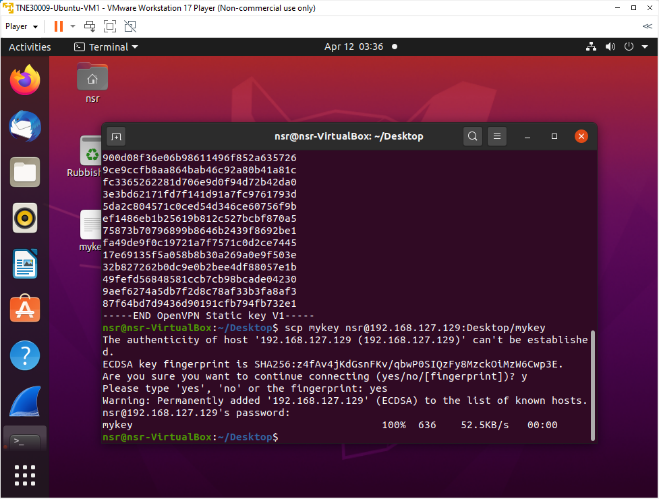


Figure 8. sending key to VM2 via ssh.

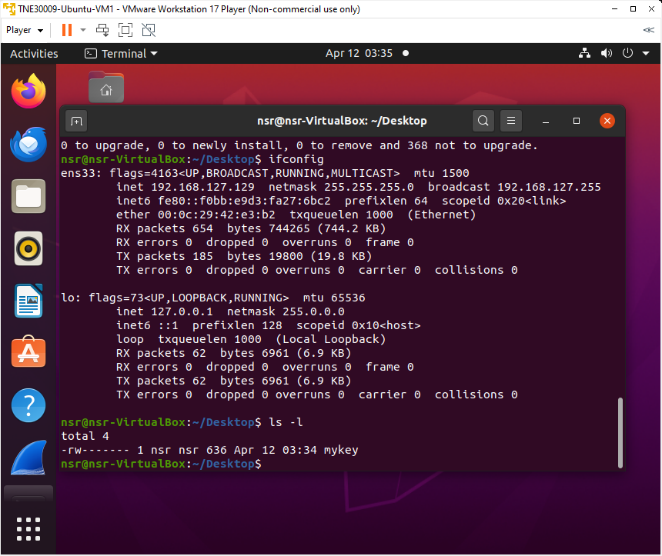


Figure 9. confirm the key file has been transferred to VM2.

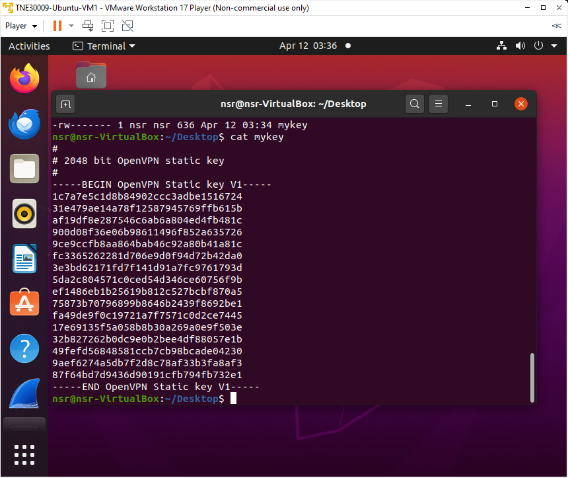


Figure 10. examine the key to confirm it is the same one.

**Set Up Encrypted Tunnel**

The next step in the lab is to finally configure the tunnels between the machines using OpenVPN.

The ip addresses the tunnels will be using are:

|  |  |
| --- | --- |
| VM1 Tunnel IP | 10.4.0.1 |
| VM2 Tunnel IP | 10.4.0.2 |

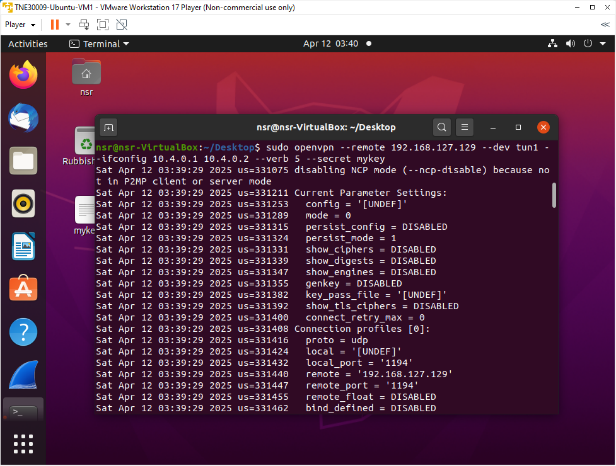


Figure 11. setup tunnel from VM1.

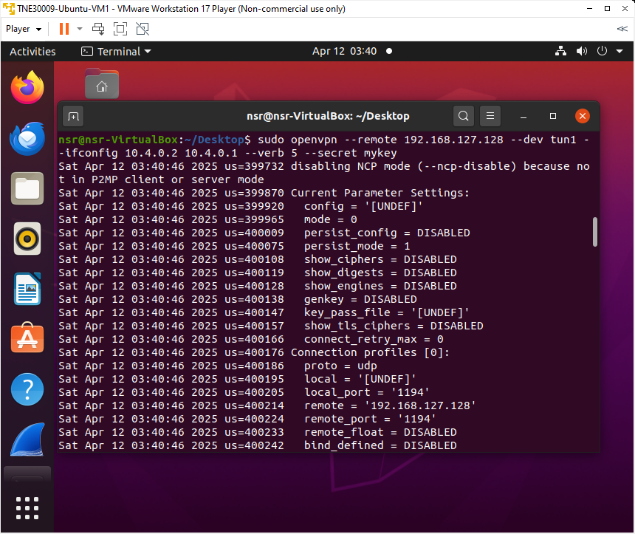


Figure 12. setup tunnel from VM2.

Using ifconfig to check that there is a tunnel interface (tun1).

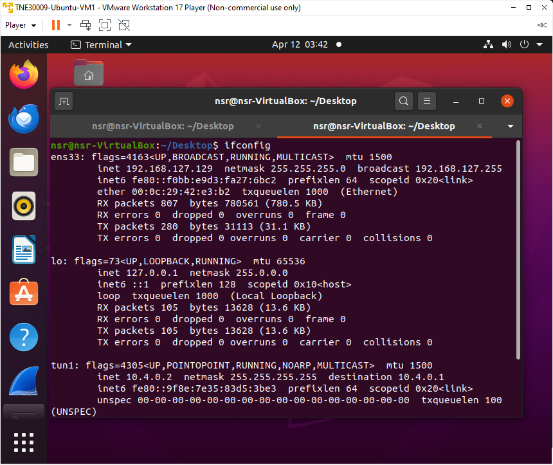


Figure 13. ifconfig on VM2.

**Using the VPN Tunnel**

To check the connectivity between the two machines using the tunnel, VM2 pings tunnel destination on VM1.

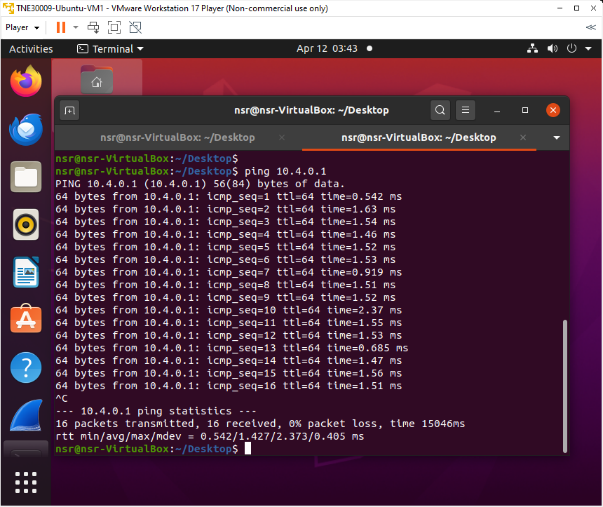


Figure 14. VM2 ping tunnel destination address.

Wireshark is now used to monitor the traffic and verify encryption.

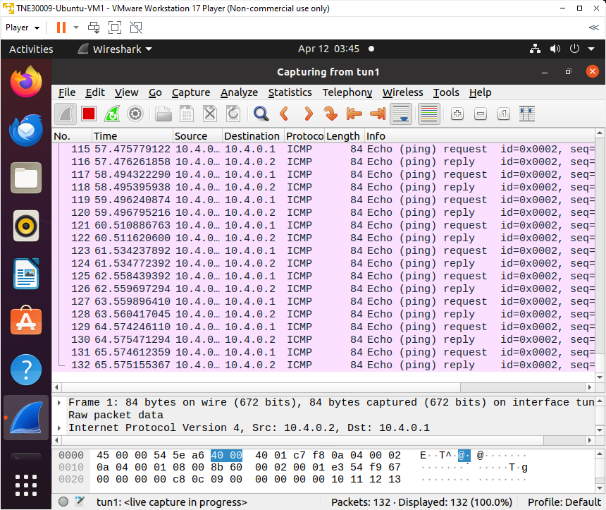


Figure 15. wireshark monitoring tun1 on VM2.

*a) Is the traffic encrypted? Why?*

No, the traffic is not encrypted as we can see the ICMP protocol.

Now wireshark is used to monitor the ethernet interface on VM2.

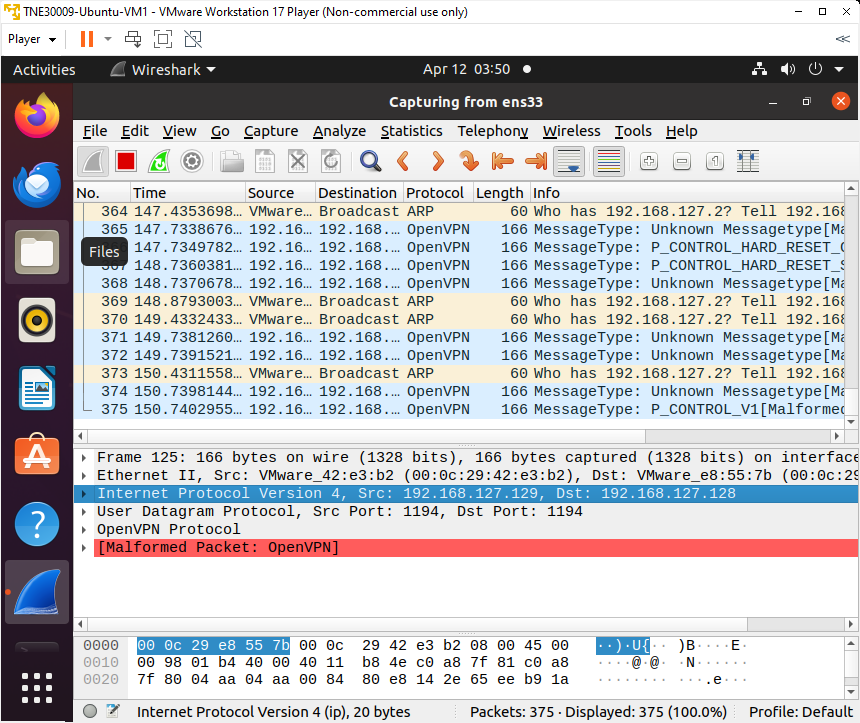


Figure 16. wireshark monitoring ethernet interface on VM2.

*b) Is the traffic encrypted?*

Yes, the traffic is encrypted on this interface.

*c) How do you explain what you see?*

The protocol of the traffic is OpenVPN and the packets have “Malformed Packet: OpenVPN” on them, indicating that it is encrypted.

Now the lab says to telnet from VM2 into the tunnel address of VM1.

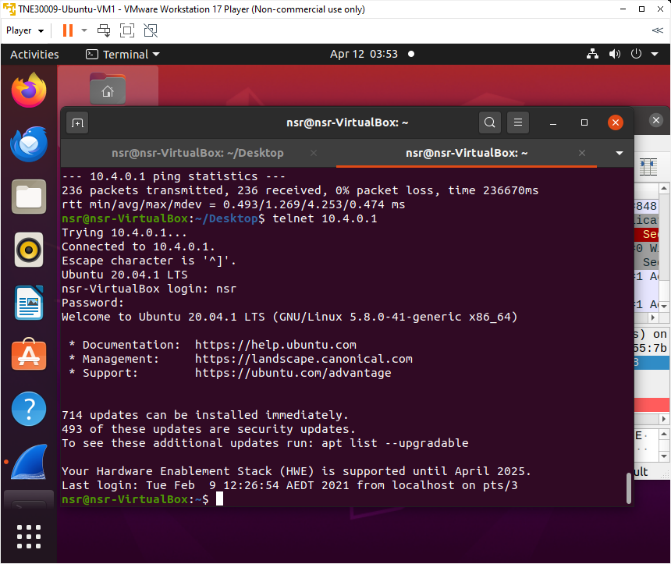


Figure 17. VM2 telnetting into tunnel address on VM1.

To verify that the telnet worked, use ifconfig to check the ip address.

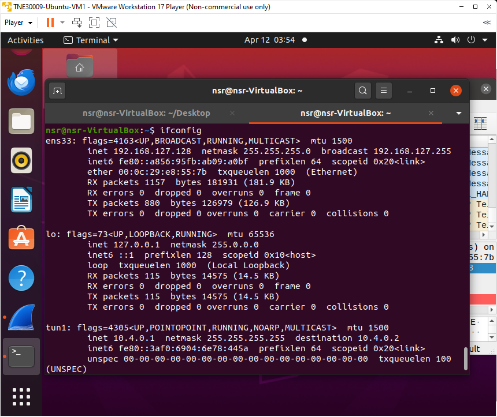


Figure 18. ifconfig on VM2 showing successful telnet.

*d) Which interface is traffic encrypted and which interface is not encrypted?*

The tun1 interface appears unencrypted when monitored with wireshark.

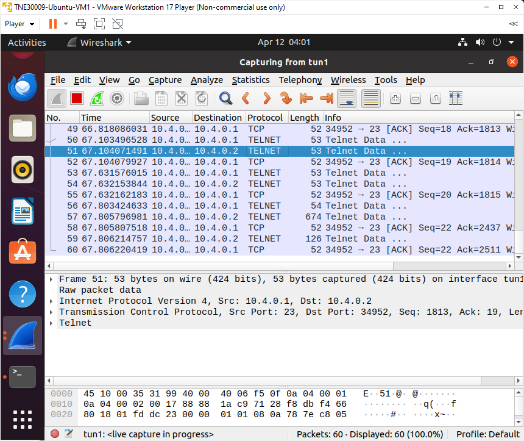


Figure 19. wireshark monitoring interface tun1.

This is because wireshark is monitoring traffic within the tunnel itself, allowing visibility into the unencrypted packets.

Interface ens33 appears encrypted when monitored in wireshark.

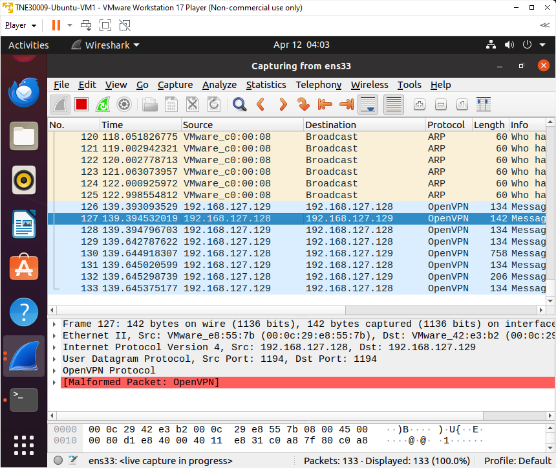


Figure 20. wireshark monitoring interface ens33.

This is because wireshark is monitoring the traffic outside the tunnel where the data is encrypted.

**What Is A VPN Tunnel?**

A VPN is a secure, encrypted connection established over public networks between two or more

# **Conclusion**

This lab successfully demonstrates the implementation of a VPN tunnel using OpenVPN between two virtual Ubuntu machines. By using a shared key and configuring the tunnel interfaces, an encrypted connection was created. By performing this experiment, it demonstrated the differences between the tunnel traffic and the physical interface traffic. Wireshark, telnet and pinging was used to verify that the connection was encrypted and validate connectivity between the two virtual machines.

# **References**

[1] “What is a VPN? A Complete Guide to Virtual Private Networks,” *Palo Alto Networks*, 2015. <https://www.paloaltonetworks.com.au/cyberpedia/what-is-a-vpn#What-is-the-difference-between-personal-and-business-VPNs>.

[2] Kaspersky, “What is a VPN and how does it work?,” *Kaspersky*, Nov. 03. 2020. <https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn>.

[3] Cloudflare, “VPN security: How VPNs help secure data and control access.” *Cloudflare.com*, 2024. <https://www.cloudflare.com/learning/access-management/vpn-security/>.

[4] R. Mendenhall, “Steps for Selecting and Setting up a Small Business Vpn,” *Yarro.org*, Oct. 05, 2022. <https://yarro.org/steps-for-selecting-and-setting-up-a-small-business-vpn/>.