

INVESTIGATE, ANALYSE AND DEMONSTRATE THE IMPORTANCE OF NETWORK SECURITY AND PENETRATION TESTING

Michael Rhys Jones

School of Applied Computing, University of Wales Trinity St David, IQ, Swansea, SA1 8EW, Email: 1909708@student.uwtsd.ac.uk

1. Introduction:

The project focuses on how to complete a scan on a device. This would be essential for users to do if they feel that there are unauthorised users inside their Network, or Device. There are always threats being made everyday, so it would be great if people would have the ability to protect themselves, rather to rely on others.

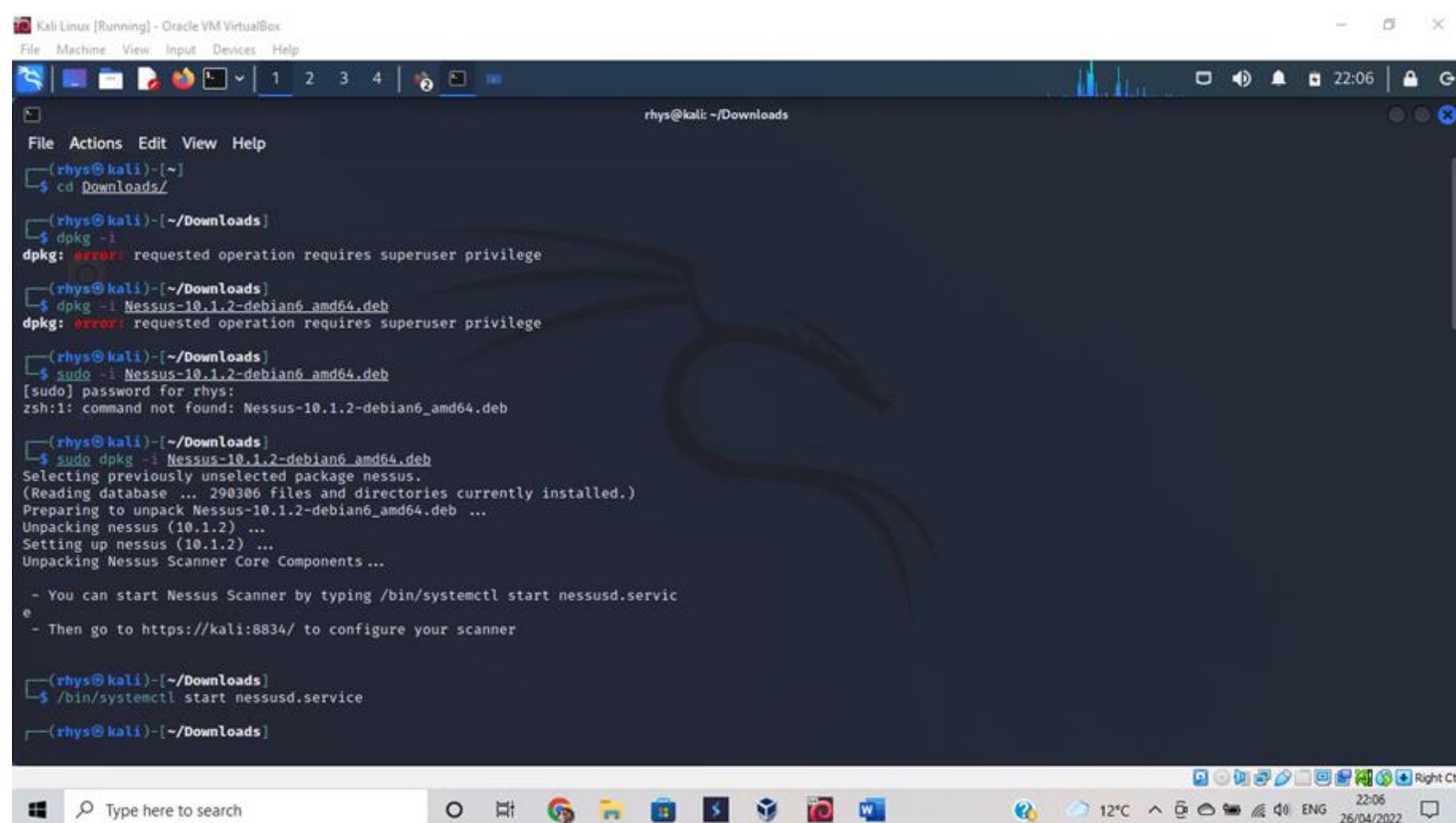


Figure 2 – Nessus

3. Implementation

A home network was used to carry out the scan. A couple of things are needed for the implementation stage of the project and they are;

- Home Router
- Kali Linux OS
- Home laptop
- Nessus

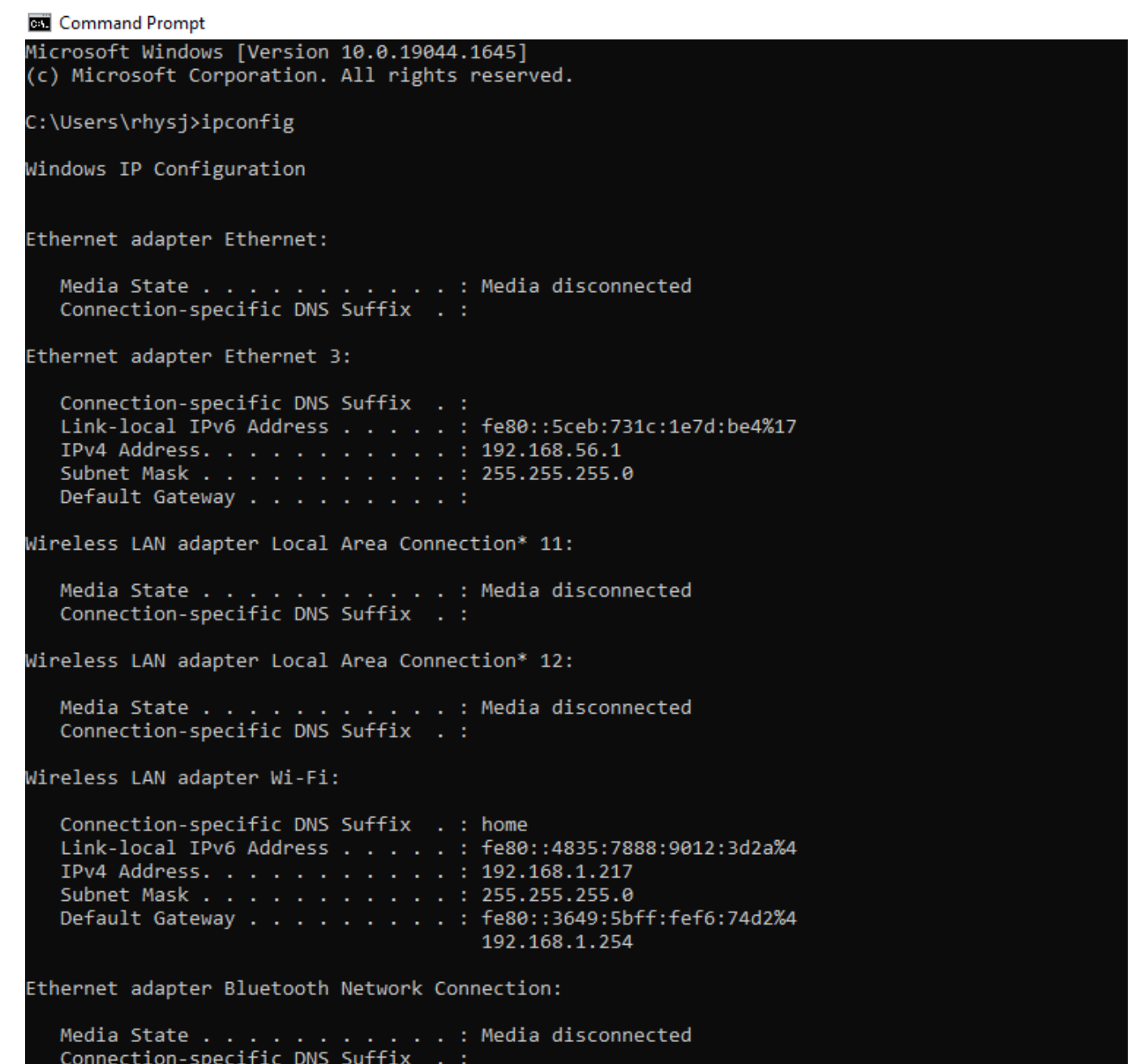


Figure 1 – Command Prompt

2. Aims and Objectives:

The aim of this project is to provide an understanding of network scanners by producing experiments to find their vulnerability. [1-5]

- Establish an understanding of Network scanner.
- Provide a critical literature review related to vulnerability scanners.
- Use the scanner to discover weaknesses.
- Provide information of persona understanding of the topic

Results:

The results can be seen in figure 3. Figure 3 is a more in-depth report of the flaws that have been found within the router. Figure 2 provides the terminal start up to initialise Nessus. Figure 1 shows how I was able to require the IP address for the router.

Conclusion:

Overall the experiment went well. With the user being able to conduct a vulnerability scan, the results can be seen in the figures provided. To note in the future, experiments would be more successful and accurate if more than one has been completed. In addition to this, further research on solution to the flaws will be stated.

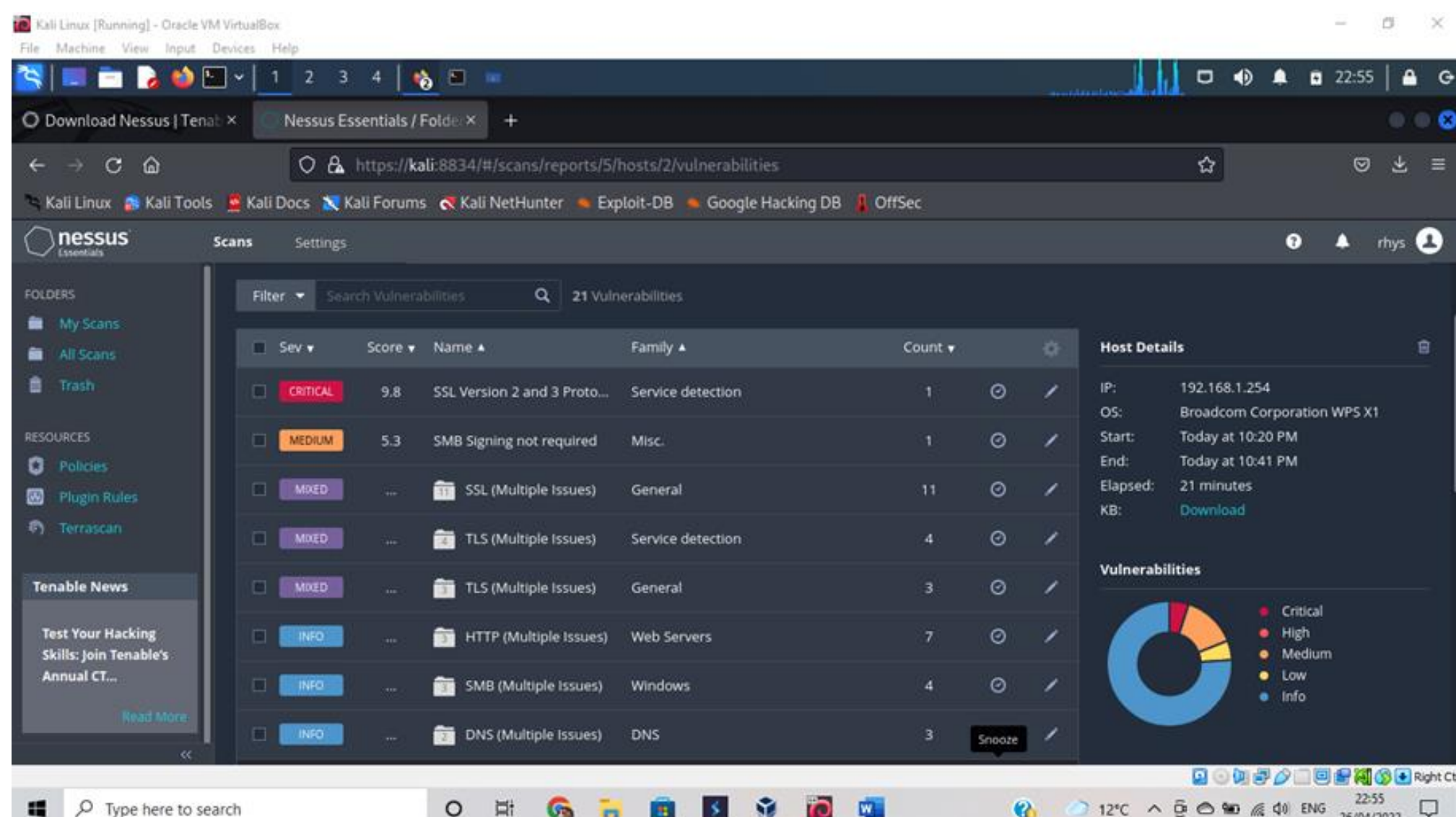


Figure 4 – Results

[1] "What is a vulnerability scanning?," 2021. [Online]. Available: <https://www.itgovernance.co.uk/vulnerability-scanning>.

[2] A. S. Tanenbaum, Computer Networks, N.J: Englewood Cliffs, 1988.

[3] E. W. Dijkstra, "Black-box vs White-box Testing," Technology Conversations , 12 December 2013. [Online]. Available: <https://technologyconversations.com/2013/12/11/black-box-vs-white-box-testing/>.

[4] S. Harvey, "5 Benefits of Regular Penetration Tests," Kirkpatrickprice, 7 July 2016. [Online]. Available: <https://kirkpatrickprice.com/blog/5-benefits-regular-penetration-tests/>.

[5] C. T. Phong, "A Study of Penetration Testing Tools and Approaches," Auckland, 2014