FINAL REPORT

The OS Security Showdown

Ciara Dunleavy C00217731

Supervisor Paul J. Barry

30th April 2021

Contents

Introduction 2

Description of Submitted Project 3

Description of Conformance to Specification and Design 5

Description of Learning 5

Technical 5

Python 5

Nmap 5

Personal 5

Review of Project 6

Acknowledgements 6

Introduction

This document presents a final report with an overview of my experience of The OS Security Showdown. It covers various topics about the completion of the project, such as the description of the end result, what technologies I incorporated in my project and how I managed it throughout. It highlights the personal aspects, as in how I would perform this project again and if I would change my approach to this project. It will compare the original specification of the project to the final implementation of the project. It will provide an incite to the personal learning outcomes that I achieved from completing this project.

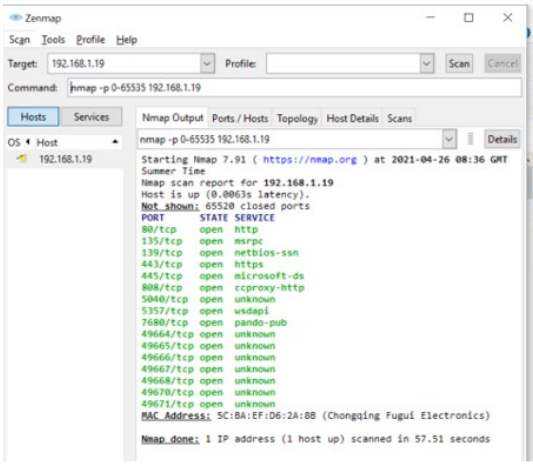
Description of Submitted Project

This Operating System Security Showdown project is the final year project of Ciara Dunleavy under the supervision of Paul J. Barry. This project was completed using the technology Nmap scanning tool and in-depth research of each operating system Linux and Windows 10, research into their history, security features and history of security.

The aim of this project was to develop a comparison with a result of which operating system is more secure, Ubuntu Linux or Windows 10. The operating system is the most important software that runs on a computer. Being able to choose an operating system that is the guaranteed more secure one is exceptionally important. An operating system is software that is managing your computer's memory, processes, software, and hardware, protecting your personal files/accounts is the operating systems main concern. Without a secure operating system, you are vulnerable and at risk.

The comparison between both operating systems is technical and detailed from using the Nmap scanning tool to locate the vulnerabilities of each OS. From just being able to detect what operating system is being used on the device, to what ports are open on each OS with and without an active firewall. Below is a screenshot of the comparison result using the All-port scan -p 0-65535 on each operating system when Apache webserver is installed on both Operating Systems.

WINDOWS

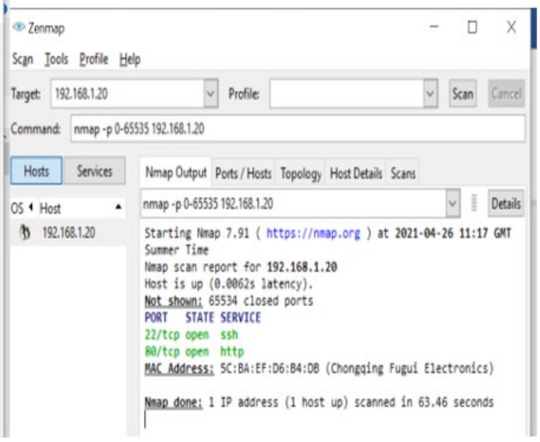


Target: 192.168.1.19

Command: nmap -p 0-65535 192.168.1.19

```
nmap -p 0-65535 192.168.1.19
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 08:36 GMT
Summer Time
Nmap scan report for 192.168.1.19
Host is up (0.0063s latency).
Not shown: 65520 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
808/tcp   open  ccproxy-http
5040/tcp  open  unknown
5357/tcp  open  wsdapi
7680/tcp  open  pando-pub
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49670/tcp open  unknown
49671/tcp open  unknown
MAC Address: 5C:BA:EF:D6:2A:8B (Chongqing Fugui Electronics)

Nmap done: 1 IP address (1 host up) scanned in 57.51 seconds
```

LINUX



Target: 192.168.1.20

Command: nmap -p 0-65535 192.168.1.20

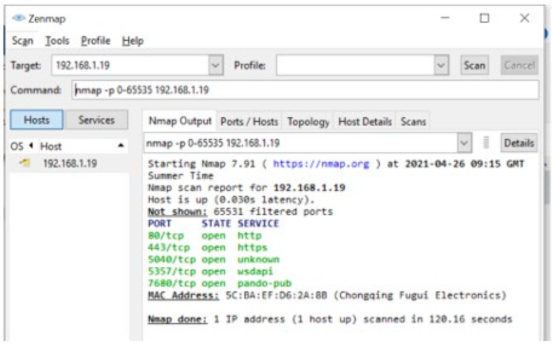
```
nmap -p 0-65535 192.168.1.20
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 11:17 GMT
Summer Time
Nmap scan report for 192.168.1.20
Host is up (0.0062s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 5C:BA:EF:D6:B4:DB (Chongqing Fugui Electronics)

Nmap done: 1 IP address (1 host up) scanned in 63.46 seconds
```

Here we can see straight away, Windows 10 OS has left itself a lot more vulnerable to malicious users as there are multiple ports open.

Linux, however, only has the two http ports open for the webserver.

Next, is a result of the operating systems with all port scan -p 0-65535, but this time it has the firewalls activated.

WINDOWS



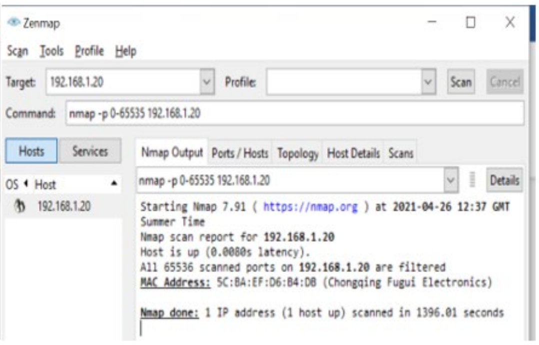
Target: 192.168.1.19
Profile:
Scan Cancel
Command: nmap -p 0-65535 192.168.1.19

192.168.1.19

```
nmap -p 0-65535 192.168.1.19
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 09:15 GMT
Summer Time
Nmap scan report for 192.168.1.19
Host is up (0.030s latency).
Not shown: 65531 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
5040/tcp open  unknown
5357/tcp open  wsdapi
7680/tcp open  pando-pub
MAC Address: 5C:BA:EF:D6:2A:8B (Chongqing Fugui Electronics)

Nmap done: 1 IP address (1 host up) scanned in 120.16 seconds
```

LINUX



Target: 192.168.1.20
Profile:
Scan Cancel
Command: nmap -p 0-65535 192.168.1.20

192.168.1.20

```
nmap -p 0-65535 192.168.1.20
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-26 12:37 GMT
Summer Time
Nmap scan report for 192.168.1.20
Host is up (0.0080s latency).
All 65536 scanned ports on 192.168.1.20 are filtered
MAC Address: 5C:BA:EF:D6:B4:DB (Chongqing Fugui Electronics)

Nmap done: 1 IP address (1 host up) scanned in 1396.01 seconds
```

These results show us how the firewall on Windows OS still leave many ports open.

Linux's firewall is working to it full extent and does not return any responses.

From start to finish, with every command, Windows responded back to Nmap with more ports open and vulnerabilities than Linux. I was expecting Windows to "step up" and show how secure it is, but in fact, it isnt.

This certifies that Ubuntu Linux is the more secure operating system in this Operating System security showdown. Linux from the start has a security layer, until SSH was installed, it would not show any useful results on Nmap. The installation of the webserver only added one more port to the results and that was only when SSH was installed. The firewall continued to portray exceptional security for the OS throughout and did not exploit itself to the network scanner once.

The analysis from the explained results in the technical manual that Ubuntu is the top OS.

Description of Conformance to Specification and Design

Description of Learning

Technical

Python

I began learning Python programming language in the middle of January of this year and spent at least 6 weeks understanding it and practising it. I used the book “Head First Learn to Code” by Eric Freeman. It was a great experience and the book helped me develop my programming mind in many ways. I then moved on to a specific module in Python called Python3-nmap which helps in using the nmap port scanner. I learned how to define each nmap command into a function and scanned the targeted network from a program.

Nmap

Nmap was my main focus throughout this project. I read through articles and the “Nmap Cookbook” to grow my knowledge in the networking port scanning tool. I studied each command, understood the meaning behind each and chose which ones would best suit my project in testing the security of these operating systems.

Personal

- Time Management: My time management skills developed over the course of the project, but I found it difficult to allocate time to factors that were a priority in the project.
- Self-Belief: I lacked belief in myself of completing this project as the course of my project was advised to be changed in the middle of it. I tried my best to take on board this advice of automating it with python, but I did not get time in the end. If I understood and got this advice from the beginning, I would have completed it. I have developed my self-belief from doing this project.
- Communication: I found it difficult to communicate virtually with any issues I had. I had difficulty in downloading Ubuntu and getting it to load accordingly. Explaining the issue over a voice call without being able to screenshare

Review of Project

I am happy with how The Operating System Security Showdown project progressed throughout the year, but I know it could be approached with a better layout of how things were done. From the start, it was stuck in my head that it was more of a research project than a technical project, so I was constantly reading up on both operating systems, their history, what users around the world preferred and the vulnerabilities of each, different tools to use and learning about Nmap.

I made my way from Mayo to Carlow and collected two Laptops from the Institute so I could run Linux OS off one and Windows 10 OS off the other and re-install them after each test, so they were back to their original state before switching on any firewalls or webservers. I am grateful the IT had these devices to help me with my project. I had difficulty in downloading both operating systems to the USB's and found it hard to do it due to having to explain my issues virtually.

My first project presentation was not until after the Christmas due to personal reasons and I presented my project for other supervisors then. I had just started scanning both operating systems and trying to figure out what commands I would be choosing. I got advised that my project was not technical enough and to enhance it. This kind of threw me off and worried me as I thought I had wasted so much time by just researching and not being more technical.

I then began my learning of Python programming Language so I could automate Nmap with it at the end. I spent over a month on this and dropped my project for the time being. I started from scratch and learned the Python-Nmap library which helps in using the Nmap port scanner. Personally, it was a great learning experience as it is something I will always have but it took a lot of time at such a busy period. I felt like if I had started this from the beginning of the project, it would have given me so much more time towards the end.

After I was fully confident in my learning of Python, I picked my project back up and began using Nmap manually again and deciding on commands. With the research on Nmap taking up a lot of time too, I did not get to automate the commands with Python in the end.

I feel as if it were set from the start and I began my learning of Python from the start of the year along with my research on Linux, Windows 10 and Nmap, that I would have completed the automation section of the project using Python on time. The technologies for my project that I used, Nmap and Python, were the correct ones and I would not change them if I were to complete it again.

Acknowledgements

Firstly, I would like to thank my supervisor Paul J. Barry for his help throughout the academic year. With constant encouragement and advise, I was able to carry out this project successfully to the best of my efforts. I would like to thank my parents for continuous support when it got stressful. Lastly, I would like to thank IT Carlow, for the use of their two devices which came in great use for my 4th year project. I would like to thank the author and publishers of Head First Learn to code book as it developed my programming and learning of Python programming language.