DESIGN MANUAL

The OS Security Showdown

Ciara Dunleavy C00217731
Supervisor: Paul J. Barry
30th April 2021

Contents

Introduction

This design manual will explain how I will carry out the comparison of The Operating System Security Showdown between Ubuntu Linux and Windows 10. It will describe each step as I plan to go through this project. It can be used as a guide if this project were to be done again.

Steps

- I will install Windows 10 from www.microsoft.com and download it to a USB so it can be re-installed after each change in the network.
- I will install Ubuntu Linux from https://ubuntu.com/ and download it to a USB so it can easily be re-installed on the device also.
- I researched Nmap and completed a table of which commands I feel will test the operating systems in every possible security aspect.
- I will carry out each command in Nmap, analysis every result and compare both operating systems to each other when they are installed in their original state.
- I will then re-install both operating systems and switch on a webserver (Apache webserver) in each and re-run the commands and compare the results.
- I will re-install the operating systems again, switch on the webserver Apache, and activate the firewall. The nmap scans will be re-run and final results will be analysed.
- I will conclude the project with proof of which operating system is more secure.

NMAP Commands

NMAP SCAN	NMAP SCAN DEFINED
-A command: Aggressive Scan	This command chooses some of the most common options in Nmap. It is a synonym for other commands (-O: OS detection, -sC: performs a script scan, –traceroute: traces the network path of the specified host) that shows.
-PN command: Don't Ping	This command skips the default discovery check and carries out a full port scan. Sometimes it scans even when a firewall is in place on the system as the firewall sometimes blocks ping probes.
-PE command: ICMP ECHO Ping	This command sends an Internet Control Message Protocol ping to the specified target to see if it replies. ICMP is required for correct operation of IP, TCP and other protocols.
-PO command: IP Protocol Ping	This command sends IP ping packets with the specified protocol to the defined target.
-sV command: Service Version Detection	This command shows us Nmaps's service detection feature. It can identify the software version and vendor of open ports.
-sS command: TCP SYN Scan	This command performs a TCP SYN command which identifies the 1000 most commonly used TCP ports by sending an SYN packet to the defined target and listens for a response.
-sU command: UDP Scan	This command performs a User Datagram Protocol (UDP) scan which checks the UDP services to get more of a complete picture of the target.
-sN command: TCP NULL Scan	This command performs a TCP NULL scan which sends packets with no TCP flags enabled. This can give a firewalled system to creating a response.
-p 0-65535 command: All Port Scan	This command scans all ports to detect if they are open
-O command: Operating System Detection	This command detects the operating system that runs on the host. If it cannot detect the OS, it will result in a fingerprint result of the OS which can then identify the OS as it uses nmap.org to figure out which OS is being used.
-sR command: Troubleshooting Version Scans	This command performs a Remote Procedure Call which shows the services running on the defined host

(Sairam, 2018)

Plan

The timeline for this project will be finished by the 30th of April, with beginning my testing in January of 2021.

References

Sairam, J., 2018. *Network scanning cookbook*. Birmingham, UK: Packt Publishing.