RESEARCH MANUAL

The OS Security Showdown

Ciara Dunleavy C00217731

Supervisor: Paul J. Barry

30th April 2021

Contents

Introduction

The objective of this project is both research and implementation on The Operating System Security Showdown. This project will answer the question "Which Operating System is more secure, Windows 10 or Ubuntu Linux?". It has always been a controversial topic which had no certain answer. Every OS user has their own preference of which OS is superior, but none the less the security aspects is not discussed.

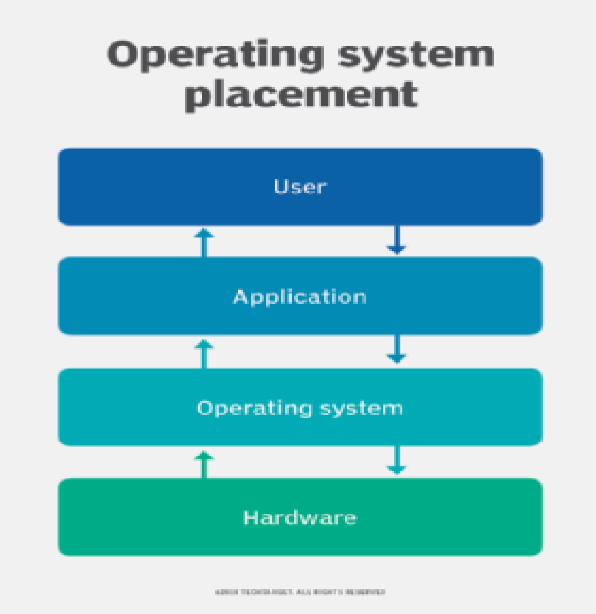
The areas I will be researching will include the history of OS security, how OS security can be tested, different tools that can be used and how to automate Nmap with Python using a Python-nmap module. This research manual layout starts with the basics of operating systems to the technical side at the end of the document.

Operating Systems

What is an Operating System?

An operating system manages and enables the computer system to function with all the applications. The OS must be initially started in the computer but once it is, it boots everything ensuring compatibility. The OS is of great use as the application programs create requests for services in an application program interface (API). The users can make direct use of the operating system too, through the user interface such as a graphical user interface (GUI) or the command-line interface (CLI). Without an operating system in the computer, each application would have to have their own user interface along with the programming code for it to be used by the underlying computer at a base functionality i.e., disk storage. Overall, an OS brings great benefits making every computer practical and usable by the user accessing any number of applications with vastly reducing the amount of time to do so. (Bigelow, 2021)

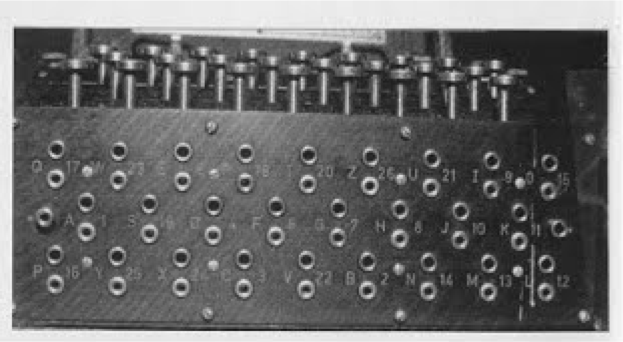
There are three capabilities of an operating system – these are: enabling a UI through a GUI or CLI; starting and managing executions in an application; identifying and exposing the computer systems hardware functions to those applications – usually using an API. (Bigelow, 2021)


Operating system placement
User
Application
Operating system
Hardware
©2019 TECHTARGET. ALL RIGHTS RESERVED

(Bigelow, 2021)

History of Operating Systems

The first generation of operating systems was between the 1940's to the early 1950's when electronic computers were first invented, they contained an operating system. All programming was executed in absolute machine language, frequently by wiring up plugboards to guide the basic functions running on the machine. For the duration of this generation, computers were mainly used for solving simple arithmetic calculations, therefor operating systems were not essential. (Murfin, 2021)



(Murfin, 2021)

The second generation of operating systems occurred between 1955 to 1965, which was when the first operating system was created. It was invented by General Motors for IBM's machine – the 701 and called GMOS. In the 1950's, the operating systems were named single-stream batch processing systems because the data was delivered in groupings. These particularly new machines were titled mainframes and were stored in sizeable computer rooms operated by professionals. As these machines were highly expensive, only major corporation or government agencies could afford them. (Murfin, 2020)

The third generation occurred between 1965 to 1980 in which a multiprogramming system was developed by designers. This system was created to allow computer programs to accomplish and execute multiple tasks at the same time. This prelude into multiprogramming was a significant part in the improvement of operating systems as it permitted the CPU to be occupied almost 100 percent of the time that it was running. A further development amidst the third generation was the exceptional increase of minicomputers, beginning with the DEC PDP-1 in 1961. The PDP-1 attained only 4k of 18-bit words, costing $120,000 per machine, it sold like wildfire. These microcomputers forged an entire new industry and the betterment of more PDP's. The PDP's furthered to the development of personal computers which were produced in the fourth generation. (Murfin, 2020)

The fourth generation of operating systems was from 1980 to today. In this generation so far, personal computers were created despite the fact that they were very much the same as minicomputers, just that they were a fraction of the cost. These personal computers were very economical in that it was possible for an individual to own one whereas minicomputers could still only be owned by major corporations. The creation of personal computing was significant as it led to the birth of Microsoft and Windows operating systems. In 1975, Paul Allen and Bill Gates took the next step and created the largest operating system operated in technology today. MS-DOS was introduced in 1981 despite its effectiveness – it produced problems for anyone who attempted to understand its cryptic commands. Today, every electronic device function off operating systems, from vehicles to smartphones, as technology is evolving, so are operating systems. (Murfin, 2021)

(Murfin, 2021)

History of OS Security

An operating system ensures the functional mechanisms with security in computer processing. Since nearly the beginning of OS's, designers as such have researched and tested ways of how to build a "secure" operating system – or an operating system that remains secure even in the case of a motivated interference as such. In recent times, a key factor of a good operating system is one that ensures this security when providing these fundamental mechanisms in computer processing. These security mechanisms are to ensure specific features to maintain a dependable operating system. Security is a problem in modern systems as we have multiple of interacts occurring at the same time in different ways along with data being shared by processes. i.e., when programming a program, an editor is used to create the programs source code, then compilers and linkers change the code into a way in which it can be executed and then a debugger is used to locate the errors when executing; information is being shared with other users and applications. In the 1940's when operating systems were first designed, there was no exposure like today with the web, e-mail etc. The major challenge today is having a secure operating system that is protected with all of the modern vulnerabilities. (Jaeger, 2008)

Windows Operating System

History of Windows OS

The introduction of the first Windows Operating System began with MS-DOS in 1981 which was created by Microsoft Corporation to run a personal computer. Windows dominated the PC market, with almost 90% of computers were running this type of operating system. In 1985, the first version of MS-DOS was developed with a GUI extension. The enabled the DOS users to have a virtual navigation desktop displaying "windows" graphically and having folders and file contents at just the click of a mouse button whereas before it was typing command and paths of directories within a text prompt. As the ongoing versions were released, there was better functionality in each one, with having File Manager, Program Manager and Print Manager programs including a higher quality dynamic interface. Windows aimed packages towards businesses such as Windows for workgroups and high-powered Windows NT.

1995 came with a complete integrated DOS and Windows. It provided internet support, that being the World Wide Web browser Internet Explorer. (Microsoft Windows | History, Versions, & Facts, 2021)

The release in 2001 was named Windows XP, which was the integration of many Windows packages under one title, producing various editions to suit businesses, consumers, multimedia developers and others. Windows XP ditched the old Windows 95 kernel that was used for years for a more effective and dominant code base that issued an increased interface and application and memory management. The Windows XP version was replaced in the late 2006 by Windows Vista that brought issues and a little resistance in the marketplace. (Microsoft Windows | History, Versions, & Facts, 2021)

Answering to the disheartening feedback on Windows Vista, Microsoft produced Windows 7 in 2009 which had an equivalent interface to Vista but a much-improved version. It met the requirements that the users wanted, increasing its speed and better system requirements. (Microsoft Windows | History, Versions, & Facts, 2021)

The next release was Windows 8 in 2012. This delivered an OS with a starting screen showing applications that were able to be synchronized to settings to if another user logged on, the applications would work on their preferred settings.

Windows 10, which is the operating system that I am comparing to Linux, was produced in 2015. This version of Windows contained Cortana, which is a personal assistant, just like Apple's Siri. Replacing Internet Explorer in Windows 10 is Microsoft Edge web browser. Microsoft also stated that this would be the last and final version of Windows. Instead of having to change to another OS, it will be regular updates for the user to update every so often. (Microsoft Windows | History, Versions, & Facts, 2021)

History of Windows OS Security

Windows OS security has greatly evolved since it was first introduced in 1985. It is a highly used operating system that allows for application availability, which is also a great weakness. It permits an open reach towards applications, but it allows it to be exposed to malware more than other operating systems are. (Belding, 2021)

The first release of Windows OS, Windows 1, contained no OS Security. Instead, it had a basic logon security which did not save passwords into the OS and was comprised of limited logging capabilities. These early releases of Windows had a restriction because they used File Allocation Tables (FAT). FAT was thought to be a durable file system for the early OS's. FAT was made for small drives with simple folder hierarchies. It contained no security mechanisms which allowed information stored on it to be easily accessed, changed, or even deleted. As well as this vulnerability, the early Windows could not hold multiple users, so each user had the same login details on the same account. It was a 16-bit version which meant if the user had to update Windows OS, it was not possible until they expanded it to a 32-bit version.

Windows NT was the first Windows OS that was security based and had a NTFS (New Technology File System). NTFS offered more to Windows then FAT by having increased object security by saving file access rights, stored logging every time information is written and encryption. (Belding, 2021)

Windows 2000 created DPAPI (Data Protection Application Programming Interface which enabled the system to asymmetrically encrypt private keys.

Windows XP was a major jump forward for Windows OS security having many modifications. It introduces a Windows Security Centre that constantly monitored the security and services of the OS. It used a disk to reset password and recognised when a removable disk was inserted. It also increased the security in DPAPI by using a SHA1 hash of the master key password. (Belding, 2021)

Windows Vista followed on from the previous versions with continuing the improvement of OS Security. Vista provided windows defender, a built-in firewall protecting the OS from unwanted software, sometime removing it, or just blocking it. It had an added feature of User Account Control (UAC) – which ensured only the administrator could make authorized changes and no other user. It contained a new encryption feature – BitLocker.

Windows 7 was accompanied with a Data Execution Prevention (DEP) that highlighted data pages as non-executable to prevent malicious users from injecting code. It also came with Address Space Layout Randomization (ASLR) which disarrays memory addresses, so it increased the difficulty for memory-based attacks to be conducted. It improved BitLocker and cryptography in the OS. (Belding, 2021)

Windows 8 OS consisted of changes to the OS security but mainly in the hardware. One change it made was the adding of AppContainer which enhanced Window OS as it enabled low-integrity apps to gain entry to medium or high-integrity objects.

Windows 10, released in 2015 is the latest version of Windows and its new security feature contain Windows Defender Credential Guard that excludes credentials so only the authorized system software can gain access to them making it more difficult to attack. It also has a better security base as it enables svchost.exe, this runs services from a dynamic-link library. (Belding, 2021)

Linux Operating System

History of Linux OS

Linux was produced in the early 1990's by Linus Torvalds and FFS (Free Software Foundation. Linux is an Open-source operating system. Open-source is where the code of the kernel of the operating system can be downloaded, changed and developed or installed by users. It allows it to be user-friendly, securer from viruses and customizable. Every user could change it to suit their needs as long as they gave back to the Linux community and showed their variation. Each time a new upgrade is made with changes to the last, it is called a distribution. Each distribution can be used with no cost to the user. "Linux is more secure than and other operating systems" (Ganguli, 2021)

I will be proving this. Linux provides a live boot system, which means there is no time required for installation.

Below, I will list three of the most popular distributions of Linux:

Ubuntu

Ubuntu Linux is the operating system that is being tested against Windows 10 in this OS security showdown. In 2004, Ubuntu was formed by Canonical and gained popularity fast. It is the topmost recognised Linux distribution. Canonical hopes Ubuntu will be operated as an easy graphical Linux desktop, without the use of a command line. It is the step up from Debian and comes with pre-installed applications and repository libraries that are easy to use.

Linux Mint

Linux Mint is a distribution of Ubuntu Linux and is based on this with similar packages as it uses its repository software. Mint has its own level of popularity as it contains media codecs and propriety software that Ubuntu does not have. It is another option to Ubuntu and uses cinnamon and mate desktop community.

Debian

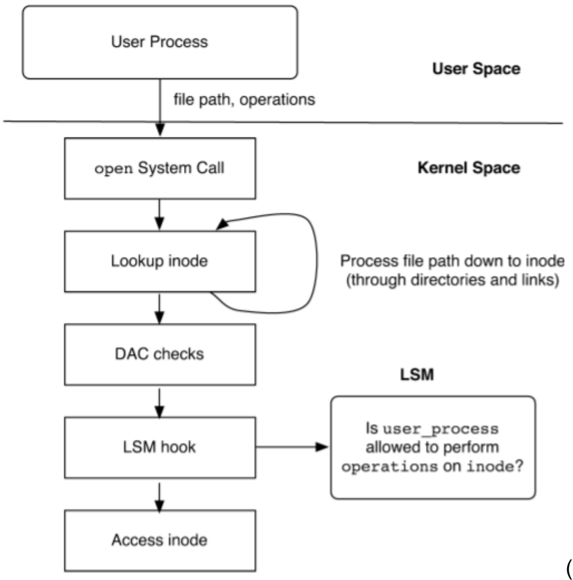
In 1993, Debian was formed and has a lot slower of version release than Mint and Ubuntu. This ensures its stability. Ubuntu is based on the Debian distribution as it increased Debian's usability and improved the core bits.

History of Linux OS Security

In the later years of the 1990's, a couple of retrofit security features were added to the Linux kernel. Due to it being open-source, many projects were produced as users were allowed to alter it as long as they published their modifications. Argus PitBull and Lids are two examples of prototypes created. Each variation was different, but each had the same goal of providing a valuable security function.

In 2001, Security-Enhanced Linux (SELinux) was designed and caught Linus Torvalds eye. Torvald had to accept the prototype and that a reference monitor was needed. There was an issue, Torvald was not a security expert so he could not pick the best approaches as he was not appropriate to choose and then the community itself could not decide on one "best" approach. Torvald stated that he wanted a single reference monitor interface for Linux, and so the Linux Security Module (LSM) framework was implemented. LSM was added to the Linux kernel once formed. It included

AppArmor (limits programs to a limited set of resources), the Linux Intrusion Detection System (LIDS), SELinux, and POSIX (portable operating system interface) practises. (Jaeger, 2008)


User Process
User Space
file path, operations
open System Call
Kernel Space
Lookup inode
Process file path down to inode (through directories and links)
DAC checks
LSM
LSM hook
Is user_process allowed to perform operations on inode?
Access inode

(Jaeger, 2008)

Security Measurement Tools

Security in Operating systems in measured using vulnerability scanning tools which locates loopholes within the OS and detecting what the potential vulnerability of that system is. The function of these vulnerability tests is to protect the OS of their vulnerabilities from malicious users and unauthorized users. It enables the OS to retain their integrity, availability, and confidentiality. These tools can be used on any computer, cloud, software, application, or network.

Types of Vulnerability Scanners

There are four general types of vulnerability scanners that are classified into their uses and how they function: Cloud scanner web applications- Joomla; Host scanners: find a single computer system; Network scanner: finds open ports and their vulnerabilities; Database scanners: find vulnerabilities in database systems. (17 Best Vulnerability Assessment Scanning Tools, 2021)

Available Tools

Nmap

Nmap is a free open-source tool that is used for vulnerability scanning and network discovery and is the tool that I am using to compare Windows 10 and Ubuntu Linux OS. Nmap stands for Network Mapper. It enables network administrators to establish what devices are working on their own systems, it locates what ports are open, shows the available hosts and the services they are presenting, and it also portrays the security risks within the system.

Nmap is useful for large networks with thousands of system and also single hosts. Nmap has changed over the years which has made it very flexible, but it is simply a port-scan tool that sends packets to the system, listens for replies, and then tells us what ports are opened or closed.

Scanning ports gives you so much information back, showing a profile description of the software which enables you to form a software and hardware inventory. It was created by Gordon Lyon in September 1997 and firstly written in C++ source code and gradually extended with Perl, Python and C. (Ferranti, 2021)

Nmap features- active port scanning, discovers hosts, detects the operating system, and shows the application version.

Unicorn

Unicorn is the next best free port scanner. It is popular for its TCP and UDP scanning performance. It includes an IP port scanner and detects the service, detects the OS remotely and ensures many modules from the command-line. (Borges, 2021)

Angry IP Scanner

Angry IP Scanner is another port scanning tool used for network discovery. It is known for its fast-scanning tempo as it contains a multi-thread approach that divides each scan. The main features of this are that it does not need to be installed, it is simply downloaded and the run; it can scan for any ports that are open on a remote network; it detects for NetBIOS information and for Webserver information; it transmits the scan results into XML, CSV, or TXT files; contains an easy plugin that integrates with Java. (Borges, 2021)

Netcat

Netcat is the oldest known tool in the network "universe", having been around since 1995 with the latest release being 2004. It works fittingly on modern operating systems. Its features are it has integrated port-scanning capabilities; supports the scanning of UDP and TCP ports; it reads in arguments from the standard input; it has forks that are useful for Windows, Linus and MacOS. (Borges, 2021)

Measuring the Security of Operating Systems

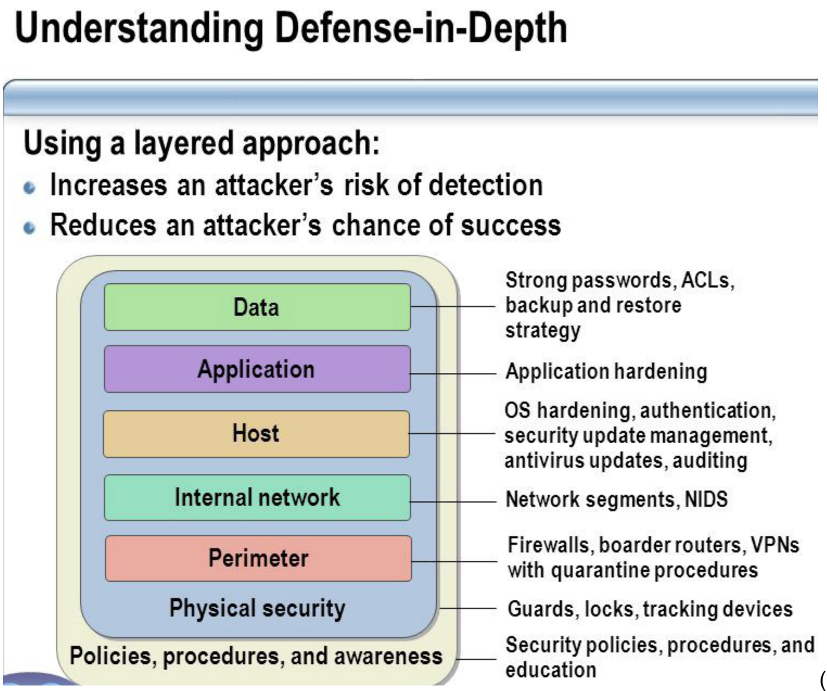
The optimal goal of a secure operating system is to provide security mechanisms to make sure the systems security goals are imposed without being affected by threats or malicious users that the system faces.

Operating system security is the process of the OS being able to ensure the user with integrity, confidentiality, and availability. There is a required set of steps that are used to protect the OS from malware, worms, viruses, threats, or remote hacker intrusions. OS security consists of techniques that prevent the control of an OS, safeguarding that the computer assets are not read or stolen, if the security is put at risk, it is edited or deleted.

The security of an Operating System in different ways along with the compliance of the following:

1. Patch updates carried out regularly
2. Antivirus software and engines are revised often
3. Obtaining a firewall to scrutinize outgoing and incoming traffic to the network
4. Devising a specific account(s) that only they have privileges within that system (user admin.)

While there is no definite implementation that could ever protect an OS from all sides, OS security must first-off understand the strengths of regular security approaches, figure-out the basic challenges of each approach, and lastly research the application of these approaches within a practical environment to show us how effective they are.



Understanding Defense-in-Depth

Using a layered approach:

- Increases an attacker's risk of detection
- Reduces an attacker's chance of success

Data	Strong passwords, ACLs, backup and restore strategy
Application	Application hardening
Host	OS hardening, authentication, security update management, antivirus updates, auditing
Internal network	Network segments, NIDS
Perimeter	Firewalls, boarder routers, VPNs with quarantine procedures
Physical security	Guards, locks, tracking devices
Policies, procedures, and awareness	Security policies, procedures, and education

(OS Security, 2021)

Webservers

A webserver is an application the replies to web page requests presented by many different types of users over the internet. It does this by using a HTTP (Hyper Text Transfer Protocol) which transmits hypertext messages between servers and clients usually using a Transmission Control Protocol (TCP). The webserver that the OS is using represents as the interface between web application and databases and the users; basically, a backbone of the internet and many different networks and apps attaching to it. Due to it being accessed by the whole world, it is obvious it is going to face exploits and vulnerabilities.

Such vulnerabilities would be:

DOS Attack: which is created to flood the webserver with requests in which prevents the legitimate users from accessing as the sever cannot reply to the request within a timely means. The requests that are sent by the malicious users are invalid and the webserver attempts to deal with all these which takes to much time creating a bottleneck in shutting down connections and delaying the reply time of the webserver.

XSRF (Cross Site Request Forgery) Attack: are attacks that successfully divert legitimate users in a website to a malicious website that is created to appear as the original website. The malicious website can obtain and steal users sensitive information, personal credentials, or the users login. Once the malicious user has this information, it can be used against the victim.

There are many different Web-Server types:

Apache HTTP Server: is the webserver that I am going to be using in this operating system security showdown. It is created by Apache Software Foundation and is the most popular webserver in the world. Like Linux, it is open-source software and can be installed on every operating system. About 60% of machines run the Apache Web Server. (Web - Server Types - Tutorialspoint, 2021)

Internet Information Services: is a highly performing webserver created by Microsoft. It is primarily used on Windows NT/2000 and 2003 platforms. IIS is very much combined with these operating systems which makes it very easy to administer.

Jigsaw Server: is another open-source free webserver that can run on many operating systems. It comes from the W3C (World Wide Web Consortium). It is designed in Java and runs PHP programs and CGI scripts.

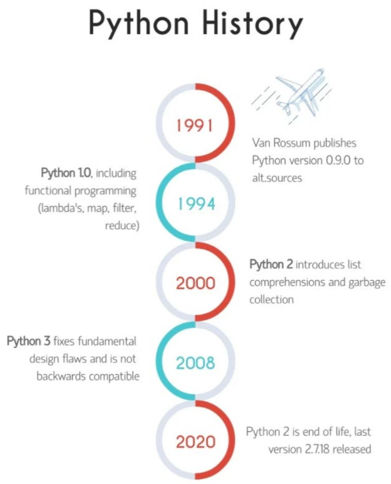
Firewalls

Firewalls are a device in the network that securely controls the incoming and outgoing traffic. It either permits or blocks the data packets depending on specific security rules. The function of a firewall is to create a barrier in between the internal network and the external network (internet) and blocking malicious traffic i.e., worms and viruses.

Python

Python is and open-source computer programming language. It is a general-purpose language that is popularly used by many people around the world, developers, in systems programming, customizing products, internet scripting and user interfaces. Python is known for its high quality, productivity, portability, and integration with other systems. (Programming Python, 2021)

It was firstly designed by Guido van Rossum in 1991 and further developed by Python Software Foundation. It was initially developed for code readability and the syntax in the language enabled users of Python to write concepts in less lines of code. (History of Python - GeeksforGeeks, 2021)


Python History
1991
Van Rossum publishes Python version 0.9.0 to alt.sources
1994
Python 1.0, including functional programming (lambda's, map, filter, reduce)
2000
Python 2 introduces list comprehensions and garbage collection
2008
Python 3 fixes fundamental design flaws and is not backwards compatible
2020
Python 2 is end of life, last version 2.7.18 released

(Baaren, 2021)

Python Nmap Module

Python -nmap is a library stored within python which assists when using nmap port scanning tool. It enables the user to easily operate scan results from nmap. It is a great tool for automizing scans and reports, supports the output of nmap scripts and it used a lot by system administrators. (Norman, 2021)

This module works by downloading a python 3 library which helps nmap. It defines each command in nmap into a python function which make it very usable when using nmap commands in other scripts.

To scan for common ports in nmap the command would be-

```
$nmap 192.168.1.19 –top-ports 10
```

When using python3-nmap, you create a function in python like this-

```
import nmap3

nmap = nmap3.Nmap()

results = nmap.scan_top_ports(192.168.1.19)
```

Your results will then be in JavaScript Object Notation (JSON) which is a format that is used to transfer data to text sent over a network. It is easy to read by both machines and humans.

Resources in this area

A very good book resource that I located found is Operating System Security written by Trent Jaeger. From reading this book, it allowed me to learn the basics of Operating Systems and their specific requirements to strengthen security and how to understand improve my management of Operating Security. (Jaeger, 2008)

Conclusions

In conclusions to this research document on both Windows 10 OS and Ubuntu Linux, the final result of which operating system is more secure will no be definite until both OS's are tested and analysed. They will be compared using Nmap port scanner with a range of commands and the final results will then be compared. I will be spending most of my time understanding each command in Nmap and defining what it really means. Windows 10 OS is the last release of Windows, apart from updates, so from researching it and it being developed for many years, it must be more secure. However, it is stated above, "Linux is more secure than and other operating systems". (Ganguli, 2021). So, the end result will be interesting in this Operating System Security Showdown.

References

Bigelow, S., 2021. *What is an Operating System (OS)?* [online] WhatIs.com. Available at: <https://whatis.techtarget.com/definition/operating-system-OS> [Accessed 30 April 2021].

Murfin, S., 2021. *History of Operating Systems - Operating systems (Windows, Linux, iOS, Android, WebOS, others)*. [online] Sites.google.com. Available at: <https://sites.google.com/site/optsytms/history-of-operating-systems> [Accessed 30 April 2021].

Jaeger, T., 2008. *Operating system security*. [San Rafael, CA]: Morgan & Claypool Publishers.

Encyclopedia Britannica. 2021. *Microsoft Windows | History, Versions, & Facts*. [online] Available at: <https://www.britannica.com/technology/Windows-OS> [Accessed 30 April 2021].

Belding, G., 2021. *Windows OS Security Brief History - Infosec Resources*. [online] Infosec Resources. Available at: <https://resources.infosecinstitute.com/topic/windows-os-security-brief-history/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A%20infosecResources%20%28InfoSec%20Resources%29> [Accessed 30 April 2021].

phoenixNAP Blog. 2021. *17 Best Vulnerability Assessment Scanning Tools*. [online] Available at: <https://phoenixnap.com/blog/vulnerability-assessment-scanning-tools> [Accessed 30 April 2021].

Ferranti, M., 2021. *What is Nmap? Why you need this network mapper*. [online] Network World. Available at: <https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html> [Accessed 30 April 2021].

Medium. 2021. *OS Security*. [online] Available at: <https://medium.com/@rezaduty/os-security-892cfae5e930> [Accessed 30 April 2021].

Tutorialspoint.com. 2021. *Web - Server Types - Tutorialspoint*. [online] Available at: <https://www.tutorialspoint.com/web_developers_guide/web_server_types.htm> [Accessed 30 April 2021].

Google Books. 2021. *Programming Python*. [online] Available at: <https://books.google.ie/books?hl=en&lr=&id=c8pV-TzyfBUC&oi=fnd&pg=PR11&dq=python&ots=n54IcLVVQW&sig=3cLRC6Gv9xHgpDo2srye8QiSyrA&redir_esc=y#v=onepage&q=python&f=false> [Accessed 30 April 2021].

GeeksforGeeks. 2021. *History of Python - GeeksforGeeks*. [online] Available at: <https://www.geeksforgeeks.org/history-of-python/> [Accessed 30 April 2021].

Baaren, E., 2021. *Python History • Python Land Tutorial*. [online] Python Land. Available at: <https://python.land/python-tutorial/python-history> [Accessed 30 April 2021].

Norman, A., 2021. *python-nmap: nmap from python*. [online] Xael.org. Available at: <https://xael.org/pages/python-nmap-en.html> [Accessed 30 April 2021].