



Nmap - Python Automation

Szymon Lewandowski - CMP320: Advanced
Ethical Hacking

2022/23

Note that Information contained in this document is for educational purposes.

Abstract

The contents of this report covers the full development procedure of automating a fingerprinting software used to scan target machines on a network. The purpose of the project was to decrease the time taken to perform scans on target networks by mitigating the need to type each and every command manually. Instead, the python script performs the scans automatically. The report was written by a third year ethical hacking student at Abertay University.

The procedure of the report showcases the step by step process of integrating the nmap library with python and the automation process of each individual scan on a target machine. Suitable background research was conducted in the area of automation and its importance.

By the end of the report, the ethical hacking student developed a fully functioning automated nmap scanner using python scripting. The script featured basic scans that included the host name, state of the host, protocols, ports and operating system as well as a vulnerability scan performed on the target host.

Contents

1 Introduction	1
1.1 Background	1
1.2 Aims	4
2 Procedure	5
2.1 Overview of Procedure	5
2.2 Project Set Up	7
2.3 Basic Scans	9
2.4 Vulnerability Scan	11
2.5 Generating Scan Report	14
3 Discussion	15
3.1 General Discussion	15
3.2 Future Work	15
References	16
Appendices	18
Appendix A - Vulnerability Scan Output	18
Appendix B - Python Nmap Script	36

1 INTRODUCTION

1.1 BACKGROUND

In today's digital age, it is vital for organizations and businesses to automate recurring tasks in an effort to reduce manual labour. Consequentially, saving money, time and increasing efficiency.

What is automation?

The most basic definition of automation is: "The use of machines or computers instead of people to do a job", (dictionary.cambridge.org, 2023).

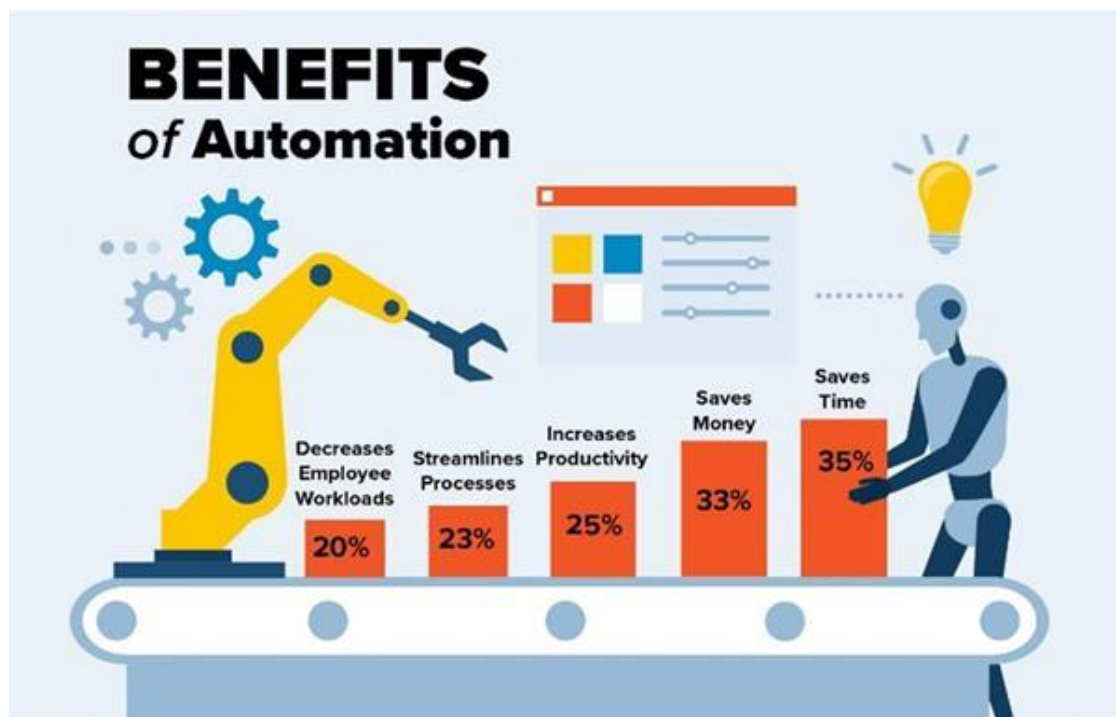


Figure 1: Benefits of Automation (www.globenewswire.com, 2022).

Automation provides many benefits. One of the main reasons for automation is decreasing time wastage and increasing productivity. Particularly to do with repetitive tasks that require a lot of time to complete. In turn, this reduces the need for extensive human manual labour and can lead to decreased employee workloads. Another benefit of automation is that it mitigates the risk of human error. Automation is beneficial for organizations and businesses as it is economical and cost-effective. As well as helping to speed up processes and improving productivity in the company.

Some examples of automation are industrial machinery, consumer electronics, escalators and many more.

Industrial machinery can aid in drastically increasing productivity as well as reducing the need for manual labour. Industrial machinery can come in many forms, robotic arms, conveyor belts, compressors and more.

On a day to day basis, automation is key to improving human lives. This is where consumer electronics come in. These include, kettles, washing machines, boilers, fridges etc. These devices save us a lot of time on a daily basis.

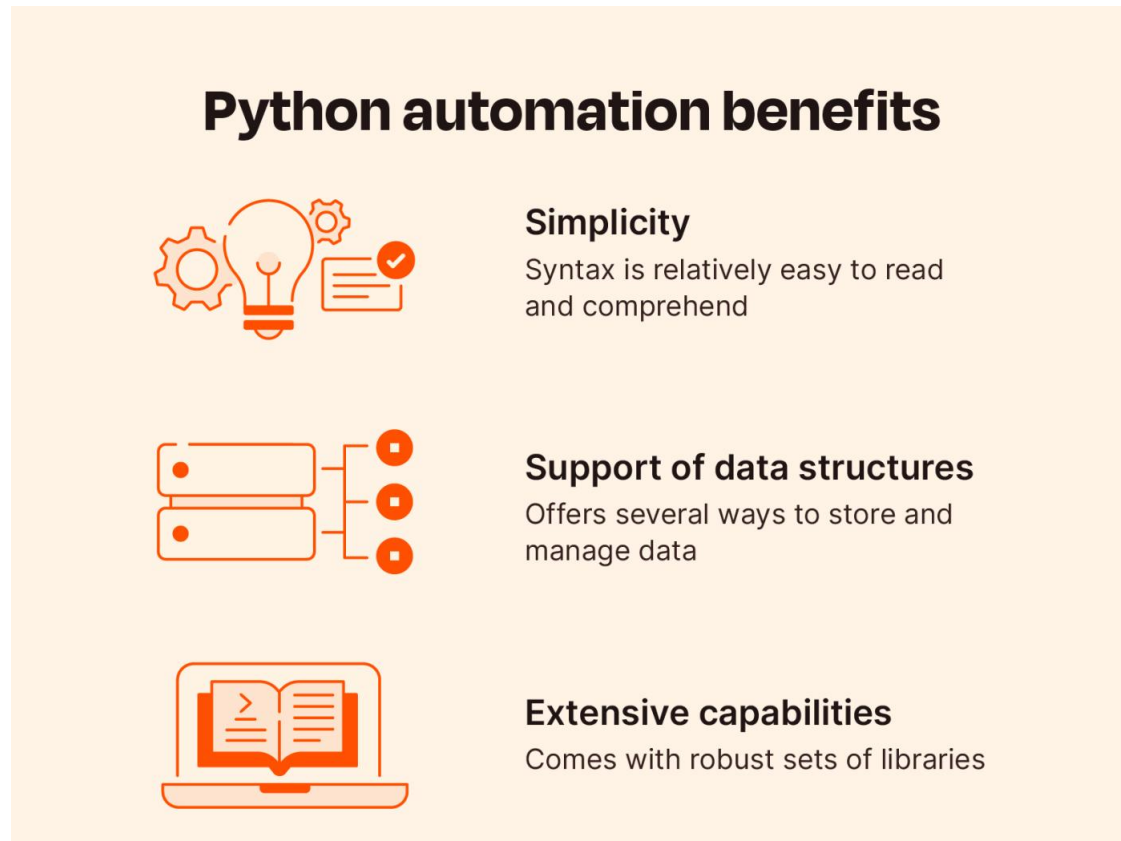


Figure 2: Benefits of Python automation(zapier.com, 2023).

Python is an object-orientated high level programming language that supports many modules, packages and libraries. Python also has a use as a scripting language and is used to tie together different components. It is fairly simple and its syntax is easy to understand.

In this report, the ethical hacking student will use python to automate a tool called Nmap. Nmap is a network scanning tool that allows the user to scan the network as well as individual devices on the network. Using this tool, users can find out information about the operating system of the device, open ports, services and more.

Nmap is used as an information gathering and fingerprinting software when testing network security.

The current problem with Nmap is that when using the software, commands need to be inputted manually in order to find information about a single device or a sub-net. Having to repeat this process multiple times on a large network can prove quite time consuming and tedious. Large networks can have tens or hundreds of sub-nets, routers, switches and devices.

With Python, the ethical hacking student is able to use the 'python-nmap' library to automate this software using a Python script. With Nmap automated, the ethical hacker could potentially scan a whole network which would include hosts, open ports, operating systems, network state with just running a single python script. Alternative to typing each and every command manually and waiting for the software to print scan results. This is a much more efficient process and is extremely beneficial in the field of cyber-security. Saving time, money and resources.

1.2 AIMS

The aims of the project are as follows:

- Automate Nmap scanning using python scripting.
- Document development procedure.
- Discuss and reflect on the outcomes of the project.

2 PROCEDURE

2.1 OVERVIEW OF PROCEDURE

To begin the procedure, the ethical hacking student ensured Nmap and Python have been installed in their lab environment. The student used Kali Linux as their choice of operating system.

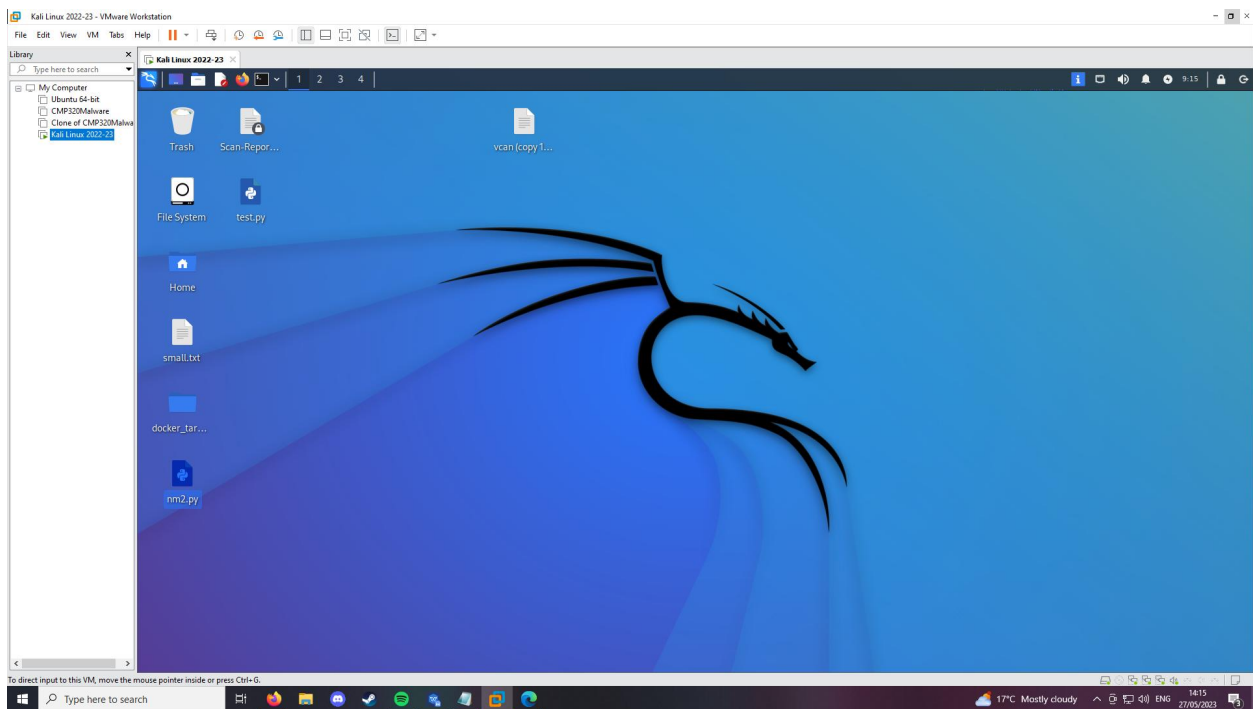


Figure 3: Kali Linux Virtual Machine

Section Overview

- Project Set Up
- Basic Scans
- Vulnerability Scan
- Scan Report Generation

The first section features the project set up. This included running the virtual environment, ensuring the system is updated as well as making sure python3 and nmap are installed on the machine. The ethical hacking student creating a new Python file with the nmap module imported in the script. The script was created with minimal user input in mind. The set up stage

covers creating the python script with arguments that have to be entered as part of running the script. This way, the user doesn't need to enter any more input into the script.

The second section features basic nmap scans on the target host. This section focused on using the nmap module library to script its functionality and print the results. Basic scans performed in this section are, host discovery scan, port scan, protocol scan, state scan as well as an operating system scan on the target machine. The objective of this section was to obtain as much information as possible about the target host and display the results to the user.

The third section covers the development of a vulnerability scan on the target host. Once the previous section was complete, the ethical hacking student had all the basic information about the target machine including its protocols, open ports, its operating system and state. At this stage, the ethical hacking student had to investigate the target host further for any potential security weaknesses and vulnerabilities.

Additionally, this section covers text file manipulation while working with large amounts of data. The ethical hacking student integrated an advanced vulnerability scan that produces a large set of results. This had to be filtered to display the most useful security vulnerabilities to the student.

The final section covers generating a scan report of the whole script. This was achieved by taking all the previous scans performed in the script and writing it to a file that can be opened and viewed by the ethical hacking student after the nmap scans were complete. This was done so that when the script was run, scan reports were generated saving the scan information. With this, the script could be run multiple times and have their own separate scan reports for every host and port range chosen by the ethical hacking student.

Tools used during development:

- VMware Workstation
- Kali Linux
- Python3
- Nmap

2.2 PROJECT SET UP

The first step in the development of the nmap-python script was to ensure the virtual machine was up to date. This was necessary before any python and nmap development could begin.



```
(kali@kali)-[~]  
$ sudo apt update && sudo apt upgrade -y
```

Figure 4: Linux update command.

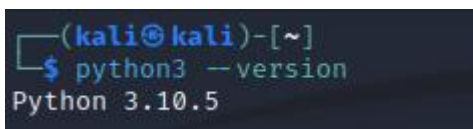
The next step in the procedure was to ensure that both python and nmap modules were installed on the virtual machine. This was performed by the ethical hacking student and the software versions were double checked.



```
(kali@kali)-[~]  
$ sudo apt install python3 python3-pip
```

Figure 5: Python installation command

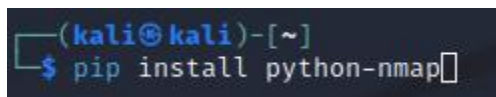
Now that python has been installed on the ethical hacking student's machine, the version of the installation can be checked.



```
(kali@kali)-[~]  
$ python3 --version  
Python 3.10.5
```

Figure 6: Python version.

After this process was complete, the 'python-nmap' python library had to be installed and imported into the script in order to be able to use the nmap scan functionality in python. This was done by the following command:



```
(kali@kali)-[~]  
$ pip install python-nmap
```

Figure 7: Python-Nmap installation.

Now that the environment setup has been complete with the installation of nmap and python including their shared python library, the python script was created and all necessary imports were included.

```
1 import nmap
2 import sys
3 import os
```

Figure 8: Script Imports.

Import nmap - This is the python-nmap library

Import sys - This helps to create arguments for the script.

Import os - This allowed for file creation and manipulation.

Before the development and usage of the python-nmap library could begin, the ethical hacking student coded arguments for the python script that had to be entered for the python script to run.

The two arguments implemented were the, 'ip address' of the target machine the script was going to scan and an argument for the, 'port range' that the ethical hacking student wished to scan. This was implemented and a print function was included to ensure the user knew what to input.

As seen by figure 9:

```
if len(sys.argv) != 3:
    print("python3 nm2.py <Target Address> <Port Range>")
    sys.exit(0)

hostaddress = sys.argv[1]
portrange = sys.argv[2]
```

Figure 9: Script arguments.

Once this was complete, the ethical hacking student started developing the python-nmap scanner.

2.3 BASIC SCANS

Now that the project has been setup, the development has been started by the ethical hacking student.

The basic scans section includes the following:

Basic Scans:

- Host Scan
- Host State Scan
- Protocol Scan
- Port Scan
- Operating System Scan

To begin, the student made a variable object referencing the nmap portscanner in the nmap library. This was named 'nmscan'.

```
nmscan=nmap.PortScanner()
```

Figure 10: Reference to the PortScanner() function.

The ethical hacker wanted to display in the script was the arguments entered by the user. This was done by printing the arguments as well as the version of nmap back to the user.

```
print("_____ " *6)
print("          Scanning Target: " +hostaddress)
print('          Nmap Version: ', nmscan.nmap_version())
print("_____ " *6)
```

Figure 11: Display of host address & nmap version.

The next step was to perform the host and state scans on the target host address. This was created using a for loop to loop through hosts and display the host names, host address and the state of the host.

```
for host in nmscan.all_hosts():
    print("Host : %s (%s)" % (targetName,hostaddress))
    print("State : %s" % nmscan[host].state())
```

Figure 12: Host and state scan.

Another for loop has been used to cycle through protocols the host is using. The protocols found were displayed to the user.

```
for proto in nmapscan[host].all_protocols():
    print("-----" * 6)
    print("Protocols : %s " % proto)
```

Figure 13: Protocol Scan.

Now that the protocol has been scanned, it was time to display open ports to the user. Another for loop has been used to scan through the range of ports specified by the second argument in the python script. The range can be freely changed to suit the range of ports the user wished to scan. Once the ports have been scanned through, open ports have been displayed to the user.

The python function sorted() has been used to display the ports neatly in two columns followed by the port and its state.

```
lport = nmapscan[host][proto].keys()
sorted(lport)
for port in lport:
    print("Port : %s \t State : %s " %(port,nmapscan[host][proto][port]['state']))
```

Figure 14: Open port scan.

The final scan performed in this section was the Operating System scan of the target host. This step is crucial in information gathering when performing network scanning. This gives the ethical hacker a better idea of how the system functions and as a result how they can go about exploiting the target system.

The difference between this scan and the other scans performed previously in this section, is that the ethical hacker add the argument '-O' which tells nmap to scan for the operating system. This scan is then stored in a variable that the python script can access.

```
osdetect = nmapscan.scan(hostaddress, portrange, arguments='-O')
print('Operating System: ', osdetect['scan'][hostaddress]['osmatch'][0]['osclass'][1]['osfamily'])
```

Figure 15: Operating system scan.

As can be seen from the figure above, the data is stored in the 'osdetect' variable. The ethical hacker had to inspect the data returned and filter out the specific piece of information they were looking for. This can be seen by the 'osmatch', 'osclass', and 'osfamily' that returns the operating system.

Note: the operating system scan requires root permissions. As a result, the script requires this permission to run a full scan.

```

1 _____
2                               Scanning Target: 192.168.0.1
3 _____
4 Host : nowtvhub.Home (192.168.0.1)
5 State : up
6 _____
7 Protocols : tcp
8 Port : 53          State : open
9 Port : 80          State : open
10 _____
11 Operating System: Linux
12 _____

```

Figure 16: Sample output #1.

2.4 VULNERABILITY SCAN

Now that the script displays the basic scans of the target host within the chosen port range, the next step is to scan the target host for potential vulnerabilities. This give the ethical hacking student an idea of potential weaknesses that can be exploited if performing a penetration test. Same as before, the output of this scan is stored in a variable called 'vulner'.

```
vulner = nmapscan.scan(hostaddress, portrange, arguments='--script vuln -sV -T4')
```

Figure 17: Vulnerability scan.

To perform a vulnerability scan, the ethical hacking student has used another script called '--script vuln' by calling it in the additional arguments needed for this scan (nmap.org/nsedoc/categories/vuln.html, 2023).

This script that can be found on the nmap documentation page incorporates other known vulnerabilities and scans the target host for each of them to check if the host is vulnerable.

```
try:
    with open('vcan.txt', 'w') as vscan:
        vscan.write(str(vulner))
        #vscan.close()
except FileNotFoundError:
    print("The directory does not exist!")
```

Figure 18: Vulnerability scan output into a text file.

As can be seen by figure 18, the results of the vulnerability scan is written into a file called 'vcan.txt'. This step was necessary as the output of this scan is quite large and featured a lot of information about potential vulnerabilities and weaknesses. An example vulnerability scan output can be seen in Appendix A - Vulnerability Scan Output.

This vulnerability output was quite large and lacked any formatting which made data extraction from the text file almost impossible. The next step in the procedure was to format the data within the text file and then extract the most useful information.

```
with open('vcan.txt', 'r') as vscan:
    raw_data = vscan.read()
    formatted_data = raw_data.replace('\n', '\n').replace('  ', '')
```

Figure 19: Formatting text file.

A few things was done at this stage. The ethical hacking student first opened the file again in read mode signified by the 'r' attribute. Then the file was read and saved to a variable called 'raw_data'.

Raw_data was accessed and wrongly formatted newline characters were replaced with formatted new line characters which formatted the file to have newlines. This made the data stored in this file much more presentable and allowed the student to filter the file by line. Double white spaces were deleted in the file as there was no use for them. This was all done by the replace() function.

```
with open('vcan.txt', 'w') as vscan:
    vscan.write(formatted_data)
    #vscan.close()
```

Figure 20: Formatting text file overwritten in the file.

The formatted raw data was then overwritten in the same text file as seen by figure 20. Now that this step was complete, the file can be accessed and filtered based on the vulnerabilities found in the file and shown back to the user.

```
with open('vcan.txt','r') as vscan:
    lines = [line.strip() for line in vscan.readlines()]
    for i, line in enumerate(lines):
        if line.startswith("VULNERABLE:"):
            print(lines[i]+'\\n',lines[i+1]+'\\n', lines[i+2]+'\\n', lines[i+3]+'\\n', lines[i+4],lines[i+5],lines[i+6], lines[i+7])
```

Figure 21: File filtered for vulnerabilities.

The file is opened again with the read attribute. The file is read line by line using the `readlines()` function. A for loop was used to cycle through the newly formatted file line by line to find the keyword '**VULNERABLE:**'.

Once the loop find the keyword, it printed out 7 lines below the initial line. This was for the purpose to display all the information in the paragraph below the keyword. This was key as these lines included the type of vulnerability and the description of how the host can be exploited in these specific ways. This method extracted every vulnerability present in the vulnerability scan output and displayed them to the user.

```
Scanning Target: 192.168.0.1
Host : nowtvhub.Home (192.168.0.1)
State : up

Protocols : tcp
Port : 83      State : open
Port : 80      State : open

Operating System: Linux

Performing Vulnerability Scan

VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
Id:CVE-2007-5708
Slowloris tries to keep many connections to the target web server open and holdthem open as long as possible.It accomplishes this by opening connections tothe target web server and sending a partial request.
By doing so, it starvesthe http server's resources causing Denial Of Service.

VULNERABLE:
Authentication bypass by HTTP verb tampering
State: VULNERABLE (Exploitable)
This web server contains password protected resources vulnerable to authentication bypass
vulnerabilities via HTTP verb tampering. This is often found in web servers that only limit access to thecommon HTTP methods and in misconfigured .htaccess files.Extra information:
```

Figure 22: Sample output #2.

2.5 GENERATING SCAN REPORT

The last part of the procedure features taking all the scans and outputs and creating a Scan-Report document that saved the scan data and can be viewed by opening a text file.

```
report = open("Scan-Report_"+hostaddress+"_"+portrange, "w")
```

Figure 23: File created for the scan report.

As can be seen by figure 23, the file is saved with the arguments in mind. This way the file won't overwrite the data when performing additional scans on other hosts or port ranges. Every scan will be named differently.

```
report.write("Host : %s (%s)" % (targetName, hostaddress)+"\n")  
report.write("State : %s" % nmscan[host].state()+"\n")
```

Figure 24: Data written into the file.

For every scan performed during the procedure of the nmap-python scan, the results of each and every scan has been written into the file and saved.

```
report.close()  
os.remove('vcan.txt')
```

Figure 25: File closed and other file removed.

The last step in the procedure was to close the report once the python script was executed. Additionally, the file used previously to store raw data from the vulnerability scan has been deleted. There was no further use for it as the ethical hacking student filtered and written the results into the scan report. Full python-nmap script can be found in Appendix B - Python Nmap Script.

3 DISCUSSION

3.1 GENERAL DISCUSSION

Throughout the procedure, the ethical hacking student has implemented nmap scan components step by step to create a fully functioning nmap integrated python automation.

The python automation features all the most important information about the target host when it comes to fingerprinting a target machine. This can later lead to performing a full penetration test of a network.

Given the field of ethical hacking, automating manual tasks such as scanning host machines can save a lot of time when working in the field of cyber-security.

The aims of the project have been met. Nmap scanning has been automated by the ethical hacking student by using python scripting and integrating the python-nmap library. The entire development process of the python script has been documented in the procedure part of the report with clear indication of each stage of development. The Python script features multiple target host scans including the host scan, protocol scan, port scan, operating scan as well as a vulnerability scan of the target host. The script generates a scan report of the target host.

The ethical hacking student will propose suitable improvements and potential additions in the following section.

3.2 FUTURE WORK

Given more time and resources, the ethical hacking student would build upon the existing nmap automation script. This would include more advanced scans that would include information about the services running on each port as well as the service versions displayed. The ethical hacking student would take into account the performance of the script and attempt to optimize it as much as possible.

Another improvement given more time, the script would be tested for running scans on multiple hosts and sub-nets to cover as many machines as possible with a single python script.

REFERENCES

For URLs:

- Ibm.com. 2023. Automation. [ONLINE] Available at: <https://www.ibm.com/topics/automation>. [Accessed 27th May 2023]
- Dictionary.cambridge.org. 2023. Automation. [ONLINE] Available at: <https://dictionary.cambridge.org/dictionary/english/automation>. [Accessed 27th May 2023]
- globenewswire.com. 2022. Automation-Shouldn-t-Spook-Companies-and-Employees-Amidst-Ongoing-Labour-Shortages. [ONLINE] Available at: <https://www.globenewswire.com/en/news-release/2022/10/26/2541881/0/en/Automation-Shouldn-t-Spook-Companies-and-Employees-Amidst-Ongoing-Labour-Shortages.html> [Accessed 27th May 2023]
- phixflow.com. 2023. why-automation-is-vital-for-the-future-business. [ONLINE] Available at: <https://www.phixflow.com/why-automation-is-vital-for-the-future-business/>. [27th May 2023]
- analyticsvidhya.com. 2023. python-automation-guide-automate-everything-with-python. [ONLINE] Available at: <https://www.analyticsvidhya.com/blog/2023/04/python-automation-guide-automate-everything-with-python/>. [27th May 2023]
- zapier.com. 2023. python-automation. [ONLINE] Available at: <https://zapier.com/blog/python-automation/>. [27th May 2023]
- freecodecamp.org. 2023. enhance-nmap-with-python. [ONLINE] Available at: - <https://www.freecodecamp.org/news/enhance-nmap-with-python/>. [27th May 2023]

- python.org. 2023. blurb. [ONLINE] Available at:
<https://www.python.org/doc/essays/blurb>. [27th May 2023]
- pypi.org. 2023. python3-nmap. [ONLINE] Available at:
<https://pypi.org/project/python3-nmap>. [27th May 2023]
- nmap.org. 2023. vuln.html. [ONLINE] Available at:
<https://nmap.org/nsedoc/categories/vuln.html>. [27th May 2023]

APPENDICES

APPENDIX A - VULNERABILITY SCAN OUTPUT

```
{'nmap': {'command_line': 'nmap -oX - -p 1-100 --script vuln -sV -T4
192.168.0.1', 'scaninfo': {'tcp': {'method': 'syn', 'services': '1-
100'}}}, 'scanstats': {'timestr': 'Thu May 25 14:15:38 2023',
'elapsed': '555.81', 'uphosts': '1', 'downhosts': '0', 'totalhosts':
'1'}}, 'scan': {'192.168.0.1': {'hostnames': [{'name':
'nowtvhub.Home', 'type': 'PTR'}]}, 'addresses': {'ipv4':
'192.168.0.1'}, 'vendor': {}, 'status': {'state': 'up', 'reason':
'reset'}, 'tcp': {53: {'state': 'open', 'reason': 'syn-ack', 'name':
'tcpwrapped', 'product': '', 'version': '', 'extrainfo': '', 'conf':
'8', 'cpe': ''}, 80: {'state': 'open', 'reason': 'syn-ack', 'name':
'http', 'product': 'BSkyB router', 'version': '', 'extrainfo': '',
'conf': '10', 'cpe': ''}, 'script': {'http-csrf': 'YnSpidering
limited to: maxdepth=3; maxpagecount=20; withinhost=nowtvhub.homeYn
Found the following possible CSRF vulnerabilities: Yn      Yn      Path:
http://nowtvhub.home:80/Yn      Form id: Yn      Form action:
Now_TV_rebootinfo.cgiYn      Yn      Path:
http://nowtvhub.home:80/Now_TV_index.htmlYn      Form id: Yn      Form
action: Now_TV_rebootinfo.cgiYn      Yn      Path:
http://nowtvhub.home:80/Now_TV_logout.htmlYn      Form id: Yn      Form
action: Now_TV_index.htmlYn', 'http-enum': 'Yn /repos/: Possible
code repository (401 Unauthorised)Yn /repo/: Possible code
repository (401 Unauthorised)Yn /svn/: Possible code repository
(401 Unauthorised)Yn /cvs/: Possible code repository (401
Unauthorised)Yn /backup/: Possible backup (401 Unauthorised)Yn
/backups/: Possible backup (401 Unauthorised)Yn /bak/: Possible
backup (401 Unauthorised)Yn /back/: Possible backup (401
Unauthorised)Yn /cache/backup/: Possible backup (401
Unauthorised)Yn /admin/backup/: Possible backup (401
Unauthorised)Yn /dbbackup.txt: Possible backup (401 Unauthorised)Yn
/example/: Sample scripts (401 Unauthorised)Yn /examples/: Sample
scripts (401 Unauthorised)Yn /iissamples/: Sample scripts (401
Unauthorised)Yn /j2eeexamples/: Sample scripts (401 Unauthorised)Yn
/j2eeexamplesjsp/: Sample scripts (401 Unauthorised)Yn /sample/:
Sample scripts (401 Unauthorised)Yn /ncsample/: Sample scripts (401
Unauthorised)Yn /fpsample/: Sample scripts (401 Unauthorised)Yn
/cmsample/: Sample scripts (401 Unauthorised)Yn /samples/: Sample
scripts (401 Unauthorised)Yn /Portal0000.htm: SCADA Siemens PCS7
(401 Unauthorised)Yn /actuator/: Spring Boot Actuator endpoint (401
Unauthorised)Yn /auditevents/: Spring Boot Actuator endpoint (401
Unauthorised)Yn /autoconfig/: Spring Boot Actuator endpoint (401
Unauthorised)Yn /beans/: Spring Boot Actuator endpoint (401
Unauthorised)Yn /configprops/: Spring Boot Actuator endpoint (401
Unauthorised)Yn /env/: Spring Boot Actuator endpoint (401
Unauthorised)Yn /flyway/: Spring Boot Actuator endpoint (401
Unauthorised)Yn /health/: Spring Boot Actuator endpoint (401
```

```

Unauthorised)¥n /healthcheck/: Spring Boot Actuator endpoint (401
Unauthorised)¥n /healthchecks/: Spring Boot Actuator endpoint (401
Unauthorised)¥n /loggers/: Spring Boot Actuator endpoint (401
Unauthorised)¥n /liquibase/: Spring Boot Actuator endpoint (401
Unauthorised)¥n /metrics/: Spring Boot Actuator endpoint (401
Unauthorised)¥n /mappings/: Spring Boot Actuator endpoint (401
Unauthorised)¥n /trace/: Spring Boot Actuator endpoint (401
Unauthorised)¥n /heapdump/: Spring MVC Endpoint (401
Unauthorised)¥n /jolokia/: Spring MVC Endpoint (401 Unauthorised)¥n
/changelog.txt: Interesting, a changelog. (401 Unauthorised)¥n
/tinyMCE/changelog.txt: Interesting, a changelog. (401
Unauthorised)¥n /readme.html: Interesting, a readme. (401
Unauthorised)¥n /pligg/readme.html: Interesting, a readme. (401
Unauthorised)¥n /digg/readme.html: Interesting, a readme. (401
Unauthorised)¥n /news/readme.html: Interesting, a readme. (401
Unauthorised)¥n /db/: BlogWorx Database (401 Unauthorised)¥n
/typo3/README.txt: Typo3 Installation (401 Unauthorised)¥n
/t3lib/README.txt: Typo3 Installation (401 Unauthorised)¥n
/README.txt: Interesting, a readme. (401 Unauthorised)¥n /0/:
Potentially interesting folder (401 Unauthorised)¥n /1/:
Potentially interesting folder (401 Unauthorised)¥n /2/:
Potentially interesting folder (401 Unauthorised)¥n /3/:
Potentially interesting folder (401 Unauthorised)¥n /4/:
Potentially interesting folder (401 Unauthorised)¥n /5/:
Potentially interesting folder (401 Unauthorised)¥n /6/:
Potentially interesting folder (401 Unauthorised)¥n /7/:
Potentially interesting folder (401 Unauthorised)¥n /8/:
Potentially interesting folder (401 Unauthorised)¥n /9/:
Potentially interesting folder (401 Unauthorised)¥n /10/:
Potentially interesting folder (401 Unauthorised)¥n /a/:
Potentially interesting folder (401 Unauthorised)¥n /b/:
Potentially interesting folder (401 Unauthorised)¥n /c/:
Potentially interesting folder (401 Unauthorised)¥n /d/:
Potentially interesting folder (401 Unauthorised)¥n /e/:
Potentially interesting folder (401 Unauthorised)¥n /f/:
Potentially interesting folder (401 Unauthorised)¥n /g/:
Potentially interesting folder (401 Unauthorised)¥n /h/:
Potentially interesting folder (401 Unauthorised)¥n /i/:
Potentially interesting folder (401 Unauthorised)¥n /j/:
Potentially interesting folder (401 Unauthorised)¥n /k/:
Potentially interesting folder (401 Unauthorised)¥n /l/:
Potentially interesting folder (401 Unauthorised)¥n /m/:
Potentially interesting folder (401 Unauthorised)¥n /n/:
Potentially interesting folder (401 Unauthorised)¥n /o/:
Potentially interesting folder (401 Unauthorised)¥n /p/:
Potentially interesting folder (401 Unauthorised)¥n /q/:
Potentially interesting folder (401 Unauthorised)¥n /r/:
Potentially interesting folder (401 Unauthorised)¥n /s/:
Potentially interesting folder (401 Unauthorised)¥n /t/:
Potentially interesting folder (401 Unauthorised)¥n /u/:
Potentially interesting folder (401 Unauthorised)¥n /v/:
Potentially interesting folder (401 Unauthorised)¥n /w/:

```

Potentially interesting folder (401 Unauthorised)¥n /x/:
 Potentially interesting folder (401 Unauthorised)¥n /y/:
 Potentially interesting folder (401 Unauthorised)¥n /z/:
 Potentially interesting folder (401 Unauthorised)¥n /accesso/:
 Potentially interesting folder (401 Unauthorised)¥n /access/:
 Potentially interesting folder (401 Unauthorised)¥n /accesswatch/:
 Potentially interesting folder (401 Unauthorised)¥n /acciones/:
 Potentially interesting folder (401 Unauthorised)¥n /account/:
 Potentially interesting folder (401 Unauthorised)¥n /accounting/:
 Potentially interesting folder (401 Unauthorised)¥n /active/:
 Potentially interesting folder (401 Unauthorised)¥n /activex/:
 Potentially interesting folder (401 Unauthorised)¥n /admcgi/:
 Potentially interesting folder (401 Unauthorised)¥n /admisapi/:
 Potentially interesting folder (401 Unauthorised)¥n /AdvWebAdmin/:
 Potentially interesting folder (401 Unauthorised)¥n /agentes/:
 Potentially interesting folder (401 Unauthorised)¥n /Agent/:
 Potentially interesting folder (401 Unauthorised)¥n /Agents/:
 Potentially interesting folder (401 Unauthorised)¥n /AlbumArt_/:
 Potentially interesting folder (401 Unauthorised)¥n /AlbumArt/:
 Potentially interesting folder (401 Unauthorised)¥n /Album/:
 Potentially interesting folder (401 Unauthorised)¥n /allow/:
 Potentially interesting folder (401 Unauthorised)¥n /analog/:
 Potentially interesting folder (401 Unauthorised)¥n /anthill/:
 Potentially interesting folder (401 Unauthorised)¥n /apache/:
 Potentially interesting folder (401 Unauthorised)¥n /api/:
 Potentially interesting folder (401 Unauthorised)¥n /api-docs/:
 Potentially interesting folder (401 Unauthorised)¥n /app/:
 Potentially interesting folder (401 Unauthorised)¥n /applets/:
 Potentially interesting folder (401 Unauthorised)¥n /appl/:
 Potentially interesting folder (401 Unauthorised)¥n /application/:
 Potentially interesting folder (401 Unauthorised)¥n /applications/:
 Potentially interesting folder (401 Unauthorised)¥n /applmgr/:
 Potentially interesting folder (401 Unauthorised)¥n /apply/:
 Potentially interesting folder (401 Unauthorised)¥n /appsec/:
 Potentially interesting folder (401 Unauthorised)¥n /apps/:
 Potentially interesting folder (401 Unauthorised)¥n /archive/:
 Potentially interesting folder (401 Unauthorised)¥n /archives/:
 Potentially interesting folder (401 Unauthorised)¥n /ar/:
 Potentially interesting folder (401 Unauthorised)¥n /asa/:
 Potentially interesting folder (401 Unauthorised)¥n /asp/:
 Potentially interesting folder (401 Unauthorised)¥n /atc/:
 Potentially interesting folder (401 Unauthorised)¥n /aut/:
 Potentially interesting folder (401 Unauthorised)¥n /authadmin/:
 Potentially interesting folder (401 Unauthorised)¥n /auth/:
 Potentially interesting folder (401 Unauthorised)¥n /author/:
 Potentially interesting folder (401 Unauthorised)¥n /authors/:
 Potentially interesting folder (401 Unauthorised)¥n /aw/:
 Potentially interesting folder (401 Unauthorised)¥n /ayuda/:
 Potentially interesting folder (401 Unauthorised)¥n /b2-include/:
 Potentially interesting folder (401 Unauthorised)¥n /backend/:
 Potentially interesting folder (401 Unauthorised)¥n /bad/:
 Potentially interesting folder (401 Unauthorised)¥n /banca/:

Potentially interesting folder (401 Unauthorised)¥n /banco/:

Potentially interesting folder (401 Unauthorised)¥n /bank/:

Potentially interesting folder (401 Unauthorised)¥n /banner01/:

Potentially interesting folder (401 Unauthorised)¥n /banner/:

Potentially interesting folder (401 Unauthorised)¥n /banners/:

Potentially interesting folder (401 Unauthorised)¥n /bar/:

Potentially interesting folder (401 Unauthorised)¥n /batch/:

Potentially interesting folder (401 Unauthorised)¥n /bb-dnbd/:

Potentially interesting folder (401 Unauthorised)¥n /bbv/:

Potentially interesting folder (401 Unauthorised)¥n /bdata/:

Potentially interesting folder (401 Unauthorised)¥n /bdatos/:

Potentially interesting folder (401 Unauthorised)¥n /beta/:

Potentially interesting folder (401 Unauthorised)¥n /billpay/:

Potentially interesting folder (401 Unauthorised)¥n /bin/:

Potentially interesting folder (401 Unauthorised)¥n /binaries/:

Potentially interesting folder (401 Unauthorised)¥n /binary/:

Potentially interesting folder (401 Unauthorised)¥n /boadmin/:

Potentially interesting folder (401 Unauthorised)¥n /boot/:

Potentially interesting folder (401 Unauthorised)¥n /bottom/:

Potentially interesting folder (401 Unauthorised)¥n /browse/:

Potentially interesting folder (401 Unauthorised)¥n /browser/:

Potentially interesting folder (401 Unauthorised)¥n /bsd/:

Potentially interesting folder (401 Unauthorised)¥n /btauxdir/:

Potentially interesting folder (401 Unauthorised)¥n /bug/:

Potentially interesting folder (401 Unauthorised)¥n /bugs/:

Potentially interesting folder (401 Unauthorised)¥n /bugzilla/:

Potentially interesting folder (401 Unauthorised)¥n /buy/:

Potentially interesting folder (401 Unauthorised)¥n /buynow/:

Potentially interesting folder (401 Unauthorised)¥n /cached/:

Potentially interesting folder (401 Unauthorised)¥n /cache/:

Potentially interesting folder (401 Unauthorised)¥n /cache-stats/:

Potentially interesting folder (401 Unauthorised)¥n /caja/:

Potentially interesting folder (401 Unauthorised)¥n /card/:

Potentially interesting folder (401 Unauthorised)¥n /cards/:

Potentially interesting folder (401 Unauthorised)¥n /cart/:

Potentially interesting folder (401 Unauthorised)¥n /cash/:

Potentially interesting folder (401 Unauthorised)¥n /caspsamp/:

Potentially interesting folder (401 Unauthorised)¥n /catalog/:

Potentially interesting folder (401 Unauthorised)¥n /cbi-bin/:

Potentially interesting folder (401 Unauthorised)¥n /ccard/:

Potentially interesting folder (401 Unauthorised)¥n /ccards/:

Potentially interesting folder (401 Unauthorised)¥n /cd-cgi/:

Potentially interesting folder (401 Unauthorised)¥n /cd/:

Potentially interesting folder (401 Unauthorised)¥n /cdrom/:

Potentially interesting folder (401 Unauthorised)¥n /ce_html/:

Potentially interesting folder (401 Unauthorised)¥n /cert/:

Potentially interesting folder (401 Unauthorised)¥n /certificado/:

Potentially interesting folder (401 Unauthorised)¥n /certificate/:

Potentially interesting folder (401 Unauthorised)¥n /cfappman/:

Potentially interesting folder (401 Unauthorised)¥n /cfdocs/:

Potentially interesting folder (401 Unauthorised)¥n /cfide/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-914/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-915/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-auth/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-bin2/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-bin/:

Potentially interesting folder (401 Unauthorised)¥n /cgibin/:

Potentially interesting folder (401 Unauthorised)¥n /cgi.cgi/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-csc/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-exe/:

Potentially interesting folder (401 Unauthorised)¥n /cgi/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-home/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-lib/:

Potentially interesting folder (401 Unauthorised)¥n /cgilib/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-local/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-perl/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-scripts/:

Potentially interesting folder (401 Unauthorised)¥n /cgiscripts/:

Potentially interesting folder (401 Unauthorised)¥n /cgis/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-shl/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-shop/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-sys/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-weddico/:

Potentially interesting folder (401 Unauthorised)¥n /cgi-win/:

Potentially interesting folder (401 Unauthorised)¥n /cgiwin/:

Potentially interesting folder (401 Unauthorised)¥n /class/:

Potentially interesting folder (401 Unauthorised)¥n /classes/:

Potentially interesting folder (401 Unauthorised)¥n /cliente/:

Potentially interesting folder (401 Unauthorised)¥n /clientes/:

Potentially interesting folder (401 Unauthorised)¥n /client/:

Potentially interesting folder (401 Unauthorised)¥n /clients/:

Potentially interesting folder (401 Unauthorised)¥n /cm/:

Potentially interesting folder (401 Unauthorised)¥n /cobalt-images/:

Potentially interesting folder (401 Unauthorised)¥n /code/:

Potentially interesting folder (401 Unauthorised)¥n /com/:

Potentially interesting folder (401 Unauthorised)¥n /comments/:

Potentially interesting folder (401 Unauthorised)¥n /common/:

Potentially interesting folder (401 Unauthorised)¥n /communicator/:

Potentially interesting folder (401 Unauthorised)¥n /company/:

Potentially interesting folder (401 Unauthorised)¥n /comp/:

Potentially interesting folder (401 Unauthorised)¥n /compra/:

Potentially interesting folder (401 Unauthorised)¥n /compras/:

Potentially interesting folder (401 Unauthorised)¥n /compressed/:

Potentially interesting folder (401 Unauthorised)¥n /conecta/:

Potentially interesting folder (401 Unauthorised)¥n /conf/:

Potentially interesting folder (401 Unauthorised)¥n /config/:

Potentially interesting folder (401 Unauthorised)¥n /configs/:

Potentially interesting folder (401 Unauthorised)¥n /configure/:

Potentially interesting folder (401 Unauthorised)¥n /connect/:

Potentially interesting folder (401 Unauthorised)¥n /console/:

Potentially interesting folder (401 Unauthorised)¥n /contact/:

Potentially interesting folder (401 Unauthorised)¥n /contacts/:

Potentially interesting folder (401 Unauthorised)¥n /content/:

Potentially interesting folder (401 Unauthorised)¥n /content.ie5/:

Potentially interesting folder (401 Unauthorised)¥n /controlpanel/:

Potentially interesting folder (401 Unauthorised)¥n /core/:

Potentially interesting folder (401 Unauthorised)¥n /corp/:

Potentially interesting folder (401 Unauthorised)¥n /correo/:

Potentially interesting folder (401 Unauthorised)¥n /counter/:

Potentially interesting folder (401 Unauthorised)¥n /credit/:

Potentially interesting folder (401 Unauthorised)¥n /cron/:

Potentially interesting folder (401 Unauthorised)¥n /crons/:

Potentially interesting folder (401 Unauthorised)¥n /crypto/:

Potentially interesting folder (401 Unauthorised)¥n /CS/:

Potentially interesting folder (401 Unauthorised)¥n /csr/:

Potentially interesting folder (401 Unauthorised)¥n /css/:

Potentially interesting folder (401 Unauthorised)¥n /cuenta/:

Potentially interesting folder (401 Unauthorised)¥n /cuentas/:

Potentially interesting folder (401 Unauthorised)¥n /currency/:

Potentially interesting folder (401 Unauthorised)¥n /cust/:

Potentially interesting folder (401 Unauthorised)¥n /customer/:

Potentially interesting folder (401 Unauthorised)¥n /customers/:

Potentially interesting folder (401 Unauthorised)¥n /custom/:

Potentially interesting folder (401 Unauthorised)¥n /CVS/:

Potentially interesting folder (401 Unauthorised)¥n /cvsweb/:

Potentially interesting folder (401 Unauthorised)¥n /cybercash/:

Potentially interesting folder (401 Unauthorised)¥n /darkportal/:

Potentially interesting folder (401 Unauthorised)¥n /database/:

Potentially interesting folder (401 Unauthorised)¥n /databases/:

Potentially interesting folder (401 Unauthorised)¥n /datafiles/:

Potentially interesting folder (401 Unauthorised)¥n /dat/:

Potentially interesting folder (401 Unauthorised)¥n /data/:

Potentially interesting folder (401 Unauthorised)¥n /dato/:

Potentially interesting folder (401 Unauthorised)¥n /datos/:

Potentially interesting folder (401 Unauthorised)¥n /db/:

Potentially interesting folder (401 Unauthorised)¥n /dbase/:

Potentially interesting folder (401 Unauthorised)¥n /dcforum/:

Potentially interesting folder (401 Unauthorised)¥n /ddreport/:

Potentially interesting folder (401 Unauthorised)¥n /ddrint/:

Potentially interesting folder (401 Unauthorised)¥n /debug/:

Potentially interesting folder (401 Unauthorised)¥n /debugs/:

Potentially interesting folder (401 Unauthorised)¥n /default/:

Potentially interesting folder (401 Unauthorised)¥n /deleted/:

Potentially interesting folder (401 Unauthorised)¥n /delete/:

Potentially interesting folder (401 Unauthorised)¥n /demoauct/:

Potentially interesting folder (401 Unauthorised)¥n /demomall/:

Potentially interesting folder (401 Unauthorised)¥n /demo/:

Potentially interesting folder (401 Unauthorised)¥n /demos/:

Potentially interesting folder (401 Unauthorised)¥n /demouser/:

Potentially interesting folder (401 Unauthorised)¥n /deny/:

Potentially interesting folder (401 Unauthorised)¥n /derived/:

Potentially interesting folder (401 Unauthorised)¥n /design/:

Potentially interesting folder (401 Unauthorised)¥n /dev/:

Potentially interesting folder (401 Unauthorised)¥n /devel/:

Potentially interesting folder (401 Unauthorised)¥n /development/:

Potentially interesting folder (401 Unauthorised)¥n /directories/:

Potentially interesting folder (401 Unauthorised)¥n /directory/:
Potentially interesting folder (401 Unauthorised)¥n
/directorymanager/: Potentially interesting folder (401
Unauthorised)¥n /dir/: Potentially interesting folder (401
Unauthorised)¥n /dl/: Potentially interesting folder (401
Unauthorised)¥n /dm/: Potentially interesting folder (401
Unauthorised)¥n /DMR/: Potentially interesting folder (401
Unauthorised)¥n /dms0/: Potentially interesting folder (401
Unauthorised)¥n /dmsdump/: Potentially interesting folder (401
Unauthorised)¥n /dms/: Potentially interesting folder (401
Unauthorised)¥n /dnn/: Potentially interesting folder (401
Unauthorised)¥n /doc1/: Potentially interesting folder (401
Unauthorised)¥n /doc/: Potentially interesting folder (401
Unauthorised)¥n /doc-html/: Potentially interesting folder (401
Unauthorised)¥n /docs1/: Potentially interesting folder (401
Unauthorised)¥n /docs/: Potentially interesting folder (401
Unauthorised)¥n /DocuColor/: Potentially interesting folder (401
Unauthorised)¥n /documentation/: Potentially interesting folder
(401 Unauthorised)¥n /document/: Potentially interesting folder
(401 Unauthorised)¥n /documents/: Potentially interesting folder
(401 Unauthorised)¥n /dotnetnuke/: Potentially interesting folder
(401 Unauthorised)¥n /down/: Potentially interesting folder (401
Unauthorised)¥n /download/: Potentially interesting folder (401
Unauthorised)¥n /downloads/: Potentially interesting folder (401
Unauthorised)¥n /dump/: Potentially interesting folder (401
Unauthorised)¥n /durep/: Potentially interesting folder (401
Unauthorised)¥n /easylog/: Potentially interesting folder (401
Unauthorised)¥n /eforum/: Potentially interesting folder (401
Unauthorised)¥n /ejemplo/: Potentially interesting folder (401
Unauthorised)¥n /ejemplos/: Potentially interesting folder (401
Unauthorised)¥n /emailclass/: Potentially interesting folder (401
Unauthorised)¥n /email/: Potentially interesting folder (401
Unauthorised)¥n /employees/: Potentially interesting folder (401
Unauthorised)¥n /empoyees/: Potentially interesting folder (401
Unauthorised)¥n /empris/: Potentially interesting folder (401
Unauthorised)¥n /enter/: Potentially interesting folder (401
Unauthorised)¥n /envia/: Potentially interesting folder (401
Unauthorised)¥n /enviamail/: Potentially interesting folder (401
Unauthorised)¥n /error.html: Potentially interesting folder (401
Unauthorised)¥n /error/: Potentially interesting folder (401
Unauthorised)¥n /errors/: Potentially interesting folder (401
Unauthorised)¥n /es/: Potentially interesting folder (401
Unauthorised)¥n /estmt/: Potentially interesting folder (401
Unauthorised)¥n /etc/: Potentially interesting folder (401
Unauthorised)¥n /etcpasswd/: Potentially interesting folder (401
Unauthorised)¥n /excel/: Potentially interesting folder (401
Unauthorised)¥n /exc/: Potentially interesting folder (401
Unauthorised)¥n /exchange/: Potentially interesting folder (401
Unauthorised)¥n /exchweb/: Potentially interesting folder (401
Unauthorised)¥n /exec/: Potentially interesting folder (401
Unauthorised)¥n /exe/: Potentially interesting folder (401
Unauthorised)¥n /exit/: Potentially interesting folder (401

Unauthorised)¥n /export/: Potentially interesting folder (401
Unauthorised)¥n /external/: Potentially interesting folder (401
Unauthorised)¥n /extranet/: Potentially interesting folder (401
Unauthorised)¥n /failure/: Potentially interesting folder (401
Unauthorised)¥n /fbbsd/: Potentially interesting folder (401
Unauthorised)¥n /fcgi-bin/: Potentially interesting folder (401
Unauthorised)¥n /fcgi/: Potentially interesting folder (401
Unauthorised)¥n /features/: Potentially interesting folder (401
Unauthorised)¥n /fileadmin/: Potentially interesting folder (401
Unauthorised)¥n /file/: Potentially interesting folder (401
Unauthorised)¥n /filemanager/: Potentially interesting folder (401
Unauthorised)¥n /files/: Potentially interesting folder (401
Unauthorised)¥n /find/: Potentially interesting folder (401
Unauthorised)¥n /flash/: Potentially interesting folder (401
Unauthorised)¥n /foldoc/: Potentially interesting folder (401
Unauthorised)¥n /foobar/: Potentially interesting folder (401
Unauthorised)¥n /foo/: Potentially interesting folder (401
Unauthorised)¥n /form/: Potentially interesting folder (401
Unauthorised)¥n /forms/: Potentially interesting folder (401
Unauthorised)¥n /formsmgr/: Potentially interesting folder (401
Unauthorised)¥n /form-totaller/: Potentially interesting folder
(401 Unauthorised)¥n /foto/: Potentially interesting folder (401
Unauthorised)¥n /fotos/: Potentially interesting folder (401
Unauthorised)¥n /fpadmin/: Potentially interesting folder (401
Unauthorised)¥n /fpclass/: Potentially interesting folder (401
Unauthorised)¥n /fpdb/: Potentially interesting folder (401
Unauthorised)¥n /fpe/: Potentially interesting folder (401
Unauthorised)¥n /framesets/: Potentially interesting folder (401
Unauthorised)¥n /frames/: Potentially interesting folder (401
Unauthorised)¥n /frontpage/: Potentially interesting folder (401
Unauthorised)¥n /ftp/: Potentially interesting folder (401
Unauthorised)¥n /ftproot/: Potentially interesting folder (401
Unauthorised)¥n /func/: Potentially interesting folder (401
Unauthorised)¥n /function/: Potentially interesting folder (401
Unauthorised)¥n /functions/: Potentially interesting folder (401
Unauthorised)¥n /fun/: Potentially interesting folder (401
Unauthorised)¥n /general/: Potentially interesting folder (401
Unauthorised)¥n /gfx/: Potentially interesting folder (401
Unauthorised)¥n /gif/: Potentially interesting folder (401
Unauthorised)¥n /gifs/: Potentially interesting folder (401
Unauthorised)¥n /global/: Potentially interesting folder (401
Unauthorised)¥n /globals/: Potentially interesting folder (401
Unauthorised)¥n /good/: Potentially interesting folder (401
Unauthorised)¥n /graphics/: Potentially interesting folder (401
Unauthorised)¥n /grocery/: Potentially interesting folder (401
Unauthorised)¥n /guestbook/: Potentially interesting folder (401
Unauthorised)¥n /guest/: Potentially interesting folder (401
Unauthorised)¥n /guests/: Potentially interesting folder (401
Unauthorised)¥n /GXApp/: Potentially interesting folder (401
Unauthorised)¥n /HB/: Potentially interesting folder (401
Unauthorised)¥n /HBTemplates/: Potentially interesting folder (401
Unauthorised)¥n /helpdesk/: Potentially interesting folder (401

Unauthorised)Yn /help/: Potentially interesting folder (401
Unauthorised)Yn /hidden/: Potentially interesting folder (401
Unauthorised)Yn /hide/: Potentially interesting folder (401
Unauthorised)Yn /hitmatic/: Potentially interesting folder (401
Unauthorised)Yn /hit_tracker/: Potentially interesting folder (401
Unauthorised)Yn /hlstats/: Potentially interesting folder (401
Unauthorised)Yn /home/: Potentially interesting folder (401
Unauthorised)Yn /hosted/: Potentially interesting folder (401
Unauthorised)Yn /host/: Potentially interesting folder (401
Unauthorised)Yn /hostingcontroller/: Potentially interesting folder
(401 Unauthorised)Yn /hosting/: Potentially interesting folder (401
Unauthorised)Yn /hp/: Potentially interesting folder (401
Unauthorised)Yn /htbin/: Potentially interesting folder (401
Unauthorised)Yn /htdocs/: Potentially interesting folder (401
Unauthorised)Yn /ht/: Potentially interesting folder (401
Unauthorised)Yn /htm/: Potentially interesting folder (401
Unauthorised)Yn /html/: Potentially interesting folder (401
Unauthorised)Yn /http/: Potentially interesting folder (401
Unauthorised)Yn /https/: Potentially interesting folder (401
Unauthorised)Yn /hyperstat/: Potentially interesting folder (401
Unauthorised)Yn /il8n/: Potentially interesting folder (401
Unauthorised)Yn /ibank/: Potentially interesting folder (401
Unauthorised)Yn /ibill/: Potentially interesting folder (401
Unauthorised)Yn /IBMWebAS/: Potentially interesting folder (401
Unauthorised)Yn /icons/: Potentially interesting folder (401
Unauthorised)Yn /idea/: Potentially interesting folder (401
Unauthorised)Yn /ideas/: Potentially interesting folder (401
Unauthorised)Yn /I/: Potentially interesting folder (401
Unauthorised)Yn /iisadmin/: Potentially interesting folder (401
Unauthorised)Yn /image/: Potentially interesting folder (401
Unauthorised)Yn /images/: Potentially interesting folder (401
Unauthorised)Yn /imagenes/: Potentially interesting folder (401
Unauthorised)Yn /imagery/: Potentially interesting folder (401
Unauthorised)Yn /img/: Potentially interesting folder (401
Unauthorised)Yn /imp/: Potentially interesting folder (401
Unauthorised)Yn /import/: Potentially interesting folder (401
Unauthorised)Yn /impreso/: Potentially interesting folder (401
Unauthorised)Yn /inc/: Potentially interesting folder (401
Unauthorised)Yn /include/: Potentially interesting folder (401
Unauthorised)Yn /includes/: Potentially interesting folder (401
Unauthorised)Yn /incoming/: Potentially interesting folder (401
Unauthorised)Yn /index/: Potentially interesting folder (401
Unauthorised)Yn /inet/: Potentially interesting folder (401
Unauthorised)Yn /inf/: Potentially interesting folder (401
Unauthorised)Yn /info/: Potentially interesting folder (401
Unauthorised)Yn /information/: Potentially interesting folder (401
Unauthorised)Yn /in/: Potentially interesting folder (401
Unauthorised)Yn /ingresa/: Potentially interesting folder (401
Unauthorised)Yn /ingreso/: Potentially interesting folder (401
Unauthorised)Yn /install/: Potentially interesting folder (401
Unauthorised)Yn /internal/: Potentially interesting folder (401
Unauthorised)Yn /internet/: Potentially interesting folder (401

Unauthorised)Yn /intranet/: Potentially interesting folder (401
 Unauthorised)Yn /inventory/: Potentially interesting folder (401
 Unauthorised)Yn /invitado/: Potentially interesting folder (401
 Unauthorised)Yn /isapi/: Potentially interesting folder (401
 Unauthorised)Yn /j2ee/: Potentially interesting folder (401
 Unauthorised)Yn /japidoc/: Potentially interesting folder (401
 Unauthorised)Yn /java/: Potentially interesting folder (401
 Unauthorised)Yn /javascript/: Potentially interesting folder (401
 Unauthorised)Yn /javasdk/: Potentially interesting folder (401
 Unauthorised)Yn /javatest/: Potentially interesting folder (401
 Unauthorised)Yn /jave/: Potentially interesting folder (401
 Unauthorised)Yn /JBookIt/: Potentially interesting folder (401
 Unauthorised)Yn /jdbc/: Potentially interesting folder (401
 Unauthorised)Yn /job/: Potentially interesting folder (401
 Unauthorised)Yn /jrun/: Potentially interesting folder (401
 Unauthorised)Yn /jsa/: Potentially interesting folder (401
 Unauthorised)Yn /jscrip/: Potentially interesting folder (401
 Unauthorised)Yn /jserv/: Potentially interesting folder (401
 Unauthorised)Yn /js/: Potentially interesting folder (401
 Unauthorised)Yn /jslib/: Potentially interesting folder (401
 Unauthorised)Yn /jsp/: Potentially interesting folder (401
 Unauthorised)Yn /junk/: Potentially interesting folder (401
 Unauthorised)Yn /kiva/: Potentially interesting folder (401
 Unauthorised)Yn /known/: Potentially interesting folder (401
 Unauthorised)Yn /labs/: Potentially interesting folder (401
 Unauthorised)Yn /lcgi/: Potentially interesting folder (401
 Unauthorised)Yn /lib/: Potentially interesting folder (401
 Unauthorised)Yn /libraries/: Potentially interesting folder (401
 Unauthorised)Yn /library/: Potentially interesting folder (401
 Unauthorised)Yn /libro/: Potentially interesting folder (401
 Unauthorised)Yn /license/: Potentially interesting folder (401
 Unauthorised)Yn /licenses/: Potentially interesting folder (401
 Unauthorised)Yn /links/: Potentially interesting folder (401
 Unauthorised)Yn /linux/: Potentially interesting folder (401
 Unauthorised)Yn /loader/: Potentially interesting folder (401
 Unauthorised)Yn /local/: Potentially interesting folder (401
 Unauthorised)Yn /location/: Potentially interesting folder (401
 Unauthorised)Yn /locations/: Potentially interesting folder (401
 Unauthorised)Yn /logfile/: Potentially interesting folder (401
 Unauthorised)Yn /logfiles/: Potentially interesting folder (401
 Unauthorised)Yn /logger/: Potentially interesting folder (401
 Unauthorised)Yn /logg/: Potentially interesting folder (401
 Unauthorised)Yn /logging/: Potentially interesting folder (401
 Unauthorised)Yn /logon/: Potentially interesting folder (401
 Unauthorised)Yn /logout/: Potentially interesting folder (401
 Unauthorised)Yn /lost+found/: Potentially interesting folder (401
 Unauthorised)Yn /mailman/: Potentially interesting folder (401
 Unauthorised)Yn /mailroot/: Potentially interesting folder (401
 Unauthorised)Yn /makefile/: Potentially interesting folder (401
 Unauthorised)Yn /manage/: Potentially interesting folder (401
 Unauthorised)Yn /management/: Potentially interesting folder (401
 Unauthorised)Yn /man/: Potentially interesting folder (401

Unauthorised)Yn /manual/: Potentially interesting folder (401
 Unauthorised)Yn /map/: Potentially interesting folder (401
 Unauthorised)Yn /maps/: Potentially interesting folder (401
 Unauthorised)Yn /marketing/: Potentially interesting folder (401
 Unauthorised)Yn /member/: Potentially interesting folder (401
 Unauthorised)Yn /members/: Potentially interesting folder (401
 Unauthorised)Yn /mem_bin/: Potentially interesting folder (401
 Unauthorised)Yn /mem/: Potentially interesting folder (401
 Unauthorised)Yn /message/: Potentially interesting folder (401
 Unauthorised)Yn /messaging/: Potentially interesting folder (401
 Unauthorised)Yn /metacart/: Potentially interesting folder (401
 Unauthorised)Yn /microsoft/: Potentially interesting folder (401
 Unauthorised)Yn /misc/: Potentially interesting folder (401
 Unauthorised)Yn /mkstats/: Potentially interesting folder (401
 Unauthorised)Yn /mod/: Potentially interesting folder (401
 Unauthorised)Yn /module/: Potentially interesting folder (401
 Unauthorised)Yn /modules/: Potentially interesting folder (401
 Unauthorised)Yn /movimientos/: Potentially interesting folder (401
 Unauthorised)Yn /mpcgi/: Potentially interesting folder (401
 Unauthorised)Yn /mqseries/: Potentially interesting folder (401
 Unauthorised)Yn /msfpe/: Potentially interesting folder (401
 Unauthorised)Yn /ms/: Potentially interesting folder (401
 Unauthorised)Yn /mysql/: Potentially interesting folder (401
 Unauthorised)Yn /Msword/: Potentially interesting folder (401
 Unauthorised)Yn /mxhtml/: Potentially interesting folder (401
 Unauthorised)Yn /mxportal/: Potentially interesting folder (401
 Unauthorised)Yn /my/: Potentially interesting folder (401
 Unauthorised)Yn /My%20Shared%20Folder/: Potentially interesting
 folder (401 Unauthorised)Yn /mysql_admin/: Potentially interesting
 folder (401 Unauthorised)Yn /mysql/: Potentially interesting folder
 (401 Unauthorised)Yn /name/: Potentially interesting folder (401
 Unauthorised)Yn /names/: Potentially interesting folder (401
 Unauthorised)Yn /ncadmin/: Potentially interesting folder (401
 Unauthorised)Yn /nchelp/: Potentially interesting folder (401
 Unauthorised)Yn /netbasic/: Potentially interesting folder (401
 Unauthorised)Yn /netcat/: Potentially interesting folder (401
 Unauthorised)Yn /NetDynamic/: Potentially interesting folder (401
 Unauthorised)Yn /NetDynamics/: Potentially interesting folder (401
 Unauthorised)Yn /net/: Potentially interesting folder (401
 Unauthorised)Yn /netmagstats/: Potentially interesting folder (401
 Unauthorised)Yn /netscape/: Potentially interesting folder (401
 Unauthorised)Yn /netshare/: Potentially interesting folder (401
 Unauthorised)Yn /nettracker/: Potentially interesting folder (401
 Unauthorised)Yn /network/: Potentially interesting folder (401
 Unauthorised)Yn /new/: Potentially interesting folder (401
 Unauthorised)Yn /news/: Potentially interesting folder (401
 Unauthorised)Yn /News/: Potentially interesting folder (401
 Unauthorised)Yn /nextgeneration/: Potentially interesting folder
 (401 Unauthorised)Yn /nl/: Potentially interesting folder (401
 Unauthorised)Yn /notes/: Potentially interesting folder (401
 Unauthorised)Yn /noticias/: Potentially interesting folder (401
 Unauthorised)Yn /NSearch/: Potentially interesting folder (401

Unauthorised)¥n /objects/: Potentially interesting folder (401
Unauthorised)¥n /odbc/: Potentially interesting folder (401
Unauthorised)¥n /officescan/: Potentially interesting folder (401
Unauthorised)¥n /ojspdemos/: Potentially interesting folder (401
Unauthorised)¥n /old_files/: Potentially interesting folder (401
Unauthorised)¥n /oldfiles/: Potentially interesting folder (401
Unauthorised)¥n /old/: Potentially interesting folder (401
Unauthorised)¥n /oprocMgr-service/: Potentially interesting folder
(401 Unauthorised)¥n /oprocMgr-status/: Potentially interesting
folder (401 Unauthorised)¥n /oracle/: Potentially interesting
folder (401 Unauthorised)¥n /oradata/: Potentially interesting
folder (401 Unauthorised)¥n /order/: Potentially interesting folder
(401 Unauthorised)¥n /orders/: Potentially interesting folder (401
Unauthorised)¥n /os/: Potentially interesting folder (401
Unauthorised)¥n /out/: Potentially interesting folder (401
Unauthorised)¥n /outgoing/: Potentially interesting folder (401
Unauthorised)¥n /owners/: Potentially interesting folder (401
Unauthorised)¥n /ows-bin/: Potentially interesting folder (401
Unauthorised)¥n /page/: Potentially interesting folder (401
Unauthorised)¥n /_pages/: Potentially interesting folder (401
Unauthorised)¥n /pages/: Potentially interesting folder (401
Unauthorised)¥n /partner/: Potentially interesting folder (401
Unauthorised)¥n /partners/: Potentially interesting folder (401
Unauthorised)¥n /passport/: Potentially interesting folder (401
Unauthorised)¥n /password/: Potentially interesting folder (401
Unauthorised)¥n /passwords/: Potentially interesting folder (401
Unauthorised)¥n /path/: Potentially interesting folder (401
Unauthorised)¥n /payment/: Potentially interesting folder (401
Unauthorised)¥n /payments/: Potentially interesting folder (401
Unauthorised)¥n /pccsmysqldm/: Potentially interesting folder (401
Unauthorised)¥n /PDG_Cart/: Potentially interesting folder (401
Unauthorised)¥n /perl5/: Potentially interesting folder (401
Unauthorised)¥n /perl/: Potentially interesting folder (401
Unauthorised)¥n /personal/: Potentially interesting folder (401
Unauthorised)¥n /pforum/: Potentially interesting folder (401
Unauthorised)¥n /phorum/: Potentially interesting folder (401
Unauthorised)¥n /phpBB/: Potentially interesting folder (401
Unauthorised)¥n /php_classes/: Potentially interesting folder (401
Unauthorised)¥n /phpclassifieds/: Potentially interesting folder
(401 Unauthorised)¥n /php/: Potentially interesting folder (401
Unauthorised)¥n /phpimageview/: Potentially interesting folder (401
Unauthorised)¥n /phpnuke/: Potentially interesting folder (401
Unauthorised)¥n /phpPhotoAlbum/: Potentially interesting folder
(401 Unauthorised)¥n /phpprojekt/: Potentially interesting folder
(401 Unauthorised)¥n /phpSecurePages/: Potentially interesting
folder (401 Unauthorised)¥n /pics/: Potentially interesting folder
(401 Unauthorised)¥n /pictures/: Potentially interesting folder
(401 Unauthorised)¥n /pike/: Potentially interesting folder (401
Unauthorised)¥n /piranha/: Potentially interesting folder (401
Unauthorised)¥n /pls/: Potentially interesting folder (401
Unauthorised)¥n /plsSql/: Potentially interesting folder (401
Unauthorised)¥n /plssampleadmin_/: Potentially interesting folder


```

(401 Unauthorised)¥n /plssampleadmin/: Potentially interesting
folder (401 Unauthorised)¥n /plssampleadmin_help/: Potentially
interesting folder (401 Unauthorised)¥n /plssample/: Potentially
interesting folder (401 Unauthorised)¥n /poll/: Potentially
interesting folder (401 Unauthorised)¥n /polls/: Potentially
interesting folder (401 Unauthorised)¥n /porn/: Potentially
interesting folder (401 Unauthorised)¥n /portal/: Potentially
interesting folder (401 Unauthorised)¥n /portals/: Potentially
interesting folder (401 Unauthorised)¥n /postgres/: Potentially
interesting folder (401 Unauthorised)¥n /postnuke/: Potentially
interesting folder (401 Unauthorised)¥n /ppwb/: Potentially
interesting folder (401 Unauthorised)¥n /printer/: Potentially
interesting folder (401 Unauthorised)¥n /printers/: Potentially
interesting folder (401 Unauthorised)¥n /privacy/: Potentially
interesting folder (401 Unauthorised)¥n /privado/: Potentially
interesting folder (401 Unauthorised)¥n /_private/: Potentially
interesting folder (401 Unauthorised)¥n /private/: Potentially
interesting folder (401 Unauthorised)¥n /priv/: Potentially
interesting folder (401 Unauthorised)¥n /prod/: Potentially
interesting folder (401 Unauthorised)¥n /projectserver/:
Potentially interesting folder (401 Unauthorised)¥n /protected/:
Potentially interesting folder (401 Unauthorised)¥n /proxy/:
Potentially interesting folder (401 Unauthorised)¥n /prueba/:
Potentially interesting folder (401 Unauthorised)¥n /pruebas/:
Potentially interesting folder (401 Unauthorised)¥n /prv/:
Potentially interesting folder (401 Unauthorised)¥n /pub/:
Potentially interesting folder (401 Unauthorised)¥n /_public/:
Potentially interesting folder (401 Unauthorised)¥n /public/:
Potentially interesting folder (401 Unauthorised)¥n /publica/:
Potentially interesting folder (401 Unauthorised)¥n /publicar/:
Potentially interesting folder (401 Unauthorised)¥n /publico/:
Potentially interesting folder (401 Unauthorised)¥n /publish/:
Potentially interesting folder (401 Unauthorised)¥n /purchase/:
Potentially interesting folder (401 Unauthorised)¥n /purchases/:
Potentially interesting folder (401 Unauthorised)¥n /pw/:
Potentially interesting folder (401 Unauthorised)¥n /python/:
Potentially interesting folder (401 Unauthorised)¥n /random_banner/:
Potentially interesting folder (401 Unauthorised)¥n /rdp/:
Potentially interesting folder (401 Unauthorised)¥n /Readme/:
Potentially interesting folder (401 Unauthorised)¥n /recycler/:
Potentially interesting folder (401 Unauthorised)¥n /registered/:
Potentially interesting folder (401 Unauthorised)¥n /register/:
Potentially interesting folder (401 Unauthorised)¥n /registry/:
Potentially interesting folder (401 Unauthorised)¥n /remote/:
Potentially interesting folder (401 Unauthorised)¥n /remove/:
Potentially interesting folder (401 Unauthorised)¥n /report/:
Potentially interesting folder (401 Unauthorised)¥n /reports/:
Potentially interesting folder (401 Unauthorised)¥n /reseller/:
Potentially interesting folder (401 Unauthorised)¥n /restricted/:
Potentially interesting folder (401 Unauthorised)¥n /retail/:
Potentially interesting folder (401 Unauthorised)¥n /reveal/:
Potentially interesting folder (401 Unauthorised)¥n /reviews/:

```

Potentially interesting folder (401 Unauthorised)¥n /ROADS/:
 Potentially interesting folder (401 Unauthorised)¥n /robot/:
 Potentially interesting folder (401 Unauthorised)¥n /robots/:
 Potentially interesting folder (401 Unauthorised)¥n /root/:
 Potentially interesting folder (401 Unauthorised)¥n /rsrc/:
 Potentially interesting folder (401 Unauthorised)¥n /ruby/:
 Potentially interesting folder (401 Unauthorised)¥n /sales/:
 Potentially interesting folder (401 Unauthorised)¥n /save/:
 Potentially interesting folder (401 Unauthorised)¥n /script/:
 Potentially interesting folder (401 Unauthorised)¥n /ScriptLibrary/:
 Potentially interesting folder (401 Unauthorised)¥n /scripts/:
 Potentially interesting folder (401 Unauthorised)¥n /search/:
 Potentially interesting folder (401 Unauthorised)¥n /search-ui/:
 Potentially interesting folder (401 Unauthorised)¥n /sec/:
 Potentially interesting folder (401 Unauthorised)¥n /secret/:
 Potentially interesting folder (401 Unauthorised)¥n /secured/:
 Potentially interesting folder (401 Unauthorised)¥n /secure/:
 Potentially interesting folder (401 Unauthorised)¥n /security/:
 Potentially interesting folder (401 Unauthorised)¥n /sell/:
 Potentially interesting folder (401 Unauthorised)¥n /server/:
 Potentially interesting folder (401 Unauthorised)¥n /server-info/:
 Potentially interesting folder (401 Unauthorised)¥n /servers/:
 Potentially interesting folder (401 Unauthorised)¥n /server_stats/:
 Potentially interesting folder (401 Unauthorised)¥n /serverstats/:
 Potentially interesting folder (401 Unauthorised)¥n /server-status/:
 Potentially interesting folder (401 Unauthorised)¥n /service/:
 Potentially interesting folder (401 Unauthorised)¥n /services/:
 Potentially interesting folder (401 Unauthorised)¥n /servicio/:
 Potentially interesting folder (401 Unauthorised)¥n /servicios/:
 Potentially interesting folder (401 Unauthorised)¥n /servlet/:
 Potentially interesting folder (401 Unauthorised)¥n /servlets/:
 Potentially interesting folder (401 Unauthorised)¥n /session/:
 Potentially interesting folder (401 Unauthorised)¥n /setup/:
 Potentially interesting folder (401 Unauthorised)¥n /shared/:
 Potentially interesting folder (401 Unauthorised)¥n /sharedtemplates/: Potentially interesting folder (401
 Unauthorised)¥n /share/: Potentially interesting folder (401
 Unauthorised)¥n /shell-cgi/: Potentially interesting folder (401
 Unauthorised)¥n /shipping/: Potentially interesting folder (401
 Unauthorised)¥n /shop/: Potentially interesting folder (401
 Unauthorised)¥n /shopper/: Potentially interesting folder (401
 Unauthorised)¥n /show/: Potentially interesting folder (401
 Unauthorised)¥n /SilverStream/: Potentially interesting folder (401
 Unauthorised)¥n /siteadmin/: Potentially interesting folder (401
 Unauthorised)¥n /site/: Potentially interesting folder (401
 Unauthorised)¥n /sitemgr/: Potentially interesting folder (401
 Unauthorised)¥n /siteminderagent/: Potentially interesting folder
 (401 Unauthorised)¥n /siteminder/: Potentially interesting folder
 (401 Unauthorised)¥n /siteserver/: Potentially interesting folder
 (401 Unauthorised)¥n /sites/: Potentially interesting folder (401
 Unauthorised)¥n /sitestats/: Potentially interesting folder (401
 Unauthorised)¥n /siteupdate/: Potentially interesting folder (401

Unauthorised)¥n /smreports/: Potentially interesting folder (401
Unauthorised)¥n /smreportsviewer/: Potentially interesting folder
(401 Unauthorised)¥n /soapdocs/: Potentially interesting folder
(401 Unauthorised)¥n /soap/: Potentially interesting folder (401
Unauthorised)¥n /software/: Potentially interesting folder (401
Unauthorised)¥n /solaris/: Potentially interesting folder (401
Unauthorised)¥n /source/: Potentially interesting folder (401
Unauthorised)¥n /sql/: Potentially interesting folder (401
Unauthorised)¥n /squid/: Potentially interesting folder (401
Unauthorised)¥n /src/: Potentially interesting folder (401
Unauthorised)¥n /srchadm/: Potentially interesting folder (401
Unauthorised)¥n /ssi/: Potentially interesting folder (401
Unauthorised)¥n /ssl/: Potentially interesting folder (401
Unauthorised)¥n /sslkeys/: Potentially interesting folder (401
Unauthorised)¥n /staff/: Potentially interesting folder (401
Unauthorised)¥n /state/: Potentially interesting folder (401
Unauthorised)¥n /stat/: Potentially interesting folder (401
Unauthorised)¥n /statistic/: Potentially interesting folder (401
Unauthorised)¥n /statistics/: Potentially interesting folder (401
Unauthorised)¥n /stats-bin-p/: Potentially interesting folder (401
Unauthorised)¥n /stats/: Potentially interesting folder (401
Unauthorised)¥n /stats_old/: Potentially interesting folder (401
Unauthorised)¥n /status/: Potentially interesting folder (401
Unauthorised)¥n /storage/: Potentially interesting folder (401
Unauthorised)¥n /StoreDB/: Potentially interesting folder (401
Unauthorised)¥n /store/: Potentially interesting folder (401
Unauthorised)¥n /storemgr/: Potentially interesting folder (401
Unauthorised)¥n /stronghold-info/: Potentially interesting folder
(401 Unauthorised)¥n /stronghold-status/: Potentially interesting
folder (401 Unauthorised)¥n /stuff/: Potentially interesting folder
(401 Unauthorised)¥n /style/: Potentially interesting folder (401
Unauthorised)¥n /styles/: Potentially interesting folder (401
Unauthorised)¥n /stylesheet/: Potentially interesting folder (401
Unauthorised)¥n /stylesheets/: Potentially interesting folder (401
Unauthorised)¥n /subir/: Potentially interesting folder (401
Unauthorised)¥n /sun/: Potentially interesting folder (401
Unauthorised)¥n /super_stats/: Potentially interesting folder (401
Unauthorised)¥n /supplier/: Potentially interesting folder (401
Unauthorised)¥n /suppliers/: Potentially interesting folder (401
Unauthorised)¥n /supply/: Potentially interesting folder (401
Unauthorised)¥n /supporter/: Potentially interesting folder (401
Unauthorised)¥n /support/: Potentially interesting folder (401
Unauthorised)¥n /sysadmin/: Potentially interesting folder (401
Unauthorised)¥n /sysbackup/: Potentially interesting folder (401
Unauthorised)¥n /sys/: Potentially interesting folder (401
Unauthorised)¥n /system/: Potentially interesting folder (401
Unauthorised)¥n /systems/: Potentially interesting folder (401
Unauthorised)¥n /tar/: Potentially interesting folder (401
Unauthorised)¥n /target/: Potentially interesting folder (401
Unauthorised)¥n /tarjetas/: Potentially interesting folder (401
Unauthorised)¥n /tech/: Potentially interesting folder (401
Unauthorised)¥n /technote/: Potentially interesting folder (401

Unauthorised)¥n /te_html/: Potentially interesting folder (401
Unauthorised)¥n /temp/: Potentially interesting folder (401
Unauthorised)¥n /template/: Potentially interesting folder (401
Unauthorised)¥n /templates/: Potentially interesting folder (401
Unauthorised)¥n /temporal/: Potentially interesting folder (401
Unauthorised)¥n /test-cgi/: Potentially interesting folder (401
Unauthorised)¥n /testing/: Potentially interesting folder (401
Unauthorised)¥n /tests/: Potentially interesting folder (401
Unauthorised)¥n /testweb/: Potentially interesting folder (401
Unauthorised)¥n /themes/: Potentially interesting folder (401
Unauthorised)¥n /ticket/: Potentially interesting folder (401
Unauthorised)¥n /tickets/: Potentially interesting folder (401
Unauthorised)¥n /tip/: Potentially interesting folder (401
Unauthorised)¥n /tips/: Potentially interesting folder (401
Unauthorised)¥n /tmp/: Potentially interesting folder (401
Unauthorised)¥n /ToDo/: Potentially interesting folder (401
Unauthorised)¥n /tool/: Potentially interesting folder (401
Unauthorised)¥n /tools/: Potentially interesting folder (401
Unauthorised)¥n /TopAccess/: Potentially interesting folder (401
Unauthorised)¥n /top/: Potentially interesting folder (401
Unauthorised)¥n /tpv/: Potentially interesting folder (401
Unauthorised)¥n /trabajo/: Potentially interesting folder (401
Unauthorised)¥n /track/: Potentially interesting folder (401
Unauthorised)¥n /tracking/: Potentially interesting folder (401
Unauthorised)¥n /transfer/: Potentially interesting folder (401
Unauthorised)¥n /transito/: Potentially interesting folder (401
Unauthorised)¥n /transpolar/: Potentially interesting folder (401
Unauthorised)¥n /tree/: Potentially interesting folder (401
Unauthorised)¥n /trees/: Potentially interesting folder (401
Unauthorised)¥n /trick/: Potentially interesting folder (401
Unauthorised)¥n /tricks/: Potentially interesting folder (401
Unauthorised)¥n /u02/: Potentially interesting folder (401
Unauthorised)¥n /unix/: Potentially interesting folder (401
Unauthorised)¥n /unknown/: Potentially interesting folder (401
Unauthorised)¥n /updates/: Potentially interesting folder (401
Unauthorised)¥n /upload/: Potentially interesting folder (401
Unauthorised)¥n /uploads/: Potentially interesting folder (401
Unauthorised)¥n /usage/: Potentially interesting folder (401
Unauthorised)¥n /userdb/: Potentially interesting folder (401
Unauthorised)¥n /user/: Potentially interesting folder (401
Unauthorised)¥n /users/: Potentially interesting folder (401
Unauthorised)¥n /us/: Potentially interesting folder (401
Unauthorised)¥n /usr/: Potentially interesting folder (401
Unauthorised)¥n /ustats/: Potentially interesting folder (401
Unauthorised)¥n /usuario/: Potentially interesting folder (401
Unauthorised)¥n /usuarios/: Potentially interesting folder (401
Unauthorised)¥n /util/: Potentially interesting folder (401
Unauthorised)¥n /utils/: Potentially interesting folder (401
Unauthorised)¥n /vendor/: Potentially interesting folder (401
Unauthorised)¥n /vfs/: Potentially interesting folder (401
Unauthorised)¥n /view/: Potentially interesting folder (401
Unauthorised)¥n /vpn/: Potentially interesting folder (401

```

Unauthorised)Yn /vti_txt/: Potentially interesting folder (401
Unauthorised)Yn /w2000/: Potentially interesting folder (401
Unauthorised)Yn /w2k/: Potentially interesting folder (401
Unauthorised)Yn /w3perl/: Potentially interesting folder (401
Unauthorised)Yn /w-agora/: Potentially interesting folder (401
Unauthorised)Yn /way-board/: Potentially interesting folder (401
Unauthorised)Yn /web800fo/: Potentially interesting folder (401
Unauthorised)Yn /webaccess/: Potentially interesting folder (401
Unauthorised)Yn /webadmin/: Potentially interesting folder (401
Unauthorised)Yn /webAdmin/: Potentially interesting folder (401
Unauthorised)Yn /webalizer/:
Potentially interesting folder (401 Unauthorised)Yn /webapps/:
Potentially interesting folder (401 Unauthorised)Yn /WebBank/:
Potentially interesting folder (401 Unauthorised)Yn /webboard/:
Potentially interesting folder (401 Unauthorised)Yn /WebCalendar/:
Potentially interesting folder (401 Unauthorised)Yn /webcart/:
Potentially interesting folder (401 Unauthorised)Yn /webcart-lite/:
Potentially interesting folder (401 Unauthorised)Yn /webcgi/:
Potentially interesting folder (401 Unauthorised)Yn /webdata/:
Potentially interesting folder (401 Unauthorised)Yn /webdav/:
Potentially interesting folder (401 Unauthorised)Yn /webdb/:
Potentially interesting folder (401 Unauthorised)Yn /webDB/:
Potentially interesting folder (401 Unauthorised)Yn /web/:
Potentially interesting folder (401 Unauthorised)Yn /webimages2/:
Potentially interesting folder (401 Unauthorised)Yn /webimages/:
Potentially interesting folder (401 Unauthorised)Yn /web-inf/:
Potentially interesting folder (401 Unauthorised)Yn /webmaster/:
Potentially interesting folder (401 Unauthorised)Yn
/webmaster_logs/: Potentially interesting folder (401
Unauthorised)Yn /webMathematica/: Potentially interesting folder
(401 Unauthorised)Yn /webpub/: Potentially interesting folder (401
Unauthorised)Yn /webpub-ui/: Potentially interesting folder (401
Unauthorised)Yn /webreports/: Potentially interesting folder (401
Unauthorised)Yn /webreps/: Potentially interesting folder (401
Unauthorised)Yn /webshare/: Potentially interesting folder (401
Unauthorised)Yn /WebShop/: Potentially interesting folder (401
Unauthorised)Yn /website/: Potentially interesting folder (401
Unauthorised)Yn /webstat/: Potentially interesting folder (401
Unauthorised)Yn /webstats/: Potentially interesting folder (401
Unauthorised)Yn /Web_store/: Potentially interesting folder (401
Unauthorised)Yn /webtrace/: Potentially interesting folder (401
Unauthorised)Yn /WebTrend/: Potentially interesting folder (401
Unauthorised)Yn /webtrends/: Potentially interesting folder (401
Unauthorised)Yn /web_usage/: Potentially interesting folder (401
Unauthorised)Yn /win2k/: Potentially interesting folder (401
Unauthorised)Yn /window/: Potentially interesting folder (401
Unauthorised)Yn /windows/: Potentially interesting folder (401
Unauthorised)Yn /win/: Potentially interesting folder (401
Unauthorised)Yn /winnt/: Potentially interesting folder (401
Unauthorised)Yn /word/: Potentially interesting folder (401
Unauthorised)Yn /work/: Potentially interesting folder (401
Unauthorised)Yn /world/: Potentially interesting folder (401

```

```

Unauthorised)¥n /wsdocs/: Potentially interesting folder (401
Unauthorised)¥n /WS_FTP/: Potentially interesting folder (401
Unauthorised)¥n /wstats/: Potentially interesting folder (401
Unauthorised)¥n /wusage/: Potentially interesting folder (401
Unauthorised)¥n /www0/: Potentially interesting folder (401
Unauthorised)¥n /www2/: Potentially interesting folder (401
Unauthorised)¥n /www3/: Potentially interesting folder (401
Unauthorised)¥n /www4/: Potentially interesting folder (401
Unauthorised)¥n /www/: Potentially interesting folder (401
Unauthorised)¥n /wwwjoin/: Potentially interesting folder (401
Unauthorised)¥n /wwwrooot/: Potentially interesting folder (401
Unauthorised)¥n /www-sql/: Potentially interesting folder (401
Unauthorised)¥n /wwwstat/: Potentially interesting folder (401
Unauthorised)¥n /wwwstats/: Potentially interesting folder (401
Unauthorised)¥n /xGB/: Potentially interesting folder (401
Unauthorised)¥n /xml/: Potentially interesting folder (401
Unauthorised)¥n /XSL/: Potentially interesting folder (401
Unauthorised)¥n /xtemp/: Potentially interesting folder (401
Unauthorised)¥n /xymon/: Potentially interesting folder (401
Unauthorised)¥n /zb41/: Potentially interesting folder (401
Unauthorised)¥n /zipfiles/: Potentially interesting folder (401
Unauthorised)¥n /zip/: Potentially interesting folder (401
Unauthorised)¥n /_docs/: Potentially interesting folder (401
Unauthorised)¥n', 'http-method-tamper': '¥n VULNERABLE:¥n
Authentication bypass by HTTP verb tampering¥n State: VULNERABLE
(Exploitable)¥n This web server contains password protected
resources vulnerable to authentication bypass¥n vulnerabilities
via HTTP verb tampering. This is often found in web servers that
only limit access to the¥n common HTTP methods and in
misconfigured .htaccess files.¥n ¥n Extra
information:¥n ¥n URIs suspected to be vulnerable to HTTP verb
tampering:¥n /Now_TV_backup_settings-erase.html [HEAD]¥n
/Now_TV_license.html [HEAD]¥n /Now_TV_wireless_password.html
[HEAD]¥n /Now_TV_wireless_onoff.html [HEAD]¥n
/Now_TV_support.html [HEAD]¥n /Now_TV_wireless_network_name.html
[HEAD]¥n /Now_TV_wireless_channel.html [HEAD]¥n
/Now_TV_set_password.html [HEAD]¥n /Now_TV_rebootinfo.cgi
[HEAD]¥n /Now_TV_logs.html [HEAD]¥n /Now_TV_router_status.html
[HEAD]¥n /Now_TV_wireless_settings.html [HEAD]¥n ¥n
References:¥n
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_%28
OWASP-CM-008%29¥n
http://www.imperva.com/resources/glossary/http_verb_tampering.html¥n
http://capec.mitre.org/data/definitions/274.html¥n
http://www.mkkit.com.ar/labs/htexploit/¥n', 'http-dombased-xss':
"Couldn't find any DOM based XSS.", 'http-server-header':
'sky_router', 'http-slowloris-check': "¥n VULNERABLE:¥n Slowloris
DOS attack¥n State: LIKELY VULNERABLE¥n IDs: CVE:CVE-2007-
6750¥n Slowloris tries to keep many connections to the target
web server open and hold¥n them open as long as possible. It
accomplishes this by opening connections to¥n the target web
server and sending a partial request. By doing so, it starves¥n

```

```
the http server's resources causing Denial Of Service.¥n      ¥n
Disclosure date: 2009-09-17¥n      References:¥n
http://ha.ckers.org/slowloris/¥n      https://cve.mitre.org/cgi-
bin/cvename.cgi?name=CVE-2007-6750¥n", 'http-stored-xss': "Couldn't
find any stored XSS vulnerabilities.", 'http-vuln-cve2014-3704':
'ERROR: Script execution failed (use -d to debug)'}}}}}}
```

APPENDIX B - PYTHON NMAP SCRIPT

```
import nmap
import sys
import os

#checks for two arguments
if len(sys.argv) !=3:
    print("python3 nm2.py <Target Address> <Port Range>")
    sys.exit(0)

#Argument #1: Ip Address
hostaddress = sys.argv[1]
#Argument #2: Port Range
portrange = sys.argv[2]

nmscan=nmap.PortScanner()

#creates text file for the scan report.
report = open("Scan-Report_"+hostaddress+"_"+portrange, "w")

#Displays host address and nmap version.
print("-----" *6)
print("          Scanning Target: " +hostaddress)
print('          Nmap Version: ', nmscan.nmap_version())
```

```

print("-----" *6)

####

report.write("-----" *6 + "\n")
report.write("                Scanning Target: " +hostaddress +"\n")
#report.write("                Nmap Version: "+nmscan.nmap_version())
report.write("-----" *6 + "\n")
####

try:

    nmscan.scan(hostaddress, portrange)

    #host scan

    targetName = nmscan[hostaddress].hostname()

    #error handling
except nmap.PortScannerError:

    print("Nmap Not Found ", sys.exc_info[0])
except:

    ("Unexpected ", sys.exc_info[0])

    #scans host and state.
for host in nmscan.all_hosts():

    print("Host : %s (%s)" % (targetName,hostaddress))

    print("State : %s" % nmscan[host].state())

    ####

    report.write("Host : %s (%s)" % (targetName,hostaddress)+"\n")

    report.write("State : %s" % nmscan[host].state()+"\n")

    ####

    #scans for protocols.

    for proto in nmscan[host].all_protocols():

```



```

print("-----" *6)

print("Protocols : %s " % proto)

####

report.write("-----" *6+"¥n")
report.write("Protocols : %s " % proto+ "¥n")
####

#scans for open ports.

lport = nmscan[host][proto].keys()

#sorts ports into columns.

sorted(lport)

for port in lport:

    print("Port : %s ¥t State : %s
" % (port,nmscan[host][proto][port]['state']))

    ####

    report.write("Port : %s ¥t State : %s
" % (port,nmscan[host][proto][port]['state'])+"¥n")

    ####

print("-----" *6)

report.write("-----" *6+'¥n')

try:

    #operating system scan.

    osdetect = nmscan.scan(hostaddress, portrange, arguments='-O')

    print('Operating System: ',
osdetect['scan'][hostaddress]['osmatch'][0]['osclass'][1]['osfamily'])

    ####

    report.write('Operating System: '+
osdetect['scan'][hostaddress]['osmatch'][0]['osclass'][1]['osfamily']
+ "¥n")

```

```

####

except nmap.PortScannerError:
    print("Nmap Not Found ", sys.exc_info[0])
except:
    ("Unexpected ", sys.exc_info[0])

print("-----" *6)
print("                Performing Vulnerability Scan")
print("-----" *6)

####
report.write("-----" *6 + "\n")
report.write("                Performing Vulnerability Scan"+ "\n")
report.write("-----" *6 + "\n")
####

#vulnerability scan.
vulner = nmscan.scan(hostaddress, portrange, arguments='--script vuln
-sV -T4')

try:
    with open('vcan.txt', 'w') as vscan:

        #writes results to file.
        vscan.write(str(vulner))

except FileNotFoundError:
    print("The directory does not exist!")

```

```

#formats the text file.
with open('vcan.txt', 'r') as vscan:
    raw_data = vscan.read()
    formatted_data = raw_data.replace('%Yn', 'Yn').replace('  ','')

#overwrites formatted data into the text file.
with open('vcan.txt', 'w') as vscan:

    vscan.write(formatted_data)


#finds all lines with keyword 'VULNERABLE:'.
with open('vcan.txt','r') as vscan:
    lines = [line.strip() for line in vscan.readlines()]
    for i, line in enumerate(lines):
        if line.startswith("VULNERABLE:"):
            print(lines[i]+'Yn',lines[i+1]+'Yn', lines[i+2]+'Yn',
lines[i+3]+'Yn', lines[i+4],lines[i+5],lines[i+6], lines[i+7])
            #prints lines below.

            #####

            report.write(lines[i]+'Yn'+lines[i+1]+'Yn'+
lines[i+2]+'Yn'+ lines[i+3]+'Yn'+ lines[i+4]+ lines[i+5]+lines[i+6]+
lines[i+7] + "Yn"+"Yn")

            #####

print("-----" *6)
print("Scan Report Generated - Scan-Report_"+hostaddress+"_"+portrange)

#####
report.write("-----" *6 + "Yn")
#####

```

```
#closes report file and removes other text file.  
report.close()  
os.remove('vcan.txt')
```