

PROFESSIONAL TRAINING REPORT
AT
SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering Degree in INFORMATION TECHNOLOGY

By
A. JEBIN EARNEST
REG NUMBER: - 39120046



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,
CHENNAI – 600119, TAMILNADU

NOVEMBER 2021



**SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY**
(DEEMED TO BE
UNIVERSITY)

Accredited with Grade "A" by NAAC
(Established under Section 3 of UGC Act, 1956)
JEPPIAAR NAGAR, RAJIV GANDHI SALAI
CHENNAI- 600119
www.sathyabama.ac.in



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **A. JEBIN EARNEST (39120046)** who carried out the project entitled "**Website Enumeration Scans**" under my supervision November 2021.

Internal Guide

Dr. L. MARY GLADENCE M.E., Ph.D.,

Head of the Department

Dr. R. SUBHASHINI M.E, Ph.D.

Submitted for Viva voce Examination held on _____

InternalExaminer

ExternalExaminer

DECLARATION

I, **A. JEBIN EARNEST** hereby declare that the project report entitled **Website Enumeration Scans** done by me under the guidance of **Dr. L. MARY GLADENCE M.E, Ph.D.** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering Degree in **INFORMATION TECHNOLOGY**

DATE:

PLACE:

CANDIDATE

SIGNATURE OF THE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph.D., Dean, School of Computing, Dr. S. Vigneshwari, M.E., Ph.D. and Dr. L. Lakshmanan, M.E., Ph.D., Heads of the Department of INFORMATION TECHNOLOGY** for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. L. MARY GLADENCE M.E., Ph.D.,** for his valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of INFORMATION TECHNOLOGY** who were helpful in many ways for the completion of the project.

TRAINING CERTIFICATE



CERTIFICATE OF COMPLETION

CSW-I-38-081121 is given to

JEBIN EARNEST

For completing the Cyber Security training that includes basics of Cyber Security, Pentesting, Networking, and WebApp.

Aaron V Sandeen

AARON SANDEEN
CEO - CSW

N. Vengatesh

VENGATESH NAGARAJAN
MENTOR

ABSTRACT

Scanning and enumeration is the phase where the attacker begins to “touch” the systems. Attackers will scan networks to discover live hosts and open port. They will then enumerate the live hosts and ports to discover services, machine names, and other network resources. An IP address lookup determines the location of any IP address. The results provide quite a bit of information, including information the city, state/region, postal/zip code, country name, ISP, and time zone. Consequently, this data is used by various agencies to find the owner of an IPv4 or IPv6 address.

Using the ISP information check whether a website is hosted in AWS cloud.

LIST OF FIGURES:

page no:

- **Screenshots** **17**
- **Screenshots** **17**

TABLE OF CONTENTS

CHAPTER No.	TITLE	PAGE No
	ABSTRACT	i
	LIST OF FIGURES	ii
	LIST OF TABLES	iii
	LIST OF ABBREVIATIONS	iv
1	INTRODUCTION	9
	1.1 WHAT IS CYBER SECURITY?	9
	1.2. IMPORTANCE OF CYBER SECURITY	9
2.	ENUMERATION SCANS	10
	2.1 Finding the IP Address	11
	2.2 Look Up the IP Address	11
3.	EXPERIMENTAL OR MATERIALS AND METHODS, REQUIREMENTS USED	13
	3.1 python3	13
	3.2 urllib.parse	13
	3.3 socket	13
	3.4 WHOIS	14
4	SUMMARY	15
	4.1 RESULT	15
	4.2 CONCLUSION	15

REFERENCES	16
APPENDIX	
A. SCREENSHOTS	17
B. SOURCE CODE	18

INTRODUCTION

1.1 What is Cyber Security?

Cybersecurity is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide. It is otherwise known as Computer Security or information Technology security.

1.2 IMPORTANCE OF CYBER SECURITY

- User's asset is protected against various cyber security risk and remain intact.
- The importance of ensuring protection from attacks, damage and authorized access on networks, computers and programs is equivalent to daily routine operation of an organization.
- Helping to understand the current trend in it and develop effective solutions.
- Reducing vulnerability in information and ICT systems and networks.

COMMON TOOLS USED FOR CYBER SECURITY

- Passwords
- Antivirus / Anti-malware software
- Software patches
- Fire walls
- Two factor authentication
- Encryption

KEY ELEMENTS OF CYBER SECURITY

- Application security
- Information security
- Network security
- Disaster security
- Operation security

ENUMERATION SCANS.

Enumeration in information security is the process of extracting user names, machine names, network resources, and other services from a system. All the gathered information is used to identify the vulnerabilities or weak points in system security and then tries to exploit it.

Enumeration can be performed on the following.

1. NetBios enumeration
2. SNMP enumeration
3. LDAP enumeration
4. NTP enumeration
5. SMTP enumeration
6. DNS enumeration
7. Windows enumeration
8. UNIX/Linux enumeration

DNS stands for Domain Name Service, and it is primarily designed as hierarchical decentralized distributed naming systems for computers, services or any resource connected to the network. DNS resolves hostnames to its respective IP addresses and vice versa.

DNS internally maintains a database for storing the records. The following are the most commonly used record types in DNS.

- Start of Authority (SOA)
- IP addresses (A and AAAA)
- SMTP mail exchangers (MX)
- Nameservers (NS)
- Pointers for reverse DNS lookups (PTR)
- Domain name aliases (CNAME)

DNS works on both UDP and TCP on port 53. It uses UDP for resolving queries and TCP for zone transfers. DNS zone transfer allows DNS databases to replicate the portion of the database from primary server to the secondary server. DNS zone transfer must only be allowed by other validated secondary DNS servers acting as clients.

2.1 Finding the IP Address

IP addresses basically provide info regarding the location of your device on the internet.

Every computational device on this network uses a unique number, necessary to send messages to computers that are present outside your local network.

Every website on the internet has one or more IP (Internal Protocol) addresses assigned to it. You may not be concerned with the IP address of any random website, but it is crucial to know the IP address of your own website.

Website IP address can be beneficial to: -

1. Divert website-blocking applications
2. Block specific sites
3. Finding the geographic location of a web server

Finding IP address of website can be a difficult task for people who have less technical knowledge.

2.2 Look Up the IP Address

An IP address lookup determines the location of any IP address. The results provide quite a bit of information, including information the city, state/region, postal/zip code, country name, ISP, and time zone. Consequently, this data is used by various agencies to find the owner of an IPv4 or IPv6 address.

It's important to understand that no IP Lookup tool is 100% accurate. IP lookup results are shown from several different IP location databases, and each database reports differently.

There are many other factors as to why results are not 100% accurate. Factors include:

- Where the IP address was registered
- Where the controlling agency is located
- Whether the user has a proxy or VPN
- Whether the connection is cellular or not

For example, if you are in the US and the controlling agency of the IP is located in Canada, the lookup data may show Canada as the IP location. It is not uncommon to see a Canadian IP while searching an IP address in the northern US.

When using an IP address lookup tool, users often think they are going to find the exact location of an IP address. This is simply not true. No IP address database can provide the exact physical address of an IP address location. At best, you'll get the exact city in which the user of the IP is located.

Only the Internet Service Provider (ISP) can provide an exact physical address of an IP. ISPs usually have logs of which user was assigned an IP at any given time. There are usually limits as to how long an ISP stores these records. However, without a police warrant, or some sort of legal document, the ISP is unlikely to turn over any information.

If you receive an offensive or fraudulent email, don't expect an ISP to give you the mailing address of the user of that IP address. Instead, turn over the communications to the authorities and let them do their job.

EXPERIMENTAL OR MATERIALS AND METHODS, REQUIREMENTS USED

3.1 PYTHON3

Python is an interpreted high-level general-purpose programming language. Its design philosophy emphasizes code readability with its use of significant indentation. Its language constructs as well as its object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects.

3.2 urllib.parse

This module defines a standard interface to break Uniform Resource Locator (URL) strings up in components (addressing scheme, network location, path etc.), to combine the components back into a URL string, and to convert a “relative URL” to an absolute URL given a “base URL.”

The module has been designed to match the internet RFC on Relative Uniform Resource Locators. It supports the following URL schemes: file, ftp, gopher, hdl, http, https, imap, mailto, mms, news, nntp, prospero, rsync, rtsp, rtspu, sftp, shhttp, sip, sips, snews, svn, svn+ssh, telnet, wais, ws, wss.

3.3 socket

Python's standard library consists of various built-in modules that support interprocess communication and networking. The network access is available at two levels. The 'socket' module defines how server and client machines can communicate at hardware level using socket endpoints on top of the operating system. The 'socket' API supports both connection-oriented and connectionless network protocols. The higher level support is available in Python libraries such as ftplib and httplib, implementing

Application level network protocols FTP and HTTP respectively. This chapter takes a look at the functionality of 'socket' module that provides access to BSD socket interface.

Given a host name the `gethostbyname()` function returns the IP address of the host.

Unlike, `gethostbyname()` returns just one ip of the host even though the host could resolve to multiple IPs from a given location.

The returned IP address is an IPv4 address.

3.4 WHOIS

WHOIS allows you to look up the name and contact information of whoever operates any website's generic domain name. As part of the registration process, you must provide your registrar with accurate and reliable contact details and promptly correct and update these details as necessary. The willful provision of inaccurate or unreliable information, or a willful failure to update information provided to a registrar, can be the basis for cancelling your registration and the loss of any right to use the domain name. The registrar that you select will ask you to provide contact and technical information, some of which is required by ICANN. The registrar will keep records of the contact information and submit certain technical and contact information to the entity, known as the registry, which maintains the central directory for that TLD. Each top-level domain has only one authoritative registry, which provides other computers on the Internet with the information necessary to send you email or to find your website. The Public Interest Registry, for example, operates the .ORG registry. As part of the registration process, you will be required to enter into a contract with the registrar that you or the reseller has selected. That contract sets forth the terms under which your registration is accepted and will be maintained. Once you have successfully completed the registration process, you become the registrant of your new domain name.

SYSTEM REQUIREMENTS

- 1TB HDD
- 8 GB RAM

TOOLS USED

- VISUAL STUDIO CODE (text editor)
- PYTHON3

RESULT

Thus, the program to scan and do enumeration on websites have been done and tested. The program works properly and finds the deep information of a given website and checks and prints out whether the website is hosted on AWS cloud.

CONCLUSION

In conclusion, with the help of Host Look Up we can identify if someone has sent a harassing or potentially fraudulent communication, the best you can do is to file a complaint with the authorities or the ISP. Then, forward all the relevant information from the questionable communication. This is a great technic to find the information of the organization behind some of the website that are harm to the society.

REFERNCES

[1] Haibin Lu and Sartaj Sahni "O (log n) Dynamic Router-Tables for Prefixes and Ranges" IEEE transactions on computers, vol. 53, no. 10, October 2004

[2] S. Nilsson, G. Karlsson," IP address lookup using LCtries", IEEE Journal on Selected Areas in Communications, vol 17, issue 6, pp 1083–1092, 1999.

- [3] R.C. Chang and B.-H. Lim “ Efficient IP routing table lookup scheme” IEE Proc. Commun., Vol. 149, No. 2, pp.77-82, April 2002
- [4] Chi-Cheng Wu Jia-Long Wu Huang-Sen Chiu “ Improving IP lookup Performance with a Routing-Table Cache” IEEE Communications Letters, Volume 7, Issue 3, March 2003
- [5] Chang, R.C. Beng-Huat Lim “Efficient IP routing table VLSI design for multigigabit routers “ IEEE International Symposium on vol 2,pp. 776-779 2002
- [6] Jinsoo Kim and Junghwan Kim “An Efficient IP Lookup Architecture with Fast Update Using SingleMatch TCAMs” Springer-Verlag Berlin Heidelberg, pp. 104–114, 2008
- [7] M. Ruiz-Sánchez, E. Biersack, and W. Dabbous, “Survey and Taxonomy of IP Address Lookup Algorithms”, IEEE Network Magazine, March/April 2001.
- [8] David Antos “Overview of Data Structures in IP Lookups “ CESNET Tchnical Report 9/2002.
- [9] V. Fuller, T. Li, J. Yu, and K. Varadhan, “Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy” RFC 1519, September 1993
- [10] Anindya Basu Girija Narlikar “Fast Incremental Updates for Pipelined Forwarding Engines” IEEE/ACM Transactions on Networking (TON), Volume 13 , Issue 3, pp. 690 – 703, June 2005

SCREENSHOTS OF THE OUTPUTS

Enter the url of the website: <https://support.microsoft.com/en-us/>

The main domain name of the URL is support.microsoft.com

The IP address of the entered URL is 104.114.102.145

The website is running on servers:

NS1-205.AZURE-DNS.COM,
NS2-205.AZURE-DNS.NET,
NS3-205.AZURE-DNS.ORG,
NS4-205.AZURE-DNS.INFO,
ns1-205.azure-dns.com,
ns4-205.azure-dns.info,
ns3-205.azure-dns.org,
ns2-205.azure-dns.net

The website is not hosted using the AWS cloud

Other deep information about the website are:

Organisation: Microsoft Corporation
Address: One Microsoft Way,
City: Redmond
Zipcode: 98052
State: WA
Country: US

Enter the url of the website: <https://www.netflix.com/in/>

The main domain name of the URL is www.netflix.com

The IP address of the entered URL is 52.214.181.141

The website is running on servers:

NS-1372.AWSDNS-43.ORG,
NS-1984.AWSDNS-56.CO.UK,
NS-659.AWSDNS-18.NET,
NS-81.AWSDNS-10.COM,
ns-1984.awsdns-56.co.uk,
ns-659.awsdns-18.net,
ns-81.awsdns-10.com,
ns-1372.awsdns-43.org

The website is hosted using the AWS cloud

Other deep information about the website are:

Organisation: Netflix, Inc.
Address: 100 Winchester Circle,
City: Los Gatos
Zipcode: 95032
State: CA
Country: US

SOURCE COUDE

```
import urllib.parse

import socket

import whois

url = input("Enter the url of the website: ")

parsed_url = urllib.parse.urlparse(url.strip())

print("\nThe main domain name of the URL is " + parsed_url.netloc +
"\n")

ip_address = socket.gethostbyname(parsed_url.netloc)

print("The IP address of the entered URL is " + ip_address + "\n")


result = whois.whois(parsed_url.netloc)

server_names = result["name_servers"]

hostInAws = False

print("The website is running on servers: \n")

print(", \n".join(server_names)+"\n")


for server in server_names:
```

```
tolower = server.lower()

if(tolower.find("awsdns") != -1):

    hostInAws = True

if(hostInAws):

    print("The website is hosted using the AWS cloud \n")

else:

    print("The website is not hosted using the AWS cloud \n")


print("Other deep information about the website are: \n")

print("Organisation: " + result["org"])

print("Address: " + result["address"])

print("City: " + result["city"])

print("Zipcode: " + result["zipcode"])

print("State: " + result["state"])

print("Country: " + result["country"])
```