

PROFESSIONAL TRAINING REPORT

at

Sathyabama Institute Science and Technology

(Deemed to be university)

Submitted in partial fulfillment of the requirements for the award of Bachelor of
Technology Degree in Information Technology.

By

Aakash.S

Reg no: 39120001

DEPARTMENT OF INFORMATION TECHNOLOGY

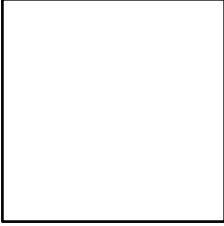
SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY

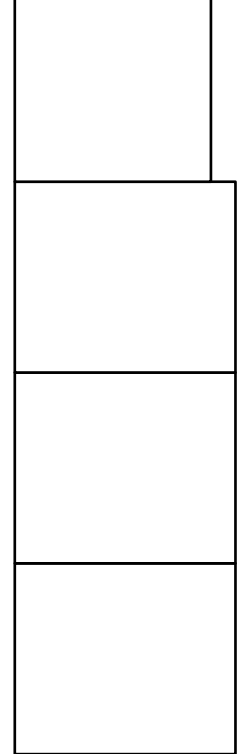
JEPPIAAR NAGAR, RAJIV GANDHI SALAI,

CHENNAI – 600119, TAMIL NADU

April 2022



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



BONAFIDE CERTIFICATE

This is to certify that this project report is the Bonafide work of Aakash.S (Reg no: 39120001) who carried out the project entitled “**Enumeration using Enum4linux**” under my supervision from February 2022 to April 2022.

Internal guide

Dr.P.Jeyanthi

Head of the department

Submitted for viva voce examination held on _____

Internal examiner

external examiner

DECLARATION

I, **Aakash.S** hereby declare that the project report entitled **Enumeration using Enum4linux** using Zybeak Technologies done by me under the guidance of **Dr.P.Jeyanthi** is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in Information Technology.

DATE: 19/04/2022

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

Acknowledgement

I am pleased to acknowledge my sincere thanks to the 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.Ed., 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 computer science and engineering 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.P.Jeyanthi**, for her valuable guidance, suggestions and constant encouragement paved the 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.

ABSTRACT

Enumeration is defined as the process of extracting user names, machine names, network resources, shares and services from a system. In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnerabilities or weak points in system security and tries to exploit in the System gaining phase. This process is essential to understand ethical attacks in cyber security. Enumeration extracts the critical information when a network/machine is targeted, it provides the information of userlist, machine details, sharelist, group details and password policy.

To simulate what happens in a real-world attack, we need to use Kali Linux to attack the target like Metasploitable etc. Enum4linux is an enumeration tool capable of detecting and extracting data from Windows and Linux operating systems, including those that are Samba (SMB) hosts on a network. Metasploitable 2 is a test environment that provides a secure place to perform penetration testing and security research. All these will be operated on a virtual box platform . Metasploitable 2 and kali linux will be installed on the virtual box and we will be working with it.

TABLE OF CONTENTS

CHAPTER NO	TITLE	PAGE NO
	ABSTRACT	i
1	INTRODUCTION	1
2	AIM AND SCOPE OF THE PRESENT INVESTIGATION	2
3	EXPERIMENTAL OR MATERIALS AND METHODS, ALGORITHM USED	3
4	RESULT AND DISCUSSION, PERFORMANCE ANALYSIS	4
5	SUMMARY AND CONCLUSION	5
	REFERENCE	6
	APPENDIX	
	SCREEN SHOT	7,8

CHAPTER 1

1.INTRODUCTION

Enumeration is part of the "Information Gathering" phase of Ethical Hacking. This is a technique in which an attacker creates a live connection with the target in order to find as many attack vectors as possible that may be utilized to further exploit the system.

Enumeration can be used to gain information on –

- Network shares.
- SNMP data, if they are not secured properly.
- IP tables.
- Usernames of different systems.
- Passwords policies lists.

Enumerations depend on the services that the systems offer. They can be –

- DNS (Domain Name Service) enumeration.
- NTP (Network Time Protocol) enumeration.
- SNMP (Simple Network Management Protocol) enumeration.
- Linux / Windows enumeration.
- SMB (Server Message Block) enumeration.

As an ethical hacker, you'll use the "Kali Distribution," which includes the community version of Metasploit as well as additional ethical hacking tools. However, if you wish to install Metasploit as a standalone programme, you may do so simply on Linux, Windows, or Mac OS X platforms. A Linux alternative to enum.exe for enumerating data from Windows and Samba hosts. Enum4linux is a tool for enumerating information from Windows and Samba systems. It is written in PERL and is basically a wrapper around the Samba tools smbclient, rpcclient, net and nmblookup.

Key Features:

- RID cycling (When Restrict Anonymous is set to 1 on Windows 2000).
- User listing (When Restrict Anonymous is set to 0 on Windows 2000).
- Listing of group membership information.
- Share enumeration.
- Detecting if the host is in a workgroup or a domain.
- Identifying the remote operating system.
- Password policy retrieval (using polenum).

CHAPTER 2

2.AIM AND SCOPE OF THE PRESENT INVESTIGATION

The aim is to enumerate the process where you collect details of the target like username, passwords, network information, hostnames, and other information that may be valuable. This allows pentesters to completely examine the systems. The pentesters collect information about the weak links during the enumeration phase of ethical hacking. The enumeration helps in finding the attack vectors and threats.

CHAPTER 3

3.EXPERIMENTAL OR MATERIALS AND METHODS USED

Hardware and software used:

- Virtual box (virtual environment).
- Kali Linux (attacker).
- Metasploitable 2 (vulnerable victim).

Step 1:

We need to get the Metasploitable target ip to get into the target server / machine.. To login into the metasploitable we use username as msfadmin. After logging in we need to use the command “ifconfig” and it gives the Ip-address. Using that we are going to gather information about the system.

Step 2:

Now, we need to get into kali Linux for enumeration. In kali Linux open the terminal window and will be typing a command sudo su. After that now we will be enumerating the target using command enum4linux. we have to type enum4linux and the Ip-address we collected using metasploitable like “enum4linux 192.168.0.5” by executing the following command, it starts extraction of all the information from the target ip-address. We can also use enum4linux parameters like -a+target(to get all details). likewise to get the userdetails we use -u, to get password policy, we use -p etc.

CHAPTER 4

4.RESULT AND DISCUSSION, PERFORMANCE ANALYSIS

In this study, we have gathered the information of the targeted system. From username, password, OS details and other details has been collected. Using this attacker can know about the weak links in the system and we are able to access the data.

CHAPTER 5

5.SUMMARY AND CONCLUSION

After we get the victim's information it is possible that we could hack the target machine and access the victim's system.. After the procedure, it is now possible to access all the information present in their system. This process can be extended using various commands in fetching more details of the system.

REFERENCES

- J Tang,Xia Hu,Huiji Gao,Huan Liu," Unsupervised Feature Selection for Multi-View Data in Social Media", Proceedings of the ACM international conference on Information and Knowledge management (2015),pp.1673-1678.
- Mohak Shah, Mario Marchand, and Jacques Corbeil, " Feature Selection with Conjunctions of Decision Stumps and Learning ", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 34, NO. 1,(2012) pp.174-186.
- Mohak Shah, Mario Marchand, and Jacques Corbeil, " Feature Selection with Conjunctions of Decision Stumps and Learning ", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 34, NO. 1,(2012) pp.174-186.

APPENDIX

SCREEN SHOT

