

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

JAYAPRADEESH. S.L

Reg no: 39120043



DEPARTMENT OF INFORMATION TECHNOLOGY

SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY

JEPPIAAR NAGAR, RAJIV GANDHI SALAI,

CHENNAI – 600119, TAMILNADU

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 JAYAPRADEESH. S.L (Reg no: 39120043) who carried out the project entitled "**Enumeration using Enum4linux**" under my supervision from February 2022 to April 2022.

Internal guide

Mrs. BEVISH JENILLA

Head of the department

Submitted for viva voce examination held on _____

Internal examiner

external examiner

DECLARATION

I, **JAYAPRADEESH. S.L** hereby declare that the project report entitled **Enumeration using Enum4linux** using Microsoft cognitive services done by me under the guidance of **Mrs.BEVISH JENILLA** is submitted in partial fulfillment of the requirements for the award of Bachelor of Technology Degree in Information Technology.

DATE: 19/11/2021

PLACE: CHENNAI

SIGNATURE OF THE CANDIDATE

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.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 **Mrs. Bevish jenilla**, for her 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



ABSTRACT

Enumeration is the collecting of data about a target in order to identify potential attack routes and help in exploitation. This process is essential for an attack to be successful because wasting time on exploits that don't work or might crash the machine can be devastating. Enumeration can be used to collect users, passwords, network information, hostnames, application data, services, or any other data that an attacker could find useful.

To simulate what happens in a real-world attack, we'll use Metasploitable 2 as the target and Kali Linux as the attacking machine. 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 provides a secure place to perform penetration testing and security research. All these will be operated on virtual box platform . Metasploitable 2 and kali linux will be imported in virtual box and 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	EXEPREMENTAL OR MATERAILS AND METHODS, ALGORITHM USED	3
4	RESULT AND DISCUSSION, PERFORMANCE ANALYSIS	4
5	SUMMARY AND CONCLUSION	5
	REFERENCE	6
	APPENDIX	
	SCREEN SHOT	7,8

1.CHAPTER

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 enumeration.
- NTP enumeration.
- SNMP enumeration.
- Linux/Windows enumeration.
- SMB 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 host is in a workgroup or a domain.
- Identifying the remote operating system.
- Password policy retrieval (using polenum).

2.CHAPTER

2.AIM AND SCOPE OF THE PRESENT INVESTIGATION

The aim is to, enumeration is process where you collect details of the target like username, passwords, network information's, 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.

3.CHAPTER

3.EXEPREMENTAL OR MATERAILS AND METHODS USED

Hardware and software used:

- virtual box (virtual environment).
- kali Linux (attacker).
- Metasploitable2 (victim).

Step 1:

The first thing is we need to get the Ip-address of the system so that we will be getting into the metasploitable2 through virtual. To login into the metasploitable we use username as msfadmin. Once getting in we need to use command ifconfig and it gives as the Ip-address. Using that we are going to gather information of the system.

Step 2:

Now, we need to get into kali Linux to enumeration. In kali Linux open terminal window and will be typing a command sudo us. After that now we will be using 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" in this way we need to type and clicking enter it starts gathering all the information of the system. Once its done you will get all the information of the system.

4.CHAPTER

4.RESULT AND DISCUSSION, PERFORMANCE ANALYSIS

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

CHAPTER .5

5.SUMMARY AND CONCLUSION

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

REFERENCE

- 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.

1. APPENDIX

SCREEN SHOT

```
(kali@kali)~$ enum4linux 192.168.1.6
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Apr 12 16:23:13 2022

|-----|
| Target Information |
|-----|
Target ..... 192.168.1.6
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

|-----|
| Enumerating Workgroup/Domain on 192.168.1.6 |
|-----|
[*] Got domain/workgroup name: WORKGROUP

|-----|
| Nbtstat Information for 192.168.1.6 |
|-----|
Looking up status of 192.168.1.6
METASPLOITABLE <00> - B <ACTIVE> Workstation Service
METASPLOITABLE <03> - B <ACTIVE> Messenger Service
METASPLOITABLE <20> - B <ACTIVE> File Server Service
WORKGROUP <00> - <GROUP> B <ACTIVE> Domain/Workgroup Name
WORKGROUP <1e> - <GROUP> B <ACTIVE> Browser Service Elections

MAC Address = 00-00-00-00-00-00

|-----|
| Session Check on 192.168.1.6 |
|-----|
[*] Server 192.168.1.6 allows sessions using username '', password ''

|-----|
| Getting domain SID for 192.168.1.6 |
|-----|
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[*] Can't determine if host is part of domain or part of a workgroup

|-----|
| OS information on 192.168.1.6 |
|-----|
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[*] Got OS info for 192.168.1.6 from smbclient:
[*] Got OS info for 192.168.1.6 from srvinfo:
METASPLOITABLE Wk Sv PrQ Unix NT SMT metasploitable server (Samba 3.0.20-Debian)
platform_id : 500
os version : 4.9
server type : 0*9a03

|-----|
| Users on 192.168.1.6 |
|-----|
index: 0*1 RID: 0*3f2 acb: 0*00000011 Account: games Name: games Desc: (null)
index: 0*2 RID: 0*1f5 acb: 0*00000011 Account: nobody Name: nobody Desc: (null)
index: 0*3 RID: 0*4ba acb: 0*00000011 Account: bind Name: (null) Desc: (null)
index: 0*4 RID: 0*402 acb: 0*00000011 Account: proxy Name: proxy Desc: (null)
index: 0*5 RID: 0*4b4 acb: 0*00000011 Account: syslog Name: (null) Desc: (null)
index: 0*6 RID: 0*bb4 acb: 0*00000010 Account: user Name: just a user,111 Desc: (null)
index: 0*7 RID: 0*42a acb: 0*00000011 Account: www-data Name: www-data Desc: (null)
index: 0*8 RID: 0*3e8 acb: 0*00000011 Account: root Name: root Desc: (null)
index: 0*9 RID: 0*3fa acb: 0*00000011 Account: news Name: news Desc: (null)
index: 0*a RID: 0*4c0 acb: 0*00000011 Account: postgres Name: PostgreSQL administrator,, Desc: (null)
index: 0*b RID: 0*3ec acb: 0*00000011 Account: bin Name: bin Desc: (null)
index: 0*c RID: 0*3f8 acb: 0*00000011 Account: mail Name: mail Desc: (null)
index: 0*d RID: 0*4c6 acb: 0*00000011 Account: distccd Name: (null) Desc: (null)
index: 0*e RID: 0*4ca acb: 0*00000011 Account: proftpd Name: (null) Desc: (null)
index: 0*f RID: 0*4b2 acb: 0*00000011 Account: dhcp Name: (null) Desc: (null)
index: 0*10 RID: 0*3ea acb: 0*00000011 Account: daemon Name: daemon Desc: (null)
index: 0*11 RID: 0*4b8 acb: 0*00000011 Account: sshd Name: (null) Desc: (null)
index: 0*12 RID: 0*3f4 acb: 0*00000011 Account: man Name: man Desc: (null)
```

```

| Password Policy Information for 192.168.1.6 |
|-----|

[+] Attaching to 192.168.1.6 using a NULL share
[+] Trying protocol 139/SMB...

[+] Found domain(s):

    [+] METASPLOITABLE
    [+] Builtin

[+] Password Info for Domain: METASPLOITABLE

    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000

    [+] Domain Refuse Password Change: 0
    [+] Domain Password Store cleartext: 0
    [+] Domain Password Lockout Admins: 0
    [+] Domain Password No Clear Change: 0
    [+] Domain Password No Anon Change: 0
    [+] Domain Password Complex: 0

    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: Not Set

[+] Retrieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 0

| Groups on 192.168.1.6 |
|-----|

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

```

```

)
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Gro
up)
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\wuwp (Local User
)
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\wuwp (Domain Gro
up)
S-1-5-21-1042354039-2475377354-766472396-1022 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1023 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1024 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Gro
up)
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local Use
r)
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Gr
oup)
S-1-5-21-1042354039-2475377354-766472396-1028 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1029 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1030 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Gro
up)
S-1-5-21-1042354039-2475377354-766472396-1032 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1033 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1034 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1035 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1036 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1037 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1038 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1039 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1040 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1042 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1044 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1046 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1047 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1048 *unknown*\*unknown* (8)
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)
S-1-5-21-1042354039-2475377354-766472396-1050 *unknown*\*unknown* (8)

| Getting printer info for 192.168.1.6 |
|-----|

No printers returned.

enum4linux complete on Tue Apr 12 16:23:18 2022

kali@kali:~$

```