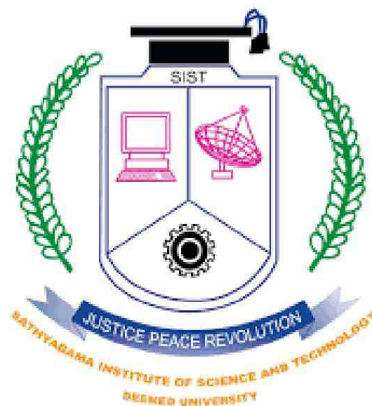


**PROFESSIONAL TRAINING REPORT**  
**at**  
**SATHYABAMA INSTITUTE OF SCIENCE AND**  
**TECHNOLOGY**  
**(DEEMED TO BE UNIVERSITY)**

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

By

**B.PRIYADHARSHANI**  
**REG. NO. 39120086**



**DEPARTMENT OF INFORMATION TECHNOLOGY**

**SCHOOL OF COMPUTING**

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

**(Established under Section 3 of UGC Act, 1956)**

**JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119**

**[www.sathyabamauniversity.ac.in](http://www.sathyabamauniversity.ac.in)**

**APRIL 2022**



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

**Accredited with Grade “A” by NAAC**  
(Established under Section 3 of DGC Act 1956)  
JEPPIYAR NAGAR, RAJIV GANDHI SALAI  
CHENNAI-600119  
[www.sathyabama.ac.in](http://www.sathyabama.ac.in)

---



**DEPARTMENT OF INFORMATION TECHNOLOGY**

**BONAFIDE CERTIFICATE**

This is to certify that this Project Report is the bonafide work Of  
**PRIYADHARSHANI. B (Reg. No: 39120086)** who carried out the project entitled  
“**Enumeration Of Target Using Nmap Scripting Engine**” under my supervision  
from March 2022 to April 2022.

**Internal Guide**

Dr.A. SIVASANGARI, M.E.,PH.D.,

**Head of the Department**

DR.R.SUBHASHINI, M.E.,PH.D.,

---

Submitted for Viva voce Examination held on \_\_\_\_\_

**Internal Examiner**

**External Examiner**

### **DECLARATION**

I, PRIYADHARSHANI.B (Reg. No. 39120086) hereby declare that the project report entitled “**Enumeration Of Target Using Nmap Scripting Engine**” done by me under the guidance of **Dr. A.SIVASANGARI, M.F.,PH.D.,** is submitted in partial fulfillment of the requirements for the award of Bachelor of Degree in Information Technology.

**DATE:**

**PLACE:**

**SIGNATURE OF THE CANDIDATE**

## **ACKNOWLEDGEMENT**

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA UNIVERSITY OF SCIENCE AND TECHNOLOGY** 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. R. Subhashini, M.E., Ph.D. Head 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. A.SIVASANGARI M.E.,PH.D.**, 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**

Nmap (Network Mapper) is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks. The Nmap Scripting Engine (NSE) is an incredibly powerful addition to Nmap, extending its functionality quite considerably. NSE Scripts are written in the Lua programming language, and can be used to do a variety of things: from scanning for vulnerabilities, to automating exploits for them.

SMB protocol commonly known as Server Message Block protocol has been a hot target among threat actors for many years because of its complexity and open nature. SMB is used to communicate over TCP/IP in a network. It is a client-server protocol used for file sharing, printers, serial ports and other resources on a network. Nbtstat is a utility that displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP), which helps troubleshoot NetBIOS name resolution issues. Normally, name resolution is performed when NetBIOS over TCP/IP is functioning correctly. A vulnerability is a flaw that could lead to the compromise of the confidentiality, integrity or availability of an information system. Vulnerability identification involves the process of discovering vulnerabilities and documenting these into an inventory within the target environment.

## TABLE OF CONTENTS

| CHAPTER<br>No. | TITLE                                                        | PAGE<br>No: |
|----------------|--------------------------------------------------------------|-------------|
|                | <b>ABSTRACT</b>                                              | i           |
|                | <b>LIST OF FIGURES</b>                                       | ii          |
|                | <b>LIST OF ABBREVIATIONS</b>                                 | iii         |
| <b>1</b>       | <b>INTRODUCTION</b>                                          |             |
|                | 1.1 WHAT IS CYBER SECURITY?                                  | 1           |
|                | 1.2 IMPORTANCE OF CYBER SECURITY                             | 1           |
|                | 1.3 COMMON TOOL USED FOR CYBER SECURITY                      | 1           |
|                | 1.4 REQUIREMENTS FOR PROJECT                                 | 1           |
| <b>2</b>       | <b>ENUMERATION OF TARGET USING<br/>NMAP SCRIPTING ENGINE</b> | <b>2</b>    |
|                | 2.1 WHAT IS NAMAP?                                           | 2           |
|                | 2.2 ADVANTAGES OF NMAP                                       | 2           |
|                | 2.3 NMAP FUNCTIONS                                           | 2           |
|                | 2.4 NMAP SCRIPTING ENGINE                                    | 3           |
|                | 2.5 NSE SCRIPT RULES                                         | 3           |
| <b>3</b>       | <b>EXPLANATION OF SMB ENUM USERS, NBSTAT<br/>AND VULN</b>    | <b>4</b>    |
|                | 3.1 SMB ENUMERATION                                          | 4           |
|                | 3.2 NMAP nbstat NSE SCRIPT                                   | 5           |
|                | 3.3 NMAP vuln NSE SCRIPTS                                    | 6           |
| <b>4</b>       | <b>RESULT AND COCLUSION</b>                                  | <b>7</b>    |
|                | 4.1 RESULT                                                   | 7           |
|                | 4.2 CONCLUSION                                               | 7           |
|                | <b>REFERENCE</b>                                             | <b>7</b>    |
|                | <b>APPENDIX</b>                                              | <b>7</b>    |
|                | A.SOURCE CODE                                                | 7           |
|                | B.SCREENSHOTS                                                | 8           |

## **LIST OF FIGURES**

| <b>FIGURE.NO</b> | <b>TITLE</b> | <b>PAGE.NO</b> |
|------------------|--------------|----------------|
| 1.1              | Kali Linux   | 1              |
| 1.2              | Vuln Script  | 6              |

## **LIST OF ABBREVIATIONS**

| <b>ABBREVIATIONS</b> | <b>EXPANSION</b>                  |
|----------------------|-----------------------------------|
| NSE                  | Nmap Scripting Engine             |
| Nmap                 | Network Mapper                    |
| SMB                  | Server Message Block              |
| IP                   | Internet Protocol                 |
| NetBIOS              | Network Basics Input\Ouput System |
| MAC                  | Media Access Control              |
| TCP                  | Transmission Contro; Protocol     |

## CHAPTER 1

### 1.INTRODUCTION

#### 1.1What is Cyber Security?

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as Information Technology Security, Ethical HackingIt 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. There are Five stages in Cybersecurity. They are,

- Information Gathering
- Enumeration /Scanning
- Vulnerability Assessment
- Reporting

Information Gathering and Enumeration plays the vital role in Cybersecurity

#### 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.

#### 1.3 COMMON TOOLS USED FOR CYBER SECURITY:

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

#### 1.4 REQUIREMENTS OF PROJECT:

1.1 kali linux

- Virtual box (Virtualization)
- Kali Linux (Main Operating system)
- Metasploitable (Vulnerable Machine)
- Nmap (sudo apt install nmap)



## CHAPTER 2

### ENUMERATION OF TARGET USING SCRIPTING ENGINE PROJECT

#### 2. OVERVIEW OF NMAP SCRIPTING ENGINE:

##### 2.1 WHAT IS NMAP?

**Nmap (Network Mapper)** It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities. Nmap can find information about the operating system running on devices. It can provide detailed information like OS versions, making it easier to plan additional approaches during penetration testing. During security auditing and vulnerability scanning, you can use Nmap to attack systems using existing scripts from the Nmap Scripting Engine

Nmap is a useful tool for network scanning and auditing purposes.

- It can search for hosts connected to the Network.
- It can search for free ports on the target host.
- It detects all services running on the host with the help of **operating system**.
- It also detects any **flaws** or **potential vulnerabilities** in networked system.

##### 2.2 ADVANTAGE OF NMAP:

- Nmap is open-source and **free** to use.
- It is used for auditing network systems as it can detect new servers.
- It will search for **subdomain** and Domain Name System.
- With the help of Nmap Scripting Engine (**NSE**), interaction can be made with the target host.
- It determines the nature of the service in the host and performs whether the host is a mail service or a web server:

##### 2.3 NMAP FUNCTIONS

Most of **Nmap's** standard functions are executed by using a single command.

- Ping Scanning
- Port Scanning
- Host scanning
- Disable DNS Resolution

## 2.4 NMAP SCRIPTING ENGINE:

The **Nmap Scripting Engine (NSE)** is an incredibly powerful addition to Nmap, extending functionality quite considerably. NSE. Its ability to let users write and share their own scripts, so you're not limited to relying on the Nmap default NSE scripts. Nmap offers a variety of types of scans in order to scan a host for its open services. Used to identify services on a host, the operating system running on the host NSE scripts are great for drafting proof-of-concept code since the modules are written in Lua, a simple yet powerful language. NSE scripts must be coded in lua language. It allows us to quickly program any task we have in mind with the help of the available NSE libraries. Its flexible syntax is easy to learn

- ❖ Needed to handle specific tasks that cannot be done easily in Nmap in C++.
- ❖ Motivations for using Lua.
- ❖ NSE uses Lua to allow scripts to run against a host in parallel.
- ❖ Scripts use bindings to Nmap libraries for performance and access to networking facilities.

NSE Scripts rule:

NSE scripts can have one of four different types of execution rule

- Prerule
- Postrule
- Portrule
- Host rule

Nmap uses the script rules to determine whether a script should be run against a target. **The Rule Section** defines necessary conditions for the script to execute. This section must contain at least one function from this list: **portrule, hostrule, prerule, postrule**

i) prerule scripts run once, before any hosts are scanned, during the script pre-scanning phase. hostrule and portrule scripts run after each batch of hosts is scanned. postrule scripts run once after all hosts have been scanned, in the script post-scanning phase. A script may run in more than one phase if it has several rules.

ii) prerule and postrule do not accept arguments. hostrule accepts a host table and may test, for example, the IP address or hostname of the target. portrule accepts both a host table and a port table for any port in the open, open|filtered, or unfiltered port states. Port rules generally test factors such as the port number, port state, or listening service name in deciding whether to run against a port

iii) Return a portrule that returns true when given an open port matching either a port number or service name and has not been listed in the exclude port directive of the nmap-service-probes file. If version intensity is lesser than rarity value, portrule always returns false.

vi) Advanced users may force a script to run regardless of the results of these rule functions by prefixing the script name (or category or other expression) with a + in the --script argument.

v) The current standard to choose between a prerule or a postrule is this: if the script is doing host discovery or any other network operation then the prerule should be used. postrule is reserved for reporting of data and statistics that were gathered during the scan.

vi) hostrule accepts a host table and may test, for example, the IP address or hostname of the target. portrule accepts both a host table and a port table for any port in the open, open|filtered, or unfiltered port.

## CHAPTER 3

### 3. EXPLANATION OF SMB ENUM USERS,NBSTAT AND VULN:

#### 3.1 SMB ENUMERATION:

**SMB (Server Message Block)** is a communication protocol for sharing files, printers and serial ports over a network. The protocol was primarily developed and designed for Windows environments, but is also used to share files between Windows and Linux. Nmap includes SMB scripts that offer service-level enumeration and vulnerability scanning, which can help identify potential misconfigurations and/or vulnerabilities. SMB is used to communicate over TCP/IP in a network. It is a client-server protocol used for file sharing, printers, serial ports and other resources on a network. SMB can allow other applications and users to access files or execute command on a remote server. A client application can read, write and execute files on the server depending upon the configuration of the SMB share. It is essential to keep the target we are achieving before enumerating any service. So in this particular case we will be getting system information, Null sessions, open shares and CVEs like Eternal Blue from this service. These open shares might include some sensitive information like Username, Password, Hashes, Keys, TGS etc. which can be used further in the process. So to conclude, as per my knowledge we enumerate SMB for below purposes:

- Null Sessions
- Open Shares
- CVEs (Eternal Blue, Eternal Romance etc)
- System Information

we can enumerate it and look for any potential vulnerabilities that can be exploited. We will be using various tools for that purpose:

- Nmap SMB Script
- SMBmap
- Rpcclient
- Nbtscan
- Enum4Linux

\ An SMB server may be configured to accept only one of two security levels, which differ in how a user is authenticated:

- User-level authentication - classic username and password authentication
- Share-level authentication - anonymous account is used to log in, after which the password is given.

User enumeration:

- ✓ System users can be enumerated through SMB with the `smb-enum-users` script: The goal of the script is to discover all users account that exist on a remote or vulnerable machine.

### 3.2 NMAP nbstat NSE SCRIPT:

A good to know command line tool that you can use is the **Nbtstat** command, this command can give you protocol statistic and TCP/IP connections using NetBIOS over TCP, and it is very useful command if you need to get information about IP address for example. It is also good for troubleshoot NetBIOS name resolution problems and to resolve NetBIOS names to IP addresses, it resolve the name using one of the following methods:

- Local cache lookup
- WINS lookup
- Network broadcast
- MHOSTS file lookup
- DNS server query

Nbtstat provides a number of options for getting NetBIOS information:

- Adapter status (-a for name, -A for address) lists a remote NetBIOS table.
- Cache (-c) lists a local cache of remote devices.
- Names (-n) lists local NetBIOS names.
- Resolved (-r) lists WINS names and broadcast names.

These Nbtstat commands allow you to communicate through NetBIOS parameters over TCP/IP. Commonly, NetBIOS is an unroutable protocol. However, the way Windows uses it over TCP/IP makes it possible to query other devices on your network by name or IP address.

From a security standpoint, you can use Nbtstat to query other machines on the network by name or IP address and understand what these users are doing.

The Nbtstat command is a great command to use when you need to display the NetBIOS over TCP/IP protocol statistics.

NetBIOS provides two primary communication methods. The datagram service allows for connectionless communication over a network, ideal for situations where fast transmission is preferred, such as error generation. The session service, on the other hand, allows two computers to establish a connection for reliable communication. NetBIOS also provides name services which allow for name and registration over the network. The nbstat.nse script attempts to retrieve the target's NetBIOS names and MAC address. The script displays the name of the computer and the logged-in user, if the verbosity is turned up, it displays all names the system thinks it owns. The nbstat.nse script does not have any arguments.

```
nmap -sU --script nbstat.nse <IP>
```

NetBIOS, which stands for network basic input/output system, is a service that allows computers to communicate over a network. However, NetBIOS is not a networking protocol, it is an **API**. It runs over TCP/IP via the NBT protocol, allowing it to function on modern networks.

To run through this technique, we'll be using Metasploitable 2, an intentionally vulnerable virtual machine, as our target machine.

### 3.3 NMAP vuln NSE SCRIPTS:

A vulnerability is a flaw that could lead to the compromise of the confidentiality, integrity or availability of an information system. Vulnerability identification involves the process of discovering vulnerabilities and documenting these into an inventory within the target environment.

The Kali Linux project, which involves the integration of multiple security tools into a security operating system. This Linux OS incorporates tools for various security tasks such as vulnerability identification.

The following are some of the vulnerability identification tools present within the Kali Linux operating system:

- Nessus Vulnerability Scanner
- OpenVAS Vulnerability Scanner
- Nikto Vulnerability Scanner
- Nmap Vulnerability Scanner
- Wapiti Vulnerability Scanner

These tools make it possible for security testers to identify a trove of information from a system, then cross-check this information for vulnerabilities. Information checked can vary from the operating system version to the patch level, software versions and so on

**vuln** are the common and most popular CVE detection scripts in the Nmap search engine. These scripts allow you to discover important information about system security flaws.

```
nmap --script=vuln <IP>
```

The scripts which come under the “vuln” category look for specific known vulnerabilities and only report back if any are identified in the target system.

```
/home/bullseye/Downloads/nmap-vulners/vulners.nse
/home/bullseye/Tools/sandmap/data/nse_external/httprecon-nse/httprecon.nse
/home/bullseye/Tools/sandmap/data/nse_external/michenriksen/http-apache-server-status.nse
/home/bullseye/Tools/sandmap/data/nse_external/michenriksen/http-rails-xml-parser.nse
/home/bullseye/Tools/sandmap/data/nse_external/s4n7h0/MS15-034.nse
/home/bullseye/Tools/sandmap/data/nse_external/s4n7h0/http-lfi.nse
/home/bullseye/Tools/sandmap/data/nse_external/s4n7h0/http-nikto-scan.nse
/home/bullseye/Tools/sandmap/data/nse_external/s4n7h0/http-shellshock.nse
/home/bullseye/Tools/sandmap/data/nse_external/s4n7h0/http-tenda-enum.nse
/home/bullseye/Tools/sandmap/data/nse_external/vulners/vulners.nse
/home/bullseye/Tools/sandmap/data/nse_external/vulscan/vulscan.nse
/usr/share/exploitdb/exploits/hardware/webapps/31527.nse
/usr/share/exploitdb/exploits/multiple/remote/33310.nse
/usr/share/golismero/wordlist/fingerprint/httprecon/httprecon.nse
/usr/share/nmap/scripts/acarsd-info.nse
/usr/share/nmap/scripts/address-info.nse
/usr/share/nmap/scripts/afp-brute.nse
/usr/share/nmap/scripts/afp-ls.nse
/usr/share/nmap/scripts/afp-path-vuln.nse
/usr/share/nmap/scripts/afp-serverinfo.nse
/usr/share/nmap/scripts/afp-showmount.nse
/usr/share/nmap/scripts/ajp-auth.nse
/usr/share/nmap/scripts/ajp-brute.nse
/usr/share/nmap/scripts/ajp-headers.nse
/usr/share/nmap/scripts/ajp-methods.nse
/usr/share/nmap/scripts/ajp-request.nse
/usr/share/nmap/scripts/allseeingeye-info.nse
```

#### 1.2 Vuln Script

## CHAPTER 4

### 4. RESULT AND CONCLUSION

#### 4.1 RESULT:

Thus I expected result of Nmap Scripting Engine to discover vulnerability is executed successfully.

#### 4.2 CONCLUSION:

- ❖ Nmap Scripting Engine helps to find the Vulnerability. NSE Scripts are written only in LUA programming language.
- ❖ Nmap is an open source Linux command line tool, Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect **vulnerability**
- ❖ Nmap Scripting Engine offers advanced service-level enumeration and takes it one step further by allowing for customized scripts.
- ❖ Nmap is commonly used for regular Network audits, but it can also be used for performing some redundant tasks like managing network inventory, managing schedules of service upgrades and monitoring uptime and downtime of different services.

#### REFERENCE:

- [1] OccupyTheWeb (2018), Linux For Hackers.
- [2] Ben Clark (2014), Red Team Field Manual..
- [3] Paulino Calderon (2018),.. Mastering the Nmap Scripting Engine

### APPENDIX

#### A.SOURCE CODE

```
sudo nmap --script smb-enum-users.nse 192.168.1.7  
sudo nmap -sU --script nbstat.nse 192.168.1.7  
sudo nmap --script=vuln 192.168.1.7
```

## B.SCREENSHOTS:

```
kali@kali:~$ sudo nmap --script smb-enum-users.nse 192.168.1.5
[6000] Passwords for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-09 11:43 EDT
Nmap scan report for 192.168.1.5
Host is up (0.00019s latency).
Not shown: 972 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2181/tcp  open  ceph-proxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6080/tcp  open  X11
9557/tcp  open  irc
9800/tcp  open  ajp13
8180/tcp  open  unknown

MAC Address: 08:00:27:55:CA:56 (Oracle VirtualBox virtual NIC)

Host script results:
smb-enum-users:
  METASPLOITABLE\Backup (RID: 1068)
    Full name: Backup
    Flags: Normal user account, Account disabled
  METASPLOITABLE\bin (RID: 1064)
    Full name: bin
    Flags: Normal user account, Account disabled
  METASPLOITABLE\bind (RID: 1210)
    Full name: bind
    Flags: Normal user account, Account disabled
  METASPLOITABLE\demon (RID: 1002)
    Full name: demon
    Flags: Normal user account, Account disabled
  METASPLOITABLE\dhcp (RID: 1202)
    Full name: dhcp
    Flags: Normal user account, Account disabled
  METASPLOITABLE\dstcda (RID: 1222)
    Full name: dstcda
    Flags: Normal user account, Account disabled
  METASPLOITABLE\ftp (RID: 1214)
    Full name: ftp
    Flags: Normal user account, Account disabled
```

```
  METASPLOITABLE\ftp (RID: 1214)
    Full name: ftp
    Flags: Normal user account, Account disabled
  METASPLOITABLE\games (RID: 1010)
    Full name: games
    Flags: Normal user account, Account disabled
  METASPLOITABLE\gnats (RID: 1002)
    Full name: Gnats Bug-Reporting System (admin)
    Flags: Normal user account, Account disabled
  METASPLOITABLE\irc (RID: 1076)
    Full name: irc
    Flags: Normal user account, Account disabled
  METASPLOITABLE\log (RID: 1206)
    Full name: log
    Flags: Normal user account, Account disabled
  METASPLOITABLE\libuid (RID: 1000)
    Full name: libuid
    Flags: Normal user account, Account disabled
  METASPLOITABLE\list (RID: 1016)
    Full name: Mailing List Manager
    Flags: Normal user account, Account disabled
  METASPLOITABLE\lp (RID: 1014)
    Full name: lp
    Flags: Normal user account, Account disabled
  METASPLOITABLE\mail (RID: 1010)
    Full name: mail
    Flags: Normal user account, Account disabled
  METASPLOITABLE\man (RID: 1012)
    Full name: man
    Flags: Normal user account, Account disabled
  METASPLOITABLE\msfadmin (RID: 3000)
    Full name: msfadmin,,,
    Flags: Normal user account
  METASPLOITABLE\mysql (RID: 1218)
    Full name: MySQL Server,,,
    Flags: Normal user account, Account disabled
  METASPLOITABLE\news (RID: 1018)
    Full name: news
    Flags: Normal user account, Account disabled
  METASPLOITABLE\nobody (RID: 501)
    Full name: nobody
    Flags: Normal user account, Account disabled
  METASPLOITABLE\postfix (RID: 1212)
    Full name: postfix
    Flags: Normal user account, Account disabled
  METASPLOITABLE\postgres (RID: 1216)
    Full name: PostgreSQL administrator,,,
    Flags: Normal user account, Account disabled
  METASPLOITABLE\proftpd (RID: 1226)
    Full name: proftpd
    Flags: Normal user account, Account disabled
  METASPLOITABLE\proxy (RID: 1026)
    Full name: proxy
    Flags: Normal user account, Account disabled
  METASPLOITABLE\root (RID: 1000)
    Full name: root
    Flags: Normal user account, Account disabled
  METASPLOITABLE\service (RID: 1004)
```

```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo nmap -sU -script nbstat.nse 192.168.1.5  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-09 11:47 EDT  
Nmap scan report for 192.168.1.5  
Host is up (0.00057s latency).  
Not shown: 993 closed ports  
PORT      STATE SERVICE  
53/udp    open  domain  
68/udp    open|filtered dhcpc  
69/udp    open|filtered tftp  
111/udp   open|filtered rpcbind  
137/udp   open|filtered netbios-ns  
138/udp   open|filtered netbios-dgm  
2049/udp  open  nfs  
MAC Address: 08:00:27:55:C4:56 (Oracle VirtualBox virtual NIC)  
  
Host script results:  
nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)  
Names:  
  METASPLOITABLE<00>  Flags: <unique><active>  
  METASPLOITABLE<03>  Flags: <unique><active>  
  METASPLOITABLE<20>  Flags: <unique><active>  
  \x01\x02_MSRWSS     \x02<01>  Flags: <group><active>  
  WORKGROUP<00>      Flags: <group><active>  
  WORKGROUP<1d>      Flags: <unique><active>  
  WORKGROUP<1e>      Flags: <group><active>  
  
Nmap done: 1 IP address (1 host up) scanned in 1088.55 seconds
```

```
kali@kali: ~  
File Actions Edit View Help  
Nmap done: 1 IP address (1 host up) scanned in 1088.55 seconds  
[kali@kali]~  
$ sudo nmap -script vuln 192.168.1.5  
[sudo] password for kali:  
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-09 12:08 EDT  
Nmap scan report for 192.168.1.5  
Host is up (0.00016s latency).  
Not shown: 977 closed ports  
PORT      STATE SERVICE  
21/tcp    open  ftp  
  ftp-vsftpd-backdoor:  
  VULNERABLE:  
  vsftpd version 2.3.4 backdoor  
  State: VULNERABLE (Exploitable)  
  IDS: CVE-2011-2523 RID:46539  
  vsftpd version 2.3.4 backdoor, this was reported on 2011-07-04.  
  Disclosure date: 2011-07-03  
  Exploit results:  
  Shell command: id  
  Results: uid=0(root) gid=0(root)  
  References:  
  https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb  
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523  
  http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html  
  https://www.securityfocus.com/bid/46539  
_sslv2-  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
  smtp-vuln-cve2018-13441:  
  - The SMTP server is not Exim: NOT VULNERABLE  
  ssl-dh-paramss:  
  VULNERABLE:  
  Anonymous Diffie-Hellman Key Exchange MITM Vulnerability  
  State: VULNERABLE  
  Transport Layer Security (TLS) services that use anonymous  
  Diffie-Hellman key exchange only provide protection against passive  
  eavesdropping, and are vulnerable to active man-in-the-middle attacks  
  which could completely compromise the confidentiality and integrity  
  of any data exchanged over the resulting session.  
  Check results:  
  ANONYMOUS DH GROUP 1  
  Cipher Suites: TLS_DH_anon_WITH_RC4_128_MD5  
  Modulus type: Safe prime  
  Modulus Source: postfix builtin  
  Modulus Length: 1024  
  Generator Length: 8  
  Public Key Length: 1024  
  References:  
  https://www.ietf.org/rfc/rfc2246.txt  
  Transport Layer Security (TLS) Protocol DHE_EXPORT Ciphers Downgrade MITM (Logjam)
```

```
File Actions Edit View Help

Diffie-Hellman Key Exchange Insufficient Group Strength
State: VULNERABLE
Transport Layer Security (TLS) services that use Diffie-Hellman groups
of insufficient strength, especially those using one of a few commonly
shared groups, may be susceptible to passive eavesdropping attacks.
Check results:
  Weak DH GROUP 1
  Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA
  Modulus type: Safe prime
  Modulus Source: postfix builtin
  Modulus Length: 1024
  Generator Length: 0
  Public Key Length: 1024
References:
  https://weakdh.org
ssl-poodle:
VULNERABLE:
SSL POODLE information leak
State: VULNERABLE
ID: CVE-2014-3566 BID:70574
The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
products, uses nondeterministic CBC padding, which makes it easier
for man-in-the-middle attackers to obtain cleartext data via a
padding-oracle attack, aka the "POODLE" issue.
Disclosure date: 2014-10-16
Check results:
  TLS_RSA_WITH_AES_128_CBC_SHA
References:
  https://www.openssl.org/~bodo/ssl-poodle.pdf
  https://www.imperialviolet.org/2014/10/16/poodle.html
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
  https://www.securityfocus.com/bid/70574
_sslv2-drown: ERROR: Script execution failed (use -d to debug)
53/tcp open domain
80/tcp open http
http-csrf:
  Spiderling limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.1.5
  found the following possible CSRF vulnerabilities:

  Path: http://192.168.1.5:80/dvwa/
  Form id:
  Form action: login.php

  Path: http://192.168.1.5:80/mutillidae/index.php?page=set-background-color.php
  Form id: id-bad-cred-tr
  Form action: index.php?page=set-background-color.php

  Path: http://192.168.1.5:80/mutillidae/index.php?page=user-poll.php
  Form id: idpollform
  Form action: index.php
_http-dombased-xss: Couldn't find any DOM based XSS.
http-enum:
```

```
File Actions Edit View Help

/docs/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
/icons/: Potentially interesting folder w/ directory listing
/index/: Potentially interesting folder
http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
ID: CVE-2007-6750
Slowloris tries to keep many connections to the target web server open and hold
them open as long as possible. It accomplishes this by opening connections to
the target web server and sending a partial request. By doing so, it starves
the http server's resources causing Denial Of Service.
Disclosure date: 2009-09-17
References:
  https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
  http://ha.ckers.org/slowloris/
http-sql-injection:
Possible sql for queries:
http://192.168.1.5:80/mutillidae/index.php?page=home.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=set-background-color.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=captured-data.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=notes.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=credits.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=home.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=home.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=documentation2how-to-access-Mutillidae-over-Virtual-Box-network.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=Framing.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=show-log.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=usage-instructions.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=show-log.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=capture-data.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?username=anonymous&page=password-generator.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=dns-lookup.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=source-viewer.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=mid-to-your-blog.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=change-log.htm?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=home.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=home.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=source-viewer.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=php-errors.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=user-info.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=site-footer-xss-discussion.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=secret-administrative-pages.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=mid-to-your-blog.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=html5-storage.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=arbitrary-file-inclusion.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=installation.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=login.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=user-info.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=documentation2vulnerabilities.php?K27K200R20sqlspider
http://192.168.1.5:80/mutillidae/index.php?page=text-file-viewer.php?K27K200R20sqlspider
```