

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
B.RAMANAN
REG. NUMBER :- 39120091



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 **B.RAMANAN (39120091)** who carried out the project entitled “**Enumeration of Target using Nmap Scripting Engine**” under my supervision November 2021.

Internal Guide

G.MATHIVANAN 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, **B. RAMANANA** hereby declare that the project report entitled **Enumeration of Target using Nmap Scripting Engine** done by me under the guidance of **Dr.G.MATHIVANAN 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:

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.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. G.MATHIVANAN 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



ABSTRACT

- **Nmap, short for 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.**
- **This chapter will introduce you to NSE, covering several topics from installation and development environment setup to advanced usage tips. If you are familiar with the following topics, you may skip this chapter**

(i)

LIST OF ABBREVIATION

ABBREVIATION	EXPANSION
NSE	Nmap Scripting Engine
Nmap	Network Mapper
SMB	Server Message Block
IP	Internet Protocol
NetBIOS	Network Basics Input Output System
MAC	Media Access Control

TABLE OF CONTENTS

No.	TITTLE	Page No.
	ABSTRACT	(i)
	List of Abbrevation	(ii)
1.	Introduction	
1.1	What is Cyber Security?	9
1.2	Importance of Cyber Security	9
1.3	Common Tool Used For Cyber Security	9
1.4	Requirements For Project	9
2.	Enumeration of Target Using Nmap Scripting Engine	
2.1	Overview of Nmap Using Scripting Engine	9
3.	Result And Conclusion	
3.1	Result	11
3.2	Conclusion	11
3.3	Reference	11
4.	Appendix	
4.1	A. Source Code	12
4.2	B. Screenshots	12

1. INTRODUCTION:-

1.1 What is Cyber Security?

Cyber security 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.

1.3 COMMON TOOLS USED FOR CYBER SECURITY

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

1.4 REQUIREMENTS FOR PROJECT:-

- Virtual box(Virtualization)
- Kali Linux(Main Operating System)
- Metasploitable(Vulnerable Machine)
- Nmap(Sudo APT Install Nmap)

2. Enumeration of Target Using Nmap Scripting Engine

2.1 Overview of Nmap Using Scripting Engine

What is Nmap?

Nmap, short for 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.

Though Nmap has evolved over the years and is extremely flexible, at heart it's a port-scan tool, gathering information by sending raw packets to system ports. It listens for responses and determines whether ports are open, closed or filtered in some way by, for example, a [firewall](#). Other terms used for port scanning include port discovery or enumeration.

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 targets 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.

Advantage of Nmap:-

Nmap has a lot of advantages that make it different from [other network scanning tools](#). Nmap is open-source and **free** to use.

Some other advantages are listed below.

- 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.

Nmap Functions:-

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

- Ping Scanning
- Port Scanning
- Host Scanning
- OS Scanning
- Scan Top Ports
- Output to Files
- Disable DNS Resolution.

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.

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 enumeration through SMB with the smb-enum users script:
`sudo nmap --script smb-enum-users.nse<IP>`
- The goal of the script is to discover all users account that exist on a remote or vulnerable machine.

NMAP nbstat NSE SCRIPT:-

The nbstat.nse script attempts to retrieve the target's NetBIOS names and MAC address. The script display the name of the computer and 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.

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

NetBIOS which stands for network basic input/output system, is a service that allows computers to communication 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.

NMAP vuln NSE SCRIPTS:

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

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

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

3. SUMMARY:-

3.1 RESULT:-

Thus I expected result of Nmap scripting engine to discover vulnerability is executed successfully.

3.2 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 admin 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 allowing for customized.

3.3 REFERENCE:-

1. Linux for hackers: Occupy The Web, 4 December 2018.
2. Red Team Field Manual: Ben clark, 11 February 2014.
3. Classic Shell Scripting: Hidden Commands that Unlock the Power of Unix.

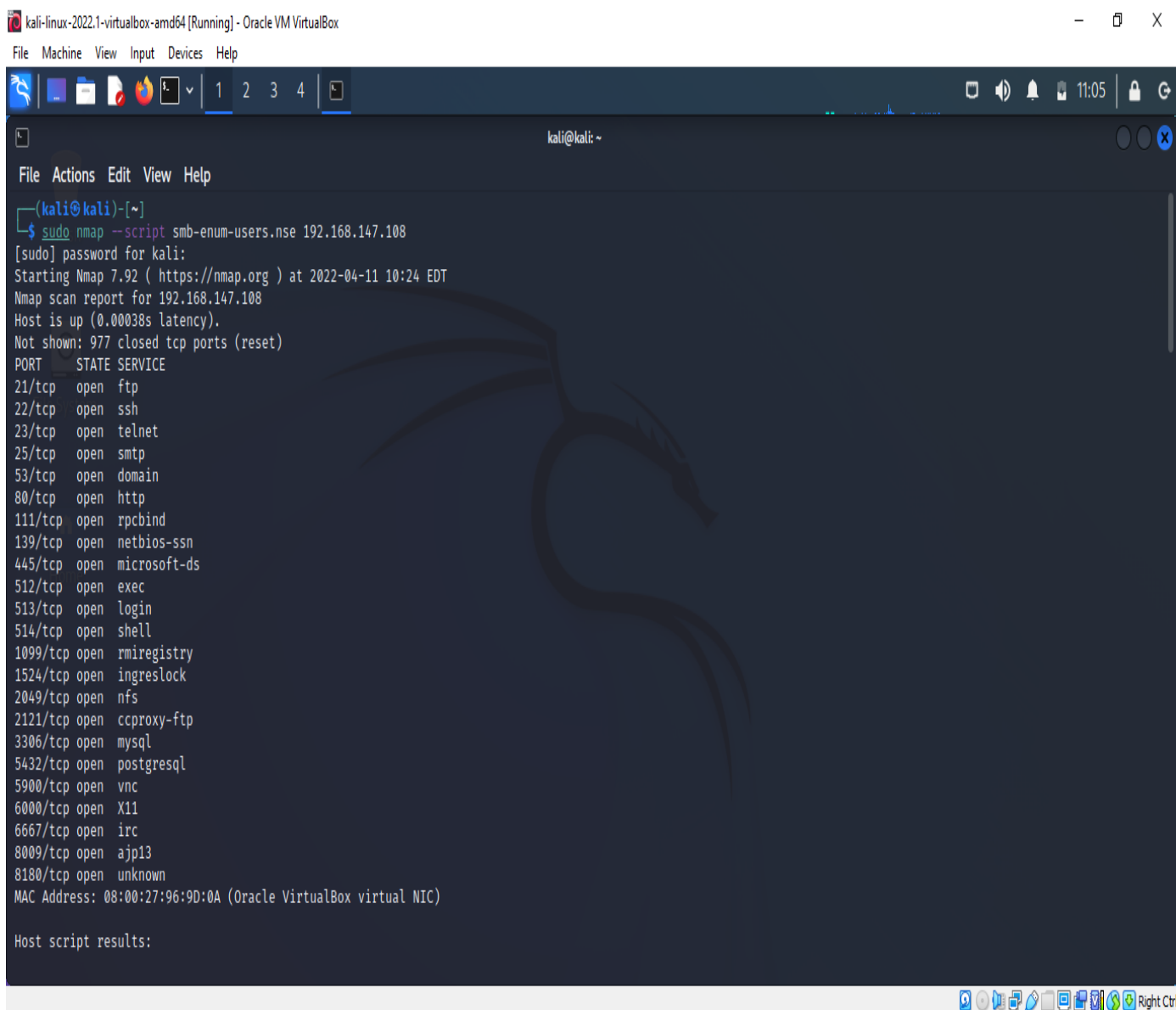
4. APPENDIX:-

4.1 SOURCE CODE:-

- i. `sudo nmap --script smb-enum-users.nse<IP>`
- ii. `sudo nmap -sU --script nbstat.nse<IP>`
- iii. `nmap -sV --script=vuln<IP>`

4.2 SCREENSHOTS:-

- i. `sudo nmap --script smb-enum-users.nse<IP>`



```
kali@kali: ~  
File Actions Edit View Help  
[kali@kali]~  
$ sudo nmap --script smb-enum-users.nse 192.168.147.108  
[sudo] password for kali:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-11 10:24 EDT  
Nmap scan report for 192.168.147.108  
Host is up (0.00038s latency).  
Not shown: 977 closed tcp ports (reset)  
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  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc  
6000/tcp  open  X11  
6667/tcp  open  irc  
8009/tcp  open  ajp13  
8180/tcp  open  unknown  
MAC Address: 08:00:27:96:9D:0A (Oracle VirtualBox virtual NIC)  
  
Host script results:
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
MAC Address: 08:00:27:96:9D:0A (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: 1004)
|   Full name: bin
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\bind (RID: 1210)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\daemon (RID: 1002)
|   Full name: daemon
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\dhcp (RID: 1202)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\distccd (RID: 1222)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\ftp (RID: 1214)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\games (RID: 1010)
|   Full name: games
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\gnats (RID: 1082)
|   Full name: Gnats Bug-Reporting System (admin)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\irc (RID: 1078)
|   Full name: ircd
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\klog (RID: 1206)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\libuuid (RID: 1200)
|   Flags: Normal user account, Account disabled
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
| METASPLOITABLE\root (RID: 1000)
|   Full name: root
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\service (RID: 3004)
|   Full name: ,,,
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\sshd (RID: 1208)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\sync (RID: 1008)
|   Full name: sync
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\sys (RID: 1006)
|   Full name: sys
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\syslog (RID: 1204)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\telnetd (RID: 1224)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\tomcat55 (RID: 1220)
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\user (RID: 3002)
|   Full name: just a user,111,,
|   Flags: Normal user account
| METASPLOITABLE\uucp (RID: 1020)
|   Full name: uucp
|   Flags: Normal user account, Account disabled
| METASPLOITABLE\www-data (RID: 1066)
|   Full name: www-data
|   Flags: Normal user account, Account disabled
|_
Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

(kali@kali)-[~]
└─$
```

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

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
| METASPLOITABLE\www-data (RID: 1066)
| Full name: www-data
| Flags: Normal user account, Account disabled

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds

(kali@kali)-[~]
└─$ sudo nmap -sU --script nbstat.nse 192.168.147.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 10:02 EDT
Nmap scan report for 192.168.147.108
Host is up (0.00085s latency).
Not shown: 957 closed udp ports (port-unreach), 39 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain
111/udp   open  rpcbind
137/udp   open  netbios-ns
2049/udp  open  nfs
MAC Address: 08:00:27:96:9D:0A (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__MSBROWSE__\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 1040.28 seconds

(kali@kali)-[~]
└─$
```

iii. `nmap -sV --script=vuln<IP>`

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
| (kali@kali)-[~]
└─$ nmap -sV --script=vuln 192.168.147.108
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-18 10:44 EDT
Nmap scan report for 192.168.147.108
Host is up (0.00081s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
| ftp-vsftpd-backdoor:
| VULNERABLE:
| vsFTPD version 2.3.4 backdoor
| State: VULNERABLE (Exploitable)
| IDs: CVE:CVE-2011-2523 BID:48539
| 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
| https://www.securityfocus.com/bid/48539
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
| sslv2-drown:
| ciphers:
| SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
| SSL2_RC2_128_CBC_WITH_MD5
| SSL2_RC4_128_WITH_MD5
| SSL2_DES_192_EDE3_CBC_WITH_MD5
| SSL2_DES_64_CBC_WITH_MD5
| SSL2_RC4_128_EXPORT40_WITH_MD5
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

SSL2_RC2_128_CBC_WITH_MD5
SSL2_RC4_128_WITH_MD5
SSL2_DES_192_EDE3_CBC_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
vulns:
CVE-2016-0800:
title: OpenSSL: Cross-protocol attack on TLS using SSLv2 (DROWN)
state: VULNERABLE
ids:
CVE:CVE-2016-0800
description:
The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and
other products, requires a server to send a ServerVerify message before establishing
that a client possesses certain plaintext RSA data, which makes it easier for remote
attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding
oracle, aka a "DROWN" attack.

refs:
https://www.openssl.org/news/secadv/20160301.txt
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0800
smtp-vuln-cve2010-4344:
The SMTP server is not Exim: NOT VULNERABLE
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
http-slowloris-check:
VULNERABLE:
Slowloris DOS attack
State: LIKELY VULNERABLE
IDs: CVE: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.
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

Disclosure date: 2009-09-17
References:
http://ha.ckers.org/slowloris/
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
http-csrf:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.147.108
Found the following possible CSRF vulnerabilities:

Path: http://192.168.147.108:80/dvwa/
Form id:
Form action: login.php

Path: http://192.168.147.108:80/dvwa/login.php
Form id:
Form action: login.php

Path: http://192.168.147.108:80/mutillidae/index.php?page=dns-lookup.php
Form id: iddnslookupform
Form action: index.php?page=dns-lookup.php

Path: http://192.168.147.108:80/mutillidae/index.php?page=text-file-viewer.php
Form id: id-bad-cred-tr
Form action: index.php?page=text-file-viewer.php
http-trace: TRACE is enabled
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-enum:
/tikiwiki/: Tikiwiki
/test/: Test page
/phpinfo.php: Possible information file
/phpMyAdmin/: phpMyAdmin
/doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
/icons/: Potentially interesting folder w/ directory listing
/index/: Potentially interesting folder
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

| /phpMyAdmin/: phpMyAdmin
| /doc/: 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-sql-injection:
| Possible sql queries:
| http://192.168.147.108:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=home.php
| http://192.168.147.108:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/?page=login.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
| http://192.168.147.108:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous
| http://192.168.147.108:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help

| http://192.168.147.108:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
| http://192.168.147.108:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
| _http-dombased-xss: Couldn't find any DOM based XSS.
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100003 2,3,4 2049/tcp nfs
| 100003 2,3,4 2049/udp nfs
| 100005 1,2,3 32972/tcp mountd
| 100005 1,2,3 35548/udp mountd
| 100021 1,3,4 48823/udp nlockmgr
| 100021 1,3,4 56011/tcp nlockmgr
| 100024 1 44264/udp status
| 100024 1 56514/tcp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
| rmi-vuln-classloader:
| VULNERABLE:
| RMI registry default configuration remote code execution vulnerability
| State: VULNERABLE
| Default configuration of RMI registry allows loading classes from remote URLs which can lead to remote code execution.
|
| References:
```

```
kali-linux-2022.1-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

kali@kali: ~
File Actions Edit View Help
| /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor File upload
| /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor File Upload
| /admin/jscript/upload.html: Lizard Cart/Remote File upload
| /webdav/: Potentially interesting folder
|_ http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_ http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf:
|_ Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.147.108
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.147.108:8180/admin/
|     Form id: username
|     Form action: j_security_check;jsessionid=F8F633C08EC0EFBB09B699B17E259EA3
|
|     Path: http://192.168.147.108:8180/servlets-examples/servlet/RequestParamExample
|     Form id:
|     Form action: RequestParamExample
|_ http-dombased-xss: Couldn't find any DOM based XSS.
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ smb-vuln-ms10-061: false
|_ smb-vuln-ms10-054: false
|_ smb-vuln-regsvc-dos: ERROR: Script execution failed (use -d to debug)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 662.90 seconds

(kali@kali)-[~]
$
```