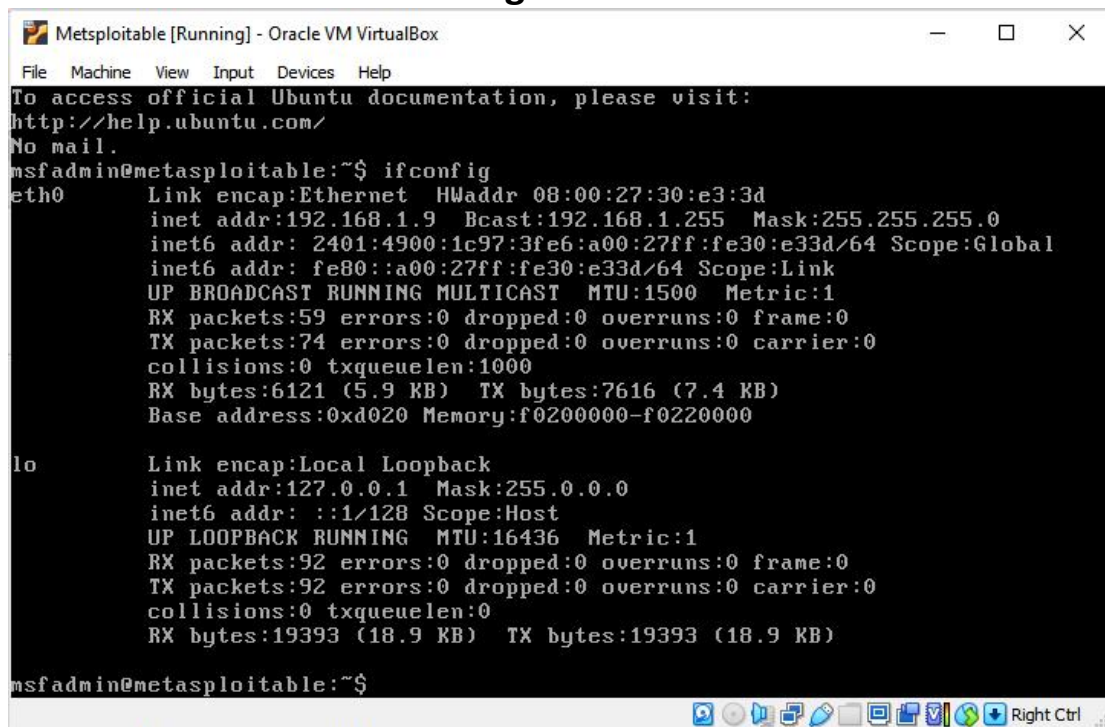


# Nmapping Report

## Finding IP ADDRESS



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:30:e3:3d
          inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2401:4900:1c97:3fe6:a00:27ff:fe30:e33d/64  Scope:Global
          inet6 addr: fe80::a00:27ff:fe30:e33d/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:59 errors:0 dropped:0 overruns:0 frame:0
          TX packets:74 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6121 (5.9 KB)  TX bytes:7616 (7.4 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

### Command to find the name of the device:

└─# **nmap -sV 192.168.1.9 -A**

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-10-01 20:37 IST

Nmap scan report for 192.168.1.9

Host is up (0.0032s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.3.4

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| FTP server status:

| Connected to 192.168.1.8

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| vsFTPD 2.3.4 - secure, fast, stable

|\_End of status  
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
| ssh-hostkey:  
| 1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)  
|\_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)  
23/tcp open telnet Linux telnetd  
25/tcp open smtp Postfix smtpd  
|\_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE  
10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,  
DSN  
| sslv2:  
| SSLv2 supported  
| ciphers:  
| SSL2\_RC2\_128\_CBC\_WITH\_MD5  
| SSL2\_DES\_192\_EDE3\_CBC\_WITH\_MD5  
| SSL2\_RC4\_128\_EXPORT40\_WITH\_MD5  
| SSL2\_RC2\_128\_CBC\_EXPORT40\_WITH\_MD5  
| SSL2\_DES\_64\_CBC\_WITH\_MD5  
|\_ SSL2\_RC4\_128\_WITH\_MD5  
| ssl-cert: Subject: commonName=ubuntu804-  
base.localdomain/organizationName=OCOSA/stateOrProvinceName=Th  
ere is no such thing outside US/countryName=XX  
| Not valid before: 2010-03-17T14:07:45  
|\_Not valid after: 2010-04-16T14:07:45  
|\_ssl-date: 2023-10-01T15:26:12+00:00; +15m46s from scanner time.  
53/tcp open domain ISC BIND 9.4.2  
| dns-nsid:  
|\_ bind.version: 9.4.2  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
|\_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2  
|\_http-title: Metasploitable2 - Linux  
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 33451/udp mountd  
| 100005 1,2,3 38263/tcp mountd

| 100021 1,3,4 37350/udp nlockmgr  
| 100021 1,3,4 53489/tcp nlockmgr  
| 100024 1 56182/udp status  
|\_ 100024 1 59872/tcp status  
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:  
WORKGROUP)  
445/tcp open :tV Samba smbd 3.0.20-Debian (workgroup:  
WORKGROUP)  
512/tcp open exec netkit-rsh rshcd  
513/tcp open login  
514/tcp open tcpwrapped  
1099/tcp open java-rmi GNU Classpath grmiregistry  
1524/tcp open bindshell Metasploitable root shell  
2049/tcp open nfs 2-4 (RPC #100003)  
2121/tcp open ftp ProFTPD 1.3.1  
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5  
| mysql-info:  
| Protocol: 10  
| Version: 5.0.51a-3ubuntu5  
| Thread ID: 10  
| Capabilities flags: 43564  
| Some Capabilities: LongColumnFlag, Support41Auth,  
SwitchToSSLAfterHandshake, SupportsCompression,  
Speaks41ProtocolNew, SupportsTransactions, ConnectWithDatabase  
| Status: Autocommit  
|\_ Salt: U;fq\$](N1GSLd1f0XN\f  
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7  
| ssl-cert: Subject: commonName=ubuntu804-  
base.localdomain/organizationName=OCOSA/stateOrProvinceName=Th  
ere is no such thing outside US/countryName=XX  
| Not valid before: 2010-03-17T14:07:45  
|\_ Not valid after: 2010-04-16T14:07:45  
|\_ ssl-date: 2023-10-01T15:26:12+00:00; +15m46s from scanner time.  
5900/tcp open vnc VNC (protocol 3.3)  
| vnc-info:  
| Protocol version: 3.3  
| Security types:  
|\_ VNC Authentication (2)  
6000/tcp open X11 (access denied)  
6667/tcp open irc UnrealIRCd

| irc-info:  
| users: 1  
| servers: 1  
| lusers: 1  
| lservers: 0  
| server: irc.Metasploitable.LAN  
| version: Unreal3.2.8.1. irc.Metasploitable.LAN  
| uptime: 0 days, 0:25:04  
| source ident: nmap  
| source host: BEFA2224.78DED367.FFFA6D49.IP  
|\_ error: Closing Link: jigsfqppo[192.168.1.8] (Quit: jigsfqppo)  
8009/tcp open ajp13?  
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1  
MAC Address: 08:00:27:30:E3:3D (Oracle VirtualBox virtual NIC)  
Device type: general purpose  
Running: Linux 2.6.X  
OS CPE: cpe:/o:linux:linux\_kernel:2.6  
OS details: Linux 2.6.9 - 2.6.33  
Network Distance: 1 hop  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN;  
OSs: Unix, Linux; CPE: cpe:/o:linux:linux\_kernel

#### Host script results:

|\_ smb2-time: Protocol negotiation failed (SMB2)  
|\_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>,  
NetBIOS MAC: <unknown> (unknown)  
| smb-os-discovery:  
| OS: Unix (Samba 3.0.20-Debian)  
| Computer name: metasploitable  
| NetBIOS computer name:  
| Domain name: localdomain  
| FQDN: metasploitable.localdomain  
|\_ System time: 2023-10-01T11:24:56-04:00  
|\_ clock-skew: mean: 1h15m46s, deviation: 2h00m01s, median: 15m45s  
| smb-security-mode:  
| account\_used: <blank>  
| authentication\_level: user  
| challenge\_response: supported  
|\_ message\_signing: disabled (dangerous, but default)

## TRACEROUTE

HOP RTT ADDRESS

1 3.15 ms 192.168.1.9

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 181.80 seconds

## Scan for Vulnerabilities

```
└─# nmap -p 21,23,25,53,80,445 --script vuln 192.168.1.9 -T5
```

Starting Nmap 7.94 ( <https://nmap.org> ) at 2023-10-01 21:15 IST

Nmap scan report for 192.168.1.9

Host is up (0.0011s latency).

PORT STATE SERVICE

21/tcp open ftp

| ftp-vsftpd-backdoor:

| VULNERABLE:

| vsFTPD version 2.3.4 backdoor

| State: VULNERABLE (Exploitable)

| IDs: BID:48539 CVE:CVE-2011-2523

| 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://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>

| <https://www.securityfocus.com/bid/48539>

|\_ <http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html>

23/tcp open telnet

25/tcp open smtp

| smtp-vuln-cve2010-4344:

|\_ The SMTP server is not Exim: NOT VULNERABLE

|\_ sslv2-drown: ERROR: Script execution failed (use -d to debug)

| ssl-poodle:

| VULNERABLE:

| SSL POODLE information leak

| State: VULNERABLE

| IDs: BID:70574 CVE:CVE-2014-3566

| 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: 2014-10-14

| Check results:

| TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

| References:

| <https://www.imperialviolet.org/2014/10/14/poodle.html>

| <https://www.openssl.org/~bodo/ssl-poodle.pdf>

| <https://www.securityfocus.com/bid/70574>

|\_ <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566>

| ssl-dh-params:

| 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 Suite: TLS\_DH\_anon\_EXPORT\_WITH\_RC4\_40\_MD5

| Modulus Type: Safe prime

| Modulus Source: Unknown/Custom-generated

| Modulus Length: 512

| Generator Length: 8

| Public Key Length: 512

| References:

| <https://www.ietf.org/rfc/rfc2246.txt>

| Transport Layer Security (TLS) Protocol DHE\_EXPORT Ciphers

Downgrade MitM (Logjam)

| State: VULNERABLE

| IDs: BID:74733 CVE:CVE-2015-4000

| The Transport Layer Security (TLS) protocol contains a flaw that is triggered when handling Diffie-Hellman key exchanges defined with the DHE\_EXPORT cipher. This may allow a man-in-the-middle

attacker

| to downgrade the security of a TLS session to 512-bit export-grade cryptography, which is significantly weaker, allowing the attacker to more easily break the encryption and monitor or tamper with the encrypted stream.

| Disclosure date: 2015-5-19

| Check results:

| EXPORT-GRADE DH GROUP 1

| Cipher Suite: TLS\_DHE\_RSA\_EXPORT\_WITH\_DES40\_CBC\_SHA

| Modulus Type: Safe prime

| Modulus Source: Unknown/Custom-generated

| Modulus Length: 512

| Generator Length: 8

| Public Key Length: 512

| References:

| <https://www.securityfocus.com/bid/74733>

| <https://weakdh.org>

| <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000>

```
| 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: 8
| Public Key Length: 1024
| References:
|_ https://weakdh.org
53/tcp open domain
80/tcp open http
|_ http-trace: TRACE is enabled
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-sql-injection:
| Possible sqli for queries:
|
http://192.168.1.9:80/mutillidae/index.php?page=login.php%27%20OR
%20sqlspider
| http://192.168.1.9:80/mutillidae/index.php?page=dns-
lookup.php%27%20OR%20sqlspider
| http://192.168.1.9:80/mutillidae/?page=user-
info.php%27%20OR%20sqlspider
| http://192.168.1.9:80/mutillidae/index.php?page=site-footer-xss-
discussion.php%27%20OR%20sqlspider
| http://192.168.1.9:80/mutillidae/index.php?page=set-background-
color.php%27%20OR%20sqlspider
|
http://192.168.1.9:80/mutillidae/index.php?page=framing.php%27%20
OR%20sqlspider
|
http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fh
```



ow-to-access-Mutillidae-over-Virtual-Box-  
network.php%27%20OR%20sqlspider  
| [http://192.168.1.9:80/mutillidae/index.php?page=browser-  
info.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=text-file-  
viewer.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider)  
|  
[http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20  
OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=html5-  
storage.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/?page=add-to-your-  
blog.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=user-  
info.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=source-  
viewer.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-  
blog.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-  
inclusion.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=user-  
poll.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider)  
|  
[http://192.168.1.9:80/mutillidae/index.php?page=notes.php%27%20OR  
%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=php-  
errors.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=capture-  
data.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-  
lookup.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=usage-  
instructions.php%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspider)  
| [http://192.168.1.9:80/mutillidae/index.php?page=change-  
log.htm%27%20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider)  
|  
[http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%  
20OR%20sqlspider](http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider)

| <http://192.168.1.9:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/?page=login.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=home.php&do=toggle-hints%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=home.php&do=toggle-security%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>

|  
<http://192.168.1.9:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=documentation%2FHow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=register.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=login.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>

|  
<http://192.168.1.9:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>  
| <http://192.168.1.9:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=login.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>

| <http://192.168.1.9:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=register.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=login.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>



| <http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>

| <http://192.168.1.9:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>

|

| <http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=login.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>

|  
<http://192.168.1.9:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>  
| <http://192.168.1.9:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>  
| <http://192.168.1.9:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>  
|  
<http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=login.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>

| <http://192.168.1.9:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>

|

<http://192.168.1.9:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=rene-magritte.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider>

|

<http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fhistory.php%27%20OR%20sqlspider>

ow-to-access-Mutillidae-over-Virtual-Box-  
network.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=browser-  
info.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=text-file-  
viewer.php%27%20OR%20sqlspider  
|  
http://192.168.1.9:80/mutillidae/index.php?page=register.php%27%20  
OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=html5-  
storage.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/?page=add-to-your-  
blog.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=user-  
info.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=source-  
viewer.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=arbitrary-file-  
inclusion.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=add-to-your-  
blog.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=capture-  
data.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=pen-test-tool-  
lookup.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=site-footer-xss-  
discussion.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=change-  
log.htm%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=set-background-  
color.php%27%20OR%20sqlspider  
| http://192.168.1.9:80/mutillidae/index.php?page=captured-  
data.php%27%20OR%20sqlspider  
|  
http://192.168.1.9:80/mutillidae/index.php?page=installation.php%27%  
20OR%20sqlspider  
|  
http://192.168.1.9:80/mutillidae/?page=login.php%27%20OR%20sqlspid  
er

- | <http://192.168.1.9:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/?page=credits.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspider&username=anonymous>
- | <http://192.168.1.9:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider>
- | <http://192.168.1.9:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider>
- | Possible sqli for forms:
- | Form at path: /mutillidae/, form's action: ./index.php?page=user-info.php. Fields that might be vulnerable:
- |\_ username
- | 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.

|    Disclosure date: 2009-09-17

|    References:

|    <http://hackers.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-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

|\_http-dombased-xss: Couldn't find any DOM based XSS.

| http-csrf:

| Spidering limited to: maxdepth=3; maxpagecount=20;

withinhost=192.168.1.9

|    Found the following possible CSRF vulnerabilities:

|    Path: <http://192.168.1.9:80/dvwa/>

|    Form id:

|    Form action: login.php

|    Path: <http://192.168.1.9:80/dvwa/login.php>

|    Form id:

|    Form action: login.php

|    Path: <http://192.168.1.9:80/mutillidae/index.php?page=login.php>

|    Form id: idloginform

|    Form action: index.php?page=login.php



| Path: http://192.168.1.9:80/mutillidae/index.php?page=dns-lookup.php

| Form id: iddnslookupform

| Form action: index.php?page=dns-lookup.php

|

| Path: http://192.168.1.9:80/mutillidae/?page=user-info.php

| Form id: id-bad-cred-tr

| Form action: ./index.php?page=user-info.php

|

| Path: http://192.168.1.9:80/mutillidae/index.php?page=set-background-color.php

| Form id: id-bad-cred-tr

|\_ Form action: index.php?page=set-background-color.php

445/tcp open microsoft-ds

MAC Address: 08:00:27:30:E3:3D (Oracle VirtualBox virtual NIC)

Host script results:

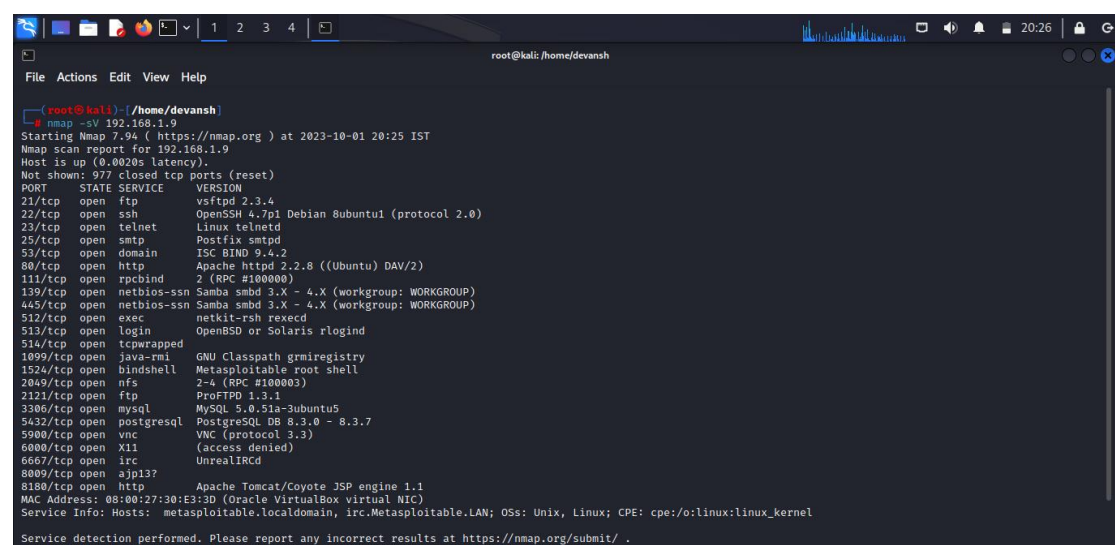
|\_smb-vuln-ms10-061: false

|\_smb-vuln-regsvcs-dos: ERROR: Script execution failed (use -d to debug)

|\_smb-vuln-ms10-054: false

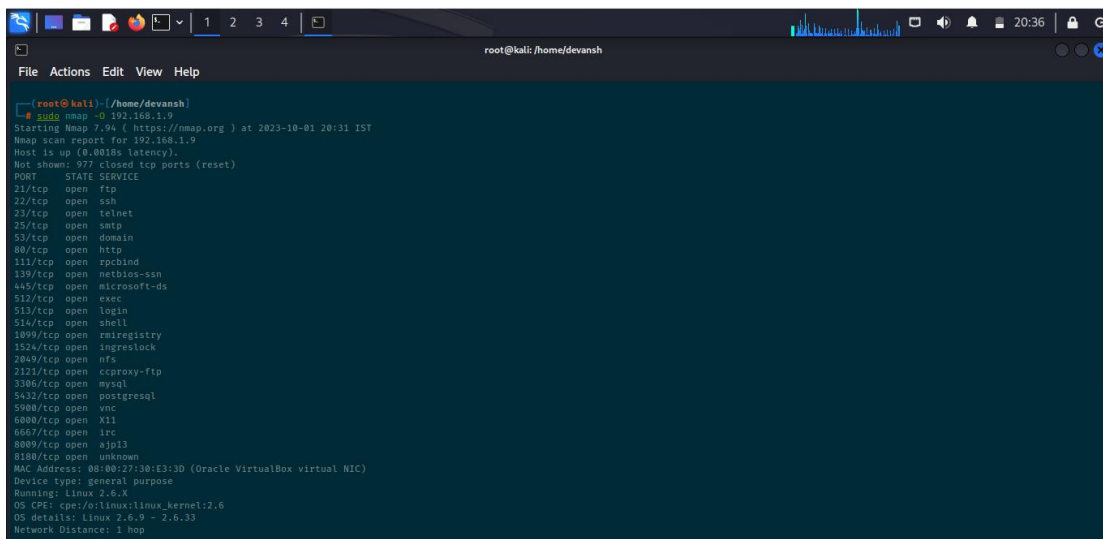
Nmap done: 1 IP address (1 host up) scanned in 324.02 seconds

## SCANNING VERSIONS



```
root@kali: /home/devansh
File Actions Edit View Help
root@kali) - (/home/devansh)
nmap -sV 192.168.1.9
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 20:25 IST
Nmap scan report for 192.168.1.9
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
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        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-nmi     GNU Classpath gmrregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13?
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:30:E3:3D (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

## SCANNING FOR OS



```
root@kali: ~/home/devansh
File Actions Edit View Help

root@kali:~/home/devansh
# sudo nmap -O 192.168.1.9
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-01 20:31 IST
Nmap scan report for 192.168.1.9
Host is up (0.0018s 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
1899/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2123/tcp  open  cproxy-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: 08:00:27:30:E3:3D (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

