

【port forwarding】 proxychains

```
kali@kali:~$ tail /etc/proxychains4.conf
```

```
kali@kali:~$ tail /etc/proxychains4.conf
#       proxy types: http, socks4, socks5, raw
#       * raw: The traffic is simply forwarded to the proxy
without modification.
#       ( auth types supported: "basic"-http "user/pass"-socks )
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 192.168.50.63 9999
```

配置了Proxychains後，現在我們可以使用我們Kali機器上的smbclient列出HRSHARES上的可用共享。與其連接到CONFLUENCE01上的埠口，我們將撰寫smbclient命令，就好像我們直接連接到PGDATABASE01一樣。與之前一樣，我們將使用-L指定列出可用共享，使用-U傳遞用戶名，並使用--password傳遞密碼。

接下來，我們只需在命令前添加proxychains。Proxychains將讀取配置文件，鉤入smbclient進程，並強制將所有流量通過我們指定的SOCKS代理。

```
kali@kali:~$ proxychains smbclient -L //172.16.50.217/ -U hr_admin --password=Welcome1234
```

```

kali@kali:~$ proxychains smbclient -L //172.16.50.217/ -U hr_admin
--password=Welcome1234
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-
gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Strict chain ... 192.168.50.63:9999 ...
172.16.50.217:445 ... OK

      Sharename      Type      Comment
      -----      -
      ADMIN$         Disk      Remote Admin
      C$              Disk      Default share
      IPC$            IPC       Remote IPC
scripts           Disk
      Users          Disk
Reconnecting with SMB1 for workgroup listing.
[proxychains] Strict chain ... 192.168.50.63:9999 ...
172.16.50.217:139 ... OK
[proxychains] Strict chain ... 192.168.50.63:9999 ...
172.16.50.217:139 ... OK
do_connect: Connection to 172.16.50.217 failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
kali@kali:~$

```

🕒 修訂版本 #1

★ 由 treeman 建立於 21 🕒 @🕒 2024 19:20:42

✍ 由 treeman 更新於 8 🕒 G🕒 2024 09:52:05