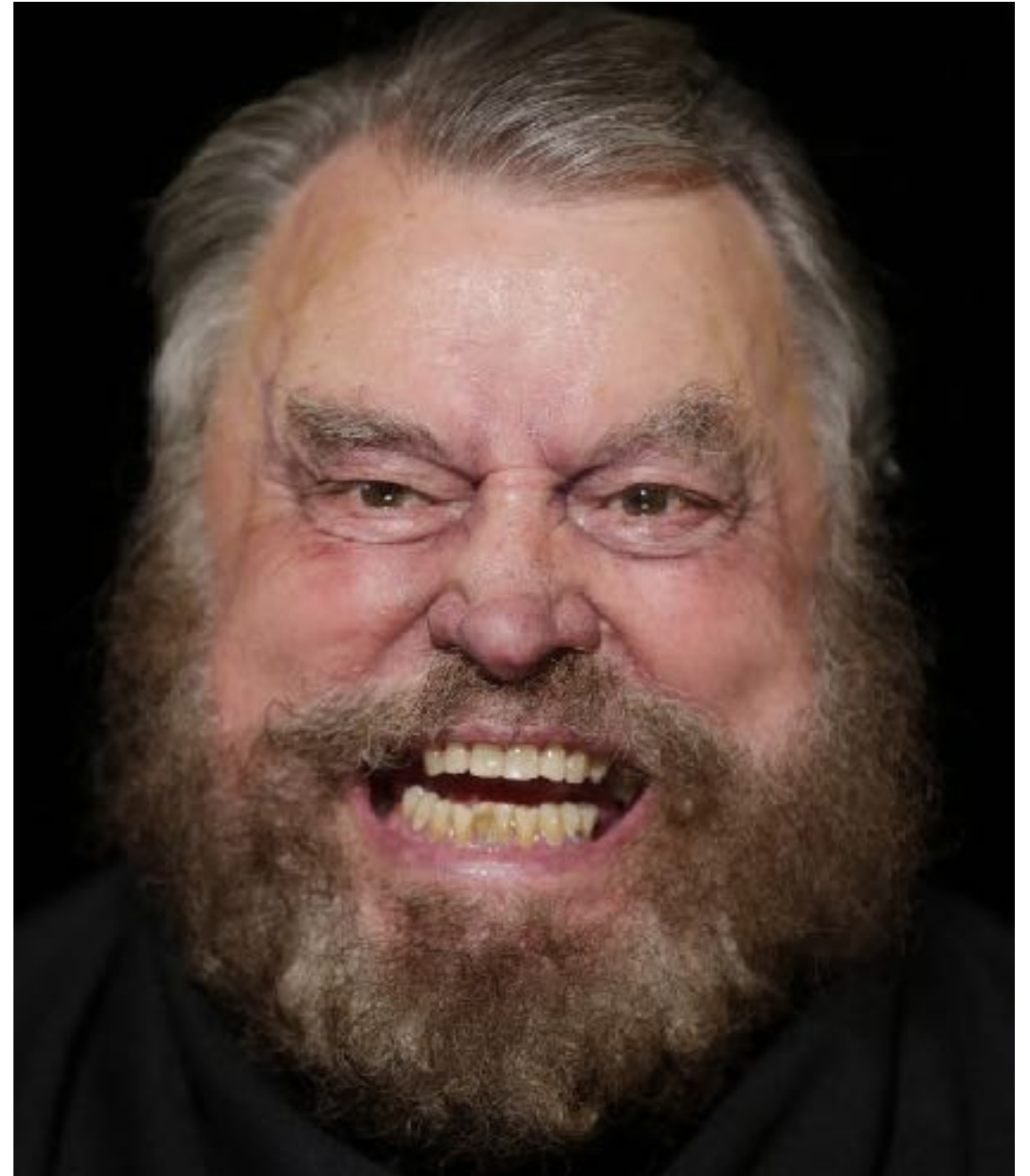


Get-GPTrashFire



Identifying and Abusing Vulnerable Configurations in MS
AD Group Policy

I'm this guy.

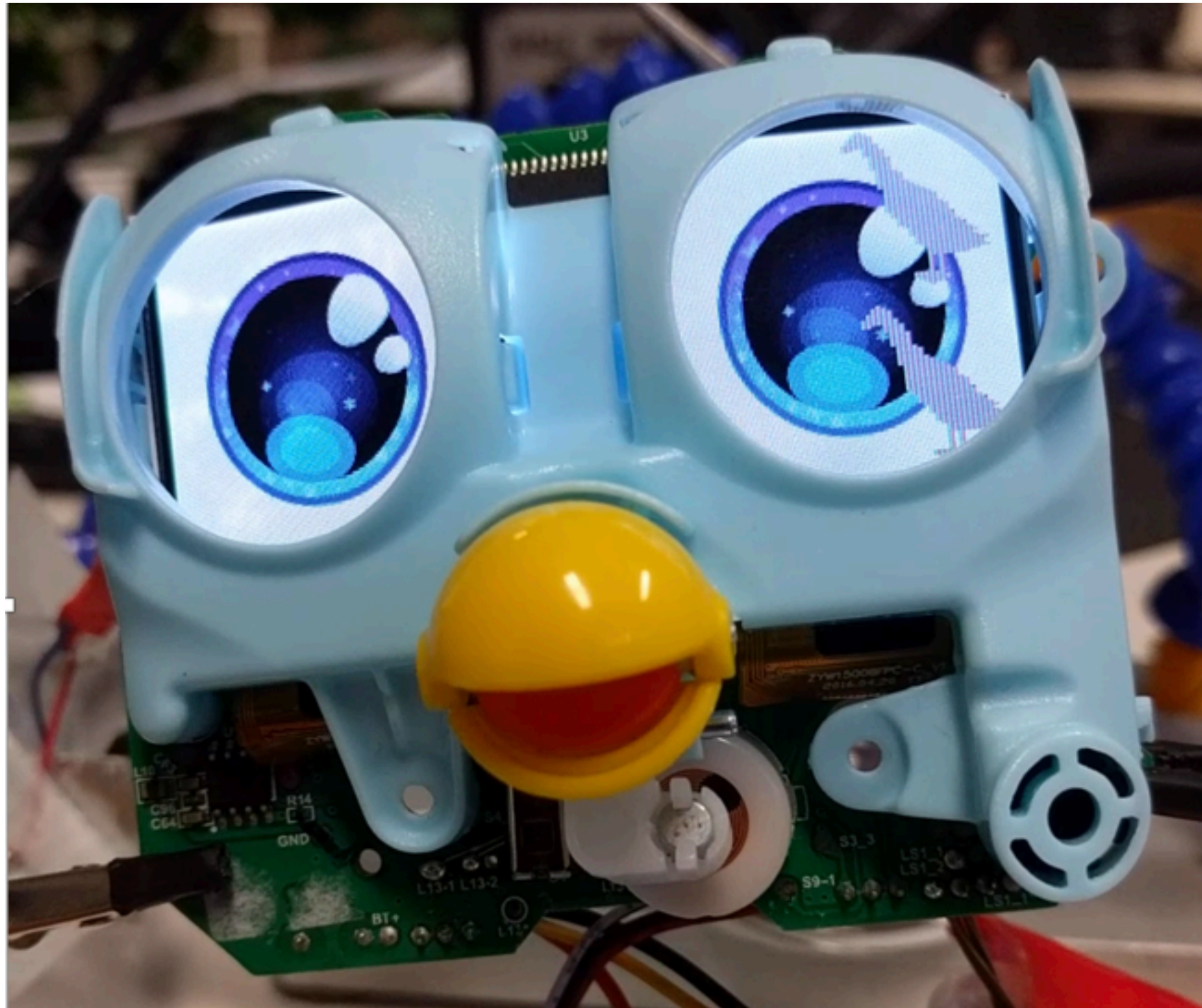
- I'm Mike Loss
- @mikeloss on Twitter
- @l0ss on Slack
- I do breaking of things.
- I'm not really that guy.
- That's Brian Blessed.



I work for one of these
guys.

IX	ISK
 A cartoon character with a large, bulbous nose, a yellow mustache, and a black tank top. He is wearing a grey helmet with white wings. He is holding a small object in his right hand and pointing with his left index finger.	 A large, bold, red asterisk symbol.

I was mean to this guy.



“You could do a whole talk about owning stuff using screwups in Group Policy.”

–Me, Self-owning at WAHCKon}OxV)] - 2017

I'm gonna try to answer these questions:

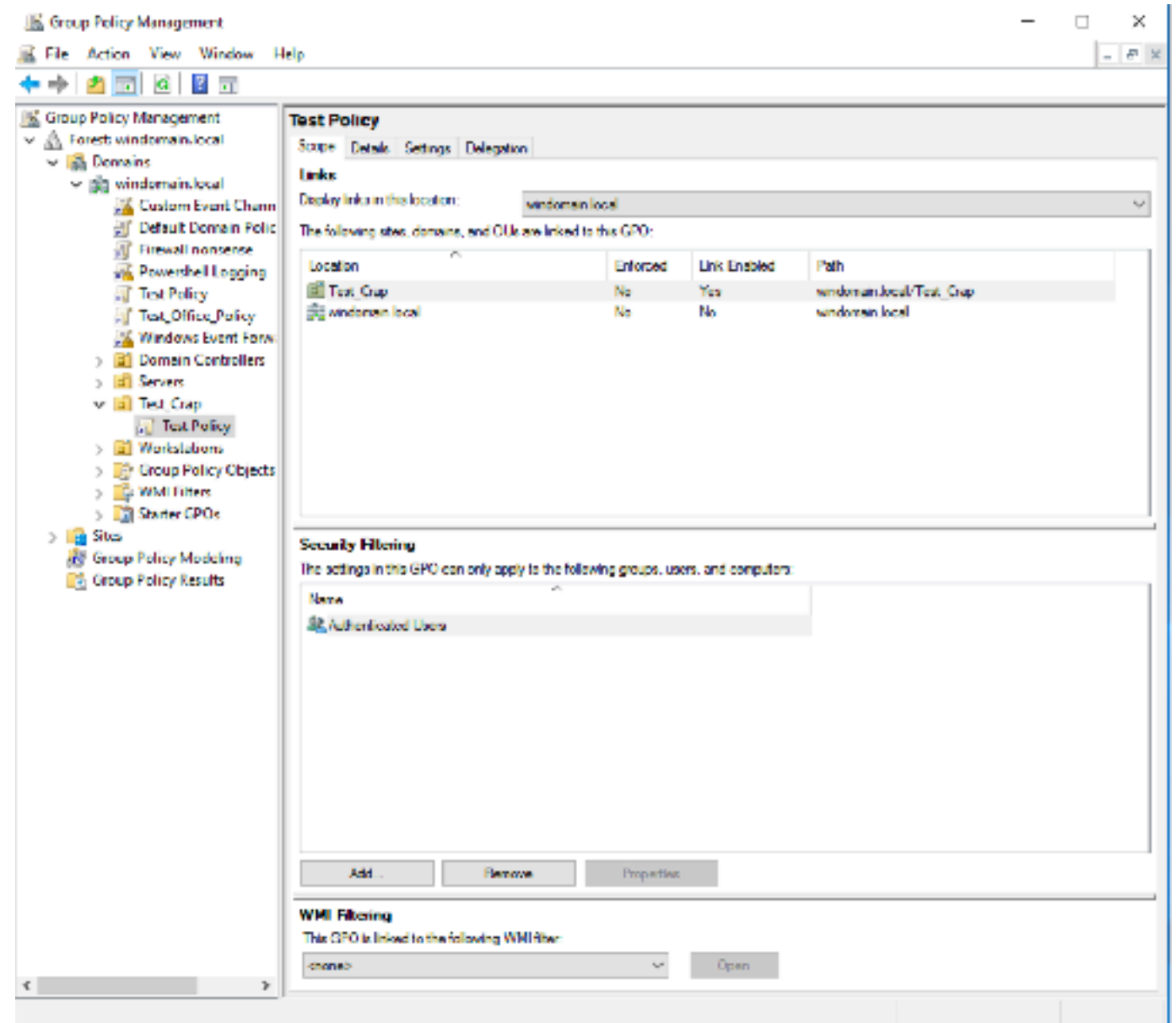
- What is Group Policy?
- Why should I, a cool hacker person, give a crap?
- How do I look at it?
- What fun things can I do with it?
- Is there a script? I'm a hacker, and hackers like scripts.

I'm gonna try to answer these questions:

- What is Group Policy?
- Why should I, a cool hacker person, give a crap?
- How do I look at it?
- What fun things can I do with it?
- Is there a script? I'm a hacker, and hackers like scripts.

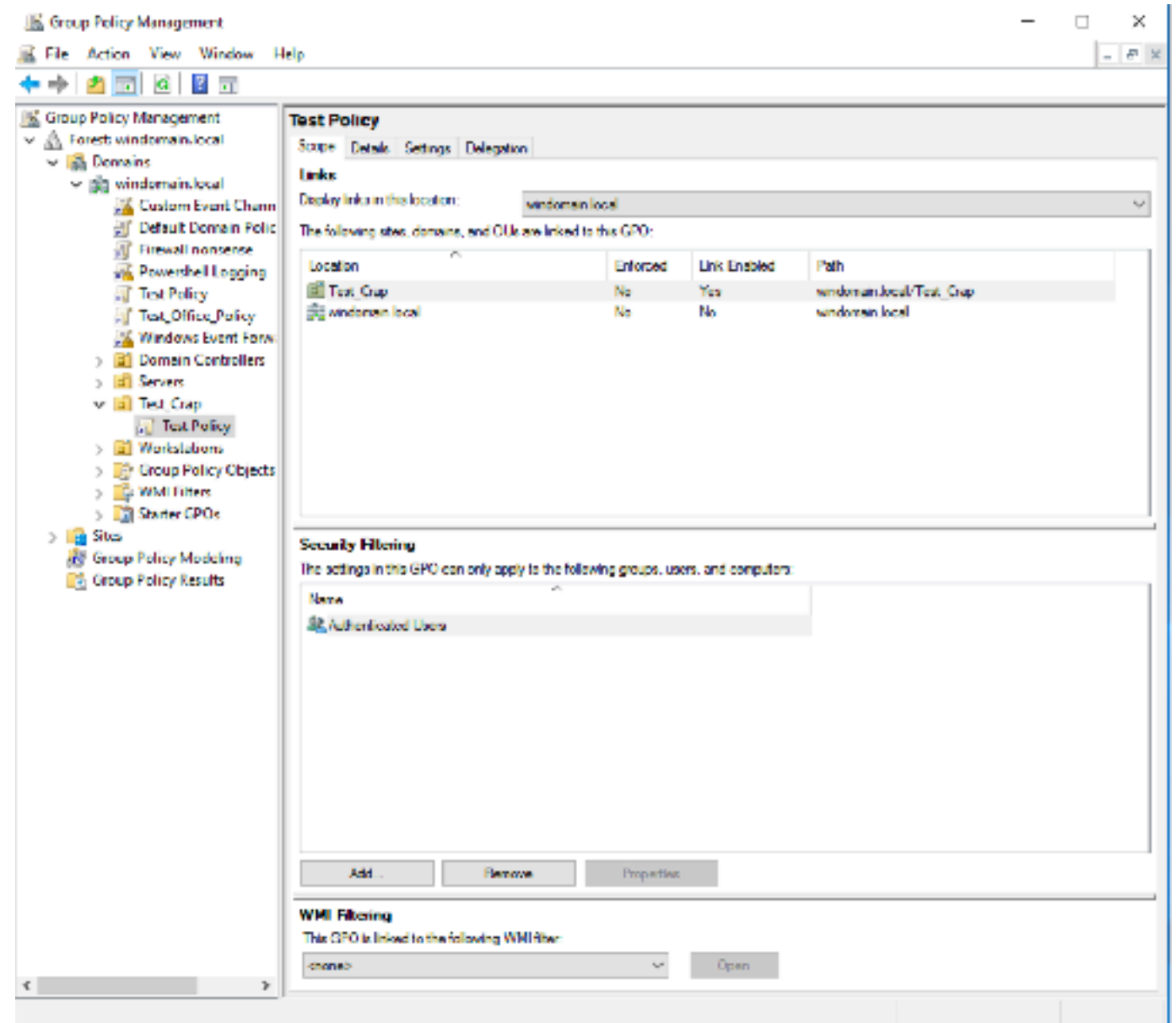
What is Group Policy?

- Built into Microsoft AD
- Sort-of configuration management system
- Configure settings in Group Policy Objects (GPOs)
 - Assign GPOs to OUs (folders) in AD
 - Settings apply automatically to users and computers in that OU
 - Applied every 90 mins (with 30 minute jitter) - every 5 minutes on Domain Controllers



What is Group Policy?

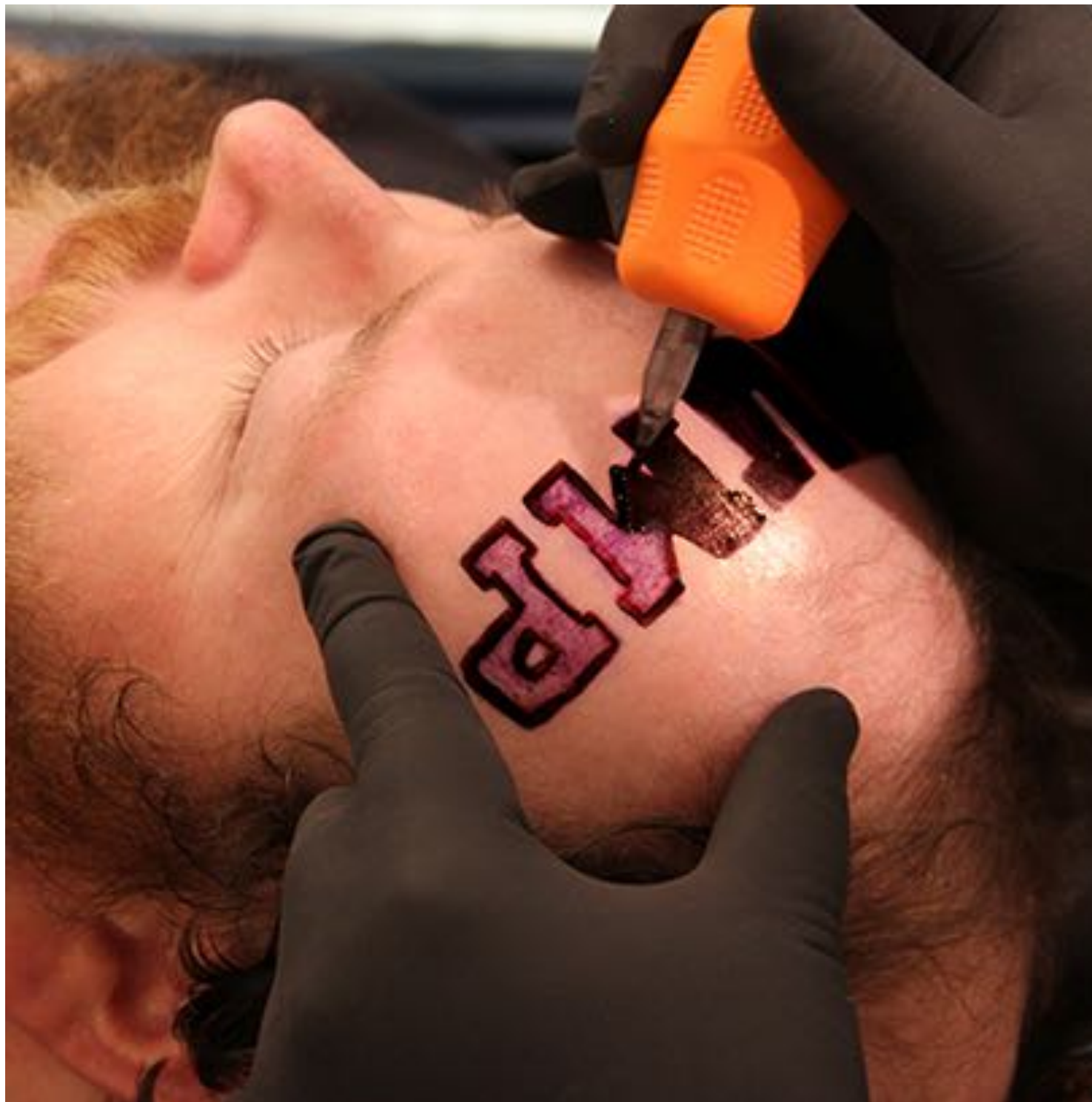
- Built into Microsoft AD
- Sort-of configuration management system
- Configure settings in Group Policy Objects (GPOs)
 - Assign GPOs to OUs (folders) in AD
 - Settings apply automatically to users and computers in that OU
 - Applied every 90 mins (with 30 minute jitter) - every 5 minutes on Domain Controllers



Why should I care?



Why should I care?



Really horrible mistakes.

**OK, I want to gawp at other
people's horrible mistakes.
How do I do that?**



Get-...pseudo-legible crap from SYSVOL?

\\domain.tld\SYSVOL\domain.tld\Policies

[illegible]

Get-GPOReport



- If you're on a machine that is a domain member:

```
Get-GPOReport -All -ReportType Html -Path C:\temp\gporeport.html -Domain $domain
```

- If not, do this first:

```
C:\windows\system32\runas.exe /netonly /user:user@domain.tld powershell.exe
```

- If you want an XML report (you do) then do it with:

```
-ReportType XML
```


So now I have 165MB of barely-legible HTML that crashes every browser I try to view it in, and an enormous wad of XML with a structure that is inconsistent at best.



This is hard and gross and I'm angry and I want someone else to make it easier.

```
github.com/mikeloss
@mikeloss
```

PowerShell because I am giant idiot.

```
github.com/mikeloss
@mikeloss
```

PowerShell because I am giant idiot.



The Goods



The Goods



Get-GPOACLs

- GPOs have ACLs.
- Admins hand out excessive privilege.
- If you can edit a GPO, you own every user and computer it applies to.

TattCorp_Workstation_Policy

Policy UID: {D7C702DB-B93E-4172-9AED-F1A2AB621BB9}

Policy created on: 1/30/18 12:19:00 PM

Policy last modified: 1/30/18 12:22:49 PM

Policy owner: forest1\Domain Admins

Linked OU: Work

Link enabled: true

GPO Permissions

#####

Trustee

AD\People_With_Tribal_Tattoos...

Access

Own stuff.

Type

Allow



Get-GP0RegKeys

- Manually defined registry entries, never know what you'll find here.
- VNC password
- AV disable password
- Autologon password

```
Get-GP0RegKeys - User Policy
#####
Action          U
Value           asdgasdg
Key             SOFTWARE
Hive            HKEY_LOCAL_MACHINE
Name           asdf
```



Get-GPORegSettings

- All kinds of settings that are defined in the registry
- If you add extra policy templates (ADMX files) to Group Policy, this is where those policies show up, e.g. MS Office, Citrix, etc.

```
Get-GPORegSettings - Computer Policy
#####
State                               Enabled
Setting Name                       Internet proxy servers for apps
Supported                          At least Windows Server 2012, Windows 8 or Windows RT
Explain                            This setting does not apply to desktop apps....
Category                           Network/Network Isolation
State                               Enabled
Name                               Domain Proxies
Value                              internal.proxy.tld

State                               Enabled
Setting Name                       Intranet proxy servers for apps
Supported                          At least Windows Server 2012, Windows 8 or Windows RT
Explain                            This setting does not apply to desktop apps....
Category                           Network/Network Isolation
State                               Enabled
Name                               Type a proxy server IP address for the intranet
Value                              whee.proxy.secret
```



Get-GPOFWSetting

- Windows Firewall settings.
- Useful to know, not gonna get you shell on its own.

```
Get-GPOFWSettings - All Policy
#####
Firewall Profile           PrivateProfile
DefaultInboundAction       false
DefaultOutboundAction      false
EnableFirewall             true

Firewall Profile           DomainProfile
EnableFirewall             false
```

Get-GPOUsers

- Creating and modifying and deleting local users.
- Good old fashioned GPP Passwords

```
Get-GPOUsers - Computer Policy
#####
Disabled                                0
neverExpires                           0
noChange                               0
Name                                   scrooge
Description                             quack quack
Password                               schedtaskpass
changeLogon                            0
UserName                               scrooge
```



Get-GPOGroups

- Changes to local groups
 - Adding/removing local and domain users and groups to them
 - Creating new ones

```
Get-GPOGroups - Computer Policy
#####
Group Name          Backup Operators
Name                Backup Operators
Action              ADD
Name                Domain Users
```



Get-GPOFileUpdate

- Usually used to copy a file from file share > local FS
- If it's an executable, and you can edit it...
- Config files often have creds, e.g. SQL conn. strings

```
Get-GPOFileUpdate - User Policy
#####
Action          U
targetPath      C:\Users\Scrooge\Desktop\fix_things.ps1
Name            fix_things.ps1
fromPath        \\badly\secured\network\share\hack_things.ps1

Get-GPOFileUpdate - Computer Policy
#####
Action          U
targetPath      C:\Users\l0ss\Desktop\eyebileachPls.ps1
Name            thing3.bat
fromPath        \\ive.seen.things\i\cant\unsee\
```



Get-GPOMSIIInstallation

- Does what it says on the tin.
- Installs an application from an MSI file, usually on a fileshare.
- If you can edit the MSI file... you get the picture.

```
Get-GPOMSIIInstallation - Computer Policy
#####
Name          Goofy Font Pack
Path          \\windomain.local\SYSVOL\windomain.local\scripts\MSI\Fonts_Not_Malware.msi
```



Get-GPOSchedTasks

- Creates, modifies, and deletes scheduled tasks on the target host.
- Definition can include creds
- If the thing being run is on a network share and you can edit it...
- Don't forget to look at args!

```
Get-GPOSchedTasks - Computer Policy
#####
args                -doesCalcHaveArgs
Action              U
runAs               Donald
Password            schedtaskpass
Name                schedtask
appName             calc.exe
startMinutes        0
startHour           22
type                DAILY
```



Get-GPOFolderRedirection

- Redirects folders in a user's homedir.
- Exploitation difficulty varies from 'trivial' to 'time to get creative'.

```
Get-GPOFolderRedirection - All Policy
```

```
#####
```

```
ID {FDD39AD0-238F-46AF-ADB4-6C85480369C7}
```

```
Target Group FOREST1\lowprivusers
```

```
DestPath C:\temp\%USERNAME%\Documents
```

```
Target SID s-1-5-21-888228836-1552922583-4278570199-1110
```



Get-GPOSecurityOption

- Misc security guff, surprisingly not that exciting
- Lots of stuff that could be useful in the right circumstances

```
Get-GPOSecurityOptions - All Policy
#####
Name                                Network access: Remotely accessible registry paths
KeyName                             MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\Machine
Path/Pipe2                           Software\Microsoft\Windows NT\CurrentVersion
Path/Pipe0                           System\CurrentControlSet\Control\ProductOptions
Path/Pipe1                           System\CurrentControlSet\Control\Server Applications

Name                                Network access: Remotely accessible registry paths and sub-paths
KeyName                             MACHINE\System\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\Machine
Path/Pipe4                           Software\Microsoft\OLAP Server
Path/Pipe2                           System\CurrentControlSet\Control\Print\Printers
Path/Pipe7                           System\CurrentControlSet\Control\Terminal Server\UserConfig
Path/Pipe6                           System\CurrentControlSet\Control\Terminal Server
Path/Pipe8                           System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Path/Pipe5                           System\CurrentControlSet\Control\ContentIndex
Path/Pipe0                           Software\Microsoft\Windows NT\CurrentVersion\Print
Path/Pipe3                           System\CurrentControlSet\Services\Eventlog
Path/Pipe1                           Software\Microsoft\Windows NT\CurrentVersion\Windows
Path/Pipe10                          System\CurrentControlSet\Services\SysmonLog
Path/Pipe9                           Software\Microsoft\Windows NT\CurrentVersion\Perflib
```

Get-GPOAccountSetting

- Password policy
- Account lockout policy
- Cleartext password storage

```
Get-GPOAccountSettings - All Policy
#####
Type                                Password
SettingBoolean                     true
Name                                ClearTextPassword
```

Get-GPOScripts

- Startup and shutdown scripts.
- If you can edit them, you own the user/computer they apply to.
- Sometimes they have hard-coded creds in them. Delightful!

```
Get-GPOScripts - Computer Policy
#####
Parameters          -dont googleBadTattoos
Command              \\i.regret.the\tattoo\theme.bat
Type                 Startup
```



Get-GPONetworkShares

- Creates, modifies, or deletes file shares.

```
Get-GPONetworkShares - All Policy
#####
Action                    U
Path                     C:\temp\backups\sql\
Name                     OverShare
PropName                 OverShare
```

Get-GPOIniFiles

- Sets application configs in .INI files.
- Rarely used, but could contain some fun stuff.

```
Get-GPOIniFiles - Computer Policy
#####
Property                                propertyname
Name                                    propertyname
Path                                    C:\temp\newini.ini
Value                                    propertyvalue
Section                                sectionname
Action                                  U

Get-GPOIniFiles - User Policy
#####
Property                                farts
Name                                    farts
Path                                    C:\temp\fart.ini
Value                                    farty
Section                                farts
Action                                  U
```

Get-GPOEnvVars

- I have never seen an admin use this.
- I can imagine it being used in insane ways, so I'm including it.

```
Get-GPOEnvVars - User Policy  
#####
```

Action	U
Value	asdf
Status	moar_env_vars_here = asdf
Name	moar_env_vars_here

Get-GPOShortcuts

- Pushes .lnk files
- Good for finding commonly used and critical apps on file shares.
- If you can modify the target...

```
Get-GPOShortcuts - Computer Policy
#####
startIn          C:\temp\doodles
Name             shortcutname
targetType       FILESYSTEM
targetPath       C:\temp\doodles
arguments        -argument1
Action           U
shortcutPath     %DesktopDir%\shortcutname
Status           shortcutname
```



Get-GPOUserRights

- Do all kinds of fun stuff:
 - SeRemoteInteractiveLogonRight = RDP Access
 - SeTcbPrivilege = “Act as part of the operating system”
 - SeMachineAccountPrivilege = Add machines to domain
 - SeBackupPrivilege = Read any file via backup API
 - AND MANY MORE!!!

```
Get-GPOUserRights - All Policy
#####
Right                SeRemoteInteractiveLogonRight
Members              Actually_Literally_Everyone
```





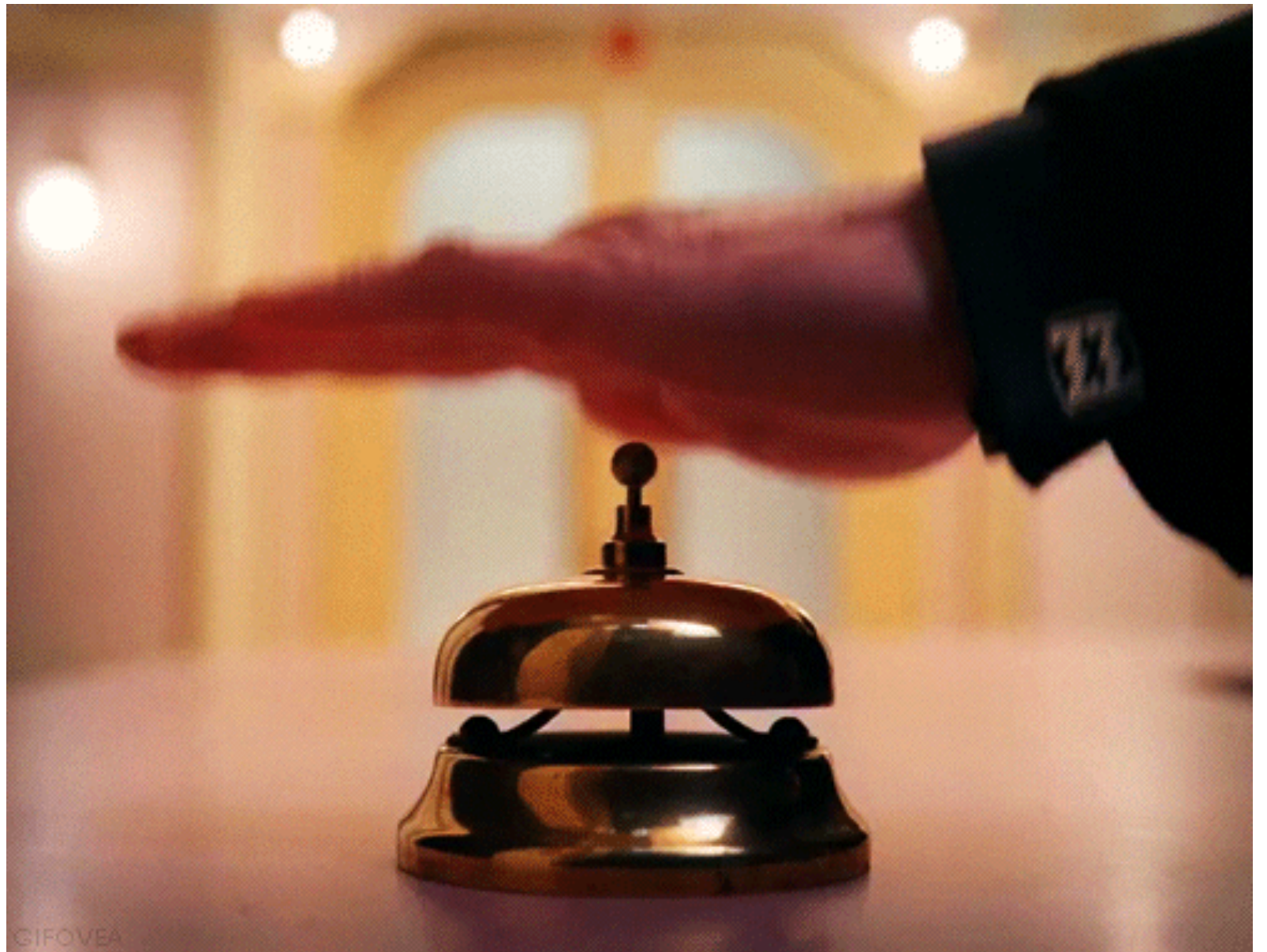
Regrets & Next Steps



- Should have used XPath queries.
- I want to further refine Grouper.
- You can probably help!

Thanks:

- the gang at Asterisk
- @sysop_host
- @prashant3535
- @harmj0y
- @liso
- the gang from the BloodHound Slack
- #ducksec





**If I rushed this, there might
be time for questions?**

Bonus Content:

How do I know which policies apply to which users and computers?

TL;DR use PowerView

To see the policies:

```
Get-DomainGPO
```

To see the policies that apply to a given user/computer:

```
Get-DomainGPO -ComputerName testserver
```

```
Get-DomainGPO -UserName lowpriv
```

To see the computers that a policy applies to:

```
Get-DomainOU | WhereObject {$_.gplink.contains("{PUT THE GPO UID HERE}")} | %{Get-DomainComputer -ADSPath $_.distinguishedname}
```

To figure out which settings from which policies actually apply and which get overwritten...

Don't bother trying to remember this:

Local GPOs are applied first.

Then GPOs linked to a site.

Then GPOs linked to the domain.

Then GPOs linked to OUs, from the top down.

If multiple GPOs are linked at the same level, they apply from the bottom-up.

Last writer of a given setting wins.

