Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d6997036fa067b80527f:::

Pass-the-Hash II: Admin's Revenge

Skip Duckwall & Chris Campbell

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b1567029113 7:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Do you know who I am?

- Skip
  - Co-presented PTH talk last year at BH, Derbycon
  - http://Passing-the-hash.blogspot.com
  - @passingthehash on twitter
  - Works for Accuvant Labs
- Chris
  - Co-presented PTH talk last year at BH, Derbycon
  - http://www.obscuresec.com
  - @obscuresec
  - Works for Crucial Security (Harris Corp)

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Why we are here

- Dispel some FUD going around with PTH
- Provide some practical things everybody can do to defend against credential attacks as well as PTH
- And do it all in less that 80 pages!

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970360fa067b80527f:::

The FUD stops here!

- We're trying to educate everybody about the issues at hand
- Pass-the-hash sounds super sexy but is NOT the biggest problem the enterprise faces
- Windows has numerous issues with authentication in addition to PTH…
  - Credential exposure (mimikatz / WCE)
  - Broken protocols still in use (MSCHAPv2 / NTLMv1)
  - Cached credentials
  - Tokens, etc…

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

PTH-The biggest problem on the network?

- Actually, PTH is only a small subset of the problems with Windows authentication
- What about easy to recover plaintext passwords being kept in memory? Thanks Mimikatz!

```
        kerberos
         * Utilisateur  : blackhat2013
         * Domaine      : DEMO.LOCAL
         * Mot de passe : P@$$W0rd!!
```

Why use PTH when you can use the actual creds?!?

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d6997036fa067b80527f:::

I can fix PTH… With a Patch!

- PTH is by design functionality. There is no fix, there is only mitigation or using some other form of auth.
- Why do you think that the MSV1_0 / NTLMSSP only saves the hash?

```
msv1_0
 * Utilisateur  : blackhat2013
 * Domaine      : DEMO
 * Hash LM      : b0109442b77b46c7a67a448822b50c99
 * Hash NTLM    : 564644a3eef2263fbd5642e1dd898154
```

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Kerberos Solves the PTH problem?

- NTLM hashes are used as the long-term secret keys
- KRBTGT hash is the master key for all Kerberos tickets
- Loss of this hash can completely undermine Kerberos
- Also, TGTs are portable, just like hashes
  - Move from one machine to another…

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

The Real Problem : Single Sign On

SSO – Ask for the password once, logon everywhere

Microsoft has a term for asking the user for their creds too many times: “Credential Fatigue”

Windows caches credentials in memory for all possible forms of authentication, even if they aren’t being used. Because you know, they *could* be used… sometime… somewhere… somehow… maybe?

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d6997036fa067b80527f:::

Microsoft has a credential problem

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b1567029113 7:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Easy to recover Plaintext PW in Memory

- Thanks Benjamin Delpy for Mimikatz!
- Multiple SSPs save both username / pw for future use
  - Digest-MD5
  - LiveSSP
  - TSPKG

```
mimikatz # sekurlsa::logonPasswords all

Authentification Id          : 0;379748
Package d'authentification   : Negotiate
Utilisateur principal        : blackhat2013
Domaine d'authentification   : DEMO
        msv1_0
         * Utilisateur  : blackhat2013
         * Domaine      : DEMO
         * Hash LM      : b0109442b77b46c7a67a448822b50c99
         * Hash NTLM    : 564644a3eef2263fbd5642e1dd898154
        kerberos
         * Utilisateur  : blackhat2013
         * Domaine      : DEMO.LOCAL
         * Mot de passe : P@$$W0rd!!
        ssp
        wdigest
         * Utilisateur  : blackhat2013
         * Domaine      : DEMO
         * Mot de passe : P@$$W0rd!!
        tspkg
         * Utilisateur  : blackhat2013
         * Domaine      : DEMO
         * Mot de passe : P@$$W0rd!!
```

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Even if nobody's logged in …

- There's at least one plaintext password for a domain in the LSA secrets.
- Computer's domain account
  - Can be used to gather info from the domain
    - Usernames
    - Group memberships
  - Can be used to browse file shares
    - There aren't any recoverable creds on any shares are there?
    - Group Policy Preferences… we'll touch on this later…
- There might be more accounts
  - Creds for accounts with saved passwords (service accounts)

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Don't forget local account hashes

- Stored in the SAM (Security Account Manager)
- Local 500 account is a dangerous account
  - Has separate UAC settings from regular user which are DISABLED by default
  - Often enabled (despite being disabled by default)
  - Often has the same password across large number of machines
  - Has access to the domain via the computer's domain account

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970360fa067b80527f:::

For Brevity….

- We aren't going to talk about Domain Cached Credentials
- Or token impersonation
- Or Services that store passwords in files
- Or plaintext password files on file servers
- Or keyloggers
- Or Phishing
- Or any of the other ways that an attacker can get creds

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Bottom Line

- An attacker has multiple ways to gain access to valid (or usable) network credentials
- Attackers take the path of least resistance
- Once an attacker has SYSTEM on one box, it's usually a matter of time until they have SYSTEM on your domain controller

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

a1

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

How ~~do you~~ make PtH worse?

does Microsoft

- Ensure that every local admin password is the same
  - Introducing a feature that makes PtH easier to exploit:
    - Group Policy Preferences
- Make sure that hashes never change
  - Over-selling an expense as a security mitigation:
    - Smart Cards

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b1567029113 7:::

a1 clean up slide
awe, 7/11/2013

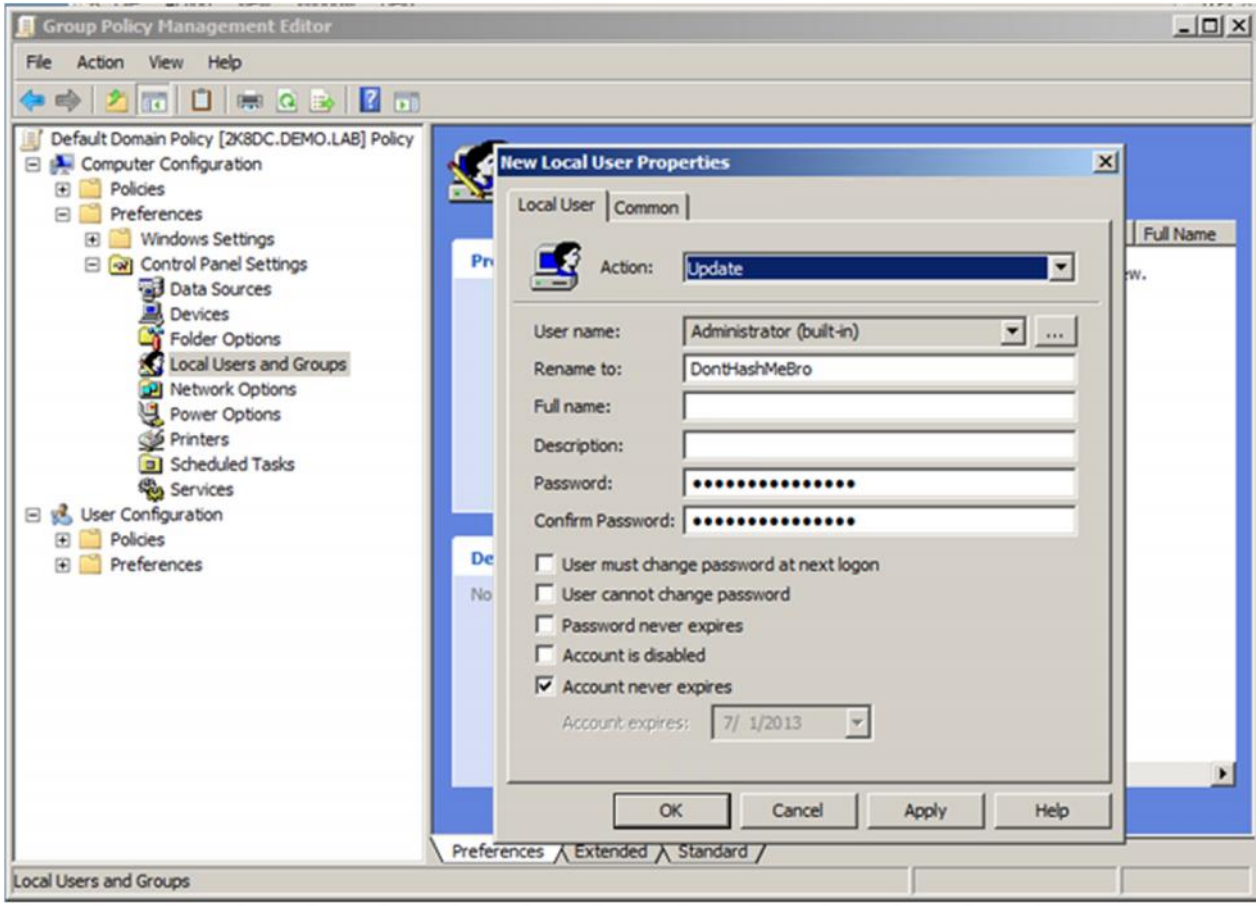
Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d6997036fa067b80527f:::

Group Policy Preference Settings

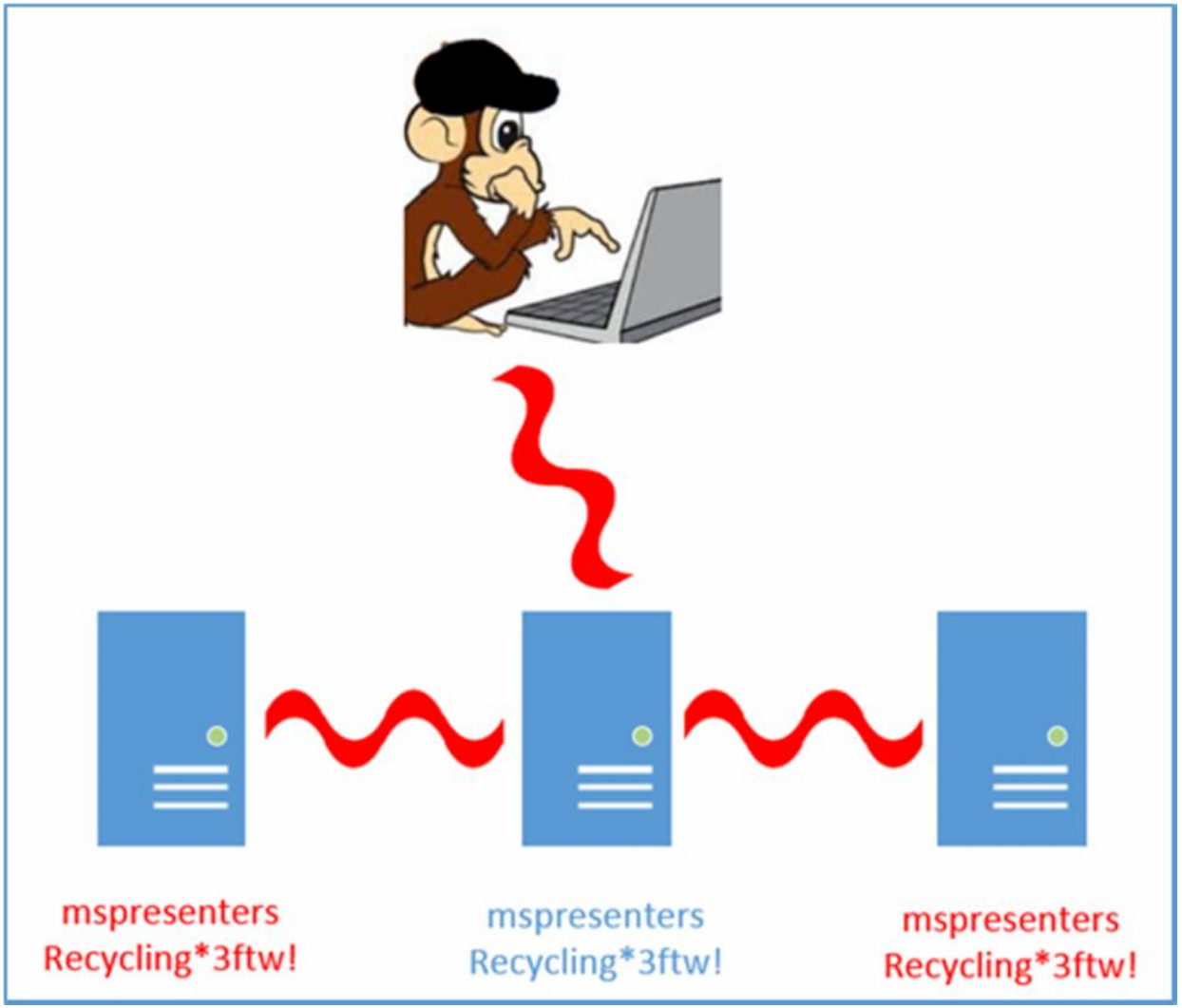
- Easy way to enforce settings on every workstation
- Popular with administrators to set passwords



Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

GPP Passwords: Making it Easy



Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d6997036fa067b80527f:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d6997036fa067b80527f:::

GPP: Its Even Worse

- Passwords are obfuscated on the domain controller
- Easily decrypted by anyone on the network
- Demo

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<2>

The 32-byte AES key is as follows:

```
4e 99 06 e8  fc b6 6c c9  fa f4 93 10  62 0f fe e8
f4 96 e8 06  cc 05 79 90  20 9b 09 a4  33 b6 6c 1b
```

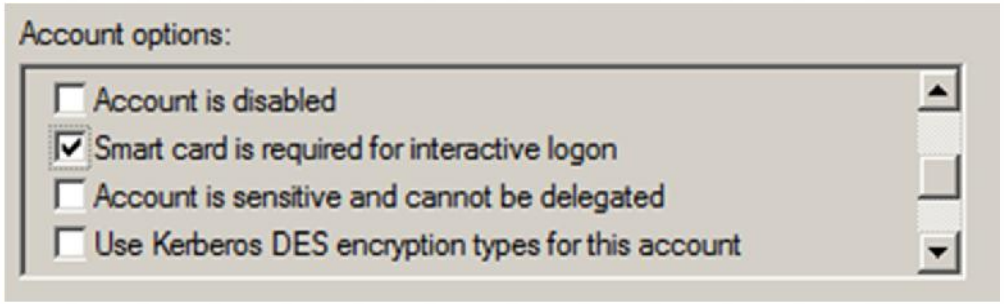
```
PS C:\demo> Get-DecryptedCpassword "9KQYhHxSxrrZjFo8Frt/nExdMLKsQM+ThhWOJKajaRc"
Recycling*3ftw!
PS C:\demo>
```

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

Smart Cards

- Who needs passwords?



- Authentication still works the same

```
66 ee b2 ba c4 5d ff 54 3d 6e cc fc 02 cc f2 8b 3b aa df 42 f9 eb 80 89 55 b5 06 7f 0c f2 f7 83
43 98 f5 fe 25 d9 74 13 7e f4 c4 67 6f 84 a4 0c 86 59 66 c5 5e d1 1a 81 6e 0a f0 07 c1 53 97 f2
1a 11 fa 49 bc 9a 51 4b 7b 86 b1 40 11 0e 22 8f 2f 9e 8b d1 28 ef d7 0c c0 79 a7 69 e5 2d 6c 98
57 b4 c2 60 88 b4 45 93 8e ce b2 7a 60 aa 7e f4 b5 f4 a4 bf 4e aa c8 25 e4 38 3f 1d a1 b8 3e 8f
3a d0 c8 e8 18 4a 5d 8a ae d4 a5 41 81 0d da 8c 2d 2f ff 21 74 0c b4 da 51 65 88 b3 f4 fe 92 4a
da 4c 9c 7d 31 5d 58 d4 ee f2 f4 4b be 5a 14 a7 01 3a a6 bd 43 9c 5c b0 2f 00 f3 0d fe 6e 1f 1a
4c 84 e0 ad b8 6f fc 5a 3c 82 c4 84 42 19 ad 9a 41 0b e9 09 f0 89 d9 e3 dc 80 a6 d2 94 00 d6 37
1f 28 43 40 ef a2 24 3a ba dc ac 0a 61 1a 8f 88
```

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d6997036fa067b80527f:::

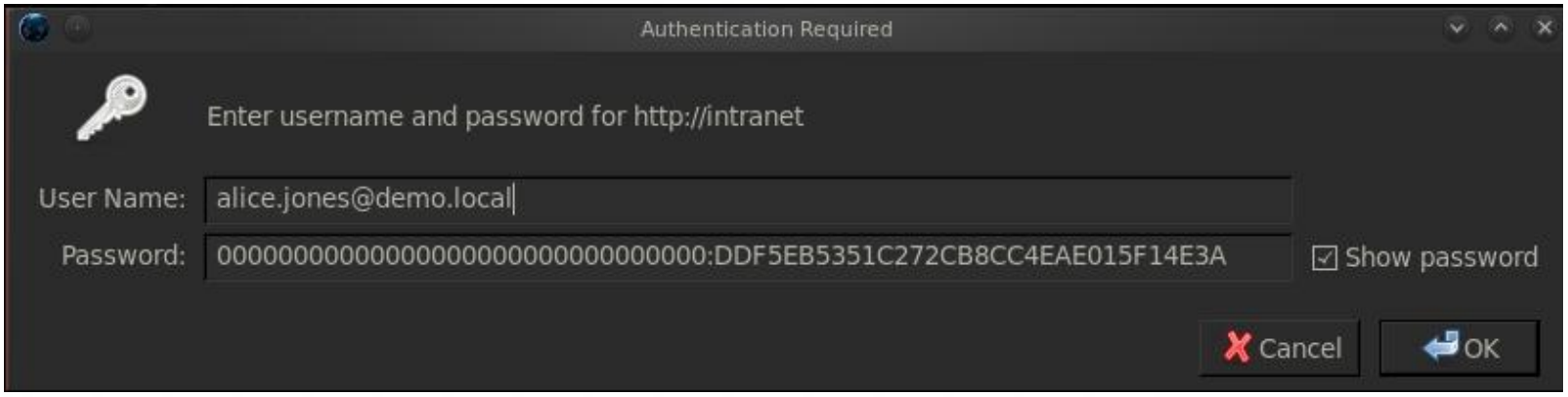
Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

Smart Cards = Persistence

- NT Hashes still look the same with smart cards

```
SmartCardUser:1105:aad3b435b51404eeaad3b435b51404ee:c4f5cb57e34555c2d19b294554187c1d:::
```

- NTLMSSP and SSO push PtH to the perimeter



exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

MS Mitigation for PtH

- Microsoft PtH whitepaper has 3 main mitigations
  - Restrict and protect high privileged domain accounts
  - Restrict and protect local accounts with admin privs
  - Restrict inbound traffic using Windows Firewall

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970367fa067b80527f:::

Our Mitigations

- Don't let the attacker get SYSTEM
  - Most of the tools don't work w/o SYSTEM privs on the workstation
  - Users almost never need admin access to their workstation (no matter how high up they are in the org)
  - ACL off unneeded command line utilities
    - CMD.EXE
    - NET.EXE
  - Patch all local privilege escalation bugs
    - Don't always show up as 'critical' or 'high' in patch software

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Don’t make it easy for them

- Use UAC, even for the local 500 account
- Don’t use GPP to set the passwords
- Disable the local 500 if you can get away with it
- Don’t use elevated creds in startup scripts
- Don’t save service account passwords on workstations

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Protect the crown jewels

- The loss of your DC means the loss of your network
- Make sure your VM environment is safe (if your DC is virtualized)
- Encrypt backups
- Don’t store backups on shares that regular users can access

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Too Many EA/DA accounts

- You probably don't need 50 enterprise (or domain) admins
- These accounts are given out too freely because they easily can solve problems
- Focus on what your specific needs are
  - Lots of tools only need specific privileges rather than full EA/DA
  - Work with the vendors for your tools to figure out what's needed
- Most service accounts don't need to be EA/DA

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Issue multiple accounts to admins

- Regular accounts
  - Use for day to day activity
  - Email, web, etc
- Privileged accounts
  - Only to be used for tasks requiring their privilege
  - Don’t give elevated accounts email addresses
  - Most admin tasks can be handled by right-click->runas and elevating that way while logged into a normal account

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Manage Tokens

- Try to minimize running tools that leave tokens lying about as admins
  - PsExec
  - McAfee scan run from EPO leaves tokens too…
- Log out of RDP sessions : Start -> logout
- Reboot periodically to get rid of tokens
  - Yes, even servers
  - Especially servers, where are admins more likely to log into?

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

The Goodies

- We aren't going to leave you hanging
- We've got some scripts to hopefully help you guys out

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

Prevent Persistence

- Reset password hash on every smart card account

```
#Import AD Module
Import-Module ActiveDirectory

#Create an array of all accounts that have smart card logon enforced
$ADUsers = (Get-AdUser -Filter * -Properties 'SmartcardLogonRequired' |
    Where-Object {($_.SmartcardLogonRequired)}).SamAccountName

if ($ADUsers -eq $null) {Write-Error "No Accounts Require Smart Cards for logon"}

#Iterate through each account that has the setting enabled and toggle
ForEach ($User in $ADUsers) {
    Get-AdUser -Identity $($User) | Set-AdUser -SmartcardLogonRequired $False
    Start-Sleep 1
    Get-AdUser -Identity $($User) | Set-AdUser -SmartcardLogonRequired $True
}
```

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

Different Pwds, Different Hashes

- Don’t use GPP, ensure passwords are unique
  - Set-UniquePassword PowerShell Function

```
-------------------------- EXAMPLE 1 --------------------------

C:\PS>Get-Content c:\demo\computers | Set-UniquePassword -Random | ConvertTo-Csv | Out-File c:\demo\password_update.csv


-------------------------- EXAMPLE 2 --------------------------

C:\PS>'localhost','test','127.0.0.1' | Set-UniquePassword -Random


-------------------------- EXAMPLE 3 --------------------------

C:\PS>Set-UniquePassword -Random


-------------------------- EXAMPLE 4 --------------------------

C:\PS>Set-UniquePassword -UserName "mspresenters" -Position "Prepend" -Phrase "Recycling*3ftw!" -Token "Serial"
```

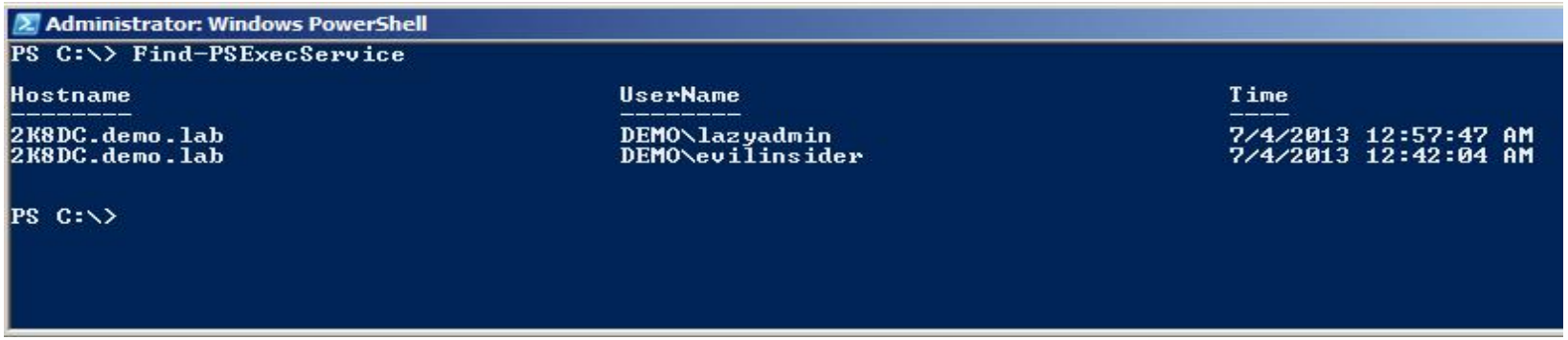
Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Detection is More Realistic

- Write “tools” for every tool out there?
  - Look for signatures in open-source tools
  - Try to stay on top of every new tool
    - Find-PSExecService
    - Find-MsfPsExec
    - Find-WinExec



Why Not Monitor Activity?

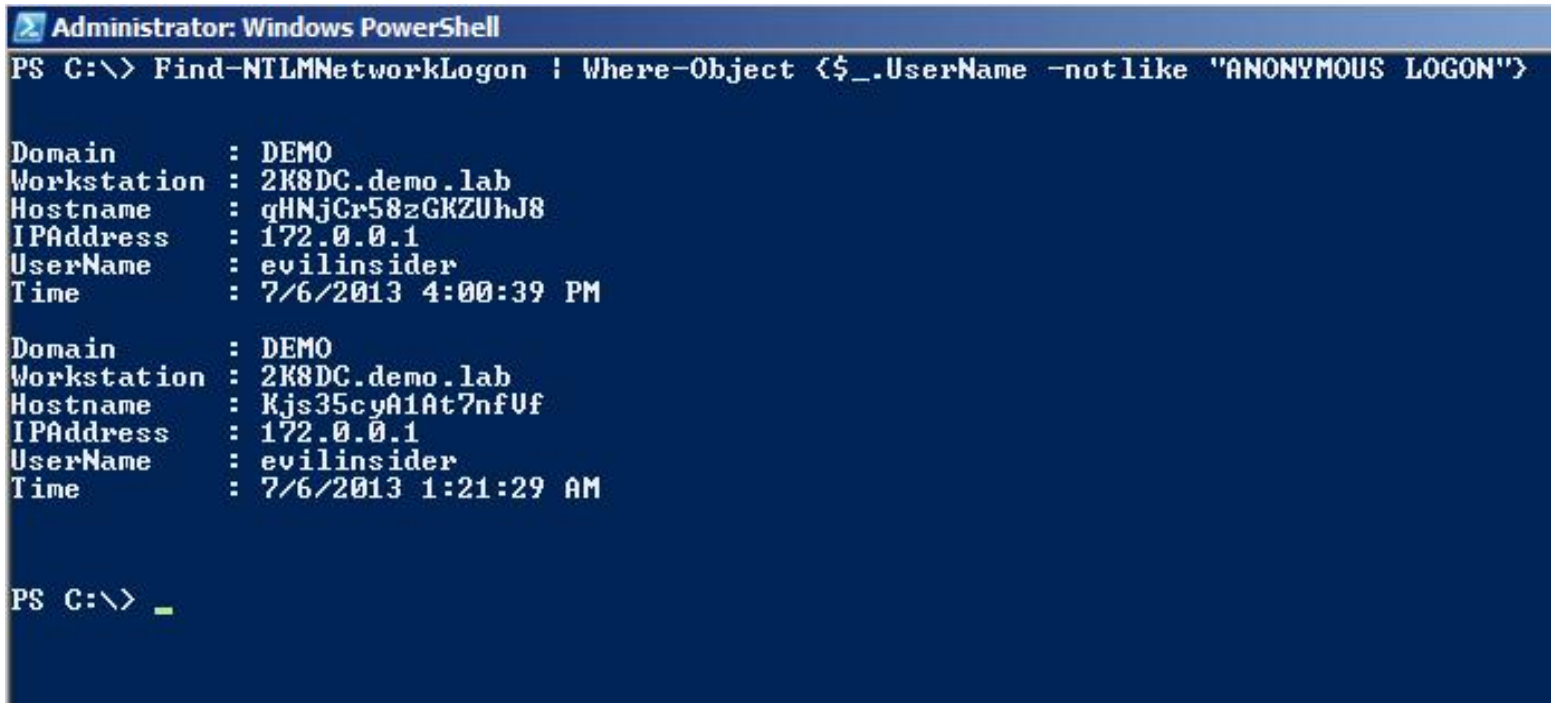
- NTLM Network Logons
- Find-NTLMNetworkLogon

```
Function Find-NTLMNetworkLogon {
    $Filter = "*[EventData[Data = 'NtLmSsp ']]"
    $Events = Get-WinEvent -Logname "security" -FilterXPath $Filter |`
        Where-Object {$_.ID -eq 4624}

        if ($Events) {$Events | ForEach-Object {

            $ObjectProps = @{'Hostname' = $_.Properties[11].value;
                             'IPAddress' = $_.Properties[18].value;
                             'UserName' = $_.Properties[5].value;
                             'Domain' = $_.Properties[6].value;
                             'Time' = $_.TimeCreated;
                             'Workstation' = $_.MachineName}

            $Results = New-Object -TypeName PSObject -Property $ObjectProps
            Write-Output $Results
            }

        }
}
```

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

Find PtH and Insider Threat

- Schedule it and use Send-MailMessage
- Don’t just catch Pen-testers, detect real incidents



exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Chris:1000:aad3b435b51404eeaad3b435b51404ee:a2345375a47a92754e2505132aca194b:::

Questions?

exorcyst:501:aad3b435b51404eeaad3b435b51404ee:b936551d3f0f2716e9b8e58418ac81f6:::

obscuresec:1001:aad3b435b51404eeaad3b435b51404ee:a295f6538fc8d69970036fa067b80527f:::

Skip:500:aad3b435b51404eeaad3b435b51404ee:f0873f3268072c7b1150b15670291137:::