#BLACKALPS17

AD Threats & Detection: Heartbeat that keeps you alive may also kill you!

Harman Singh
www.defendza.com
@defendzaltd

DEFENDZA

whoami

- Managing consultant at Defendza
- Pen Tester/Security Consulting
- Tweets are welcome @digitalamli #BlackAlps17
- Hacktivity, BlackAlps ☺, Bsides, BlackHat USA 2015
- Sometimes clients listen and fix issues, sometimes they blame me, other times they don't fix ☹!

DEFENDZA

tl;dr

- whoami
- Active Directory
  - Fundamentals
  - Latest Features (2016)
- Nuts & Bolts of a DC
- Threats
- Detections
- Q&A

Ange Albertini

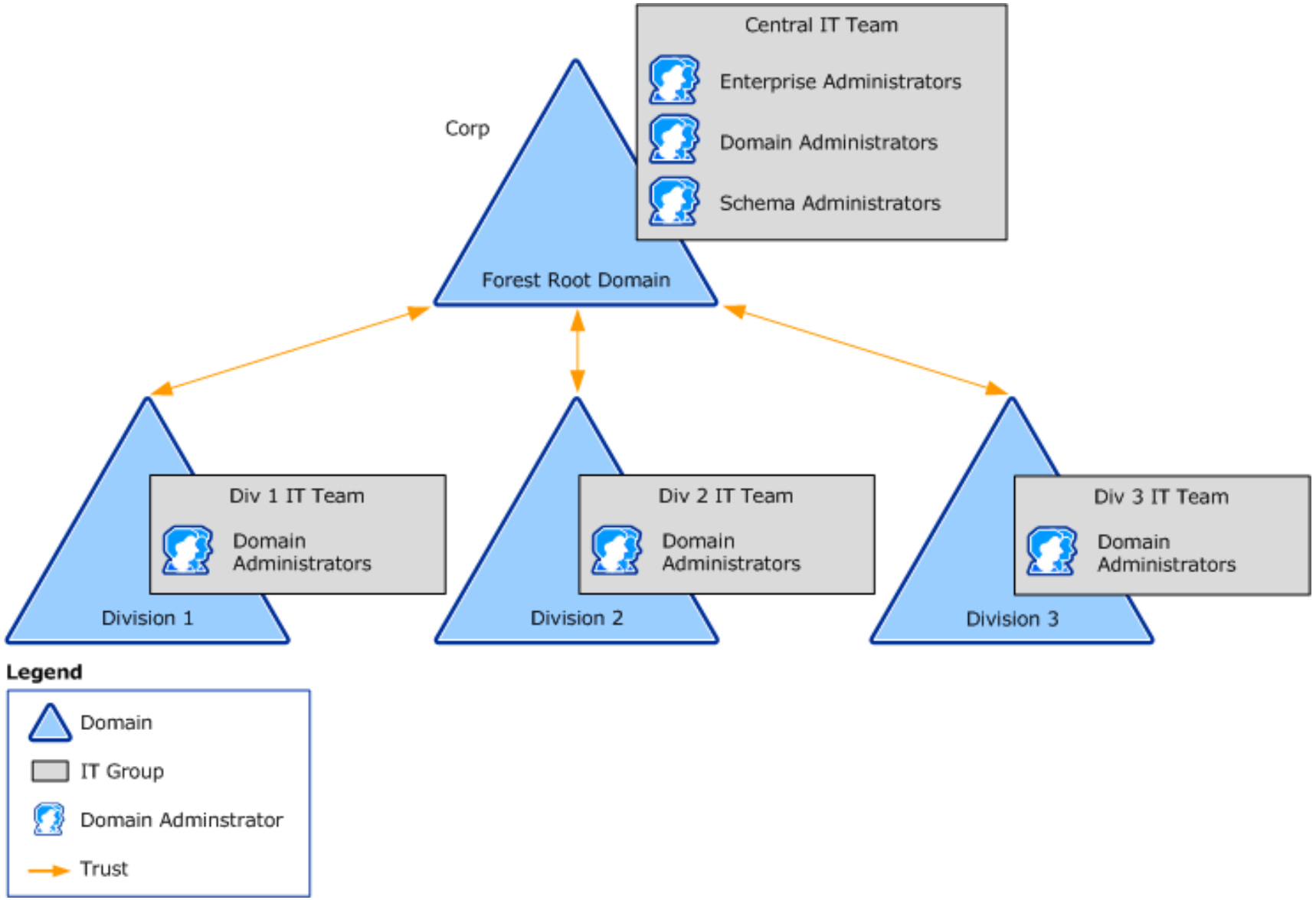
DEFENDZA

Disclaimer

- No new exploits/CVE/<~~groundbreaking stuff~~> being released today, just a few ways to help improve threat detection capabilities
- Attack details are stressed to ensure understanding helps the thought process around detection work
- These issues have affected or still affect AD environments - yes, you are part of this game!

Active Directory Fundamentals

- AD?
- Basic structure
  - Forest
  - Domain
  - OU
  - Sites


Central IT Team
Enterprise Administrators
Domain Administrators
Schema Administrators
Corp
Forest Root Domain
Div 1 IT Team
Domain Administrators
Division 1
Div 2 IT Team
Domain Administrators
Division 2
Div 3 IT Team
Domain Administrators
Division 3
Legend
Domain
IT Group
Domain Adminstrator
Trust

Active Directory Services

- Domain Services
- Certificate Services
- Federation Services
- Lightweight Directory Services
- Rights Management Services

DEFENDZA

AD Domain Services

- AD DS?
- Role
- Benefits
  - Forests
  - Scalability
  - Delegation
  - Security (Authentication + Access Control) – A single network logon = ~~compromise~~☺

AD DS Features

- Features
  - Schema
  - Global catalog
  - A query and index mechanism
  - Replication
  - Operations master roles/FSMO

DEFENDZA

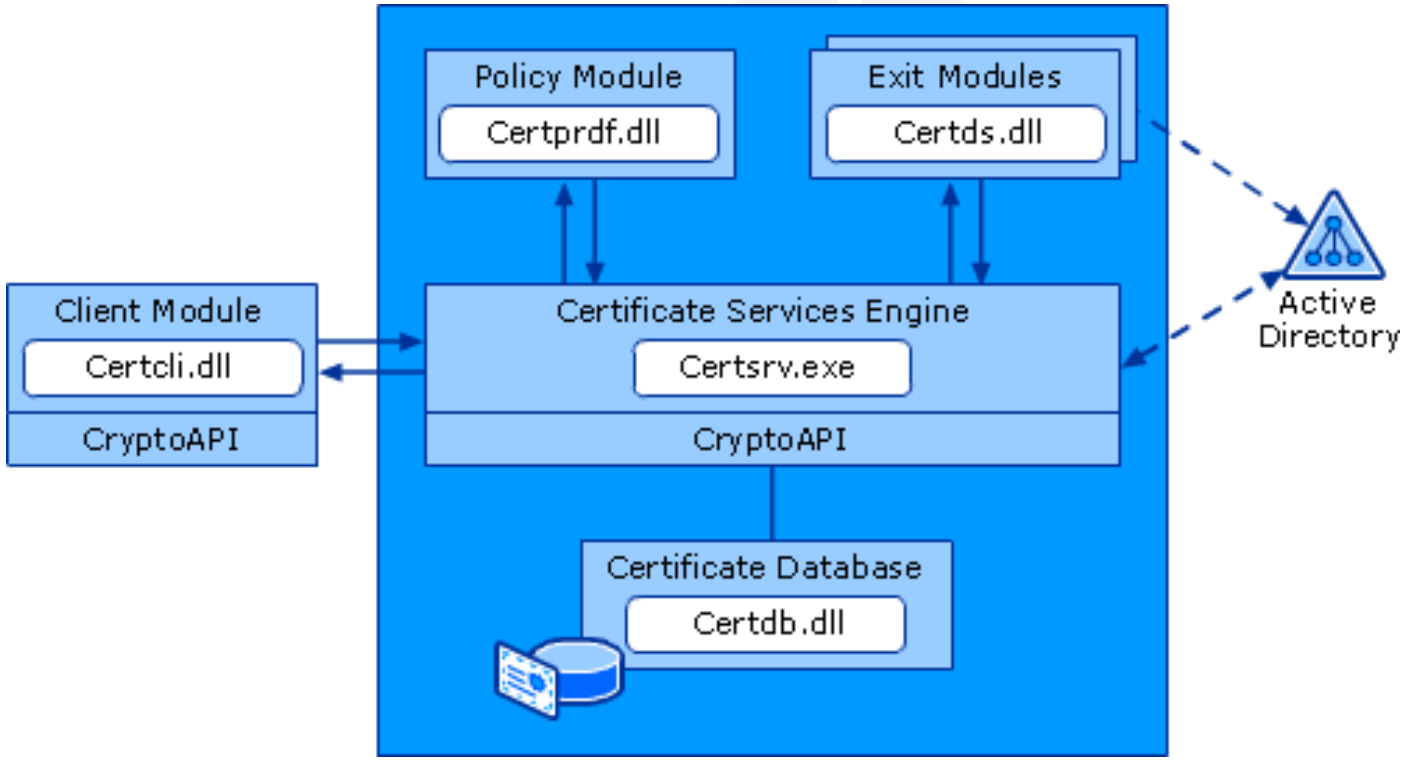
New AD DS Features

- Since Win Server 2008
  - RODC
  - Admin role separation
  - Secure installation media
  - Restartable AD DS
  - Fine-grained Password Policy
  - a few more…

AD Certification Services

- AD CS
- Benefits of AD CS
- Certificate Services
  - CA's
  - Web Enrolment
  - Online Responder
  - Network Device Enrolment Service
- CS Architecture

Certification Services Architecture



File System Info

- Logs
  - The only directory (by default) in use *systemdir*\CertLog
  - Certutil.exe -> *systemroot*\certutil.log
  - CA snap-in logs -> windir\certmmc.log
- Certs and CRLs
  - \\Localhost\Certenroll
  - \\Localhost\Certconfig
  - SystemCertificates\My folder located at:

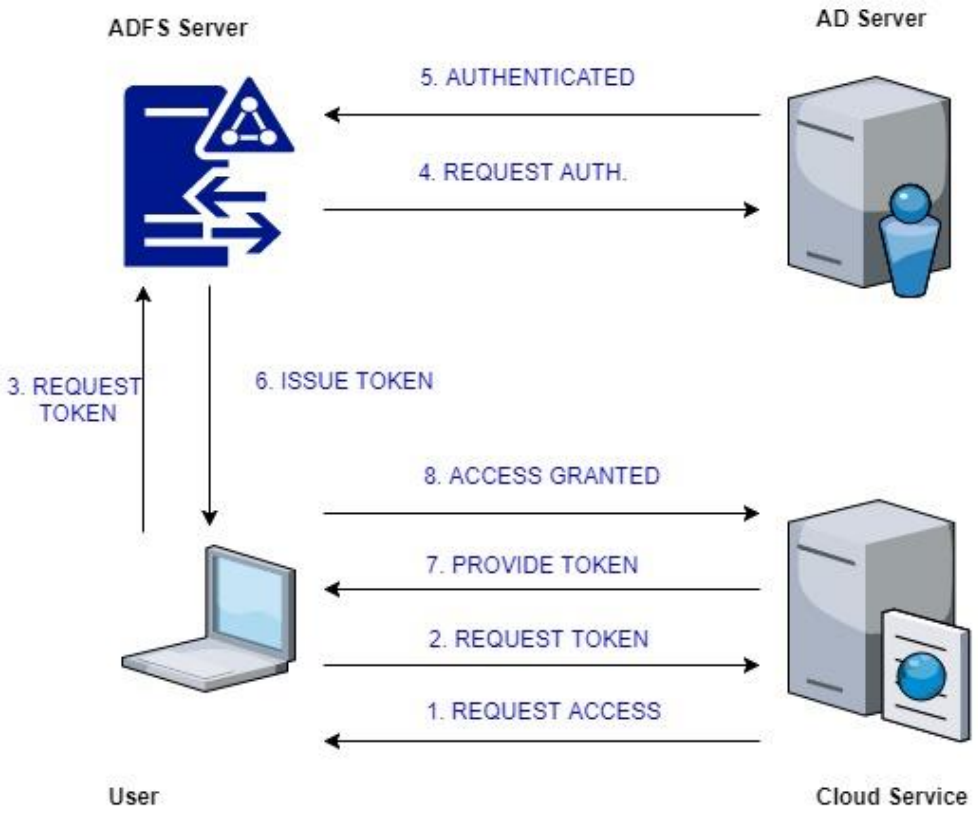
    `C:\Users\<username>\Application Data\Microsoft\SystemCertificates\My`
  - Trusted root CA container

    `HKEY_Local_Machine\Software\Microsoft\SystemCertificates\Root`

AD Federation Services

- AD FS?
- ADFS Features
- ADFS Role Services
  - Federation Services
  - Proxy
  - Claims-aware
  - Windows Token-based

Federation Services



AD Lightweight Directory Services

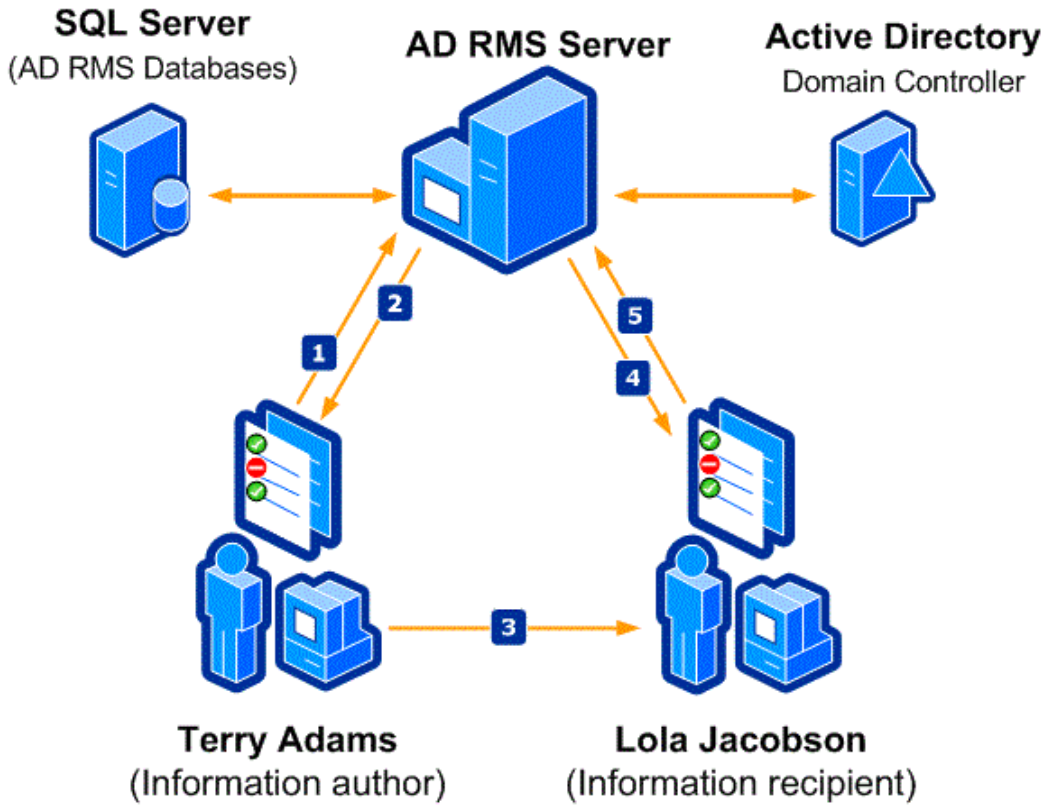
- AD LDS (ADAM? 😐)
  - Much of the same as AD DS
  - Deployment of domains/DC's not required
  - Multiple instances of LDS on a single computer
  - Can use AD DS for authentication of Windows security principals.
- Why is it a big deal?
  - Enterprise directory store
  - Extranet authentication store
  - …

DEFENDZA

AD Rights Management Services

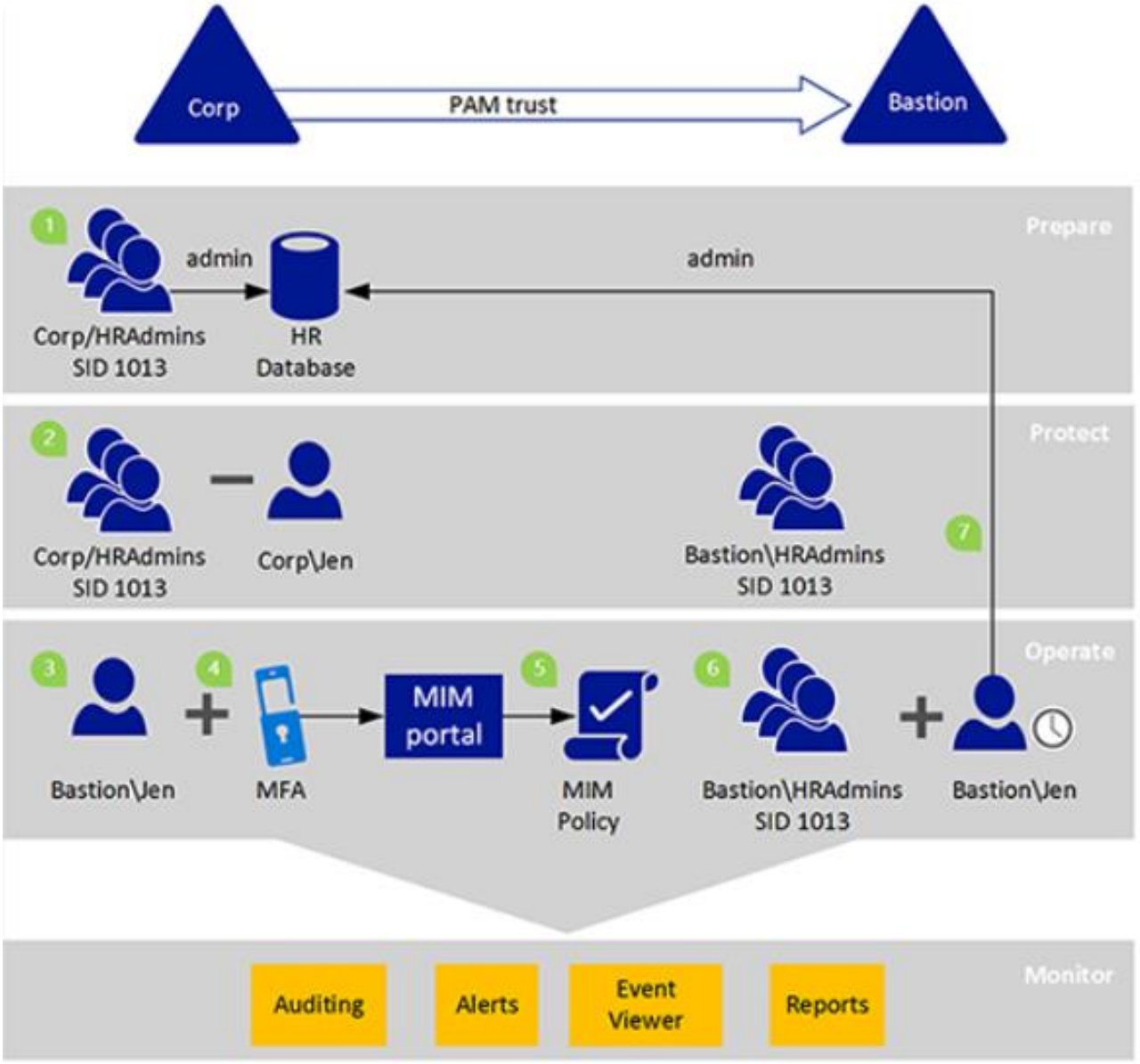
- AD RMS?
- Role description
- Benefits?
  - Persistent use policies
  - Preventing authorized users from unauthorized use
  - Supports file expiration
  - Enforce corporate policies
  - HSM support
- What it does not?

AD RMS Example



AD DS 2016

- Security & Cloud !
- Major improvements:
  - PAM
  - Azure AD Join
  - MS Passport
- Other improvements
  - Time synchronisation
  - Group membership expiration
- Forest/domain functional level (2008)


Corp
PAM trust
Bastion
Prepare
1
admin
admin
Corp/HRAdmins
SID 1013
HR
Database
Protect
2
Corp/HRAdmins
SID 1013
Corp\Jen
Bastion\HRAdmins
SID 1013
7
Operate
3
4
5
6
MIM
portal
Bastion\Jen
MFA
MIM
Policy
Bastion\HRAdmins
SID 1013
Bastion\Jen
Monitor
Auditing
Alerts
Event
Viewer
Reports

DEFENDZA

PAM Advantages

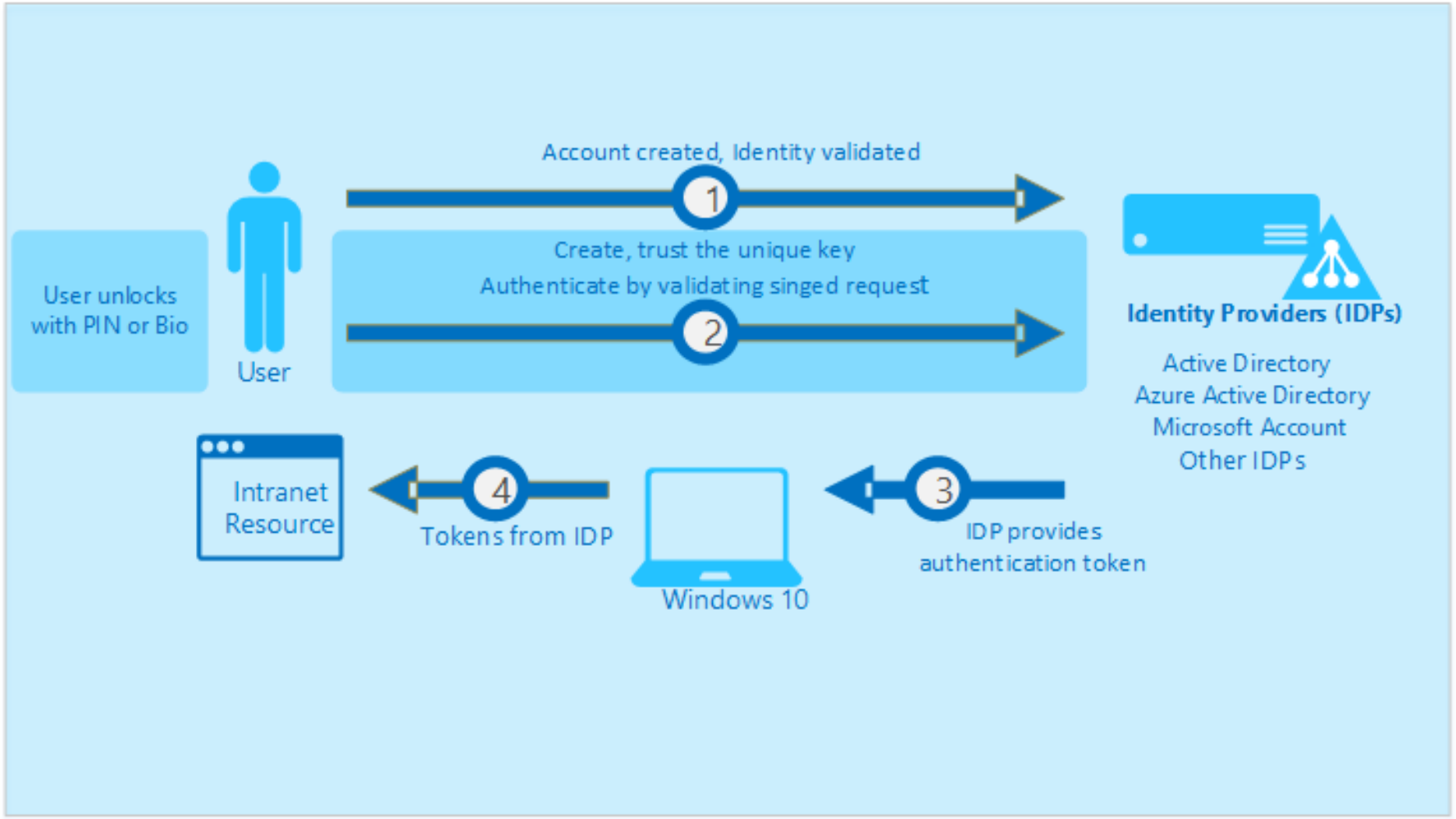
- Isolation/scoping of privileges
- Step up
- Additional logging
- Customizable workflow
  - ✓Credential Theft, pth, and other credential theft mitigations – stay tuned

Azure AD Join

- Azure AD Join:
  - Register
  - Join
- Benefits:
  - Single-Sign On (MS & other Apps)
  - BYOD devices
  - MDM Integration
  - Access organizational resources on mobile devices
  - Modern Settings (Backup and restore, roaming , etc) , Imaging, Dev experience, etc.

Microsoft Passport/Hello for Business

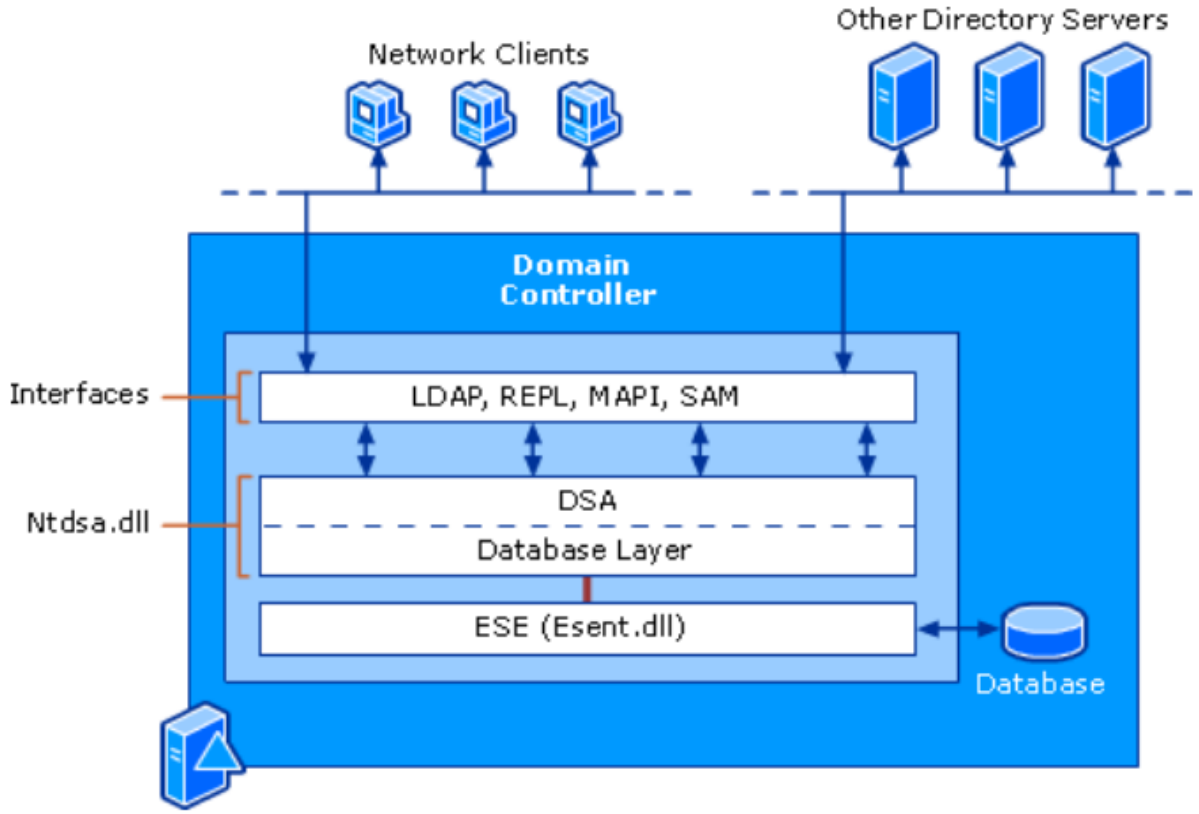
- MS Passport
  - Key-based auth
  - Breach, theft and phish-resistant (Microsoft claims that!)
  - Authenticating identities without passwords
- Windows Hello for Business
  - Cert based auth, supports MS and non-MS accounts (using FIDO)
  - Keys generated on TPM 1.2 or TPM 2.0 (Hardware preferred option)
  - Complexity and length of the PIN
  - Support for smart card-like scenarios by using cert based trust



https://docs.microsoft.com/en-us/azure/active-directory/active-directory-azureadjoin-passport

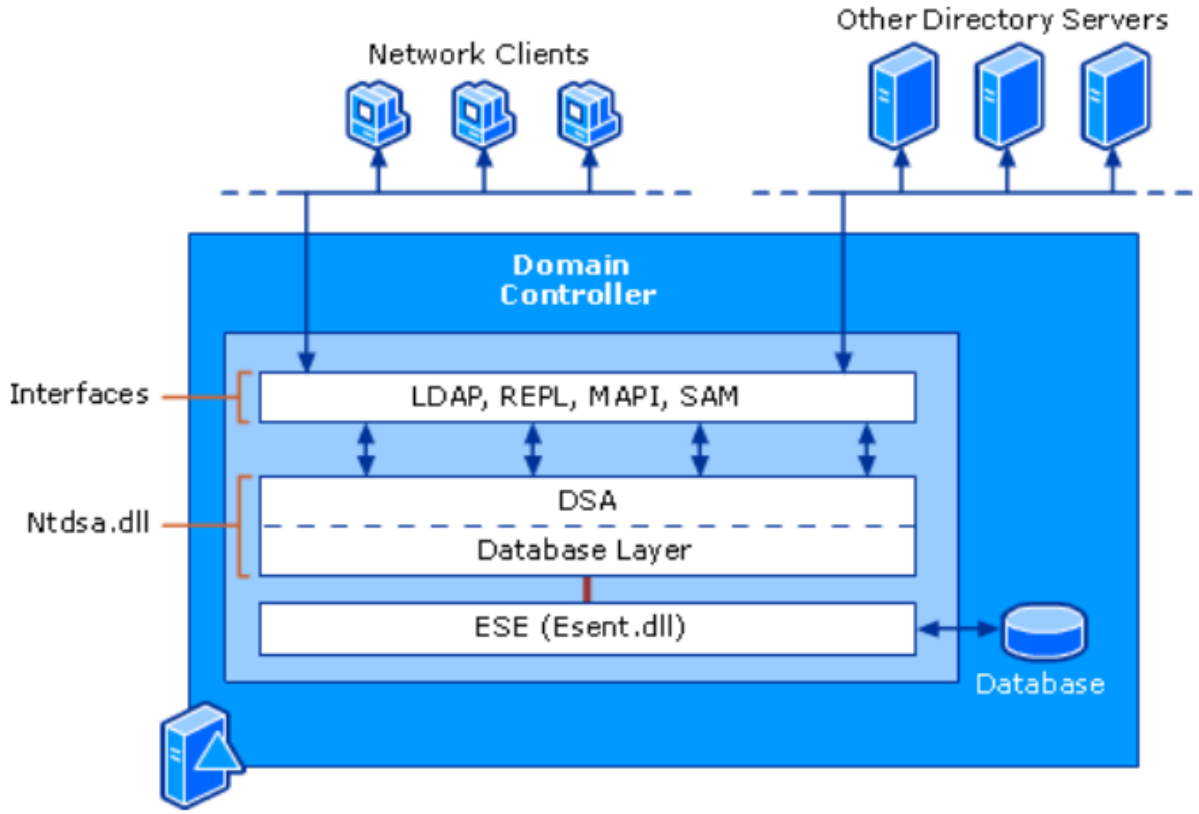
Nuts & Bolts of a DC

- DSA



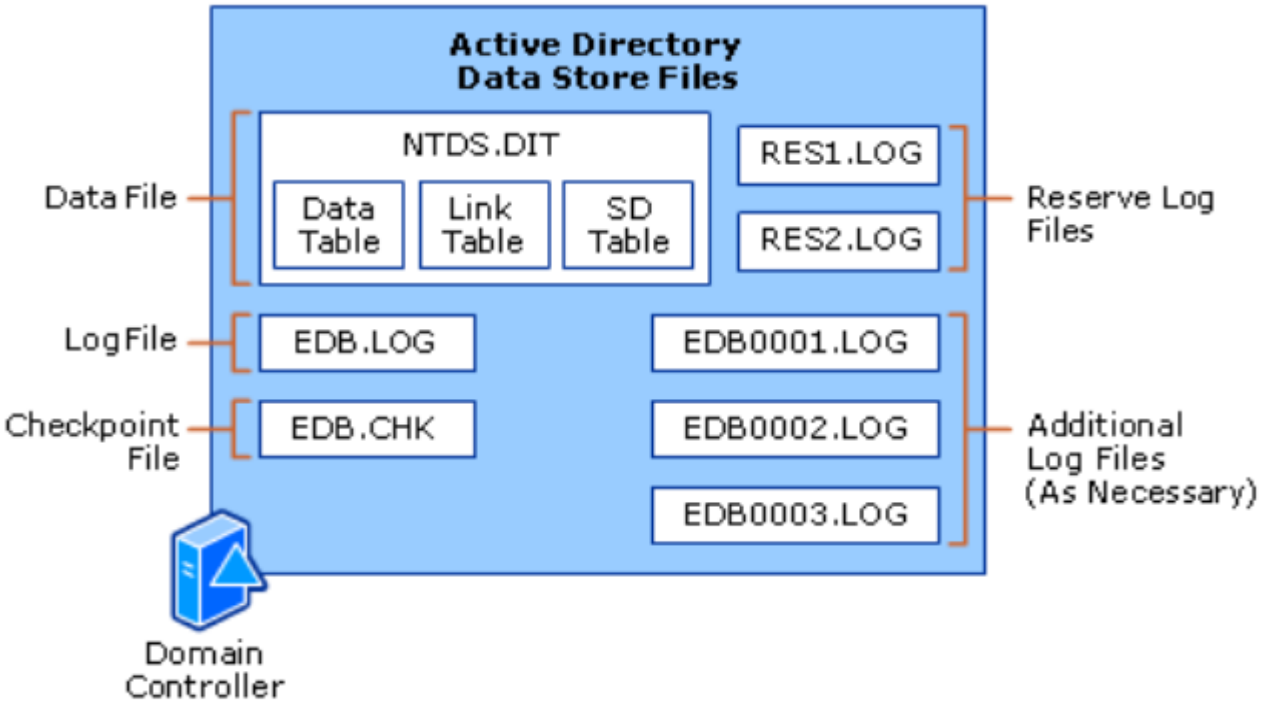
Nuts & Bolts of a DC

- DSA

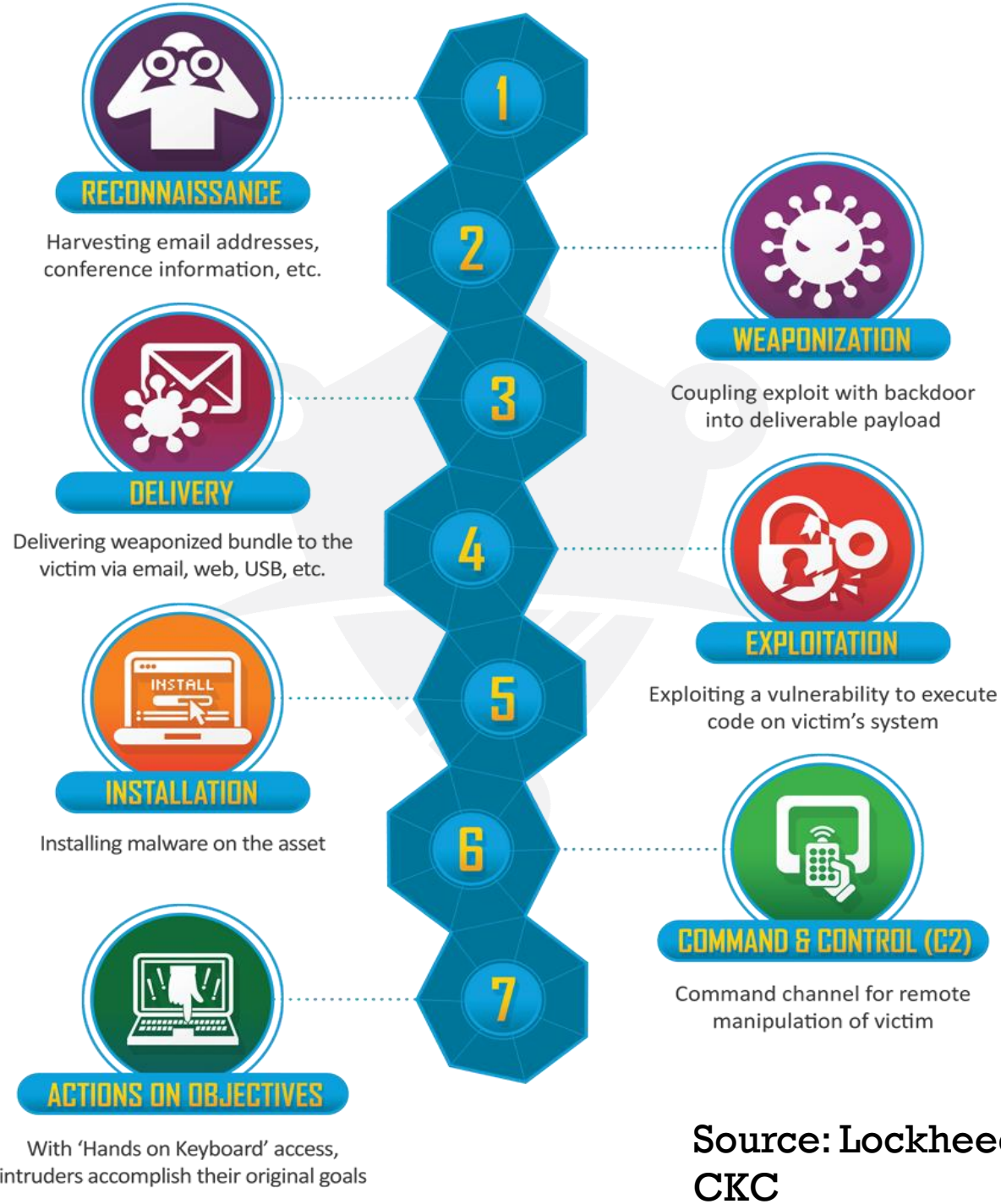


Nuts & Bolts of a DC

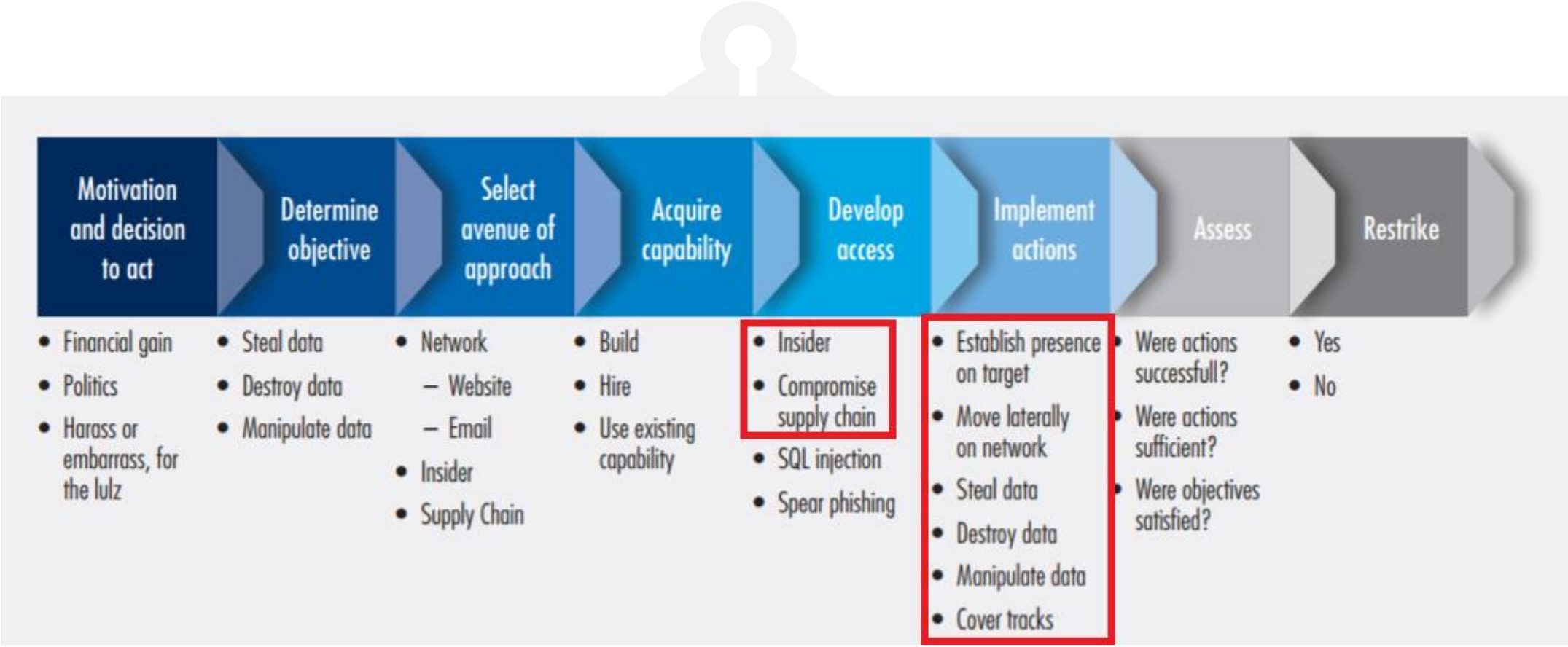
- Data Store Physical Structure



Hacks Ahead



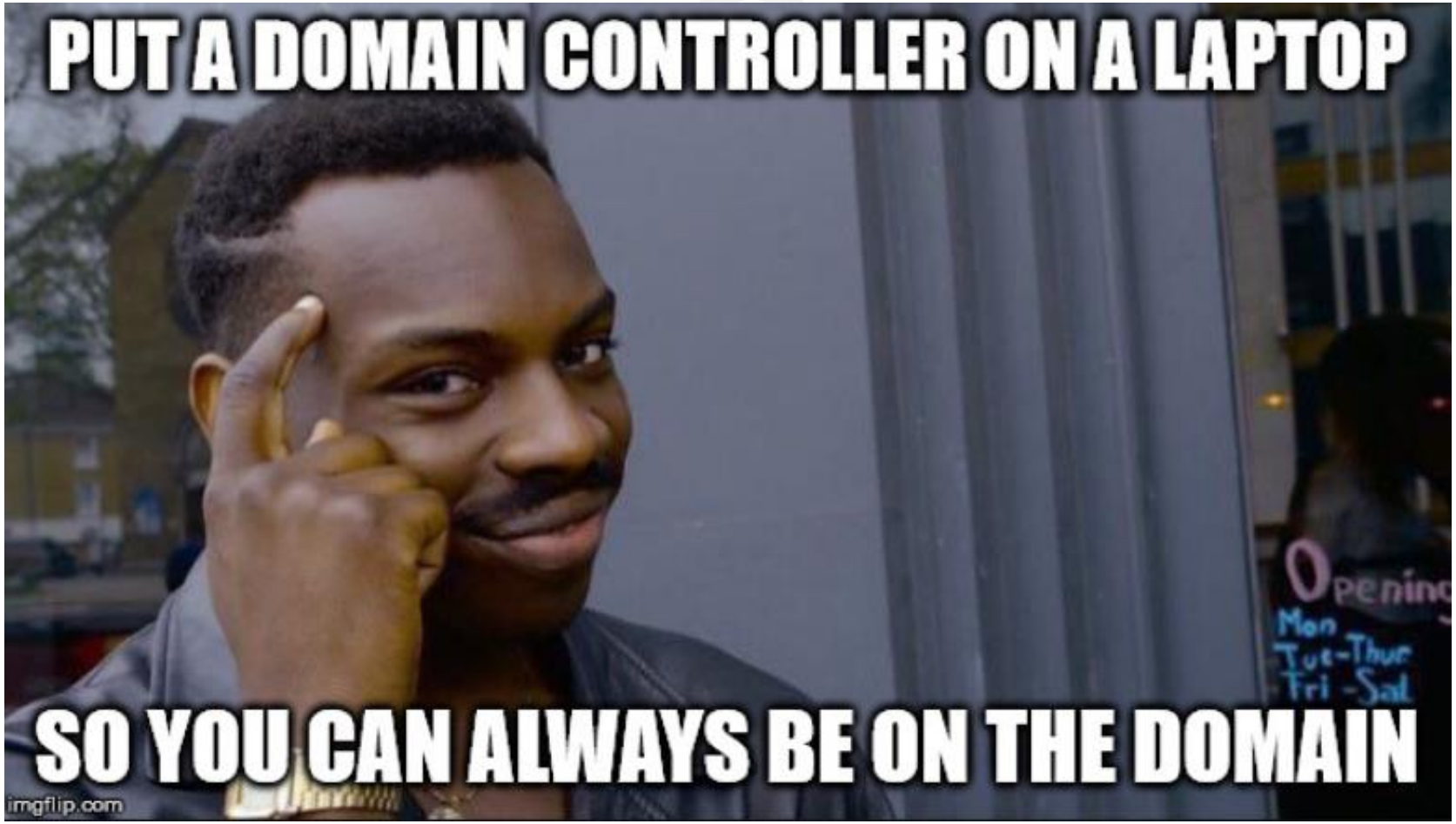
Source: Lockheed Martin CKC



Source: https://www.nist.gov/sites/default/files/documents/2017/06/08/20131213_charles_alsup_insa_part3.pdf

Attack Techniques

- Building up the ground:
  - Enumeration
  - Information collection and analysis
- Privilege Escalation
- Accessing Secrets
  - Token stealing/impersonation
  - Hash Dumping


PUT A DOMAIN CONTROLLER ON A LAPTOP
SO YOU CAN ALWAYS BE ON THE DOMAIN
imgflip.com

OFFENSE - Recon, Escalation, Persistence

- Recon – Identifying targets, gathering the surrounding info for attack prep.
- Escalation – Target exploitation to gain access and escalate privileges
- Persistence – Maintain access

RID Cycling

- RID cycling is used to enumerate user accounts through null sessions and the SID to RID enum.
- SID (Security Identifier)
  - ✓ Just like AD users refer to accounts by name, OS refers to accounts by SID numbers.
  - ✓ primary key for any object in AD unique to a domain.
  - ✓ No two accounts or groups on the computer ever share the same SID.
- RID (Relative Identifier)
  - ✓ unique, and assigned sequentially by domain controller
- For eg: A security identifier(SID) is actually **SID** + **RID**
  - ✓ **S-1-5-21-2000478354-1708537768-1957994488-500**

RID Cycling

- Well-known RID's:
  - ✓ Accounts & Groups - 500-999. For eg: 500 - Administrator, 501 - Guest, 502 - Krbtgt.
  - ✓ Users, groups, computers start at 1000.
- Well known security identifiers list : https://support.microsoft.com/en-us/kb/243330
- RID Cycling over NULL session may not work on Windows 2k8 onwards.
- RID Cycling over an authenticated "domain user account" will always work
  - Attackers run a rid cycling enumeration with valid domain user even if it works over null session as the former reveals some "extra" juicy information.
  - The juicy information include domain groups, account description, password policy etc.

RID Cycling

- enum4linux example (both auth and unauth attempts)

```
S-1-5-21-121509350-3731568236-3798821747-1108 *unknown*\*unknown* (8)
S-1-5-21-121509350-3731568236-3798821747-1109 *unknown*\*unknown* (8)
S-1-5-21-121509350-3731568236-3798821747-1110 HEADQUARTER\DnsAdmins (Local Grou
)
S-1-5-21-121509350-3731568236-3798821747-1111 HEADQUARTER\DnsUpdateProxy (Domai
 Group)
S-1-5-21-121509350-3731568236-3798821747-1112 HEADQUARTER\WINXP1$ (Local User)
S-1-5-21-121509350-3731568236-3798821747-1113 *unknown*\*unknown* (8)
S-1-5-21-121509350-3731568236-3798821747-1114 *unknown*\*unknown* (8)
S-1-5-21-121509350-3731568236-3798821747-1115 HEADQUARTER\rdpuser (Local User)
S-1-5-21-121509350-3731568236-3798821747-1116 *unknown*\*unknown* (8)
S-1-5-21-121509350-3731568236-3798821747-1117 *unknown*\*unknown* (8)
S-1-5-21-121509350-3731568236-3798821747-1118 *unknown*\*unknown* (8)
S-1-5-21-121509350-3731568236-3798821747-1119 *unknown*\*unknown* (8)
```

Priv. Esc. - Fundamentals

Info Gathering Exercises

- OS Information ,echo "%username%" or 'whoami'
- Patch levels – "wmic qfe get description,hotfixid,installedon"

KiTrap0D (KB979682), MS11-011 (KB2393802), MS10-059 (KB982799), MS10-021 (KB979683), MS11-080 (KB2592799).

- Networking – route print, arp –A, ipconfig /all , netstat –ano
- Firewall state – 'netsh firewall show state', 'netsh firewall show config'
- What is running – 'schtasks /query /fo LIST /v'
- Services under each process 'tasklist /svc', Modules - C:\>tasklist /M wind*
- Running Services 'net start'
- WMIC info gathering

Priv. Esc. - Fundamentals

- Unattended Installation Files (clear text, base 64 , may be encrypted at times)
  - ✓ c:\sysprep.inf
  - ✓ c:\sysprep\sysprep.xml
  - ✓ %WINDIR%\Software\Unattended.xml
- Registry settings "AlwaysInstallElevated"
- GPP saved passwords
- Insecure File/Service Permissions
- many more ways …

Priv. Esc. - Continued

- These include but not limited:
  - Insecure Password Storage Practices (clear text credentials in text readable configs, registry)
  - Write access to System32 Dir (Remember – sticky keys ☺)
  - Write access to all users start up folder/Weak file permissions (such as c:\, start-up folder)
  - Insecure configurations (Applications running as SYSTEM)
  - Unquoted Service/Binary Path Enumeration
  - DLL Hijacking (Insecure Library Loading) Attacks
  - Install a user-defined service, or replace that as a malicious service ☺ - come back when you want!
  - Local exploits (MS14-058, MS15-077, MS10-015, Kerberos fake TGT, token kidnapping, etc)

Attack Techniques

- Your five of five a day → Domain Controller ☺
  - Common ways for DC:
    - AD Kerberos attacks
    - PtH/PtT/OPtH
    - Insecure Service Permissions
    - Stepping up using other member servers
    - Nested administration groups

Kerberos Attacks

- SPN Scanning
  - MSSQL, RDP, Exchange Client Access Servers, Hyper-V, Vcenter, WinRM, PS Remoting.
  - https://github.com/PyroTek3/PowerShell-AD-Recon
- Silver and Golden Ticket (forged Kerberos TGS, TGT tickets)
- MS14-068 Kerberos Fake TGT Attacks
- "Kerberoast" technique?

Kerberos Attacks

- SPN Scanning
  - https://github.com/PyroTek3/PowerShell-AD-Recon
- Silver and Golden Ticket (forged Kerberos TGS, TGT tickets)
- MS14-068 Kerberos Fake TGT Attacks
- "Kerberoast" technique?


KEEP
CALM
AND
KEEP
SNIFFING

Pwning Compromising Domain – MS14-068

- The date : 04/12/2014
- The issue : MS14-068
  - Request a TGT without a PAC by sending a AS-REQ with PA-PAC-REQUEST set to false.
  - Forge a PAC claiming membership of DA group. 'Sign' it using plain MD5.
  - Create a TGS-ERQ message with krbtgt as the target. The TGT from the first step is used along the fake PAC encrypted with a sub-session key.
  - Send this to a vulnerable DC. KDC service will accept the forged and issue you a new TGT that contains a PAC, injected into memory.
- The exploit : PyKEK
- The DC : it's yours☺

Pwning Compromising Domain – MS14-068

- PyKEK ms14-068.py needs:
  - ✓ User Principal Name for e.g. bob@skyfall.local
  - ✓ User Password : W0rdP@ss987$$
  - ✓ SID (User security identifier): S-1-5-21-2812033177-3903828100-4160366606-1107
  - ✓ DC: pdc.skyfall.local
  - ✓ Don't' forget to config synch (/etc/resolv.conf)

Pwning Compromising Domain – MS14-068

- Obtain Kerberos ticket of the user bob from DC

```
root@kali:~/Tools/pykek-master# python ms14-068.py -u bob@SKYFALL.LOCAL -s S-1-5-21-281
2033177-3903828100-4160366606-1107 -d PDC.SKYFALL.LOCAL
Password:
  [+] Building AS-REQ for PDC.SKYFALL.LOCAL... Done!
  [+] Sending AS-REQ to PDC.SKYFALL.LOCAL... Done!
  [+] Receiving AS-REP from PDC.SKYFALL.LOCAL... Done!
  [+] Parsing AS-REP from PDC.SKYFALL.LOCAL... Done!
  [+] Building TGS-REQ for PDC.SKYFALL.LOCAL... Done!
  [+] Sending TGS-REQ to PDC.SKYFALL.LOCAL... Done!
  [+] Receiving TGS-REP from PDC.SKYFALL.LOCAL... Done!
  [+] Parsing TGS-REP from PDC.SKYFALL.LOCAL... Done!
  [+] Creating ccache file 'TGT_bob@SKYFALL.LOCAL.ccache'... Done!
root@kali:~/Tools/pykek-master#
```

- Copy this Kerberos ticket to local cache:
- "mv TGT_bob@skyfall.local.ccache /tmp/krb6cc_0"

Pwning Compromising Domain – MS14-068

- Check if it's valid ticket:

```
root@kali:~/Tools/smbexec-2-master/progs# smbclient -W skyfall.local -k //PDC.skyfall.l
ocal/C$
OS=[Windows Server 2008 R2 Datacenter 7601 Service Pack 1] Server=[Windows Server 2008
R2 Datacenter 6.1]
smb: \> ls
  $Recycle.Bin                       DHS        0  Tue Jul 14 03:34:39 2009
  .rnd                                 A     1024  Tue Mar 29 14:29:54 2016
  Boot                               DHS        0  Tue Mar  1 17:18:00 2016
  bootmgr                          AHSR   383786  Sun Nov 21 03:24:02 2010
  BOOTSECT.BAK                     AHSR     8192  Tue Mar  1 17:18:00 2016
  Documents and Settings             DHS        0  Tue Jul 14 06:06:44 2009
  pagefile.sys                       AHS 4600549376  Tue Mar 29 14:30:15 2016
  PerfLogs                             D        0  Tue Jul 14 04:20:08 2009
  Program Files                       DR        0  Tue Mar 29 14:29:44 2016
  Program Files (x86)                 DR        0  Tue Mar  1 15:58:49 2016
  ProgramData                         DH        0  Tue Mar  1 09:26:06 2016
  Recovery                           DHS        0  Tue Mar  1 09:23:43 2016
  System Volume Information          DHS        0  Tue Mar  1 15:58:59 2016
  tmp                                  D        0  Tue Mar  1 10:02:51 2016
  Users                               DR        0  Tue Mar  1 09:23:56 2016
  Windows                              D        0  Tue Mar 29 14:51:29 2016

                39999 blocks of size 524288. 15506 blocks available
smb: \>
```

DEFENDZA

Offensive Powershell

- Mimikatz, related modules ported into PowerShell
- PowerShell frameworks for offensive use
  - PowerView, PowerUp
  - Empire
  - Nishang
  - PowerOPS
  - …

Dumping Hashes

- Passwords

Everchanging Attack Landscape

- Today's attacks are outsmarting traditional attacks:
  - ✓ Utilizing inbuilt/IT tools rather than tools written by security community to avoid detection. Multiple scenarios include:
    - ✓ Enumeration and discovery exercises using inbuilt tools
    - ✓ Priv escalation work – Info gathering using inbuilt tools
    - ✓ ntds.dit dump using ntdsutil
    - ✓ Kerberoasting
    - ✓ Powershell techniques to evade AV's and other defences.

- Security Analytics

Threat Detection and Prevention

DEFENSE - Detect, Mitigate, Prevent

- Detect – Identifying the malicious events in action (incident and event monitoring)
- Mitigate – Mitigating threats to the organization (vulnerability management)
- Prevent – Raising the game (costs/difficulty – purple stuff)

Detect – Kerberos Attacks

- Kerberos Attacks Detection
  - Look for Kerberos RC4 stuff!
  - Ensure forest trusts support and AES is enabled*, otherwise watch out for RC4 usage (0x17 events)
  - Audit Kerberos Service Ticket Operations via GPO
  - Advanced Audit Policy Configuration

(If TGS fails, failure events with Failure Code field 0x0 on DC's)

Event ID	Event
4769	A Kerberos service ticket was requested
4770	A Kerberos service ticket was renewed

- Trust Properties -AES* : https://technet.microsoft.com/en-us/library/dd145414.aspx

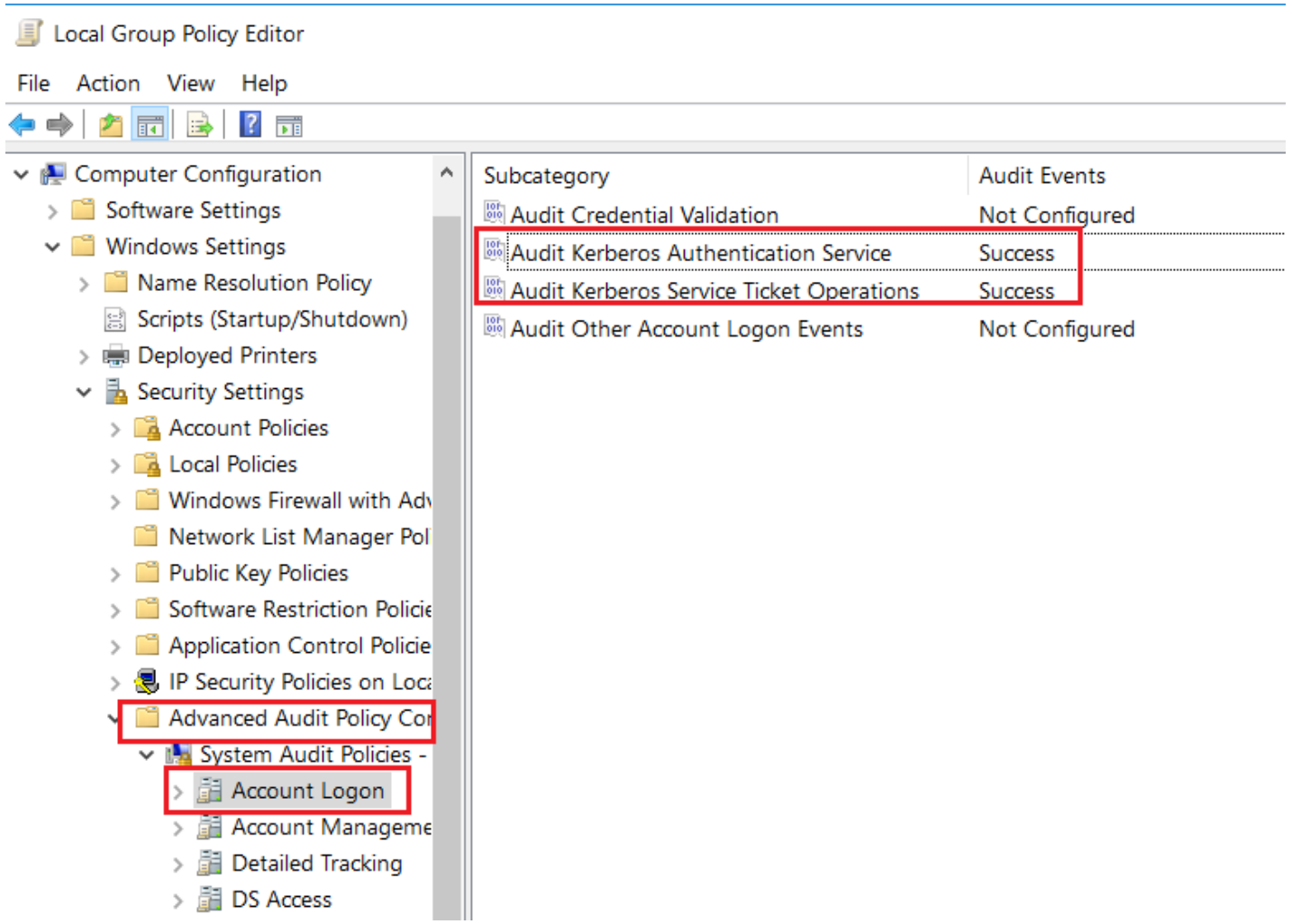
Detect – Kerberos Attacks

- Admin logon, logon and logoff events
- Golden – DC
- Silver - members

Kerberos Encryption Types

Hex	Etype
0x1	des-cbc-crc
0x2	des-cbc-md4
0x3	des-cbc-md5
0x4	[reserved]
0x5	des3-cbc-md5
0x6	[reserved]
0x7	des3-cbc-sha1
0x9	dsaWithSHA1-CmsOID
0xa	md5WithRSAEncryption-CmsOID
0xb	sha1WithRSAEncryption-CmsOID
0xc	rc2CBC-EnvOID
0xd	rsaEncryption-EnvOID
0xe	rsaES-OAEP-ENV-OID
0xf	des-ede3-cbc-Env-OID
0x10	des3-cbc-sha1-kd
0x11	aes128-cts-hmac-sha1-96
0x12	aes256-cts-hmac-sha1-96
0x17	rc4-hmac
0x18	rc4-hmac-exp
0x41	subkey-keymaterial

Source : https://blogs.technet.microsoft.com/askds/2010/10/19/hunting-down-des-in-order-to-securely-deploy-kerberos/


Local Group Policy Editor
File Action View Help
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Firewall with Adv
Network List Manager Pol
Public Key Policies
Software Restriction Policie
Application Control Policie
IP Security Policies on Loca
Advanced Audit Policy Con
System Audit Policies -
Account Logon
Account Manageme
Detailed Tracking
DS Access
Subcategory
Audit Events
Audit Credential Validation
Not Configured
Audit Kerberos Authentication Service
Success
Audit Kerberos Service Ticket Operations
Success
Audit Other Account Logon Events
Not Configured

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-A5BA-3E3B0328C30D}" />
<EventID>4769</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>14337</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2017-10-07T18:13:46.043256100Z" />
<EventRecordID>166746</EventRecordID>
<Correlation />
<Execution ProcessID="520" ThreadID="1496" />
<Channel>Security</Channel>
<Computer>DC02.skyfall.local</Computer>
<Security />
</System>
- <EventData>
<Data Name="TargetUserName">admin@skyfall.LOCAL</Data>
<Data Name="TargetDomainName">skyfall.LOCAL</Data>
<Data Name="ServiceName">WIN2008R2$</Data>
<Data Name="ServiceSid">S-1-5-21-3457937927-2983337994-983703824-1107</Data>
<Data Name="TicketOptions">0x40810000</Data>
<Data Name="TicketEncryptionType">0x12</Data>
<Data Name="IpAddress">::ffff:10.0.0.12</Data>
<Data Name="IpPort">49272</Data>
<Data Name="Status">0x0</Data>
<Data Name="LogonGuid">{F85C455E-C66E-205C-6B39-F6C60A7FE453}</Data>
<Data Name="TransmittedServices">-</Data>
</EventData>
</Event>
```

Whom to monitor?

- Monitoring Recommendations
  - Account Naming Conventions
  - High Privilege Accounts (EA, DA, BA, DBA, so on)
  - Outside working hours, external vendors with VPN access, or other anomalies with malicious action probability
  - Non-active, disabled or guest accounts that should never be used
  - Restricted Use systems/devices

Detect – PowerShell

- Offensive Powershell
  - PowerShell logging via GPO

```
Computer Configuration\Policies\Administrative
Template\Windows Components\Windows PowerShell
```

  - Modules Logging
  - Script Block Logging
  - Transcription Logging

Detect – PowerShell

- Automatic Script Block Logging
  - Microsoft-Windows-PowerShell/Operational
  - Log events – EventId 4104
  - Invocation logging – EventId 4105
- Tools
  - System.reflection , Token_privileges, Token_impersonate, token_duplicate, token_privileges
  - 4103

Detect – Signs of compromise

- Monitoring AD

Event ID	P. Criticality	Event
4618	High	A monitored security event pattern
4649	High	Replay attack
4719	High	System audit policy changed
4765	High	SID history was added to an account
4766	High	An attempt for SID history change failed
4794	High	DS restore mode attempt
4706	High	A new trust was created to a domain
1102	Medium to High	Audit log was cleared

Detect – Signs of compromise

Event ID	P. Criticality	Event
4672	High	Assigned special privileges to a new logon
4673	High	Called a privilege service
4674	Medium	Attempted an operation on a privileged object

- Audit Sensitive Privilege Use

https://technet.microsoft.com/en-us/library/dd772724%28v=ws.10%29.aspx

Mitigate - Kerberos Attacks

- Kerberoasting
  - Ensure that service account passwords are longer than 25 characters
  - Ensure that passwords aren't easily guessable

- AMSI (Antimalware Scan Interface) Integration
  - Antimalware, Security and Identity, PowerShell, Jscript, VBScript

Prevent - Reducing the Attack Surface

- Implementing Least-Privilege Administrative Model
- Implementing Secure Administrative Hosts
- Securing Domain Controllers against an attack

Least-Privilege Administrative Model

- *Everyone knows, NO ONE follows* 😐
- The Privilege Problem
  - Overuse of privileges - Permanently granted
  - Pass the hash attacks
    - ✓ Easily obtained deep privs to be sprayed around
    - ✓ Excessive number of permanent accounts with high priv.
- 🚫 EA, DA, BA are all powerful groups

Least-Privilege Administrative Model

- Excessive Privilege Problems
  - Active Directory
  - Member Server
  - Workstations
  - Applications

Reducing Privileges

- Securing Local Administrator Accounts
  - Disabling local admin
  - Configuring GPOs to Restrict Administrator Accounts on Domain-Joined Systems (**Computer Configuration\Policies\Windows Settings\Security Settings\Local Settings\User Rights Assignments**)
- Securing Local Privileged Accounts and Groups in AD
  - Securing built-in accounts in AD
  - Controls for built-in Administrator Accounts

Controls for built-in Administrator Accounts

- Goal is to slow down attacker's progress and limit the damage
  - Enable the "`Account is sensitive and cannot be delegated`" flag on the account
  - Enable the "`Smart card is required for interactive logon`" flag on the account
  - Disable the account
  - Configuring GPOs to Restrict Domains' Administrator Accounts on Domain-Joined Systems & Domain Controllers

Secure Administrative Hosts

- Principles
  - Never administer a trusted system from a less-trusted host
  - Do not rely on a single auth factor when performing privileged tasks. Configuring GPOs to Restrict Domains' Administrator Accounts on Domain-Joined Systems & Domain Controllers
  - Do not forget physical security when designing and implementing secure administrative hosts

Secure Administrative Hosts and DC's

- Account Configuration
- Physical Security
- AppLocker
- RDP Restrictions
- Patch and Configuration Management
- Blocking Internet Access
- Virtualization
- Perimeter FW settings

References/Sources

- Images Sources – Mostly Technet
- Best Practices for Securing AD

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory

- Events to monitor

https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

- A very good resource

https://adsecurity.org/

Further…

- Microsoft ATA (formerly Aorato)
- Upcoming Players

Merci
Obrigada
Grazie
ThankYou

harman@defendza.com
@digitalamli