Active Directory Tiering & Protection

Hands-on AD Analysis and Protection





Slavi Parpulev

IT Security Expert

sparpulev@ine.com

@binary_raider

linkedin.com/in/slavi-parpulev/

eCPTX

eWPTX

OFFENSIVE Security OSCP

OFFENSIVE Security OSCE

GIAC CERTIFIED FORENSIC ANALYST GCFA

Course Outline

Common AD Attacks & Tools

- Kerberoast, DCSync, Golden ticket and many more
- BloodHound, PingCastle, New-ADReport

AD Tiering and Protection

- AD Tiering
- Privileged Access Workstation
- Passwords and Password Policies

Add-on tools and topics

- Windows Defender for Identities

Common AD Attacks & Tools



Common AD Attacks & Tools

- Kerberoasting & ASREPRoast
- Plain Text Passwords (shares, AD object attributes)
- Lateral movement with Local Administrator
- Kerberos Delegation (and the Printer bug)
- Group Policy Preferences
- DCSync
- BloodHound (nested groups, OU delegations)
- PingCastle (broad output, looks also at ability for all users to modify logon scripts, GPOs etc.)
- New-ADReport

Kerberoasting & ASREPRoast

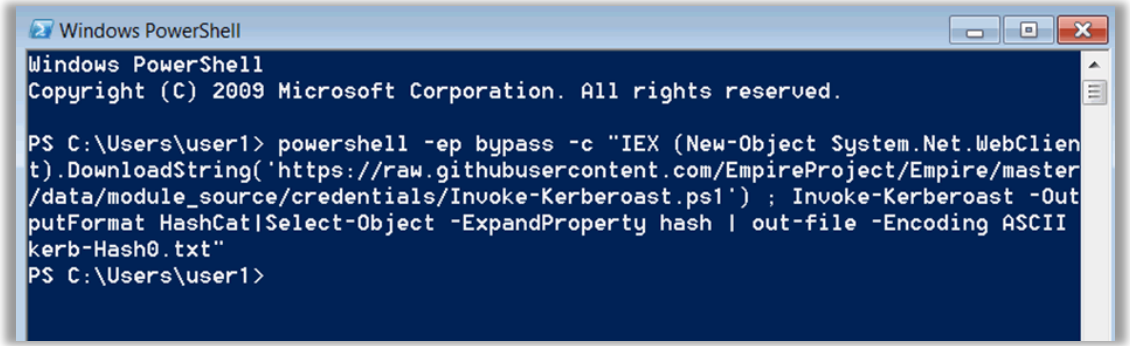
Common AD Attacks & Tools



Kerberoast

Kerberoast is:

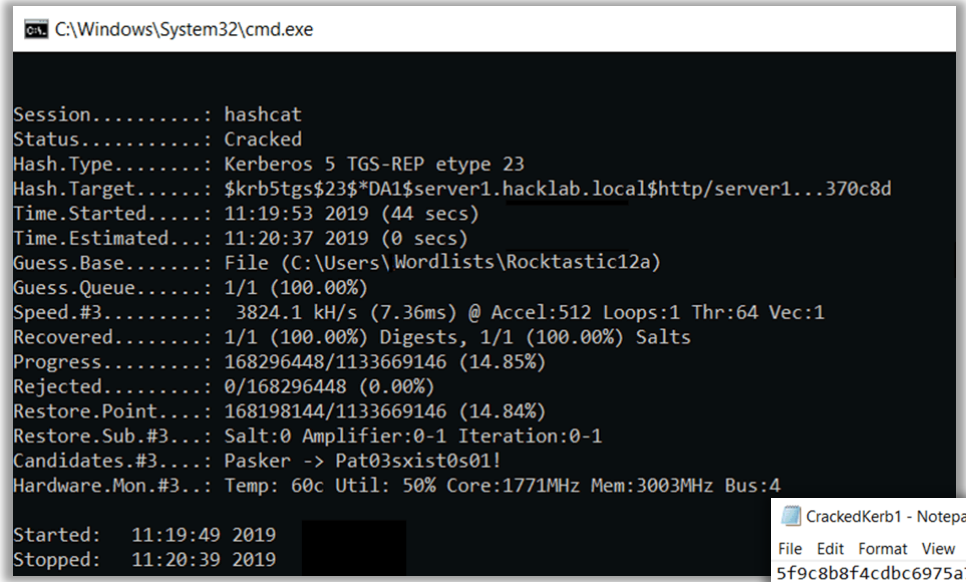
+ Requesting a Kerberos TGS service ticket for an account with SPN. The ticket is encrypted with the service user's NTLM password hash.

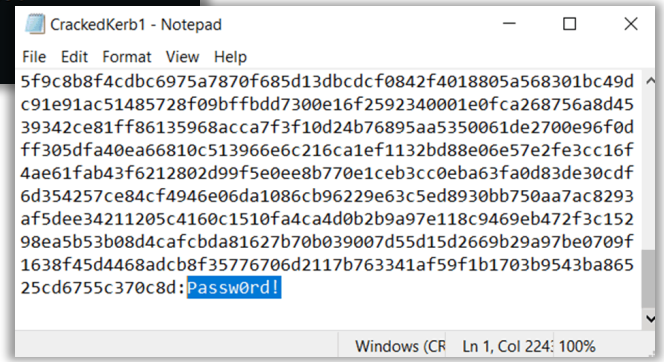


https://www.pentestpartners.com/security-blog/how-to-kerberoast-like-a-boss/

Kerberoast

Crack the obtained ticket





https://www.pentestpartners.com/security-blog/how-to-kerberoast-like-a-boss/

Kerberoast

- Weak service account passwords make this attack possible.

- Prevent Kerberoast:
  - Group Managed Service Accounts
  - Normal Service Accounts with LONG passwords

https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/group-managed-service-accounts-overview

ASREPRoast

- Is a similar style attack to Kerberoast but it extracts crackable tickets for users who do not require Kerberos pre-authentication (SPNs not required).

- The success of the attack depends on the strength of the user's password.

https://www.harmj0y.net/blog/activedirectory/roasting-as-reps/

ASREPRoast

PROTECTION

Do not set user to not require Kerberos pre-authentication.

+ If needed, ensure long, uncrackable passwords.

https://www.harmj0y.net/blog/activedirectory/roasting-as-reps/

Plain Text Passwords

Common AD Attacks & Tools

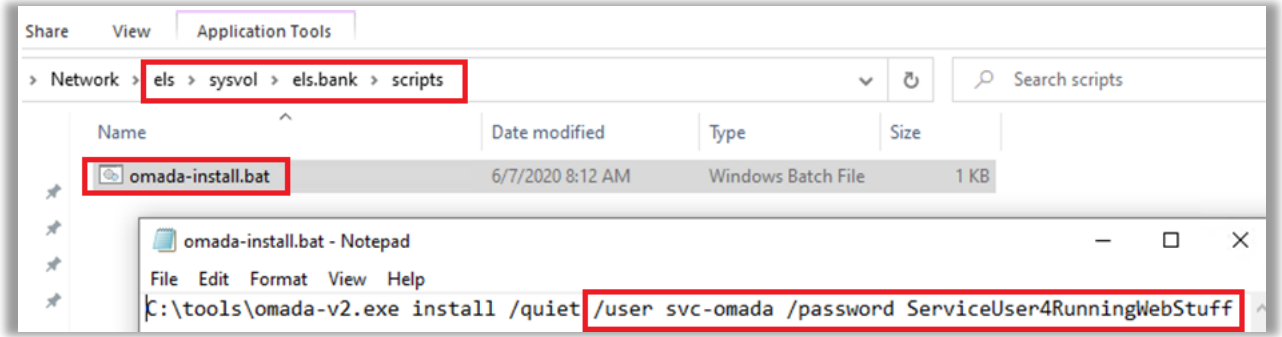


Plain Text Passwords

- Passwords in scripts placed on shares
  - Invoke-ShareFinder

findstr /s /i /m "pass" \\SHARE\PATH.<FILEEXTENSION>*
findstr /s /i /m "pass" \\FileServer01\Scripts.ini*

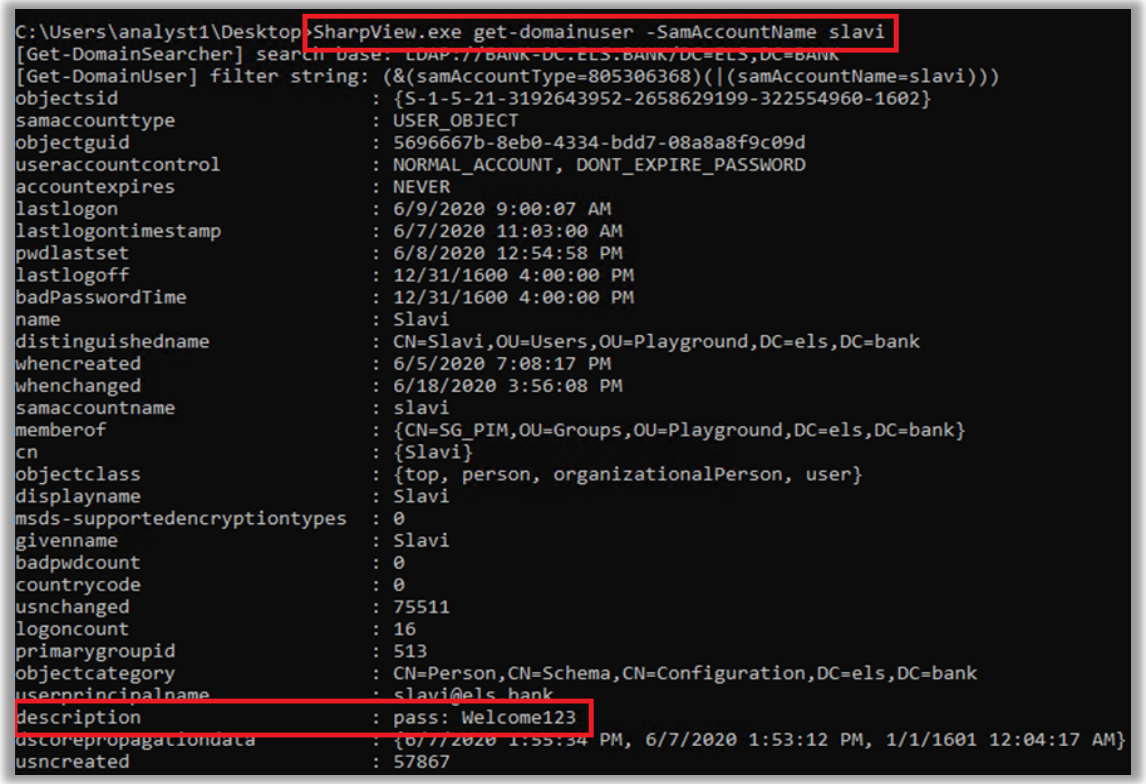
.ini
.conf
.config
.cmd
.bat
.vbs
.ps1



https://improsec.com/tech-blog/securing-windows-environments
https://github.com/PowerShellMafia/PowerSploit/blob/dev/Recon/PowerView.ps1

Plain Text Passwords

Passwords in AD Object attributes



https://github.com/binaryAccess/highway_to_hell/blob/master/SearchUser.ps1
https://github.com/binaryAccess/highway_to_hell/blob/master/SearchGroup.ps1

Plain Text Passwords

It is extremely hard to prevent.

- Regular scans should be performed to identify
- Teach employees to not store plain text passwords (they may do it anyway)

Lateral Movement with Local Administrator

Common AD Attacks & Tools



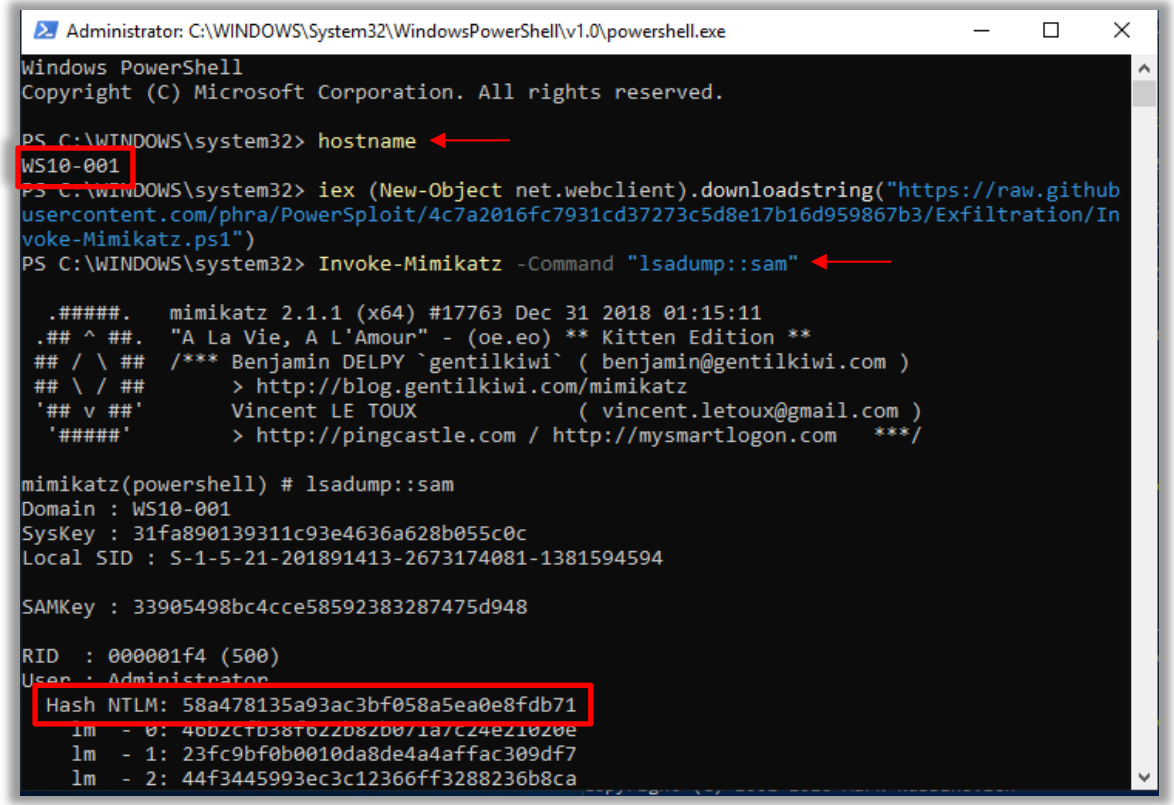
Lateral Movement with Local Administrator

THE PROBLEM

- Same password reused across all workstations/servers.
- Password hash stored locally in the Registry Hive files.
- Connect remotely to another machine with the password hash.

Lateral Movement with Local Administrator

Extracting the password hash



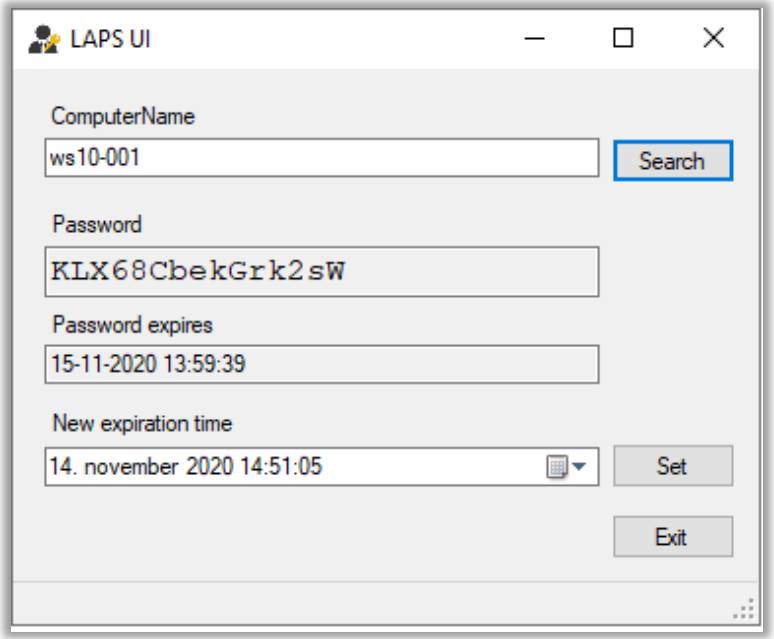
Lateral Movement with Local Administrator

Using the password hash

```
root@THP:~# crackmapexec smb server01.prod.local -u 'Administrator' -H '58a478135a93ac3bf058a5ea0e8fdb71' -x hostname --local-auth
CME          server01.prod.local:445 SERVER01       [*] Windows 10.0 Build 17763 (name:SERVER01) (domain:PROD)
CME          server01.prod.local:445 SERVER01       [+] SERVER01\Administrator 58a478135a93ac3bf058a5ea0e8fdb71 (Pwn3d!)
CME          server01.prod.local:445 SERVER01       [+] Executed command
CME          server01.prod.local:445 SERVER01       Server01
[*] KTHXBYE!
root@THP:~#
```

Lateral Movement with Local Administrator

- To prevent lateral movement with local users, we need unique passwords for each user!



https://www.microsoft.com/en-us/download/details.aspx?id=46899

Kerberos Delegation

Common AD Attacks & Tools



Kerberos Delegation

"Kerberos delegation enables an application to access resources hosted on a different server... Instead of giving the service account running the web server access to the database directly, you can allow the web server service account to be delegated to the SQL server service. Once a user logs into the website, the web server service account will request access to the SQL server service on behalf of that user. This allows the user to get access to the content in the database that they've been provisioned to, without having to provision any access to the web server service account itself."

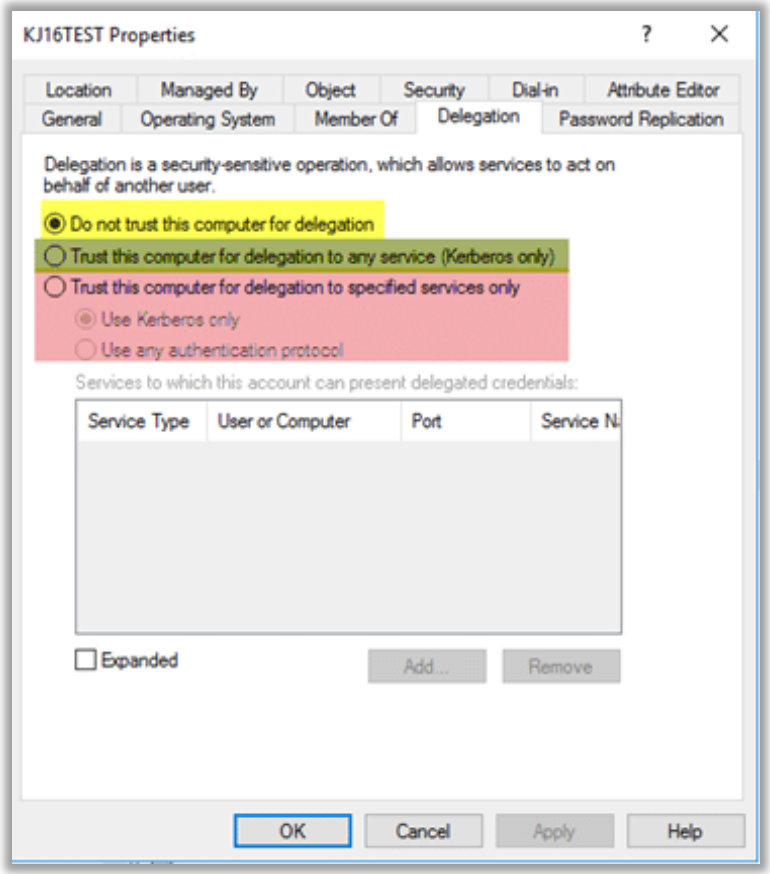
https://stealthbits.com/blog/what-is-kerberos-delegation-an-overview-of-kerberos-delegation/



Kerb
Deleg

There are 3 ty
delegation:

+ Unconstrai
+ Constraine
  (link)
+ Resource-B
  Delegation



https://stealthbits.com/blog/what-is-kerberos-delegation-an-overview-of-kerberos-delegation/
https://posts.specterops.io/kerberosity-killed-the-domain-an-offensive-kerberos-overview-eb04b1402c61
https://www.parpulev.com/2019/05/the-mind-blowing-kerberos-use-any.html

Kerberos Delegation

DEMO (Unconstrained Delegation + Printer Bug)



Kerberos Delegation

PROTECTION

- “This Account is Sensitive and Cannot be Delegated”
- “Protected Users” group
- Protect users and computers which are used in delegation.
- Kerberos Delegation brings risks to the environment, avoid using to the extend possible and clean up if not used anymore.

Group Policy Preferences

Common AD Attacks & Tools



Group Policy Preferences

- Stored encrypted credentials in GPP files (e.g. Scheduled tasks).
- Encryption key published online:



2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key.<3>

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
```

https://adsecurity.org/?p=2288

Group Policy Preferences

- Example of GPP file with encrypted password:

```
<?xml version="1.0" encoding="utf-8" ?>
- <Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}">
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-
      02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}">
      <Properties action="U" newName="ADSAdmin" fullName="" description=""
        cpassword="RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ"
        changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator
        (built-in)" expires="2015-02-17" />
    </User>
  </Groups>
```

- Decrypting the password:

```
PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiI0Cau1DtrtTe3wdFwzCiWB5PSAxXMDstchJt3bL0Uie0BaZ/7rdQjuqTonF3ZWAKa1iRvd4JGQ'
#Super@Secure&Password$2015?
```

https://adsecurity.org/?p=2288

Group Policy Preferences

PROTECTION

- Microsoft released a Patch that protects admins from entering credentials in those files but it does not fixed already existing credentials!
- Scan yourself and remove all files containing the password.

https://adsecurity.org/?p=2288

DCSync

Common AD Attacks & Tools



DCSync

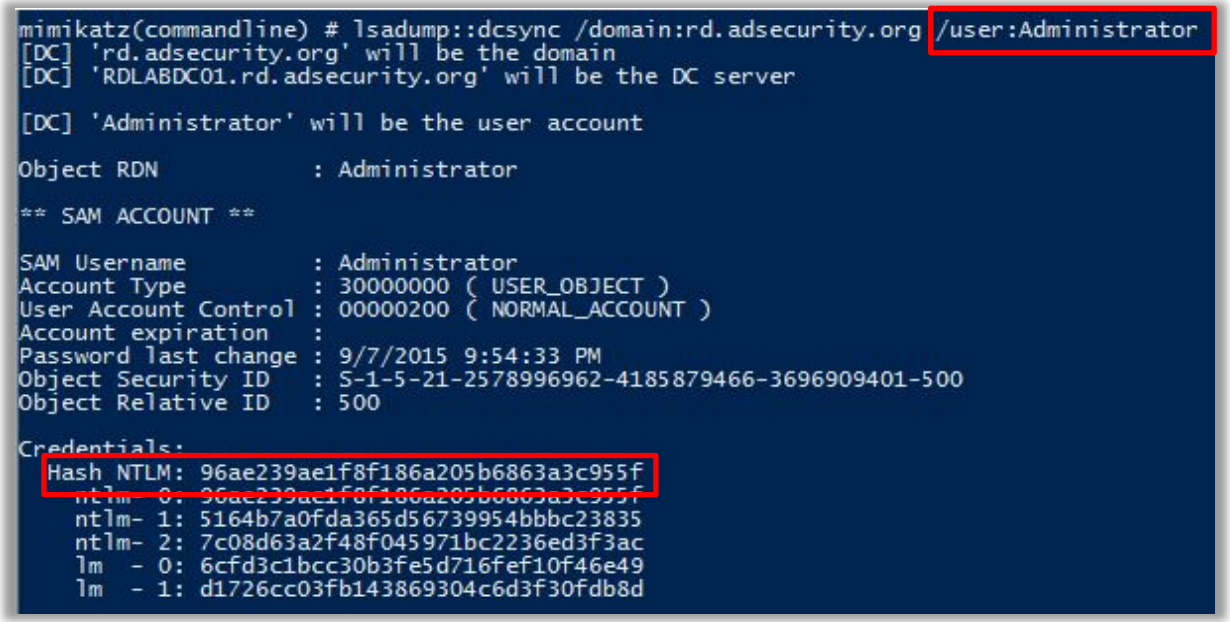
- An attack which “impersonates” a Domain Controller and performs replication that extracts password hashes from Active Directory.

https://adsecurity.org/?p=1729

DCSync

Require permissions:

+ Directory Replicate Changes
+ Directory Replicate Changes All



https://adsecurity.org/?p=1729

DCSync

PROTECTION

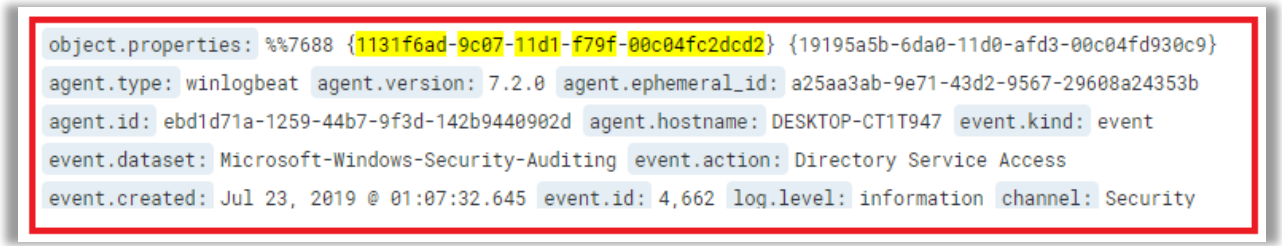
- Avoid granting replication permissions to users or computers in the environment. If needed, ensure long, complex passwords for users.
- Detection is easier – alert on replication triggered by anything but Domain Controller.

https://adsecurity.org/?p=1729

DCSync

Detection

```
event.id:4662 AND NOT (user.name:*$ OR user.name:AUTHORITY OR user.name:Window) AND
(object.properties:1131f6ad-9c07-11d1-f79f-00c04fc2dcd2 OR
object.properties:Replicating)
```



BloodHound

Common AD Attacks & Tools



BloodHound

- BloodHound is a tool that can “reveal the hidden and often unintended relationships within an Active Directory environment.”
- “Attackers can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths.”

https://github.com/BloodHoundAD/BloodHound

BloodHound

BloodHound consists of 2 parts:

1. An ingestor, which captures the data (executed in the environment).
    + SharpHound (C# Implementation, very fast!)
    + Can extract data for local group membership, domain trusts, sessions on devices, domain group membership, ACLs on objects and more.

https://github.com/BloodHoundAD/BloodHound
https://github.com/BloodHoundAD/SharpHound3

INE

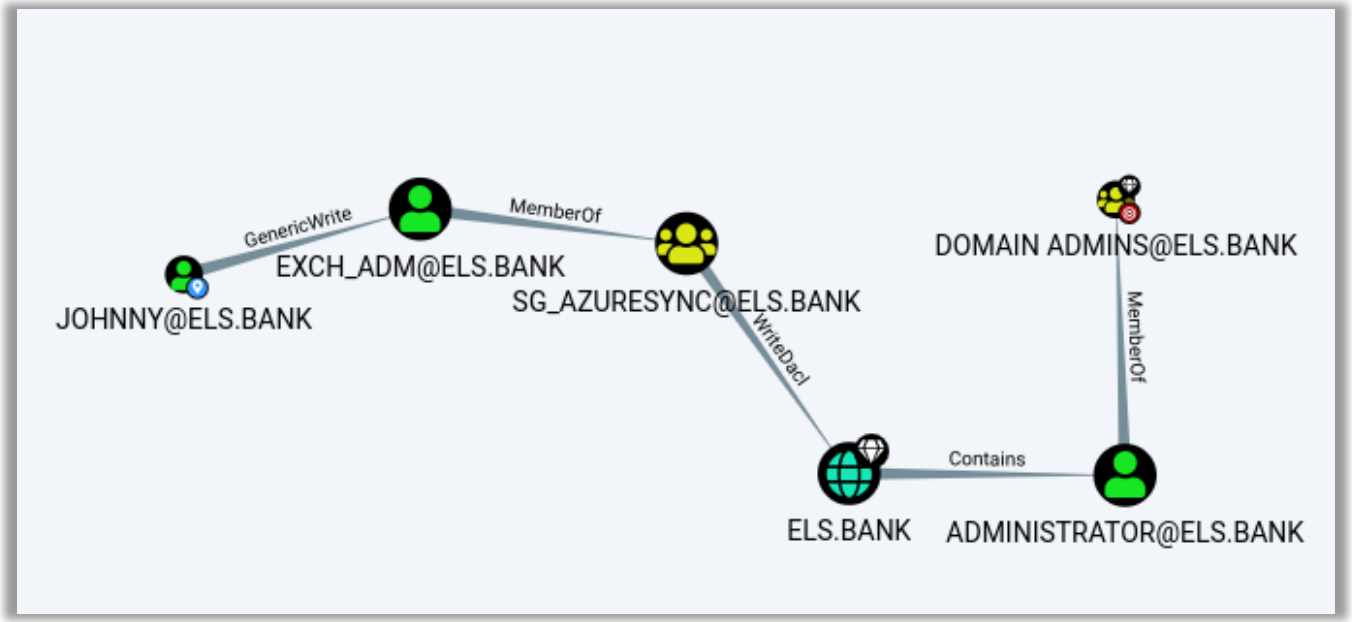
BloodHound

BloodHound consists of 2 parts (continued):

2. GUI that analyses and displays the data (can be executed offline).
    + Visualizes complex paths that may exist from a starting user/computer to a target (can be group, user, computer).
    + E.g. search if there is a path from user “Slavi” to “Domain admins.

https://github.com/BloodHoundAD/BloodHound
https://github.com/BloodHoundAD/SharpHound3

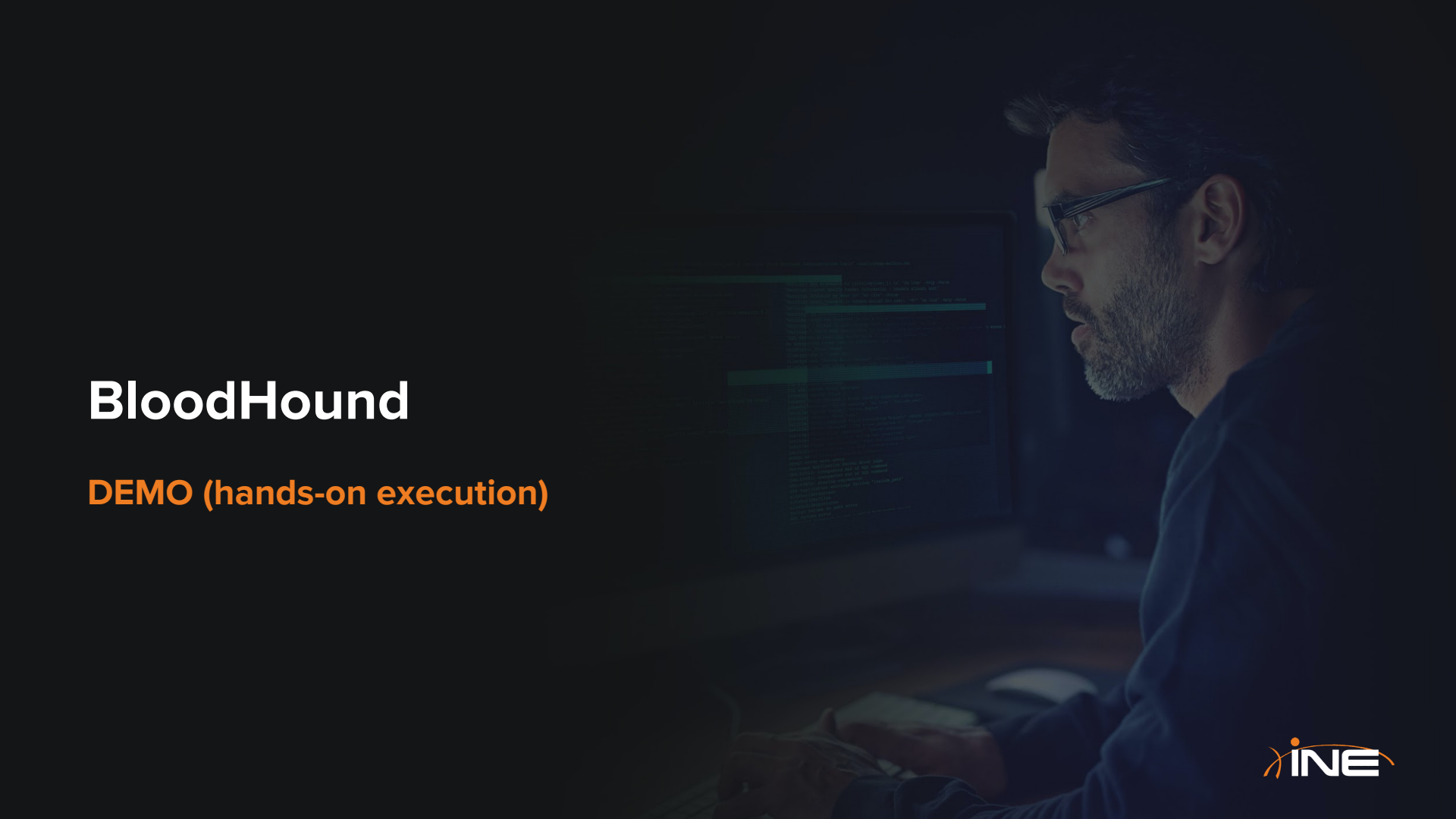
BloodHound Example



https://github.com/BloodHoundAD/BloodHound
https://github.com/BloodHoundAD/SharpHound3

BloodHound

DEMO (hands-on execution)



Ping Castle

Common AD Attacks & Tools

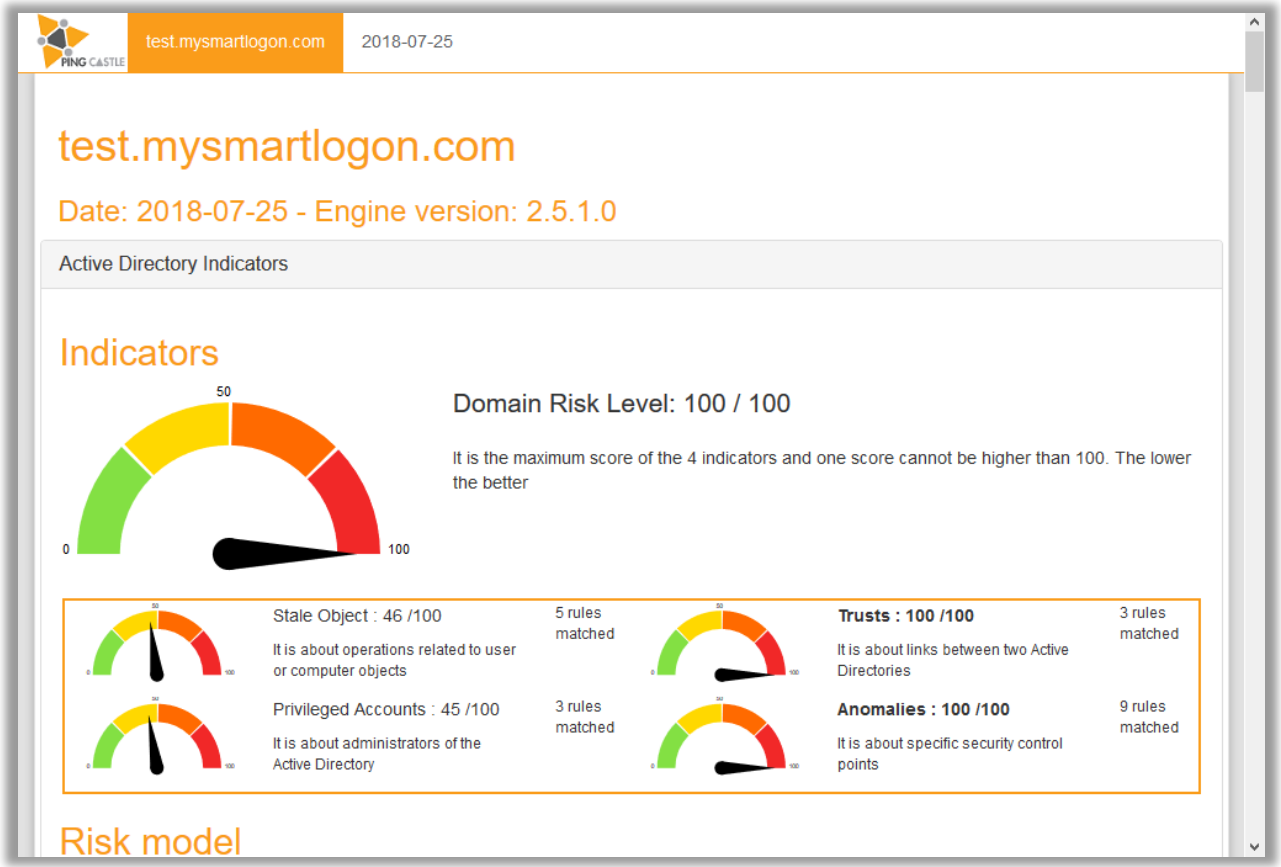


Ping Castle

- Ping Castle is a tool that scans your environment and generates a report, which rates the severity of the findings.

https://www.pingcastle.com/

Ping Castle



https://www.pingcastle.com/

Ping Castle

PingCastle has an extremely broad range of issues that it may flag, so the best way to learn about them is really to use the tool:

+ It will show information about all computers and users.
+ Common issues such as GPP passwords, SMBv1 and Spooler on DCs.
+ Misconfigured ACLs such as “Domain Users” having full control over a GPO.
+ Checks LAPS is installed.
+ Many more …

https://www.pingcastle.com/

Ping Castle



https://www.pingcastle.com/

Ping Castle



https://www.pingcastle.com/

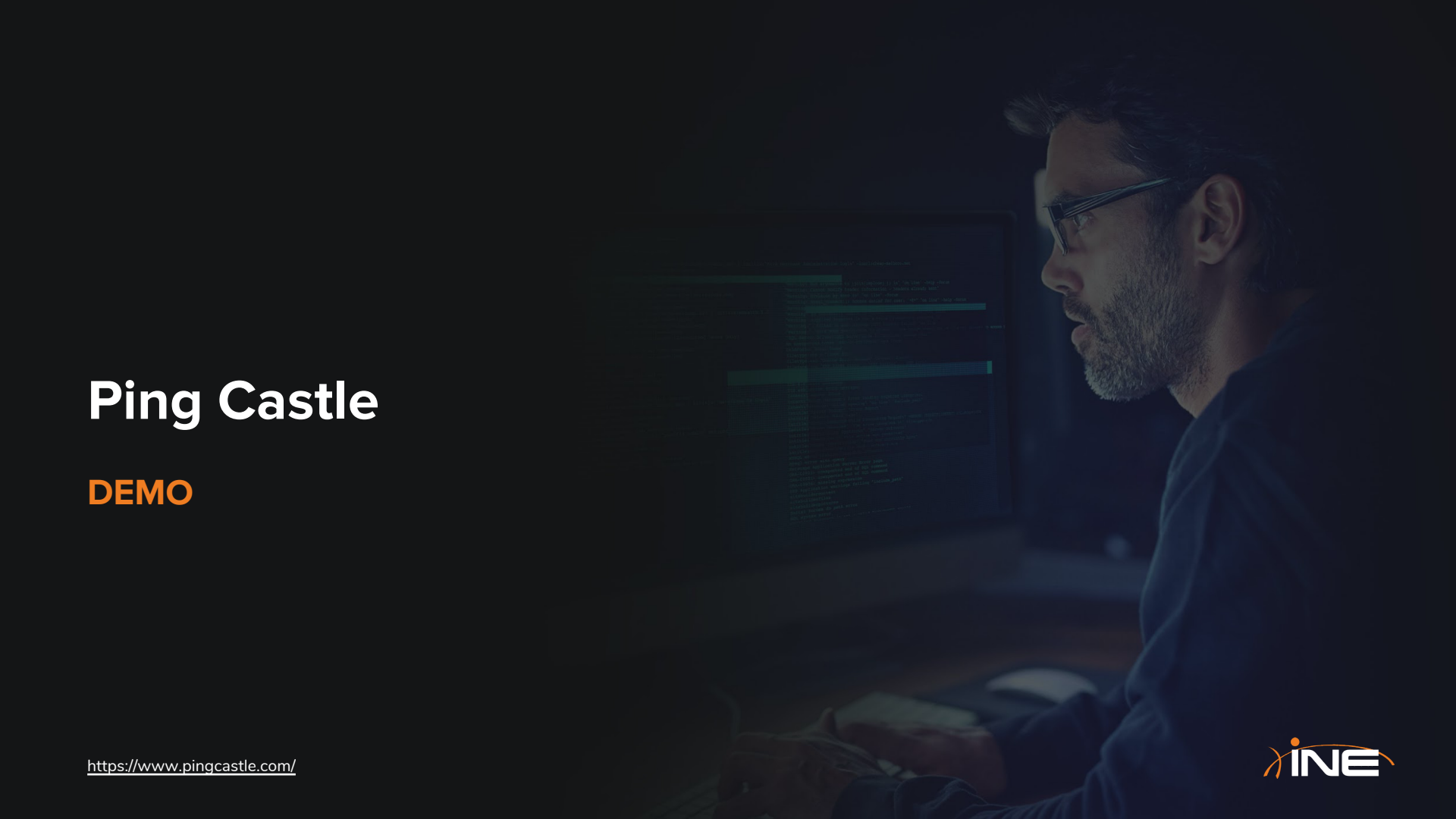
Ping Castle



https://www.pingcastle.com/

Ping Castle

DEMO



https://www.pingcastle.com/

New-ADReport

Common AD Attacks & Tools



New-ADReport

- A PowerShell script that will collect information about all users and computers in active directory. It will output the information in a CSV file, which can be used with programs such as Excel for filtering afterwards.
- Requires RSAT PowerShell Module

https://github.com/ZilentJack/New-ADReport

New-ADReport

```
PS C:\users\Administrator\Desktop\newad> New-ADReport -DumpFile_ComputerInfo -DumpFile_PrivilegedUserInfo
-DumpFile_UserInfo -WriteHost_FinalReport -Verbose
VERBOSE: Scan AD version                : 1.30
VERBOSE: - File Time Stamp              : 20201115224341
VERBOSE: - Start Time                   : 11/15/2020 22:43:41
VERBOSE: Progress: Getting forest info...
VERBOSE: Progress: Getting domain info...
VERBOSE: Progress: Getting default domain password policy...
VERBOSE: Progress: Checking for fine grained password policies...
VERBOSE: Progress: Getting AD trust info...
VERBOSE: Progress: Finding special accounts...
VERBOSE: Progress: Getting AD users...
VERBOSE: Progress: Getting AD computers...
VERBOSE: Progress: Getting DC information...
VERBOSE: Progress: Getting enabled AD accounts...
VERBOSE: Progress: Getting disabled AD accounts...
VERBOSE: Progress: Getting members of interesting groups...
VERBOSE: GlobalCatalog used: DC01.prod.local:3268
```

https://github.com/ZilentJack/New-ADReport

New-ADReport

ADReport-prod.local-20201115224341-Report.txt - Notepad

File Edit Format View Help

```
"New-ADReport version          : [1.30]
 - File Time Stamp             : [20201115224341]
 - Start Time                  : [11/15/2020 22:43:41]

[ACTIVE DIRECTORY]
Basic info:
 - DNSRoot                     : prod.local
 - NetBIOS Name                : PROD
 - Domain SID                  : S-1-5-21-3731479394-1286008385-2671550507
 - Forest                      : prod.local
 - Forest Root Domain          : True
 - Domain Functional Level     : Windows2016Domain
 - Forest Functional Level     : Windows2016Forest
 - Number of trusts            : 0
 - Last krbtgt reset           : 04/03/2019 12:23:22
 - Administrator name (500)    : PROD\administrator
 - Guest name (501)            : PROD\Guest
```

Name	SID	SIDHistory	DNSHo	IPv4Ad	Enable	Created	AllowRevers	DoesN
DC01	S-1-5-21-3731479394-1286008385-2671550507-1000		DC01.proc	192.168.1(	TRUE	03/04/2019 12:23	FALSE	FALSE
SERVER01	S-1-5-21-3731479394-1286008385-2671550507-1104		Server01.p	192.168.1(	TRUE	24/04/2019 13:18	FALSE	FALSE
WS10-001	S-1-5-21-3731479394-1286008385-2671550507-1106		WS10-001	192.168.1(	TRUE	17/12/2019 16:38	FALSE	FALSE

https://github.com/ZilentJack/New-ADReport

Krbtgt & Golden tickets



Krbtgt & Golden tickets

- Krbtgt (Golden tickets)
- DEMO – Reset the password with the recommended Scripts

Krbtgt (Golden tickets)

- “krbtgt” is a disabled account that exists in all Active Directory domains. It cannot be deleted or renamed.
- It is the service account for the Key Distribution Center service.
- It encrypts and signs all Kerberos tickets.

https://adsecurity.org/?p=483

Krbtgt (Golden tickets)

THE PROBLEM

+ Anyone can create valid Kerberos TGTs if the password hash of “krbtgt” is known (Golden ticket)

https://adsecurity.org/?p=483

Krbtgt (Golden tickets)

- Resetting the password of “krbtgt” periodically is highly recommended.
  - Use the recommended scripts.

- If Active Directory forest has been compromised, you need to reset the passwords of all users, and for “krbtgt”, it has to be twice (due to password history n-1).

https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

Krbtgt (Golden tickets)

FUN FACT

+ Changing the password to a known value will get overwritten to a random one automatically

https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

Krbtgt (Golden tickets)

DEMO – Reset the password with the recommended Scripts



https://gallery.technet.microsoft.com/Reset-the-krbtgt-account-581a9e51

Active Directory Tiering

Part 1 - Theory



Active Directory Design and Protection

- The Problem - Credential and Identity Theft
- Active Directory Tiering Model

The Problem

Credential and Identity theft

```
  .#####.   mimikatz 2.0 alpha (x86) release "Kiwi en C" (Apr  6 2014 22:02:03)
 .## ^ ##.
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   https://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with  13 modules * * */


mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 515764 (00000000:0007deb4)
Session           : Interactive from 2
User Name         : Gentil Kiwi
Domain            : vm-w7-ult-x
SID               : S-1-5-21-1982681256-1210654043-1600862990-1000
        msv :
         [00000003] Primary
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * LM       : d0e9aee149655a6075e4540af1f22d3b
         * NTLM     : cc36cf7a8514893efccd332446158b1a
         * SHA1     : a299912f3dc7cf0023aef8e4361abfc03e9a8c30
        tspkg :
         * Username : Gentil Kiwi
         * Domain   : vm-w7-ult-x
         * Password : waza1234/
```

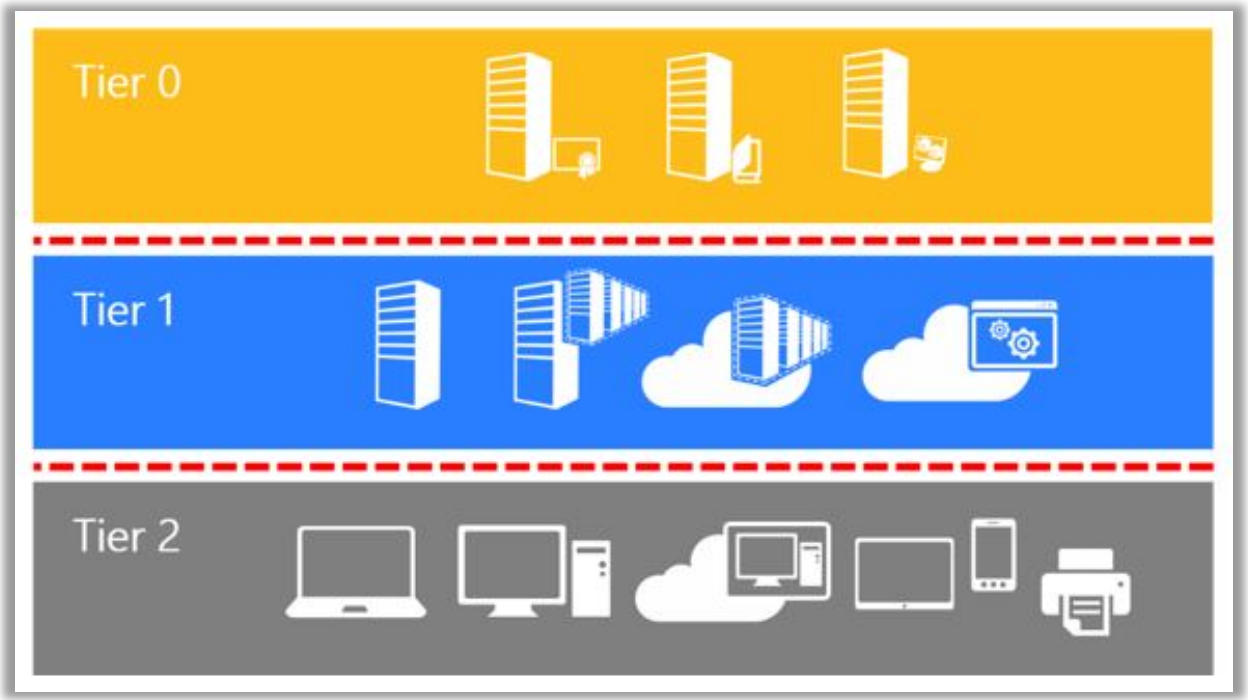
https://github.com/gentilkiwi/mimikatz

The problem - Credential and Identity theft

DEMO:

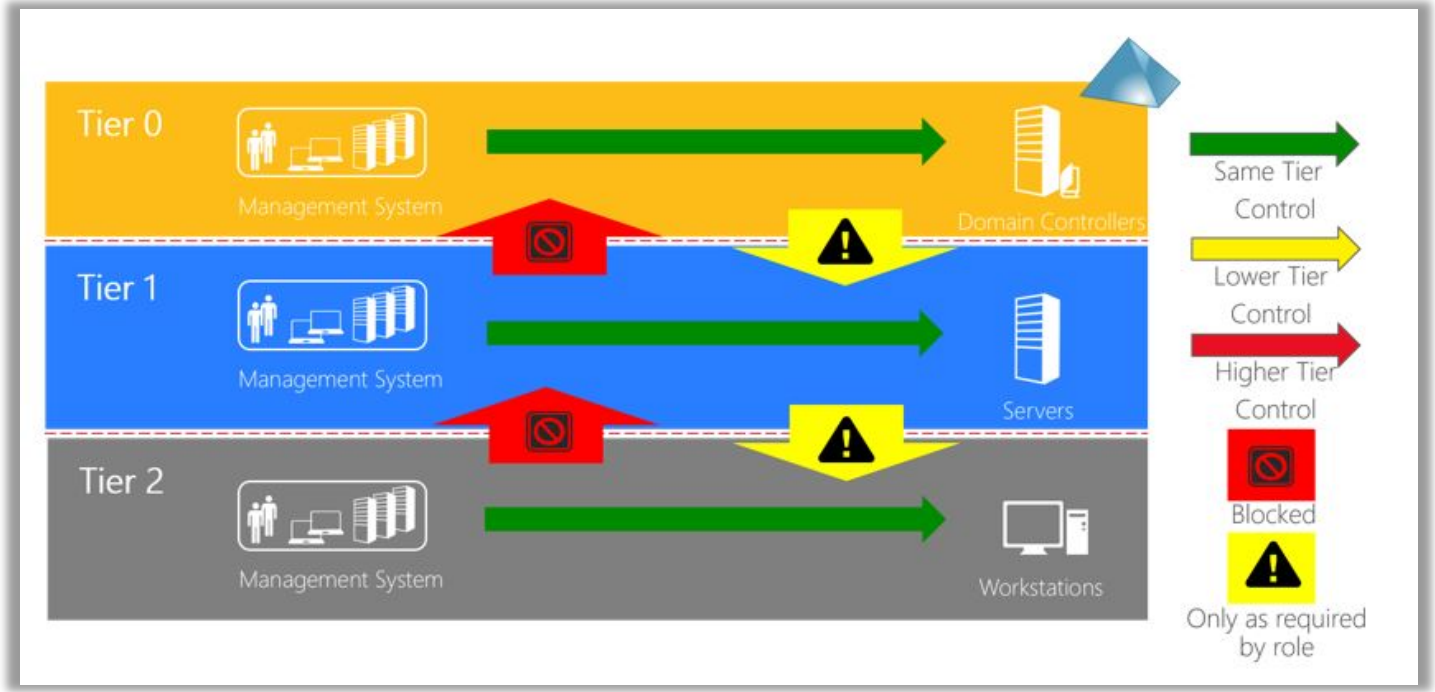
1) Stealing and using credentials
2) Hijacking an identity

Active Directory Tiering Model



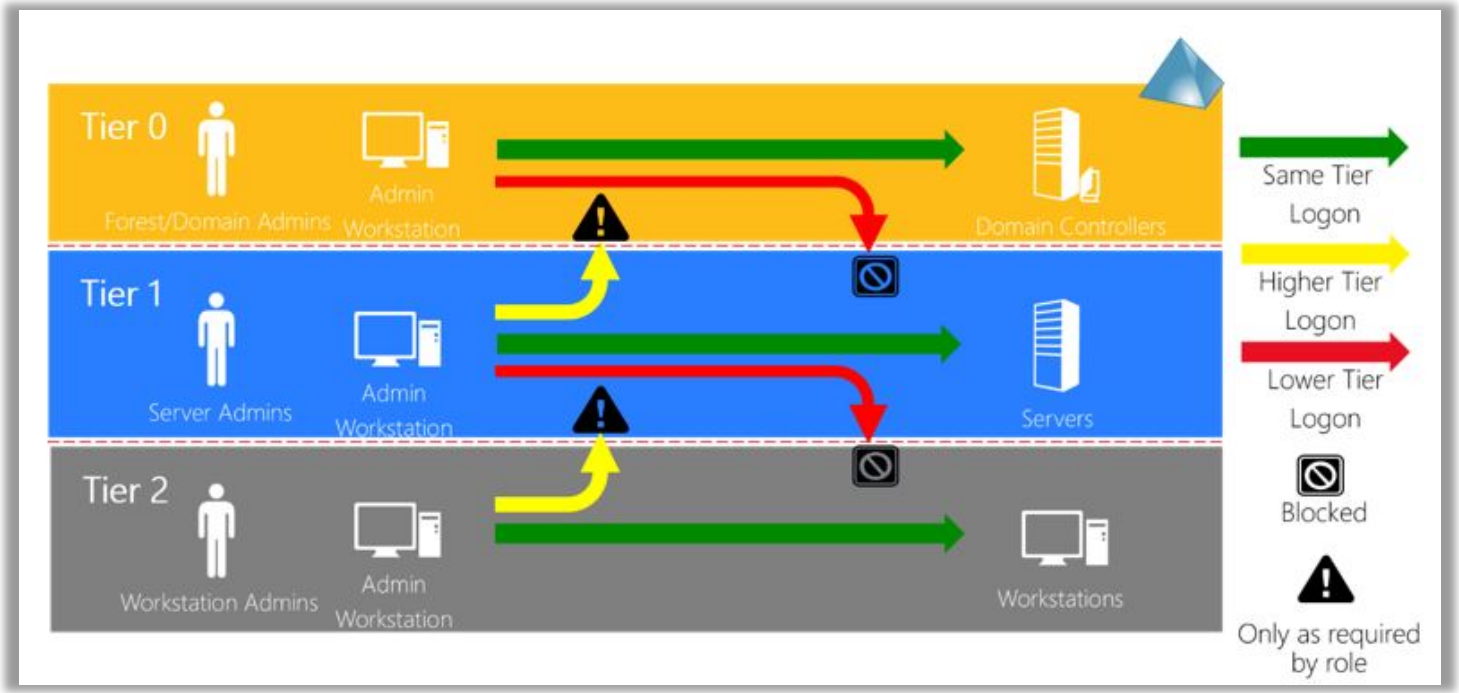
https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Active Directory Tiering Model



https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Active Directory Tiering Model



https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Active Directory Tiering Model

Some of the requirements for the model to be effective:

+ Servers are AD joined
+ Administrative users are members of Protected Users
+ LAPS is deployed across the entire environment
+ Effective patch management is in place
+ Workstation/Server hardening is applied

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Active Directory Tiering Model

The least privilege:

- Limit the count of administrators or members of privileged groups (minimum 2 though!)
- Delegate fewer privileges to accounts
- Provide time-bound privileges on demand

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Active Directory Tiering Model



Tier 0	Tier 1	Tier 2	Standard
			Administrator Enablement, Accountability, and Lifecycle Enforcement
●	●	●	Administrative personnel standards
●	●	●	Administrative security briefing and accountability
●	●	●	Provisioning and de-provisioning processes for administrative accounts
			Operationalize Least Privilege
●	●	●	Limit count of administrators
▲	▲	▲	Dynamically assign privileges
			Manage Risk of Credential Exposure
●	●	●	Separate administrative accounts
●	●	●	Administrator logon practices
●	●	●	Use of approved support technology and methods
●	●	●	No browsing the public internet with admin accounts or from admin workstations
●	●	●	No accessing email with admin accounts or from admin workstations
●	●	●	Store service and application account passwords in a secure location.
			Strong Authentication
●	▲	▲	Enforce smartcard multi-factor authentication for all admin accounts
●	▲	▲	Enforce multi-factor authentication for all cloud admin accounts
			Rare Use / Emergency Procedures
●	N/A	N/A	Correctly follow established processes for all emergency access accounts
●	N/A	N/A	Restrict and monitor usage of emergency access accounts
●	N/A	N/A	Temporarily assign Enterprise Admin and Schema Admin membership

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Using Privileged Users

	Allowed remote login	Physical server login	Forbidden login
Tier 0	Remote tools that use network logons (type 3). RDP Session (preferably with Remote Credentials Guard) from an admin workstation with domain account.	No specific administrative tool usage restrictions.	
Tier 1	Remote tools that use network logons (type 3). Use RDP with Remote Credentials Guard from an admin workstation. Log on to the server by using a local account password that is set by LAPS from an admin workstation.	Retrieve the local account password set by LAPS from an admin workstation before logging on to the server.	Standard RDP may not be used with a domain account. Using the domain account credentials while in the session (for example, using RunAs). Logging on with a domain account is not allowed in this scenario on a physical server.
Tier 2	Remote Assistance, Skype for Business, or similar user-screen sharing may be used for assistance. Use RDP with Remote Credentials Guard from an admin workstation with a domain account. Retrieve a local account password set by LAPS from an admin workstation before connecting to user workstation.	Retrieve the local account password set by LAPS from an admin workstation before connecting to user workstation.	Logging on with domain account administrative credentials is not allowed. Use of standard RDP with a domain account.

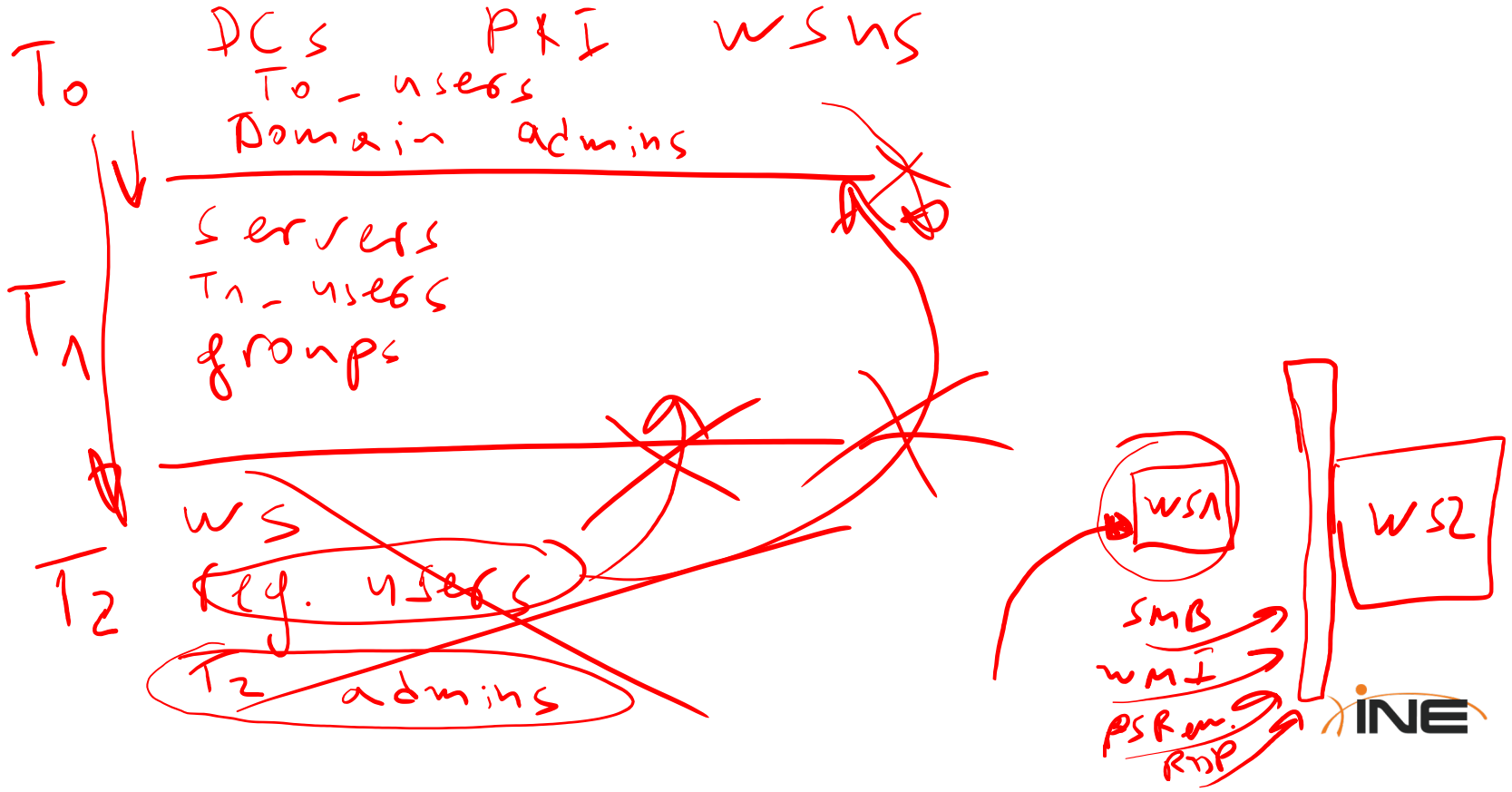
https://www.parpulev.com/2019/02/securing-windows-environments.html

Active Directory Tiering

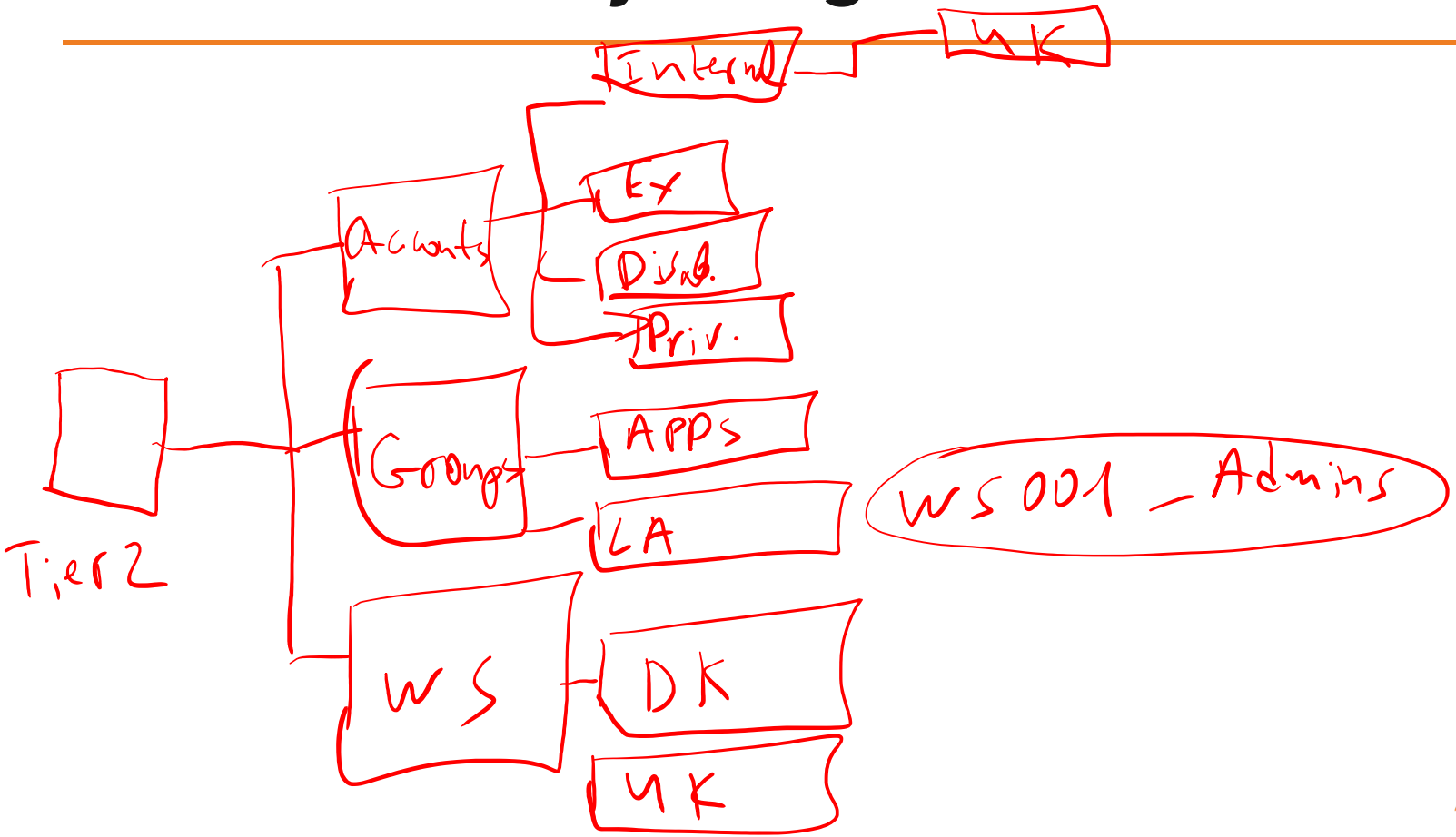
Part 2 - Implementation



Active Directory Design and Protection



Active Directory Design and Protection



Active Directory Tiering

DEMO showcasing technical tiering



Privileged Access Workstation



Privileged Access Workstation

- The Problem – Privileged Credentials on Untrusted Devices
- Privileged Access Workstation (PAW)
- DEMO

The Problem



- Risk to managed assets if an attacker gains control of a user workstation where sensitive credentials are used

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

Privileged Access Workstation

- Dedicated workstation for administrative tasks
- It is a security hardened, feature and functionality locked-down
- Protection from phishing attacks and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations
https://improsec.com/tech-blog/paw

Privileged Access Workstation

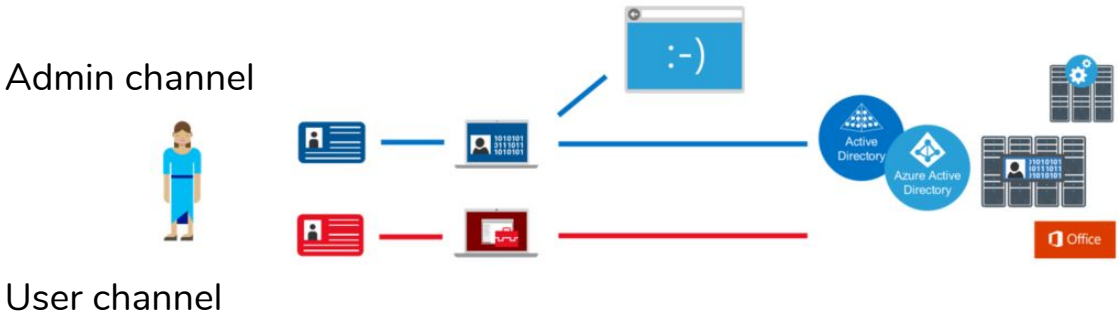
- PAW creates a trusted workstation environment that can be used by one or more accounts
- Account to workstation mapping is not required

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

Privileged Access Workstation

PAW Implementation:

- Separate physical machine
- Same machine with virtualization (host is PAW)
- Alternatives …



https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

Privileged Access Workstation

PAW hardening (some of the actions):

- LAPS
- Strict Host Firewall
- Bitlocker
- Credential Guard
- Windows Defender Application Control
- Custom User Right Assignments

Privileged Access Workstation

DEMO



Passwords & Password Policies



Passwords & Password Policies

- Passwords
- Password Policies
- Fine-Grained Password Policies
- DEMO
- Auditing passwords with Get-bADpassword
- DEMO

Passwords

TOP 10 passwords of 2020:

- 123456
- 123456789
- qwerty
- password
- 1234567
- 12345678
- 12345
- iloveyou
- 111111
- 123123

https://www.wtoc.com/2020/05/07/national-password-day-how-make-your-accounts-safer/

Passwords

- **Weak Password** – 123456, password, admin, secret
- **Complex but Weak Password** – Password1, Winter2020
- **Strong Password** – DailyCoffee4EarlYbirdz
- We want to prevent users from having the ability to set and/or use Weak passwords

https://www.wtoc.com/2020/05/07/national-password-day-how-make-your-accounts-safer/

Password Policies

Why are we talking about "policies"?

- Regular users
- Administrative Accounts
- Service Accounts
- VIP Accounts

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	180 days
Minimum password age	1 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	180 days
Minimum password age	1 days
Minimum password length	20 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

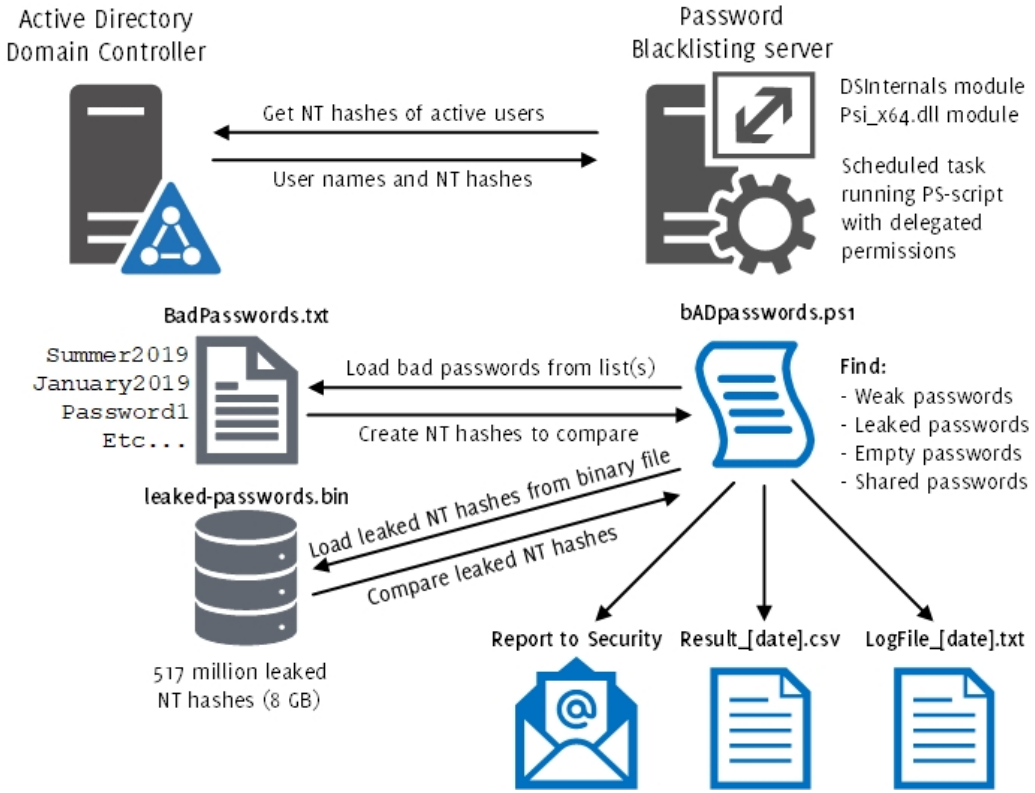
Fine-Grained Password Policies

Fine-Grained Password Policies

- Allows for multiple password policies in the same domain
- Can only be applied to global security groups
- Let’s go and create a Fine-Grained Password Policy for Administrators - DEMO

Auditing Passwords

Get-bADpassword



https://github.com/improsec/Get-bADpasswords

Auditing Passwords

DEMO Get-bADPassword



Protected Users



Protected Users

- The “Protected Users” group
- Demo showcasing a problem/feature

The “Protected Users” group

“*… designed as part of a strategy to manage credential exposure within the enterprise. Members of this group automatically have non-configurable protections applied to their accounts.*” - Microsoft

https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

The “Protected Users” group

- Originally for Windows Domains 2012R2 but backported to 2008R2 and 2012.
- In 2008R2/2012 only partial protection is provided.
- The protection is divided into host protection and domain protection.

https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

The “Protected Users” group

HOST PROTECTION:

- Credential delegation (CredSSP) will not cache the user's plain text credentials.
- With Windows 8.1 and Windows Server 2012 R2, Windows Digest will not cache the user's plain text credentials.
- NTLM will not cache the user's plain text credentials or NT one-way function.

https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

The “Protected Users” group

HOST PROTECTION (continued):

- Kerberos will no longer create DES or RC4 keys.
- A cached verifier is not created at sign-in or unlock, so offline sign-in is no longer supported.

https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

The “Protected Users” group

Domain Protection prohibits members to:

- Authenticate with NTLM authentication.
- Use DES or RC4 encryption types in Kerberos pre-authentication.
- Be delegated with unconstrained or constrained delegation.
- Renew the Kerberos TGTs beyond the initial four-hour lifetime.

https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

The “Protected Users” group

DEMO (showcasing the problems)



Device Hardening & MDfI



Device Hardening & MDfI

- Device Hardening
- Microsoft Defender for Identity (formerly Azure ATP)

Device Hardening

Device hardening is crucial.

- Limiting and disabling unused features reduces the attack surface towards the devices.
- Limiting access and placing network boundaries prevents lateral movement.
- Disk encryption will prevent stolen devices or data on them from being accessed.
- Application Whitelisting to block execution of unwanted software.
- Log, Monitor and Alert on suspicious events.

Microsoft Defender for Identity

"cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization"

- Microsoft

https://docs.microsoft.com/en-us/defender-for-identity/what-is

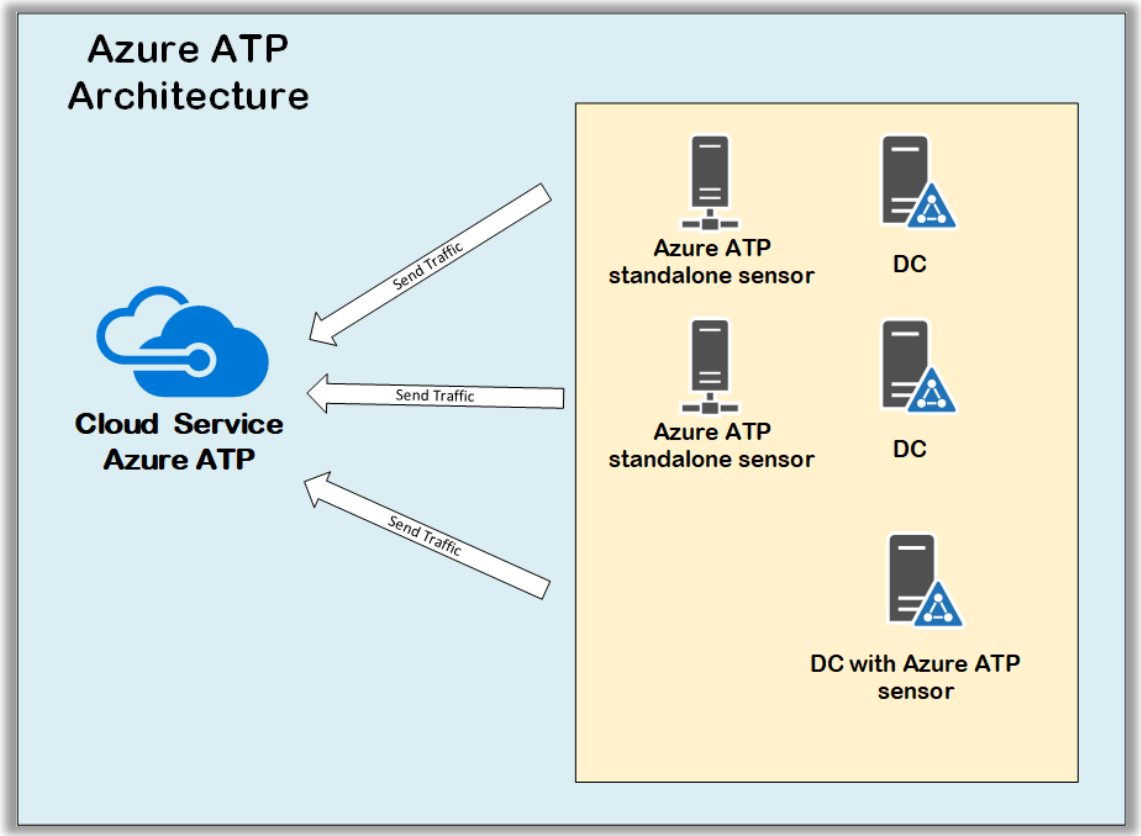
Microsoft Defender for Identity

- Monitor and profile user behavior and activities.
- Identify suspicious activities and advanced attacks across the cyber-attack kill-chain.

https://docs.microsoft.com/en-us/defender-for-identity/what-is

Microsoft Defender for Identity

Architecture



https://blog.ahasayen.com/azure-advanced-threat-protection-or-azure-atp/

Microsoft Defender for Identity

Review



Active Directory Tiering & Protection



Course Outline

- Common AD Attacks & Tools
- AD Tiering and Protection
  - AD Tiering
  - Privileged Access Workstation
  - Passwords and Password Policies
- Add-on tools and topics
  - Windows Defender for Identities