

Does Security Always Have to Be Expensive?

Security Quick Wins in the
Microsoft Windows Environment



Speaker Introduction



Enterprise and IT-Security

- 2016 – 2020 Bachelor
- 2020 – 2022 Master



- 2022 NVISO



Software Security
Assessment Team

Agenda

1. Some Facts and What Are Quick Wins?
2. Quick Wins
3. Tools
4. Conclusion

Some Facts and What Are Quick Wins?



QW#01: Notepad as Default Editor



Prevention:

◆ Unintentional execution of malicious scripts

→ .js, .wsh, .vbs, .sct, .wsf, .shs, .shb, .hta, .cmd, .bat, .cab, .ps1 ...

QW#02: Strong Password Policy

**Set min.
password length**

12

**Require
Complexity**

A-Z, a-z, 0-9,
+ # - , . ? \ _ ! § \$ % & ...

**Prohibit most likely
words / patterns**

Name of:

- Person
- Product
- Organization

Dissimilarity

Significantly
different from
your previous
passwords

[1]



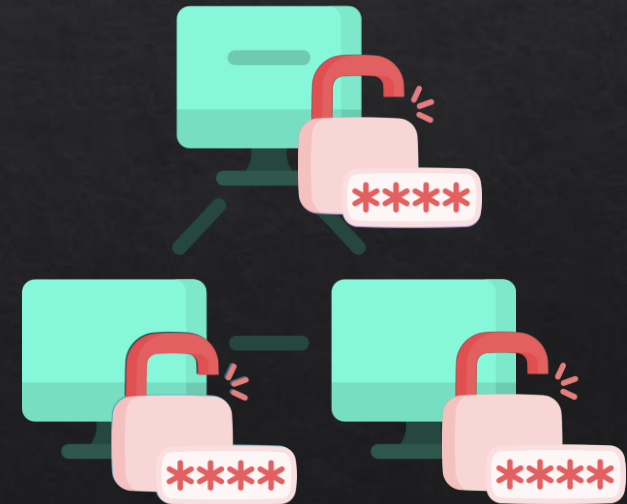
Prevention:

- ◇ Easy guessable passwords
- ◇ Password based attacks such as brute-force or dictionary attacks
- ◇ Credential stuffing
- ◇ Password spraying

QW#03: Use LAPS

Local Administrator Password Solution (LAPS) is a Windows feature that automatically manages and backs up the password of all local administrator accounts in a domain [\[2\]](#)

Without LAPS



Prevention:

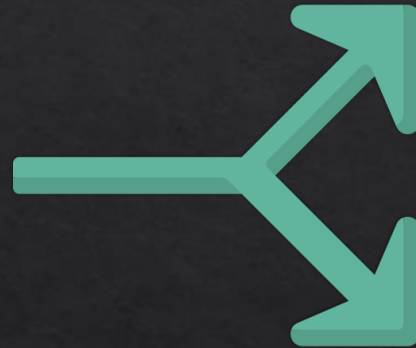
- ◆ Lateral-traversal attacks

QW#04: Account Separation

Administrator



Michel



Username: michel



Username: michel_adm



Prevention:

- ◆ It is more difficult to compromise highly privileged accounts

QW#05: Get Rid of Stored Credentials & Open Shares



- ◇ Description fields of AD accounts
- ◇ Text files, Excel sheets, or Word documents locally
- ◇ Scripts & config files (mostly on network shares)



Prevention:

- ◇ Lateral-traversal and privilege escalation attacks

QW#X06: ms-DS-MachineAccountQuota = 0

AD user attribute, that defines the number of machine accounts that a user is allowed to create in a domain [3]

ms-DS-MachineAccountQuota =

0

Recommended
Value

~~10~~

Default Value

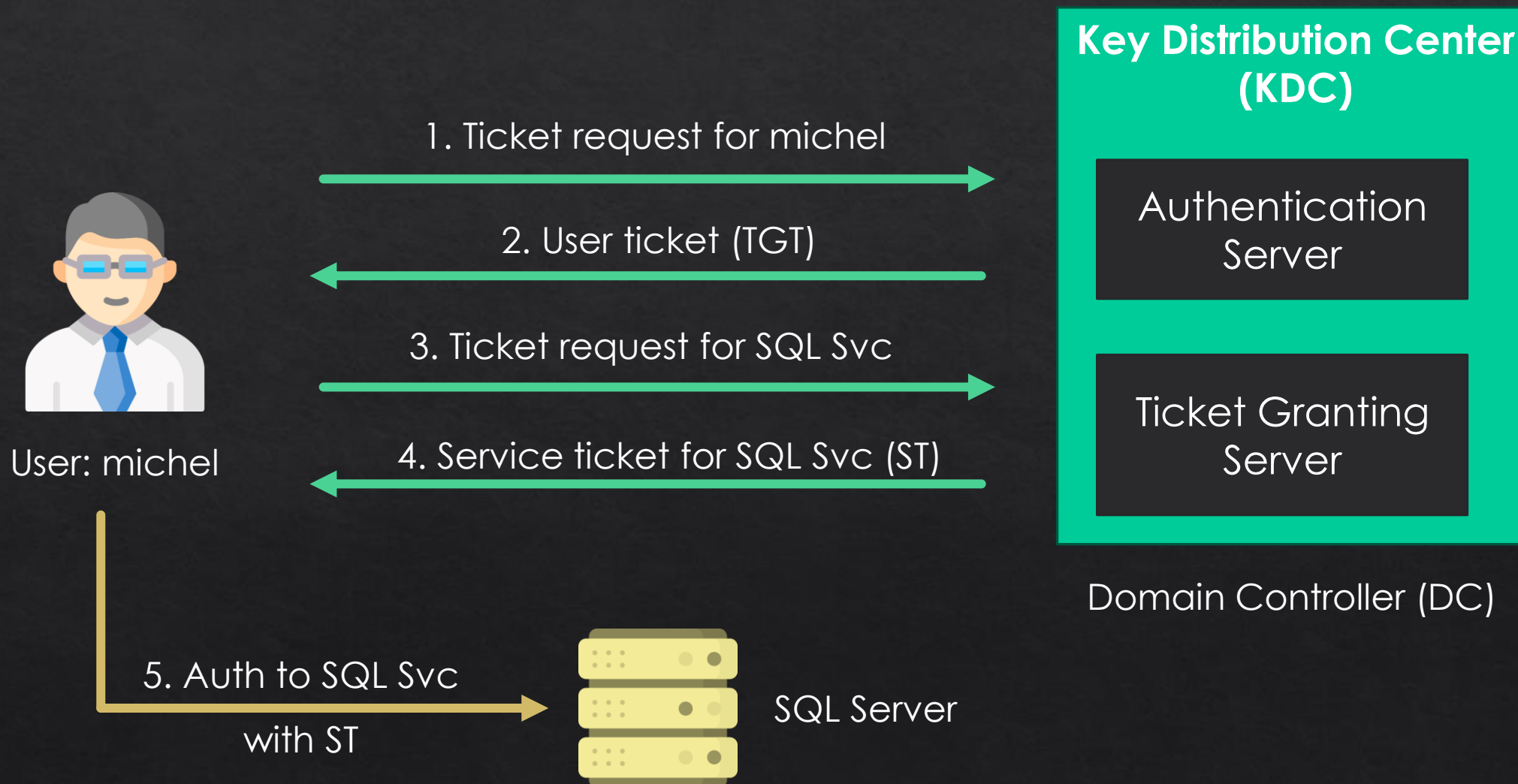


Prevention:

- ◆ Shadow IT
- ◆ Attacks such as noPack or Resource-Based Constrained Delegation



Kerberos Authentication



QW#07: DoesNotRequirePreAuth = False

AD user attribute, that indicates whether Kerberos pre-authentication is required to logon [4]

Settings
Account option



Do not require Kerberos preauthentication



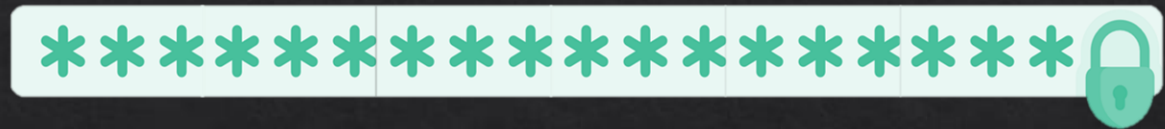
Prevention:

◆ AS-REPRoasting

QW#08: Audit Service Accounts

Service accounts are elevated authorized accounts used by applications, services, or processes to perform specific functions within an IT environment [\[5\]](#)

SA passwords: long & complex



periodically changed



Prevention:

- ◆ Kerberoasting

QW#09: Disable RC4 Encryption Type

RC4 is an insecure encryption type used to encrypt Kerberos tickets [\[6\]](#)

RC4
encryption
key



User's NT hash
(part of the
NTLM hash)



~~RC4 and DES~~
AES or other strong
encryption



Prevention:

- ◆ Fast offline password brute force (AS-REP Roasting & Kerberoasting)

QW#10: KRBTGT Password Change

The KRBTGT account is a local default account that acts as a service account for the KDC service.^[7]

Change of KRBTGT password:



Times



Min. 10 h waiting period



~ Every 180 days

[8]



Prevention:

- ◆ Compromised AD by Golden Ticket attack

QW#11: Regular Use of Free Tools

- ◇ Finding strings / credentials:
 - ◇ SauronEye - <https://github.com/vivami/SauronEye>
 - ◇ PowerHuntShares <https://github.com/NetSPI/PowerHuntShares>
- ◇ Windows vulnerabilities & misconfigurations
 - ◇ winPEAS - <https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS>
 - ◇ Seatbelt - <https://github.com/GhostPack/Seatbelt>
 - ◇ PowerUp - <https://github.com/PowerShellEmpire/PowerTools/blob/master/PowerUp>
- ◇ Active Directory vulnerabilities & misconfigurations
 - ◇ BloodHound - <https://github.com/BloodHoundAD/BloodHound>
 - ◇ PingCastle - <https://www.pingcastle.com/>
 - ◇ PurpleKnight - <https://www.purple-knight.com/>
 - ◇ Group3r - <https://github.com/Group3r/Group3r>
 - ◇ Adalanche - <https://github.com/lkarlslund/Adalanche>
 - ◇ ADExplorer - <https://learn.microsoft.com/en-us/sysinternals/downloads/adexplor>
 - ◇ PowerView - <https://github.com/PowerShellEmpire/PowerTools/tree/master/PowerView>
 - ◇ Certify - <https://github.com/GhostPack/Certify>

Conclusion



References

All icons created by Freepik – <https://www.flaticon.com/authors/freepik>

[1] <https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb>

[2] <https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview>

[3] <https://learn.microsoft.com/en-us/windows/win32/adschema/a-ms-ds-machineaccountquota>

[4] <https://learn.microsoft.com/en-us/powershell/module/activedirectory/set-adaccountcontrol?view=windowsserver2022-ps>

[5] <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-service-accounts>

[6] <https://syfuhs.net/lessons-in-disabling-rc4-in-active-directory>

[7] <https://adsecurity.org/?p=483>

[8] <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-reset-the-krbtgt-password>

Q&A

