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

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

**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]
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

Prevention:
- Shadow IT
- Attacks such as noPack or Resource-Based Constrained Delegation
Kerberos Authentication

1. Ticket request for michel
2. User ticket (TGT)
3. Ticket request for SQL Svc
4. Service ticket for SQL Svc (ST)
5. Auth to SQL Svc with ST

Key Distribution Center (KDC)
- Authentication Server
- Ticket Granting Server

Domain Controller (DC)

User: michel

SQL Server
**QW#07: DoesNotRequirePreAuth = False**

**Settings**
Account option

- Do not require Kerberos preauthentication

**Prevention:**
- AS-REPROasting

AD user attribute, that indicates whether Kerberos pre-authentication is required to logon [4]
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. [51]

SA passwords:
- long & complex
- periodically changed

Prevention:
- Kerberoasting
RC4 is an insecure encryption type used to encrypt Kerberos tickets [6].

Prevention:

- Fast offline password brute force (AS-REP Roasting & Kerberoasting)
The KRBTGT account is a local default account that acts as a service account for the KDC service.

Change of KRBTGT password: Times
Min. 10 h waiting period
～ Every 180 days

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/master/PowerUp

- Active Directory vulnerabilities & misconfigurations
  - PingCastle - https://www.pingcastle.com/
  - PurpleKnight - https://www.purple-knight.com/
  - Group3r - https://github.com/Group3r/Group3r
  - Adalanche - https://github.com/lkarlslund/Adalanche
  - PowerView - https://github.com/PowerShellEmpire/PowerTools/tree/master/master/PowerView
  - Certify - https://github.com/GhostPack/Certify
Conclusion

QUICK WINS

invest
References

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


