

Windows Hardening

HOW HARD CAN IT BE?

Who are we



Mirjam Blumstein - @cyberminza

Research Assistant at ZHAW

Project work about hardening and group policies within the scope of her master studies

Michael Schneider - @ox6d69636b

Pentester at scip AG

Creator of HardeningKitty, a PowerShell script to audit and harden Windows Systems



Why Windows Hardening?

“DON'T CHANGE A RUNNING SYSTEM”

“EIGENVERANTWORTUNG”

Why Windows Hardening?

- Default settings of Windows are not secure
- Same configuration for machines and users
- Control your environment
- “Schrödinger’s Macros from the internet”
- Use features like Attack Surface Reduction (ASR)

The Microsoft Way

HOW TO CONFIGURE YOUR WINDOWS

How to harden a system?

- Active Directory => Group Policy Management
- Azure Active Directory => Microsoft Intune
- Standalone => Local Group Policies
- Standalone => Windows Settings?
- Third-Party Tools

Group Policies

- Group Policy Editor
- Machine and User settings
- Local: *%WindowsDir%\System32\GroupPolicy*
- AD: *SYSVOL\%Domainname%\Policies*
- Registry settings are stored in *Registry.pol*
- Additional settings like Advanced Audit Policy are in other formats like csv

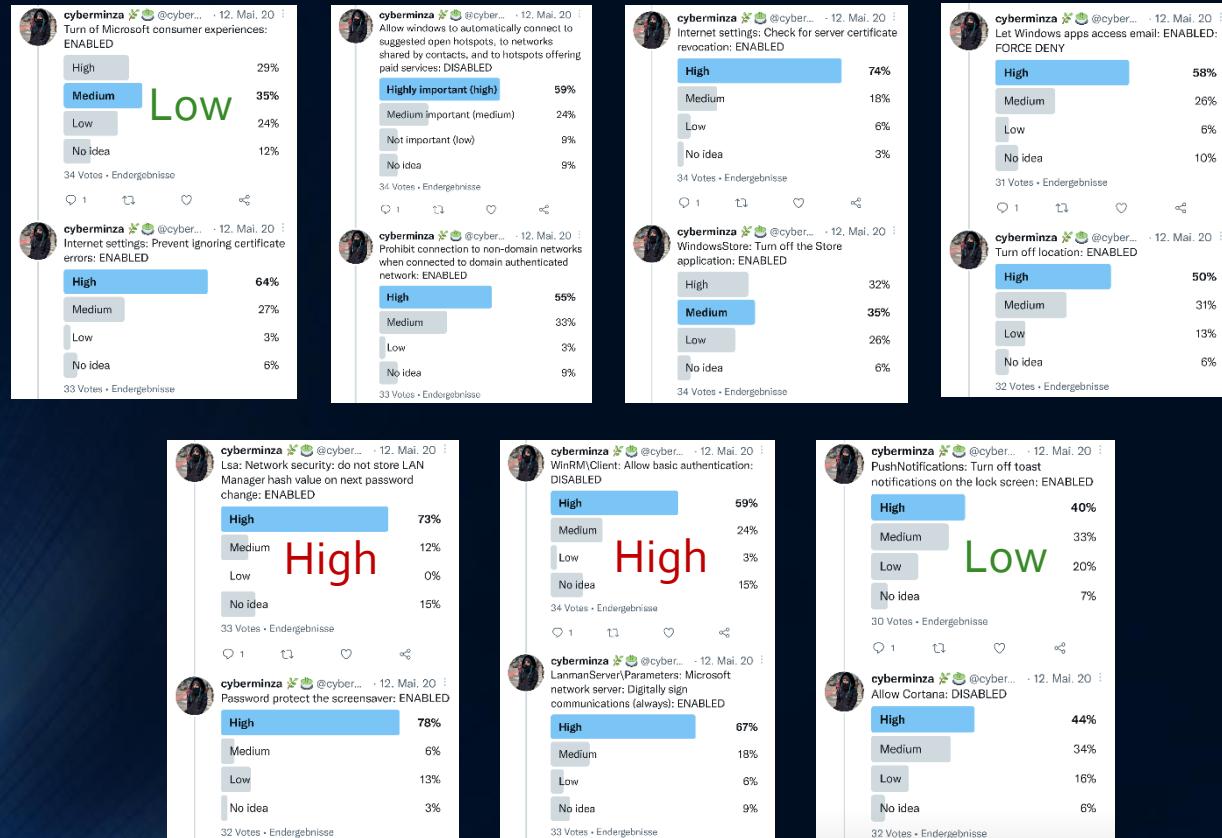
Guidelines and Benchmarks

COMPARISON OF GUIDELINES AND PRACTICES

Hardening Settings

- Which of these settings are necessary and what the impact of them?
- What is the correct *LAN Manager authentication level*?
- Should I turn on *PowerShell Script Block Logging*?
- How to enable *LSASS Protection Mode*?
- Can I disable RC4 encryption type for Kerberos?

Challenges with Classifying Settings



- Almost every setting was voted “high”
- DoD only voted two high, and even two as low
- Difficult to estimate the potential extent of damage, especially without context

Technical and Organizational Challenges

- How to configure the settings (securely)
- How can the security level/status within the GPOs be measured/audited?
- Hard for externals (consultants, auditors) to audit (report format from clients, what baseline to compare to)
- Mix between registry and non-registry settings
- Difficult to locate settings (especially without path information)
- Manual configuration consumes enormous amounts of time

Most Popular Guidelines

- CIS Benchmark
- Microsoft Security Baselines
- BSI SiSyPHuS
- DoD STIG

What Do They Offer?

	CIS	MS	BSI	DoD
Documentation	Very extensive	Extensive	Sufficient	Extensive
GPOs	Windows 7-11, Office, IE, Edge, Chrome	Windows 10/11, Office, IE, Edge	Windows 10	Windows 10/11, Office, IE, Edge, Chrome, Firefox, Adobe Acrobat
Levels	Yes	No	Yes	Yes
Language	English	English, ADMX files in different languages	German/English	English
Tool	Yes	Yes	No	No
Peculiarities	GPOs (build kits) and Tool not for free	PolicyAnalyzer can compare GPOs, they provide ps-scripts & further tools	Compared their own settings with MS and CIS	Severity classification, downloadable as csv, json, xml

Challenges with Guidelines


- Templates can contain hidden dependencies
- GPOs follow a hierarchy system and can overwrite each other
- Different Languages => problems with import/comparison
- Different recommendations (PowerShell Script Block Logging)
- Updates of guidelines

- Also, the challenge of measuring and audit still exists

Audit Your System

HOW TO ANALYSE AND AUDIT YOUR CONFIGURATION

Microsoft Baseline Security Analyzer (MBSA)

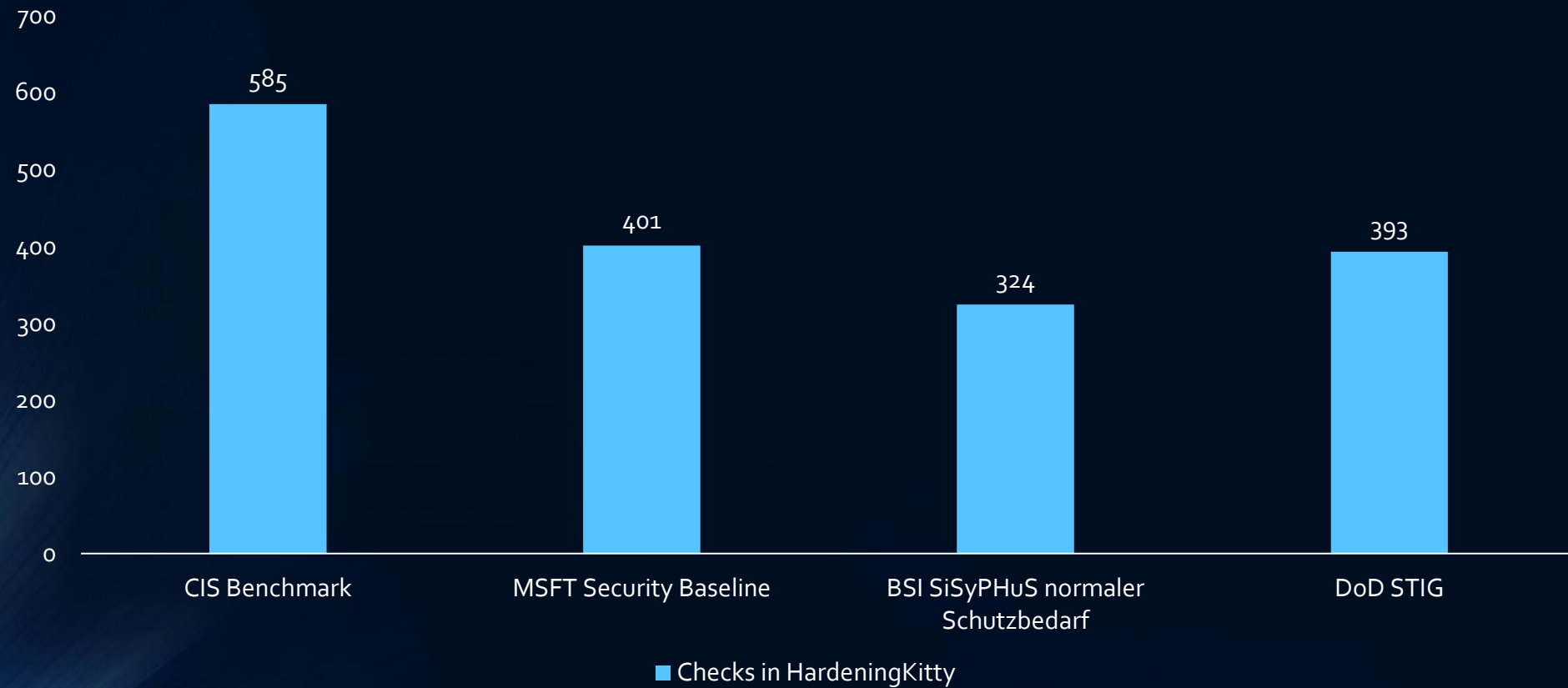


The screenshot displays the Microsoft Baseline Security Analyzer 2.3 interface. The main content area is titled "Windows Scan Results" and shows a section for "Administrative Vulnerabilities". A table lists several issues with their scores, descriptions, and links for further details.

Score	Issue	Result
✖	Local Account Password Test	Some user accounts (5 of 9) have blank or simple passwords, or could not be analyzed. What was scanned Result details How to correct this
✖	Autologon	Autologon is configured on this computer. What was scanned How to correct this
⚠	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, then the computer may be at risk until the computer is restarted. What was scanned How to correct this
⚠	Password Expiration	All user accounts (9) have non-expiring passwords. What was scanned Result details How to correct this
ℹ	Windows Firewall	Windows Firewall is disabled and has exceptions configured. What was scanned Result details How to correct this
✔	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned

At the bottom of the window, there are navigation buttons: "Print this report", "Copy to clipboard", "Previous security report", and "Next security report". An "OK" button is located in the bottom right corner.

Windows 10 Enterprise (Machine)



Microsoft Tools

- Get-GPOReport or gpresult => generates HTML or XML
- Policy Analyzer
- Local Group Policy Object Utility (LGPO.exe)
- Missing information like Advanced Audit Policies or User Rights Assignment

HardeningKitty

- Can I use only PowerShell? Nope
- accesschk supports only ANSI encoding => use secedit
- Administrators != Administratoren => Live SID translation
- auditpol and *Success/Failure* or *Erfolg/Fehler*
- Convert Benchmarks/Guidelines to HardeningKitty
- Client, server (member or domain controller), old and new systems

How Hard Is It?

SUMMARY OF CHALLENGES IN THE PROCESS

It Is Hard!

- Choose/build your own guideline
- Harden your systems and re-audit it
- Gather information about registry keys and strange formats (Registry.pol)
- Documentation of Microsoft Intune settings?

Thank you and see you in the discussion!