All about AD-Hardening *by*

TEMS SECURITY SERVICES GMBH

&

TEMS GMBH

PRESENTATION

Philip Berger
Managing Director

Stephan Emich
Senior Security Consultant

Michael Meixner, CISSP
Managing Director

tems security

Agenda

- Example Hacker-Script
- Dumping Domain Passwords
- Sample GPO`s
- GPO Setup / How it works
- GPO order
- GPO updates from console
- GPO Enforcement
- Create new Audit GPO-Policy
- Create new GPO-Policy from DoD
- CIS-Docs – Server / Workstation
- KRBTGT PW Reset
- DC Reboot
- Machine certificate (3 Days)

They call me 007

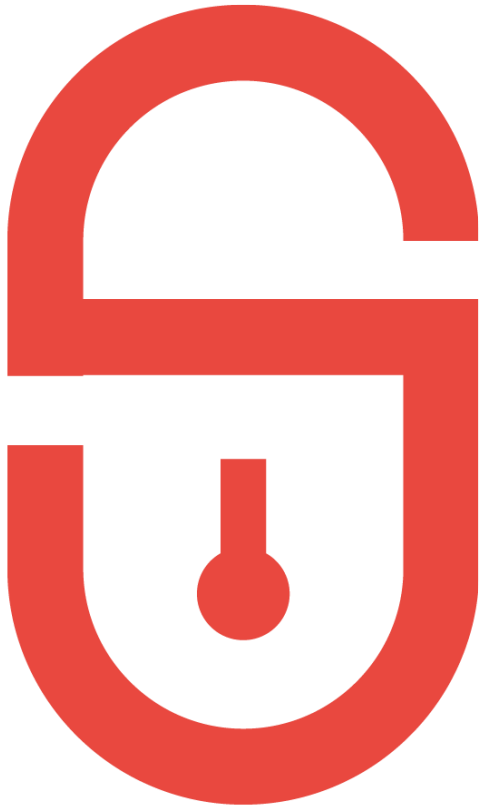
0 security budget

0 security engineers

7 breaches

Know your limits

Source: Internet



Two types of Hardening

- Secure & Harden Active Directory
- Configure Logging & Active Log-Management

The key risk and mitigation

- The hacker needs **only one vulnerability or instance of misconfiguration,** and the hacker has access to an organisation's network.
- An organisation can catch the hacker by detecting **command and control or lateral movement** within the network.

Knowledge and skills acquired through training and practice are the key

Why should we harden our Active Directory?

- Because, by default it isn’t secure
- Only Basic logging is enabled per default
- Because we have a clear IT-Security focus in our job
- Implement clever Honeypot systems
- and we are the good ones
- Implement JEA
- because we know it

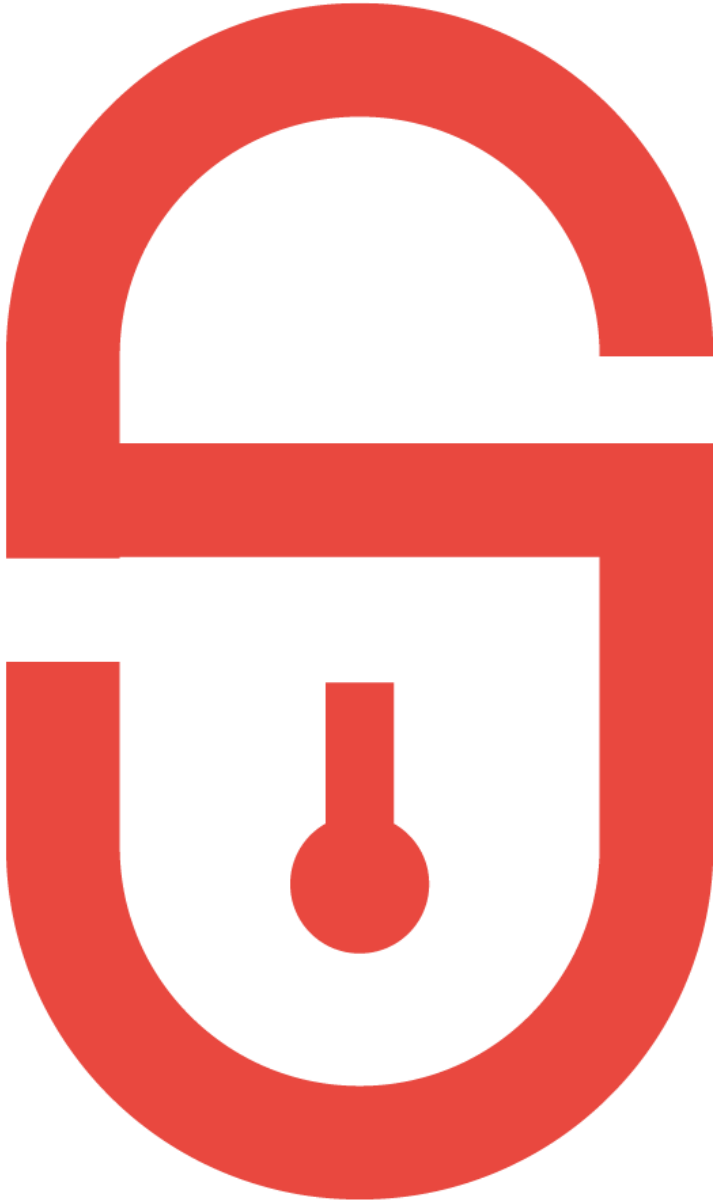
Reducing the Active Directory Attack Surface to a minimum

tems security

Dumping Domain Password Hashes

- ✓ Mimikatz
- ✓ Empire
- ✓ Nishang
- ✓ PowerSploit
- ✓ Invoke-DCSync
- ✓ **Ntdsutil**
- ✓ DiskShadow
- ✓ WMI – Volume Shadow copy
- ✓ Memorydump
- ✓ Pass the Hash
- ✓ vssadmin
- ✓ vssown
- ✓ Metasploit
- ✓ fgdump
- ✓ **Offline NTDS modification**
- ✓ adXtract (script)
- ✓ Hiberfil.sys
- ✓ DC Shadow
- ✓ Procdump
- ✓ Windows Credential Manager

tems security



Sample Hacker script

During a cyber forensic investigation in the Summer of 2022, we found a hacker script we want to share today.

C:\Users\
Meixner\OneDrive -

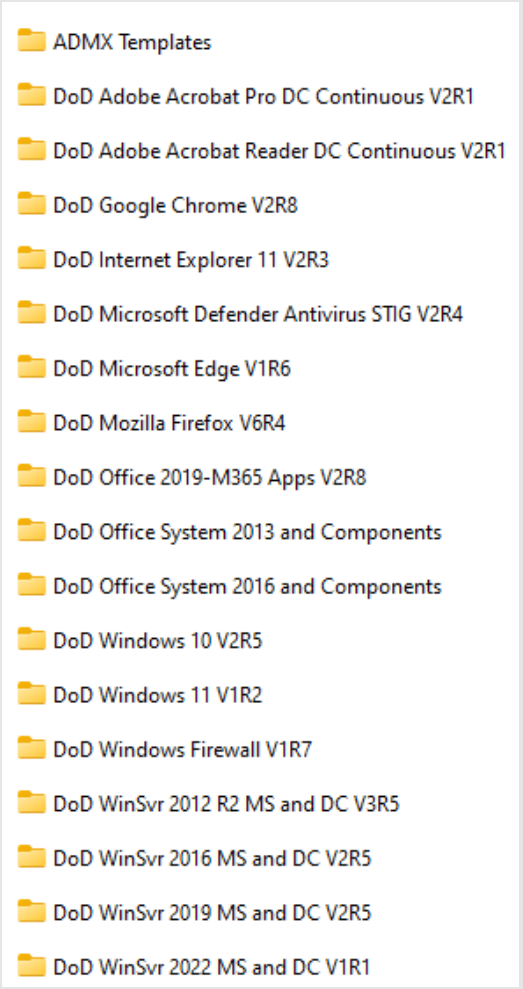
Recommended sources 1/2

temS security

We recommend the following sources for MS-Active Directory Security

DoD CYBER EXCHANGE PUBLIC

https://public.cyber.mil/stigs/gpo/



Recommended sources 2/2

tems security

We recommend the following sources for MS-Active Directory Security

CIS Center for Internet Security®
Creating Confidence in the Connected World.

[CIS WorkBench / Benchmarks (cisecurity.org)]

Benchmarks

The listing below displays all the benchmarks you currently have access to.

Search | Status: All | Filter

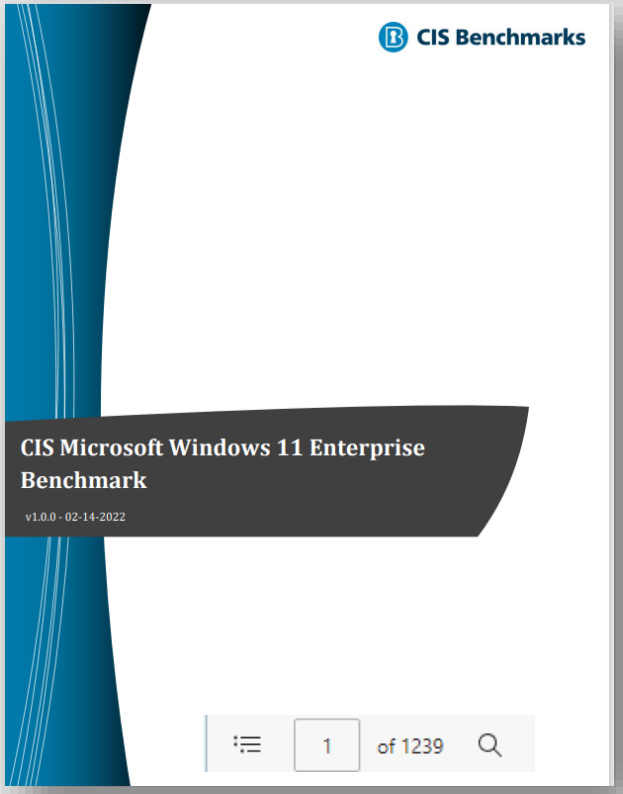
All 865

Benchmarks

The listing below displays all the benchmarks you currently have access to.

Search: microsoft | Status: Published | Filter | clear

All 202



Live AD Hardening by Stephan

Basics

GPO Setup / How it works

GPO order

GPO updates from console

GPO Enforcement

Create new Audit GPO-Policy

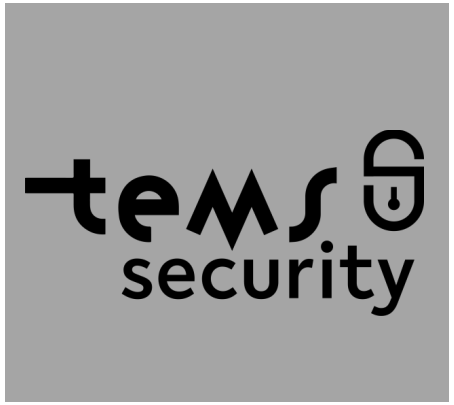
Create new GPO-Policy from DoD

Implementation

Good practice to start

Implement and test GPOs

Testing testing testing



Log Monitoring

Windows Event Forwarding

- Just configure
- Good for a POC
- A lot of manual work
- Good scripting know-how required

SIEM mit Kibana

- Free for on-prem use
- A lot of IT-Sec know-how within the system
- Implement within days

elastic

tems security

Some other things to take care of

LAPS

Credential Guard

Sysvol Shares

Auto Install scripts – write access

Auto install scripts – password

Active Directory Attributes

Next On-Site Meeting April 19th

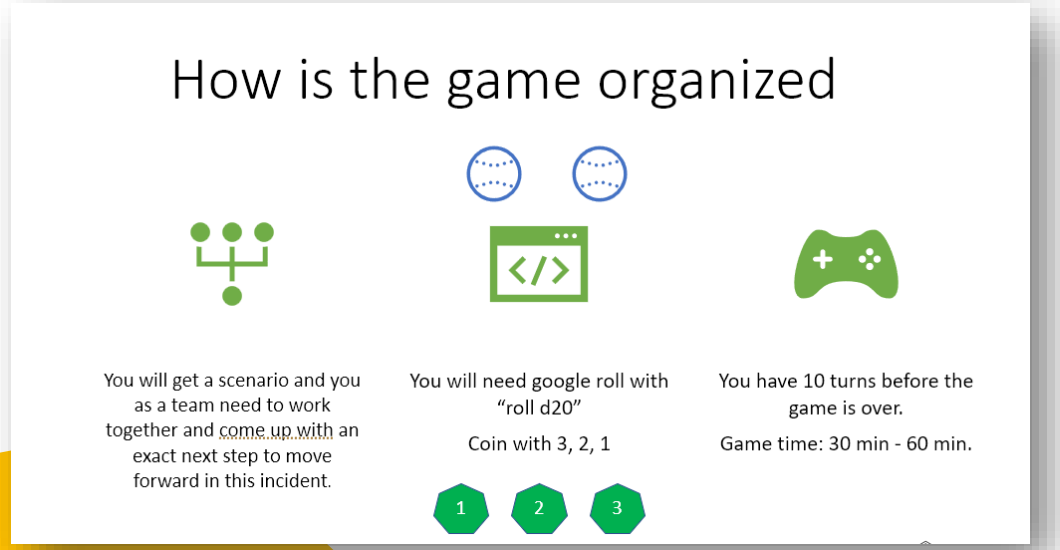
We plan an on-site event at ADMIRAL Sportbar with our Partner Elastic® in the 2nd District on April 19th 2023, from 09:00am to lunchtime.

TOPIC: Threat Hunting with Kibana

A: Yes I will join on-site

B: No, I prefer to join online

tems security



Special Incident Response online Event

TOPIC: Incident Response tabletop game

We will host an Incident Response tabletop game.

With a group of max. eight persons, we hold a one hour online IR game with you.

Please contact us if you're interested:

IR-tablegame@tems-security.at

Get in contact with us

Philip Berger
Managing Director
+43(664) 343 8644
Philip.berger@tems-security.at

Michael Meixner, CISSP
Managing Director
+43(664) 1453328
Michael.meixner@tems-security.at

tems security