Fra default til default sikker

Bjørn Henninen

Sicra®

Root# Whoami

Bjørn Henninen

- Sikkerhetsarkitekt Sicra
- Samler av sertifiseringer: CISSP, GXPN, GCIH, GCFE, GCAD, Azure
- Opptatt av proaktiv sikkerhet såkalt reformert pentester
- Tidligere Incident Response
- Ruller terninger

Sicra®

Agenda

1. Logging og Log policy
2. Usikre Nettverkstjenester
3. Tilgjengelige verktøy og teknologier
4. Verifisering med verktøy
5. Diverse

Ha en plan

Sicra®

Logging og log policy

Hva logges og hvor logges det

- PowerShell
- Nye administratorer
- Passord endring på administratorer
- Innmelding I privilegerte grupper
- Nettverkslogg og brannmurlogg

- Sysmon ?

ArcticWolf minimum ad-log

https://docs.arcticwolf.com/bundle/m_active_directory/page/configure_an_arctic_wolf_gpo_advanced_audit_policy.html

Account Logon	Audit Credential Validation	Success and Failure
Account Logon	Audit Kerberos Authentication Service	Success and Failure
Account Logon	Audit Kerberos Service Ticket Operations	Success and Failure
Account Logon	Audit Other Account Logon Events	Success and Failure
Account Management	Audit Computer Account Management	Success and Failure
Account Management	Audit Other Account Management Events	Success and Failure
Account Management	Audit Security Group Management	Success and Failure
Account Management	Audit User Account Management	Success and Failure
Detailed Tracking	Audit DPAPI Activity	Success
Detailed Tracking	Audit Process Creation	Success
Detailed Tracking	Audit Process Termination	Success
Detailed Tracking	Audit Token Right Adjusted	Success
DS Access	Audit Directory Service Access	Success
DS Access	Audit Directory Service Changes	Success
Logon/Logoff	Audit Account Lockout	Success and Failure
Logon/Logoff	Audit Logoff	Success and Failure
Logon/Logoff	Audit Logon	Success and Failure
Logon/Logoff	Audit Network Policy Server	Success and Failure
Logon/Logoff	Audit Other Logon/Logoff Events	Success and Failure
Logon/Logoff	Audit Special Logon	Success and Failure
Object Access	Audit Detailed File Share	Success and Failure

Sicra®

Usikre nettverks tjenester

Netbios
NTLM
SMB Uten Signering
LDAP uten signering og channel binding
Kerberos (Utdatert kryptering rc4/des

NetBios

NTLM

Hovedsaklig hvordan finne ut om man har NTLM v1 og hvordan man blir kvitt det

Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

Network security: LAN Manager authentication level → Send NTLMv2 response only. Refuse LM & NTLM

Set-ItemProperty -Path "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" -Name "LmCompatibilityLevel" -Value 5

itor

lelp

Policy	Security Setting
Network access: Restrict clients allowed to make remote calls to SAM	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Classic - local users auth...
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client encryption requirements	Negotiate sealing
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined

SMB signering

- Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

- Microsoft network client: Digitally sign communications (always) → Enabled
- Microsoft network client: Digitally sign communications (if server agrees) → Enabled
- Microsoft network server: Digitally sign communications (always) → Enabled
- Microsoft network server: Digitally sign communications (if client agrees) → Enabled

LDAP signering og channel binding

Se etter eventid 2889 i Directory Service Log for usignerte LDAP bindinger
Bruk 2887 for å se hvor ofte det brukes

Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

EnabledDomain controller: LDAP server signing requirements → Require signing

På domene controller

```
New-ItemProperty -Path
"HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters" `
  -Name "LDAPEnforceChannelBinding" -Value 2 -PropertyType DWORD -Force
```

Sicra®

Kerberos sikring

Monitorering (Event IDs 4768, 4769, 4770, 4771, 4776).
Sjekk for bruk av des og rc4 og blokker
Roter KRBTGT passordet regelmessig (to ganger)

Bruk verktøyene som er tilgjengelige

- Protected users group
- Group Managed Service Accounts
- LAPS
- Microsoft ASR regler

Protected users group

Krav Server 2012 R2

- Legger bare brukere til i gruppen protected users

Tvinger kerberos uten rc4 eller des

- Forhindrer delegering
- Kerberos ticketen er 4 timer
- Forhindrer cached credentials

Group Managed Service Accounts

Automatisk passord mangement
Tvungen kerberos
Bedre sporbarhet

Group Managed Service Accounts

```
# Step 1: Initialize the KDS Root Key (once per forest)
Add-KdsRootKey -EffectiveImmediately
# Step 2: Create a Security Group for Member Servers
# This group will contain all servers allowed to retrieve the gMSA password.
New-ADGroup -Name "gMSA_MemberServers" -GroupScope Global -Path "CN=Users,DC=yourdomain,DC=com"
# Add member servers to the group (replace with actual server names)
Add-ADGroupMember -Identity "gMSA_MemberServers" -Members "Server01$", "Server02$"
# Step 3: Create the gMSA Account
# Replace 'yourdomain.com' with your actual domain name.
New-ADServiceAccount -Name "MyServiceAccount" -DNSHostName "yourdomain.com" `
  -PrincipalsAllowedToRetrieveManagedPassword "gMSA_MemberServers"
# Step 4: Install the gMSA on Member Servers
# Run this on each server that will use the gMSA.
Install-ADServiceAccount -Identity "MyServiceAccount"
# Step 5: Verify Installation
Test-ADServiceAccount -Identity "MyServiceAccount"
```

LAPS

Microsoft ASR regler

```
Set-MpPreference -AttackSurfaceReductionRules_Ids @(
    "D4F940AB-401B-4EFC-AADC-AD5F3C50688A",  # Block executable content from email and webmail
    "3B576869-A4EC-4529-8536-B80A7769E899",  # Use advanced protection against ransomware
    "75668C1F-73B5-4CF0-BB93-3ECF5CB7CC84",  # Block credential stealing from LSASS
    "DCB9C6F1-4C2E-4C44-AF96-4F6C5D8D2C2D",  # Block executable files from running unless they meet aprevalence, age,
or trusted list criteria
    "D3E037E1-3EB8-44C8-A917-57927947596D",  # Block credential stealing from web browsers
    "5BEB7EFE-FD9A-4556-801D-275E5FFC04CC",  # Block Office applications from creating child processes
    "3E37E320-7E43-4E8F-8E73-7D8E4B8C5D6E",  # Block Office applications from injecting code into other processes
    "26190899-1602-49E8-8B27-EB1D0A1CE869",  # Block JavaScript or VBScript from launching downloadedexecutable content
    "9E6B2F53-2FBC-4F6B-84D0-1B38E738F4FB",  # Block Win32 API calls from Office macros
    "B2B3F03D-6A65-4F7B-A9C7-1C7EF74A9BA4",  # Block untrusted and unsigned processes that run from USB
    "C1DB55AB-C21A-4637-BB3F-A12568109D35",  # Block process creations originating from PSExec and WMIcommands
    "E6DB77E5-3DF2-4CF1-B95A-636979351EDE",  # Block persistence through WMI event subscription
    "D1E49AAC-8F56-4280-B9BA-993A6D77406C"   # Block Office communication application from creating childprocesses
) -AttackSurfaceReductionRules_Actions Enabled
```

Verfisering

- Audit verktøy: Pingcastle og Purple Knight,
- Maester: https://maester.dev/
- Locksmith, ADCS https://github.com/jakehildreth/Locksmith
- ADeleginator, https://github.com/techspence/ADeleginator
- ScriptSentry (Feil i logon scripts) https://github.com/techspence/ScriptSentry
- Bloodhound angreps paths https://github.com/SpecterOps/BloodHound

Diverse

- PAW
- MachineAccountQuata
- Description
- dSHeuristics
- Azure

PAW

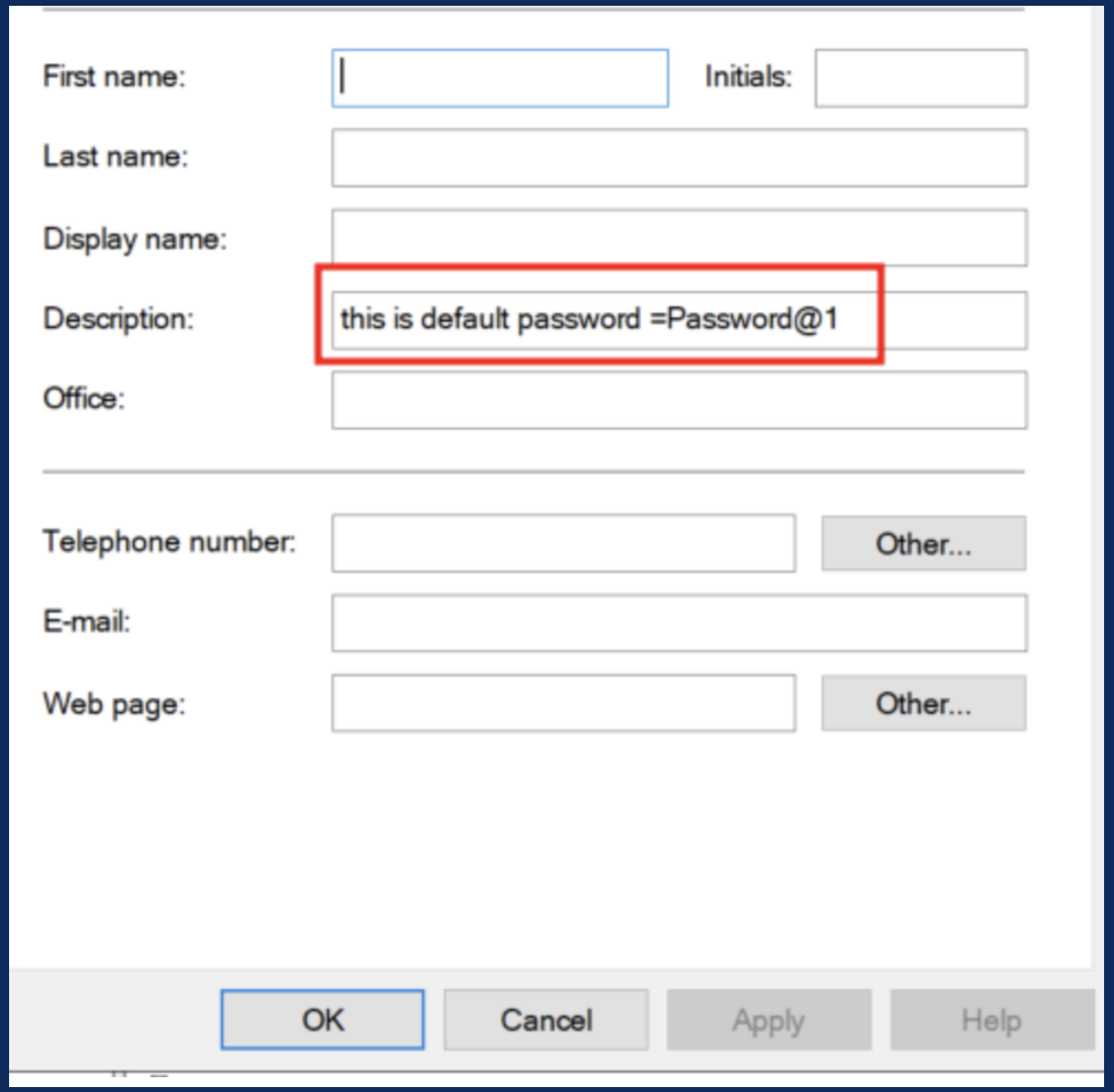
Sicra®

MachineAccountQuota

```
Get-ADDomain | Select-Object -Property Name, DistinguishedName,
MachineAccountQuota

Set-ADDomain -Identity "Domene.no" -Replace
@{MachineAccountQuota=0}
```

Description i ad er public



dSHeuristics

000000000100000001

3 → Begrenser annonyme tilganger
9 → Begrenser lesing av sensitive grupper
12 → Begrenser lesing av sensitive attributer
18 → Delegering av linking av forign kontoer.

Azure

- Gjestekontoer kan invitere gjestekontoer
- Oppretting av subscriptions
- Teams , kan sende og motta meldinger fra eksterne
- Token protection
- Password protection
- Continuous access evaluation

Takk for meg

https://www.linkedin.com/in/henninen/
bjorn@sicra.no

Sicra®