KOVERT

Slik gjør du jobben min vanskeligere

- et hjertesukk fra en pentester

KiNS-tech 20.09.22

Litt om meg

- 28 år
- CEO/Pentester i Kovert AS
  - SOC/Utvikler/Pentester i BDO CERT
  - SecOps konsulent Syscom

- B.Sc Programmering NITH
- M.Sc Information Security NTNU Gjøvik

- Spilt på landslaget i hacking
- “Norgesmester i Cybersikkerhet” på et tidspunkt

- Twitter: @Mrtn9, og **add meg gjerne på LinkedIn**

1. Hva gjør jobben min lett?
2. Hvorfor vil jeg at du skal gjøre den vanskeligere?
3. Hvordan kan du gjøre den vanskeligere?

1 Hva...

KOVERT

2 Hvorfor...

Hvorfor vil jeg at dere skal gjøre jobben min vanskeligere?

1. Det er teit at dere skal kaste bort penger på sikkerhetstest, når vi finner ting dere kunne funnet selv

2. Sjansen for at man ser seg blind på de “lette” svakhetene og ikke ser de mer komplekse sårbarhetene som eksisterer i nettverket

3. Det utfordrer oss ikke til å innovere, være kreative eller flytte grenser

3

Hvordan...

KOVERT

Filshare

Filshare

Det finnes nesten alltid noe på filshare som ikke burde vært der!

- Backups av VMer
- IT-avdelingens rotemappe
- Passord.xlsx
- OneNote
- Citrix hjemmemapper 😍
- SYSVOL

Filshare - tips & tricks #1

Skrivbare filer i SYSVOL er alltid spennende.

Hvem vet, kanskje de blir kjørt av noe(n)?

```
Legg til dette i .bat-filen du er usikker på:

echo %date%-%computername%-%username% >> kovert.txt
```

Filshare - tips & tricks #2

Ta en “rusken”-øvelse i de interne filsharene før pentesterne kommer på besøk!

https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

```
Find-DomainShare -CheckShareAccess

Find all domain shares in the current domain that the current user has
read access to.
```

Passordgjetting

“Old but gold”
Finnes et utall måter å gjette passord på

- AD
- OWA
- O365
- Lync
- Random tjenester med AD-integrasjon

Funker fordi det ALLTID er noen med <årstid><årstall> som passord…

Passordgjetting - tips #1

Ikke passORD 😠

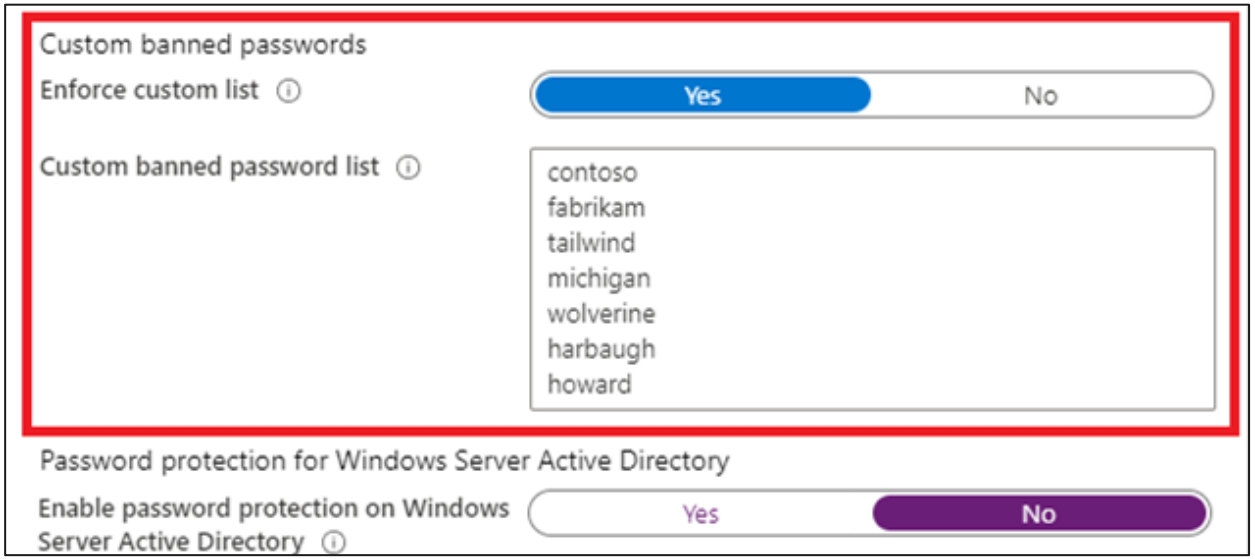
passSETNINGER 😍

Vær snill med brukerne deres, ikke tving de til å bytte passord hele tiden!

Men selvsagt, er det spor av at brukeren har blitt kompromittert….

Passordgjetting - tips #2

[Password protection in Azure Active Directory | Microsoft Docs]
[Deploy on-premises Azure AD Password Protection | Microsoft Docs]



Passordgjetting - tips #2.5 DYI-edition

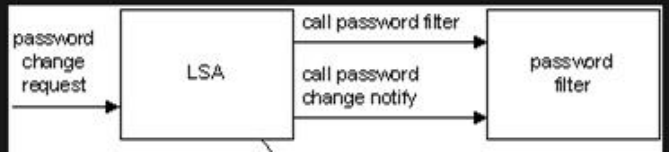
https://learn.microsoft.com/en-us/windows/win32/secmgmt/password-filters

Password Filters

Article • 01/07/2021 • 2 minutes to read • 5 contributors

Password filters provide a way for you to implement password policy and change notification.

When a password change request is made, the *Local Security Authority* (LSA) calls the password filters registered on the system. Each password filter is called twice: first to validate the new password and then, after all filters have validated the new password, to notify the filters that the change has been made. The following illustration shows this process.



Passordgjetting - tips #3

DERE HAR FASITEN!

- Volume Shadow Copy
- secretsdump.py
- ntdsutil.exe
- Invoke-NinjaCopy

+

hashcat

Hvordan VI knekker passordhasher 👍

Kerberoasting

Servicekontoer i AD med servicePrincipalName satt

(Alt for) ofte del av privilegierte grupper

Alle domenebrukere kan slå opp hvem disse er, og forespørre en “Ticket-Granting-Service (TGS) Ticket” som kan knekkes for å finne frem til passordet til servicekontoen.

(Gitt RC4_HMAC_MD5)

Kerberoasting - tips #1

- TGS Tickets er relativt tunge å knekke
- Jo lengre og vanskeligere passord, jo mindre sannsynlig at man klarer å knekke dem
- Skru av RC4 encryption type for Kerberos (PS: Dette brekker antageligvis stuff)

Kerberoasting - tips #2

Group Managed Service Accounts (gMSA) eller Standalone Managed Service Accounts (sMSA)

https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/service-accounts-on-premises

Kerberoasting - tips #3

Snakk med leverandørene deres, og få de til å innse at hvis de trenger en servicekonto med Enterprise Admin for at programmet dems skal fungere....

Kerberoasting - tips #3

Snakk med leverandørene deres, og få de til å innse at hvis de trenger en servicekonto med Enterprise Admin for at programmet dems skal fungere….

Så er programmet dems søppel.

Machine in the Middle

- LLMNR
- NetBIOS
- WPAD
- IPv6

- Responder
  - https://github.com/lgandx/Responder
- Inveigh
  - https://github.com/Kevin-Robertson/Inveigh

Machine in the Middle - tips #1 part 1

- Skru på SMB signing:
  - https://www.rootusers.com/configure-smb-signing-via-group-policy/
- Skru av LLMNR:
  - https://www.blackhillsinfosec.com/how-to-disable-llmnr-why-you-want-to/
- Skru av NetBIOS:
  - http://woshub.com/how-to-disable-netbios-over-tcpip-and-llmnr-using-gpo/

Machine in the Middle - tips #1 part 2

- LDAP channel binding:
  - Use the LdapEnforceChannelBinding registry entry to make LDAP authentication over SSL/TLS more secure
- Skru av WPAD via GPO
  - Hvis i bruk: manuelt spesifiser path til WPAD config, ikke autoconfig
- Gi IPv4 presedens over IPv6
  - Configure IPv6 for advanced users - Windows Server | Microsoft Docs

Active Directory Certificate Services

Fordi hvem har vel ikke lyst til å bygge sin egen PKI?

Tilbyr:

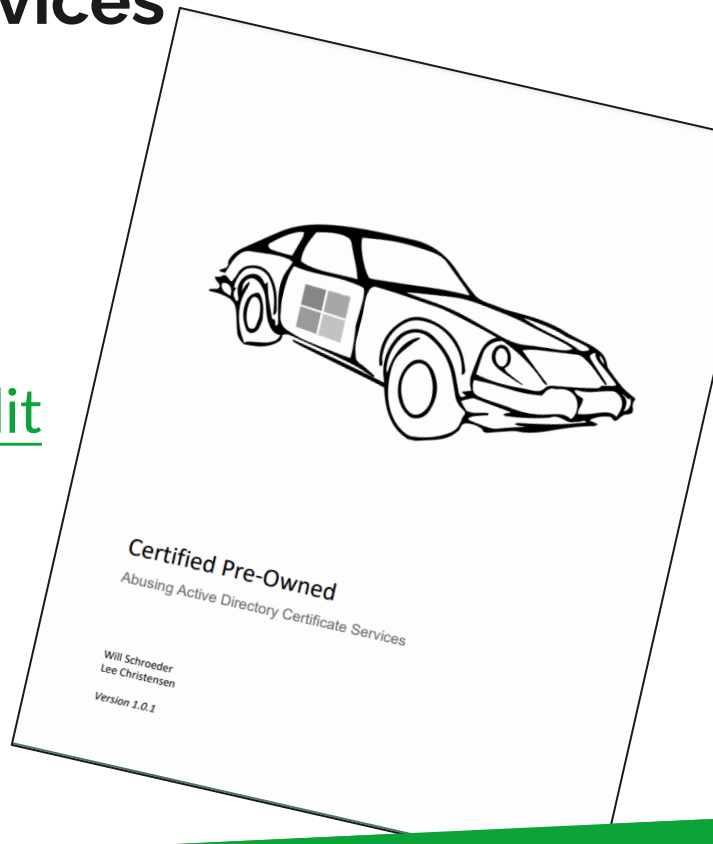
- kryptering (eg filsystem)
- Digitale signaturer (kodesignering)
- Autentisering (mot AD)

Active Directory Certificate Services

[Certified Pre-Owned Whitepaper]

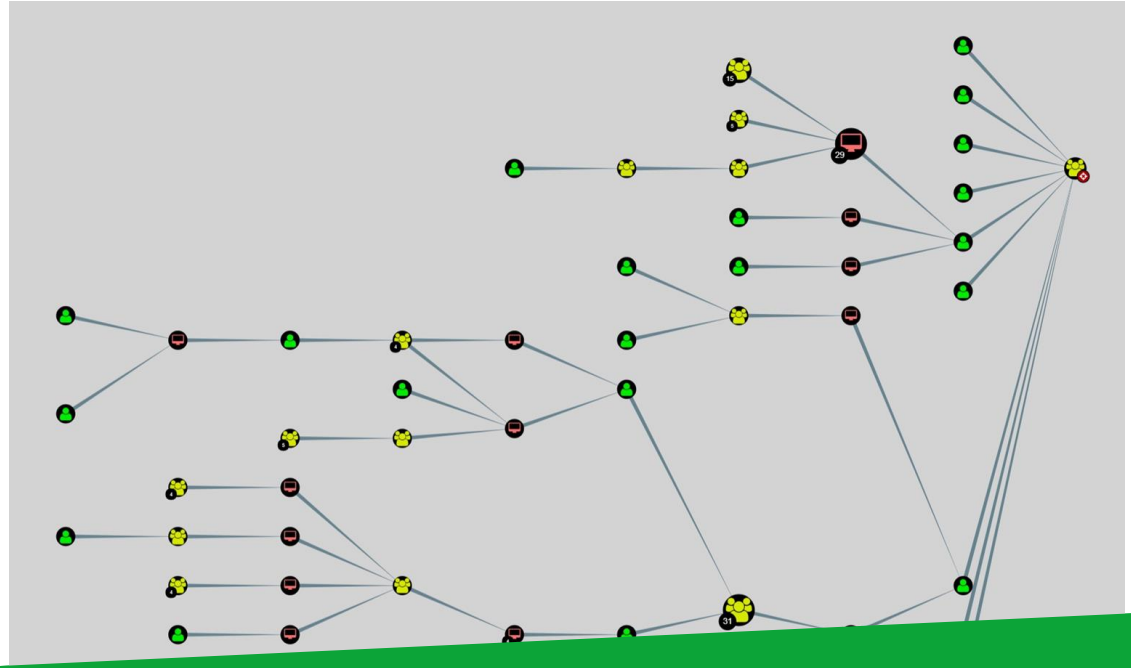
https://github.com/GhostPack/PSPKIAudit

https://github.com/GhostPack/Certify



Do It Yourself!

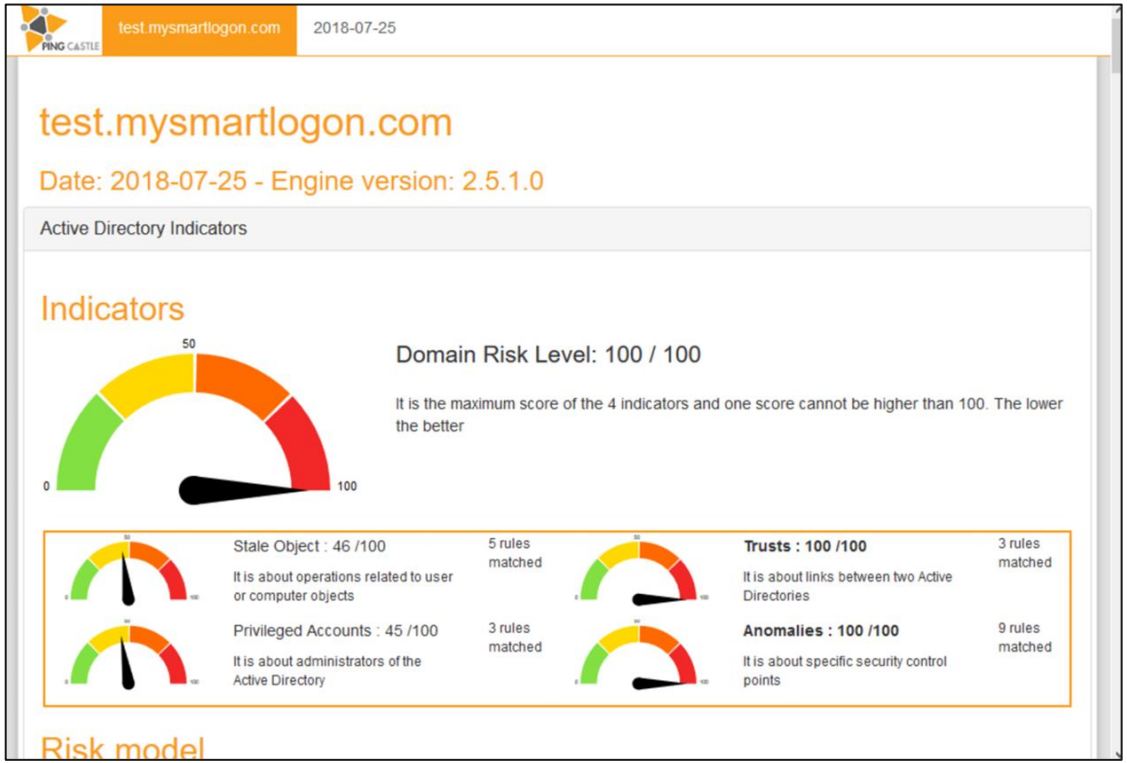
https://github.com/BloodHoundAD/BloodHound



Do It Yourself!

https://www.pingcastle.com

"With the default license, the binary program can be **run for free,** as long as you do not derive any revenue from it. **For example, any for-profit organizations can use it to audit their own systems.**"



Do It Yourself!

- Kjøp og kjør Nessus Professional selv.
- 50% på Black Friday salg hvert eneste år!
  - 17 742,-

Takeaways

- Gjør disse tingene før dere kjøper pentest
- Spør konkret om hvilke verktøy og metoder som testerne benyttet for å finne sårbarheter
    - Repliser og valider deres egen fiks
- Offensive verktøy er også defensive verktøy!

ASSUME BREACH

RED TEAM OG
ADVERSARY SIMULATION

PENETRASJONSTESTING

HARDWARE/IOT

WEBAPPLIKASJONER

MOBILAPPLIKASJONER

ATTACK SURFACE MANAGEMENT
AND
ALWAYS-ON PENETRATION
TESTING

E-post:
martin.ingesen@kovert.no

Telefon:
99 12 50 88

Nettside:
https://kovert.no

KOVERT