Active Directory Hardening

Turning Your Forest into a Jungle

Colin F. Tortoise – IKT-rådgiver

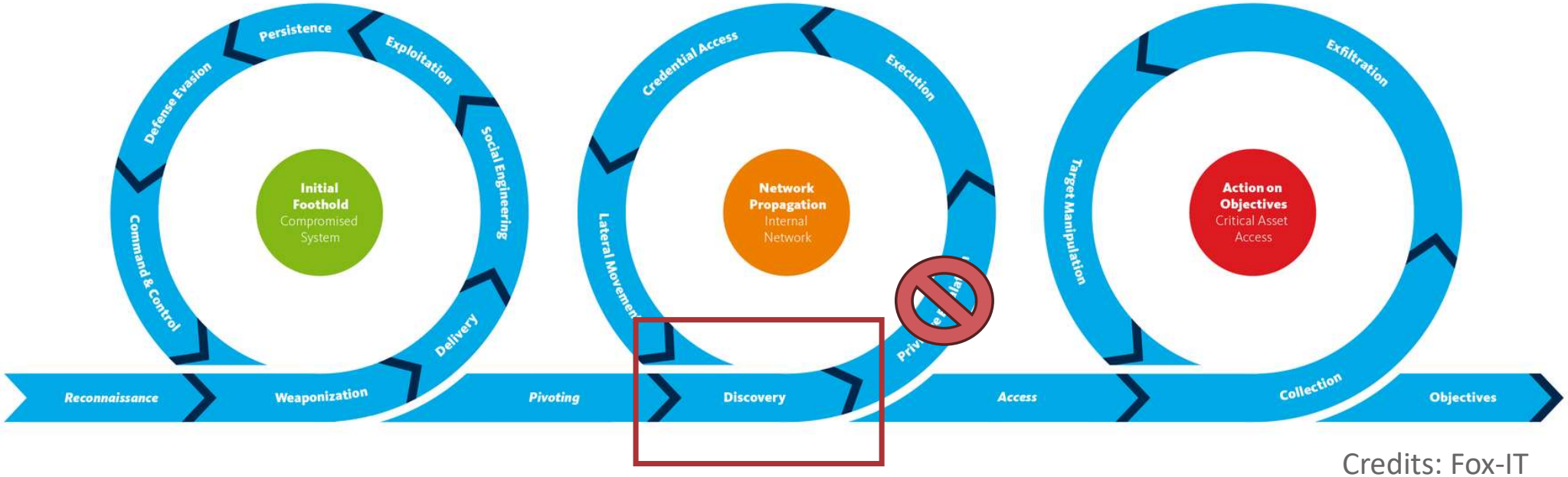
HORTEN
KOMMUNE

Intro

- Litt om meg
- Living off the land & purple team mindset
- Bakgrunn for sikkerhetsarbeidet
- Viktigheten av AD
- Tekniske write-ups: https://github.com/ActualTortoise/AD-Forest2Jungle

HORTEN
KOMMUNE

Cyber Kill Chain

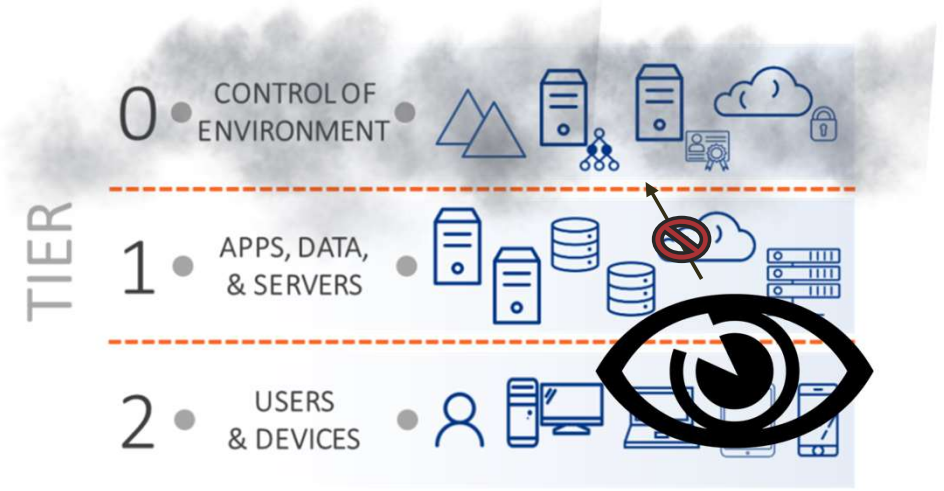


Credits: Fox-IT

HORTEN
KOMMUNE

AdminSDHolder Obfuskering

- Litt om AdminSDHolder
- SDProp
- Utnytte AdminSDHolder for å beskytte AD-miljøet.
- Er det egentlig behov for at Tier 2 og Tier 1 objekter har muligheten å lese ut Tier 0 objekter?



Credits: Ravenwood Technology Group

HORTEN KOMMUNE

AdminSDHolder Obfuskering

- Hva får organisasjonen ut av det?
- Hvordan skal en angriper ta kontroll over et objekt de ikke engang er klar over er tilstede?
- De aller fleste automatiske verktøy blir ubrukelige *og* misvisende.
- Tvinge angriperen til å oppføre seg på en måte som gir deg en fordel.
- Delay, Delay, Delay (*og frustrere!)*

Credits: Ravenwood Technology Group

AdminSDHolder Obfuskering

Før:

```
PS C:[redacted]> Get-ADGroup -identity "Domain Admins"


DistinguishedName : CN=Domain Admins
GroupCategory     : Security
GroupScope        : Global
Name              : Domain Admins
ObjectClass       : group
ObjectGUID        : [redacted]
SamAccountName    : Domain Admins
SID               : [redacted]
```

Etter:

```
PS C:[redacted] Get-ADGroup -ider[redacted]
Get-ADGroup : Cannot find an object w[redacted]
At line:1 char:1
+ Get-ADGroup -identity "Domain Admins"
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (Domain Admins:ADGroup) [Get-ADGroup], ADIdentityNotFoundException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityNotFoundException,M
   icrosoft.ActiveDirectory.Management.Commands.GetADGroup
```

AdminSDHolder Obfuskering

Pentest Runde 2:

Pentester (Ekstern) 12:59

har dere gjort noe slik rare greier at brukere ikke får ut all info om andre i domenet?

13:00

Pentester (Ekstern) 13:00

bastards

HORTEN
KOMMUNE

AdminSDHolder Obfuskering

- Write-up:
  https://github.com/ActualTortoise/AD-Forest2Jungle/blob/main/AdminSDHolderObfuscation.md

- Forskningsartikkel – Guido Grillenmeier (Semperis):

  https://www.semperis.com/wp-content/uploads/resources-pdfs/resources-improving-ad-security-posture-adminsdholder.pdf

HORTEN
KOMMUNE

Auditing i Active Directory

- Litt om Auditing i AD
- Veldig lite som er slått på som standard.
- Det er for sent å begynne etter en hendelse har inntruffet!
- Hvilken objekter kan overvåkes?
- Vurder å ta en titt gjennom diagnostic event logging. (F.eks LDAP)

HORTEN
KOMMUNE

Auditing i Active Directory

- Kontinuerlig forbedring – gjennomgang av logger med utgangspunkt i pentestrapporter.
- Inferens – Avdekke uønsket oppførsel; f.eks password spraying, enumerering.
- Opprydning – Fjerne objekter som ikke er i bruk. Fjern rettigheter det ikke er behov for.
- Honeypots

Auditing i Active Directory

- Write-up: https://github.com/ActualTortoise/AD-Forest2Jungle/blob/main/AuditingInActiveDirectory.md
- Microsoft – Advanced Security Auditing https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/advanced-security-auditing-faq
- Microsoft – AD Diagnostic Logs https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/configure-ad-and-lds-event-logging

Honeypots

- Tenke som en angriper. Hva er neste steget når man ikke får ut domain admins?
- Undersøke de mest brukte enumereringsverktøyene. Hvilken objekter henter de ut fra domenet?
- Hva er målet til angriperen? Kan det være noen objekter som er direkte knyttet til dette målet?
- *Alle* objekter i domenet kan overvåkes!

HORTEN
KOMMUNE

Honeypots

- Noen eksempler:
- Det dukker opp 4625 (failed logon) 2-3 ganger mot en honeypot konto som ikke er i bruk. Tyder på passord spray!
- Det oppstår 4662 (access attempt, read) mot flere honeypot objekter i domenet innen et kort tidsrom. Dette tyder på bruk av enumereringsverktøy.

HORTEN
KOMMUNE

Honeypots

- AD auditing må være på plass for å benytte seg av honeypots i miljøet. SIEM er ikke nødvendig men *sterkt anbefalt*.

- Kreativitet er eneste begrensningen her – tenk som en angriper; del gjerne ideer!

- Write-up: https://github.com/ActualTortoise/AD-Forest2Jungle/blob/main/Honeypots.md

HORTEN
KOMMUNE

Intern pentesting mot AD

- Hva innebærer en intern pentest?
- Hva er vitsen, hva får organisasjonen ut av det?
- Måle forbedringer over tid.
- Noe man kan vise til for å få ekstra midler fra ledelsen.
- Reverse engineer oppførselen ut ifra telemetrien og lage alerts med høy sikkerhet.
- Tette hull og feilkonfigurasjoner før de blir utnyttet enten av angriper eller ekstern pentester.

HORTEN
KOMMUNE

Intern pentesting mot AD

- Vi anbefaler:
- PingCastle og PurpleKnight
  Sårbårheter/Feilkonfigurasjoner
- ForestDruid (eller BloodHound)
  Path to Tier0, utilsiktet tilganger
- hashcat
  Forsøk å cracke passordene dine!
- Snaffler
  SMB/Fileshare enumerering
- 110% gratis :)))

HORTEN
KOMMUNE

Intern pentesting mot AD

- Write-up: https://github.com/ActualTortoise/AD-Forest2Jungle/blob/main/In-HousePenetrationTestingInAD.md

HORTEN
KOMMUNE

Outro

- Herding av AD er et kontinuerlig arbeid, dessverre.
- Bare å begynne! Et eneste tiltak mye bedre enn ingen tiltak.
- Tekniske gjennomganger finner du på GitHub siden: https://github.com/ActualTortoise/AD-Forest2Jungle
- Bonus: Gjennomgang av AD-tiering
- Tar *gjerne* i mot tips av alle slag i form av honeypots /verktøy/sikkerhetstiltak.
- Spørsmål? Bare å spørre! Epostadressen kan fås etter ønske.

HORTEN
KOMMUNE