Sitzungsprotokoll

Projekt:	Readiness for Tailored Attacks and Lateral Movement
Woche:	11
Datum / Zeit	27.11.2018 08:30 - 09:30

Sitzungsteilnehmer / E-Mail

Claudio Mattes	claudio.mattes@hsr.ch
Lukas Kellenberger	lukas.kellenberger@hsr.ch
Cyrill Brunschwiler	cyrill.brunschwiler@hsr.ch

Traktanden

- Stand des Projekts
- Fragen
- Weiteres Vorgehen

Stand des Projekts

Arbeiten	Status
Dokumentation	in Bearbeitung
Pester-Tests	in Bearbeitung
UC05: Display missing or wrong system configuration	in Bearbeitung
UC07: Create Main Script	in Bearbeitung
UC08: Get Domain Information	in Bearbeitung

Unterstützungen

Art der Unterstützung	Hilfsperson
Keine	-

Fragen

- Flotten-Prüfung (Informationen bei einzelnen Clients abholen) sinnvoll?
  - Security-Risks
  - Besser nur Group Policies auf SYSVOL prüfen

Weiteres Vorgehen

Was	Verantwortlichkeit
Pester Tests	Team
Dokumentation	Team
UC05: Display missing or wrong system configuration - Logik	Lukas
UC07: Create Main Script	Claudio
UC08: Get Domain Information	Claudio
English Consulting	Team

Nächster Termin

Datum:	04.12.2018
Zeit:	08:30 - 09:30
Ort:	Standort Alice

Kommende Abwesenheiten

Person	Von	Bis
-	-	-

Beschlüsse (Diskussion)

SA

- Informationen bei einzelnen Clients abholen nicht sinnvoll → besser Prüfung der GPOs
- Alle GPOs aus SYSVOL prüfen - nicht nur einzelne
- Bringen die Sysmon Logs wirklich einen Benefit?
- Sysmon kann auch einen anderen Service-Namen haben → anders prüfen
- Kann Force Audit Policy und CAPI2 wirklich nicht über RSoP geprüft werden?
- Im Text die Audit Policies pro Kategorie anzeigen

BA

- Wie wollen wir das ganze darstellen?
- Können wir vorhandenes Powershell einfach in C# portieren?
- Flottenfunktionalität: Forests, Domains, OUs
- Readiness Optimiser: GPO Templates ausgeben zum applizieren (Delta oder Erweiterung)
- Sysmon auf Flotte verteilen
- Zentrales Logging
- Aussagen über Performance und Speicherbedarf Logging
- Eventuell wird dann eine DB nötig