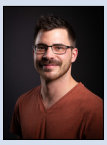

Claudio Mattes

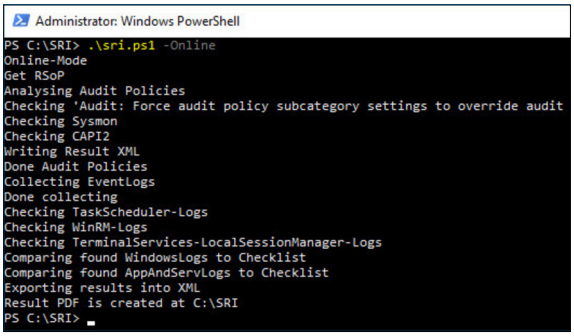

Lukas Kellenberger

Students	Claudio Mattes, Lukas Kellenberger
Examiner	Cyrill Brunschwiler
Subject Area	Security

Readiness for Tailored Attacks and Lateral Movement Detection

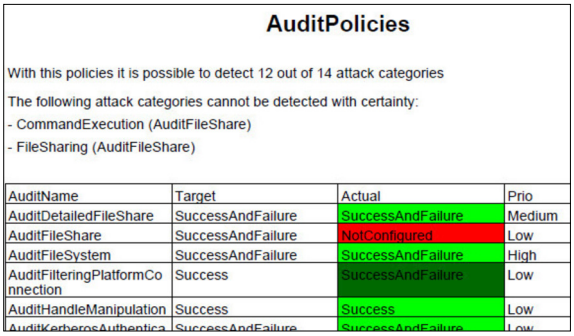
Symbol image bad guy (www.flickr.com/photos/cyberhades/)

Introduction: The number of cyber-attacks where malicious code is used has massively increased recently. These attacks not only settle on the infected system, but can also infect other systems through lateral movements in the network. The outcome is often the complete infiltration of the organization due to the use of advanced persistent threats (APT). Although the configuration of these targeted networks varies depending on the organization, common patterns in the attack methods can be detected. In the analysis of such patterns and events, information and time are key factors to success. Hence, readiness for such an event is a decisive factor.



Console output during online mode of SRI

Procedure / Result: The project was limited to the operating system Windows 10 Pro or Windows Server 16. In the elaboration phase, research was carried out into how the goal of determining readiness of a system could be implemented. The decision was made to implement a proof of concept (PoC) based on the paper "Detecting Lateral Movement through Tracking Event Logs" of the "Japan Computer Emergency Response Team Coordination Center". Existing tools and/or products were evaluated, on which can be built on. Unfortunately, no suitable products were found and so we decided that such a PoC should be redesigned. As technology served Windows PowerShell because it is close to the Microsoft operating system and fulfills the non functional requirement to be a portable script. Moreover, the PoC should be a headless tool which can be started without any GUI and the possibility to be executed offline.



AuditPolicies

With this policies it is possible to detect 12 out of 14 attack categories

The following attack categories cannot be detected with certainty:

- CommandExecution (AuditFileShare)
- FileSharing (AuditFileShare)

AuditName	Target	Actual	Prio
AuditDetailedFileShare	SuccessAndFailure	SuccessAndFailure	Medium
AuditFileShare	SuccessAndFailure	NotConfigured	Low
AuditFileSystem	SuccessAndFailure	SuccessAndFailure	High
AuditFilteringPlatformConnection	Success	SuccessAndFailure	Low
AuditHandleManipulation	Success	Success	Low

Result of SRI

Result: During the construction phase the "System Readiness Inspector - SRI", a Windows PowerShell script, was developed. This phase was completed using the Scrum method. The SRI has four different modes: Online, Offline, GroupPolicy, AllGroupPolicies. The online mode is limited to the current system and thus determines its readiness. The offline mode is used to be able to make a statement about any system by means of exports. The GroupPolicy mode is limited to a specific Group Policy, which is checked for its audit settings. In the AllGroupPolicies mode, all group policies of the current domain are examined.