HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

COMPUTER SCIENCE

STUDYTHESIS

Readiness for Tailored Attacks and Lateral Movement Detection

Authors:

Claudio MATTES
claudio.mattes@hsr.ch

Lukas KELLENBERGER
lukas.kellenberger@hsr.ch

Supervisor:

Cyrill BRUNSCHWILER
Hochschule für Technik Rapperswil
cyrill.brunschwiler@hsr.ch

DEPARTEMENT COMPUTER SCIENCES
HSR UNIVERSITY OF APPLIED SCIENCES RAPPERSWIL
CH-8640 RAPPERSWIL, SWITZERLAND

October 28, 2018

Abstract

Management Summary

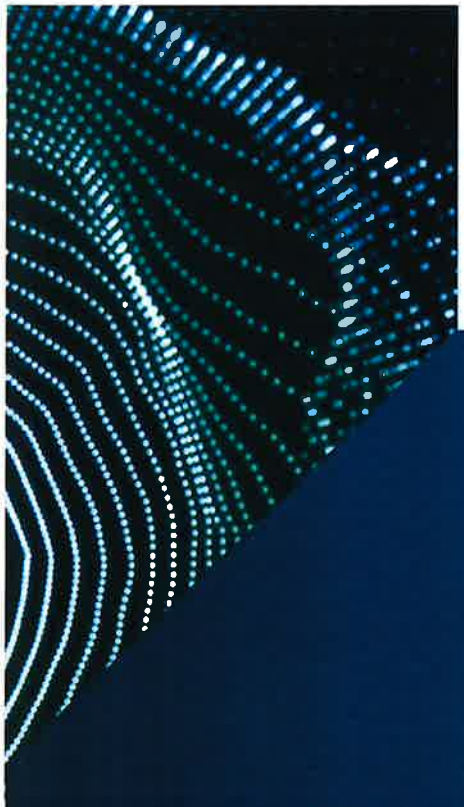
Initial Situation

Procedure

Results

Outlook

Task Definition



Readiness for Tailored Attacks and Lateral Movement Detection

Aufgabenstellung SA Herbst 2018

Datum:	**September 28., 2018**
Author:	**Cyrill Brunschwiler, Compass Security Schweiz AG**
Classification:	**INTERNAL**

Compass Security Schweiz AG, Werkstrasse 20, Postfach 2038, CH-8645 Jona
T +41 55 214 41 60, team.csch@compass-security.com, www.compass-security.com

Table of Contents

1 Einführung

Es werden vermehrt Cyberangriffe publik, wo Schadcode im Einsatz ist, welcher sich nicht nur auf einem infizierten System niederlässt, sondern weitere Systeme im Netz befällt. Das Ziel oder Resultat ist dabei oft die komplette Infiltrierung einer Organisation. In der Analyse solcher Fälle sind Information und Zeit ein Schlüssel zum Erfolg. Folglich ist die Bereitschaft "Readiness" für ein solches Ereignis ein entscheidender Faktor.

2 Aufgabe

Ziel dieser Arbeit ist es, ein Tool zu erstellen, welches die Bewertung der eigene Readiness erlaubt aber auch im Analysefall eine Unterstützung bietet. Readiness betrifft viele Aspekte und einfache Dinge wie korrekte Zeitstempel in Logs, deren Vollständigkeit oder die Bereitstellung von Backups. In der konkreten Aufgabenstellung soll die Readiness-Analyse primär für Windows-Infrastrukturen anhand von Logs und spezifischen Events erfolgen. Unter anderem soll auf den neusten Publikationen des japanischen Computer Emergency Response Teams (JPCERT/CC) und der öffentlichen Datenbank der MITRE Corporation, dem Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™) Wissenspool, basiert werden. Das JPCERT und MITRE haben dabei die Werkzeuge und das generelle Vorgehen von Angreifern analysiert und geben Hinweise, welche Events auf eine mögliche Verseuchung hinweisen.

2.1 Abgrenzung

Es geht nicht darum neue Angriffsvektoren zu finden.

2.2 Tätigkeiten

- Projektmanagement und Dokumentation
- Einarbeitung in Incident Handling und Forensik
- Einarbeitung in Angriffstechniken und Werkzeuge
- Einarbeitung in Abwehrtechniken und Härtung von Systemen
- Studium öffentlicher Quellen und verfügbaren Tools
- Umsetzung eines Analyzers gemäss Anforderungen basierend auf etablierten Frameworks

3 Vorgehen

Im Rahmen der allgemeinen Richtlinien zur Durchführung von Studien- und Bachelorarbeiten gemäss eigenem Projektmanagementplan. Dieser Projektmanagementplan ist als Erstes zu erstellen und enthält insbesondere:

- Die Beschreibung des dem Projektcharakter angepassten Vorgehensmodells.
- Eine erste Aufteilung der Aufgabe in gemeinsam und einzeln zu bearbeitende Teile unter Berücksichtigung der vorgegebenen Teilaspekte. Die genaue Aufteilung muss spätestens nach der Technologiestudie (Elaboration) erfolgen.
- Den Projektplan (Zeitplan) und die Meilensteine.

4 Anforderungen

Es geht primär darum einen Analyzer zu erstellen um die "Readiness for Tailored Attacks and Lateral Movement Detection" beurteilen zu können. Idealerweise kann dieses Tool von einem IT Administrator ohne spezielle Kenntnisse und grossartige Installationsprozeder ausgeführt werden.

Schematisch aber nicht bindend werden folgende Schritte auszuführen sein

- Definition der Requirements für einen neuen/verbesserten Analyzer
- Design und Analyse basierend auf den Vorgaben
- Vorschläge für die Umsetzung oder Verbesserung eines
    - Readiness Analyzers
    - Readiness Optimizers
    - Compromise Analyzers
- Implementation der Funktionalität und Erstellung eines Benutzerhandbuch
- Erweiterung der Analyzer um neue Erkenntnisse, Werkzeuge und Indicators
- Dokumentation der Software und Skripte

4.1.1 Technologien

- Windows Workstations, Windows Server, Windows Security generell
- Windows Event Logs, Security und Audit Logs
- Windows On-Board Tools, Sysinternals Toolkit
- Active Directory Service (AD) Services
- Group Policy Objects (GPO)
- PowerShell, .NET, Python, Windows Batch

5 Infrastruktur

Die Arbeiten werden auf den Rechnern der Studenten durchgeführt. Zusätzlich benötigte Software oder Hardware wird bei Bedarf und nach Rücksprache mit Compass Security zur Verfügung gestellt.

6 Erwartete Resultate

6.1 In elektronischer Form:

- lauffähiges Toolkit und kompletter Source Code
- komplette Software Dokumentation (Use Cases, Klassenmodell, Sequenzdiagramme usw. in UML)
- komplette Use Cases und Erfolgs-Szenarien resp. Musterlösungen
- alle Dokumente und Protokolle (vorzugsweise in englischer Sprache)

6.2 Auf Papier:

Gemäss der Anleitung der HSR: \\hsr.ch\root\alg\skripte\Informatik\Fachbereich\Studienarbeit_Informatik

Es muss aus den abgegebenen Dokumenten klar hervorgehen, wer für welchen Teil der Arbeit und der Dokumentation verantwortlich war (detaillierte Zeiterfassung).

7 Termine

7.1 Start/Ende

- Termine gemäss \\hsr.ch\root\alg\skripte\Informatik\Fachbereich\Studienarbeit_Informatik\SAI\Termine

Datum	Task
17.09.2018	Beginn der Arbeit, Ausgabe der Aufgabenstellung durch den Betreuer.
18.12.2018	Erfassung des Abstracts im Online-Tool https://abstract.hsr.ch/ Die Studierenden geben den Abstract für die Diplomarbeitsbroschüre zur Kontrolle an ihren Betreuer/Examinator frei. Der Betreuer/Examinator gibt das Dokument mit dem korrekten und vollständigen Abstract zur Weiterverarbeitung an das Studiengangsekretariat frei. Vorlagen sowie eine ausführliche Anleitung betreffend Dokumentation stehen auf dem Skripteserver zur Verfügung.
21.12.2018	Hochladen aller verlangten Dokumente auf archiv-i.hsr.ch Abgabe des Berichts an den Betreuer bis 12.00 Uhr

7.2 Zeitplan und Meilensteine

Zeitplan und Meilensteine für das Projekt sind von den Studenten selber zu erarbeiten und zusammen mit dem Projektmanagementplan abzuliefern. Die Meilensteine sind bindend. Der erste Meilenstein ist vorgegeben. Mit den Betreuern werden regelmässige Sitzungen zur Fortschrittskontrolle durchgeführt.

8 Betreuung

Die Arbeiten werden durch Cyrill Brunschwiler betreut. Der Gegenleser ist noch nicht bestimmt.

8.1 Kontakt

Cyrill Brunschwiler, Managing Director, Compass Security Schweiz AG
Weststrasse 50, 8003 Zürich, Switzerland
Werkstrasse 20, 8645 Jona, Switzerland

+41 55 214 41 73
cyrill.brunschwiler@compass-security.com
cyrill.brunschwiler@hsr.ch
https://fb.compass-security.com/inbox/hUGXMr2EeZ2V7b

9 Referenzen

- JPCERT/CC Detecting Lateral Movement through Tracking Event Logs
  https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf
- JPCERT/CC Detecting Lateral Movement through Tracking Event Logs v2
  https://www.jpcert.or.jp/english/pub/sr/Detecting%20Lateral%20Movement%20through%20Tracking%20Event%20Logs_version2.pdf
- JPCERT/CC Detecting Lateral Movement in APTs, https://www.first.org/resources/papers/conf2016/FIRST-2016-105.pdf
- JPCERT/CC Online Results Sheet, https://jpcertcc.github.io/ToolAnalysisResultSheet/
- JPCERT/CC Logon Tracer, https://github.com/JPCERTCC/LogonTracer
- CERT-EU Security Whitepaper 17-002, http://cert.europa.eu/static/WhitePapers/CERT-EU_SWP_17-002_Lateral_Movements.pdf
- NSA Spotting the Adversary, https://www.iad.gov/iad/library/ia-guidance/security-configuration/applications/spotting-the-adversary-with-windows-event-log-monitoring.cfm
- MS (Sysinternals) Sysmon https://docs.microsoft.com/de-ch/sysinternals/downloads/sysmon
- MS Logparser http://www.microsoft.com/en-us/download/details.aspx?id=24659
- MS Windows Defender ATP Advanced Hunting https://github.com/MicrosoftWindowsDefenderATP-Hunting-Queries
- MS Poorman Monitoring https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/
- MITRE ATT&CK Adversarial Tactics, Techniques & Common Knowledge https://attack.mitre.org/
- The CALDERA automated adversary emulation system https://github.com/mitre/caldera
- The APT Simulator Windows Batch https://github.com/NextronSystems/APTSimulator
- Infection Monkey - An automated pentest tool https://github.com/guardicore/monkey
- Flightsim - A utility to generate malicious network traffic and evaluate controls
  https://github.com/alphasoc/flightsim

10 Unterschriften

Jona, 28. September 2018

Cyrill Brunschwiler | Claudio Mattes | Lukas Kellenberger

Contents

Part I

Technical Report

1 Introduction and Overview

As described in the introduction of the task definition the key for a successful analysis in case of an advanced persistence threat (APT) or lateral movement in a network, it is fundamental to have solid event logging of all systems participating in the network.

Shusei Tomonaga at the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) has shown with the study "Detecting Lateral Movement through Tracking Event Logs" [1] how important it is to configure solid event logging to analyze attacks. JPCERT/CC found in their study that APT and lateral movements could be detected with the correct settings in the audit policy and with the help of Sysmon 37 of 44 attacks.

2 Analysis

This chapter describes the first step of this project, the research of published technical reports and tools which are considered interesting for this project.

2.1 BloodHound / SharpHound

2.1.1 Description

BloodHound describes itself on its wiki page on GitHub as follows:

> *"BloodHound is a single page Javascript web application, built on top of Linkurious, compiled with Electron, with a Neo4j database fed by a PowerShell/C# ingestor. BloodHound uses graph theory to reveal the hidden and often unintended relationships within an Active Directory environment. Attacks can use BloodHound to easily identify highly complex attack paths that would otherwise be impossible to quickly identify. Defenders can use BloodHound to identify and eliminate those same attack paths. Both blue and red teams can use BloodHound to easily gain a deeper understanding of privilege relationships in an Active Directory environment."* [2]

2.1.2 Difficulties

BloodHound was tested in the test environment describes later in this chapter. Both, the C# and Python ingestors were successfully installed and tested. The only problem which occurred was that the Python-ingestor does not yet run on the latest Python release. One must have a Python 2.7.x version installed to run the scripts successfully.

2.1.3 Conclusion

The, for our project, most interesting part about BloodHound is the way they retrieve their data. Due to the decision that the application, in a first step, only reads the data of the local computer and not the whole domain, BloodHound will only be important in a later part of the project.

2.2 WEFFLES

2.2.1 Description

WEFFLES (Windows Event Logging Forensic Logging Enhancement Services) is a Threat Hunting/Incident Response Console with Windows Event Forwarding and PowerBI, coded and published by Microsoft-Security-Employee Jessica Payne. It is build to help setting up the Windows Event Forwarding, so that all the collected logs of a system are stored on one centralized server, and afterwards to analyse the collected data. Jessica Payne wrote an installation instruction on the Microsoft TechNet blog `https://blogs.technet.microsoft.com/jepayne/2017/12/08/weffles/`. Once the data is collected one could simply import the generated weffels.csv file into Excel an start filtering the logs to gain the needed. Jessica Payne recommends to use PowerBI, a business analytics tool designed by Microsoft. In her published blog she also gives a short introduction on what to look out for, which event ids are important and other useful tips and tricks for detecting suspicious activities in the network.

2.2.2 Conclusion

WEFFELS will not be the product on which this project is based, but could become an important point of reference.

2.3 Microsoft Security Compliance Toolkit

2.3.1 Description

The Microsoft Security Compliance Toolkit (SCT) [3] allows security administrators to analyze their configured enterprise Group Policy Objects (GPO) in comparison to the Microsoft-recommended GPO baselines. The toolkit is handed with several baseline GPO's for different versions of Microsoft Windows Client and Servers:

- Windows 10 security baselines
  - Windows 10 Version 1803 (April 2018 Update)
  - Windows 10 Version 1709 (Fall Creators Update)
  - Windows 10 Version 1703 (Creators Update)
  - Windows 10 Version 1607 (Anniversary Update)
  - Windows 10 Version 1511 (November Update)
  - Windows 10 Version 1507
- Windows Server security baselines
  - Windows Server 2016
  - Windows Server 2012 R2
- Microsoft Office security baseline
  - Office 2016

2.3.2 Difficulties

The toolkit is very simple and could be understood and used without any difficulties. The handling is very intuitive and does not require much training. Please note, however, that the toolkit cannot be used with Windows 10 Home, since active directory support is not provided with this version.

2.3.3 Conclusion

This toolkit can be used for a very baseline GPO in enterprise environment. With the handed baselines it is easy to compare the configured GPO and to see the readiness of the enterprise GPO. The toolkit gives also the ability to compare different local GPO's installed on different Clients or Servers to check their consistency. In addition the handed baselines can be used for building new GPO's. Furthermore, Microsoft delivers with the SCT a Local Group Policy Object Utility (LGPO.exe) to:

- Import and apply policy settings
- Export local policy to a GPO backup
- Parse a registry.pol file to "LGPO text" format
- Build a registry.pol file from "LGPO text"

This toolkit is very interesting, but cannot be used to build on it. The reason for this is that the source code of the complete toolkit is not available. However, it can be used as additional help for checking the readiness of an enterprise environment.

2.4 LogonTracer

2.4.1 Description

JPCERT/CCs LogonTracer is a tool built to investigate malicious logons on a system based on the research described in section 2.9 JPCERT/CC - Detecting Lateral Movement in APTs. The tool links hostnames or IP addresses with the *"account name found in logon-related events and displays it as a graph"*. [4] The following event ids are checked with the tool:

- 4624:Successful logon
- 4625:Logon failure
- 4768:Kerberos Authentication(TGT Req.)
- 4769:Kerberos Service Ticket (ST Req.)
- 4776:NTLM Authentication
- 4672:Assign special privileges

The following figure shows a sample graph from the test environment:

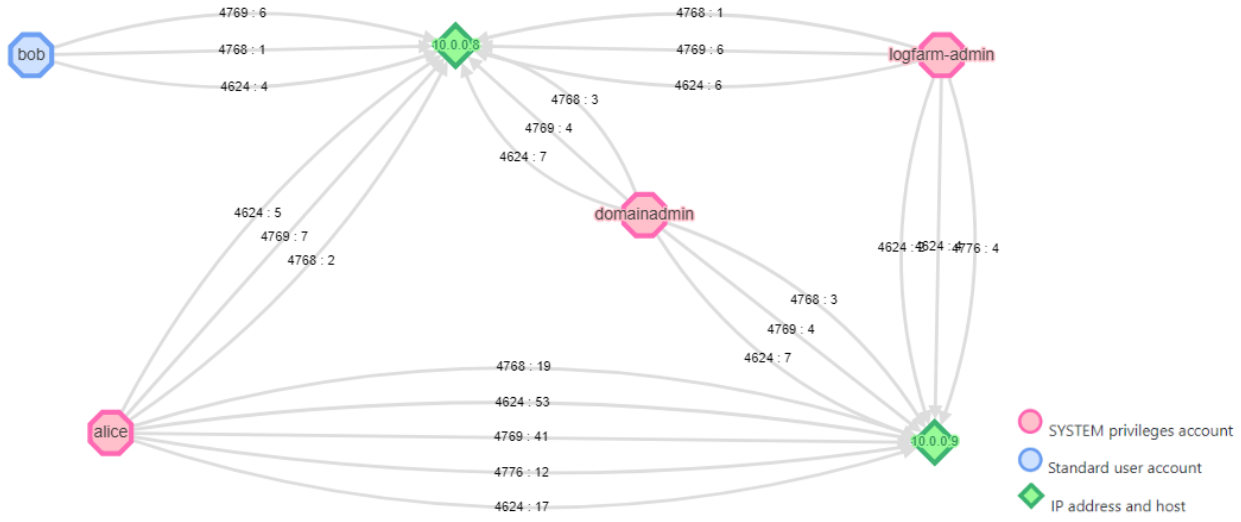


Figure 1.1: LogonTracer: Sample Graph from Test Environment

To use the LogonTracer, there is only a .evtx-File (Windows XML Event Log - export of Windows event logs) needed to be uploaded. At best the export of the security event log of the domain controller to get as much information of the network as possible. With the built in analysis of logins, by using machine learning models and statistical analysis, LogonTracer is able to provide a ranking of the most malicious users which tried to log in. [5]

In addition, LogonTracer provides a timeline for all or selected users to see when each user logged in. The timeline can also be displayed as a graph with the LogonTracer, allowing anomalies to be detected more quickly.

The test environment showed that this graph can quickly become confusing - especially in a larger corporate environment. Although only a small environment as described in the section was used, it turned out that various users wanted to log on to the virtual machines. The reason for this is that the test environment is accessible via public IP addresses in the cloud.

Nevertheless, with meaningful filters the search can be restricted and the graph can be used efficiently, as shown in the figure 1.1 LogonTracer: Sample Graph from Test Environment

2.4.2 Difficulties

During the test phase of LogonTracer some difficulties were detected. It's pretty easy to get the docker container, but starting LogonTracer is a bit of a challenge. JPCERT/CC gives the following instructions for starting the docker container:

Listing 1.1: LogonTracer: given docker run command

```
$ docker run --detach \
--publish=7474:7474 --publish=7687:7687 --publish=8080:8080 \
-e LTHOSTNAME=[IP_Address] jpcertcc/docker-logontracer
```

The Problem was that the parameter `[IP_Address]` was not described well. If the command `docker ps` was executed it always showed the following `PORTS`:

Listing 1.2: LogonTraceer: docker ps (PORTS)

```
PORTS
0.0.0.0:7474->7474/tcp, 0.0.0.0:7687->7687/tcp, 7473/tcp, 0.0.0.0:8080->8080/tcp
```

After a lot of investigation and further tests it turned out that under `PORTS` the ports respectively ip addresses of the container can be bound to the host. But these are not relevant for the LogonTracer, because it provides a web application under the defined parameter `[IP_Address]` and after enough patience it can be reached via `localhost:8080`. If this parameter was set to `127.0.0.1`, the database containing the imported .evtx file could not be accessed. Thus the graph was never displayed. The parameter `[IP_Address]` set to `localhost` solved this problem.

Listing 1.3: LogonTracer: recommended docker run command

```
$ docker run --detach \
--publish=7474:7474 --publish=7687:7687 --publish=8080:8080 \
-e LTHOSTNAME=localhost jpcertcc/docker-logontracer
```

2.4.3 Conclussion

The LogonTracer is unique in its form and should not be underestimated for the detection of lateral movements. This is because user access to the components available in the network can be visualized simply and graphically and conclusions can be drawn from it as to exactly what has happened.

However, the LogonTracer is not suitable for detection readiness and cannot be used to build on it. Nonetheless, approaches for reading the event log for further work could be used. And for a further detection of lateral movements this tool is extremely interesting.

2.5 Microsoft Monitoring Active Directory for Signs of Compromise

2.5.1 Description

This article "Microsoft Monitoring Active Directory for Signs of Compromise" [6] is about configuration of an solid event log monitoring for Microsoft servers. The article gives a quiet well overview about the audit policy in Microsoft systems and what each policy stands for. The article gives information about the most important audit policies and how noisy (if a lot of data is produced by them) they are. This study does not go into the details of the audit policies in detail. Furthermore the article describes how the policies can be read with powershell.

To this article Microsoft compiles in Appendix L [7] all important event ids which are necessary for a successful detection of APTs and lateral movements.

2.5.2 Conclussion

Due to the fact that audit policies are an important setting for solid event logging, this article and appendix L will be a central part of the toolkit to be built. As a next step and part of this study these event ids have to be correlated with the event ids found in the JPCERT/CC's study "Detecting Lateral Movement through Tracking Event Logs" [1] to make a clear statement which event ids have to be logged.

2.6 MITRE ATT&CK

2.6.1 Description

MITRE ATT&CK introduces itself on its website as follows:

> *"MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community."* [8]

The portal offers a variety of attacks and their patterns, which are currently known in different operating systems. MITRE ATT&CK describes the attack in short words and then lists possibilities for detection and mitigation. Various attack tools are described on the portal as well. With which goal they are used and what effects they can have. In addition, the corresponding attacks are always cross-referenced. This is a great advantage for a quick search, especially when time is of the essence.

2.6.2 Conclusion

Although many attacks are described and how they can be detected and fended off, MITRE ATT&CK is not quite suitable for our task. The readiness of a system to detect tailored attacks and lateral movements is only roughly described and would be associated with a time-consuming analysis in order to draw exact conclusions.

2.7 sysmon-modular

2.7.1 Description

With sysmon-modular [9] a clean configuration of the Windows system service System Monitor (Sysmon), an xml-file which is loaded by Sysmon, is provided. Noisy process creations, which are done by legitimate programs, are suppressed as far as possible by Sysmon. The tool offers the possibility and it is expressly recommended by the developer to adapt the configuration to the respective organization. Furthermore sysmon-modular implements various attacks in MITRE ATT&CK for detection with Sysmon. It offers the possibility to detect the attacks shown in the figure 1.2 with Sysmon.

Figure 1.2: Detectable attacks with sysmon-modular

2.7.2 Conclusion

Sysmon-modular offers a very good basic configuration for Sysmon which is based on the platform MITRE ATT&CK which is widely used in the security scene. Unfortunately sysmon-modular was discovered when decisions were made to develop a tool based on the study "Detecting Lateral Movement through Tracking Event Logs" by JPCERT/CC. The readiness of a system with the basis of MITRE ATT&CK patterns would probably have had an even greater impact. However, Sysmon-modular will probably not be included in the tool during this study, unless there are still enough time reserves for such an integration.

2.8 Sysmon Tools

2.8.1 Description

Sysmon Tools [10] contains some useful functions to make better use of Sysmon. Among other things there are different views for the representation of the single entries which were recorded by Sysmon. A Process View is provided which can be used to examine a process in more detail. Related processes are taken into account and represented in a simple data-flow-like view, sorted by chronological order. With the Map View you can include geo-locate IP addresses during the import phase and Map View tries to geo-map the network destinations with ipstack [11]. The All Events View represents a full search by Sysmon and can be filtered and grouped accordingly. Furthermore, Sysmon Tools offers a Sysmon Shell, which can be used to create a customized XML configuration for Sysmon using a GUI. Templates are also provided for further building.

2.8.2 Conclusion

This tool can also be a great help for detecting attacks and with the Sysmon Shell a robust configuration for Sysmon can be created. However, Sysmon Tool will have no basis for the project "Readiness for Tailored Attacks and Lateral Movement Detection".

2.9 JPCERT/CC - Detecting Lateral Movement in APTs

2.9.1 Description

This document [12] is from a presentation by Shingo Abe, a JPCERT/CC employee. In it he describes how to find system intruders more effectively using Windows Event Logs. The collected data is used to better detect inconsistencies, such as when an administrator logs on to another machine or when an administrator logs on suspiciously often.

2.9.2 Conclusion

This presentation contains interesting information which could be built into the project at a later point. The information this document contains are more suitable for monitoring purposes than for checking the readiness of a system.

2.10 JPCERT/CC - Detecting Lateral Movement through Tracking Event Logs

2.10.1 Description

This is a document [1] the Japan Computer Emergency Response Team Coordination Center, or short JPCERT/CC, has published in the year 2017. It describes how, in their experience, attackers proceed with lateral movement. In a very detailed 81-page report they describe step by step the procedure, the tools used and what is most interesting for the project, the logs generated while doing so.

2.10.2 Conclusion

This report will have the biggest impact on this project, it shows which logs have to be read in any case. In addition, JPCERT/CC describes in this report which configurations are necessary for solid logging. The appendix not only describes the individual event log IDs, but also the audit policy that can be used to achieve them. For this reason, the checklist to be used will mainly be based on this report. With the given information we see the greatest potential to develop a suitable tool for the accomplishment of the task in the given time.

2.11 Test environment

A virtual network was set up on Azure-Cloud as a test environment. The test network was set up in the cloud so that the development team can access the network regardless of its location. The test network consists of a Windows server and two Windows clients. Active Directory service was configured on the server to manage the client computer. The following operating systems were installed in this test network:

Server:

- Windows Server 2016

Clients:

- Windows 10 Pro, Version 1709

The network is structured as followed:

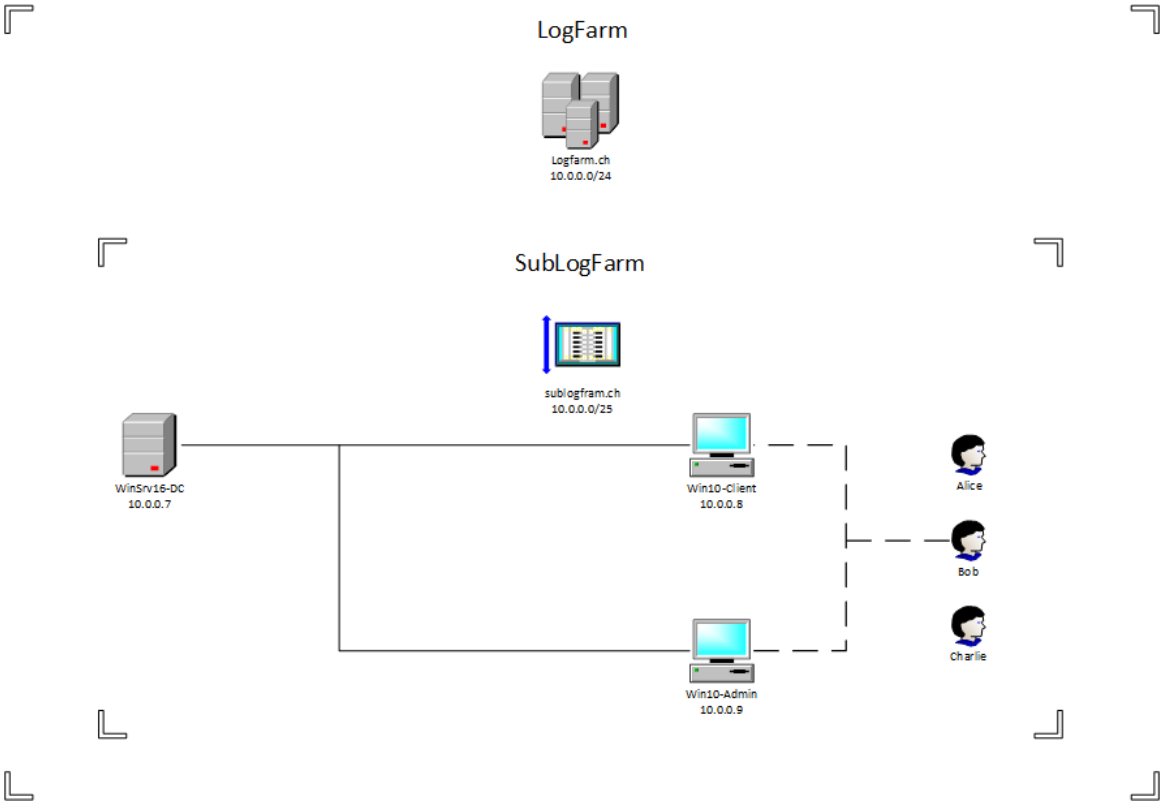


Figure 1.3: Test Environment

2.11.1 User

Three different user were configured for the logfarm-network:

Name	Permissions
alice	administrator
bob	user
charlie	user

Table 1.1: Test Environment User

2.11.2 Difficulties

Various difficulties occurred which are presented in this subsection.

Connect to the virtuel machines via RDP
After setting up the virtual machines on Azure, the developers tried to connect to the devices via the Remote Desktop Protocol. First, the developers suspected it was the incoming port rules, so reinstall the machines. However, this did not fix the error.It turned out that the problem was not with the virtual machines, but with the network they were in. Their firewall blocked the RDP-connection. In order to avoid this, the developers used a VPN-Connection.

Firewall setting for ICMP
After the virtual network has been set up, the developers tested the connections in the virtual network. The configured DNS ran without any problem and could translate all hostnames. Testing the network using Pings showed that all clients were receiving pings, but the ping-requests by Win10-Client remained unanswered. It turned out that, for some inexplicable reason, the incoming ICMP-firewall-settings were different on this client. After adjusting the setting the ping-requests were answered positively.

RDP connection for Bob and Charlie
Due to the fact that the user Alice owns administrator privileges, she was able to connect over RDP without an error. Bob and Charlie on the other hand did not have this permissions. The developers had to create a group for them, the RDP-Group. This group was then allowed to login over RDP on the clients Win10-Client and Win10-Admin.

2.12 Domain Analysis

The following section describes the problem domain which is faced during this project. Despite the decision to not programm an object orientated solution, there are several things to be aware of and to think carefully through. For this reason building a domain model is a simple and suitable suitable technique to use for. The following figure 1.4 shows the domain model and will be explained in some details afterwards.

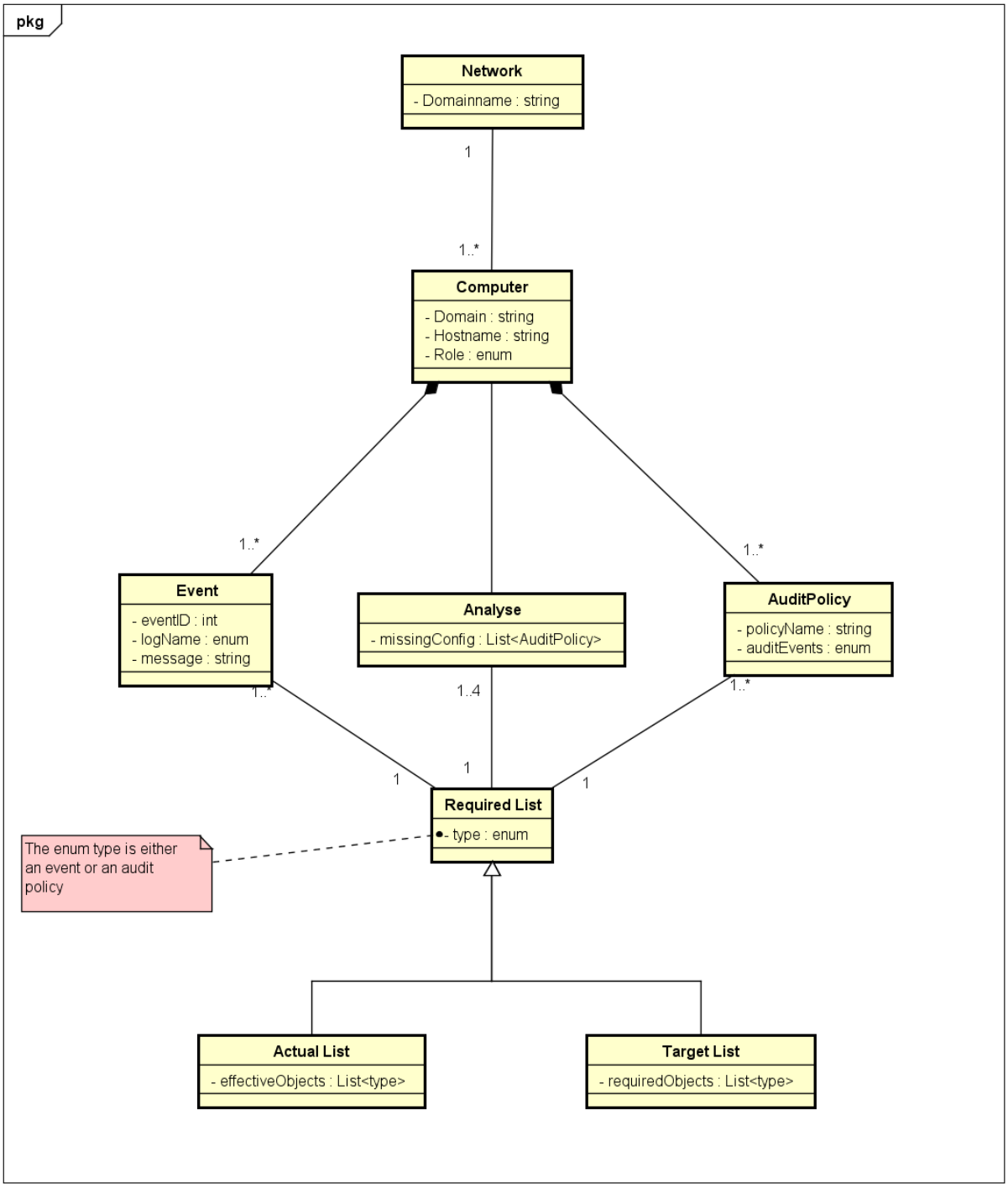


Figure 1.4: Domain Model

2.12.1 Network

The class network depicts the organizations wide network which is used to connect all clients and servers together. In this project the main goal is to locally detect the readiness of the system and not to extend the detection for a system-wide infrastructure. For further development on this project and a system-wide extension the network is already considered in this domain model.

2.12.2 Computer

A computer illustrates a either a client like a Windows 10 machine or a server in particular a domain controller running on a Windows Server 2016. In principle, however, every Windows computer is represented. A computer is a core component in our project, because the detection is done on a single client or server.

2.12.3 Event

An event represents a single event log entry in simplified form.

2.12.4 AuditPolicy

AuditPolicy displays the individual settings of the audit policies of the group policy, which can be found under "Computer Configuration > Windows Settings". However, only the settings under "Security Settings > Advanced Audit Policy Configuration" are considered and not the settings under "Security Settings > Local Policies > Audit Policy". The reason for this is that Microsoft recommends that only one of the two policies to be used:

> *[...] do not use both the basic audit policy settings under Local Policies\Audit Policy and the advanced settings under Security Settings\Advanced Audit Policy Configuration. Using both basic and advanced audit policy settings can cause unexpected results in audit reporting.* [13]

A single audit policy setting represents one or more event IDs logged by this configuration.

2.12.5 Required List

Actual List The actual list represents the current state of the system. It reflects the event log IDs that have occurred and the audit policies that have been set.

Target List The target list represents either the list of event logs or configured audit policies which must be present for a solid detection of attacks.

2.12.6 Analysis

Based on the required lists and the current state of the computer, the analysis shows which settings are missing in the audit policies.

3 System Architecture

In this section the following main question is answered:

"How would a system architecture look like to fulfill the described problem domain?"

This includes the coverage of use cases, non-functional requirements, technologies used ...

3.1 Use Cases

A visual representation of the use cases with a use case diagram was deliberately omitted, because there is only one actor involved - the security advisor. The actor is not specifically mentioned in the use cases every time, because it is always the same.

3.1.1 UC01 - Read Resultant Set of Policies

Description
The specified audit policies are read and saved in a temporary file.

Precondition
The system is running and the tool must possess administrator permissions.

Main Success Scenario

1. Read the specified audit policies from the system
2. Save the needed information from the audit policies in a temporary file for analysis purposes.

3.1.2 UC02 - Analyse Audit Policies

Description
The list which was created in UC01 is compared to a "perfect settings"-list. Missing or wrong settings are going to be exported into a separate file.

Precondition
UC01 is fulfilled: the temporary file is available.

Main Success Scenario

1. The temporary files can be read
2. Creates a list of incorrect settings

3.1.3 UC03 - Find Event Logs

Description
Event logs are search by ID and marked in an external file as found or missing.

Precondition
The system is running and must have valid event logs. The tool must possess administrator permissions.

Main Success Scenario

1. Search for the specified event logs from the local system
2. Save the result from the search in a temporary file for analysis purposes.

3.1.4 UC04 - Analyse Found Event Logs

Description
The implemented logic analyzes, by defined event ids, which events occurred or are missing and creates a list of events that did not occurred or are not logged yet.

Precondition
UC03 is fulfilled: the temporary file is available.

Main Success Scenario

1. The temporary file can be read
2. The list with the defined event ids is available
3. Create a list of events which occurred and which are missing

3.1.5 UC05 - Display missing or wrong system configuration

Description
Based on the list created in UC02 and UC04 the user gets an overview of missing configurations (the result) which would improve the readiness of the system for a good attack detection.

Precondition
The lists from UC02 and UC04 are available.

Main Success Scenario

1. Displays a visual output of missing or wrong system configurations

3.1.6 UC06 - Save Result to specific path

Description
The actor has the possibility to save the overview from UC05 to a file in a specific path defined by the actor himself. This file contains the result from UC05 in a descriptive way.

Precondition
UC05 is fulfilled: the result, respectively the overview is available

Main Success Scenario

1. A file is saved to a specific path with the result from UC05
2. The path can be defined by the actor

3.2 Non Functional Requirements

NFR-No.	Description
NRF01	The Toolkit must remain the system in the status quo. More specific the system shall not deliberately alter any existing entry in the event logs and registry. However, the tool may will produce new event logs.
NFR02	The user shall not notice significant performance degradation from the system when using the Toolkit.
NFR03	The Toolkit must be portable with no installation procedure before use.
NFR04	The minimal target version of the system for the Toolkit to run must be Microsoft Windows 10 Professional or Microsoft Server 2016.
NFR05	The Toolkit runs in one go, but can also be executed in single steps with the possibility to skip single steps (pause/abort in case of performance problems)

Table 1.2: Non Functional Requirements

3.3 Technologies

3.3.1 Choosen Technologies

PowerShell & Visual Studio Code
The decision, which technology will be used, was made in favour of PowerShell. The reason why PowerShell will be used was, that it is close to the Microsoft Operating System and that it has a large and detailed documentation at its disposal.

The scripts are written in Visual Studio Code with the extension packet 'PowerShell'. Visual Studio code is preferred to PowerShell ISE because it only requires working in one IDE for implementation and documentation.

LaTeX & Visual Studio Code
The documentation is written with LaTeX in Visual Studio Code wit the LaTeX Workshop extension. The main reason for LaTex was that the developers are already familiar with it. Furthermore, LaTeX offers a very simple way for referencing sources. On the other hand we have made the experience that with LaTeX the formatting is more reliable than for example when Microsoft Word is used.

Azure Cloud
The test environment is set up, like in '2.9 Test environment' described, in the azure cloud. One server and two clients form a virtual network, this brings the advantage that the developers can access it from anywhere to any given time. A disadvantage is the changing public IP-addresses to access the VMs. In the end, the advantages outweigh the disadvantages.

GitHub
GitHub is used as a version control tool for source code and documentation. GitHub has been elected because of its good reputation and the experience the developers already gained with.

3.3.2 Rejected Technologies

Continuous Integration
Continuous integration is not used in this project because it will be a simple toolkit that is not written object-oriented. On the other hand,

Python
The decision to use PowerShell and C# instead of Python was made because the developers do not have much experience with Python. Also PowerShell is closer to the Microsoft-OS. With Python there is no guarantee that the libraries which would be used are as powerful to solve the requirements.

4 Results

5 Conclusion

Glossary

List of Figures

List of Tables

Bibliography

[1] JPCERT/CC. Detecting Lateral Movement through Tracking Event Logs. , 2017.

[2] harmj0y Andrew Robbins, Rohan Vazarkar. BloodHound - Wiki. https://github.com/BloodHoundAD/BloodHound/wiki, 2018.

[3] Microsoft. Microsoft Security Complience Toolkit. https://docs.microsoft.com/en-us/windows/security/threat-protection/security-compliance-toolkit-10, 2018.

[4] JPCERT/CC. LogonTracer. https://github.com/JPCERTCC/LogonTracer, 2018.

[5] Shusei Tomonaga. Visualise Event Logs to Identify Compromised Accounts - LogonTracer -. https://blog.jpcert.or.jp/2017/11/visualise-event-logs-to-identify-compromised-accounts—logontracer-.html , 2017.

[6] Microsoft. Monitoring Active Directory for Signs of Compromise | Microsoft Docs. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise, 2017.

[7] Microsoft. Appendix L: Events. https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l–events-to-monitor, 2018.

[8] MITRE ATT&CK. MITRE ATT&CK Website. https://attack.mitre.org/, 2018.

[9] Olaf Hartong. sysmon-modular. https://attack.mitre.org/, 2018.

[10] Nader Shalabi. Sysmon Tools. https://github.com/olafhartong/sysmon-modular, 2018.

[11] ipstack. Locate and identify website visitors by IP address. https://ipstack.com/, 2018.

[12] Shingo Abe. Detecting Lateral Movement in APTs - Analysis Approach on Windows Event Logs Introduction to JPCERT / CC. 2016.

[13] Microsoft. Advanced security auditing FAQ. https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq, 2017.