applied sciences

MDPI

Article

Revisiting the Detection of Lateral Movement through Sysmon

Christos Smiliotopoulos [1], Konstantia Barmpatsalou [1] and Georgios Kambourakis [2,*]

[1] Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Karlovasi, Greece; csmiliotopoulos@aegean.gr (C.S.); konstantia@aegean.gr (K.B.)
[2] European Commission, Joint Research Centre, 21027 Ispra, Italy
* Correspondence: georgios.kampourakis@ec.europa.eu or gkamb@aegean.gr

Abstract: This work attempts to answer in a clear way the following key questions regarding the optimal initialization of the Sysmon tool for the identification of Lateral Movement in the MS Windows ecosystem. First, from an expert's standpoint and with reference to the relevant literature, what are the criteria for determining the possibly optimal initialization features of the Sysmon event monitoring tool, which are also applicable as custom rules within the config.xml configuration file? Second, based on the identified features, how can a functional configuration file, able to identify as many LM variants as possible, be generated? To answer these questions, we relied on the MITRE ATT and CK knowledge base of adversary tactics and techniques and focused on the execution of the nine commonest LM methods. The conducted experiments, performed on a properly configured testbed, suggested a great number of interrelated networking features that were implemented as custom rules in the Sysmon's config.xml file. Moreover, by capitalizing on the rich corpus of the 870K Sysmon logs collected, we created and evaluated, in terms of TP and FP rates, an extensible Python .evtx file analyzer, dubbed *PeX*, which can be used towards automatizing the parsing and scrutiny of such voluminous files. Both the .evtx logs dataset and the developed PeX tool are provided publicly for further propelling future research in this interesting and rapidly evolving field.

Keywords: lateral movement; Sysmon; dataset; attacks; network security; hacking

check for updates

Citation: Smiliotopoulos, C.; Barmpatsalou, K.; Kambourakis, G. Revisiting the Detection of Lateral Movement through Sysmon. *Appl. Sci.* **2022**, *12*, 7746. https://doi.org/10.3390/app12157746

Academic Editor: Konstantinos Rantos, Konstantinos Demertzis and George Drosatos

Received: 11 July 2022
Accepted: 28 July 2022
Published: 1 August 2022

1. Introduction

Lateral Movement (LM) refers to a wider set of techniques that adversaries use to gain initial access through a network's vulnerable endpoint for the lateral escalation of their presence in search of sensitive data and other valuable assets to compromise or exfiltrate. Simply put, after an attacker has acquired an initial foothold in a network and performed an internal reconnaissance, they will most probably seek to expand and reinforce that foothold while systematically gaining further access to important data or systems. For effectively dealing with such incidents in a prompt and effective manner, e.g., avoiding the overabundance of security alerts and false positives, a targeted and fresh approach is a necessity. Once the threat is remediated, and the log evidence related to the attack is collected, the impact calculation of the damage will be used as the basis for the constitution of remedial measures toward an effective Endpoint Detect and Response (EDR) policy.

While the configuration of a network targeted by an adversary varies depending on its structure, there are some common patterns regarding LM methods. At first, typically, the attacker concentrates on the identification and enumeration of the targeted system, in parallel with the exfiltration of crucial information with tools such as Mimikatz, ipconfig, systeminfo, and others. The initial target is chosen with mediation, as this will be the first step for the rest of the LM to be expanded. Credential dumping follows; this will permit the perpetrator to acquire the necessary credential information, leveraging tools such as Mimikatz, pwdump, LazagneProject, or even malware in an effort to infect the targeted host and acquire administrative access. Common techniques presented in MITRE's records [1] reveal that in such conventional similar assault cases, the adversaries repeatedly leverage a limited number of penetration tools. Therefore, the key points that this paper aims to address are narrowed down to the fundamental and technical particles of each attack, specifically related to the so-called "5Ws" analysis, namely Who-What-When-Where-Why.

Precisely, the work at hand relies on the execution of the most frequently encountered LM techniques based on their impact, as presented on MITRE's ATT and CK database of adversaries, tactics and techniques [1]. Particularly, we exploit a properly designed testbed via nine diverse LM techniques, namely "Exploitation of Remote Services (ERS)" (four variants of ERS attack), "Pass the Hash (PtH)", "Pass the Ticket (PtT)", "Golden Ticket (GT)", "Silver Ticket (ST)" and "Post Exploitation on Stored Passwords with (LZP)". Our aim is to provide concrete answers to the following key questions: (a) Based on related theory and domain expertise's best practices, are there any solid criteria for determining the most effective, upon LM identification, rule-based features of the system monitoring tool (Sysmon)?, and (b) how could the proposed criteria combined with the extracted features lead to the formation of a top-notch rule-based and event-driven methodology, which generalizes the identification of any LM attack? Overall, the main contributions of this work vis-a-vis the relevant literature are summarized as follows:

- From a defender's viewpoint, we elaborate on the outcomes of the executed experiments in an attempt to define solid criteria, which act as signatures per examined attack.
- Based on the derived criteria, the most impactful features were extracted as related to Sysmon's identification of an adversary moving laterally.
- The proposed criteria, along with their related features, are evaluated based on their effectiveness on a potential lateral incident's identification through Sysmon.
- A rule-based methodology is proposed that is dedicated to the identification, verification, and categorization of each lateral technique.
- The proposed methodology is implemented in a Python analyzing tool dubbed "PeX". The tool along with the large dataset of Sysmon logs collected during the experiments are made publicly available to the community [2].

The remainder of this paper is structured as follows. Section 2 discusses the related work, whereas Section 3 encloses a general description pertinent to this work's fundamental LM techniques. Section 4 presents the testbed, while Section 5 details the commonestLM attack techniques based on their final impact. The proposed data-driven methodology is provided in Section 6. Section 7 focuses on the presentation of the *"PeX"* tool. The last section concludes and suggests directions for future work.

2. Related Work

The current section provides a brief review of the key pertinent literature on the subject. The concentration is on the methodology of each relevant work regarding event-driven identification of the most impactful LM techniques through Sysmon. Particularly, we focus on the logs collection of the specified examined attacks, the utilized rule-based policy, and the impact upon the successful incidence response. To facilitate the parsing of the relevant literature, Table 1 recaps the relevant characteristics of every work included in this section.

JPCERT/CC, the first Computer Security Incident Response Team (CSIRT) established in Japan, was also one of the first organizations to conduct a full-fledged survey regarding the categories of logs produced during the execution of LM [3]. The commonest LM techniques at that time were executed against both compromised servers and targeted clients related to each attack method. Logging information was collected and categorized via Sysmon [4] and the MS Windows audit policy. The work concluded with the proposition of a log-oriented MS Windows regulatory policy, allowing the optimal collection of useful information related to potential LM methods. The final report was published in June 2017 and updated on v2 [5] in December of the same year. On the downside, considering the exponential occurrence of LM events and the daily lessons learned from the Russo-Ukrainian war, this survey is considered quite outdated to cope with MITRE's [1] database of malicious LM tactics and techniques on real-life observations. For instance, the aforementioned work can be extended to incorporate LM events in cloud and satellite communication facilities, such as the incident of February 2022 against Viasat's KA-SAT network [6], resulting in a targeted interruption of the satellite broadband services across the Ukraine territory and other European countries.

Mavroeidis et al. [7] introduced a data-driven threat classification methodology, which relies on the continuous analysis and assessment of aggregated Sysmon logs. The first part of this work was dedicated to the development of their proposed Cyber Threat Intelligence Ontology (CTIO), which was based on the Cyber Threat Intelligence (CTI) model also published by them in [8]. The second part of that paper proposed a threat assessment system that incorporated CTIO for the classification of event-logs generated by Sysmon in four distinct threat categories, namely high, medium, low, and unknown. Despite the promising results, the proposed threat assessment methodology is prone to long delays when it comes to voluminous logging data on real-life scenarios.

Berady et al. [9] presented a threat hunting model based on the common acceptance of the conclusion that the attacker and defender should mutually understand each other. The analysis was performed from both an offensive and defensive perspective. Offensive experiments were conducted upon the *APT29* dataset, which is included in the Mordor Project of pre-recorded event-related logs of malicious activities. The two-staged attack emulation scenario initially incorporated the exfiltration of sensitive data for the targeted host and, then, the compromise of the target via an injected toolkit. The network activity of the targeted host was monitored with Sysmon to produce a dataset comprising two days of log recording. The finally proposed "Indicators of Compromise" enhanced the defender's common knowledge of the offender's best practices, seemingly improving the preventive identification of threats. Nevertheless, it seems that the proposed model is incapable of dealing effectively with the vast existence of false-positives due to the lack of Sysmon's rule-based configuration policy.

The work in [10] proposed a Dynamic Link Library (DLL)-oriented method for malicious file detection towards logs collected by Sysmon. Numerous DLL files were collected and analyzed from four different tools, namely China Chopper, Mimikatz, PowerShell Empire, and HUC Packet Transmitter, to reveal the existence of significant differences in the specific files among various versions of the MS Windows Operating System (OS) and the aforementioned tools. The work concludes with the extraction of a list with the commonly loaded DLLs per tool, regardless of the Windows OS environment and the introduction of a detection-specific logging method based on the open-source ELK Stack. The researchers in [11,12] also attempted to introduce a DLL-oriented malware detection methodology through the analysis of potentially malicious files on sandbox environments, such as *Cuckoo*. However, only the authors in [10] proposed a list with the most commonly appeared DDL files related to malicious intrusion tools. Additionally, the contributions in [11,12] relied on classification techniques with Machine Learning (ML) algorithms, which at this point fall out of the scope of the current research. It can be said that the enhancement of the DLL detection policy, particularly focused on each LM method used for Sysmon event logs, will expand the detection accuracy and diminish the false positive results.

The ELK Stack was also used by the authors in [13,14] for the analysis of massive log records and the identification of malicious behavior. Specifically, the work in [13] implemented a *logstash* massive data processing pipeline to collect a critical mass of logs, whereas [14] generated Sysmon logging events. In both cases, the ELK stack was utilized for log file iteration and the identification of malicious patterns. On the downside, both works were tightly bonded to ELK stack practices, neglecting the need for a general purpose rule-based EDR system.

The work in [15] focused on Advance Persistent Threat (APT) detection of the Mimikatz password stealing tool utilized in the context of LM. To increase the true positive rates, the authors implemented *Mutex* memory objects in parallel with the identification of Mimikatz-related DLL files. It can be argued that even with the introduction of *Mutex-oriented* DLL file analysis, the Mimikatz tool can be deliberately obfuscated by the adversary, thus evading identification by even advanced EDR and IDS systems.

Last but not least, the work in [16] considered the detection of malware Application Programming Interface (API) call patterns for the identification of behavioral anomaly signatures. Despite the high true positive rates, the proposed methodology affects the performance of the examined system and omits it from incorporating Sysmon event logs. On the other hand, the authors in [17] suggested an LM detection system, dubbed "Hopper", which is fed by real-life generated logs. The user's login activity was tracked and outlined through a graph of interrelated logins among the implicated hosts. This contributes to anomaly detection among logins, referring to LM attacks. On the flip side, despite "Hopper's" effectiveness, the system ignores logs generated with Sysmon. In this respect, the aforementioned two papers are considered out of the scope of this study.

Table 1. Summary of the most important aspects of the works included in Section 2. The works are presented in chronological ascending order.

Related Work		
Title	**Year**	**Summary**
A novel approach for detecting malware based on API call sequence analysis [16]	2015	Detection of malware API call patterns towards the identification of behavioral anomaly signatures
Detecting lateral movement through tracking event logs (v1 & 2) [3,5]	2017	Execution of LM through well-known penetration testing tools. Collection of logs with Sysmon and MS Windows Audit Policy. Categorization of logs per attack and proposition of optimal MS Windows infiltration settings for effective identification of LM activity.
Data-driven threat hunting using Sysmon [7]	2018	Data-driven threat classification methodology based on aggregated logs created by Sysmon. Proposed a threat analysis system, which is based on the developed by the authors CTI ontology.
Lateral movement detection using ELK stack [14]	2018	A way to generate event logs with Sysmon related to the execution of various LM attacks and the associated malicious tools on MS Windows-based environments. Implementation of ELK stack towards the analysis of possible abnormalities in the collected logs due to the existence of LM.
Real-time detection system against malicious tools by monitoring DLL on client computers [10]	2019	Proposed a DLL-oriented method for malicious file detection through logs collected by Sysmon [4]. Common DLL list per malicious tool, independent of MS Windows OS version.
Detecting Mimikatz in lateral movements using Mutex [15]	2020	APT detection of Mimikatz while utilized in LM. Implementation of Mutex memory objects in conjunction with DLL files analysis. Mimikatz's misidentification while deliberately obfuscated.
From TTP to IoC: Advanced persistent graphs for threat hunting [9]	2021	Threat hunting model which evaluates Sysmon's logs from both an offender's and defender's perspective. Based on indicators of compromise, proactive threat detection is possibly enhanced. A high rate of false positives due to the absence of rule-based Sysmon's configuration.
Hopper: Modeling and detecting lateral movement [17]	2021	System for LM attack detection based on real-life generated logs. Login activity is tracked and outlined through a graph of interrelated logins among the implicated hosts to conclude in the detection of anomalies among logins referring to LM.
Network forensics investigation in virtual data centers using ELK [13]	2021	Generating log records with *Logstash*. Network forensic analysis via the implementation of Elastic Search and towards the identification of RDP LM-related attacks, Ransomware, Data Exfiltration, etc., as part of a criminal investigation.

3. Preliminaries on Lateral Movement

This section comprises a descriptive presentation of the most prominent and fundamental techniques with which an adversary may move laterally and compromise computing systems and accounts in a Small Office Home Office (SOHO) or corporate networking environments. For an attacker to compromise a targeted host, initial access is gained through the continuous and iterative enumeration of the systemic parts of the network to identify accounts with potentially elevated user privileges. What typically follows is the combined execution of a large repertoire of offensive tools, including Metasploit framework, malware propagation and Mimikatz hashing compromising tool. In brief, during the execution of LM, the aggressors occupy asset's account credentials of the low or medium access level of the targeted network, escalating their privileges up to their final target. This is achieved through various techniques, which are detailed in Sections 5 and 6.

The boundary between the internal network's perimeter and the outside world could be depicted as a horizontal line, in which the upper half comprises the outside world, whereas the environment under the line represents the closed, say, corporate network. For a malevolent intruder to penetrate a network, the movement should be executed vertically and towards the aforesaid horizontal boundary line. Mostly, this kind of movement is called "North to South" [18], and from a defender's viewpoint, it usually appears as an abnormality in the network's activity. When credentials are exposed, an anchor point is created, and the intruder can maneuver with privileged access horizontally and around the network components, gradually reaching and compromising the most valuable targets ("East to West" movement). Naturally, while it seems normal for a network component to communicate with certain terminals inside the same network domain, continuous connection attempts to open ports or manipulation of credential acquisition services via unregistered username or passwords are considered suspicious at least. Overall, there are two fundamental methodologies for moving laterally within a targeted network:

- The first method refers to network mapping and identification of the special characteristics of each distinct component along with potential vulnerabilities. During the reconnaissance phase, many OS's built-in tools can be used. For instance, the ipconfig and ifconfig commands reveal IP configurations and localization information, while Netstat summarizes the most current network connections along with their users. Additionally, the local routing table tracks all the interconnected network paths, while the Address Resolution Protocol (ARP) cache reveals the matching of network IP addresses to their equivalent link layer (MAC) addresses. Vulnerability assessment and mapping tools are also in the attackers' quiver, namely Nmap or its commercial equivalent Nessus [19]. Once the relevant information is gathered, the adversary is able to intrude and move laterally.
- The second customary method refers to the use of phishing techniques for the acquisition of account credentials by any means. To this end, the opponent can take advantage of tools, say, Metasploit Pro, to craft numerous phishing emails that have been perfectly cloned to appear as originating from a legitimate source. Additionally, keylogger tools, including Revealer Keylogger Free, KidLogger, and BlackBox Express, provide a powerful equivalent solution for activity monitoring and screen recording at the victim's side. Mimikatz, presented in Section 6.2, is another powerful credential exploitation and hash dumping penetration testing tool.

4. Testbed

For the purposes of log file gathering (in .csv, .evtx, .xml form), as depicted in Figure 1, we created a mixed testbed comprised of both virtual and physical stations that realistically emulates a typical SOHO environment. In total, eight different physical and Virtual Machines (VMs) were utilized. Three of them were used as client stations (1 Ubuntu Desktop 20.0.4 LTS, 1 Kali Linux Desktop 2020.4 LTS, 1 MS Windows 10), one both as the client station and host PC on which VMs have been installed, and two smartphones as clients (1 Android smartphone Samsung A8 and 1 iOS iPhone XR). Moreover, one physical laptop (MacBook Air) simulated the attacker's interface. Finally, one MS Windows Server 2019 64-Bit was created as a VM station to dissemble the malicious LM's final target. The wireless Access Point (AP) was a SERCOM Speedport Plus router. The SOHO's network topology is presented in detail in Figure 1, while the role and the characteristics per machine are included in Table 2.

To simulate as realistically as possible the workload of a typical SOHO network, the *SYSMON_SET domain* was created within an MS Windows 2019 Server VM. Six client accounts were configured and initialized via the *MS Windows Server Account Management* service and joined the SYSMON_SET domain. For the needs of the execution of the various credential exploitation attacks detailed in Section 6.2 each of the server's accounts was granted domain administrative privileges in advance.

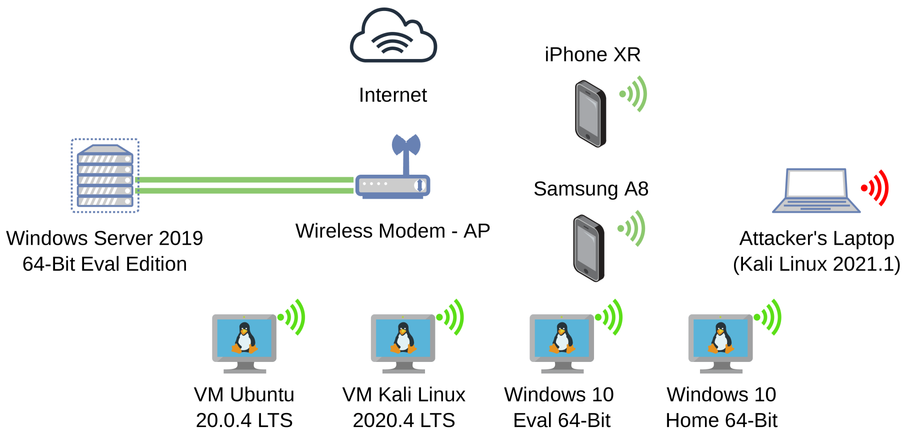


Figure 1. High-level view of the testbed network topology. The MS Windows Server 2019 uses a wired connection with the AP, presented as a double green line. The network traffic flow for disparate categories of VM and physical stations is shown in a different color, namely green for Wi-Fi traffic and red for the attacker.

Table 2. Summary of key technical characteristics related to the machines utilized during the execution of the LM experiments.

Technical Characteristics and Utilization of Each STA (Physical and VM)							
Station	**Type**	**Operating System**	**Kernel_Version**	**CPU/RAM**	**IP_Address**	**MAC_Address**	**Username**
AP	Wireless_AP	SERCOM_Firmware	09022001.00.031 OTE2	-	80.107.57.231, 192.168.1.1	7C:8F:DE:46:66:11	N/A
Client STA 1	VM	Ubuntu 20.0.4	5.8.0-53-generic-x64	VM dual_core, 2 GB	192.168.1.6	08:00:27:4e:4e:e6	adminchr
Client STA 2	VM	Kali 2021.1	5.10.0-kali7-amd64	VM dual_core, 2 GB	192.168.1.11	08:00:27:3e:b5:a7	nicksaitas
Client STA 3	VM	Win10 Eval. x64	2004	VM dual_core, 2 GB	192.168.1.7	08:00:27:3d:c5:a9	chr.smilio
Client STA 4	Laptop	Win10 Home x64	2004	i7-9750H CPU, 16 GB DDR4	192.168.1.28	98:AF:65:32:E8:21	laptop-ropr18ak_chrsm
Windows 2019 Server	VM	Win2019 Server x64	1809	VM dual_core, 2 GB VM RAM	192.168.1.8	08:00:27:4f:d3:32	christossmiliotopoulos
Client STA 5	Smartphone	iOS 15.0	14.4.2	Hexa-core, 64GB RAM	192.168.1.3	06:16:EC:81:F9:68	iPhone-Christos
Client STA 6	Smartphone	Android 9	Knoxx 3.3	Exynos 7 Octa 7885	192.168.1.13	3C:DC:BC:7F:73:B7	A8-Maraki

5. Lateral Movement Categories on Windows Environments

As already mentioned, LM techniques are leveraged by cyber criminals to intrude and remotely control network systems and hosts. Network reconnaissance and target identification are followed by the penetration of the protected networking perimeter. That is achieved with the installation of remote accessing tools on systems, the credentials of which were successfully extracted, and then it escalates incrementally to other hosts. Based on the revised MITRE ATT and CK open-access database [1], among the many available techniques and practices, in the context of this paper, the nine commonest were chosen based on their impact. These attacks were applied on the testbed's nodes of Section 4 and are described in the following subsections.

5.1. Exploitation of Remote Services

Cybercriminals may exploit MS Windows systems' remote services to gain unauthorized access to the various nodes of a network. This kind of exploitation is successful when the adversary takes advantage of a revealed vulnerability of the targeted system, known or currently unknown. To determine whether the system is in a vulnerable state, the assailant makes use of numerous information-gathering techniques to reveal unpatched OS components or even the lack of updated IDS and antivirus software. Among the most common, port scanning and vulnerability assessment tools are included, which are loaded and installed remotely on the system under attack. Server nodes are considered the most high-value targets during the execution of LM. Mostly, they comprise the final destination of an attacker after gaining initial access to a network node and hopping from one system to another.

There are many well-known vulnerabilities concerning the various MS Windows OS versions. Server Message Block (SMB), Authenticated Remote Code Execution (RCE) and Remote Desktop Protocol (RDP) are two of the most popular misconfigurations. Within the context of this paper, exploitation of remote services was performed against the testbed described in Section 4. Precisely, the EternalBlue vulnerability was used in three different ways to exploit the SMB of an unpatched version of Windows Server 2019, which was left vulnerable on purpose, while the RDP exploit was tested with BlueKeep (CVE-2019-0708) RCE. Overall, four different instances of the Exploitation of Remote Services attack were executed. First, SMB was exploited via the Metasploit's ms17-010 module. Next, the SMB EternalBlue vulnerability was used towards the final execution of the arbitrary remote commands on the targeted system via Metasploit's *smb_login* auxiliary service. To expand the analysis of the remote exploitation on the targeted server, the testbed was infected with the worm-like *WannaCry* malware. To allow the propagation of the malware, User Account Control (UAC) of the server was disabled remotely with the use of the *smbexec 2.0* tool. Finally, Metasploit's CVE-2019-0708 dedicated module was utilized to leverage the targeted Server's RDP misconfiguration.

5.2. Pass the Hash Credential Override

Hash transmission is a method that provides account identification and credentials integrity check without the requirement for any username or password in plaintext form. This method overrides traditional user authentication, which requires a personal access password in plaintext form, and proceeds directly to the host's approval with the use of hash algorithm-encrypted character chains. Hash distribution instead of plaintext account credentials was considered a tough-to-crack identification and authentication method. Despite the robustness of the aforesaid authentication mechanism, penetration techniques have been developed to allow the collection and extraction of all the hashes related to valid accounts. These techniques fall under the general category of "Credential Access". MITRE ATT and CK [1] describe this attack vector as the *keylogging* and *credential dumping* techniques, making LM more effective and harder to be identified in real-time.

PtH is a method for achieving successful authentication without the possession of the original credentials (usernames and passwords) in cleartext form. It is considered a very successful and targeted attack for bypassing traditional authentication procedures via stolen hashing credentials. Through PtH, access control services of Windows can be compromised, considering an adversary's LM as legit. PtH is a credential theft technique and LM attack at the same time, with which the attacker can leverage the challenge-and-response nature of the Windows New Technology LAN Manager (NTLM) authentication procedures utilized from the network's hosts in place of traditional plaintext credentials. With standard security protocols, NTLM hashes change only when the plaintext passwords are changed. This is the feature that makes PtH ideal for threat actors to move laterally across a network. For easy reference, the Windows Kerberos hashing authentication procedure along with the NTLM hash extraction vulnerability is illustrated in Figure 2.

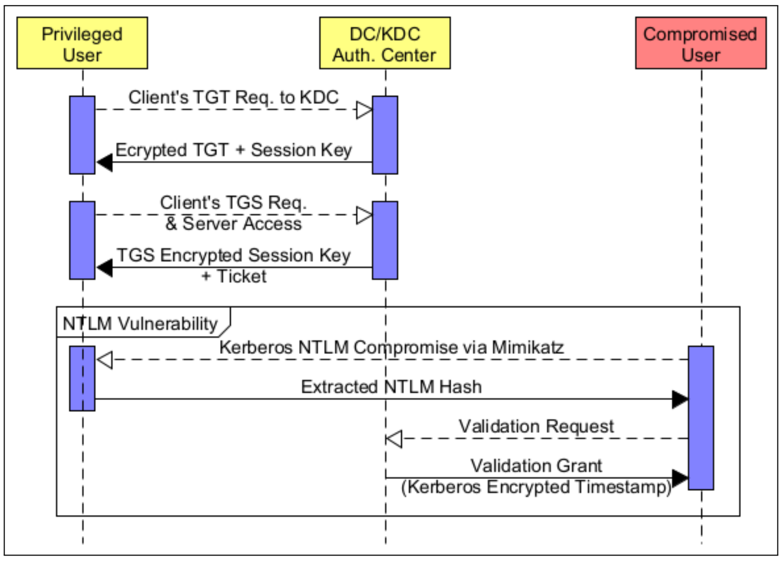

Privileged User
DC/KDC Auth. Center
Compromised User
Client's TGT Req. to KDC
Ecrypted TGT + Session Key
Client's TGS Req. & Server Access
TGS Encrypted Session Key + Ticket
NTLM Vulnerability
Kerberos NTLM Compromise via Mimikatz
Extracted NTLM Hash
Validation Request
Validation Grant (Kerberos Encrypted Timestamp)

Figure 2. High-level view of Kerberos Authentication procedure, along with the NTLM hash extraction vulnerability, that makes KDC prone to the Hashing Exploitation Attacks of Section 6.2, namely, PtH, PtT, Golden/Silver Ticket.

5.3. Pass the Ticket Credential Override

By exploiting the Pass-the-Ticket (PtT) method, an adversary may move laterally within a network by using stolen Windows Kerberos Tickets as legitimate credentials. PtT is based on the Windows OS's Local Security Authority Subsystem Service (LSASS) process, which is a fundamental part of the Windows credential administration system and is also related to PtH. The aforementioned process stores and handles Kerberos tickets and is related to the extraction of the Kerberos Service Tickets and Ticket Granting Tickets (TGT), depending on the level of access of the compromised host. Recall that a service ticket permits access to a particular process, whereas a TGT is responsible for requesting the aforesaid service tickets from Kerberos TGS to acquire access to any resource that the targeted host has access to. Specifically, for this attack to be successful, the targeted host needs to communicate with LSASS and retrieve the legitimate tickets in its possession. If the attacked host is related to a non-administrative user, then only one ticket will be retrieved, whereas if administrative accounts are compromised, all the tickets related to the targeted server can be harvested. Within the context of this survey, Mimikatz was the preferred tool for the execution of the PtT attack.

5.4. Golden Ticket

Golden Ticket is another Active Directory attack related to Kerberos authentication exploitation techniques. While access with administrative privileges is important for the adversary, persistence during lateral movement within a targeted network is the real challenge. This aspect is crucial for an opponent to reach its target within network environments in which the domain's admin password changes frequently.

Golden Ticket migrates features from both PtH and PtT LM methods. Precisely, it exploits the Kerberos authentication protocol's lack of validation procedures during the impersonation of a legitimate host. This is due to the design of the Kerberos protocol to allow users that hold a TGT for a session to be considered trusted for any other network resource related to ticket authentication.

In the context of this work, Mimikatz is used as a standalone tool for the realization of GT. There is also the possibility of the Metasploit Framework's automated *meterpreter* extension as a faster solution for the execution of the attack.

5.5. Silver Ticket

Silver Ticket is another Active Directory attack related to Kerberos authentication tickets' exploitation. This technique capitalizes on a forged TGS ticket. The latter is used to authenticate and impersonate an adversary with escalated privileges for the service it represents. A malicious user may create an ST through the exploitation of a targeted host's credentials, including their account password. The ST attack has a limited scope of application compared to the GT. That is, while the first relies on a forged TGS, i.e., specifically initialized for a single service on the targeted server, the latter relies on a forged TGT that can be used as valid for the authentication of adversary hosts to any Kerberized service. Since the required hash for the execution of the ST attack is easily obtained, and no communication with the domain controller is required while in use, that makes its detection harder than the GT. A high-level view of the execution of PtH and PtT in conjunction with the exploited Kerberos authentication mechanism is depicted in a UML Activity Diagram in Figure 3.

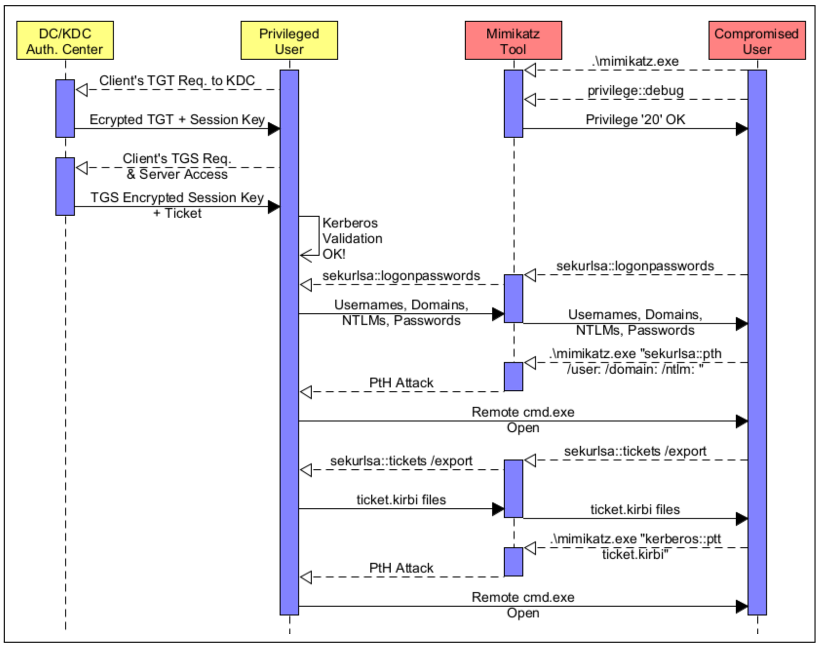

DC/KDC Auth. Center
Privileged User
Mimikatz Tool
Compromised User
.\mimikatz.exe
Client's TGT Req. to KDC
privilege::debug
Ecrypted TGT + Session Key
Privilege '20' OK
Client's TGS Req. & Server Access
TGS Encrypted Session Key + Ticket
Kerberos Validation OK!
sekurlsa::logonpasswords
sekurlsa::logonpasswords
Usernames, Domains, NTLMs, Passwords
Usernames, Domains, NTLMs, Passwords
.\mimikatz.exe "sekurlsa::pth /user: /domain: /ntlm: "
PtH Attack
Remote cmd.exe Open
sekurlsa::tickets /export
sekurlsa::tickets /export
ticket.kirbi files
ticket.kirbi files
.\mimikatz.exe "kerberos::ptt ticket.kirbi"
PtH Attack
Remote cmd.exe Open

Figure 3. High-level view of Kerberos authentication procedure, along with the NTLM hash extraction vulnerability, that makes KDC prone to hashing exploitation attacks, namely PtH, PtT, and Golden/Silver Ticket.

5.6. Post Exploitation on Stored Passwords with LaZagne Project

The last implemented attack pertains to the post-exploitation of the already saved credentials on the server's random-access memory. This was achieved through the open-source application named "LaZagne Project". It was performed in conjunction with the Exploitation of a Remote Services attack, presented in Section 5.1 and following the exploitation of the server's SMB file sharing protocol via Metasploit's *smb_login* auxiliary service. This is a penetration testing tool that directly injects its Python code into the volatile memory of the targeted machine without leaving any trace. In this aspect, the method comprises a straightforward process for the adversary to compromise the victim's stored credentials without raising any suspicion.

6. Methodology

For the needs of this work, we relied on log files produced by Sysmon, which is both a Windows system service and a device driver. Once installed, it is resilient to all the OS activities, including reboots and the event logger. Sysmon monitors and gathers event-oriented information in detail, namely process creations, network connections and modification actions, while organizing them simultaneously in folders and files of different compatible formats, namely .evtx, .xml, .csv, and .txt, to be available for further analysis.

Sysmon currently supports 27 distinct types of case-sensitive events, which may be generated during logging activity of networking traffic and OS processes. The second column of Table 3 designates the Event IDs that were recognized in the context of the present work either as normal or suspicious and implemented them in the proposed rule-based policy detailed in Sections 6.1 and 6.2 and Appendices A.1 and A.2. The rightmost column of the same table specifies the designated per attack vector and Event ID related subsection. It is important to note that any Event ID that was not recognized during the analysis of the conducted experiments is omitted from Table 3, as it is irrelevant to the context of this paper. The basic features and capabilities of Sysmon, along with the full list of the supported Event IDs, can be found on the tool's official website in [4].

Table 3. Sysmon-generated events during the conducted experiments of Sections 6.1 and 6.2. The star exhibitor denotes normal traffic exclusively.

No.	Event ID	Description	Subsection
1	*Event ID 1*	Process creation	Sections 6.1 and 6.2
2	*Event ID 2*	A process changed a file creation time	Sections 6.1.3, 6.1.4 and 6.2
3	*Event ID 3*	Network connection	Sections 6.1.4 and 6.2.1–6.2.3
4	*Event ID 5*	Process terminated	Sections 6.1 and 6.2
5	*Event ID 10*	Process Access	Sections 6.2.1–6.2.3 and 6.2.5
6	*Event ID 11*	FileCreate	Sections 6.2.1–6.2.3
7	*Event ID 13*	RegistryEvent (Value Set)	Sections 6.2.1–6.2.3
8	*Event ID 22*	DNSEvent (DNS query)	Sections 6.2.1–6.2.3
9	*Event ID 23*	FileDelete (File Delete archived)	Section 7.2*
10	*Event ID 255*	Event ID 255: Error	Section 7.2*

Sysmon allows the adoption of a rule-based custom configuration approach for the *config.xml* file. Each event is identified and filtered through a specified tag placed under the EventFiltering section in the *config.xml* file. The detailed list of all the available tags, along with the list of the conditional statements, which are necessary for the initialization of the *config.xml* file, are available in the tool's official documentation [4].

Precisely, within the context of this paper, Sysmon was used to filter and identify events related to the executed LM attacks included in Section 5. Specifically for the attacks, due to their nature, they were divided into two main categories, namely *Exploitation of Remote Services and Credential Exploitation Attacks*, and discussed in Sections 6.1 and 6.2, respectively. Listing 1 presents the necessary initialization statements for the *config.xml* file to be loaded in Sysmon's configuration. As seen in the first line of the listing, the declaration of the *schemaversion*, under the tag <*Sysmon schemaversion="13.30"*>, is fundamental for the initialization of the *config.xml* file. Moreover, the declaration of the utilized *hashalgorithms* as well as the <EventFiltering> tag, which states that the nature of the configuration file has to do with the filtering of Sysmon Events, are both of equal importance. The final required statement of xml code is the necessary specification for each concept *RuleGroup*.

```xml
<Sysmon schemaversion="13.30">
  <HashAlgorithms>md5,sha256,IMPHASH</HashAlgorithms>
  <CheckRevocation/>
  <EventFiltering>
  <RuleGroup name="Sysmon_Event_1(ProcessCreate)" groupRelation="or">
```

Listing 1. Sysmon config.xml initial statements.

For the purposes of the configuration of the *config.xml* file, with the proposed rule-based methodology, more than 150 rules have been created. The rationale behind the creation of these rules is detailed in Sections 6.1 and 6.2. The current work relies on the analysis of the particular characteristics associated with each attack separately and in combination with the observations of network traffic during the execution of each attack given in Section 5. The experiments continued with the collection and analysis of the DLL files; these were loaded as legitimate from the malicious tools with which the LM experiments were executed. The results of the analysis of the DLL files related to the malicious tools with which the LM of Section 5 were executed are integrated into the proposed rule-based calibration of the Sysmon tool. The final result is a novel EDR solution based on Sysmon. Simply put, our proposed solution particularly focuses on the generic identification of potential malicious LM by means of legitimate logging activity.

According to the related work in [10,20,21], the utilization of an EDR system that is calibrated with custom rules to filter malicious processes based on their names, hashes, and network characteristics is proposed as a necessity for the avoidance of modern and sophisticated LM. However, this approach does not guarantee the effective identification of the very special characteristics that many malicious tools enclose, which prevents the successful recognition of these tools, either through being renamed or rebuilt by the opponent. A solution to the problem of the identification and detection of malicious tools is proposed by researchers in [10–12] through the incorporation of DLL analysis and the careful study of their unique per-tool characteristics.

6.1. Exploitation of Remote Services

Four variations of this attack were executed and presented below, namely *"Exploitations of ms17-010-EternalBlue-Bluekeep vulnerabilities"* and *"WannaCry's malware propagation"*. In all four variants, the final goal of the attacker was the execution of remote commands via a PowerShell terminal. For the feature extraction needs, which will be related to the finally proposed rule-based EDR policy, 30,000 Sysmon logs were collected, representing 1 hour of the described attack. Precisely, each sub-category of the T1210 technique [1] was performed consecutively for 10 min each, not exceeding one hour in total. The three distinct variations of the remote services attack plus the extra fourth, along with the discussion per subject, are presented in more detail as follows.

6.1.1. Exploitation of ms17-010

This was conducted successfully against a vulnerable MS Windows server with the aid of Metasploit. It is worth mentioning that the targeted server responded with a successfully activated *Meterpreter* session of the EternalBlue vulnerability after several repeated attempts (at least ten). The attack is deemed successful when PowerShell admin rights are available for the execution of core Windows commands and LM expansion to other hosts.

Discussion: With reference to malicious endpoint command abuse, the analysis revealed the Process Creation vector, i.e., *Event ID 1* with reference to Table 3, as the most prone to exploitation from opponents. Specifically, more than 25% or 7500 logs were related to the creation of processes on either the source or destination hosts. Command line administrative tools were among the most recognized on the logs related to the attacker's machine, namely *sc.exe*, *schtasks.exe*, *winrs.exe*, *PowerShell*, *cmd.exe* and many others. On the other hand, among the most identified parent processes linked to the aforementioned potentially malicious Windows Services features were *services.exe (SCM)*, *svchost.exe (Scheduled Tasks)*, *wmiprsve.exe (WMI)*, *mmc.exe (DCOM)*, *wsmprovhost.exe (WinRM)*, and *explorer.exe (RDP)*. In addition, the existence of *svchost.exe* and *mmc.exe* process features in the *Sysmon* logging activity may also be a distinctive indicator of remote execution of *Impacket Python scripts*. That is, *Impacket* Python classes are used for Microsoft's network protocol implementation and are popular among threat actors regarding concealing their presence during an attack.

6.1.2. Exploitation of EternalBlue

This attack was performed via Metasploit's *smb_login* auxiliary module and *psexec*, revealing the targeted server of Figure 1 as prone to the *smb_login* credential leakage and execution of remote command vulnerability. A *Meterpreter* session also needs to be activated for the attack to be considered successful. *Discussion:* With respect to *EternalBlue* vulnerability via *smb_login* and *PsExec*, the conducted experiments revealed leveraging of Windows SMB as potentially malicious. Specifically, SMB access with administrative privileges, namely *admin$*, *ipc$* and *c$*, is considered suspicious behavior, which implies the manipulation of the Windows system's binaries. This behavior was identified within the collected logs during the execution of the Metasploit's *smb_login* module and *PsExec* tool and prior to the execution of remote services through the *Meterpreter* session on the targeted host. In the context of this work, we utilized the *net.exe* service to connect via Metaspoilt to the SMB protocol's sharing environment for privilege escalation. SMB share's enumeration followed, through the mapping of the server's *smb-admin c$*, generating a number of interesting *Sysmon* log entries on the targeted host. To begin with, since mapping of the *c$ admin shares* within the borders of a SOHO or corporate network do not constitute a legitimate user's normal activity, any event generated on Sysmon with *Event ID 1* related to the *net.exe* should be identified as potentially malicious. Similar to the age of *net.exe*, a *ProcessCreate* rule for the *whoami.exe* was also included. Despite being a Windows native executable, it is uncommon for a legitimate user with basic credential access to run it through PowerShell [22]. This pattern was observed within the collected logs and was integrated as a proactive threat-hunting measure and not as a rule that could serve as a standalone.

6.1.3. Deployment of WannaCry

In addition to the two aforementioned versions of the *"Exploitation of Remote Services"* attack, the well-known *WannaCry* ransomware was propagated deliberately to the VMs of the testbed. To assist the expansion of the malware, server's UAC was disabled remotely with the use of the *smbexec* 2.0 tool. The latter is a post-exploitation tool, which, among the many disabling UAC, is particularly useful for malware establishment on a network host. WannaCry was downloaded from GitHub and used to infect the Windows Server 2019 VM. After the exploitation of the EternalBlue vulnerability, WannaCry encrypted every file in the targeted server, displaying a message demanding payment in Bitcoin. At the same time, *Wireshark* has been used to capture the network activity. As expected, after the VM's infection, a mass packet exchange started, demonstrating unknown packets to the proposed testBed IP addresses, such as 89.163.210.241 and 34.107.221.82.

Discussion: Regarding the *WannaCry* spread on the targeted server, *"ProcessCreation"* and *"ProcessChanged"* events *(Event IDs 1 and 2)* were identified as the most relevant to the target's infection, representing more than 40% (or 12,000 logs) of the logging activity during the execution of the experiments. Specifically, both events are generated when a *Process* alters a file and do not constitute an indication of malicious activity when used in isolation. However, when combined with a number of factors, namely *CommandLine*, *CurrentDirectory*, *Hashes*, *ParentImage*, *Parent* and *CommandLine* rules, they form an effective data-driven proactive detection mechanism towards the identification of *WannaCry* expansion. With reference to the identified processes after the deliberate execution of *WannaCry*, *Wcry.exe* and *tasksche.exe* were isolated as the most relevant logs to the attack, along with their *path* and *ProcessID 3024*. On the other hand, the execution of the *Wcry.exe* process generated a number of interrelated *"r.wnry"* executables. Precisely, those files are generated during the decryption of the infected files and after the ransom's payment in bitcoin through the *"s.wnry"* file. The *"taskse.exe"* process was identified as a *ProcessCreation* log that was also created by *Wcry.exe* for reasons of Windows RDP sessions enumeration, whereas *"taskdl.exe"* was also created for file encryption with the *".WNCRYT"* extension. The creation of the *"t.wnry"* and *"u.wnry"* files was also identified as generated by *Wcry.exe* for reasons of AES encryption and decryption, respectively. Malware spreading behavior produced two more log categories, namely "attrib.exe" and "icacls.exe", which are related to the execution of commands altering the attributes of the targeted files. The former is related to the malware's tendency to hide the infected files, whereas the latter grants administrative access to all the directories and sub-directories. Regarding the above-mentioned behavior, there were 12,000 (or ≈40%) "ProcessCreation" and "ProcessChange" Sysmon's event-logs, and 3258 (or ≈11%) were identified as exclusively related to the WannaCry infection.

6.1.4. Exploitation of BlueKeep

To extend the conducted research, and as a proof of concept of the generic nature of the proposed data-driven methodology for the identification of Exploitation of Remote Services attacks, the server (Figure 1 and Table 2) was exposed to the BlueKeep (CVE-2019-0708) RCE vulnerability. BlueKeep is related to Windows RDP and RDS, revealing a similar behavior to the above-mentioned WannaCry exploitation of the EternalBlue vulnerability. The exploitation was conducted via Metasploit's CVE-2019-0708 dedicated module.

Discussion: With respect to the proposed rule-based Sysmon policy, 689 (or ≈4%) *"ProcessCreation"* and *"ProcessChanged"* related logs *(Event IDs 1 and 2)* were identified as strongly correlated to suspicious LM behavior on RDP. The examined rules were exported during the first stage of the experiments presented in Section 6.1. Despite promising results, the in-depth reexamination of the collected logs revealed the absence of *"NetworkConnection"* logging activity with *"Event ID 3"*, specialized enough to describe the core functions of the RDP and RDS Windows protocol and services, respectively. Sysmon was updated with rules, generic enough to alert in the case of RDP BlueKeep exploitation. Simply put, Windows services that utilize the same port as the RDP protocol, namely *Destination Port 3389*, were identified and imported as rules. Their complete description is presented as follows:

- *mstsc.exe*: It is related to Microsoft Terminal Services Client (MSTSC) Windows shared library (DLL) and allows access to RDP clients to perform a remote desktop connection through command line or PowerShell. If leveraged by an adversary, the relevant DLL may allow the execution of arbitrary controversial code remotely without the mediation of GUI or a SOCKS proxy connection [23].
- *RTSApp.exe*: It is related to the Royal TS remote management software from *code4ward*. Royal TS supports both Windows RDP and RDS, protocol and services. If not found in `C:\\ProgramFiles\\code4ward\\royal_ts`, then it should be checked for potential malware activity, which refers to an LM attack [24,25].
- *ws_TunnelService.exe*: This process belongs to VMware and there are no references to Virustotal for potential malicious behavior. However, when identified in a system that neglects VMware from its utilities, then the collected digital signature's hash algorithm of the file should be checked as potentially malicious [26].
- *RemoteDesktopManagerFree.exe*, *RemoteDesktopManager.exe*, *RemoteDesktopManager64.exe*, *mRemote.exe*: The mentioned processes are strongly related to Windows handling of remote desktop connections. They comprise nonstandard tools of Windows that utilize destination port 3389 and should be considered potentially dangerous for LM orchestration [25,27,28].
- *Terminals.exe*, *spiceworks-finder.exe*, *thor.exe*, *thor64.exe*: These executable files are not Windows native and, when in existence, should be evaluated as potentially malicious and related to malware-based LM behavior [24].
- *reg.exe*, *chrome.exe*: The second process is one of the most common among Windows users, as it is the executable of the Chrome browser. Despite the reliability of the

process, adversaries can take advantage of the frequency with which it appears on the target system by leveraging Chrome's launcher. This is accomplished through the remote manipulation of the target's registry permissions to eventually grant RCE and RDP exploitation. The simultaneous presence of the two processes or the occurrence of the second in a subfolder of the user's profile folder, in conjunction with the utilization of TCP port 3389, should be examined as malicious [29,30].

Regarding the aforesaid Sysmon's networking logging activity, 456 "Network Connection" Event ID 3 logs were identified, with more than half of them (or ≈242 Sysmon logs) related to the executed LM attacks. For easy reference, Table A1 in Appendix A.1 summarizes the most important rule-based features of this Section 6.1 as they emerged from the four executed experimental variants of the Exploitation of Remote Services attack.

6.2. Credential Exploitation Attacks

With reference to credential exploitation techniques, five distinct attacks were executed, namely PtH, PtT, GT, ST and Post Exploitation on Stored Passwords with LZP. For the needs of the rule-based analysis presented in this work, 60,000 Sysmon logs were collected, representing 60 min of continuous execution of each credential exploitation, respectively. Precisely, to demonstrate as clearly as possible the distinct characteristics of the current experiments, each sub-category of Mitre's T1550 Technique [1] was performed consecutively for 60 min each and not exceeding 240 min in total.

As already noted, for executing the experiments, we relied on the *Mimikatz* tool. This choice was driven by factors such as the tool's popularity among adversaries, the multiple versions available (*GitHub legacy edition*, *PowerShell Invoke-mimikatz*, ransomware such as *BadRabbit* or *NotPetya)*, and the possibility of executing the tool with the *Metasploit framework*.

6.2.1. Pass the Hash

As already mentioned in Section 5.2, PtH is a credential theft technique and LM attack at the same time. PtH was executed against client 3 of Table 2. The targeted Windows 10 system stored the passwords in NTLM hashing form. Mimikatz was chosen for the execution not only of *PtH* attack but also for the *PtT* and *GT/ST* ones. For the related accounts with username *chr.smilio*, hashing passwords were extracted from the server's memory and the Windows LSASS.exe service through *Mimikatz's* administrative command line remote execution. To acquire admin rights the *"Privilege "20" OK"* message needs to be revealed in the command line for the PtH command to be successfully executed (*"./mimikatz.exe "sekurlsa::pth /user:chr.smilio /domain:SYSMON_SET /ntlm: eed224b4784bb040aab50b8856fe9f02""*). Finally, a new compromised command line was opened denoting the success of the whole process. *Mimikatz* extracted the NTLM hashing strings in a few minutes and cracked the targeted system's encrypted passwords in plaintext with brute-force techniques.

6.2.2. Pass the Ticket

As mentioned in Section 5.3, PtT is similar to PtH regarding Mimikatz's execution. The major difference between the two attacks is the duration of the access that is granted to the compromised host. PtT has a limited exploitation timeline, with Kerberos TGTs expiring after 10 hours of usage. On the other hand, PtH has an unlimited timeline as it is related to hashes that do not change on a frequent basis. PtT was executed with the same Mimikatz methodology that is presented for PtH in Section 5.2 up to the point of the successful acquisition of administrative privileges. All the Kerberos tickets were extracted with the *".kirbi"* extension in order to be used for the final exploitation of the Kerberos ticket client–server authentication procedure. Finally, the extracted ticket was *"passed"* with Mimikatz (*"./mimikatz.exe "kerberos::ptt ticket.kirbi"*) for the acquisition of remote access to the targeted server's *"/192.168.1.7/admin$"* folder.

6.2.3. Golden/Silver Ticket

As it concerns the GT attack, Mimikatz supports its execution toward the successful creation of a *"golden"* Kerberos ticket. For the needs of this work, and with reference to Figure 1 and Table 2, the *SYSMON_SET* domain's *"chr.smilio"* account of Client STA 3 was leveraged and exploited. As mentioned in Sections 5.4 and 5.5, this set of attacks is a combination of the already presented PtH and PtT attacks. For the creation of a GT to be successful, the exploitation of an extracted NTLM *"Krbtgt"* hash is a requirement, along with the domain's *Name*, the *SID*, and the *Username* of the targeted host. These four elements are combined with Mimikatz to successfully create the *"golden ticket"* (*"kerberos::golden /user:krbtgt /domain:SYSMON_SET /sid:S-1-5-21-902028059-194221605-2102066478 /krbtgt:d125e4f69c851529045ec95ca80fa37e /ticket: krbtgt.tck /ptt")* and allow the adversary to move laterally. All the submitted tickets after the execution of this attack were retrieved with the *"kerberos::list"* command. After the generation of the NTLM Hash for the *"Krbtgt"* account, Kerberos will perceive this TGT as trusted, enhancing its owner with administrative privileges and unlimited access to network facilities related to Kerberos authentication. It should be noted that the same procedure was followed during the creation of a forged TGS ticket and the exploitation of the related service. The only difference is in the use of the *PtT* parameters implemented during the ticket's production process to indicate the use of the *PtT* technique to produce the Silver ticket (*"kerberos::golden /domain:SYSMON_SET /sid:S-1-5-21-902028059-194221605-2102066478 /target:WIN-J23NIGGP1Q6.sysmon_set.lobal /service:cifs /rc4:1d86942baf284a38c97b63025fc8ccb8 /user: Administrator /ptt"*).

6.2.4. Discussion on Mimikatz-related Attacks

From an attacker's perspective, during PtH execution, a recognizable number of more than 1500 (or 2.5% of the total log file) *ProcessAccess* event logs (*Event ID 10*) were identified as the most pertinent to Mimikatz-related attacks of Section 6.2. Specifically, the aforesaid activity is related to the unauthorized access in the *Windows LSASS* process by the adversary with Mimikatz (as in this paper) or any other dumping tool of password and hashes. As shown in the fourth column of Table A2, the log activity analysis revealed a significant number of Sysmon's *"EventFields"* related to *Event ID 10* events. Specifically, *lsass.exe* (*"EventField: TargetImage"*) executable was the most prominent, with 600 out of 1,500 identified logs due to the repeated execution of the attack and exploitation of the *LSASS* process through *NTLM hash dumping*.

It is important to note that the identified activity of *LSASS* accessing was executed in parallel with an equal number of elevated privileges on access granting events, with *0x1010* and *0x1410* identifiers (*"EventField: GrantedAccess"*). The limited presence of three more *"GrantedAccess"* identifiers was also perceived, namely *0x1438(a)*, *0x1FFFFF* and *0x143a*, all scattered throughout 50 *Event ID 10* events out of the 600 logs. Above that, a number of ≈600 *mimikatz.exe* executable processes (*"EventField: SourceImage"*) with *"TargetProcessId"* equal to 492 were identified in combination with ≈200 powershell.exe and cmd.exe instances. Note that the aforesaid features in isolation do not guarantee the identification of PtH; however, in combination, they could be considered the springboard of the overall process of unveiling the *"sekurlsa"* module of the Mimikatz-related credential theft techniques presented in this section.

Overall, we consider that the application of the hitherto recognized *PtH-related* rule-based features is fully compatible to be extended in *PtT*, *GT*, and *ST* attacks. This conclusion emerges from the study of each attack's functionality presented in this section. Specifically, *PtH* is based on the successful extraction of *NTLM hashes*, which are used via the *"sekurlsa::pth"* module of Mimikatz to pass the hash and acquire a legit and stealth access to the targeted system. On the other hand, PtT is strongly related to the extraction of TGT tickets in *.kirbi* files, and their utilization of authenticating as a legitimate user. As in PtH, PtT also leverages Mimikatz's *"sekurlsa"* module to pass the ticket to the target. Moreover, the GT and ST techniques comprise both NTLM hash dumping techniques and TGT ticket forging for the creation of the migrated Golden and Silver passed tickets. Summing up, in terms of the common behavior and operation of the three aforementioned attacks, the rule-based policy proposed for the PtH attack finds scope in them as well.

Despite the vast existence of *ProcessAccess* events (*Event ID 10*) related to the abuse of the *lsass.exe* process, another 3200 events with *Event ID 1* (*ProcessCreation*), *ID 5* (*ProcessTermination*) and *ID 11* (*FileCreate*) stood out in the collected Sysmon's logs. Precisely, the events with *IDs 1* and *5* were exclusively related to Mimikatz's execution in the targeted system, either via *psexec* or *Metasploit*. On the other hand, events described with the *"FileCreate"* rule flag were captured by Sysmon during the extraction with Mimikatz of all the Kerberos tickets into a specified folder to be used for the final exploitation of Kerberos tickets in PtT, GT, and ST attacks. The identification of the *.kirbi* extension in the filenames (*EventField: TargetFilename*) of the extracted files is the most obvious indication of the existence of tickets related to the Kerberos protocol. Among the aforesaid 3200 logs, the majority (or ≈2400) was flagged by the *"TargetFilename"* rule. In addition, through Sysmon's log traffic observation, and due to the nature of the three executed Kerberos ticket attacks, the identified number of ≈360 *Event ID 11* (*FileCreate*) can be considered a strong indicator of the Kerberos *TGT* ticket exploitation of *.kirbi* extension files.

Moreover, the presented research was extended to identify extra features for each specified attack vector in isolation. Remotely executable tools were identified as applicable to the process of compromising the targeted server and the successful acquisition of administrative rights, namely *klist.exe*, *mimikatz.exe*, *lazagne.exe*, *psexec.exe*, *smb.exe*, as shown in Listing 2. These tools are strongly related to the extraction of *NTLM hashes* and *TGT tickets*, which follow the privilege escalation phase. Moreover, with reference to Listing 2, *klist.exe ProcessCreate* was included as one of the most obvious proofs of the execution of Kerberos tickets related to LM, namely PtH, PtT, GT, and ST. Specifically, *"klist.exe"* is an executable Windows command line that prints a list with the most recently cached Kerberos tickets. It should be noted that for *"klist"*, as for most aforesaid executables, administrative privileges come as a prerequisite.

```
<ProcessCreate onmatch="include">
  <CommandLine condition="contains">C:\Windows\system32\lsass.exe</CommandLine> <!--
       Possible indication for the execution of the Lateral Movement Skeleton Key
       Attack -->
  <CommandLine condition="contains">C:\Windows\system32\smb.exe</CommandLine>
  <ParentCommandLine condition="is">lazagne.exe windows</ParentCommandLine>
  <CommandLine condition="is">C:\Users\Administrator\mimikatz_trunk\x64\mimikatz.exe</
       CommandLine>
  <Image name="lsass ProcessCreate" condition="is">C:\Windows\system32\lsass.exe</
       Image>
  <Image name="svchost ProcessCreate" condition="is">C:\Windows\System32\svchost.exe</
       Image>
  <Image name="ProcessCreate" condition="end with">smb.exe</Image>
  <Image name="Mimikatz Execution" condition="is">C:\Users\Administrator\
       mimikatz_trunk\x64\mimikatz.exe</Image>
  <Image name="lazagne" condition="is">C:\Users\Administrator\Downloads\lazagne.exe</
       Image> <!-- The LaZagne project is an open source application used to retrieve
       lots of passwords stored on a local computer. -->
  <Image name="klist" condition="is">C:\Windows\System32\klist.exe</Image>
</ProcessCreate>
```

Listing 2. The lsass.exe "include" rule related to the executed tickets attacks.

As concerns privilege escalation techniques, *Event ID 1 ProcessCreate* rules were the most extensively identified during the execution of LM. Precisely, the *CommandLine EventFiels* presented in Listing 3, comprise the identification of *keylogging* or *keyboard capturing* (*"Get-Keystrokes"*), the capturing of screenshots from the targeted machine (*"Get-TimedScreenshot"*), and the extraction of cleartext credential Windows objects (*"Get-VaultCredential"*, *"Invoke-CredentialInjection"*). Further, the aforesaid executables refer to

PowerShell Windows modules, which can be executed during the target's enumeration and privilege escalation phases, within the context of a penetration test or a real-life LM.

In addition, the possibility of the execution of credential extraction and manipulation attacks via *PsExec* as an escalation of one of the aforementioned exploitations of remote services operations revealed the importance of *Event ID 3 NetworkConnection* and *Event ID 22 DNSEvent* (*DNS query*) events. Regarding the former, 150 logs were collected as related to successful remote connections via the RDP protocol (*"C:/Windows/PSEXESVC.exe" (EventField: Image)"*) and also associated with the source and destination IP addresses of the attacker's machine and the targeted server host, respectively (SourceIp: 192.168.1.11, DestinationIp: 192.168.1.8, as presented in Table 2). Regarding *DNSEvents*, 80 logs were collected by *Sysmon* with *"EventField: Image:.../PSEXEC.exe"* and *"QueryName: sysmon_set"* as the domain's name, all revealing potential domain exfiltration for stored hashes and passwords with Mimikatz.

```xml
<ProcessCreate onmatch="include">
  <CommandLine name="Privilege Escalation" condition="contains">Get-Keystrokes</
      CommandLine> <!-- keylogging or keyboard capturing, is the action of logging
      keys pressed, time and the active window. -->
  <CommandLine name="Privilege Escalation" condition="contains">Get-TimedScreenshot</
      CommandLine> <!-- Takes screenshots and saves them to a folder, with a
      timestamp to reveal the time and date of the screenshot. -->
  <CommandLine name="Privilege Escalation" condition="contains">Get-VaultCredential</
      CommandLine> <!-- Displays Windows vault credential objects including cleartext
       web credentials. -->
  <CommandLine name="Privilege Escalation" condition="contains">Invoke-
      CredentialInjection</CommandLine> <!-- Displays Windows vault credential
      objects including cleartext web credentials. -->
  <CommandLine name="Privilege Escalation" condition="contains">mimikatz</CommandLine>
       <!-- Mimikatz is an open-source application that allows users to view and save
       Kerberos tickets and hashes. -->
</ProcessCreate>
```

Listing 3. Privilege escalation ProcessCreate rules.

To make the collected features as generic as possible, two more interventions were implemented in the targeted server. The former is related to the activation of the *"WDigest"* authentication and the latter with enabling *"Manages Microsoft Base Smart Card Crypto"* capability. As it concerns *WDigest*, if enabled, it forces *lsass.exe* to store on the system's memory user-related passwords in plaintext form. On the other hand, when *Smart Card Crypto* capability is enabled, it makes *LSASS* store the NT hash dedicated to each user along with the unique key of the card itself. Both events were captured by *Sysmon* as *Event ID 13* (*RegistryEvent (Value Set)*), with *"Image: C://WINDOWS//regedit.exe"* and *"TargetObject: HKLM/SYSTEM/CurrentControlSet/Control/SecurityProviders/WDigest"*, *"TargetObject: HKLM/SOFTWARE/Microsoft/Cryptography/Defaults/Provider/Microsoft Base Smart Card Crypto Provider"*, respectively.

Many rules have also been *excluded*, meaning that they were filtered continuously until their rule was matched. Most of the time, these are common Windows OS processes that should be excluded to avoid causing unwanted noise to the Sysmon event filtering.

Mimikatz's DLL Analysis: In addition to the *rule-based EDR* policy proposed, log analysis was taken further to the identification of the DDL information that was transferred during the Mimikatz execution. The captured DLLs were included within the collected 60,000 Sysmon logs that were taken during the extraction of the NTLM hashes, the exploitation of PtH, PtT, GT, and ST attacks. According to the authors in [10], even though adversaries tend to rename or even rebuild malicious applications such as Mimikatz, the existence of legitimate DLLs, which are loaded together with the aforesaid tool, may give great insight regarding the uniqueness of the DLL relationship between distinct editions of Mimikatz and Windows OS, leading eventually to a robust and effective proactive identification of LM.

Specifically, 3500 *DLL files* (≈ 6% of the total log record corpus) were identified over the 60,000 logs; however, only 460 of them (≈13%) were related to *Mimikatz*. More precisely, 14 different DLL information files were identified, whereas only 9 (64%) are referenced by the related work so far r [10], as follows:

- *DLLs identified in both this paper and [10]*: cryptbase.dll, imm32.dll, kernel32.dll, msctf.dll, ntdll.dll, sechost.dll, shell32.dll , user32.dll, wininet.dll
- *DLLs identified only in this paper*: cryptdll.dll, hid.dll, samlib.dll, vaultcli.dll, WinSCard.dll

We argue that future work on the subject of EDR will evolve the presented rule-based policy and list of the *Mimikatz*-related DLL files into a signature-driven deep-learning-driven IDS solution. Tables A1 and A2 summarize the most important rule-based features of Sections 6.1 and 6.2 as they emerged from the conducted experiments and the extended DLL analysis.

6.2.5. Post Exploitation on Stored Passwords with LaZagne Project

The execution of this attack started at the end of the previously presented exploitation of the *smb_login* vulnerability of the Windows Server with Metasploit and the successful acquisition of the meterpreter session of the targeted host, presented in Section 6.1. The *lazange.exe* tool was remotely uploaded and executed on the targeted host's *"/Downloads"* folder through the command line utility with administrative rights. After several attempts, a great variety of usernames and passwords were collected, namely mail, Git repository credentials, Windows domain passwords, sysadmin, browser-stored credentials and passwords loaded on the random access memory of the targeted host.

6.2.6. Discussion upon Password Exploitation with LaZagne Project

With reference to the LaZagne Project password stealing attack, *ParentImage="C:/Users/ /Administrator/.../lazagne.exe"* was included to outline the execution of the password spoofing LM attack with the use of the popular penetration framework *LaZagne Project*. The rule was enhanced with various extra *"ParentCommandLine"* features in an attempt to capture all the possible password stealing attempts from the targeted server's client *windows accounts*, *sysadmin*, *mail*, *databases etc.*, as presented in Listing 4.

```
<ProcessCreate onmatch="include">
   <ParentImage condition="is">C:\Users\Administrator\Downloads\lazagne.exe</
        ParentImage>
   <ParentCommandLine condition="is">lazagne.exe windows</ParentCommandLine>
   <ParentCommandLine condition="is"> lazagne.exe mails</ParentCommandLine>
   <ParentCommandLine condition="is"> lazagne.exe project all</ParentCommandLine>
</ProcessCreate>
```

Listing 4. The lazagne.exe password spoofing.

7. Python_Evtx_Analyzer

The analysis of large log files is always a demanding procedure for incident response teams struggling with shortages of computational power to manipulate the millions of logs produced on a daily basis. Despite the variety in propriety and open-source Security Information and Event Management (SIEM) solutions for centralized logging and analyzing activities, most of them require multi-step procedures regarding log parsing, event analyzing, exception handling, and monitoring parameter initialization. That is, the literature lacks a lightweight and easily configurable tool that can be used to automate the parsing and threat analysis of extended *.evtx* log sets. To cover this need, this section presents and evaluates an analytical Python scripting tool dubbed *"Python_Evtx_Analyzer" (PeX)*, which caters to the analysis of voluminous Sysmon logs and, therefore, contributes to the identification of LM events in a timely manner.

From a bird's eye view, *PeX* was developed to serve as a proof of concept for the proposed rule-based policy's efficiency discussed in Section 6. Towards this goal, the optimization of Sysmon's logging activity is concentrated on filtering the least unwanted *noise* possible and being as targeted as possible to LM. Simply put, the essence of *PeX's* operation is to provide a portable and OS-independent command line (or IDE executable) tool that helps EDR teams analyze massive *.evtx* logs and successfully identify LM. It should be noted that *PeX's* events identification is based on LM-oriented features that were extracted from Sysmon's pre-configured rules in the enclosed config.xml file, as presented in Appendices A.1 and A.2. What makes *PeX* special is its ability to be fully customizable by incident response researching teams to analyze and identify any kind of logging activity captured by Sysmon, either normal or malicious. As a result, *PeX* can be used in the context of other researchers in this timely field as it is made publicly available as open source in [2].

In brief, the analyzer has dependencies on six Python libraries, namely *mmap*, *argparse*, *minidom*, *evtx.Evtx*, *evtx.Views* and *ElementTree)*, which should either be imported during the building of the IDE project or installed to the OS prior to the code execution with the terminal. It allows the following functions:

- Memory mapping of massive Sysmon log files as inputs in .evtx form.
- Provision of basic arguments supporting a user-friendly command-line execution of the Python script's source code.
- Parsing and transformation of the logs included in the *.evtx* file into an easily manipulated and analyzed *.xml* format.
- Custom header filtering of the *.xml* created file. This is based on pre-selected Sysmon's Event ID tags, presented in tree-based form on the command line's screen or stored externally to a *.txt* file.
- Manipulation of the tree-based *.xml* structure and filtering based on pre-configured features as enclosed in Sysmon's *config.xml*.
- Enumeration of the identified LM events, alert message generation per attack denoting the number of identified malicious events and making an assumption of the type of potentially executed attack.

From an OS version's perspective, the analyzer can run on all mainstream platforms, including *Windows 10*, *MacOS Big Sur v11.6.5* and *Ubuntu v22.04*.

7.1. PeX Operation

With all the prerequisite libraries imported, the main function's statements (*Function (def python_Evtx_Analyzer (-f , -i, -o) :)*) are executed, revealing their potential, as presented in Algorithm 1. The latter describes the procedures of the input folder identification, *.evtx* files insertion, the output folder creation, and the buffering of the *.evtx* log headers in an algorithmic pseudocode format. Note that Algorithm 1 is implemented in conjunction with Algorithms 2 and 3 and run as a single Python script.

At first, the necessary arguments of input folder (*-f*), the ID of the *evtx* file (*-i*) and the optional output folder (*-o*) are imported and parsed via *Argparse* into the (*"evtxAnalyzer"*) variable. Next, the existence of the *outputfolder* variable is checked if it is set to true, and outputfolder is opened with the append (a+) permission. If set to false, the analyzer proceeds with terminal standard output, as presented in ll.6-7 of Algorithm 1.

The input folder contents are mapped via the *Memory Mapped file support (mmap)* library and stored in the *evtxBuffer* to be set as input in the *evtx.Evtx FileHeader()* function. The buffered logs are enumerated based on their tag headers to be finally stored in the *fileheader* variable. Recall that the *mmap* is a Python library, which allows the manipulation through mapping of various input and output (I/O) file objects. The *fileheader* variable is manipulated as a collection of *xml* objects through the *evtx.Views* library to eventually store the parsed headers to the *xmlToStr* variable. The collected *xml* entries of the *xmlToStr* object are parsed via the *Minidom* Python library, called *Minimal DOM*, based on <*Event ID*> *tags* and stored in the *xmlToDoc* variable, as presented in Algorithm 2 (ll. 3).

Algorithm 1 PeX's arguments and folders initialization algorithm

```
Require: python $setup.py$ install
Require: pip install $mmap$, $argparse$, $minidom - ext$, $python - evtx$ libraries
Require: import $mmap$, $argparse$, $minidom$ $(from\ xml.dom)$, $evtx.Evtx.FileHeader$, $evtx.Views$,
    $xml.etree.ElementTree$
Require: $data$, $Sysmon$ files in $.evtx$ format
Require: Function def $python\_Evtx\_Analyzer(-f, -i, -o)$ :
    $evtxAnalyzer \leftarrow data[str][--iFolder, --evtxId, --outputFolder]$
    $arguments \leftarrow data[str][evtxAnalyzer.parse\_args()]$
 3: $outputFolder \leftarrow data[Boolean][False]$
    if $arguments.outputFolder \neq None$ then
        $outputFolder \leftarrow append("+a")permissions$
 6: else if $arguments.outputFolder == None$ then
        $return 0$
    end if
 9: for $arguments.ifolder \leftarrow read("r")permissions$ do
        $evtxBuffer \leftarrow read("r")permissions$
        $evtxBuffer \leftarrow data[Sysmon.evtxfiles][mmap.mmap(ifolder)]$
12:     $fileheader \leftarrow data[evtxBuffer][evtx.Evtx.FileHeader(evtxBuffer)]$
        $xmlHeaderOutput \leftarrow data[fileheader]$    ▷ The header of every xml file is stored to the
    xmlHeaderOutput variable.
        if $outputFolder == True$ then
15:         $outputFolder \leftarrow data[xmlHeaderOutput]$
        else if $outputFolder == False$ then
            $print(xmlHeaderOutput)$
18:     end if
    end for
```

Algorithm 2 PeX's evtx-to-xml transformation algorithm

```
    for $xmlToStr \leftarrow in[evtx.Views][fileheader]$ do
        $xmlToDoc \leftarrow [minidom.parseString][xmlToStr]$
 3:     $eventsByID \leftarrow [getElementsByTagName][xmlToDoc]$
    end for
    if $arguments.id == "all"$ then
 6:     if $outputFolder$ then
            $outputFolder \leftarrow data[xmlToDoc]$
        else if $arguments.outputFolder == None$ then
 9:         $cmd(Terminal) \leftarrow data[xmlToDoc]$
        end if
    else if $eventsByID == arguments.id$ then
12:     if $outputFolder$ then
            $outputFolder \leftarrow data[xmlToDoc]$
        else if $arguments.outputFolder == None$ then
15:         $cmd(Terminal) \leftarrow data[xmlToDoc]$
        end if
    end if
```

The *ElementTree* module is combined with the "for tag in doc.findall("Name"):" loop and the desired pre-selected filtering features per attack, as presented in Algorithm 3 (ll. 3). The selected per-attack case filters are iterated over a loop against the provided .evtx input file. The existence of each filter is counted and stored as a *"countVar"* variable. With the completion of the enumeration and filtering of the suspicious log file, the analyzer prints two different messages to the user depending on the existence or not of suspicious network log traffic. In the case of the attack's existence, the printed message is combined with the *"countVar"* variable to demonstrate the total number of identified packets. The results are summarized in a final report that is printed at the end of the analyzer's execution.

Algorithm 3 PeX's xml parsing and LM identification algorithm

```
    $counter == 0$
    $doc \leftarrow [ElementTree][xmlToStr]$
 3: for $tag \leftarrow [doc][findall("Name")]$ do
        if $tag \leftarrow [attrib][SysmonEventIDField] == "PreselectedValue\_01"$ or $tag \leftarrow [attrib][SysmonEventIDField] == "PreselectedValue\_02"$ then
            $doc \leftarrow [remove][tag]$
 6:     end if
        $print \leftarrow [ElementTree][doc]$
    end for
 9: for $countVar \leftarrow [xmlToStr][count("PreselectedValue")]$ do
        if $countVar >= 1$ then
            $counter++$
12:         $print \leftarrow [counter][Windows\_terminal\_Alert\_Message.]$
        end if
        $print \leftarrow [ElementTree][doc]$
15: end for
    $print \leftarrow [Analyzer\_Final\_Report][doc]$
    $evtxBuffer \leftarrow [close()]$
18: $return$
```

7.2. Dataset

PeX was evaluated over a 10-day dataset regarding the analyzer's detection and alert rates. Those are processed as attack-related fractions based on the detected rule-based logs, along with the False Positive (FP) and False Negative (FN) alert messages it generates. The collected data contain normal and malicious logs generated from the continuous interaction with the constituent systems of the SOHO network in Figure 1. Specifically, the nine LM attacks of Section 6 were re-executed multiple times over the 10-day period and mixed with legitimate user activity upon the targeted SOHO network. The legitimate traffic includes the captured logs of the first day, consisting basically of user logins and system logouts, web browser usage and Internet surfing, file sharing among the various stations of the network, email traffic and various social media account logins and user interactions with each of the six client stations included in Table 2. For reasons of reproducibility, but also for advancing research efforts in this area, the resulting dataset is publicly offered at [2].

Regarding the malicious traffic generated, the three variants of the *Exploitation of Remote Services* LM methodology were executed continuously for the first three days in a row, simultaneously with the normal utilization network traffic. The next four days were devoted to the execution of the *Credential Exploitation Hashing Attacks*. Finally, the last two days of the 10-day testing period were concentrated on a mixed repetition of the aforesaid attacks, leading to the creation of an ≈870,000 log dataset of Sysmon *.evtx* files. It should be noted that each day represents 3 to 6 h of continuous capturing of network logs activity and not a whole 24 h.

7.3. Evaluation

As a proof of concept, *Pex* was implemented with Python 3 on a VM Linux machine with 16 GB of RAM and a quad-core processor. As presented in Table 4, four different subsets of the pre-collected logs were extracted, namely, *Normal* (or ≈80,000 Event IDs), *NormalVsMalicious01* (or ≈290,000 Event IDs), *NormalVsMalicious02* (or ≈415,000 Event IDs) and *FullSet* (or ≈870,000 Event IDs). Table 5 summarizes the total number of tests that were conducted with *PeX* per attack and subset, including the number of logs and TP/FP rates. All the experiments were performed using the extended rule-based filtering mode presented in Appendices A.1 and A.2.

Indicatively, *Pex* took an average analyzing time of ≈15 min and 14 s of CPU time regarding the first three subsets of Table 4. As it concerns the *FullSet*, the analyzer took an average of 16 min and 22 s. This is translated to an increase of ≈7.13% vis-à-vis the average processing and analysis time that was perceived for the first three subsets of Table 4.

Regarding the conducted experiments, *PeX* successfully achieved an average detection rate above 90%, as it concerns the summed percentage of TP and FN identified incidents per subset. On the other hand, during each *.evtx* subset analysis, *PeX* generated a mean rate of ≈10% *FP* and ≈1.5% *FN* misidentification incidents, respectively.

Table 4. Subsets examined with *PeX*, including the total number of *.evtx* logs per subset.

Tested Subsets	Sysmon Event IDs (Logs)
Normal	≈80,000
NormalVsMalicious01	≈290,000
NormalVsMalicious02	≈415,000
FullSet	≈870,000

PeX evaluation started with the *Normal* subset and was examined under the proposed rule-based policy of Appendices A.1 and A.2. First, the logs were tested against the proposed rule-based filtering features without the implementation of the identified Mimikatz's *".dll"* rules given in Section 6.2.4. As depicted in Table 5, *PeX* successfully identified 70,641 Event ID logs (or else 88% TP rate) related to normal network traffic, plus another ≈2000 logs revealing 2.5% of TN results. Overall, it achieved a score of 90.5% regarding the identification of *Normal* network traffic, as the sum of TP and TN rates. On the other hand, the analyzer misidentified 7224 logs as malicious, revealing a tendency of 9% on FP events regarding the *"Normal"* subset. The majority of FP events are related to the fictitious presence of Mimikatz's *ProcessCreate Event IDs*, specifically the logs with *TargetImages: "C:/Windows/System32/lsass.exe, services.exe, reg.exe, svchost.exe"* and *GrandedAccess: "0x1010, 0x1410"*.

Table 5. Total number of tests performed with *PeX* per attack and subset, including FP and TP percentages.

Attack Vector	Subset	No. of Logs	TP (%)	TN (%)	FP (%)	FN (%)
Normal Network Traffic	*Normal*	80,274	88.0%	2.5%	9.0%	1.5%
Remote Services Exploitation + Normal Net Traffic	*NormalVsMalicious01*	293,520	85.4%	5.3%	8.0%	1.3%
Hashing Pass Exploitation + Normal Net Traffic	*NormalVsMalicious02*	416,029	83.5%	3.3%	11.5%	1.7%
Total Attacking Vector + Normal Net Traffic	*FullSet*	870,119	84.6%	2.4%	11.6%	1.4%

On the positive side, despite the initial concerns that a FP rate of ≈10% may arise, this figure falls under 1.5% (1.35% precisely) when combined with the *".dll"* related rules of Section 6.2.4. The aforesaid percentage, if examined in conjunction with the 1.5% of the fourth column's FN events, it is statistically acceptable for the operational nature of a parsing and analysis tool. The reader should keep in mind that the FN events presented in Table 5 are related to Sysmon's rules that were generated and implemented in *config.xml* file for ignoring any unwanted noise within the event filtering procedure.

Regarding the *NormalVsMalicious01* subset, which comprises logs related to the experiments of Section 6.1, *PeX* successfully identified 250,666 (or 85.4%) TP logs as potentially malicious or normal, together with 15,556 (or 5.3%) more TN Event IDs. The same promising rates regarding TP and FP logs were also identified during the evaluation of the *NormalVsMalicious02* subset of password hashing Exploitation attacks of Section 6.2. Precisely, 83.5% (or 347,384 logs) of the collected logs was successfully identified, while another 3.3% (or 13,728 logs) was also flagged correctly as TN.

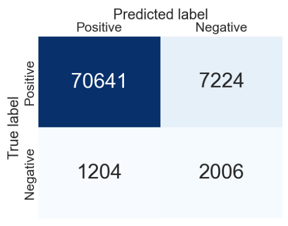
With reference to the penultimate column of Table 5, FP presented an average of 9.75% on both the *NormaVsMalicious* subsets. In more detail, *PeX* recognized 23,481 (or 8%) and 47,843 (or 11.5%) logs incorrectly per *NormaVsMalicious* subset, respectively. It is noteworthy that most of the misclassified logs of both subsets were related to Mimikatz extracted log files. For this reason, these records were re-evaluated under the implementation of the *.dll ParentImage* signatures of Section 6.2.4, reducing erroneous FP rates by 1.9% and 2.3% for each subset, as presented in Table 6, respectively. Regarding the identified FNs per subset, the records of Table 6 do not exceed 1.6%, a fact that, within the context of this work, is deemed acceptable.

Table 6. Total number of tests performed with *PeX* per attack and subset, including FP and TP percentages. The evaluation of the depicted logs was executed under the extended rule-based policy, including the *".dll"* analysis of Section 6.2.4.

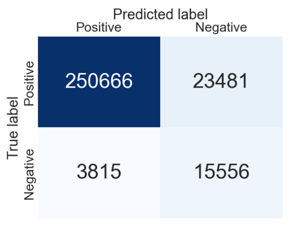
Subset	No. of Logs	TP (%)	TN (%)	FP (%)	FN (%)
Normal	80,274	89.63%	7.60%	1.35%	1.42%
NormalVsMalicious01	293,520	88.65%	8.20%	1.90%	1.25%
NormalVsMalicious02	416,029	88.25%	7.85%	2.30%	1.60%
FullSet	870,119	88.55%	7.90%	2.20%	1.35%

No less important, *PeX* was tested against the extended *FullSet* dataset, which comprises the three pre-selected log records of Table 5 plus the events of the last two days of the 10-day period testing. The final evaluation of the analyzer was conducted under the eventually configured rule-based policy, including the *".dll"* filtering parameters. Table 5 presents *PeX* scoring without the inclusion of the *.dll* Event ID's fields, while Table 6 contains the re-evaluated log values under the enhanced rule-based policy.

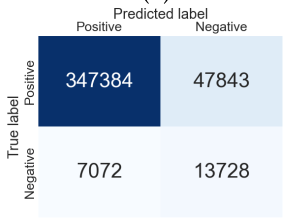
Last but not least, the confusion matrices presented in Figures 4 and 5 demonstrate, in a log-oriented form, the evaluation percentages of Tables 5 and 6, namely TP, TN, FP, FN rates, for *PeX's* execution per technique and subset.



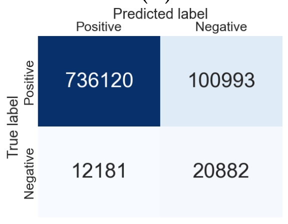
(**a**)



(**b**)

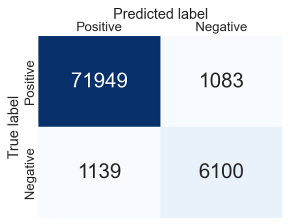


(**c**)

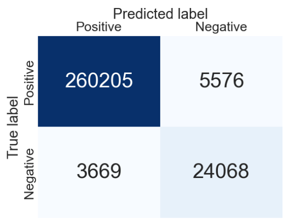


(**d**)

Figure 4. Confusion matrices for the evaluation percentages presented in Table 5, namely TP, TN, FP, FN rates, for *PeX's* execution per technique and subset. (**a**) Normal Subset; (**b**) NormalVsMalicious01 Subset; (**c**) NormalVsMalicious02 Subset; (**d**) FullSet Subset.

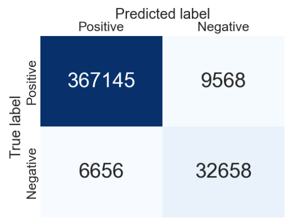


(**a**)

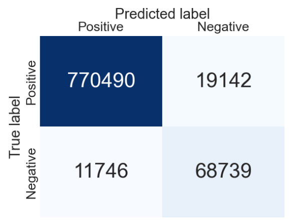


(**b**)

Figure 5. *Cont*.



(**c**)



(**d**)

Figure 5. Confusion matrices for the evaluation percentages presented in Table 6, namely TP, TN, FP, FN rates, for *PeX's* execution per technique and subset; (**a**) Normal Subset; (**b**) NormalVsMalicious01 Subset; (**c**) NormalVsMalicious02 Subset; (**d**) FullSet Subset.

8. Conclusions

In recent years, many organizations have suffered damages as a result of targeted LM. As it becomes apparent, the tasks of incidence response teams to further address such damages acquire significant weight. Many penetration testing tools leave no concrete evidence regarding their execution when filtered with Sysmon's default settings, leaving several data exfiltration incidents unsolved. In this context, the current study aspires to set the stage for a fresh EDR rule-based policy regarding Sysmon identification and alerting of LM events. In addition, a publicly available Python tool, namely *PeX* is implemented, giving greater insight in terms of understanding the mechanisms that fall under LM methods.

As an extension of the work conducted on this topic so far, the ultimate goal of the current work is the collection and investigation of evidential logs related to LM attacks. In short, the effort is concentrated on the creation of custom filtering Sysmon rules, along with the initialization of Sysmon's config.xml file specifically oriented towards the alerting of LM. The conducted analysis suggests two different sets of Sysmon rules, as presented in Appendices A.1 and A.2, one for each of the Exploitation of Remote Services and Credential Exploitation attack experiments, respectively. The adoption of the aforementioned rules comes as a direct result of the thorough network traffic and pattern study, as derived from the execution of each attack.

With reference to the conducted experiments, the proposed rule-based approach was incorporated with Sysmon in the form of the *config.xml* file, presenting an identification TP rate above ≈95%. Finally, yet importantly, the proposed EDR policy, including the *.dll* analysis of Section 6.2.4, was imported and evaluated through *PeX* against four subsets, revealing a tendency above ≈96% in terms of the TP and TN metrics. The combination of the proposed EDR policy with machine learning techniques may reveal its importance as the basis for the creation of an LM-oriented IDS solution. Nevertheless, a thorough investigation of this potential is well beyond the scope of this paper and is left for future work.

Author Contributions: Conceptualization, C.S., K.B. and G.K.; methodology, C.S., K.B. and G.K.; validation, C.S., K.B. and G.K.; formal analysis, C.S. and G.K.; investigation, C.S., K.B. and G.K.; writing—original draft preparation, C.S.; writing—review and editing, C.S., K.B. and G.K.; supervision, G.K. and K.B.; project administration, C.S. G.K.. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement:

The "Python_Evtx_Analyzer (PeX)" tool along with the large dataset of Sysmon logs collected during the experiments are made publicly available to the community for download at https://github.com/ChristosSmiliotopoulos/Python_Evtx_Analyzer.git.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

5Ws	Who-When-Where-What-Why
Argparse	Argument Parser Python Library
API	Application Programming Interface
ARP	Address Resolution Protocol
CMD	Command Line
CME	CrackMapExec
CSIRT	Computer Security Incident Response Team
CSV	Comma-Separated Values
DLL	Dynamic Link Library
DOM	Document Object Model Interface
Domain SID	Domain Security Identifier
EDR System	Endpoint Detection and Response System
Event ID	Event Identification
evtx	Windows XML EventLog
FN	False Negative
FP	False Positive
GUID	Global Unique Identifier
I/O	Input/Output
IDE	Integrated Development Environment
IDS	Intrusion Detection System
IP	Internet Protocol
KDC	Kerberos Key Distribution Center
klist	Kerberos List
LSASS	Local Security Authority Subsystem Service
LTS	Long Time Support
MAC Address	Media Access Control Address
MMAP	Memory Mapped File Support Python Library
MSTSC	Microsoft Terminal Services Client
NMAP	Network Mapper
NTLM	Network Lan Manager
PeX	Python_Evtx_Analyzer
PtH	Pass the Hash
PtT	Pass the Ticket
RAM	Random Access Memory
RDP	Remote Desktop Protocol
SIEM	Security Information and Event Management
SMB	Service Message Block
SOHO	Small Office Home Office
STA	Station
Sysmon	System Monitoring
TN	True Negative
TP	True Positive
UAC	User Account Control
USB	Universal Serial Bus
VM	Virtual Machine
WIDS	Wireless Intrusion Detection Systems
Wi-Fi	Wireless Fidelity
xml	Extensible Markup Language

Appendix A

Appendix A.1

Table A1. Summary of the most important rule-based features included in Section 6.1. The imported superscripts are described as follows: Number 1 of the first column denotes Microsoft's vulnerability with code MS-17-010 "EternalChampion SMB Remote Command Execution", Number 2 indicates Impacket Python scripts exploitation, Number 3 is related to "Escalation to SYSTEM privilege with Metasploit smb_login exploitation", Number 4 presents UAC bypass–privilege escalation with smbexec.py, Number 5 is the exploitation of the EternalBlue vulnerability on SMB file-sharing services, and Number 6 demonstrates BlueKeep RDP misconfiguration most related features.

Tool	Tool Attack Utilization	COM Port	Sysmon-Event Log
^{1,2} PsExec	Remote command execution on clients and servers within a domain.	135/tcp, 445/tcp, or a random high port	**Event IDs 1,5** (ProcessCreate, ProcessTerminate), **path:** "%SystemRoot%/PSEXESVC.exe", **Images:** "C:/Windows/PSEXESVC.exe", "C:/Windows/services.exe", "C:/Windows/wmiprsv.exe" User: "SYSTEM", **Additional Info:** date, UtcTime the "Image: "C:/Windows/PSEXESVC.exe" was executed".
^{1,2} WinRM	Target enumeration-investigation on the remote host via command execution.	5985/tcp (HTTP) or 5986/tcp (HTTPS)	**Event IDs 1,5** (ProcessCreate, ProcessTerminate), **Images:** "C:/Windows/System32/cscript.exe", "C:/Windows/System32/svchost.exe", "C:/Windows/System32/wsmprovhost.exe" "C:/Windows/System32/mmc.exe" **Additional Info:** ProcessID, UtcTime, CommandLine, User.
^{2,4} smbexec	Execution of applications that are normally controlled by the bypassed User Account Control (UAC) as a user with administrator privileges.	-	**Event IDs 1,5** (ProcessCreate, ProcessTerminate), **Images:** "C:/Windows/System32/smbexec.py", "C:/Windows/System32/sdbinst.py" User: "SYSTEM", **Additional Info:** "Process Start/End Time and Date (UTC), Process CommandLine, ProcessID, SDB File Used".
^{1,2} smb_login (Metasploit)	Privilege Escalation within host or domain.	445/tcp	**Event IDs 1,5** (ProcessCreate, ProcessTerminate), **path:** "%SystemRoot%/PSEXESVC.exe", **Images:** "C:/Windows/PSEXESVC.exe", "C:/Windows/System32/cmd.exe", "C:/Windows/System32/powershell.exe", "C:/Windows/System32/net.exe", "C:/Windows/System32/whoami.exe" , **Additional Info:** Administrative privileges "//*/IPC$", "//*/admin$", "//*/c$" Images - CommandLine-CurrentDirectory-Hashes-ParentImage-ParentCommandLine related to net.exe and whoami.exe.
^{5} Wannacry malware	Malware infection to leverage MS17-010 EternalBlue vulnerability on SMB file-sharing services.	139/tcp, 445/tcp, 137–138/udp	**Event IDs 1,2,5** (ProcessCreate, ProcessChange, ProcessTerminate), **path:** "%SystemRoot%/Wcry.exe", "%SystemRoot%/taskce.exe" **Images:** "C:/Windows/Users/Desktop/Wcry.exe", "C:/Windows/Users/Desktop/tasksche.exe", "C:/Windows/Users/Desktop/r.wnry.exe", "C:/Windows/Users/Desktop/s.wnry.exe", "C:/Windows/Users/Desktop/t.wnry.exe", "C:/Windows/Users/Desktop/u.wnry.exe", "C:/Windows/Users/Desktop/taskse.exe", "C:/Windows/Users/Desktop/taskdl.exe", "C:/.../attrib.exe", "C:/.../icacls.exe" **Additional Info: ProcessID:** 3024, Files with extension ".WNCRYT" or "C://Users//...//Desktop//Eula.txt.WNCRYT" objects which denote ransomware's expansion, **CommandLine:** "attrib +h", "icacls . /grant Everyone:F /T /C /Q".

Table A1. *Cont.*

Tool	Tool Attack Utilization	COM Port	Sysmon-Event Log
[6] BlueKeep (CVE-2019-0708)	Worm-like (Wannacry similiral) cybersecurity vulnerability of Windows Remote Desktop Protocol (RDP) and Services (RDS) which allows the remote execution of arbitrary malicious code.	3389/tcp	**Event IDs 1,2,5** (ProcessCreate, ProcessChange, ProcessTerminate) as in [1–5], **Event ID 3** (NetworkConnection), **path:** "%SystemRoot%/", **Images:** "C:/Windows/System32/rdpv.exe", "C:/Windows/System32/mstsc.exe", "C:/Windows/System32/RTSApp.exe", "C:/Windows/System32/ws_TunnelService.exe.exe", "C:/Windows/System32/RemoteDesktopManagerFree.exe", "C:/Windows/System32/RemoteDesktopManager.exe", "C:/Windows/System32/RemoteDesktopManager64.exe", "C:/Windows/System32/mRemote.exe", "C:/Windows/System32/Terminals.exe", "C:/Windows/System32/spiceworks-finder.exe", "C:/Windows/System32/thor.exe", "C:/Windows/System32/thor64.exe", "C:/Windows/System32/reg.exe", "C:/Windows/System32/chrome.exe" **Sysmon's Additional Info:** Administrative privileges "//*/IPC$", "//*/admin$", "//*/c$", Images-CommandLine-CurrentDirectory - Hashes-ParentImage-ParentCommandLine-ProcessID-UtcTime, User related to the identified **Images**.

Appendix A.2

Table A2. Summary of the most important rule-based features included in Section 6.2. The imported superscripts are described as follows: Number 1 presents the most significant features of the PtH attack, Number 2 , Number 3–5 are dedicated to the description of the Pass-the-Ticket (PtT), Golden and Silver Tickets attacks, Number 5 presents LaZagne Project-related features regarding Windows password compromise, and Number 6 is related to the Privilege Escalation and enumeration procedure.

Tool	Tool Attack Utilization	COM Port	Sysmon-Event Log
[1] PtH (PowerShell Invoke-Mimikatz)	Credential theft and Lateral Movement technique in which the adversary leverages Windows NTLM hash without cracking it to authenticate as legit.	445/tcp	**Event IDs 1,2,5** (ProcessCreate, ProcessChange, ProcessTerminate) as in [1–6] of Table A1, **Event ID 3** (NetworkConnection), **Event ID 10** (ProcessAccess), **Event ID 11** (FileCreate), **Event ID 22** (DNSEvent (DNS query)), **Event ID 13** (RegistryEvent (Value Set)), **path:** "%SystemRoot%/", "%SystemRoot%/PSEXESVC.exe", **ParentImage:** "C:/Users/Administrator/Desktop/mimikatz_trunk /x64/mimikatz.exe", "C:/Windows/system32/sppsvc.exe" **TargetImage:** "C:/Windows/System32/lsass.exe", "C:/Windows/System32/lsass.exe", "C:/Windows/System32/reg.exe", "C:/Windows/System32/svchost.exe", "C:/Windows/PSEXESVC.exe", "C:/Windows/services.exe", "C:/Windows/wmiprsv.exe" **GrantedAccess:** "0 × 1010", "0 × 1410", "×1438", "×1438a", "0 × 1FFFFF", "0 × 143a", **CommandLine:** "sekurlsa", "mimikatz", "reg SAVE", "dumpcr", **Sysmon's Additional Info:** Administrative privileges "//*/IPC$", "//*/admin$", "//*/c$", Images-CommandLine-CurrentDirectory-Hashes-ParentImage-ParentCommandLine-ProcessID-UtcTime, User related to the identified **Images**, TargetFilename: "C:/Users/Administrator/Desktop/.../filename.kirbi", DNS QueryName: "sysmon_set (or the desired name of the targeted domain)"

Table A2. *Cont.*

Tool	Tool Attack Utilization	COM Port	Sysmon-Event Log
[2] PtT, [3] Golden Ticket, [4] Silver Ticket	Capturing the Domain Administrator Privilege and Account Credentials. Leverages an unauthorized Kerberos ticket that is valid for an arbitrary period and grants access without additional authentication.	445/tcp	**Event IDs 1,2,5** (ProcessCreate, ProcessChange, ProcessTerminate), **Event ID 3** (NetworkConnection), **Event ID 10** (ProcessAccess), **Event ID 11** (FileCreate), **Event ID 22** (DNSEvent (DNS query)), **Event ID 13** (RegistryEvent (Value Set)), **path:** "%System-Root%/","%SystemRoot%/PSEXESVC.exe", as in [1–7] of Table A1, **ParentImage:** as in [1–7], plus, C:/Windows/System32/klist.exe, C:/Windows/mimikatz.exe, "C:/Windows/PSEXESVC.exe", **CommandLine:** "sekurlsa", "mimikatz", "reg SAVE", "dumpcr", "Get-Keystrokes", "Get-TimedScreenshot", "Get-VaultCredential", "Invoke-CredentialInjection", "Invoke-CredentialInjection"
[5] LaZagne	Open source application used for passwords exploitation which are stored on a local targeted host.	3389/tcp	**Event IDs 1,2,5** (ProcessCreate, ProcessChange, ProcessTerminate), **Event ID 10** (ProcessAccess), **path:** "%System-Root%/","%SystemRoot%/PSEXESVC.exe", **ParentImage:** "C:/Windows/System32/lazagne.exe", **CommandLine:** "lazagne.exe windows", "... sysadmin, mail, project mail, project databases, project windows, project all"
[6] Privilege Escalation	The basis of each Lateral Movement attack. Target acquisition, weak points enumeration, access gained within the security perimeter of a domain, gradual escalation of privileges and extension of the Lateral Movement of the adversary.	80, 53, 25, 110, 143, 139, 445, 3389, 6000/TCP	**Event IDs 1,2,5** (ProcessCreate, ProcessChange, ProcessTerminate), **CommandLine:** "Get-Keystrokes", "Get-TimedScreenshot", "Get-VaultCredential", "Invoke-CredentialInjection", "mimikatz"

References

1. MITRE. Lateral Movement-The Adversary Is Trying to Move through Your Environment. *Mitre*, 12 July 2019.
2. Smiliotopoulos, C.; Barmpatsalou, K.; Kambourakis, G. Python_Evtx_Analyzer (PeX-v1). Available online: https://github.com/ChristosSmiliotopoulos/Python_Evtx_Analyzer.git (accessed on 25 June 2022).
3. Coordination, J. *Detecting Lateral Movement through Tracking Event Logs*; JPCERT Coordination Center: Tokyo, Japan, June 2017.
4. Russinovich, M.; Garnier, T. Sysmon v13. 22. https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=90022 (accessed on 25 June 2022).
5. Coordination, J. *Detecting Lateral Movement through Tracking Event Logs (Ver. 2)*; JPCERT Coordination Center: Tokyo, Japan, December 2017.
6. Viasat. KaSat-Network Cyber Attack Overview. Available online: https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/ (accessed on 4 April 2022).
7. Mavroeidis, V.; Jøsang, A. Data-driven threat hunting using sysmon. In Proceedings of the 2nd International Conference on Cryptography, Security and Privacy, Guiyang, China, 16–19 March 2018; pp. 82–88.
8. Mavroeidis, V.; Bromander, S. Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence. In Proceedings of the 2017 European Intelligence and Security Informatics Conference (EISIC), Athens, Greece, 11–13 September, 2017; pp. 91–98. https://doi.org/10.1109/EISIC.2017.20.
9. Berady, A.; Jaume, M.; Tong, V.V.T.; Guette, G. From TTP to IoC: Advanced Persistent Graphs for Threat Hunting. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 1321–1333. https://doi.org/10.1109/TNSM.2021.3056999.
10. Matsuda, W.; Fujimoto, M.; Mitsunaga, T. Real-Time Detection System Against Malicious Tools by Monitoring DLL on Client Computers. In Proceedings of the 2019 IEEE Conference on Application, Information and Network Security (AINS), Penang, Malaysia, 19–21 March 2019; pp. 36–41. https://doi.org/10.1109/AINS47559.2019.8968697.
11. Juwono, J.T.; Lim, C.; Erwin, A. A comparative study of behavior analysis sandboxes in malware detection. In Proceedings of the International Conference on New Media (CONMEDIA), Jakarta, Indonesia, 27 November 2015; p.73–78.
12. Narouei, M.; Ahmadi, M.; Giacinto, G.; Takabi, H.; Sami, A. DLLMiner: Structural mining for malware detection. *Secur. Commun. Netw.* **2015**, *8*, 3311–3322.
13. Rajesh, P.; Ismail. Ismail. B, M.; Alam, M.; Tahernezhadi, M. Network Forensics Investigation in Virtual Data Centers Using ELK. In Proceedings of the 2021 International Symposium on Electrical, Electronics and Information Engineering, Online, 19–21 February 2021; pp. 175–179.
14. Jain, U. Lateral Movement Detection Using ELK Stack. Ph.D. Thesis, University of Houston, Houston, MA, USA, 2018.

15. El-Hadidi, M.G.; Azer, M.A. Detecting Mimikatz in Lateral Movements Using Mutex. In Proceedings of the 2020 15th International Conference on Computer Engineering and Systems (ICCES), Cairo, Egypt, 15–16 December 2020; pp. 1–6. https://doi.org/10.1109/ICCES51560.2020.9334643.
16. Ki, Y.; Kim, E.; Kim, H.K. A Novel Approach to Detect Malware Based on API Call Sequence Analysis. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 659101.
17. Ho, G.; Dhiman, M.; Akhawe, D.; Paxson, V.; Savage, S.; Voelker, G.M.; Wagner, D. Hopper: Modeling and Detecting Lateral Movement. In *Proceedings of the 30th USENIX Security Symposium (USENIX Security 21)*; USENIX Association: Berkeley, CA, USA, 2021; pp. 3093–3110.
18. Bhasin, H.P.S.; Ramsdell, E.; Alva, A.; Sreedhar, R.; Bhadkamkar, M. Data center application security: Lateral movement detection of malware using behavioral models. *SMU Data Sci. Rev.* **2018**, *1*, 10.
19. Coffey, K.; Smith, R.; Maglaras, L.; Janicke, H. Vulnerability analysis of network scanning on SCADA systems. *Secur. Commun. Netw.* **2018**, *2018*, 3794603.
20. Mulder, J.; Stingley, M. Mimikatz Overview, Defenses and Detection. SANS Institute, February 2016; p. 1–18. Available online: https://www.sans.org/white-papers/36780/ (accessed on 15 April 2022).
21. Ussath, M.; Jaeger, D.; Cheng, F.; Meinel, C. Advanced persistent threats: Behind the scenes. In Proceedings of the IEEE 2016 Annual Conference on Information Science and Systems (CISS), Princeton, NJ, USA, 15–18 March 2016, pp. 181–186.
22. Kazanciyan, R.; Hastings, M. *Investigating Powershell Attacks*; Black Hat: San Francisco, CA, USA, 2014; p. 1–25.
23. Steven F. Revisiting Remote Desktop Lateral Movement. Medium. 2022. Available online: https://posts.specterops.io/ (accessed on 12 April 2022).
24. logPoint. MITRE ATT&CK Analytics—Alert Rules Latest Documentation. 2022. Available online: https://docs.logpoint.com/docs/alert-rules/en/latest/MITRE.html (accessed on 15 April 2022).
25. Goet, M. Protect Yourself against #BlueKeep Using Azure Sentinel and Defender ATP. Medium. 2022. Available online: https://medium.com/@maarten.goet/protect-yourself-against-bluekeep-using-azure-sentinel-and-defender-atp-d308f566d5cf (accessed on 12 April 2022).
26. SandBoxCloud, J. Windows Analysis Report. SandBoxCloud. 2022. Available online: https://www.joesandbox.com/analysis (accessed on 24 May 2022).
27. Sandbox, F. Free Automated Malware Analysis Service, "RemoteDesktopManagerFree.exe". Sandbox. 2022. Available online: https://www.hybrid-analysis.com/sample/b26ede46a0be62f361b4a28d2e67fa2e2f35c9bbc995ae84a2c0c7f4141f65b0?environmentId=100 (accessed on 17 April 2022).
28. Sorensen, S. Remote Desktop Manager Free. LO4D.com. 2022. Available online: https://remote-desktop-manager-free.en.lo4d.com/windows (accessed on 18 May 2022).
29. Bezverkhyi, A. Proactive Detection Content: CVE-2019-0708 vs ATT&CK, Sigma, Elastic and ArcSight-SOC Prime. SOC Prime. 2022. Available online: https://socprime.com/blog/proactive-detection-content-cve-2019-0708-vs-attck-sigma-elastic-and-arcsight (accessed on 15 May 2022).
30. s0i37—HackMag. Lateral Movement Guide: Remote Code Execution in Windows. Available online: https://hackmag.com/security/lateral-guide/ (accessed on 26 May 2022).