第 48 卷 第 6 期
2021 年 6 月

湖南大学学报（自然科学版）
Journal of Hunan University（Natural Sciences）

Vol. 48. No. 6.
June 2021

Integrated Security System Implementation for Network Intrusion

Resevoa Moral Muhammad, Indrarini Dyah Irawati, Muhammad Iqbal

School of Applied Science, Telkom University, Bandung, Indonesia

Abstract: Network security systems vary much according to the circumstances and conditions concerned. A network security system plays a very important role in maintaining network security to prevent attacks and protect us from frequent attacks on a device through a network both in terms of malware administration and data theft. This research aims to build a Honeypot security system as a trap, detect attacks, and be able to get useful information from malware analysis results. It is also focused on the extent to which HIDS-based IDS can detect attacks common in the network, with Honeypot Dionaea, which serves as an attracter for attackers, and what information will be obtained when performing analysis malware using Cuckoo Sandbox. This implementation is carried out with six active users in one network and pays attention to whether IDS can detect the attacker. The results show that HIDS-based IDS has the advantage of monitoring digital data, and based on the results of brute force attack attempts obtained, 65.55% detected an attempt to log in using an unregistered username, 29.16% detected a failed login attempt, 4.17% detected double log in a short time, and 1.11% detected a brute force attempt to gain access to the system. Cuckoo Sandbox can provide malware information in the form of what types of malware are analyzed, how the malware behaves, and how it impacts the malware on the systems attacked.

Keywords: Honeypot, Intrusion Detection System, malware, network, security.

网络入侵的集成安全系统实现

摘要：网络安全系统根据相关情况和条件而有很大不同。网络安全系统在维护网络安全方面起着非常重要的作用，以防止恶意软件管理和数据盗窃，从而防止攻击并保护我们免受通过网络对设备的频繁攻击。这项研究旨在将蜜罐安全系统构建为陷阱，检测攻击并能够从恶意软件分析结果中获取有用的信息。它还重点关注基于 HIDS 的入侵检测系统可以检测到网络中常见的攻击的程度，蜜罐狄奥尼娅充当攻击者的诱饵，以及使用布谷鸟沙盒执行分析恶意软件时将获得哪些信息。此实现是在一个网络中由六个活动用户执行的，并注意入侵检测系统是否可以检测到攻击者。结果表明，基于 HIDS 的入侵检测系统具有监视数字数据的优势，并且基于获得的暴力攻击尝试的结果，发现 65.55％的用户尝试使用未注册的用户名登录，29.16％的用户检测到失败的登录尝试，4.17％。％的用户在短时间内检测到两次对数日志，而 1.11％的用户检测到暴力尝试获取系统访问权限。布谷鸟沙盒可以提供以下形式的恶意软件信息：分析了哪些类型的恶意软件，恶意软件的行为以及它如何影响恶意软件对受攻击系统的影响。

关键词：蜜罐，入侵侦测系统，恶意软件，网络，安全性。

1. Introduction

The rapid development of technology creates threats and disruptions that will affect the performance of the technology. The transmission of information must be protected because a novice can attack the system using existing network attack tools. For this reason, a

Received: March 6, 2021 / Revised: April 4, 2021 / Accepted: May 9, 2021 / Published: June 28, 2021

About the authors: Resevoa Moral Muhammad, Indrarini Dyah Irawati, Muhammad Iqbal, School of Applied Science, Telkom University, Bandung, Indonesia

disruption detection system, known as Intrusion Detection System (IDS), was created. In addition to IDS, there is also a honeypot that serves as an attacker trapper and Cuckoo Sandbox that performs malware analysis.

This research was conducted based on previous researches. In [1] stated that honeypot is one of the tools for analyzing malware and attack methods. The main idea of the Honeypot operation is to make the decoy system expose security issues such as vulnerabilities. Research [2] declared honeypot is a forgery system used at the network entrance to trap hackers, usually inducing malware to attack the real server and identify malicious activities performed over the Internet. Research [3] stated that IDS analyzes the traffic of the network to find malicious attacks. It depends on the dimension of the system structure used. In [4], IDS is an effective security technique that can protect the system from cyber-attacks by analyzing network traffic. Research [5] stated doing malware analysis is important to overcome and prevent malware attacks appropriately because each type of malware has its threats and ways of working. Another research [6] states that malware analysis aims to provide the information necessary to deal with malware attacks by knowing what is happening in the system, where the infected file is located, detecting the malware activity, and the types of malware it belongs to. In [7], a honeypot is a certain security measure facility designed to authorize the purpose of being attacked and disclosed its information system resources to Luring unauthorized and illegal access. IDS was implemented in [8] as a software or hardware system that can identify malicious behaviors on computer systems to maintain system security. IDS implementation discussed in [9] contributes to find and abolish malicious activities in computer and network security. In [10], the research was conducted to improve IDS performance by using NSL-KDD training and test data sets with binary classification. It aims to decrease the number of irrelevant features, thus increasing classification accuracy.

In this paper, the implementation of a local network security system using a Dionaea honeypot and IDS. In addition, malware analysis is carried out using system malware analysis, focusing on the security side of users with Host-based IDS for one user. The honeypot acts as a trap for attackers by deliberately opening fake ports to attract the attacker's attention. This system is applied to servers with high intensity for data entry and exit. The malware analysis system used is the cuckoo sandbox. Cuckoo sandbox can provide suspicious application tests with a score of 0-2 for the safe category, 3-5 for the suspicious category, and 6-10 for the danger category. The cuckoo sandbox is also able to display the behavior of suspicious applications and can record these behaviors. This research is performed specially for host-based IDS using the Wazuh tool as a comprehensive Open Source Security Platform. Wazuh supports maintaining network security.

2. Basic Theory

Honeypots are made to be attacked, investigated, and exploited. Honeypot is designed to provide information rather than improve it [11]. Honeypot can be clarified based on the interaction it has. Low Interaction Honeypot is designed to emulate services like on the original server. Attackers can only check and connect to one or more ports; meanwhile, high interaction honeypot has an operating system where attackers can interact directly. There are no restrictions that limit those interactions. Removing these restrictions is high risk because attackers can have root access.

IDS has similarities with firewalls, but IDS also has its own advantages. IDS generally collects data from network resources monitored by IDS and analyzes the data. However, this does not solve all safety-related issues. IDS cannot overcome the weak identification and authentication procedures, including problems in network protocols [12]. IDS can conduct traffic inspections both inbound and outbound within a system or network. Itgeneratesexplanation and find proof of attempted intrusions. In Network-Based IDS Implementation, the traffic passing on the network will be analyzed if an intrusion event is detected. NIDS is usually located at the entrance of the network or where the server is located. The disadvantage of NIDS is that it is quite complicated to be implemented in a network that uses ethernet switches. Meanwhile, in Host-Based IDS, a network host activity will be monitored, regardless of whether there is an attempted attack or interference. HIDS is usually placed on the primary server on the network, such as Firewall, web server, or internet server.

Software that enters the system without being detected by the user is malware. Malware has a destructive nature. Malware plays a role in gaining access to computer systems and network resources, disrupting computer operations, and collecting personal information, thus threatening internet availability, host integrity, and user privacy [13]. The purpose of malware is undoubtedly to destroy or steal data from the incoming device. Malware is specifically designed to perform destructive activities—other malware such as trojan horses, viruses, spyware, and exploits [14]. The purpose of creating malware is to perform malicious activities that can negatively impact the victim, such as wiretapping and theft of personal information. Malware analysis is a process for determining the functionality, source, and potential impact of specific malware samples such as viruses, worms, trojan horses, rootkits, or backdoors. There are two methods to do malware analysis. The first one is called dynamic analysis. It is a method of analyzing malware by comparing system behavior before

malware is run with system behavior after the malware is run. Dynamic analysis methods usually use virtual software such as Virtualbox, VMware, and others. If the malware run causes damage to the system, the main system will not be damaged by the malware. The second method is called static analysis. It is a method used to perform malware analysis by directly observing the source code of malware. In [15], the performance of each malware execution chain was performed by reverse engineering analysis.

3. Methods

In this section, we test several attack scenarios such as SSH Brute force, RDP Brute force, and DoS Attacks.

The system scans the possible targets to be attacked. Fig 1 shows port scanning using NMAP.

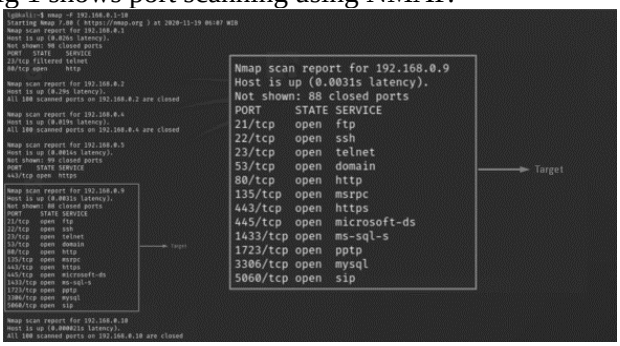

Fig. 1 Port scanning using NMAP

After getting the target, we can attack the system. Fig 2 shows the results of SSH Brute force using Metasploit. We must set up a library that contains a list of usernames and passwords to brute force.

```
msf5 > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.0.9
rhosts ⇒ 192.168.0.9
msf5 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf5 auxiliary(scanner/ssh/ssh_login) > set user_file users.txt
user_file ⇒ users.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file passwords.txt
pass_file ⇒ passwords.txt
msf5 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose ⇒ true
msf5 auxiliary(scanner/ssh/ssh_login) > run
```

Fig. 2 SSH Brute force

Fig 3 shows the second attack scenario. It performs RDP Brute force where it takes a remote crack Desktop. The attack tool is Hydra with the username “George” and a list of existing passwords used as passwords for remote desktop access.

```
lg@kali:~$ hydra -t 4 -V -f -l george -P passwords.txt rdp://192.168.0.7
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organi
zations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-11-12 03:56:40
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10 login tries (l:1/p:10), ~3 tries per task
[DATA] attacking rdp://192.168.0.7:3389/
[ATTEMPT] target 192.168.0.7 - login "george" - pass "1234" - 1 of 10 [child 0] (0/0)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "hahahihi" - 2 of 10 [child 1] (0/0)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "test" - 3 of 10 [child 2] (0/0)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "admin" - 4 of 10 [child 3] (0/0)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "password" - 5 of 12 [child 0] (0/2)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "halo" - 6 of 12 [child 3] (0/2)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "test1227" - 7 of 12 [child 1] (0/2)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "1234567890" - 8 of 12 [child 2] (0/2)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "blimey" - 9 of 12 [child 2] (0/2)
[ATTEMPT] target 192.168.0.7 - login "george" - pass "hola" - 10 of 12 [child 1] (0/2)
[REDO-ATTEMPT] target 192.168.0.7 - login "george" - pass "1234" - 11 of 12 [child 0] (1/2)
[REDO-ATTEMPT] target 192.168.0.7 - login "george" - pass "admin" - 12 of 12 [child 2] (2/2)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-11-12 03:56:42
lg@kali:~$
```

Fig. 3 RDP Brute force

The 3rd attacker scenario is a DoS attack using hping3 that shown in Fig 4. This attack will utilize port 80 that has been opened by Honeypot Dionaea, as a trap.

We also test malware by using pirated applications. It has resulted in a blog that provides pirated applications along with malware brought ransomware.

```
root@kali:/home/lg# hping3 -S -p 80 --flood 192.168.0.9
HPING 192.168.0.9 (eth0 192.168.0.9): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.0.9 hping statistic ---
1076469 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:/home/lg#
```

Fig. 4 DoS attack

The result is shown in Fig. 5.

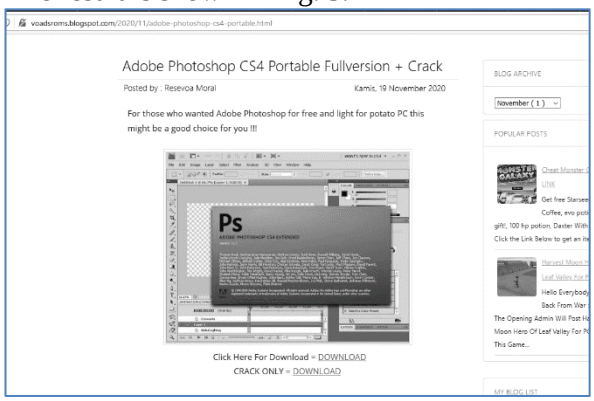

Fig. 5 Pirated application provider blog

4. Results and Discussion

4.1. Brute Force

Fig. 6 shows activities recorded from SSH Brute force. The results are obtained from Wazuh. The information on the existence of SSH logins takes on certain hours. The other information, such as a targeted attack, IP attacker, and the user used to login SSH, can be detected.

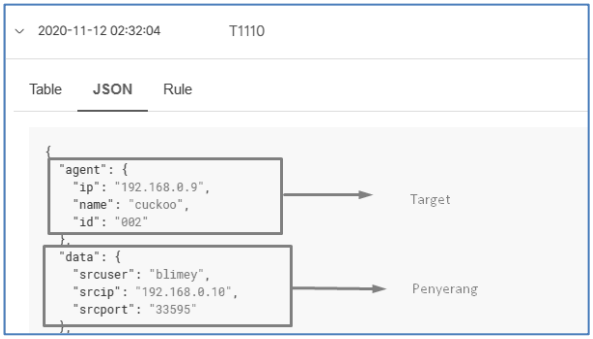

Fig. 6 Recorded activity from SSH Brute force

Fig. 7 shows the five Wazuh highest alerts from 12:00 p.m. to 9:00 p.m. It is stated that the alert for the attempted log in using a username that is not listed on the target as much as 65.55%, then the failure in the login as much as 29.16%, then a 4.17% double log in short attempt, then a brute force attempt to gain access to the system by 1.11% and the last one was an alert from vulnerabilities against lebnettel6 based on CVE-2018-16869 of 0.01%. Broadly speaking, for log-in experiment alerts using unregistered usernames, login failures, attempted logins shortly, and detected brute-force attacks, these are all included in the alerts for

brute-force attacks that are broken down specifically into their activity. Thus, in total, 99.99% of brute-force attacks have been detected.

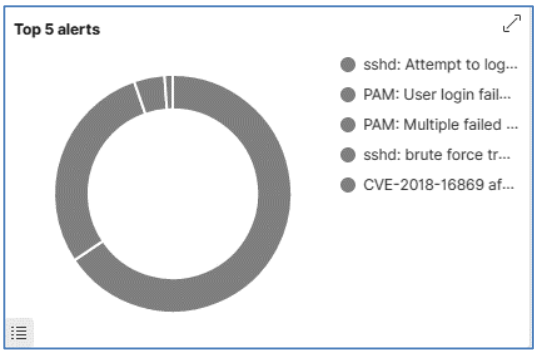

Fig. 7 Top five alerts

4.2. DoS

Fig 8 shows the information from Wazuh in the DoS scenario. The DoS attack took advantage of port 80, opened by Honeypot Dionaea, but the result obtained by Wazuh is the absence of attack activity. This happens because HIDS-based IDS is indeed more reliable in monitoring digital data, mentioned in the Wazuh website, which states that Wazuh is one of the best HIDS to analyze log activity in each registered agent device. However, some security issues are more often detected by inspecting network traffic.

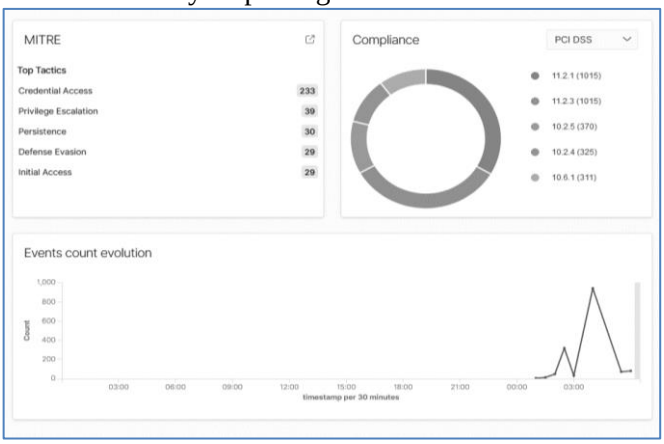

Fig. 8 Wazuh did not detect DoS attack

4.3. Integrity and Vulnerability Monitoring

Integrity Monitoring is one of the Wazuh features to ensure that digital data is content that can be trusted and accurate. Fig 9 shows this experiment. The monitoring is done by creating files, editing, and deleting files. All activities can be recorded properly by the Wazuh.

Time	syscheck.path	syscheck.event
Nov 12, 2020 @ 04:46:03.862	c:\apple\test.txt	deleted
Nov 12, 2020 @ 04:45:57.868	c:\apple\test.txt	modified
Nov 12, 2020 @ 04:45:55.063	c:\apple\test.txt	added
Nov 12, 2020 @ 04:45:55.047	c:\apple\new text document.txt	deleted
Nov 12, 2020 @ 04:45:52.239	c:\apple\new text document.txt	added

Fig. 9 Integrity monitoring

Vulnerability Monitoring on Wazuh works based on CVE. All applications are scanned within the agent connected to the Wazuh. Fig 10 shows the monitoring results. The Wazuh detects security gaps in each existing application.

Most common rules

Rule ID	Description	Count
23506	CVE-2020-26154 affects libproxy1v5	1
23506	CVE-2020-26154 affects libproxy1-plugin-networkmanager	1
23506	CVE-2020-26154 affects libproxy1-plugin-gsettings	1
23506	CVE-2020-15683 affects thunderbird-gnome-support	1
23506	CVE-2020-15683 affects thunderbird	1

Export: Raw Formatted

1 2 3 4 »

Fig. 10 Vulnerability monitoring

4.4. Malware Analysis

The malware analysis provides some important information, including malware type, the attack behavior scenario, and the impact resulting from the malware attack. In this case, the analysis revealed ransomware as a malware type, and several processes carried out by the malware, making hidden system files, creating some additional programs, and doing the read and write process on memory protection. In Fig 11, it is alleged that the malware, according to the cuckoo sandbox 10 out of 10 points of the malware, is highly suspect.

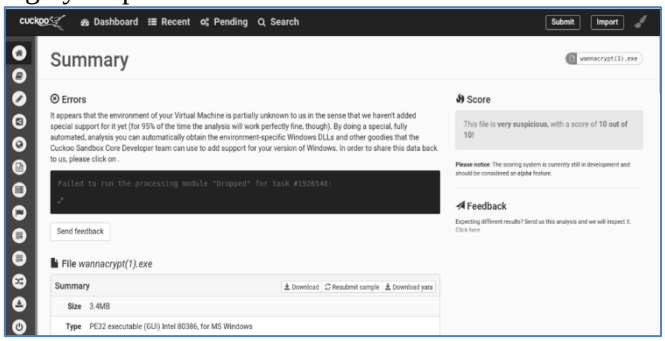

Fig. 9 Cuckoo Sandbox

Fig. 12 shows the behavior of the malware when the malware is run. One of them is an experiment to inhibit the task of analysis, create documents on system files, create files that can be run on system files, perform suspicious processes, and many others that have been recorded by the cuckoo sandbox.

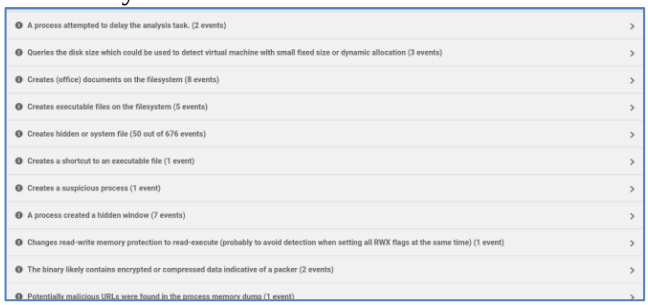

Fig. 10 Malware behaviors

5. Conclusion

We can develop an integrated security system for preventing network intrusion. The system shows that the honeypot being used serves as a catcher for the

attacker as it opens multiple ports, but the original system is not affected by the attack. Wazuh as a detection system works well for maintaining digital data. HIDS-based IDS has the advantage of monitoring log activities on each connected agent. IDS could detect brute-force attacks with a percentage of 65.55% detected attempts logged in using unregistered usernames, 29.16% detected a failed log-in attempt, 4.17% detected double log in at an adjacent time, and 1.11% detected a brute-force attempt to gain access to the system. In the malware analysis, information is obtained, including the type of malware, malware behavior, and its impact. The sandbox cuckoo assesses the danger level of malware based on the malware behavior. The more malware behavior, the higher the hazard value.

We can add an auto report feature using social media and instant messaging to the security system on the network for further work. This feature will facilitate the system administrator's task in monitoring attacks into the network system.

References

[1] SAIKAWA K. and KLYUEV V. Detection and Classification of Malicious Access using a Dionaea Honeypot. *Proc. 2019 10th IEEE Int. Conf. Intell. Data Acquis. Adv. Comput. Syst. Technol. Appl. IDAACS* 2019, 2: 844–848, doi: 10.1109/IDAACS.2019.8924340.

[2] SETHIA V. and JEYASEKAR A. Malware capturing and analysis using dionaea honeypot. *Proc. - Int. Carnahan Conf. Secur. Technol.*, 2019, 0–3, doi: 10.1109/CCST.2019.8888409.

[3] USTEBAY S., TURGUT Z., and AYDIN M. A. Intrusion Detection System with Recursive Feature Elimination by Using Random Forest and Deep Learning Classifier. *Int. Congr. Big Data, Deep Learn. Fight. Cyber Terror. IBIGDELFT 2018 - Proc.* 2019: 71–76, doi: 10.1109/IBIGDELFT.2018.8625318.

[4] VIJAYANAND R., DEVARAJ D., and KANNAPIRAN B. Intrusion detection system for wireless mesh network using multiple support vector machine classifiers with genetic-algorithm-based feature selection. *Comput. Secur.*, 2018, 77: 304–314, doi: 10.1016/j.cose.2018.04.010.

[5] MEGIRA S., PANGESTI A. R., and WIBOWO F. W. Malware Analysis and Detection Using Reverse Engineering Technique. *J. Phys. Conf. Ser.*, 2018, 1140(1), doi: 10.1088/1742-6596/1140/1/012042.

[6] JEREMIAH J. Intrusion Detection System to Enhance Network Security Using Raspberry PI Honeypot in Kali Linux. *2019 Int. Conf. Cybersecurity, ICoCSec* 2019: 91–95, doi: 10.1109/ICoCSec47621.2019.8971117.

[7] FAN W., DU Z., SMITH-CREASEY M., and FERNANDEZ D. HoneyDOC: An Efficient Honeypot Architecture Enabling All-Round Design. *IEEE J. Sel. Areas Commun.*, 2019, 37, (3): 683–697, doi: 10.1109/JSAC.2019.2894307.

[8] KHRAISAT A., GONDAL I., VAMPLEW P., and KAMRUZZAMAN J. Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*, 2019, 2(1), doi: 10.1186/s42400-019-0038-7.

[9] TAMA B., COMUZZI A. M., and RHEE K. H. TSE-IDS: A Two-Stage Classifier Ensemble for Intelligent Anomaly-Based Intrusion Detection System. *IEEE Access*, 7: 94497–94507, 2019, doi: 10.1109/ACCESS.2019.2928048.

[10] PHAM N. T., FOO E., SURIADI S., JEFFREY H., and LAHZA H. F. M. Improving performance of intrusion detection system using ensemble methods and feature selection. *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3167918.3167951.

[11] WIDODO T., MUHSINA E. A., and SUGIANTORO B. Honeypot Log Analysis as a Network Security Support. *IJID (International J. Informatics Dev.*, 2019, 2(1): 8–12.

[12] TAHER K. A., MOHAMMED YASIN JISAN B., and RAHMAN M. M. Network intrusion detection using supervised machine learning technique with feature selection," *1st Int. Conf. Robot. Electr. Signal Process. Tech. ICREST 2019*: 643–646, doi: 10.1109/ICREST.2019.8644161.

[13] TALUKDER S. and TALUKDER Z. A Survey on Malware Detection and Analysis Tools. *Int. J. Netw. Secur. Its Appl.*, 2020, 12(2): 37–57, doi: 10.5121/ijnsa.2020.12203.

[14] SIHWAIL R., OMAR K., and ZAINOL ARIFFIN K. A. A Survey on Malware analysis Techniques: Static, Dynamic, Hybrid, and Memory Analysis. *Int. J. Adv. Sci. Eng. Inf. Technol.*, 2018, 8(4–2): 1662–1671.

[15] HSIAO S. C. and KAO D. Y. The static analysis of WannaCry ransomware. *Int. Conf. Adv. Commun. Technol. ICACT*, 2018-February: 153–158, doi: 10.23919/ICACT.2018.8323680.

参考文:

[1] SAIKAWA K. 和 KLYUEV V. 使用狄奥尼耶蜜罐进行恶意访问的检测和分类。程序。2019第十届电气工程师学会国际Conf。智力数据采集。进阶计算系统。技术。应用 IDAACS 2019，2：2：844–848，土井：10.1109/IDAACS.2019.8924340。

[2] SETHIA V. 和 JEYASEKAR A. 使用狄奥尼娅蜜罐进行恶意软件捕获和分析。程序。-诠释卡纳汉会议。安全。技术，2019，0–3，doi：10.1109/CCST.2019.8888409。

[3] USTEBAY S.，TURGUT Z. 和 AYDIN M. A. 通过使用随机森林和深度学习分类器消除递归特征的入侵检测系统。诠释大会大数据，深度学习。斗争。网络恐怖。IBIGDELFT 2018-Proc.：71 – 76，2019，土井：10.1109/IBIGDELFT.2018.8625318。

[4] VIJAYANAND R.，DEVARAJ D. 和 KANNAPIRAN B。无线网状网络的入侵检测系统，它使用多个支持向量机分类器以及基于遗传算法的特征选择。计算安全。，2018，77：304–314，doi：10.1016/j.cose.2018.04.010。

[5] MEGIRA S.，PANGESTI A. R. 和 WIBOWO F. W. 使用逆向工程技术进行恶意软件分析和检测。J.物理Conf

。系列，2018，1140（1），土井：10.1088/1742-6596/1140/1/012042。

[6] JEREMIAH J. 在卡利Linux中使用覆盆子PI 蜜罐增强网络安全性的入侵检测系统。2019年国际Conf。网络安全，联合会2019：91–95，土井：10.1109/ICoCSec47621.2019.8971117。

[7] FAN W.，DU Z.，SMITH-CREASEY M. 和 FERNANDEZ D. 蜂蜜DOC：实现全方位设计的高效蜜罐架构。电气工程师学会J. 塞尔。地区社区，2019，37，（3）：683–697，土井：10.1109/JSAC.2019.2894307。

[8] KHRAISAT A.，GONDAL I.，VAMPLEW P. 和 KAMRUZZAMAN J. 入侵检测系统概述：技术，数据集和挑战。网络安全，2019，2（1），土井：10.1186/s42400-019-0038-7。

[9] TAMA B.，COMUZZI A. M. 和 RHEE K. H. 东京证券交易所-入侵检测系统：基于智能异常的入侵检测系统的两阶段分类器集合。电气工程师学会访问，2019，7：94497–94507，土井：10.1109/ACCESS.2019.2928048。

[10] PHAM N. T.，FOO E.，SURIADI S.，JEFFREY H. 和 LAHZA H. F. M. 使用集成方法和特征选择来提高入侵检测系统的性能。ACM国际Conf。会议论文集，2018，土井：10.1145/3167918.3167951。

[11] WIDODO T.，MUHSINA E. A. 和 SUGIANTORO B. 作为网络安全支持的蜜罐日志分析。IJID（国际的J. 信息学开发。，2019，2（1）：8-12）。

[12] TAHER K. A.，MOHAMMED YASIN JISAN B. 和 RAHMAN M. M. 使用具有特征选择功能的监督机器学习技术进行网络入侵检测，”第1篇诠释。Conf。机器人。电器。信号处理。科技ICREST 2019：643–646，土井：10.1109 / ICREST.2019.8644161。

[13] TALUKDER S. 和 TALUKDER Z。关于恶意软件检测和分析工具的调查。诠释J. 网络。安全。它的应用，2020，12（2）：37-57，土井：10.5121/ijnsa.2020.12203。

[14] SIHWAIL R.，OMAR K. 和 ZAINOL ARIFFIN K. A. 恶意软件分析技术概述：静态，动态，混合和内存分析。诠释J.高级科学。信息。技术，2018，8（4–2）：1662–1671。

[15] HSIAO S. C. 和 KAO D. Y. 想哭勒索软件的静态分析。诠释Conf。进阶公社技术。ICACT，2018, 2：153-158，doi：10.23919/ICACT.2018.8323680。