Deception-Based Proactive Defense Against Ransomware in VMWare ESXI Systems

Thanh-Tam Tran Thi
ICT Department
FPT University
Hanoi 10000, Vietnam
tamttthe161665@fpt.edu.vn

Hai-Ha Tran
ICT Department
FPT University
Hanoi 10000, Vietnam
hathhe161777@fpt.edu.vn

Minh-Quan Do
ICT Department
FPT University
Hanoi 10000, Vietnam
quandmhe161803@fpt.edu.vn

Nhat-Nam Nguyen
ICT Department
FPT University
Hanoi 10000, Vietnam
namnnhe163790@fpt.edu.vn

Tung-Son Trinh
ICT Department
FPT University
Hanoi 10000, Vietnam
sontthe163856@fpt.edu.vn

Minh-Tri Luu
ICT Department
FPT University
Hanoi 10000, Vietnam
trilm29@fe.edu.vn

Anh-Nhat Nguyen
ICT Department
FPT University
Hanoi 10000, Vietnam
nhatna3@fe.edu.vn

Tung-Son Ngo
ICT Department
FPT University
Hanoi 10000, Vietnam
sonnt69@fe.edu.vn

***Abstract*—This study focuses on the vulnerabilities and attack vectors connected with ransomware in Elastic Sky X integrated (ESXi) settings. We offer a novel technique to address these concerns by mimicking an ESXi environment, focusing on honeypot deployment and monitoring behaviours. Our strategy is creating a controlled emulation of ESXi in which we place honeypots to lure and capture ransomware activity. Furthermore, we use sophisticated monitoring methods to watch and evaluate ransomware behaviours in this simulated environment. Our approach's effectiveness is tested using the simulated ESXi environment's detection and response capabilities. The findings show that using honeypots in conjunction with careful behavioural monitoring can considerably improve the identification and mitigation of ransomware threats in virtualized environments.**

***Index Terms*—VMWare ESXi, Ransomware, Deception, Behavioral Monitoring**

I. Introduction

Ransomware has quickly become a major cyber threat, increasingly targeting virtual environments due to their critical role in IT infrastructure and potential for significant disruptions [1]. VMware ESXi, a widely used hypervisor in data centers and enterprise networks, is particularly vulnerable because of its extensive use in server consolidation, resource optimization, and cloud computing, amplifying the impact of attacks [2].

While ESXi's unique architecture provides performance and efficiency benefits, it also creates security issues. As a bare-metal hypervisor, compromising ESXi gives attackers access to all virtual machines running on that host, dramatically enhancing the effect of a ransomware assault. Furthermore, specific components such as the VMkernel and vSphere Client provide distinct attack vectors that ransomware operators can use to acquire unauthorised access and distribute malicious payloads.

A successful ransomware attack on an ESXi environment can have devastating financial and operational consequences, resulting in extended downtime, disruption of critical business operations and services, data loss, and costly recovery efforts, which frequently include data restoration from backups, system rebuilds, and potential ransom payments [3]. This highlights the critical necessity for proactive and effective security solutions to safeguard ESXi environments from this emerging threat.

This study employs multi-layered simulation trap methodologies to mislead and analyze ransomware for VMware ESXi [4]. Our solution is built around a properly designed honeypot that simulates a vulnerable ESXi host. The honeypot includes accurate simulations of the ESXi file system, a shell, and simulated services with carefully placed flaws. To improve the honeypot's effectiveness, we use two deception techniques: a honeypot file [5], services and ports with known vulnerabilities that serve as decoys to trigger ransomware encryption attempts, and a system that analyzes file access patterns to detect ransomware behavior [6]. A sophisticated logging system captures all attacker activity within the honeypot, providing useful data for investigation. Furthermore, honeypots can be connected with SIEM systems to provide centralized monitoring and threat intelligence. A dedicated control module simplifies honeypot management by providing a user-friendly command line interface that enables administrators to easily control and monitor honeypot operations. The primary contributions of the paper are:

- We develope an ESXi simulation environment called LUAGA. This tool employs a variety of deception techniques, including intentionally placed traps designed to entice attackers. After successfully engaging with the placed traps, the tool extensively collects information on attacker activities and processes, generating a valuable data source for future research.
- In this ESXi honeypot, we create a modular and extendable shell environment, with each command implemented

as a different class. This method increases code structure and facilitates the inclusion of additional commands. The shell interacts with a synthetic filesystem that resembles the structure of a genuine ESXi system. This structure improves the identification and mitigation of ransomware attacks. By analyzing attacker instructions and parameters, the honeypot can detect harmful tendencies and respond appropriately, simulating failures or delaying responses to provide a realistic experience and acquire more intelligence. The separated filesystem prevents actual harm and allows for speedy recovery following an assault.

- We Improve ransomware handling with a powerful shell interpreter, deeper analysis of attacker scripts, and behavioral analysis engine to detect unusual activity beyond command patterns. Additionally, integrating with a threat intelligence platform would allow for real-time threat detection and proactive defense measures.

The rest of this paper is structured as follows: Section II presentation of methodology. Section III presents and discusses the test case. Finally, the conclusions are drawn in Section IV.

II. Related works

This section delves into existing research and literature pertinent to the core themes of this study: ransomware threats targeting VMware ESXi systems, the limitations of traditional security measures, the application of deception technology, and the utilization of honeypots for proactive defense.

A. Ransomware and ESXi: A Growing Threat

The prevalence and sophistication of ransomware attacks have surged in recent years, with virtualized environments, particularly VMware ESXi, becoming prime targets [1], [2]. Aalam *et al.* provide a comprehensive review of hypervisor and virtual machine security, highlighting the unique vulnerabilities of ESXi systems [2]. Kaspersky reports on the alarming increase in attacks targeting virtualization systems and Linux servers, emphasizing the critical need for robust security measures. The Cybersecurity and Infrastructure Security Agency (CISA) has issued an alert detailing the growing threat of ransomware targeting ESXi, emphasizing the importance of patching vulnerabilities and implementing security best practices.

B. Inadequacies of Traditional Defenses

Traditional security solutions, such as antivirus software and intrusion detection systems, often prove insufficient against modern ransomware variants [3], [7]. Guvci & Senol discuss the shortcomings of signature-based methods and advocate for more proactive defense strategies [7]. Thomas & Galligher focus on the importance of robust backup systems and the need for improved evaluation methodologies in security risk assessments [3].

C. Deception Technology: A Proactive Approach

Deception technology offers a proactive defense approach, creating deceptive environments to lure and mislead attackers [8], [9]. Han *et al.* present a research perspective on deception techniques in computer security, highlighting the various methods used to deceive attackers, including honeypots, fake data, and misleading system responses [8]. Zhang *et al.* provide a comprehensive review of three decades of deception techniques in active cyber defense, tracing the evolution of these techniques and their effectiveness in mitigating threats [9]. Dark Reading emphasizes the practical benefits of cyber deception in countering evolving and advanced threat landscapes, arguing for its inclusion in a comprehensive security strategy.

D. Honeypots: A Powerful Tool for Deception

Honeypots have emerged as a valuable tool for implementing deception-based defenses, attracting attackers and providing insights into their tactics [10]–[13]. Othman *et al.* explore the potential applications of honeypot technology in intrusion detection systems, highlighting their effectiveness in gathering threat intelligence and improving incident response [10]. Kandanaarachchi *et al.* introduce Honeyboost, a system that enhances honeypot performance with data fusion and anomaly detection, showcasing the potential of advanced analytics in improving honeypot effectiveness [11]. Cowrie *et al.* are two widely used honeypot frameworks offering diverse capabilities for simulating various systems and services [12], [13]. Honeytrap documentation specifically details its support for various services, making it a versatile tool for honeypot deployment.

E. Addressing the Gap: ESXi-Specific Deception

Despite the existing research on honeypots and deception, there is a limited focus on ESXi-specific solutions. Raja & Venkatesh and Sheen et al. propose honeypot techniques for ransomware detection, but their scope is not specifically tailored to ESXi [5], [6]. Our project addresses this gap by developing LuaGa, a honeypot system designed specifically to deceive and analyze ransomware targeting VMware ESXi. By focusing on ESXi-specific vulnerabilities, attack vectors, and services, LuaGa provides a targeted and effective defense mechanism against this evolving threat.

III. Methodology

A. Common virtualization attack methodology

Threat actors typically gain initial access through phishing, downloading malicious files, or exploiting known vulnerabilities in internet-facing assets. Once inside, they escalate privileges to obtain credentials for ESXi hosts or vCenter, validating their access by enabling SSH on ESXi servers, resetting server passwords, or executing remote commands using custom vSphere Installation Bundles (VIBs). The attackers then deploy ransomware on ESXi hosts and compromise backup systems to hinder recovery efforts, often engaging in double extortion by exfiltrating data and threatening public

release. The ransomware encrypts the /vmfs/volumes folder of the ESXi filesystem after shutting down all virtual machines, As demonstrated in Fig. 1.

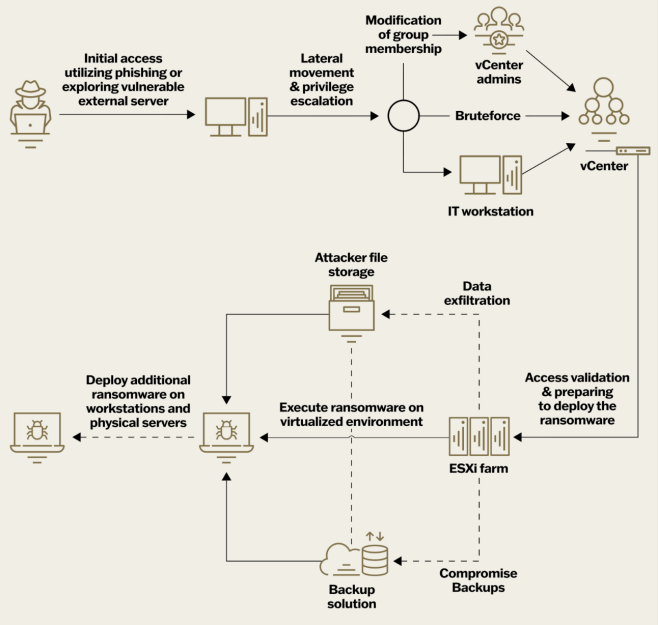

Fig. 1: ESXi Ransomware Attack Kill-Chain.

B. Defense methodology

Our defense methodology involves creating a simulated ESXi environment with various defensive modules:

- Simulation of Services: Replicating essential ESXi services to observe and analyze potential attack vectors.
- Honey Backup Files: Deploying decoy backup files designed to attract and trap attackers with fake data size, no resource-consuming.
- Activity Monitoring: Continuously monitoring all activities within the ESXi shell, virtual file system, virtual machine network, services, and network traffic to detect suspicious behavior.
- Comprehensive Logging: Logging all detected activities in real-time and sending these logs to a central console server for analysis.
- Alert Forwarding to SIEM/SOAR: Forwarding alerts generated from the console server to a Security Information and Event Management (SIEM) system for timely detection and response.

C. Environment simulation

As demonstrated in Fig. 2, threat actors typically gain initial access through phishing, malicious file downloads, or exploiting known vulnerabilities in internet-facing assets. Once inside, they escalate privileges to obtain credentials for ESXi hosts or vCenter, enabling SSH on ESXi servers, resetting server passwords, or executing remote commands with custom vSphere Installation Bundles (VIBs). They then deploy ransomware on ESXi hosts and compromise backup systems to hinder recovery efforts, often engaging in double extortion by exfiltrating data and threatening public release. The ransomware encrypts the /vmfs/volumes folder of the ESXi filesystem after shutting down all virtual machines.

1) Emulated ESXi Shell environment: Our approach differs by emulating nearly complete ESXi shell environments to trap attackers. We studied the real ESXi shell through official documentation and direct interaction to understand command syntax, outputs, and error messages, creating a realistic replica in the honeypot. Each ESXi command was recreated to produce convincing outputs, mimicking genuine system responses. We focused on core functionalities, implementing essential commands like ”esxcli” and ”vim-cmd,” along with common shell commands like ”ls,” ”cat,” and ”pwd”. This simulated shell serves as the main interface for attackers, enabling interaction with the underlying filesystem and services to reveal their tactics and intentions, shown as Fig 3. For detecting ransomware attacks, we have employed a sophisticated simulated execution environment for shell and Python scripts. This environment identifies malicious patterns within scripts using regular expressions, mimicking the execution of commands, and preventing any real-world harm. The honeypot also creates simulated encrypted files within the targeted directory to further deceive attackers. Strategic delays mimic real system processing times, keeping attackers engaged. All actions are diligently logged, providing a rich dataset for understanding attacker tactics and techniques.

2) Honey Backup files: The ”Virtual File System and Virtual Machine” module emulates a real ESXi system, including essential file structures and virtual machine files to capture and record malicious activities. It creates a detailed ESXi directory structure with key files like esx.conf, passwd, and shadow, and generates large virtual machine files with metadata that do not consume actual disk space. Symbolic links between files are displayed via the ls -la command. The module also generates fake Windows and Linux virtual machines with meaningful names and fake large file sizes, including configuration files like .vmdk, .vmx, .vmsn, and .nvram. Additionally, it periodically backs up ESXi system databases and virtual machines, compressing them into ZIP files. Data from attacker interactions is recorded for security analysis.

3) Dynamic Vulnerability response in emulated ESXi service & networking: Attackers exploit ESXi using services that are vulnerable to CVEs and zero-day exploits. By emulating typical system responses, we can deceive attackers into believing they are successfully infiltrating the system, leading them into a trapped shell. The ”Network and Services” module, one of four critical components, simulates essential VMware ESXi network services to attract and record malicious activities. This module listens on ports commonly used by ESXi, creating a realistic environment. To enhance authenticity, it uses deception techniques such as fake banners, delayed responses, simulated errors, and spoofed system information. Actions performed by attackers, including SSH access and ransomware execution, are executed through the simulated shell command. These

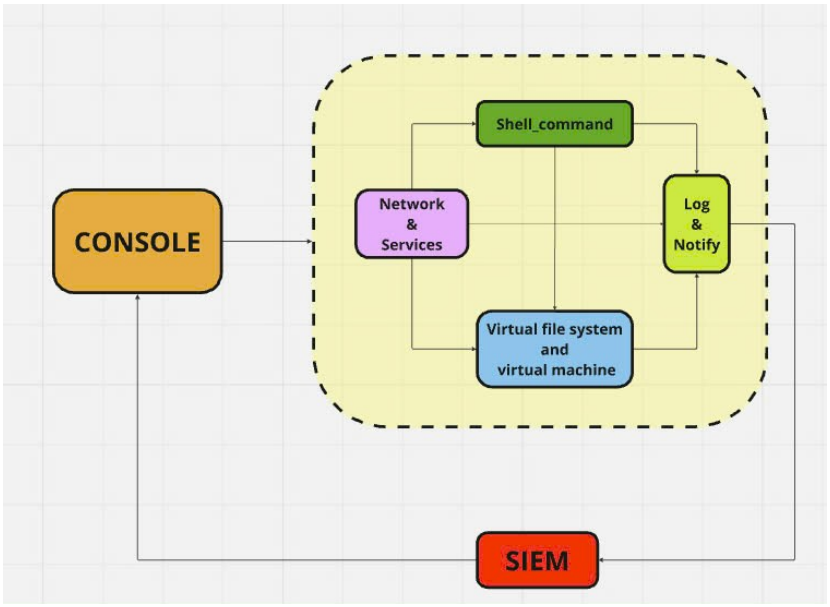

Fig. 2: The architecture of LUAGA.

Fig. 3: LUAGA console.

actions are meticulously recorded and processed by the Log and Notification module, ensuring comprehensive monitoring and analysis of malicious activities for further review and response.

4) Alerting & SIEM integration: Each module has its own logging and monitoring features. All activities are sent to the Console server in real-time, where events are scored and alerts are sent to SIEM/SOAR systems for quick response by security analysts. The "Log and Notify" module processes raw log data from honeypot components, linking real-time threat detection with detailed analysis [14]. It analyzes data for suspicious patterns, triggers alerts when thresholds are exceeded, and enables swift incident response. The module structures raw data (e.g., .json), enforces storage limits (Fig. 2), and uses log rotation for efficient management. Processed data is then sent to an SIEM system for in-depth analysis, correlation, and archival. This approach provides security teams with immediate threat awareness and actionable intelligence for proactive defense [15].

D. Dynamic defense with Centralize Console

The Honeypot Console acts in a Client-Server model, which offers a command-line interface (CLI) to manage and interact with the ESXi honeypots. It empowers users with various functionalities through easy-to-use flags, allowing you to create, deploy, monitor, and interact with your ESXi honeypot instances within an isolated and controlled environment using Docker technology, shown as Fig. 3. Security analysts can interact with honeypots to lure the attacker, understand them, and stop the attack.

E. Docker

Docker, a framework that allows us to create another layer of security between the operating system and honeypot. These benefits include container isolation, minimizing the risk of impacting the host system. This helps prevent attackers from easily performing lateral movement from the decoy system to the real system, enhancing security. Additionally, it allows administrators flexibility in deploying across various platforms (Linux, Windows, macOS) and environments (physical servers, virtual machines, cloud), wherever Docker is supported. The honeypot would be deployed within the container by using Console and it could contain all the modules of ESXi honeypot, shown as Fig. 2.

IV. Test-case scenario and Discussion

A. Test case scenario

In this subsection we present two scenarios to test the defensive performance of our proposed system.

1) Scenario 1 (Automated Attack using ESXiArgs): This scenario showcases an automated, opportunistic attack targeting known ESXi vulnerabilities.

- Scanning: [Network Scan] The attacker scans for vulnerable ESXi systems exposing the OpenSLP service using Shodan or masscan.
- Exploitation: [Exploit] The attacker leverages the ESXiArgs exploit to gain remote code execution by taking advantage of the OpenSLP vulnerability (CVE-2021-21974).
- Service Disruption: [Service Control] The attacker attempts to disable essential services like vCenter to prevent recovery or backups.
- Data Encryption: [Encryption] The core ransomware payload encrypts critical files like .vmx, .vmdk, and logs on the targeted datastore.
- Ransom Note: [Ransomware Activity] A ransom note is dropped, demanding payment for decryption keys.

2) Scenario 2 (Manual Attack using HelloKitty): This scenario involves a more hands-on approach, possibly indicative of a targeted attack or a more skilled attacker.

- Scanning: [Network Scan] The attacker scans for ESXi systems with open SSH ports.
- Brute-Force: [Credential Access] Attackers employ brute-force techniques using common or leaked credentials to gain SSH access.
- Privilege Escalation: [Privilege Escalation] Attackers exploit kernel vulnerabilities to gain root privileges on the ESXi host.
- Ransomware Upload: [File Transfer] The ransomware payload is uploaded using methods like scp or wget.
- Execution and Encryption: [Ransomware Activity] The attacker executes the ransomware, leading to data encryption and the placement of a ransom note.

B. Discussion

The two ransomware attack scenarios, shown as TABLE I, mimicking the ESXiArgs and HelloKitty attacks, offer a realistic representation of threats commonly encountered by ESXi systems. These scenarios are crafted based on observed attack patterns documented in the MITRE ATT&CK framework and real-world incidents involving these specific ransomware strains. They leverage common attacker tactics like exploiting known vulnerabilities (OpenSLP in ESXiArgs) and brute-forcing SSH credentials (HelloKitty).

There are trade-offs in the complexity and effectiveness of these scenarios. ESXiArgs, simulating an automated attack, is simpler to implement, relying on pattern recognition and basic command simulation, but may be less effective in revealing advanced attacker tactics. In contrast, HelloKitty, simulating a manual attack, enables more complex scenarios with privilege escalation, backdoor installation, and data exfiltration. This requires a more intricate honeypot setup with simulated vulnerabilities and sophisticated deception mechanisms, demanding greater development effort. TABLE II provides a clear overview of each attack step, assisting in understanding the flow of events and potential attack vectors, although an attacker may use a variety of tools and techniques.

V. Conclusion

This study introduces a novel deception-based proactive defense strategy against ransomware attacks in VMware ESXi systems. By developing the LUAGA simulation environment, we effectively used honeypots to attract, capture, and analyze ransomware behaviors. Our multi-layered approach, which includes monitoring and logging, significantly improved the detection and mitigation of ransomware threats. The proposed deception-based defense has high detection accuracy, effective in capturing detailed attacker behaviors, comprehensive logs for forensic analysis, moderate resource overhead, and scalable. Conventional Honeypot has Moderate to high detection accuracy, near real-time alerts, logs depend on interaction level, low to moderate resource overhead, and moderate scalability. Future research will refine the LUAGA environment, develop a web interface, upgrade emulation capabilities, integrate advanced machine learning for anomaly detection, and enhance real-time threat intelligence. This work contributes to a more resilient and secure IT infrastructure capable of resisting sophisticated ransomware attacks.

References

[1] M. Benmalek, "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 186–202, 2024.

[2] Z. Aalam, V. Kumar, and S. Gour, "A review paper on hypervisor and virtual machine security," *Journal of Physics: Conference Series*, vol. 1950, no. 1, p. 012027, 2021.

[3] J. E. Thomas and G. C. Galligher, "Improving backup system evaluations in information security risk assessments to combat ransomware," *Computer and Information Science*, vol. 11, no. 1, pp. 14–25, 2018.

[4] C. S. Georgina, F. Sakinah, M. R. Fadholi, S. Yazid, and W. Syafitri, "Deception based techniques against ransomwares: A systematic review," *Jurnal Teknik Informatika (Jutif)*, vol. 4, no. 3, pp. 529–553, Jun. 2023.

[5] S. Raja and K. Venkatesh, "Using honey pot technique ransomeware get detected," in *2023 International Conference on Computer Communication and Informatics (ICCCI)*, 2023, pp. 1–4.

[6] S. Sheen, K. A. Asmitha, and S. Venkatesan, "R-sentry: Deception based ransomware detection using file access patterns," *Computers and Electrical Engineering*, vol. 103, p. 108346, 2022.

[7] F. Guvçi and A. Şenol, "An improved protection approach for protecting from ransomware attacks," *Journal of Data Applications*, no. 1, pp. 69–82, 2023.

[8] X. Han, N. Kheir, and D. Balzarotti, "Deception techniques in computer security: A research perspective," *ACM Comput. Surv.*, vol. 51, no. 4, Jul. 2018.

[9] L. Zhang and V. Thing, "Three decades of deception techniques in active cyber defense - retrospect and outlook," *Computers & Security*, vol. 106, p. 102288, 2021.

[10] M. Baykara and R. Daş, "A survey on potential applications of honeypot technology in intrusion detection systems," *International Journal of Computer Networks and Applications (IJCNA)*, vol. 2, no. 5, pp. 203–211, 2015.

TABLE I: Two ransomware attack scenarios.

Scenario	Advantages	Disadvantages
ESXiArgs	- Simulates widespread, automated attacks - Relatively simple to implement	- Limited in scope, only covers specific vulnerability - Might not reveal advanced attacker techniques
HelloKitty	- Provides insights into more targeted, manual attacks - Can encompass a broader range of techniques, including privilege escalation and lateral movement	- Requires more sophisticated honeypot logic (e.g., simulating privilege escalation exploits). - Can be more complex to implement and analyze.

TABLE II: A clear overview of each attack step

Scenarios	Attack phase	Attacker behavior	Proposed solution: LuaGa	Cowrie	Honeytrap
ESXiArgs	Initial compromise	Attacker scan for vulnerable ESXi systems exposing the OpenSLP service using Shodan or masscan	Logs scan attempts, identified services (OpenSLP)	May not supported for services, logs scan attempts	May not supported for services, logs scan attempts
	Vulnerability exploitation	Attacker leverages the ESXiArgs exploit to gain remote code execution by exploiting OpenSLP vulnerability (CVE-2021-21974)	Simulates vulnerability, logs exploitation attempt and emulate results	May not supported for vulnerability, logs exploitation attempt	May not accurately simulate vulnerability, logs exploitation attempt
	Service disruption	Attacker attempts to disable essential services like vCenter to prevent recovery or backups	Logs commands used to disable services, simulates responses, sends alerts	Logs commands, may not support for specific command in ESXi	Logs commands used to disable services, may not simulate responses
	Data encryption	Ransomware payload encrypts critical files like .vmx, .vmdk, and logs on the targeted datastore	Simulates finding and encrypting files on datastores, creates fake ".ESXiARGS" files. Logs commands and arguments	Support creating script files but may not simulate encryption	Logs file access patterns, may not simulate encryption
	Ransom note deployment	Attacker leaves a ransom note demanding payment for decryption keys	Captures ransom note creation, logs content, forwards to central monitoring system	Capture files creation, logs to monitoring system	Captures ransom note creation, logs content
HelloKitty	Initial reconnaissance	Attacker scans for ESXi systems with open SSH ports using tools like nmap	Logs reconnaissance activity, alerts security team	Logs reconnaissance activity, identified services	Logs reconnaissance activity, identified services
	Credential theft	Attacker uses brute-force techniques or stolen credentials to gain SSH access to the ESXi host	Simulates SSH service, logs login attempts, alerts administrators	Simulates SSH brute-force, logs login attempts	Simulates SSH service, logs login attempts
	Privilege escalation	Attacker exploits kernel vulnerabilities to gain root privileges on the ESXi host	Logs commands used, simulates errors or displays fake success messages.	Logs commands, simulates responses, may not support simulation of privilege escalation on ESXi.	Logs privilege escalation attempts, may not simulate responses
	Ransomware deployment	Attacker uploads ransomware payload to the ESXi host using methods like scp or wget	Logs file transfer activities, simulates upload process, captures payload	Logs file transfer and capture commands, may not simulates process	Logs file transfer activities, may not simulate upload process
	Ransomware execution and encryption	Attacker executes ransomware, leading to data encryption and deployment of ransom note	Simulates file encryption and renaming by appending ".crypted " extension. Logs commands and arguments	Logs execution commands, may not simulate data encryption	Logs execution commands, may not simulate data encryption

[11] S. Kandanaarachchi, H. Ochiai, and A. Rao, "Honeyboost: Boosting honeypot performance with data fusion and anomaly detection," *Expert Systems with Applications*, vol. 201, p. 117073, 2022.

[12] W. Cabral, C. Valli, L. Sikos, and S. Wakeling, "Review and analysis of cowrie artefacts and their potential to be used deceptively," in *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2019, pp. 166–171.

[13] Y. Manzano, "Honeytraps , a network forensic tool," 2002. [Online]. Available: https://api.semanticscholar.org/CorpusID:18178060

[14] P. S. Negi, A. Garg, and R. Lal, "Intrusion detection and prevention using honeypot network for cloud security," in *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2020, pp. 129–132.

[15] P. Shelke and T. Hämäläinen, "Analysing multidimensional strategies for cyber threat detection in security monitoring," in *Proceedings of the European Conference on Cyber Warfare and Security*, vol. 23, no. 1. Academic Conferences International Ltd, 2024.