WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Unified Linux Attack Tools Based on MITRE ATT & CK Tactics

Ayush Gupta and Sharadadevi Kaganurmath

R.V. College of Engineering, Bengaluru, Karnataka, 560059

ABSTRACT

MITRE ATT&CK is a comprehensive knowledge database that captures adversary tactics and techniques based on real-world observations of incidents. Effectively defending against these attack tactics and techniques requires the development of tools capable of detecting and preventing them. A crucial aspect of this endeavor is the creation of a unified attack tool that can address all identified attack techniques and tactics. By harnessing the power of osquery—an operating system instrumentation, monitoring, and analytics framework—it becomes feasible to monitor and analyze the outcomes of these attacks in real-time and conduct global historic searches. This capability empowers security researchers and practitioners to identify potential vulnerabilities and enhance their defenses against attack techniques.

The integration of osquery with MITRE ATT&CK provides a powerful combination for security teams to proactively stay ahead of emerging threats. By leveraging osquery's flexible querying capabilities and rich dataset, security analysts can easily map observed behaviors and indicators of compromise to known adversary techniques and tactics documented in the MITRE ATT&CK framework. The real-time monitoring and analysis of attack results allow for swift detection and response to ongoing attacks, minimizing the potential impact on organizational assets. Additionally, the global historic search capability provided by osquery enables retrospective analysis of past incidents, aiding in the identification of patterns and trends that can inform proactive defense strategies.

Keywords: MITRE ATT&CK, osquery, vulnerability

1. Introduction

In today's digital age, cyber attacks have become a major concern for organizations of all sizes and industries. Cyber attackers are constantly evolving their tactics and techniques to bypass security measures and gain access to sensitive data. To combat these threats, security researchers and practitioners rely on frameworks like MITRE ATT&CK to document and understand these attack tactics and techniques.

This project aims to develop such a tool based on the MITRE ATT&CK tactics. By leveraging osqueries, an operating system instrumentation, monitoring, and analytics framework, we can monitor and analyze the results of these attacks in real-time and global historic search.

The unified attack tool will enable security researchers and practitioners to quickly identify potential vulnerabilities and improve their defenses against attack techniques. With the help of this tool, organizations can stay one step ahead of cyber attackers and safeguard their data and assets.

Integrating real-time threat intelligence with automated response capabilities, this tool can also help organizations respond quickly and effectively to cyber incidents, minimizing damage and reducing downtime.

2. Literature Review

A study by Johnson et al. (2020) delved into the effectiveness of osqueries as an instrumentation framework for real-time system monitoring. The research demonstrated the capability of osqueries in capturing and analyzing system-level events, providing deep visibility into potential security breaches. The study highlighted osqueries ability to generate alerts for suspicious activities, enabling security researchers to proactively detect and respond to threats. The integration of osqueries in the proposed approach offers the advantage of real-time monitoring and analysis, enabling organizations to identify potential vulnerabilities promptly. In a study conducted by Chen et al. (2019), the researchers explored the development of a unified attack tool to combat a wide range of attack techniques and tactics. The paper focused on consolidating various detection algorithms, rule sets, and preventive measures into a single tool. The unified attack tool facilitated comprehensive threat detection and prevention, simplifying security operations and enabling organizations to effectively defend against evolving threats. The integration of this unified tool in the proposed approach adds a crucial component to the defense strategy, allowing for centralized detection and prevention capabilities.

These research papers collectively highlight the benefits of integrating MITRE ATT&CK, osqueries, and a unified attack tool in improving defense against adversary tactics and techniques. The integration offers real-time monitoring, deep system visibility, and comprehensive threat detection and prevention capabilities. By leveraging the extensive knowledge base of MITRE ATT&CK, organizations can proactively identify and address potential

vulnerabilities. The osqueries framework enhances the approach by providing real-time monitoring and analysis of system-level events. The development of a unified attack tool further strengthens the defense strategy, enabling centralized detection and prevention mechanisms.

3. Hypothesis

By leveraging MITRE ATT&CK as a knowledge database, developing a unified attack tool that covers all identified attack techniques and tactics, and integrating osqueries for real-time monitoring and analysis, it is hypothesized that security researchers and practitioners will be able to effectively identify potential vulnerabilities and improve their defenses against adversary attack techniques.

The hypothesis assumes that utilizing the comprehensive knowledge base of MITRE ATT&CK, along with a unified attack tool, will enhance the capability to detect and prevent various attack tactics and techniques. Additionally, the integration of osqueries as an operating system instrumentation, monitoring, and analytics framework will enable real-time monitoring and global historic search, allowing for in-depth analysis of attack results.

It is expected that the combination of these elements will empower security researchers and practitioners to proactively identify potential vulnerabilities and enhance their defenses against attack techniques, leading to an improved security posture and better protection against emerging threats.

4. Methodology

1. This methodology involves using an ebpf (extended Berkeley Packet Filter) tool to capture system calls via kprobe. Kprobe is a debugging feature in the Linux kernel that allows for inserting probes (i.e., breakpoints) into kernel functions. After capturing the system calls using kprobe, the ebpf tool can be used to filter and analyze the data based on the specific parameters needed for the alerting mechanism.

2. The ebpf tool is used to log data about the process, PID (process ID), and complete ancestor list. The data captured by the ebpf tool can be stored in a database or log file for later analysis. This can be useful for identifying patterns of behavior or for forensic analysis in the event of a security breach. The ancestor list is the chain of processes that have spawned each other, starting from the root process.

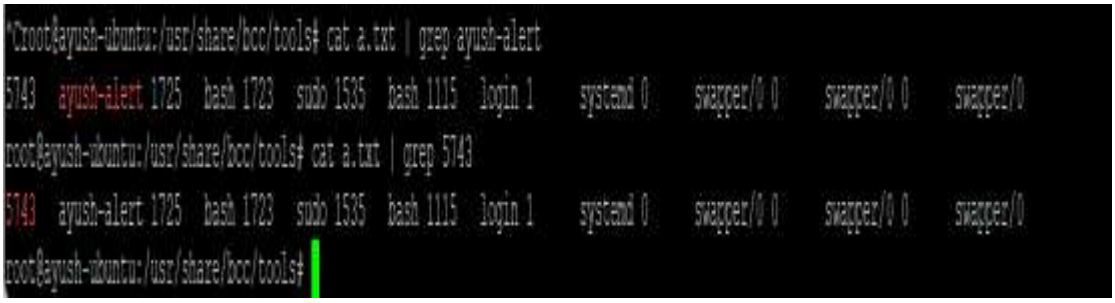
3. The event alert table can be created based on known attack patterns or suspicious activity identified through threat intelligence feeds or other security sources. The parameters used to trigger an alert can be refined over time based on the analysis of captured data and the effectiveness of previous alerts. The security team creates an event alert table, which captures specified attacks. This table includes data fields that, if matched to any of the alerted parameters, will create an alert.

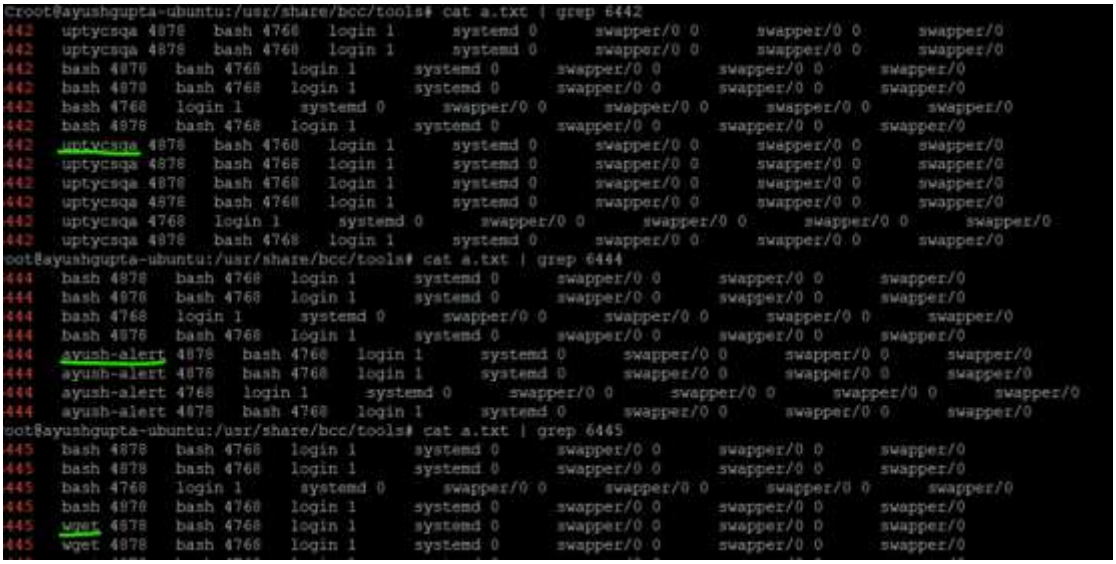
4. When an alert is triggered, the detection graph can be used to visualize the event and its relationship to other alerts or system events. This can help to identify the scope and severity of the attack and to determine the appropriate response.

5. Depending on the severity of the alert, the security team may take various actions to mitigate the threat. This could include blocking network traffic or shutting down affected systems, or may involve more extensive forensic analysis to identify the source and extent of the attack.

5. Result and Analysis

The process_pid, process name, parent_pid, parent process name followed by ancestor list is displayed which are marked as suspicious





All the processes marked as an alert are getting registered and a complete ancestor list is being generated for all the alerted processes. This representation is further segregated into process events, socket events, file events, dns lookup events and http events depending on the type of telemetry being called. The nodes are marked into different colors depending on the severity of the alert to mitigate the process and have more knowledge on the suspicious processes.

6. Conclusion and Future Work

MITRE ATT&CK serves as a valuable and extensive knowledge database that captures adversary tactics and techniques based on real-world incidents. To effectively defend against these evolving attack tactics and techniques, it is crucial to develop robust detection and prevention tools. The creation of a unified attack tool that addresses all identified attack techniques and tactics plays a vital role in this endeavor.By leveraging osqueries, an operating system instrumentation, monitoring, and analytics framework, it becomes possible to monitor and analyze the outcomes of these attacks in real-time and through global historic searches. This powerful capability empowers security researchers and practitioners to proactively identify potential vulnerabilities and enhance their defenses against various attack techniques.

Future enhancements would include integration with Machine Learning and AI: applying machine learning and artificial intelligence techniques to MITRE ATT&CK and osquery can improve the detection and prevention of attacks by analyzing large volumes of data, these technologies can identify patterns, anomalies, and potential threats that may go unnoticed by traditional rule-based approaches. Expanded coverage and regular updates: continuously expanding and updating MITRE ATT&CK to encompass a broader range of attack techniques and tactics will enhance its relevance and effectiveness. This includes capturing emerging and sophisticated attack methods and providing timely updates to the knowledge base.

7. References

[1] Operating Systems: https://tryhackme.com/dashboard

[2] https://www.cybrary.it/

[3] https://bjpcjp.github.io/pdfs/devops/linux-commands-handbook.pdf

[4] Book for Unix by Sumitabha Das:

https://v2vclass.com/images/coursepdf/bsc-cssem1/bsc-cssem1/foss/freeopensourcesoftware.pdf

[5] Bendovschi, Andreea (2015). "Cyber-Attacks – Trends, Patterns and Security Countermeasures"

[6] Ritchie, Dennis M. (January 1993). "The Development of the C Language" . Archived from the original on 11 June 2015. Retrieved 30 July 2022.

[7] https://www.infoq.com/articles/gentle-linux-ebpf-introduction

[8] "What Is Linux: An Overview of the Linux Operating System". Medium. Archived from the original on June 12, 2020. Retrieved December 21, 2019

[9] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing MITRE ATT&CK cyber-security culture framework,” Sensors,vol.21,no.9,p.3267,2021.

[10] D J Bodeau, C D McCollum and D B Fox ,"Cyber threat modeling : Survey, assessment, and representative framework,"MITRE CORP MCLEAN VA MCLEAN, Tech.Rep ,2018.

[11] Encarnacion ,Lewis. "Perform A Man in the middle attack with Kali Linux and Ettercap"

[12] Chiem Trieu Phong, "A study of penetration Testing Tools and Approaches" Eds. Auckland :Academic,2014

[13] A. Georgiadou, S . Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK risk using a cyber-security culture framework," Sensors, vol.21, no.9 ,p.3267, 2021.

[14] G.Cascavilla, D.A. Tamburri, and W.-J.Van Den Heuvel," Cyber Crime Threat Intelligence: A system at ic multi-vocal literature review," Computers & Security, vol.105,p.102258,2021.

[15] S. Kriaand Y.Chaabane, "Sec KG: Leveraging attack detection and prediction using knowledge graphs,"in 2021 12th International Conference on Information and Communication Systems (ICICS). IEEE, 2021,pp.112–119

[16] Rebecca Bace and Peter Mell, "Intrusion Detection System", NIST special publication on Intrusion Detection System, 2001.

[17] Jeff Reinhard, "Network Intrusion Detection System", Pen Tele Data, Palmerton

[18] John McHugh et al, "The Role of Intrusion Detection Systems", IEEE Software September/October 2000. doi:10.1109/52.877859

[19] Taylor Merry, "Linux Kernel Hardening", SANS Institute- 2003.

[20] Tejinder Aulakh, "Intrusion Detection and Prevention System: CGI Attacks", The Faculty of the Department of Computer Science, San Jose State University, 2009.

[21] K. Ilgun. "USTAT - A Real-time Intrusion Detection System for UNIX," Master's Thesis, University of California at Santa Barbara, Nov. 1992.

[22] I.B. Tekaya, M. Graiet, and B. Ayeb. Intrusion detection in Linux/Unix commands using formal verification. In The Fourth IEEE International Symposium on Innovation in Information and Communication Technology (2011

[23] M. Santana, "Chapter 6 - Linux and Unix Security, Computer and Information Security" Handbook 2009, pp. 79-92.

[24] J. P. Anderson, "Computer Security Threat Monitoring and Surveillance," Technical report, Washing, PA, James P. Anderson Co., 1980.

[25] F.Mottini,"Osquery-ATT&CK,"https://github.com/teoseller/ osquery-attack,2022