International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Automation Response To Cyber Threat

Vinay Dutt Jangampet
Staff App Ops Engineer,
Intuit
yanivdutt@gmail.com

Abstract:

In the internet world, cyberattacks raise the level of risk, which in turn increases the level of risk for organizations and service providers. As a result of the fact that late actions cause damage to reputations and loss in business costs, an automated response should be implemented in any cyber-attack. Most of it involves internet use, which is unsafe without security measures. It is necessary to initiate a response to address the security issue of our systems.

I. Implementing Automation Response

To implement Automation responses in any system, we must interact with the operating system to perform specific actions under certain conditions. It can be command execution on the operating system. The automated commands can be executed as an existing script. In the operating system, as a daemon process. The problem is that we want to trigger an action upon which our script will execute. It can be obtained by integrating third-party apps such as security information event management (SIEM) and Security orchestration automation response (SOAR) solutions. We can combine triggers based on an event in the form of a log.

A. Demon Scripts Logic to Prevent Attack

To make a demon script, we have to make PowerShell or command line instructions such that they are being executed on the system's boot-up so they are running without user interference. In the script, we can see the monitor of the traffic coming to our endpoint. Suppose it's a Windows Server or Ubuntu Serve, and we monitor the active sessions. Suppose we have a DDoS attack; too many requests are coming to our end device. In that case, we can block the current request sessions by creating the rules inside our script in case of a DDoS attack. If we assume 100 requests from the same IP address come to our server in less than 10 seconds, we must block that IP address in our firewall. To do that, we create a script that monitors the incoming and outgoing traffic and compares it to our rules on the violations. It makes the source IP address and puts it in the block list of the firewall. In the Linux case, it will be added to the block list of the IP tables firewall rules. To prevent a brute force attack, we can make a script that monitors the system login activity, and upon more failures than the required time, we can add the IP address to the block list, and we don't need a third-party service; this is our script pre-built in our endpoint. We can also make a list of blocked IP addresses, which are constantly being updated, and tell the hand that if any connections incoming or outgoing go to that particular IP address or domain name, it should be blocked, and it will discard the connections on incoming and outgoing connections. We can use a third-party

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

service that maintains this service's blocked IP addresses and domain names.

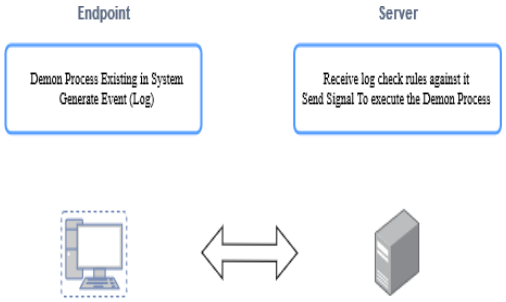

Fig 1.1

A. Demon Scripts Logic to Prevent Attack

We can integrate our system logs with security information event management (SIEM) solutions to monitor the records. In addition, we have blinded this rule ID threshold level of the attack against the forms, and we can send a signal up to this log level (command to execute the script we created to respond actively). WAZUH, which stands for Elastic Stack as Logs (SIEM) solutions, is the most widely used. Commercial solutions for security information and event management (SIEM), such as IBM Qradar and Splunk, can integrate the records and execute the commands based on a particular log rule ID. In addition, we will keep an eye on it in the papers. After the script has been executed, it will make a record of its execution in the directory that we have specified. This will allow us to determine whether or not our documents have been executed. We need to have knowledge of threat intelligence in the open-source community to keep the block list of IP addresses and domain names up-to-date. This information can be found in the virus total, missed threat intelligence, abuse IP, and other premium threat intelligence such as Cisco Talos, IBM X intelligence, and other similar resources. They all possess the most recent malicious IP address and URL that can be discovered in cyberattacks. Combining all of these integrations can assist us in developing an automated response system to cyber-attacks, reducing the time required to identify the threat.

B. Detection Compromised system commands

Once the system is compromised due to any cyber attack, an attacker will try to do some activity, and event anyone executed creates a process. If we have configured advance monitoring, we can monitor the command being executed upon execution, which means we can watch any commands or PowerShell execution now we have observed those logs. In those logs, if we see an order not being executed by us, it is evident that our system has been compromised. We can make a script to monitor the current events of command execution. Upon that execution, we can make a custom active response action to isolate the system or block the recent network sessions and send an alert to another system solution, which can be used in reporting and monitoring.

A. Reporting and monitoring

A customized script can be made to send the log created for any of the actions to ship to a mail or SMS by attaching the SMPT addresses in hand to automatically deliver an email of the record and customized data we stated upon execution of that type of script we made. It sends the form to our mail or by SMS, and in active time, whenever the attacks happen, it is reported to our mobile or by email. Even this automation reporting is attached to our SIEM solutions to send alerts to run time and further customizations of customized levels of logs. We receive a record as an example that an unknown command has been executed. Our system is isolated, so before isolation, our script is performed.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

We have received an alert in the mail or SMS that the device is isolated due to cyber-attacks, and such scenarios can be easily tackled.

References

[1] U. Bartwal, S. Mukhopadhyay, R. Negi and S. Shukla, "Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots," 2022 IEEE Conference on Dependable and Secure Computing (DSC), Edinburgh, United Kingdom, 2022, pp. 1-8, doi: 10.1109/DSC54232.2022.9888808.

[2] D. Tuličić, D. Delija, G. Sirovatka and M. Mrkoci, "Windows Admin GUI Model for Learning PowerShell Commands," 2023 46th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2023, pp. 590-595, doi: 10.23919/MIPRO57284.2023.10159862.

[3] Fang, Yong & Zhou, Xiangyu & Huang, Cheng. (2021). A practical method for detecting malicious PowerShell scripts based on hybrid features. Neurocomputing. 448. 10.1016/j.neucom.2021.03.117.