Intrusion Detection using Security Onion Based on Kill Chain Approach

Beatrice Ssowmiya J[1], Prabhakaran S[2]

[1]Cyber Security Research Center, SRM University, Chennai, India

[2]M.Tech, Information Security and Cyber Forensics, SRM University, Chennai, India

Abstract: ***Log Management and Intrusion Detection solution have been evolving for years. But, it remains a biggest challenge for every organization of all sizes to meet the operational, audit and security needs using these solutions. A new class of threats, appropriately dubbed the "Advanced Persistent Threat" (APT), is a network attack in which unauthorized person gains access to an organization network and stays there undetected for a long period of time to steal confidential data. This paper presents a solution for intrusion detection based on Advanced Persistent Threat and network based intrusion detection using Security Onion Linux Distribution with the implementation of Kill Chain approach. It walks through the logging, monitoring, correlating and alerting approach necessary for security, compliance and quality of service.***

Keywords: Intrusion detection, kill chain, logs, correlation, intrusion analysis, intelligence, threat, APT, computer network defense, attacks.

1. Introduction

Since, global computer networks have existed, so have malicious users intent on exploiting vulnerabilities. Early developments of threats to computer networks involved in self-propagating code. Changes over time in anti-virus technology significantly reduced this automated risk. More recently, a new class of threats, committed on the compromise of data for economic or military advancement, emerged as the largest element of risk facing some industries. This class of threats is named as "Advanced Persistent Treat," or APT.

In a common attack, the intruder tries to get in and out as quickly as possible in order to avoid detection by the Intrusion detection system. But, in APT attack, the goal is to achieve ongoing access for long term by rewrite code continuously and employ refined evasion techniques. An APT attacker often uses spear fishing, social engineering to gain access to the network through legitimate means.

Although APT attacks are difficult to identify, detecting anomalies in outbound data is the best way for an administrator to discover that his network has been the target of an APT attack. Kill Chain is a phase-based model to describe the stages of an attack, which also helps inform ways to prevent such attacks and detect in which stage the attacker is in. The main thesis of the paper is to detect intrusion by collecting the logs, analysis the logs and correlating the collected logs by using Security Onion Linux Distribution with the concept based on Kill Chain.

2. Literature Review

A. Security Information and Event Management (SIEM)

Security information and event management (SIEM) is a term for software products and services combining security information management (SIM) and security event management (SEM). SIEM technology provides real-time analysis of logs will grab's the entire event (security and audit events) from all the assets presented in the organizations like switches, firewall, router, database, Intrusion Detection System (IDS), etc. It collects and converts them into human readable format. So, as an admin can understand what happen on network and the particular host system and then does correlation. Correlation is finding out bigger picture from the different pieces. In computer term, collecting different logs from the network assets and shows how an intrusion is happened. Capabilities of Security Information and Event Management (SIEM): Data aggregation, correlation, alerting, Dashboard, compliance, retention, and forensic analysis.[1]

B. Advanced persistent threat (APT)

An advanced persistent threat (APT) is a network attack in which an attacker gains access to a network and stays there undetected for a long period of time. The objective of an APT attack is to steal data rather than to cause damage to the network or organization. APT attacks target organizations such as national defense, manufacturing and the financial industry.

In a common attack, the attacker tries to get in and out as quickly as possible in order to avoid detection by the network's intrusion detection system (IDS). In an APT attack, the goal is not to get in and out but to achieve ongoing access to maintain access without discovery, the intruder must continuously rewrite code and employ erudite evasion techniques. Some APTs are so complex that they require a full time administrator. An APT attacker often uses spear fishing, a type of social engineering, to gain access to the network through legitimate means. Once access has been achieved, the attacker establishes a back door.

The next step is to gather valid user credentials and move across the network, installing more back doors. The back doors allow the attacker to install fake utilities and create a "ghost infrastructure" for distributing malware that remains hidden in plain sight.

APT attacks are difficult to identify, detecting anomalies in outbound data is the best way for an administrator to discover that his network has been the target of an APT attack. Kill Chain is one of the approach used to find the APT attacks and determine in which stage the attacker is in.[2]

C. Cyber Kill Chain Approach

“Kill Chain” is a phase-based model to describe the stages of an attack, which also helps inform ways to prevent such attacks. U.S military targeting doctrine defines the steps of this process as find, fix, track, target, engage, assess. Find opponent targets suitable for engagement; fix their location; track and observe; target with suitable weapon or asset to create desired effects; employ opponent; assess effects (U.S. Department of Defense, 2007). This is an integrated, end-to-end process which is described as a “chain” because any one deficiency will interrupt the entire process.

This paper presents a Cyber kill chain model, one specifically for intrusions. The principle of an intrusion is that the aggressor must develop a payload to breach a trusted boundary, establish a presence inside a trusted environment, and from that presence, take actions towards their objectives, be they moving across inside the environment or violating the confidentiality, integrity, or availability of a system in the environment. The intrusion kill chain is defined as reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives.

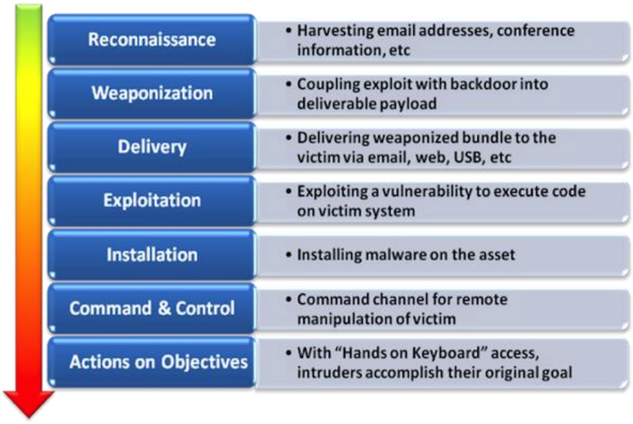

Reconnaissance
• Harvesting email addresses, conference information, etc
Weaponization
• Coupling exploit with backdoor into deliverable payload
Delivery
• Delivering weaponized bundle to the victim via email, web, USB, etc
Exploitation
• Exploiting a vulnerability to execute code on victim system
Installation
• Installing malware on the asset
Command & Control
• Command channel for remote manipulation of victim
Actions on Objectives
• With “Hands on Keyboard” access, intruders accomplish their original goal

Figure 1: Kill Chain Stages

a) *Reconnaissance* - Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies similar like information gathering.

b) *Weaponization* - Coupling a remote access Trojan with an exploit into a deliverable payload, typically by means of an automated tool. Client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

c) *Delivery* - Transmission of the weapon to the targeted environment via email, web, USB, etc.

d) *Exploitation* - After the weapon is delivered to victim system, exploitation triggers intruders’ code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.

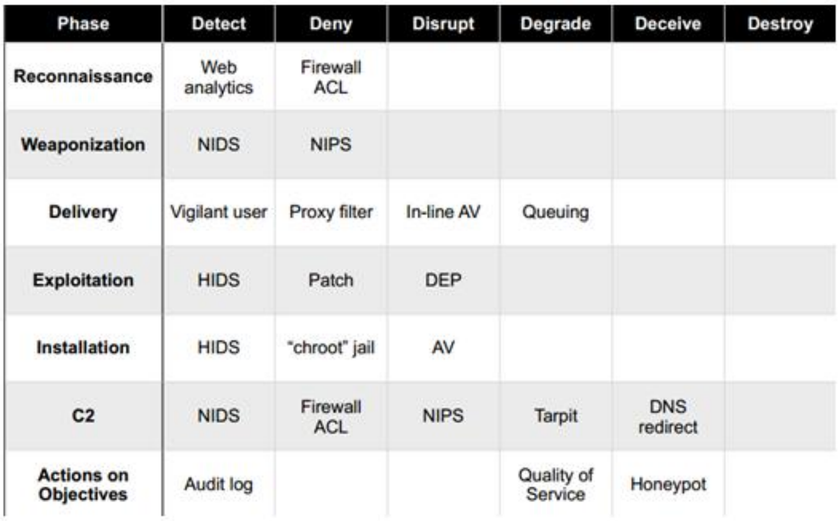
e) *Installation* - Installation of a remote access trojan or backdoor on the victim system allows the opponent to maintain persistence inside the environment.

f) *Command and Control (C2)* - compromised hosts must beacon outbound to an internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have “hands on the keyboard” access inside the target environment.

g) *Actions on Objectives* -after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violationsof data integrity or availability are potential objectives as well. [3]

D. Course of Action

Defenders can measure the performance as well as the effectiveness of these actions, and plan investment roadmaps to correct any capability gaps.



Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Figure 2: Course for action matrix

Fig.2, represents a course of action matrix using the actions of detect, deny, disrupt, degrade, deceive, and destroy from DoD information operations (IO) doctrine (U.S. Department of Defense, 2006). This matrix represents in the exploitation phase, for example, that host intrusion detection systems (HIDS) can passively *detect* exploits, patching *denies* exploitation altogether, and data execution prevention (DEP) can *disrupt* the exploit once it initiates. Illustrating the spectrum of capabilities defenders can employ, the matrix includes traditional systems like network intrusion detection systems (NIDS) and firewall access control lists (ACL), system hardening best practices like audit logging, but also vigilant users themselves who can detect suspicious activity.

E. Log Management Functions

Log management infrastructures typically perform several functions that help in the storage, analysis, and disposal of log data. These functions are normally performed in such a way that they do not alter the original logs.

General functions of log management infrastructure include log parsing, event filtering and event aggregation. On the storage side, log management has to provide for log rotation, log archival, log compression, log reduction, log conversion, log normalization and log file integrity. Event correlation, log viewing and log reporting are some of the analysis functions of a log management infrastructure. Following are the log management benefits:

- Detect/Prevent Unauthorized Access and insider Abuse
- Meet Regulatory Requirement.
- Forensic Analysis and Correlation.
- Ensure Regulatory Compliance.
- Track Suspicious Behavior.
- IT Troubleshooting and Network Operation.
- Monitor User Activity.
- Deliver Reports to Departments.
- Measure Application Performance.
- Achieve ROI or Cost Reduction in System Maintenance.[4]

3. Design

Organizations should establish logging standards and procedures to ensure that adequate information is collected by logs and security software and that the data is reviewed regularly. The length of time to maintain log data is dependent on several factors, including the organization’s data retention policies and the volume of data. As each business has different needs and regulatory requirements, legal counsel should be obtained to determine the appropriate retention schedule for logs.

This paper uses the Security Onion (SO) created by Doug Burks for detecting intrusion (Especially APT attacks) in a network, based on Kill Chain approach. Snort is used as the intrusion detection engine. Sguil, Squert and Snorby provide the management console to view and classify sensor alerts. OSSEC’s ability for log analysis, integrity checking, rootkit detection, real-time alerting and active response across platforms makes it an excellent choice for host based intrusion detection. This paper utilizes OSSEC as the log collector on the SO monitor to archive logs as well as review log files in real time, while inspecting them for known attack patterns.

A. Security Onion

Security Onion is a Linux distro for IDS (Intrusion Detection) and NSM (Network Security Monitoring). It's based on Ubuntu and contains Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, NetworkMiner, and many other security tools.

B. Snort

Snort is an open source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, it is the most widely deployed IDS/IPS technology worldwide.

C. Squert

Squert is a web application that is used to query and view event data stored in a Sguil database (typically IDS alert data). Squert is a visual tool that attempts to provide additional context to events through the use of metadata, time series representations and weighted and logically grouped result sets.

D. OSSEC

OSSEC is an Open Source Host-based Intrusion Detection System (HIDS). It performs log analysis, integrity checking, Windows registry monitoring, rootkit detection, real-time alerting and active response. It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris and Windows.

4. Conclusion

There are hundreds of millions of malware variations, which make it extremely challenging to protect organizations from APT. While APT activities are stealthy and hard to detect, the command and control network traffic associated with APT can be detected at the network layer level. Deep log analyses and log correlation from various sources can be useful in detecting APT activities. Agents can be used to collect logs (TCP and UDP) directly from assets into a syslog server. Then a Security Information and Event Management (SIEM) tool can correlate and analyze logs.

This paper shows the importance of log managements and network monitoring for the effective security monitoring and compliance of an organization. The solution is based on a framework provided by the Security Onion, which makes it possible to integrate necessary applications on one platform which provide a cost effective logging, monitoring and alerting by correlating the logs based kill chain approach to identify the intrusion.

References

[1] “The Complete Guide to Log and Event Management” by Dr. Anton Chuvakin (http://www.chuvakin.org)
[2] “Advanced Persistent Threats: Detection, Protection and Prevention”, by Barbara Hudson, Senior Product Marketing Manager
[3] “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and

Intrusion Kill Chains", by Eric M. Hutchins, Michael J. Cloppert.

[4] "Logging and Monitoring to Detect Network Intrusion and Compliance Violations in the Environment" by Sunil Gupta

[5] "Log Correlation for Intrusion Detection" Cristina Abad, Jed Taylor, CigdemSengul