International Journal For Technological Research In Engineering
Volume 5, Issue 7, March-2018 *ISSN (Online): 2347 - 4718*

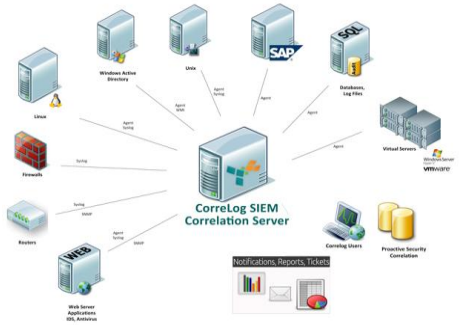
EXPLICIT NETWORK SECURITY HARDENING USING ACTIVE DEFENSE TECHNOLOGY FOR DOD SERVERS

P. Elamparithi[1], P. Raja Ganesh[2], R.Sanoj Kumar[3]
[1]Assistant Professor, [2,3]Student
Department of Computer Science & Engineering, AAA College of Engineering & Technology, Sivakasi.

ABSTRACT: Information security is a rising concern today in this era of the internet because of the rapid development of the new attack techniques. The pre-existing security mechanisms such as traditional Intrusion Detection Systems, firewalls and encryption are the passive defense mechanisms. This has paved a path to emerging interest in the Active Defense technology like Honeypots. Honeypots are fake computer Systems which appears to be vulnerable to exploit though it actually prevents access to valuable sensitive data and administrative controls. A well designed and developed Honeypot provide data to the research community to study issues in network and information security. In this paper we examine different Types of Honeypots, Honeypot concepts and approaches in order to determine how we can intend measures to enhance security using these technologies.
Keywords: Snort, Artillery, Honeyd, NOVA

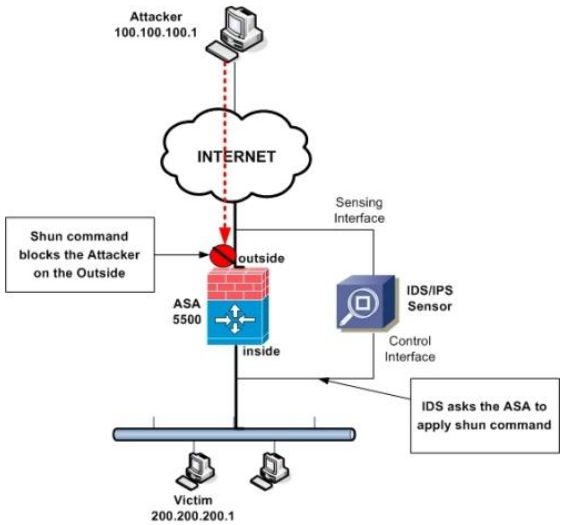
I. INTRODUCTION

As attacks show tremendous complexity due tothe sophistication, organization and inspiration of adversaries, defensive strategies must be enriched in order to remain active.Looking at the framework of an intrusion using a kill chain approach allows protectors to calculatetheir ability to suitably thwart an attack before the attackersattain their destination, which is typically data exfiltration. The term "kill chain" has been adapted from a military context and can be used describe the progression and phases of an intrusion. The related approach involves avaluation of security posture as well as intelligence gathering abilities at each individual phase of an intrusion.Because of the breadth of the attack surface as well as the current deficiencies in preventive controls, successful attacks against endpoints allow adversaries to accomplish several early phases of an intrusion while avoiding detection. Once the initial attack vector allows a Remote Access Trojan or backdoor to be installed on a victim's endpoint, an attacker has a pivot point into the internal network with several possibilities.



At this point, all reconnaissance occurs behind the perimeter firewalls; command and control traffic can be encrypted and tunneled within other legitimate protocols to bypass egress inspection and filtering systems. SIEM and properly configured IDS devices are essential to detecting these types of attacks and post-exploitation activities. However, even with these systems in place, attackers are still successfully evading detection while locating and exfiltration of the data they desire. With the implementation of active defense systems on non-Internet facing, private networks, defenders can slow down and contain attackers who have already breached perimeter defenses. Furthermore, these systems can be used to augment the effectiveness of internal IDS/IPS and SIEM systems. Active defense systems can be defined as "any measures originated by the defender against the attacker" and broken into categories of "counterattack, preemptive attack, and active deception." Counterattack techniques and Pre-emptive attacks are outside the scope of this paper due to the legal liabilities associated with these actions.

II. RELATED WORK



The existing Linux version of Artillery provides several features, including honeypot functionality, file system monitoring, brute-force and DoS protections, and threat intelligence feeds. The pre-available snort system is used only for traffic to and from a network.Snort is a tool used only for monitoring network traffic while artillery is used only for monitoring local file system. Being distinct tools a DoD server with high security cannot be monitored on the whole efficiently, hence we use our system to integrate and provide a maximal efficiency with minimal maintenance.

III. SYSTEM DESIGN

1. Security Information and Event Management (SIEM):

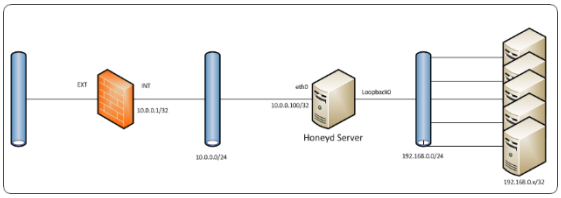
In the field of computer security, security information and event management (SIEM) software products and services combine security information management (SIM) and security event management (SEM). They provide real-time scrutiny of security alerts produced by applications and network hardware. SIEMS can detect covert, malicious communications and encrypted channels.

2. Intrusion Detection System (IDS):

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malevolent activity or policy violations. Any identified activity or destruction is typically informed either to an administrator or collected centrally using a security evidence and event management (SIEM) system. Some IDS have the ability to respond to intrusions.

3. Artillery:

Artillery is an open-source Python application created by David Kennedy fromTrustedSec, also the creator of the popular Social Engineer Toolkit (SET). Artillery providesdefenders the ability to install this active defense utility directly on a system that needs to beprotected, and an important benefit of Artillery is the ability to install this utility on existingservers without affecting their functionality on the network. The Python-based application runson Linux, Windows, and Mac OS X; however, the Linux version is the most full-featured. TheLinux version of Artillery offers several features, including honeypot functionality, filesystem monitoring, brute-force and DoS protections, and threat intelligence feeds.



IV. PROPOSED WORK

Once Nova is installed, configured and running on a private network, the system can generate Snort rules automatically to isolate when honeypots receive connections from unauthorized sources. IP ranges can be defined and categorized in the Snort configuration file so that Novarelated alerts will not be prompted when connections are made to the real servers on the network. For example, if the Nova Haystack uses the 192.168.78.132-192.168.78.135 IP addresses, the following declaration could allow the haystack to be utilized in Snort rules. Once the addresses of the Nova haystack are defined, a rule can be created to alert and tag sources coming from any other IP address to the haystack. This affordsprotectors with aimproved picture of what an attacker is doing on the network.

```
alert tcp any any -> $NOVA_HAYSTACK
any (msg: "Internal IP to Nova node";priority:
2;tag: host, 300, seconds, src; sid: 1000002;)
```

The tools established below are designed based on the following network design and scenario. Consider the network layout where an attacker has used malware or a client-side attack to compromise a PC on a company's internal network. The internal PC user network (172.20.10.0/24) is not segmented from an internal server network (192.168.78.0/24) with a firewall, but a Snort IDS sensor is inspecting all connections between the two networks. The server network consists of several Windows and Linux-based systems. The attacker on the network has installed a Remote Access Trojan on the PC with the address 172.20.10.128.A skilled attacker would not make as much clumsy "noise" on the network as shown in the above examples, but active defense systems limit the amount of reconnaissance and number of mistakes an attacker can make before being detected. They also slow down an attacker's ability to accurately map an internal network using active reconnaissance techniques after breaching perimeter defenses. Since these systems can be implemented on spare hardware and have limited to no negative impact on production networks, they can be a quick and easy win for network administrators to augment their defenses.

V. CONCLUSION

Although active defense techniques can be used on Internet-facing systems, their value may be limited since Internet-facing hosts are expected to be on the receiving end of continuous reconnaissance. Acting as yet another layer of security, active defense systems can be implemented to specifically identify, alert on, and hinder this type of activity.Internal systems providing active deception capabilities can increase the cost and time required for an attacker to successfully exfiltration data. However,active defense, SIEM and IDS systems are more useful when integrated together than when operating individually. When IDS alerts for honeypot IP addresses and ports are triggered, a single alert does notprovide significant value and could be caused by a misconfigured system or a simple typo. On the other hand, when a SIEM can present one of these alerts with output from an active defense system as well as any other events associated with the potential offender.

VI. FUTURE WORK

The research on honeypot technology can be categorizedinto five major areas:

- New types of honeypots to deal with emergent newsecurity threats.
- To reduce the maintenance and configuration cost of honeypots as well as to improve the threat detections accuracy.
- Honeypot output data utilization to improve the accuracy in threat detections.

REFERENCES

[1] P. H. Corredor and M. E. Ruiz, "Against all odds," IEEE Power Energy Mag., vol. 9, no. 2, pp. 59–66, Mar./Apr. 2011.

[2] E. White, New Attack on Electricity Lines in Yemen. [Online].

[3] D. Bienstock and A. Verma, "The problem in power grids: New models, formulations, and numerical experiments," SIAM J. Optimiz., vol. 20, no. 5, pp. 2352–2380, 2010.
[4] D. A. Jones, C. E. Davis, M. A. Turnquist, and L. K. Nozick, "Physical security and vulnerability modeling for infrastructure facilities," in Proc. Hawaii Int. Conf. Syst. Sci., 2006.
[5] G. Brown, M. Carlyle, J. Salmeron, and K. Wood, "Defending critical infrastructure," Interfaces, vol. 36, no. 6, pp. 530–544, 2006.
[6] R. Powell, "Allocating defensive resources with private information about vulnerability," Amer. Polit. Sci. Rev., vol. 101, no. 4, pp. 799–809, 2007.
[7] G. Chen, Z. Y. Dong, D. J. Hill, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted attacks," IEEE Trans. Power Syst, vol. 26, no. 3, pp. 1000–1009, Aug. 2011.

