Global Information Assurance Certification Paper

Need for pure integration between intrusion detection and vulnerability assessment

Introduction:

The current times have been depicted as the golden age of hacking due to the large number of vulnerabilities that have been found in the systems on the Internet and the sophistication of tools available for the attackers. Every day more and more vulnerabilities are discovered and published. It has become increasingly difficult for the Information Security professional to keep track of known vulnerabilities and to monitor for these attacks on their systems. In many instances, there is a time lag between the announcement of the vulnerability and the vendor issuing a patch. In addition, configuration management and testing need to be done before a patch issued by a vendor can be applied on a production system. It is therefore critical for the Information Security professional to identify existing system vulnerabilities and monitor for intrusions and attacks based on them until the vendor issues a patch and it is applied.

The Problem:

One of the primary issues faced by the Security professional is the customization of rules for the host and network based Intrusion detection systems to monitor for attacks based on its known vulnerabilities. Most of the current Intrusion detection systems monitor for generic attacks and probes and it is up to the security engineer to manually customize the filters to their unique requirements. While most of the vulnerabilities are addressed by the generic rule-sets, there are many instances when new rules need to be created to meet unique requirements and other instances when inapplicable rules need to be removed.

Lack of direct information exchange between vulnerability assessment and Intrusion detection systems leaves it to the security engineer to manually update Intrusion detection systems with rules for all new vulnerabilities. The daily inflow of new vulnerabilities and the lack of resources is causing Intrusion detection filters to be out of date and intrusions based on newer vulnerabilities to go undetected.

Current Attack Trends:

Traditionally attackers perform scans and probes of networks and do reconnaissance prior to launching attacks. Due to the automated nature of attack tools and the increasing use of worm like propagation, the current trend is towards blind attacks on systems with little or no reconnaissance. Majority of the attacks on systems currently are mis-directed due to their blind nature. Use of generic rule-sets on IDS's causes many false positives and extra workload on the security team.

Vulnerability Assessment (VA):

Vulnerability assessment tools are available to monitor and enforce the adoption of a company's security requirements. The vulnerability assessment tools can provide a hacker's eye view of the protected systems and networks. The tools can be used to identify the exploitable vulnerabilities and to take proactive and preventive measures to protect the networks and systems. These tools help identify all known weaknesses in the systems to systems administrators.

Types of vulnerability assessment tools

There are numerous vulnerability assessment (VA) tools that have evolved based on the common techniques used by the hacker community. The most common VA tools include host based, network based, modem detection and password cracking tools. We will discuss the host and network based VA tools only, as they are relevant to this paper.

Network based VA tools use the network as a medium to scan individual hosts and usually can find remotely exploitable vulnerabilities. A centralized host is used to scan the protected network and reports on all the discovered vulnerabilities.

Host based VA tools install agents on the monitored servers. These agents collect vulnerability information that include local and remote exploits and usually report to a centralized server.

Function of VA tools:

The primary goal of VA is to detect known deficiencies in a particular environment that could potentially lead to a system compromise. The tools look at the following aspects in an environment.

Operating Systems Holes: Most operating systems when installed with the default configuration are very insecure. In addition, there are many known bugs that have not been patched that could lead to the compromise of the server.

System Utilities: Many of the system utilities such as DNS, Sendmail have many vulnerabilities associated with them and can be potentially used for system compromise.

Network Deficiencies: Many times firewalls are misconfigured and this results in unintended holes. The access control rules may be defective or written in the wrong order providing unexpected vulnerabilities.

Applications: There are many vulnerabilities associated with user applications such as web, database, email, etc. that can also lead to system compromise. These might also include backdoors into the application, poor access controls and buffer overflows. Buffer overflows can occur when there are inappropriate bounds checking for variables in the application, leading to unauthorized access of the server.

Some Limitations of VA:

Vulnerability assessment tools can detect only known vulnerabilities. VA can help protect against most common attackers such as script kiddies, but not necessarily protect against more sophisticated attackers who could be using unknown vulnerabilities and attack techniques.

VA tools could consume significant amount of system and network resources should be used in such a way as to minimize impact.

New vulnerabilities are discovered almost on a daily basis. These tools should be updated on a fairly regular for them to be effective.

Important points about VA tools:

VA tools provide a powerful technique to look at the environment from the eyes of a hacker. If used appropriately, the can help to maintain a good security posture and to foster awareness of the risks and vulnerabilities that exists on the network. When used with other tools such as Intrusion detection, they can provide a good baseline for intrusion monitoring.

Intrusion Detection:

Intrusion detection seeks to monitor and prevent attacks or attempts at compromising the protected network and system resources. Intrusion detection can use a set of mechanisms to warn of intruder attempts for unauthorized access and to take some steps to deny access to intruders.

Function of Intrusion Detection:

Intrusion detection is one of the critical tools for a defense in depth strategy. It is used with other tools such as authentication mechanisms, firewalls, vulnerability assessment, etc. as an added layer for monitoring and protection.

Types of Intrusion Detection:

There are two major types of Intrusion Detection systems that include network and host based intrusion detection systems:

Network Based Intrusion Detection System (NIDS):

These systems are placed on the network and sniff all packets destined to the network or the system it monitors. The sniffed packets are examined for any unauthorized activity. Most of the network based Intrusion detection systems apply pattern matching algorithms on the payloads of the sniffed network packets to detect different types of attacks. In some instances they can intercept an attack and prevent it from happening. Others tasks performed by NIDS systems include monitoring the network for port scans, monitor for well know attacks and to identify different types of IP spoofing.

NIDS systems can be placed at various strategic points on the network or on systems to monitor for all kinds of intrusions. An NIDS system outside the firewall can be used to monitor all attacks that are coming in from outside sources. An NIDS system inside the firewall can be used to monitor all attacks and traffic that make it through the firewall and can be used to verify that the firewall is operating appropriately and may also be used to detect compromise of the firewall itself.

Host Based Intrusion Detection System (HIDS):

These are installed on the actual system to be monitored. These monitor the system for any unauthorized changes or other anomalous activity. There are two

types of host based intrusion detection which include network monitors and host monitors.

Network Monitors:

Network monitors look at incoming network connections and check them to see if they pose any threat to the system. The most common use of this is to detect connections to unauthorized ports and to detect port scans.

Host Monitors:

Host monitors look at login activity, administrator activity, files, file systems, logs and other parts of the host to detect any intrusions or anomalous activities. One variant of host monitoring also monitors for kernel based intrusion detection. Attackers could have obtained login access to the system through social engineering or other techniques. Host monitors look at login activity on the host and subsequent behavior for detection of intruders. Hackers try to gain administrative access after gaining access to the system, which can be potentially detected by host monitors.

Host monitors also look for any changes to monitored files and filesystems. Attackers commonly install Trojans, backdoors and root kits after a system has been compromised. These changes can be detected and used to warn system administrators of intrusions and unauthorized changes. Some of the more recent type of attacks use kernel level rootkits. When a kernel level rootkit is installed, the kernel is modified by the attackers without any changes to the files, that host monitors could detect. The system calls are intercepted by the attacker to perform covert activities. Certain types of host monitors that check for file modifications and changes in check cannot detect kernel level attacks. There are special host monitors available that can be used prevent these kinds of attacks.

Some issues with current IDS systems and their usage:

False Positives:

If the default configuration provided by the vendor is used, the majority of the alerts produced by these systems tend to be false positives. This is because in many instances, what is normal activity for a particular organization could be an attack under certain circumstances. The vendors provide rule-sets for all kinds of attacks and it is up to the organization to prune the rule-sets from false positives.

IDS Configuration Issues:

The security team should have an intrinsic knowledge of all the hosts, their functions and their vulnerabilities. They need to configure the host based and network based intrusion detection systems granularly based on each hosts

unique functions and vulnerabilities. In most organizations, this is a manual process that involves using knowledge gained from different sources to generate rules for the Intrusion detection systems and is extremely cumbersome.

If and when new vulnerabilities are detected, the Intrusion detection system signatures need to updated. With the constant barrage of new vulnerabilities, it is becoming increasingly difficult for the security team in an organization to stay up to date on their IDS configurations. Organizations having a multitude of systems running many different applications, it is always a game of catch up to provide for up to date intrusion detection. As Intrusion Detection systems evolve, there is an increased need for automation to reduce human involvement.

Pure Integration between VA and IDS Systems:

Most of the modern day attacks are automated and happen through automated scripts and worm based mechanisms. Recently there is sadmind/IIS worm that exploits a vulnerability in sadmind to compromise a Solaris machine and then uses the compromised host to attack IIS servers using the Unicode exploit.

To counter automated attacks, it is absolutely essential that the tools used to secure and monitor networks communicated with each other in an automated fashion. The VA tools provide a clear picture of all hosts on the network, the services that they provide and also information on the known vulnerabilities that exist in the network. Intrusion detection systems need data on what needs to be monitored on the network. If there is automated interchange of information, where the data from the vulnerability assessment system is automatically used to generate filters for the Intrusion detection system, the number of false positives is greatly reduced. Most alerts on the IDS are genuine and will be taken seriously.

This is an essential evolution for vulnerability assessment and the IDS systems in order for security professionals to keep up with the increased sophistication of the attackers. In order for this marriage to work reliably, the vulnerability assessment systems should be kept up to date with any changes to the network and with the latest vulnerabilities.

References:

1.CERT/CC "CERT® Advisory CA-2001-11 sadmind/IIS Worm" 2001
http://www.cert.org/advisories/CA-2001-11.html (May 2001)

2. Jeff Forristal and Greg Shipley "Vulnerability Assessment Scanners" 2001
http://www.networkcomputing.com/1201/1201f1b1.html January 8, 2001

3. Hackers Club "Exploits for Windows NT/2000" 2001
http://www.hackersclub.com/km/files/nt/index.html May 2001.

4. Panagiotis Astithas "Intrusion Detection Systems" 1990
http://www.daemonnews.org/199905/ids.html May 1999

5. Daniel Ragsdale, Curtis Carver, Jeffery Humphries, Udo Pooch "Adaptation Techniques for Intrusion Detection and Intrusion Response Systems" 2000
http://citeseer.nj.nec.com/ragsdale00adaptation.html

6. SANS "Intrusion Detection FAQ" Version 1.51
http://www.sans.org/newlook/resources/IDFAQ/ID_FAQ.htm May 2001

7. Mikhail Gordeev "Intrusion Detection: Techniques and Approaches" 2000
http://www.infosys.tuwien.ac.at/Teaching/Courses/AK2/vor99/t13/ February 2000.

8. David "Del" Elson "Intrusion Detection, Theory and Practice" 2000
http://www.securityfocus.com/focus/ids/articles/davidelson.html March 2000

9. Steve Miksell, Scott Nainist, Henry James "Security Vulnerability Assessment Tools For Internet Applications" 2001
http://www.itsc.state.md.us/ITSC/delvrbles/S-3-1/S_3_1_Security_Assessment_Paper_Final.pdf March 2001

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS