



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Using VAX/VMS to augment security of a large UNIX environment

Helping remote syslog configurations

John Jenkinson

It is recommended practice in UNIX host security to turn up logging in syslog and have those log entries go to another host as well. Turning up logging involves adding facilities to the syslog.conf file and choosing a level providing more information than in the standard configuration file provided by the operating system vendor. Theory being that a [cr|h]acker will remove syslog entries to hide their actions and having a copy or entry on another host will add the task of finding these entries and removing them as well in order to hide their actions. While we do this remote host syslogging, we also realise there are some problems with this approach.

The log system is typically a like platform (UNIX or NT) and thus is possibly hackable via a like means as the attacked system.

The log system has syslog entries in a well known location and format. If the intrusion was successful, the location is easily found.

The entries transverse the network so can be intercepted, the network configured to not pass these syslog entries, or the syslog port on either end can be altered.

If no realtime monitoring is occurring, the attacker has time to find and alter these log host's syslog entries

It is difficult and /or error prone to time correlate entries from more than one host even with a time daemon running. Thus if the attack was against multiple hosts at a time, determining the chronology is also difficult and /or error prone.

Additional scripting or programming needs to be done to shift through the normal entries looking for the items that might indicate an intrusion.

Syslog can only log syslog entries. Other happenings on the machine that are reported on the console of the machine will not be captured. Nor will any console messages from applications not using the syslog service be logged.

Nodes that are a part of the UNIX environment, but aren't UNIX syslog capable will also not be captured via the syslog restear to a remote syslog host. Examples are NAS (Network Attached Storage) servers, network gear, and other systems like VAX, mainframe, and such.

While there are more issues with the remote syslog host approach, it is worth doing. Here is what we do to address the above mentioned issues to add some more security to our environment.

We use VCS (VAXcluster Console System), a product from Digital Equipment Corporation before they were purchased by Compaq. The product was designed to monitor and control consoles of VAXen. The product then became POLYCENTER Console Manager then was purchased by CA some time later. Some like products exist like VCC from Singlepoint Systems. There are also some strict console server products available as well with less features. While the product glosses tout the ability to manage a large number of computer consoles as the primary features, we do gain some security by using VCS to address the issues mentioned above.

VCS runs on a VAX and has serial asynchronous adapters and/or terminal server ports connected to the console or serial asynchronous adapter port of the machines to be controlled and monitored. VCS has reads pending on all the terminal lines it controls. Each character is captured and logged to a log file on the VAX, the line time stamped with the VAX time, displayed on a console monitor, has a user configurable scanner to locate strings and optionally take a user defined action, manage those logs, and can change color of a graphical representation of the machines based on the user assigned priority of the captured event. For each of the above issues in order:

The VCS system runs VAX/VMS, thus not prone to the UNIX problems that provided the compromise.

The VCS log is not in syslog format nor even a streamLF formatted file. The logfile is a VAX/VMS Indexed Prolog: 3 file.

VCS reads the terminal line (usually the console) so the network between the monitored node and the monitoring node isn't necessary to capture the information.

VCS scans the messages in near realtime, thus the information is in the log file, on the console display, and a user definable action (like a pager notification) will have occurred within seconds of the event.

Each console monitored is timestamped and all the monitored nodes are in one file (closed and opened anew for each day). Thus it can be reviewed with the information from any or all nodes displayed in the order the data was received. This gives a true chronology of the events.

VCS comes with many scan profiles, users can easily add/delete/modify these with a GUI (Graphical User Interface) to the scanner.

VCS monitors items like boot events, raid box events, etc. It can also force (re)boot or reset of a machine.

VCS also monitors our Network Appliance Servers. We also have had it monitor our encryption boxes and other types of gear.

It should be mentioned that consistency checking the three logs (VCS, local syslog, syslog to loghost) should be done. Having entries that belong in all three with one or more missing should indicate a check of the configurations of all three. If these are consistent and working, then a check for an intrusion should follow

We have experience with VCS so mention its specific features. As indicated before the product does have follow-ons and competitors. There are also console monitors that though are not quite as feature rich, they do provide the console management and some subset of the security features mentioned in this paper.

Resources

Papers recommending syslog to loghost

Farmer, Dan and Venema, Wietse. "Improving the Security of Your Site by Breaking Into it"

<http://www.alw.nih.gov/Security/Docs/admin-guide-to-cracking.101.html>

Boran, Seán. "Hardening Red Hat Linux with Bastille"

<http://www.securityportal.com/coverstory20000501.html>

Boran, Seán. "Hardening Solaris"

http://jamus.xpert.com/~roman/doc/hardening_solaris7.html

Sites on console managers

Compaq Computer Corporation. VAXcluster Console System, Version 1.4

<http://www.digital.com/info/SP2746/>

CA ACQUIRES SELECTED POLYCENTER PRODUCTS

<http://www5.compaq.com/inform/issues/issue12/html/in12a21a.html>

Singlepoint Systems VCC

<http://www.singlepointsys.com/products/VCC/default.cfm>

Upcoming Training

Click Here to
{Get CERTIFIED!}



SANS Miami 2019	Miami, FL	Jan 21, 2019 - Jan 26, 2019	Live Event
SANS Las Vegas 2019	Las Vegas, NV	Jan 28, 2019 - Feb 02, 2019	Live Event
SANS Security East 2019	New Orleans, LA	Feb 02, 2019 - Feb 09, 2019	Live Event
Security East 2019 - SEC401: Security Essentials Bootcamp Style	New Orleans, LA	Feb 04, 2019 - Feb 09, 2019	vLive
SANS Northern VA Spring- Tysons 2019	Tysons, VA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Anaheim 2019	Anaheim, CA	Feb 11, 2019 - Feb 16, 2019	Live Event
SANS Secure Japan 2019	Tokyo, Japan	Feb 18, 2019 - Mar 02, 2019	Live Event
SANS Scottsdale 2019	Scottsdale, AZ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS New York Metro Winter 2019	Jersey City, NJ	Feb 18, 2019 - Feb 23, 2019	Live Event
SANS Dallas 2019	Dallas, TX	Feb 18, 2019 - Feb 23, 2019	Live Event
Open-Source Intelligence Summit & Training 2019	Alexandria, VA	Feb 25, 2019 - Mar 03, 2019	Live Event
SANS Reno Tahoe 2019	Reno, NV	Feb 25, 2019 - Mar 02, 2019	Live Event
Mentor Session @Work - SEC401	Raleigh, NC	Feb 27, 2019 - Mar 06, 2019	Mentor
SANS Baltimore Spring 2019	Baltimore, MD	Mar 02, 2019 - Mar 09, 2019	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Mar 04, 2019 - Mar 09, 2019	Community SANS
SANS Secure India 2019	Bangalore, India	Mar 04, 2019 - Mar 09, 2019	Live Event
Baltimore Spring 2019 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Mar 04, 2019 - Mar 09, 2019	vLive
SANS San Francisco Spring 2019	San Francisco, CA	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS St. Louis 2019	St. Louis, MO	Mar 11, 2019 - Mar 16, 2019	Live Event
SANS Secure Singapore 2019	Singapore, Singapore	Mar 11, 2019 - Mar 23, 2019	Live Event
SANS London March 2019	London, United Kingdom	Mar 11, 2019 - Mar 16, 2019	Live Event
Mentor Session - SEC401	Fredericksburg, VA	Mar 12, 2019 - May 14, 2019	Mentor
SANS Norfolk 2019	Norfolk, VA	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Munich March 2019	Munich, Germany	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS Secure Canberra 2019	Canberra, Australia	Mar 18, 2019 - Mar 23, 2019	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201903,	Mar 19, 2019 - Apr 25, 2019	vLive
SANS 2019 - SEC401: Security Essentials Bootcamp Style	Orlando, FL	Apr 01, 2019 - Apr 06, 2019	vLive
SANS 2019	Orlando, FL	Apr 01, 2019 - Apr 08, 2019	Live Event
Community SANS Raleigh SEC401	Raleigh, NC	Apr 01, 2019 - Apr 06, 2019	Community SANS
SANS London April 2019	London, United Kingdom	Apr 08, 2019 - Apr 13, 2019	Live Event
Blue Team Summit & Training 2019	Louisville, KY	Apr 11, 2019 - Apr 18, 2019	Live Event