Global Information Assurance Certification Paper

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 form any or all nodes displayed in the order the data was received. This gives a true chronology of the events.

VCS comes with may 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 consistancy 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 consistant 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 followons 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