Bipartisan server politi...er, security

By Russ McRee – ISSA member, Puget Sound (Seattle), USA chapter

Prerequisites

Linux
Windows
An objective, moderate, OS-agnostic view

Similar Projects

Helios[1]
OCS Inventory NG[2]

As I believe in a moderate political stance, I so, too, believe in a balanced server environment. Our mandate as security professionals is to first do no harm, followed by the need to protect all assets to the best of our ability. Therein lies the challenge. So many computing environments can be considered heterogeneous, requiring a skill set capable of defending a variety of platforms. While I am writing this in early October, you're likely reading it just prior or soon after the United States presidential election. So often in American politics we suffer partisanship, where the disparity between parties is so deep that little is accomplished that can be considered of true benefit to the people. Let us not bring this challenged mindset into our production environments. We must treat all servers equally! It is in this spirit, we shall discuss server security tools for both parties…er, operating systems. I will proceed in alphabetical order so as to avoid bias, and each tool will be listed alphabetically as well. It is also my intention to discuss tools we've not yet covered; most Linux administrators have heard of Bastille and most Windows administrators are familiar with the MBSA. Therefore, should you learn of a security tool not yet in your toolkit, we will have come through on our campaign promise.

Enhancing Linux security

Remember Brian Provost's *The Big Ol' Ubuntu Security Resource* as a great starting point for recommendations: include modifying default settings including shared memory, SSH root login, and limiting super user access, enabling automatic security updates, securing the home directory, a list of essential security installs, bootup security, and an additional list of secondary security enhancements. For new Ubuntu users and old hands alike this is an excellent checklist.

PortSentry

In the oldie but goodie category we find PortSentry, practically a classic by most standards, but still entirely relevant. PortSentry, for protection from portscans on *nix platforms, is one of the three Sentry tools that also include LogSentry and HostSentry. Installation of PortSentry on an Ubuntu/Debian system is as simple as `sudo apt-get install portsentry`. It'll include the Exim mail server as well, as it is mail message capable upon receipt of attack traffic.

By default PortSentry does not block. Check `/etc/portsenrtry/portsentry.conf` if you'd like to change where it writes messages; default is `/var/log/syslog`. See also `/etc/default/portsentry` for startup options and `/etc/portsentry/portsentry.ignore.static` for hosts and interfaces to ignore. The default configurations are ample to get under way. If you do make changes to the config file be sure to `sudo /etc/init.d/portsentry restart`, or the comparable command for your distribution. PortSentry "listens" on a number of ports; when you scan a host running PortSentry as I did in my lab, don't be shocked to see all the "open" ports. I hit my PortSentry host with a TCP connect nmap scan: `nmap -v -sT 192.168.248.108`.

The result in /var/log/syslogd is as follows:

```
Oct  7 23:26:24 hio-ubuntu-02 portsentry[9682]:
  attackalert: Connect from host: 192.168.248.101/
  192.168.248.101 to TCP port: 32774

Oct  7 23:26:24 hio-ubuntu-02 portsentry[9682]:
  attackalert: Host: 192.168.248.101 is already
  blocked. Ignoring

Oct  7 23:26:33 hio-ubuntu-02 portsentry[9682]:
  attackalert: Connect from host: 192.168.248.101/
  192.168.248.101 to TCP port: 31337

Oct  7 23:26:33 hio-ubuntu-02 portsentry[9682]:
  attackalert: Host: 192.168.248.101 is already
  blocked. Ignoring

Oct  7 23:27:04 hio-ubuntu-02 portsentry[9682]:
  attackalert: Connect from host: 192.168.248.101/
  192.168.248.101 to TCP port: 1524

Oct  7 23:27:04 hio-ubuntu-02 portsentry[9682]:
  attackalert: Host: 192.168.248.101 is already
  blocked. Ignoring

Oct  7 23:27:20 hio-ubuntu-02 portsentry[9682]:
  attackalert: Connect from host: 192.168.248.101/
  192.168.248.101 to TCP port: 1080

Oct  7 23:27:20 hio-ubuntu-02 portsentry[9682]:
  attackalert: Host: 192.168.248.101 is already
  blocked. Ignoring
```

1 http://www.antirootkit.com/software/Helios.htm.

2 http://sourceforge.net/projects/ocsinventory.

```
Oct  7 23:27:27 hio-ubuntu-02
  portsentry[9682]: attackalert:
  Connect from host: 192.168.248.101/192.
  168.248.101 to TCP port: 32772
Oct  7 23:27:27 hio-ubuntu-02
  portsentry[9682]: attackalert: Host:
  192.168.248.101 is already blocked.
  Ignoring
Oct  7 23:27:34 hio-ubuntu-02
  portsentry[9682]: attackalert:
  Connect from host: 192.168.248.101/192.
  168.248.101 to TCP port: 635
Oct  7 23:27:34 hio-ubuntu-02
  portsentry[9682]: attackalert: Host:
  192.168.248.101 is already blocked.
  Ignoring
```

As my system is already blocking unnecessary traffic, PortSentry doesn't have much work to do here, but it can block if configure appropriately. "To block a scan, PortSentry can either insert a route into the host's route table, which directs the offending traffic to a veritable "black hole," or it can use one of several packet filtering software packages (ipfwadm, ipchains, ipf, ipfw, or iptables) to block traffic from the scanning host. The action is determined by the setting of the configuration variable `KILL_ROUTE`."[3]

If you wish a more detailed play by play of PortSentry, see SecurityFocus's two-part series PortSentry for Attack Detection.[4]

Figure 1 – Rootkit Hunter finding before infection.

Rootkit Hunter

Rootkit Hunter, from rootkit.nl,[5] is a well-developed rootkit scanner for *nix systems that "supports" numerous rootkits, backdoors, LKM's, and worms. Available since 2005, Rootkit Hunter is now in version 1.3.2. I tested it on BackTrack 3,[6] as it is included in this familiar distribution, by infecting my BackTrack 3 virtual machine with the SVH5 rootkit.

Running Rootkit Hunter is as simple as `rkhunter -c`; you'll do so via sudo on systems other than BackTrack. It writes output to the console as well as all findings to `/var/log/rkhunter.log`.

You'll note that Rootkit Hunter on BackTrack 3 finds four "suspicious" files by default.

```
/bin/groups
/usr/bin/ldd
/usr/bin/whatis
/usr/sbin/adduser
```

These are Bourne shell script replacements and are not problematic.

I chose to comment out "disable_tests" in `/usr/local/etc/rkhunter.conf`, the Rootkit Hunter configuration file (location varies per distribution), to allow a more thorough scan including suspicious and deleted files, as well as hidden process and packet capture apps.

A run of Rootkit Hunter on a clean system appears as seen in Figure 1.

After "installing" the SVH5 rootkit I ran `rkhunter -c` again. Following is a version of `/var/log/rkhunter.log`, edited to show you the highlights of Rootkit Hunter's capabilities. I've posted the entire log unedited on my website.[7] You'll note it passes good files, warns of immutable files, and scans for a variety of rootkits.

The following is truncated to save space:

```
[22:56:14] Running Rootkit Hunter version 1.3.2 on
  B33nPwn3d
[22:56:14] Info: Start date is Tue Oct  7 22:56:14
  GMT 2008
[22:56:14] Checking configuration file and command-
  line options...
[22:56:14] Info: Detected operating system is
  'Linux'
```

3 http://www.securityfocus.com/infocus/1586.

4 PortSentry for Attack Detection: Part 1, http://www.securityfocus.com/infocus/1580; Part 2, http://www.securityfocus.com/infocus/1586.

5 http://www.rootkit.nl/projects/rootkit_hunter.html.

6 http://www.remote-exploit.org/backtrack_download.html.

7 http://holisticinfosec.org/toolsmith/files/1108/rkhunter.log.

```
[22:56:14] Info: Cnommand line is /usr/local/bin/
  rkhunter -c
[22:56:14] Info: Environment shell is /bin/bash;
  rkhunter is using bash
[22:56:14] Info: Using configuration file '/usr/
  local/etc/rkhunter.conf'
[22:56:22] /bin/login                        [OK]
[22:56:22] /bin/ls                       [Warning]
[22:56:23] Warning: File '/bin/ls' has the
  immutable-bit set.
[22:56:23] /bin/mv                           [OK]
[22:56:23] /bin/netstat                  [Warning]
[22:56:23] Warning: File '/bin/netstat' has the
  immutable-bit set.
[22:56:23] /bin/ps                       [Warning]
[22:56:23] Warning: File '/bin/ps' has the
  immutable-bit set.
[22:56:23] /bin/pwd                          [OK]
[22:56:26] /usr/bin/find                 [Warning]
[22:56:26] Warning: File '/usr/bin/find' has the
  immutable-bit set.
[22:56:56] Warning: SHV4 Rootkit         [Warning]
[22:56:56] File '/lib/lidps1.so' found
[22:56:56] Checking for SHV5 Rootkit...
[22:56:56] Checking for file '/etc/sh.conf' [Found]
[22:56:56] Checking for file '/dev/srd0'    [Found]
[22:56:57] Checking for directory '/usr/lib/libsh'
  [Found]
[22:56:57] Warning: SHV5 Rootkit         [Warning]
[22:56:57] File '/etc/sh.conf' found
[22:56:57] File '/dev/
  srd0' found
[22:56:57] Directory '/
  usr/lib/libsh' found
[22:57:27] System checks
  summary
[22:57:27]
  ====================
[22:57:27] File
  properties checks...
[22:57:27] Required
  commands check failed
[22:57:27] Files checked:
  165
[22:57:27] Suspect files:
  16
[22:57:27] Rootkit
  checks...
[22:57:27] Rootkits
  checked : 113
[22:57:27] Possible
  rootkits: 2
[22:57:27] Rootkit names
  : SHV4 Rootkit, SHV5
  Rootkit
[22:57:28] The system checks took: 1 minute and 12
  seconds
[22:57:28] Info: End date is Tue Oct  7 22:57:28
  GMT 2008
```

Out of 165 scanned Rootkit Hunter identified 16 suspicious files, all written as immutable by SVH5 and clear indication of SVH4/5 detection.

Ensure you install it on your Linux systems via `sudo yum install rkhunter`, `sudo apt-get install rkhunter`, or your preferred installation methodology.

Windows host integrity monitoring

If you haven't heard the adage "disable unnecessary services" you best turn in your CISSP right now. ;-)

Yet, it always holds true, on any OS. But even after you've followed all recommended standards (see Required Reading), there are always additional steps that can be taken, depending on the environment you seek to protect or the compliance standard you must adhere to. If you have to answer to the PCI DSS, you likely have a need to conduct host integrity monitoring, key OS files in particular. Following is a method that allows you to conduct regular host integrity scans and report results via syslog and email, without having to buy expensive commercial products.

Kiwi Syslog

Kiwi Syslog is an excellent syslogd daemon that can be used in limited fashion for free and is also quite reasonable to purchase. I'll point you to an old article I wrote that includes

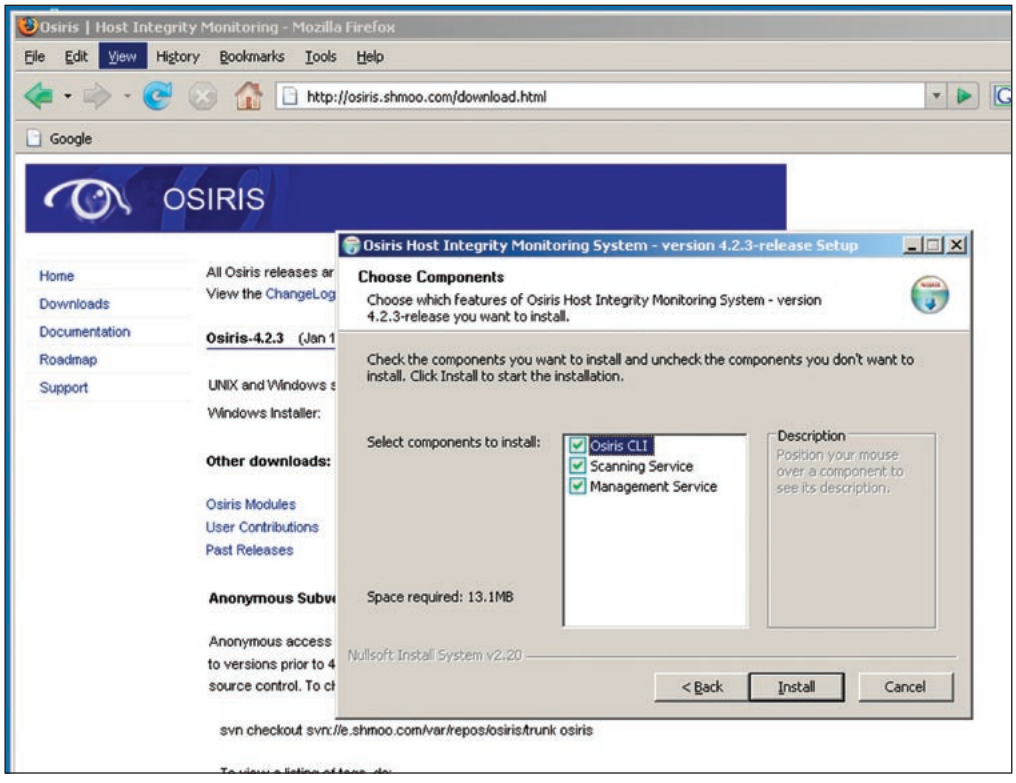

Figure 2 – Osiris installation.

a lot of Kiwi details: "Smoothwall, MySQL and Kiwi Syslog Daemon: Cost Effective Firewall and Logging with Database and Analysis."[8]

The basics of Kiwi setup are simple. Download and install Kiwi,[9] using the install as a service option using the local system account. I won't detail its installation and configuration further here (space limitations) but there's another great doc on Kiwi setup from Joe Kocan.[10]

Osiris Windows

Next, download the Osiris Windows installer[11] and accept installation defaults.

Once installed, open a command prompt, and execute `osiris`.

Choose *yes* to connect to localhost. Username is *admin*, password is *blank*; immediately establish a password using the passwd command. Once logged in you can pass a question mark (?) and see all available management and host commands. My test bed is a Windows Server 2003 virtual machine called *hio-test* that is serving as the Osiris management server and a host.

As you pass a command, ensure that you pass the host name as well. After checking my details via `host-detail hio-test`, I passed `edit-host hio-test` in order to ensure the system keeps an archive of the scan database. You can choose to enable log files, but all log entries are sent to the management console via syslog so you don't have to choose this. Logs are written to `C:\WINDOWS\osiris\hosts\hostname\logs` by default. Make use of alertmsg.dll[12] from neweve.net to fix a logging bug as Osiris writes to Windows Event Logs. On Windows servers Osiris events are written to the Application log in Event Logs. There are Event Log to syslog converters like Snare and Lasso, but you might consider eventsys from Purdue University,[13] as mentioned Joe in his handy Osiris doc.[14] You can also choose to send email notifications of scan results as well.

After conducting your first manual scan (it ran one automatically during installation) `via start-scan hostname`, be sure to `list-db` and see which database is set as your baseline. It should be 2 in this case.

At this stage, I "infected" my Windows Server 2003 VM by renaming `iedw.exe to iedw.cracked`, and then rescanned.

```
1       compare time: Thu Oct 09 13:07:55 2008
2               host: hio-test
3        scan config: default.windowsserver2003 (63f6bd00)
4           log file: 2
5      base database: 2
6   compare database: 3
7
8   [219][hio-test][cmp][C:\Program Files\Internet Explorer\iedw.exe][gro
9   [203][hio-test][new][C:\Program Files\WinSCP\DragExt.dll]
10  [203][hio-test][new][C:\Program Files\WinSCP\PuTTY\pageant.exe]
11  [203][hio-test][new][C:\Program Files\WinSCP\PuTTY\puttygen.exe]
12  [203][hio-test][new][C:\Program Files\WinSCP\WinSCP.com]
13  [203][hio-test][new][C:\Program Files\WinSCP\WinSCP.exe]
14  [203][hio-test][new][C:\Program Files\WinSCP\unins000.exe]
15  [223][hio-test][cmp][mod_kmods][service:RasMan][service:RasMan;dname:
    Connection Manager;status:running]
16  [223][hio-test][cmp][mod_kmods][service:TapiSrv][service:TapiSrv;dnam
17
18  Change Statistics:
19  ----------------------------------
20          checksums: 0
21         SUID files: 0
22   root-owned files: 0
23   file permissions: 0
24                new: 6
25            missing: 0
26
27  total differences: 9
28
```

Figure 3 – Osiris log comparison.

Not only was this change noted, I was additionally satisfied to discover that Osiris had diffed some other changes I'd made, including the installation of WinSCP.

Note: Osiris does not currently offer a default config file for Vista. The Osiris project website offers a reasonable installation and usage guide.

Logging host and file integrity is one certain step towards PCI compliance, and being able to log multiple hosts to a central console and syslog server, all for free, has an obvious upside.

Required reading

Following are some excellent articles and resources regarding our topic of choice:

— Five-ways-to-harden-Windows-Server[15]

— NIST's Guide to General Server Security SP-800-123[16]

— NSA's Windows Server 2003 Guides[17]

— NSA's RedHat Enterprise Linux Guides[18]

— Big Ol' Ubuntu Security Resource[19]

Benefits and drawbacks

There are no drawbacks to Rootkit Hunter; I consider it an automatic on all my Linux systems.

PortSentry is has achieved esteem for its simplicity and effectiveness; here too there is no reason not to use this tool.

8 http://www.securitydocs.com/library/2900.

9 http://www.kiwisyslog.com/kiwi-syslog-daemon-overview.

10 http://www.neweve.net/support/Kiwi-Syslog-Configuraiton-Standard.pdf.

11 http://osiris.shmoo.com/download.html.

12 http://www.neweve.net/modules/download_gallery/dlc.php?file=22.

13 https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys.

14 http://www.neweve.net/support/Osiris-Configuration-Standard.pdf.

15 http://searchsecurity.techtarget.com.au/articles/26001-Five-ways-to-harden-Windows-Server.

16 http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf.

17 http://www.nsa.gov/snac/downloads_win2003.cfm?MenuID=scg10.3.1.1.

18 http://www.nsa.gov/snac/downloads_redhat.cfm?MenuID=scg10.3.1.1.

19 http://www.itsecurity.com/features/ubuntu-secure-install-resource.

I feel very strongly about host and file integrity practices and Osiris goes a long way to providing a considerable ally in the process to monitor and log on behalf of PCI and best practices.

In conclusion

With an open mind, and a desire to reach out to our fellow admins, analysts, and engineers across the aisle, we can avoid being too "mavericky," and enjoy balance and assurance in our heterogeneous environments. Security and integrity for all! May our national political scene accomplish the same. Cheers…until next month.

Acknowledgments

Joseph A. Kocan of New Eve Technologies for his Osiris and Kiwi Syslog docs, as well as the alertmsg.dll fix.

About the Author

Russ McRee, GCIH, GCFA, CISSP, is a security analyst working in the Seattle area. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.