

The continuing saga of creating the UNIX SAIT environment

By: Jennifer Frazier

Let's Create the JSS Environment

- This is done because it takes a little "WHILE" to do the initial setup of JSS.
- Let's take a looky.

What have I accomplished thus far?

MILESTONES

Which Tools?

- Intrusion Detection
 - Sniffer - TCPEDump, Sniffit
 - Host - Portsentry, TCP Wrapper, Watcher, Tripwire
 - Network - Gabriel, Argus, Courtney, Snort, Swatch
- Authentication
 - Hashes - Snefru, MD5
- Vulnerability Mgmt.
 - PW Assess - John the Ripper, Crack
 - Port Scanner - NMAP, Whisker, Strobe
 - Security Assess - Saint, Sara, Tiger, COPS, Nessus
 - Lockdown - Titan, Chkacct, CheckXusers
- Miscellaneous
 - Front End - Merlin, TCPSlice

JSS

- Initial Bash Script
- Demonstration
- Test with a Tool

What happened to the tools?

- Have set a weekly goal of completing at least 10 tools and to have them documented on my website with readme info and source code.
- Tools I have completed towards my goal:

Merlin	COPS	TCPDUMP	NMAP
TIGER	SARA	TCPSlice	SAINT

How's the coding coming along?

- The initial sandbox building script for the server is complete.
- Next I wanted to research the RSYNC program and get it working from the command line.

RSYNC

- Rsync must be installed on the client and server machines.
- Connects using SSH.
- Preserves permissions, user ownership, group, and times (creation and modification times)
- Most current version for Solaris 8 is 2.3.1

Rsync's numerous options but let's only discuss the ones that serve my purpose

- verbose – makes the output more verbose
- checksum – compares files according to their checksum
- recursive – recursive into directories
- links – preserve soft links
- perms – preserve permissions
- owner – preserve ownership
- group – preserve groups
- times – preserve creation and modification times
- dry-run – for testing purposes
- rsh=command
- rsync-path=PATH
- force – forces deletion of directories
- delete-excluded – delete excluded files that do not exist on the sending side
- progress – show progress during transfer

Let's do an example run

Next Step:

- Need to get exelc to execute the rsync command.
- Need to begin working towards allowing the user to act as root inside the sandbox.
- Complete my 10 tools and web documentation per week.

Accomplishment

- Have Researched and Installed 42
 - (with additional 2 pending security tools.)
- Have finished JSS
- Have written rough draft of Project Documentation
- Waiting to Install in SAIT

Tools Completed

- Intrusion Detection
 - Sniffers
 - TCPEDump, Sniffit, TCPFlow
 - Host
 - TCP Wrappers, Watcher, Tripwire, L5
 - Network
 - Gabriel, Argus, Courtney, Snort, Swatch,
 - Arp Watch
 - Hybrid
 - Big Brother, Nessus
 - Auditing
 - Portsenry, Antiroute
- Firewalls
 - SocksV, Muffin

Miscellaneous More Tools

- Miscellaneous
 - Testing Tools
 - TCPReplay, Fragrouter
 - System Sanitizer
 - SCRUB
- Authentication and Encryption
 - Hashes
 - Snefru, MD5
 - GPG
 - Encryption/Decryption
 - DES

And Still More Tools

- Vulnerability Management
 - Password Assessment
 - John the Ripper, Crack, MDCrack
 - Port Scanners
 - NMAP, Whisker, Strobe, ISS, Queso, ScanSSH
 - Security Assessment Scanners
 - Saint, Sara, Tiger, Cops
 - Lockdown/Hardening
 - Titan, Chkacct, CheckXusers

Tool Example

- Netscape
 - `execve("/usr/dt/appconfig/netscape/netscape", 0xFFBEFC64, 0xFFBEFC6C) argc = 1`
 - `stat("/usr/dt/appconfig/netscape/netscape", 0xFFBEF9B0) = 0`
 - `open("/lib/libXm.so.3", O_RDONLY) = 3`
 - `open("/lib/libXt.so.4", O_RDONLY) = 3`
 - `open("/lib/libX11.so.4", O_RDONLY) = 3`
 - `open("/lib/libICE.so.6", O_RDONLY) = 3`
 - `open("/lib/libXext.so.0", O_RDONLY) = 3`

There's Still a Few More

- Netscape (cont)
 - `open("/lib/libsocket.so.1", O_RDONLY) = 3`
 - `open("/lib/libdl.so.1", O_RDONLY) = 3`
 - `open("/usr/platform/SUNW,Ultra-5_10/lib/libc_psr.so.1", O_RDONLY) = 3`
 - `chdir("/usr/dt/appconfig/netscape") = 0`
 - `lstat64("/usr", 0xFFBECB90) = 0`
 - `stat("/usr/dt/appconfig/netscape/lib/locale/C/app-defaults/netscape.cfg", 0xFFBEDA70) = 0`
 - `stat("/.netscape/bookmarks.html", 0xFFBEBA98) = 0`
- Plus Symlinks

Let's Do A Demo ...