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 looksy.

What have I accomplished thus far?

MILESTONES

Which Tools?

- Intrusion Detection
  - Sniffer – TCPDump, 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:

<table>
<thead>
<tr>
<th>Merlin</th>
<th>COPS</th>
<th>TCPDUMP</th>
<th>NMAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIGER</td>
<td>SARA</td>
<td>TCPSlice</td>
<td>SAINT</td>
</tr>
</tbody>
</table>
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 (creating 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 exec 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**
- Sniffers
  - TCPDump, Sniffit, TCPFlow
- Host
  - TCP Wrappers, Watcher, Tripwire, L5
  - Arp Watch
  - Big Brother, Nessus
- Auditing
  - PortMap, Antiroute
- Firewalls
  - SocksV, Muffin

**Intrusion Detection**
- **TCP**
  - Sniffers
    - TCPDump, Sniffit, TCPFlow
- **Host**
  - TCP Wrappers, Watcher, Tripwire, L5
  - Arp Watch
  - Big Brother, Nessus
- **Auditing**
  - PortMap, Antiroute
- **Firewalls**
  - SocksV, Muffin

**Miscellaneous**
- **More Tools**
  - Merlin, TCPSlice
- **Testing Tools**
  - System Sanitizer
  - SCRUB
- **Authentication and Encryption**
  - **Hashes**
    - 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

**Netscape (cont)**
- open("/lib/libsocket.so.1", O_RDONLY) = 3
- open("/lib/libdl.so.1", O_RDONLY) = 3
  - 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
- open("/lib/libsocket.so.1", O_RDONLY) = 3
- open("/lib/libdl.so.1", O_RDONLY) = 3
- chdir("/usr/dt/appconfig/netscape") = 0
- lstat64("/usr", 0xFFFBEA90) = 0
- open("/usr/platform/SUNW,Ultra-5_10/lib/libc_psr.so.1", O_RDONLY) = 3

**Let’s Do A Demo ...**
- exev("/usr/dt/appconfig/netscape/netscape", 0xFFFBEFC64, 0xFFFBEFC6C) argc = 1
- stat("/usr/dt/appconfig/netscape/netscape", 0xFFFBEF9B0) = 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
- chdir("/usr/dt/appconfig/netscape") = 0
- lstat64("/usr", 0xFFFBEA90) = 0
- open("/usr/platform/SUNW,Ultra-5_10/lib/libc_psr.so.1", O_RDONLY) = 3

**There's Still a Few More**
- Netscape
  - exev("/usr/dt/appconfig/netscape/netscape", 0xFFFBEFC64, 0xFFFBEFC6C) argc = 1
  - stat("/usr/dt/appconfig/netscape/netscape", 0xFFFBEF9B0) = 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

**Plus Symlinks**
- netscape (cont)