Lab 12.1 Tripwire
IN715 Networks Three

October 21, 2014

Introduction

An important principle of security is *defense in depth.* We use firewalls to protect the perimeter of our networks. We use network IDSs to monitor the interior of our networks. In this lab we will set up *tripwire* to monitor the integrity of individual machines. Tripwire works by monitoring filesystems and notifying us when files that should not change without warning (e.g., system binaries) do change. Tripwire runs on nearly any POSIX-compliant system, like BSD, Linux and most proprietary unicies.

1 Prerequisites

Before you install tripwire on one of your BSD systems, be sure that the system has proper Internet connectivity. Then install needed packages with the commands

```
pkg_add wget
pkg_add bzip2
```

Change your working directory to `/usr/src` and download and unzip the tripwire code with the commands

```
wget http://kate.ict.op.ac.nz/~tclark/tripwire.tar.bz2
tar -xjf tripwire.tar.bz2
```

2 Build and install tripwire

Move into the new directory, tripwire-2.4.2.2-src and run the following commands

```
./configure --prefix=/usr/local
make
make install
```

These commands, especially the `make` will take a little time. The install script will prompt you for site and local passwords to use with tripwire. In our case it is acceptable if they are both the same.

This process will install the tripwire binaries, configuration, and other resources under `/usr/local`

3 Initial setup

Tripwire works by comparing the filesystem with a snapshot taken when the system was in a known good state. For this reason, it's good to set up tripwire when a system is initially deployed.

First, we create our scan policies by editing the file `usr/local/etc/twpol.txt`.

Look for a section named "Mount Points". In that rule, comment out the lines with `cdrom` and `floppy`. We don't have those. Change the policy for `home` to be "`Dynamic`" since we expect that filesystem to change frequently. Add policy lines for `/usr/X11R6`, `/usr/local`, `/usr/obj`, and `/usr/src`. Set their scan policies to "`Readonly"`. Also, look for policies referring to `/stand` and `/var/msgs/bounds` and comment them out. Save and close the file.

Tripwire doesn't use this file directly. Instead it uses a crytpographically signed policy file that we generate with the command

```
/usr/sbin/twadmin -m P /usr/local/etc/tripwire/twpol.txt
```

Best practice it the remove the unsigned `twpol.txt` and `twcfg.txt` files once they have been processed, but do not delete them until you're sure the configuration and policies are correct. Once the policy is processed, run a baseline scan with the cammand

```
tripwire -m i
```

This will take a few minutes as it captures the baseline snapshot of your system. Once this is done you can run a scan with the command

```
tripwire -m c
```

Since there should not have been any suspicious changes to your filesystems, the report should come back clean. To see a report with a result, change something in a filesystem that should be static. For example, use the command `touch /usr/bin/monkeys` to create a new file in `/usr/bin`. Run a new scan and note that your are notified of the change to `/usr/bin`.

4 Running reports

You can run reports from the command line whenever you want to check things, but it also makes sense to run tripwire as a `cron` job to produce daily reports.