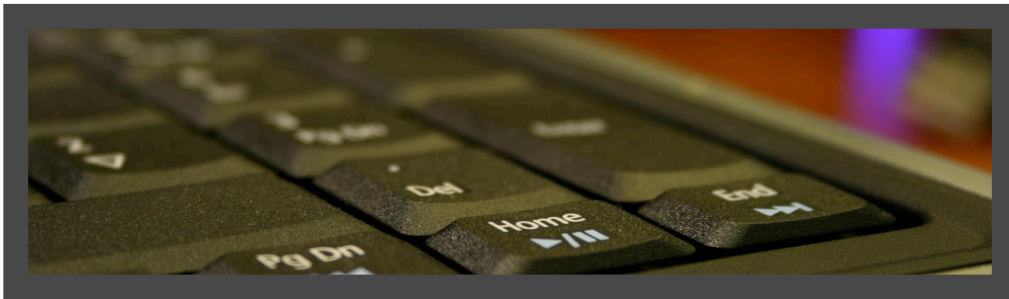


SECURITY AUTOMATION

Better Living through Common Protocols



Bruce Potter
Summer 2007

SECURITY AUTOMATION

Better Living through Common Protocols

Bruce Potter (bpotter@pontetec.com)
Ponte Technologies LLC
Summer 2007

For some, information security is an altruistic goal; making systems more secure is what drives many IT security professionals to get out of bed in the morning. This type of security professionals can be highly motivated and very passionate about their work. However, a dose of reality is needed for the overly-zealous security professional. Security is generally not an end in and of itself. It is a means to an end for a larger business concern. For instance, an online store like Amazon.com does not exist for the sole purpose of paying the salary of its security staff. Rather, the security staff are hired in order to ensure that Amazon.com's software and systems are resilient enough to meet the business needs of the corporation. No more, no less.

In a large enterprise, efficiency of the security processes is as important as the effectiveness of those processes. If it takes weeks to make firewall changes and months to track incidents occurring on the wire, it doesn't matter how effective the actions. The inefficiency of an IT security operations organization can render them as useless as an organization that lacks the core knowledge needed to do their job.

Automation of security processes is a key aspect in running a successful IT security organization. As much as IT is viewed as an enabler of business needs, it is also a tax on the cost of running the overall organization. Security is even worse as it is usually difficult to put an ROI value on IT security. Therefore it is critically important that security processes be automated as much as possible in an effort to make overall IT operations more economical.

Security automation comes in many forms. In general, IT security processes revolve around designing, configuring, deploying, auditing, and maintaining the security of IT systems and the security infrastructure. It is important to automate the processes around each of these areas as much as possible. Some automation can occur by simply modifying how IT staff are interacting with systems while other automation steps may require custom software and new hardware on which to run it. Some automation may only be possible if the vendor adopts open standards or redesigns their software.

SCAP

It is important to understand the role of open standards in make IT security operations more efficient. Without the use of open standards, each role within a security organization effectively becomes a stovepipe. As a simple example, think about different systems get patched. A sysadmin must first understand the desired lockdown state for all the servers in

the infrastructure. This goal is based on the amount of assurance desired, the services to be offered by the server, the quality of the software running on the host, and the level of usability required.

Once the sysadmin understands the security goals, she must then map these goals into the configuration of all the servers. This requires first knowing the configuration state of each system, and then understanding how to modify the configuration to meet the desired goals. In highly heterogeneous environments found in most enterprises, this requires deep knowledge about multiple platforms and operating systems such as Solaris on Sparc servers, AIX on PowerPC servers, and Windows on Intel machines. Once you include all the different patch levels and versions of software on all the systems, the problem becomes unbelievably complex.

Thankfully there are efforts underway to create standards around complex problems such as standard configurations, platform enumeration, and configuration assessment. The most notable of these programs is the Security Content Automation Program (SCAP) from the National Institute for Standards and Technology in the United States. SCAP is a suite of protocols designed to assist in the automation of the spectrum of roles and issues in a security operations department. SCAP consists of the following standards:

- Common Vulnerability Enumeration (CVE) – Structured data on known security vulnerabilities within software
- Common Configuration Enumeration (CCE) – Similar to CVE, however CCE is explicitly concerned with documenting misconfiguration, not software flaws
- Common Platform Enumeration (CPE) – Standard method for describe a particular hardware platform
- Common Vulnerability Scoring System (CVSS) – A means for describing the potential impact of a given security vulnerability
- Open Vulnerability and Assessment Language (OVAL) – An XML schema and database that standardizes the manner in which a host is evaluated to see if it is vulnerable to a particular vulnerability
- Extensible Checklist Configuration Description Formation (XCCDF) – A standard manner of specifying the “checklists” used to lockdown host configuration

The goal of all these protocols is to assist in the seamless integration of products and processes across the security operations lifecycle. By creating standard means of specifying configuration, validating configurations, and understanding vulnerabilities, products should be able to write to these standards and thereby interoperate more effectively. Greater interoperation should lead to more efficiency and ultimately more secure and effective enterprises.

Configuration Automation

While the goal of SCAP is admirable, the standards in some cases are still being solidified, and few products are available in the market today that support a broad spectrum of SCAP

protocols. Even without wide adoption of open standards, there are still actions that organizations can take today that will assist in the automation of their security operations.

Configuring systems for deployment can be a time consuming process that is fraught with chances for mistakes. Even in large enterprises, deploying new servers may not happen on a regular basis. The configuration of each host may vary based on what system administrator installed the operating systems or even on the amount of attention paid to the installation process. Unfortunately, small mistakes made at the time of initial configuration can have disastrous consequences.

Consistency of configuration adds an element of integrity to a network. If all servers are deployed with the same configuration, then at least the environment of the systems is known even if a vulnerability is discovered at some future time. While checklists are a great way to manually attempt to ensure this consistency, the human element can still lead to mistakes. A better way to ensure consistency is through a “gold loading” process that uses the same image to install many systems. Gold loads have been common in the desktop arena for years using programs such as Symantec’s Ghost. Mass installation capabilities for UNIX operating systems are common, but don’t necessarily have traction in the data center. Red-Hat’s Kickstart, modeled after Sun’s Jumpstart process, allows for repetitive installation of an operating system image on host after host after host. Setting up a Kickstart server may take some effort in the beginning, the long term impact on automation and security for your RedHat systems can be impressive.

Beyond technologies such as KickStart, virtualization is the next step in automating a consistent configuration on systems. Through virtualization technologies an operating system can be booted from exactly the same image on a variety of machines over and over again. By simply changing the one image, many machines can be modified to address patching issues, apply configuration changes, or do wholesale operating system upgrades. In the event of a compromise, virtualization allows sysadmins to quickly recover to a known good state. Even if the known good state isn’t “secure” in the face of a potentially unknown vulnerability, at least it serves as a starting point where an attacker is known to not be in the system. Virtualization promises to not only automate the configuration process but also the recovery process.

Automating the Auditing Process

Another area ripe for automation is the auditing process. There are a variety reasons to audit your systems: audit for compliance to policy, audit to look for intruders, or audit for understanding of deployed systems. Again, this is an area where manual processes and home grown scripts can get the job done. However, these manual processes may not be efficient and may prevent you from obtaining a holistic view of what’s going on inside your enterprise.

Checking configurations can be automated by programs such as Microsoft’s SMS or BelArc Advisor. These and other programs can help you understand, at a large scale, what is in-

stalled and running in your enterprise. By looking for outlawed programs such as instant messengers, P2P, or desktop search tools (all of which are verboten in many organizations), these tools allow you to rapidly look for compliance violations.

Also, your IDS infrastructure may be best suited for looking for internal compliance issues rather than monitoring for attacks from the outside. IDS's have sophisticated protocol and traffic analysis capabilities and are able to see "deeper" into networks than most firewalls. By turning your IDS inward and monitoring traffic between internal systems and the Internet, you may be able to find not only compromised systems, but also violators of corporate policy.

Parting Shots

IT security operations is not just about keeping your enterprise secure; it is also about doing so in as efficient a manner as possible. The more automated processes that you can deploy, the more assurance you will have of your assets and the better equipped you will be to handle the unexpected. There is no playbook to run a secure enterprise, but by having high level tools that assist in the secure configuration, maintenance, and operations of your systems you'll hopefully be one step ahead of those attempting to do harm to your business.