How to pentest well-known CMS

Frameworks and good design implementation
Backdoors hiding malicious payloads inside cascading style sheets
Why an automated vulnerability assessment is not enough
Vulnerability assessment should be a key part to your information security program. It's important to keep up to date with the ever-changing attack surface your network presents and automated scanning can help you keep on top of it. This week I’ve been looking at the Penetrator vulnerability assessment appliance from Secpoint (http://www.secpoint.com/penetrator.html) which offers a simple, straightforward way to scan your systems for remote vulnerabilities.

The Penetrator is available in several flavours, chiefly as a hardware appliance or as a VMware virtual machine. There’s also an option to buy the software-only product. Pricing is based on the number of IP addresses that can be scanned concurrently. The starting price for the appliance is $2,025.00 for an 8 concurrent IP address license and $675.00 for the VMWare virtual appliance with 4 IP addresses. You can change addresses being scanned as often as you wish so it’s good for consultants with multiple customers or companies with a larger block of addresses to scan and smaller budgets. I’ve been looking at the Penetrator S600 which is good for 16 concurrent IP addresses.

Once you plug in the appliance and power in a few minutes the device is ready to go. Log in to the web interface with your browser and you’re presented with a dashboard showing some quick links to commonly used functionality, a list of the previous audit scans and the status of the appliance. The Penetrator has a database of over 54,000 remote vulnerabilities and security issues.
Setting up a vulnerability scan is a breeze. Click on start audit, give your scan a name and add a list of IP addresses to scan and you’re ready to go. You can tweak the audit to scan additional ports over and above the default list and specify web server virtual hosts and directories to scan. You also have the option to enable plugins that may cause a denial of service and to attempt brute-force password attacks.

To aid managing your vulnerability assessments you can define audit templates with IP addresses and scan options and schedule audits to take place at a certain time or to run periodically. This way you can scan your machines at a time that suits and run regular checks to look for new vulnerabilities. Run your scans regularly and you can compare results to check for newly added vulnerability checks and to examine the change in state of your environment. New attack surfaces will present themselves if your environment is anything other than static.

As well as the vulnerability scanner there are other extra tools provided, including tools for performing brute force attacks on password hashes, zip files and network services including telnet, FTP, and databases servers. Attach a monitor, keyboard and mouse and you can log into the Linux console and launch Armitage, the GUI for the popular Metasploit exploit framework. While this is beyond what you might expect from a vulnerability assessment tool extra features like this a nice to have, rounds out the product and helps earn it the name Penetrator. One feature which is absent is the ability to perform credentialed scans to check for missing security patches or vulnerable software. Perhaps we can look forward to seeing this added in a future release.

The Secpoint penetrator is a neat, ready-to-use solution for anyone in need of a vulnerability scanner. It is simple to use and comparatively well priced with many of its competitors. I can see this being useful particularly for the SME market; the licensing based on concurrent IP certainly would suit growing businesses. With options ranging from virtual appliances to rack-mounted servers you’ll likely find a solution that suits your environment.

Check out SecPoint weekly news about Latest in IT Security Industry

by Jimmy Halfpenny