COMPARISON OF 5 TOP BROWSERS: FIND THE ONE STEP BY STEP

CHROME FORENSICS – HOW TO TRACE YOUR INTERNET ACCESS BEHAVIOR

HOW TO AVOID SECURITY FLAWS IN APPS USING IOS WEB VIEWS

GOOGLE CHROME – THE FUTURE OF WEB COMPUTING

SECOPOINT CLOUD PENETRATOR
Network security has rapidly become a significant part of Information Technology Infrastructure consisting of policies to prevent unauthorized access to data in a network. Without a strong security plan companies find themselves vulnerable to intrusion without any knowledge of a threat. The best solution is to hire a Security Specialist but this isn’t always applicable; many companies can’t afford to pay a specialist, or when they can, can they be sure their company is truly protected?

SecPoint introduces a service that will provide assistance monitoring network(s) of security risk that rapidly changes. To tell you the truth I’m always skeptical about the next great vulnerability scanner on the market. SecPoint once again lived up to their name; the Cloud Penetrator gives you an easy to use on demand vulnerability management system, and all that is needed is access to a web browser.

The Cloud Penetrator is one of a kind environment SecPoint created allowing customers to scan their network without any additional hardware or software. The web interface is very pleasant and has stress-free navigation. The Cloud Penetrator provides the ability to create specific scan templates, schedules, and standard vulnerability scans from anywhere that has internet access. The web interface also provides statistics, history, logs, and network tools (ping, whois, port scan, and mail server finder).

The Cloud Penetrator allows you to create scans multiple ways. Using a template allows you to receive email notifications when a new vulnerability is found. Creating a schedule allows you to repeat scans (Daily, Weekly, Monthly, and Yearly). No matter how the scan is created the setup of how the system is analyzed is always the same. First, the scan should have a name that is easily distinguishable. This way you don’t get lost after a few scans. After the scan is named you simply add the IP address or CIDR. These are IP addresses that you’re approved to scan, and already provided SecPoint with the appropriate agreement form. Finally, the type of scan will need to be chosen. This is where everything gets interesting. The Cloud Penetrator provides 7 default scans which can be further modified with advanced options. The default scans are Quick, Quick Web, Normal, OWSAP Top 10, Aggressive DoS, Extensive, and Extensive Firewall. Deciding which scan to run requires knowledge of what each scan does. Below each scan is listed and more information please visit: http://www.secpoint.com/datasheet/Penetrator-Schematics_web.pdf.

The information provided above will allow educated decisions to be made when deciding which
scan to use and when to use them. Always remember the more extensive scan will require more time. Once the type of scan has been chosen we can easily be done, but let’s dive into the advanced setup options.

The Advanced setup enables each scan to be modified, allowing anyone to customize their scan to meet their specific needs. The advanced setup allows you six options to configure notes, ports, dirs, vhost, email, and aggressive. Notes allow you to add a note to the scan, maybe the specific purpose of each scan. The ports option sets specific ports that the system will scan. Dirs allow single directories to be audited, targeting each attack only at that specific directory (Example: www.mydomain.com/chickens) you would only add "chickens". Vhost are

![SecPoint Cloud Penetrator](image)

**SCAN TYPES:**

**QUICK SCAN**
Quick Scan over most common TCP/IP port numbers

**QUICK WEB SCAN ONLY**
Designed to be non-harmful and not flood the services by simulating humans’ behavior
- Non harmful Scan with ports: 80,443, 8000, 8080, 8443
- Web Application Vulnerability Scanner WAS
- Web Crawler
- Google Hacking DB
- Joomla Security Scan
- Google Safe Browsing
- 50+ Blacklist Checks
- Wordpress Security Scan
- Windows, MAC, Linux, Nix, and other OS’s

**NORMAL RECOMMENDED SCAN**
Designed to be non-harmful and not flood the services by simulating humans’ behavior
- Scans 8000 among the most common ports
- Performs 55+ checks
- Firewall, DNS, FTP, Web, SSL, SSH, SQL, NetBIOS, and much more.
- Everything Included in Quick Web Scan

**OWASP TOP 10 SCAN**
The OWASP Top 10 is a list of most common web application vulnerabilities.

**AGGRESSIVE DOS SCAN**
- Designed to be a harmful scan
- Full Scan of all 65535 ports
- Overflow Attacks
- DoS Attacks
- Includes everything in Normal Scan

**EXTENSIVE SCAN – NON HARMFUL**
- Full Scan of all 65535 ports
- Includes everything in Normal Scan

**EXTENSIVE FIREWALL SCAN – NON HARMFUL**
- Same as Extensive Scan but designed for firewalls, because it tries to scan address that appears offline.

*Information above was obtained from within SecPoint Cloud Penetrator.*

**Figure 1. Cloud Penetrator Scan types and description**

<table>
<thead>
<tr>
<th>Sel. Date</th>
<th>Scan Name</th>
<th>profile</th>
<th>Status</th>
<th>H. M. L. I.</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-06-24</td>
<td>aggressive</td>
<td>Aggressive DoS...</td>
<td>Completed</td>
<td>3 2 0 3</td>
<td></td>
</tr>
<tr>
<td>2013-08-22</td>
<td>extensive</td>
<td>Extensive Firew...</td>
<td>Completed</td>
<td>3 2 0 3</td>
<td></td>
</tr>
<tr>
<td>2013-06-19</td>
<td>Night Scan</td>
<td>OWASP Top 10 Sc..</td>
<td>Completed</td>
<td>3 2 0 3</td>
<td></td>
</tr>
<tr>
<td>2013-06-03</td>
<td>Normal Recommen.</td>
<td></td>
<td>Completed</td>
<td>3 2 0 3</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2. Completed Scan Options**
used when several domain names run on the same IP address, and email simply notifies you when the scan has been completed. The aggressive are intended to be harmful, always remember that when you set them. They allow you to set the attack types exactly as it’s needed. Once the scan has been set up the duration of the scan will depend on the options selected and the network it’s scanning. Each scan preformed on my personal network took approximately 45 minutes. The process of setting up a scan from the web GUI was very user friendly, allowing you to fine tune the scan to exactly what is needed. I was very satisfied with the simplicity of setting up the audit, and I have confidence you will feel the similar experience.

This whole process of setting up the scan and waiting for it to finish would be pointless without valuable results. Once the scan is completed SecPoint allows you Many Options for viewing the report PDF, Web, One Page Summary, Full without Solution, and XML. With so many options these reports can be viewed on virtually any device (Figure 2). Within these options you also have the capability to recreate the PDF reports, repeat the scan, add false positives, archive, and delete the scan.

The Full report with solutions is the most informative report. It has 9 different sections packed with information about the audit. The first two sections are the Introduction and the Vulnerability Details. These sections of the report are fully informative on how the rest of the report is laid out. The first part of the report that is exclusive for the particular audit is the Executive Summary. This is a

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Status</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>463</td>
<td>tcp</td>
<td>open</td>
<td>alpes</td>
</tr>
<tr>
<td>862</td>
<td>tcp</td>
<td>open</td>
<td>Two-way Active Measurement Protocol (TWAMP) Control</td>
</tr>
<tr>
<td>1723</td>
<td>tcp</td>
<td>open</td>
<td>pptp</td>
</tr>
</tbody>
</table>

Figure 4. Ports are services results

<table>
<thead>
<tr>
<th>Banner name</th>
<th>SSHd Version Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>862/tcp</td>
</tr>
<tr>
<td>Details</td>
<td>SSH-2.0-OpenSSH_5.4p1 FreeBSD-20100308</td>
</tr>
</tbody>
</table>

Figure 5. Services Version Banner outputs

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Point-To-Point (PPTP) Protocol tcp port 1723 identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Level</td>
<td>Medium</td>
</tr>
<tr>
<td>SecPoint ID</td>
<td>53</td>
</tr>
<tr>
<td>BugtraqID</td>
<td>2111</td>
</tr>
<tr>
<td>BugtraqID</td>
<td>2549</td>
</tr>
<tr>
<td>BugtraqID</td>
<td>3022</td>
</tr>
<tr>
<td>BugtraqID</td>
<td>2549</td>
</tr>
<tr>
<td>BugtraqID</td>
<td>7582</td>
</tr>
<tr>
<td>BugtraqID</td>
<td>7590</td>
</tr>
<tr>
<td>Impact</td>
<td>Several services running the identified port is subject to many vulnerabilities specially Denial of Service attacks.</td>
</tr>
</tbody>
</table>

Figure 6. Vulnerability Identification output
quick overview of the scan results, made for management personnel. The last six sections of the report are very informative, presenting the results of the audit more in-depth for IT professionals. Traceroute, Ports and Services, Banner Identification, Summary of Vulnerabilities, Vulnerabilities, and Gap Analysis. This report has everything you need to really analyze any network. Each section has valuable information; the traceroute section correctly verified that my network was blocking ICMP traffic. While the Ports and Services section shows what the ports services are commonly tied to, not what service is actually using them (Figure 4).

This could be looked at as a bad thing, but in reality this is exactly what a penetration tester will be looking at until they get more information. Where do they get that information, well SecPoint included it in the results too Banner Identification, it shows any banner information provided by the actually service running on the system (Figure 5).

As you can see I’m truly not running Two-way Active Measurement Protocol Control on port 862. Also you might have noticed that I have not added any solutions with my images. I figured it would be best if I kept them out so you can discover them for yourselves.

The next two sections are dedicated to the vulnerabilities found during the audit. The summary gives a brief description of each risk category and the treats found. While the Vulnerabilities a section provides further details into each threat. Surprisingly the only High risk vulnerabilities found during the audit was three different blacklists. I say surprisingly because I did not expect to see a blacklist anywhere with each vulnerability assessment provided is the impact it can have for any business. Provided listed as vulnerabilities but I defiantly understand the impact it can have for any business. Provided with each vulnerability assessment provided is the risk level, SecPoint ID, Impact, and Solution. The SecPoint ID is the official SecPoint ID of the vulnerability. For more information on each vulnerability please visit http://www.secpoint.com/libpage.php If applicable SecPoint also provides you with BugtraqID, CVE, and USN information that you can easily click the number to verify the existence of the discovered vulnerabilities (Figure 6).

The final section of the report is the Gap Analysis which will show you what has changed since the last audit. This section can be very important when wanting to know the differences between scans without having to investigate each section. Besides the Full report the 1 page summary is a good report to give to management. Showing the number discoveries found during the audit in an easy to read report.

Scan statistics is another great feature SecPoint provides, but be warned that you need to enable global logging, global logging saves sensitive information associated with your IP to the system. If you do not wish to have your sensitive information saved you need to turn global logging off. Statistics shows the information obtained by each audit. As you can see my results never changed since I have not made any modification to my network (Figure 7).

SecPoint Cloud Penetrator is a great service, any great service can constantly be improved. I was only disappointed with the results of my aggressive scan, which took advantage of overflow, DoS, and bruteforce attacks. Setting up the scan worked as I expected, but once I got the report I realized that no information was provided about the success or failure of any of the attacks. I think SecPoint should provide this information to make their service truly irreplaceable. As a convenience it would be more practical for SecPoint to provide links to their SecPoint ID like they do for Bugtraq ID’s. The only other section I felt could be improved was the information provided with in the blacklist results. I felt like I was reading the same information for each discovery except no information was truly provide on how to resolve the issue. Overall each person will have their own experience. I challenge you to try this service for yourself for free at: http://www.secpoint.com/free-vulnerability-scan.php.

There are two approaches to security, proactive and active. May organizations only rely on active measures (Only fix something once it’s actually broken). SecPoint Cloud Penetrator gives you a proactive approach allowing you to resolve insecure areas of your network before it’s too late. I was impressed with functionality and quality of the service SecPoint is providing. I would recommend this service to anyone looking for a reliable way to audit their network. With SecPoint Cloud Penetrator you no longer have to have the “we’re safe, until it’s too late” approach leaving your network infrastructure and private data secure.

Purchasing and more information can be found at http://www.secpoint.com/cloud-penetrator.html.