HARDSHAPE HACKING
Data Recovery

DATA RETENTION FOR SMARTPHONES
RECOVERING USB DATA
CONTENT-AWARE E-MAIL RECOVERY

PLUS

DO IT YOURSELF
DATA RECOVERY
SecPoint Cloud Penetrator
Online Vulnerability Assessment Scan

Waking up every morning a skeptic is not that difficult. By 10 AM there are usually two or three interactions that prove I was right.

I was invited by Hakin9 to do an evaluation of a product called “SecPoint® Cloud Penetrator”, a service provided by SecPoint® of Copenhagen Denmark (my first thought was that I needed to do an on-site assessment – and visit Tivoli gardens – it’s been over 40 years since my last visit – but I still remember it well). In reviewing their web site I noted that they provide many tools in the security arena, both products and services, on-site and off. In my disclosure request to Hakin9 I was informed “They collaborated with us long time ago, and they refreshed the co-op two weeks ago”. Hakin9 also provided me a copy of an assessment of the SecPoint® Penetrator S300 (an onsite system) by Michael Munt some years ago.

As a true skeptic, I need to be skeptical of the customer also. I find there are basically two types of customers for this type of product: Customers who want the best confidentiality, integrity, and availability possible; and the second type who needs the appearance of security for management or compliance purposes.

Management overview: If you are a customer who needs the appearance of security for management or compliance reasons, this tool provides excellent reports that can be filed in your compliance file. If you are a customer to whom true security, confidentiality, integrity, and availability are of crucial or of utmost importance - this is, in my opinion, one of the better tools to help you towards that goal.

For those of you who are interested in TRUE security, confidentiality, integrity, and availability:
This is a product that, in my opinion, should be in your tool kit.

The time and study that would be required to duplicate the quality of this analysis would be far more than the cost of the service. Plus having a whole team dealing with new threats appearing daily would cost far more than the daily cost of $0.44 per day (1 IP, 6 months service) up to $2.41 per day (8 IPs, 1 Year Service).

The quick look at the overall assessment in a graphic is very useful to visualize which server to work on first.

Because of operational difficulties (I used up my two free scans only to find out that their cloud based service couldn’t “see” the test targets), I did not run the scans myself, and they were run by SecPoint®s team. As a consequence, I have no opinion on the ease of use or user interface, I would commend you to Mr. Munt’s article: (http://www.secpoint.com/awards/HAKIN9-Product-Review-PP3000-English-June-2010.pdf).

Before starting the scan I was required to provide written proof of “ownership” of the to-be-scanned IP’s, and permission for SecPoint® to run the scan.
They provided evidence of scans of the two requested IPs and I was favourably impressed. The scan of “.6” took 17 hours and 58 minutes and was performed by SecPoint® Cloud Penetrator 8.8.1.115 . The scan of “.10” took almost 10 hours and 28 minutes and was the same version of Cloud Penetrator. Both of these evaluations were run simultaneously (“.10” was started 2 seconds after “.6”) so they were potentially competing for bandwidth (our side 10 MBPS Fibre Optic). According to Mr. Munt’s article there is a “Quick Audit”, which may be considerably faster.

The reports listed all the vulnerabilities and issues reported by a competing product (of considerable higher cost) run 1 day later on unmodified servers.

Of note, the reports provided by SecPoint® provided not only the reference to the vulnerability/issue in Bugtraq (Securityfocus.com) and the Official CVE (maintained by Mitre under a US Government contract), but the Impact information (“what does this mean to me”), so I didn’t have to go to CVE or Bugtraq to find out what issue was. This saves me considerable time over the competing product (did I mention higher priced?) which simply gave me a reference to the CVE and left me on my own to research the issue.

From a compliance and evidentiary (forensic) viewpoint, there were some things I would have liked to have seen in the reports. I would have liked to have seen both the source IP and the target IP listed on each page of the report (26 pages for one scan and 36 pages for the other scan) to prevent page replacement. The report listed the time in Eastern European time on every page of the report (excellent) this was presumably because that was the time at the scanning site. For multinational organizations this would be much better if it also listed UTC. I have testified in court where a simple issue of “what time was it” was used by the defense to obfuscate whether two reports were simultaneous, and I spent 40 minutes being questioned by the prosecution to clarify simple time conversions because the reports had different times on them.

SecPoint® seems to get other things right. On the “.6” server they reported that the IP was listed on the barracudacentral blacklist (the higher priced spread did not get this one), but better than that, they correctly, in my opinion, listed it as a “High” risk (Can you spell Availability). Arguably email is the most pervasive use of the web, and this single issue (it is not a vulnerability) can cause your email never to be received.

My overall assessment of the tool was favourable, and I would highly recommend it to customers. Of course your mileage may vary, but starting out with a high mileage tool is always better than finding out you were using a higher cost, lower mileage tool.

Figure 2: Risk Factor

![Risk Factor Diagram](image)

ABOUT THE EVALUATOR

DAVID VON VISTAUXX, CHS®, PMP®, CISSP®. Can be reached at: hakin.secpoint.article@infrastructuresecurity.net