

Re: Experiences with company nCircle and their IP360 product

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-11/0252.html>

From: Tom Stracener (*strace_at_gmail.com*)

Date: 11/25/05

Date: Fri, 25 Nov 2005 16:10:14 -0600

To: "Bongers, Coen" <coen.bongers@logicacmg.com>

Coen,

On the issue of unique or distinguishing features I would comment on nCircle's quantitative risk metrics for vulnerabilities. I created the formulas for this system back in 1999, and worked with other founding members to further refine and enhance the system over the next couple of years. Since then nCircle has continued to make modifications and improvements to the core risk analysis algorithms, and the result has been the development of a highly scalable risk analysis metric that allows you to view the risk of vulnerabilities, hosts, and networks at a glance.

To help you understand the technical premises of vulnerability metrics, you can think of a vulnerability as having a penetration depth, to what degree does a successful attack correlate with elevated privileges. A sophistication factor, how difficult is it to exploit the vulnerability, what types of exploits, tools, worms, or exploit frameworks exist for the issue. An attack vector, how is the vulnerability exploited. Also, what is the vulnerability life-cycle state in relation to time. In essence, vulnerability risk is sort of parabolic over time, although with the delayed rate of patching and long-term persistence of vulnerabilities, the curve is less parabolic than you would think.

These are just a few of the important assumptions. The importance or critically of the system on which a vulnerability is resident, the relation of the vulnerability to the network perimeter, etc., are also key factors. This should give you an idea of the advantage of using quantitative metrics in risk analysis, because you get a weighted generalization of all these factors with the benefit of granularity and succinct mathematical expression. High scoring systems and networks can then get your first attention, a significant advancement over having lists of thousands of low/medium/high qualitative labels.

I don't know the extent to which IP360 still uses the factors above,

SecurityFocus Penetration: Re: Experiences with company nCircle and their IP360 product

but if you have an opportunity to view its output and reporting, know that the vulnerability and network scoring metrics were not technical windings tacked on at the behest of marketing -- but core technical features that have undergone years of serious scrutiny and refinement.

Mike Murray has also done some amazing work on vulnerability signature precision. Be sure to check it out:

http://www.ncircle.com/pdf/papers/nCircle_Precision_Metrics.pdf

Hope my comments interest you.

-Tom

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do! Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831
