Información personal

Nombre completo: Paulino Calderón Pale
Nacionalidad: Mexicana
Fecha de nacimiento: 27/04/1986
Correo electrónico: paulino@calderonpale.com
Sitio web: http://calderonpale.com
Idiomas: Español e inglés fluido.

Capacidades técnicas

- Experiencia con sistemas operativos de la familias Microsoft Windows, Linux y BSD.
- Experiencia en proyectos de consultoría en el sector financiero, privado y gubernamental.
- Conocimiento avanzado en procesos de descubrimiento y explotación de vulnerabilidades en aplicaciones web y móviles.
- Conocimiento avanzado de procesos de descubrimiento y explotación de vulnerabilidades en redes informáticas.
- Familiarizado con metodologías de evaluación de vulnerabilidades como OSSTMM, OWASP y NIST SP800-115.
- Familiarizado con el sistema de evaluación de criticidad de vulnerabilidades CVSSv2.
- Familiarizado con las clasificaciones de patrones de ataques CAPEC y debilidades en software CWE.
- Conocimiento de las fases y procesos del SDLC.
- Experiencia en administración de sistemas como servidores web, bases de datos, sistemas de correo y firewalls.
- Experiencia con arquitecturas de cómputo distribuido como Apache Storm y Hadoop.
- Conocimiento en análisis de tráfico de red.
- Conocimiento en Lua, Java, PHP, ASP.NET, Perl, Ruby, C, C++, Bash scripting, Python y x86 asm.
- Contribuciones a proyectos de software libre: Nmap, Metasploit, Dnmap, CakePHP, CroogoCMS y MantisBT.
- Participante exitoso del programa Google Summer of Code 2011 en el cual mejoró las capacidades de escaneo web del proyecto Nmap.
- Mentor del proyecto Nmap durante Google Summer of Code 2015 en el cual se dedico a detección y explotación de vulnerabilidades.
- Forma parte del equipo oficial de desarrolladores de Nmap.

Vulnerabilidades descubiertas

- Vulnerabilidades de tipo SQL inyección en content providers del sistema Android [https://code.google.com/p/android/issues/detail?id=46573] (0day)
- Path traversal en dispositivos TP-Link WDR740 [http://www.websec.mx/publicacion/advisories/tplink-wdr740-path-traversal]
- Ejecución de comandos remota en dispositivos TP-Link WDR 740 [http://www.websec.mx/publicacion/advisories/puerta-trasera-tplink-wdr740]
- Vulnerabilidades de tipo Cross Site Scripting/inyección HTML en Croogo CMS [http://www.securityfocus.com/bid/38593]
- Vulnerabilidades de tipo XSS en MantisBT [https://www.mantisbt.org/bugs/view.php?id=13191]

Desarrollo de exploits

- lansweeper_collector - Extrae y descifra credenciales almacenadas en Lansweeper [https://www.rapid7.com/db/modules/auxiliary/gather/lansweeper_collector]
- apache_tomcat_transfer_encoding - Explota vulnerabilidad que revela codigo fuente de aplicaciones en servidores Apache Tomcat vulnerables [https://www.rapid7.com/db/modules/auxiliary/dos/http/apache_tomcat_transfer_encoding]
- http_form_fuzzer - Explota aplicaciones web vulnerables a entrada de datos malformadas [https://www.rapid7.com/db/modules/auxiliary/fuzzers/http/http_form_field]
- http-vuln-cve2015-1635 - Explota sistemas Windows vulnerables a MS15-034 [https://nmap.org/nsedoc/scripts/http-vuln-cve2015-1635.html]
- http-coldfusion-subzero - Explota servidores ColdFusion [https://nmap.org/nsedoc/scripts/http-coldfusion-subzero.html]
- http-adobe-coldfusion-apsa1301 - Explota servidores ColdFusion. [https://nmap.org/nsedoc/scripts/http-adobe-coldfusion-apsa1301.html]
- http-shellshock - Explota la vulnerabilidad conocida como Shellshock. [https://nmap.org/nsedoc/scripts/http-shellshock.html]
- http-tplink-dir-traversal - Explota una vulnerabilidad 0day de tipo path traversal en dispositivos TPLink. [https://nmap.org/nsedoc/scripts/http-tplink-dir-traversal.html]
- mysql-vuln-cve2012-2122 - Explota un fallo en el sistema de autenticación de gestores MySQL/MariaDB. [https://nmap.org/nsedoc/scripts/mysql-vuln-cve2012-2122.html]
- http-axis2-dir-traversal - Explota una vulnerabilidad de tipo path traversal en instalaciones Apache Axis2 [https://nmap.org/nsedoc/scripts/http-axis2-dir-traversal.html]
- http-huawei-hg5xx-vuln - Explota dos vulnerabilidades criticas en dispositivos Huawei. [https://nmap.org/nsedoc/scripts/http-huawei-hg5xx-vuln.html]
- supermicro-ipmi-conf - Explota controladores Supermicro Onboard IPMI [https://nmap.org/nsedoc/scripts/supermicro-ipmi-conf.html]

- http-awstatstotals-exec - Explota un RCE en Awstatstotal [https://nmap.org/nsedoc/scripts/http-awstatstotals-exec.html]
- http-vuln-cve2012-1823 - Explota instalaciones PHP-CGI vulnerables a CVE-2012-1823 [https://nmap.org/nsedoc/scripts/http-vuln-cve2012-1823.html]
- http-litespeed-sourcecode-download - Explota servidores web LiteSpeed [https://nmap.org/nsedoc/scripts/http-litespeed-sourcecode-download.html]
- smb-vuln-ms08-067 - Explota la famosa vulnerabilidad en sistemas Windows conocida como MS08-067 [https://nmap.org/nsedoc/scripts/smb-vuln-ms08-067.html]
- smb-vuln-cve2009-3103 - Explota sistemas Windows CVE2009-3103 [https://nmap.org/nsedoc/scripts/smb-vuln-cve2009-3103.html]
- smb-vuln-ms07-029 - Explota sistemas Windows CVE 2007-029 [https://nmap.org/nsedoc/scripts/smb-vuln-ms07-029.html]
- http-iis-short-name-brute - Explota IIS servers para obtener los nombres cortos de los archivos en el webroot [https://nmap.org/nsedoc/scripts/http-iis-short-name-brute.html]
- http-avaya-ipoffice-users - Explota dispositivos Avaya IPOffice [https://nmap.org/nsedoc/scripts/http-avaya-ipoffice-users.html]
- http-cross-domain-policy - Detecta politicas inseguras de crossdomain [https://nmap.org/nsedoc/scripts/http-cross-domain-policy.html]
- http-majordomo2-dir-traversal - Explota instalaciones vulnerables de Majordomo2 [https://nmap.org/nsedoc/scripts/http-majordomo2-dir-traversal.html]
- http-phpself-xss - Explota vulnerabilidades XSS en la variable PHPSELF [https://nmap.org/nsedoc/scripts/http-phpself-xss.html]
- http-method-tamper - Explota servidores web vulnerables a verb tampering [https://nmap.org/nsedoc/scripts/http-method-tamper.html]
- http-vuln-cve2013-0156 - Explota aplicaciones Ruby on Rails vulnerables a RCE [https://nmap.org/nsedoc/scripts/http-vuln-cve2013-0156.html]
- polarisoffice-filemon - Explota una vulnerabilidad en content providers vulnerables de la aplicacion polarisoffice para android [https://github.com/cldrn/polarisoffice-filemon]

Conferencias impartidas

Más de 20 conferencias sobre seguridad informática impartidas en México, Estados Unidos, Canadá, Colombia, Perú y Bolivia. Los detalles los pueden encontrar en la siguiente dirección: http://calderonpale.com/about-me/.

Talleres impartidos

El arte de la exploración de redes

Taller sobre el descubrimiento de activos en redes informáticas.
Liga: http://www.slideshare.net/Websecmx/exploracin-de-redes-con-nmap

Desarrollando para el Nmap Scripting Engine

Taller sobre desarrollo de scripts para el motor de scripts de Nmap.

Liga:
http://www.slideshare.net/Websecmx/desarrollando-para-nmap-scripting-engine-nse-guadalajaracon-2013

Búsqueda de vulnerabilidades en aplicaciones Android

Taller sobre auditoría de seguridad de aplicaciones Android.
Liga:
http://www.slideshare.net/Websecmx/bsqueda-de-vulnerabilidades-en-aplicaciones-de-android-guadalajaracon-2013

Pentesting 101

Taller introductorio a las pruebas de penetración y análisis de vulnerabilidades de redes informáticas.
Liga: http://www.slideshare.net/Websecmx/pentesting-101

Publicaciones, artículos y talleres

Nmap 6: Network Exploration and Security Auditing Cookbook

Libro digital e impreso sobre auditorías de seguridad y exploración de redes utilizando la herramienta Nmap.
Liga:
http://www.amazon.com/Nmap-exploration-security-auditing-Cookbook/dp/1849517487/

Mastering the Nmap Scripting Engine

Libro digital e impreso sobre desarrollo de módulos para el motor de scripts de Nmap.
Liga: http://www.amazon.com/gp/product/1782168311/

Censo de seguridad de redes wifi en México 2015

Censo de seguridad de redes wifi en México.
Liga: http://www.websec.mx/publicacion/blog/infografia-seguridad-wifi-mexico-2015

Comprometiendo Lansweeper

Vulnerabilidades descubiertas en software de administración de activos de TI.
Liga:
http://www.websec.mx/publicacion/blog/comprometiendo-las-crendenciales-de-lansweeper

Gathering Web server information

Artículo sobre el proceso de recolección de información realizado a servidores web.
Liga: http://calderonpale.com/uploads/NSE_Information_gathering.pdf

Estadísticas de redes inalámbricas 802.11 en México

Estudio sobre el ecosistema de redes wifi en México durante el 2013.
Liga: http://www.websec.mx/Estadisticas_2013_de_Redes_802.11_en_MX.pdf

(IN)seguridad de datos de sesión en Codeigniter

Artículo sobre vulnerabilidades en el manejo de datos de sesión en aplicaciones hechas con el framework Codeigniter.
Liga: http://www.websec.mx/blog/ver/inseguridad-datos-sesion-codeigniter

Proyectos de desarrollo de software

- Más de 50 scripts de detección y explotación de vulnerabilidades que se distribuyen con Nmap oficialmente. (https://github.com/cldrn/nmap-nse-scripts/tree/master/scripts/6.x)
- 3 modulos de explotación de vulnerabilidades que se distribuyen con Metasploit oficialmente (http://www.rapid7.com/db/search?q=Paulino+Calderon)
- HHG5XX mac2wepkey scanner (+6 millones de descargas) (https://play.google.com/store/apps/details?id=mx.websec.mac2wepkey.hhg5xx)
- Rainmap-lite (https://github.com/cldrn/rainmap-lite)
- InsecureProgrammingDB (https://github.com/cldrn/InsecureProgrammingDB)
- Ip2hosts (+50 mil usuarios activos mensuales) (http://ip2hosts.com)
- Wardrive analytics (https://github.com/cldrn/wardrive-analytics)
- Enum4linux 0.9 (https://github.com/cldrn/enum4linux-0.9)
- Davtest 1.1 (https://github.com/cldrn/davtest)
- Detector de Puertas Traseras (http://www.websec.mx/blog/ver/detector-puertas-traseras-websec)
- Cakephpids (https://github.com/cldrn/cakephpids)
- recaptcha-cakephp (https://github.com/cldrn/recaptcha-cakephp)
- Contribuciones al proyecto Dnmap (http://sourceforge.net/projects/dnmap)
- Vecinitum de fibra (https://play.google.com/store/apps/details?id=mx.websec.mac2wepkey.al)
- Otros proyectos se pueden encontrar en https://github.com/cldrn/.

Educación

- Computer Science, Networking option. University of Victoria. Victoria, British Columbia, Canada. (2005-2010) [Carrera trunca].
- Especialización en Big Data. UC San Diego. Coursera.org
- Pwning and Responding to SCADA Devices and Networks. Curso en DerbyCON.

Premios

- 1er lugar en App Challenge - TelmexHUB Mérida (2011).

- 1er lugar en Reto de seguridad Movistar - Campus Party México (2014).