Evaluación del Ataque ShellShock

William Sani, Roger Jaimes, y Jessenia Ramón

williamwrsa@gmail.com, rogerj007@gmail.com, jessenia.ramonc@gmail.com

Abstract— **Actualmente las aplicaciones Web son cada vez más utilizadas por los usuarios en el ciberespacio, lo que ha provocado que cada vez se vayan incrementando y descubriendo las vulnerabilidades de los servidores y aplicaciones a fin de realizar ataques informáticas con un fin determinado. Una vulnerabilidad presente en algunos servidores Web, es el conocido ShellShock, que es una vulnerabilidad en el Shell Bash de los sistemas operativos Linux/Unix, el cual permite ejecutar comandos por atacantes de manera remota, por lo que se le conoce también con el nombre de Bashdoor. Considerando lo indicado, se realizó un análisis y evaluación del vector de ataque usado por ShellShock utilizando herramientas open source bajo un ambiente virtualizado de experimentación, el cual permitió de manera práctica realizar un ataque backdoor a un servidor Web vulnerable. Adicionalmente se instaló un WAF, como un mecanismo de mitigación para este tipo de ataques. De la experimentación realizada se pudo determinar la criticidad de este tipo de ataques y la importancia de realizar una actualización de dispositivos que utilizan Bash Shell o implementar WAF a fin de mitigar ese tipo de ataques.**

Palabras clave— *Exploit, CVS, ShellShock, pruebas de penetración, WAF.*

I. INTRODUCCIÓN

Los ataques "ShellShock" o Bashdoor podrían permitir a un atacante tomar control remoto de millones de servidores y computadores en todo el mundo. El nombre oficial de esta vulnerabilidad es GNU Bash Remote Code Execution Vulnerability (CVE-2014-6271). Esta vulnerabilidad permite a hackers realizar ataques con inyección de código remoto y tomar el control del sistema objetivo Linux, Unix o Mac. En este momento más de la mitad de los servidores de Internet y teléfonos Android se encuentran afectados, dado que el 51% de los servidores web de todo el mundo funcionan con Linux.[1] El alcance contemplado por esta falla teniendo en cuenta que no se requiere autenticación para explotar esta vulnerabilidad sobre el código abarca principalmente la divulgación no autorizada de información; modificación sobre la configuración del sistema operativo y la interrupción del servicio derivada de los dos puntos anteriores.[2]

La comunidad científica ha investigado e implementado mecanismos para disminuir y mitigar estos ataques. La mayoría de distribuciones de GNU/Linux han lanzado actualizaciones tanto para sistemas de escritorio como para servidores Linux; pero el verdadero problema radica en aquellos sistemas que no se actualizan (parches), bien porque no hay nadie que los mantenga o porque se trata de sistemas incrustados en dispositivos que no están preparados para recibir actualizaciones o el fabricante ha dejado de publicarlas para ciertos modelos[3]. También se debe considerar que esta vulnerabilidad puede realizarse utilizando el protocolo SSH y con DHCP, esto en determinados equipos, como por ejemplo: routers y switch, que pueden estar sin soporte por parte de los fabricantes por lo que algunos de estos seguirán con la vulnerabilidad.

Esta investigación se enfoca en el análisis y evaluación del ataque ShellShock, utilizando como plataforma de experimentación un ambiente virtual de red para identificar como actúa dicho ataque, utilizando VMware como hypervisor. Para llevarlo a cabo se ha implementó una red LAN y WAN con la finalidad de inhabilitar los accesos internos y eternos. Como contribución se ha implementado un Web Application Firewall para mitigar este tipo de ataques. Se instaló el WAF Open Source ModSecurity, el cual se integra con el servidor Web Apache.

Finalizando la experimentación se pudo determinar la criticidad de este tipo de ataques y la importancia de realizar una actualización de dispositivos que utilizan Bash Shell o implementar otros mecanismos de seguridad como WAF, a fin de mitigar ese tipo de ataques.

Las principales contribuciones del presente trabajo son: i) análisis y evaluación del ataque ShellShock; y, ii) implementación de un WAF que permita detectar y mitigar estos ataques.

El resto del artículo ha sido organizado de la siguiente manera: la sección 2 describe el fundamento teórico. La sección 3 muestra los componentes del experimento, así como el proceso de mitigación. La sección 4 ilustra los resultados obtenidos. La sección 5 muestra trabajos relacionados con el tema, Finalmente en la sección 6 se exponen las conclusiones y trabajo futuro.

II. FUNDAMENTO TEÓRICO

La vulnerabilidad en el Shell bash, de sistemas operativos Unix/Linux, tiene algunos vectores de ataques. Una vulnerabilidad es un punto abierto en un o más sistemas informáticos que podría afectar los objetivos de confidencialidad, integridad, disponibilidad, no repudio y autenticación de la información. Un vector de ataque, por su parte, es el método que utiliza una amenaza para atacar un sistema. Entre los principales se tienen los siguientes:

A. *Servidores HTTP*

El error ShellShock está atacando principalmente los servidores Web HTTP. Aquellos servidores que se ejecutan en FastCGI o CGI son capaces de exponer el bash al vector de petición de HTTP. Las peticiones HTTP maliciosas permiten a los ciberdelincuentes integrar comandos en el servidor y el Bash puede ejecutarlas.

El atacante puede utilizar esta conexión para realizar diferentes tipos de ataques, como DDOS o para obtener información.

Existen lenguajes de programación, como Perl, PHP y scripts de Python que no son utilizados a través de los sistemas de CGI anteriormente mencionados por lo que probablemente no se verán afectados por esta vulnerabilidad.[4]

B. *Clientes DHCP*

Los clientes de DHCP también podrían ser vulnerables debido a del error ShellShock. Esto es válido para UNIX y el sistema Linux, pero no está afectando al sistema OSX.

Los clientes DHCP pueden pasar comandos de Bash, un sistema vulnerable puede ser atacado cuando se conecta a una red abierta Wi-Fi. Un cliente DHCP típicamente solicita y recibe direcciones IP de un servidor DHCP, pero también puede proveer una serie de opciones adicionales. Un servidor DHCP infectado puede proveer, en una de estas opciones un string hecho de tal forma que ejecute un código malicioso en una computadora de trabajo

Durante el ataque, el criminal cibernético también puede utilizar el vector CGI con el fin de poner en peligro el servicio DHCP en un servidor que es legítimo.[4]

C. *SSH*

La mayoría de los sistemas de SSH están configurados de tal manera que restringe los comandos que el usuario puede aplicar. Los atacantes utilizan el bug Bash en las sesiones SSH con el fin de ir vulnerar las restricciones aplicadas. Sin embargo, esto requiere autenticación y es por eso es que este vector ofrece una escalada de privilegios.

Los sistemas que utilizan SSH, incluyendo rsync, rlogin, subversión, y otros también pueden verse afectados.[4]

D. *Sistema Unix Printing Común (CUPS)*

Un servidor de impresión, el Common UNIX Printing System está disponible en muchos UNIX, los sistemas BSD y Linux. Trabaja con variables que son controlados por el usuario y basado en esto se establecen las variables de entorno en el tratamiento de los filtros. Puede actuar como un vector para la vulnerabilidad Sheshock, en el caso de que el Bash sea inicializado por el sistema de impresión común de UNIX. Actualmente, este vector es teórico.

E. *Shellshock Attack*

El concepto de ShellShock attack consiste en el uso de la vulnerabilidad en el Shell bash. El Shell se utiliza para ejecutar comandos en Unix / Linux; es decir, actúa como un intérprete de lenguaje de comandos. ShellShock puede incluso afectar a las versiones más recientes del Shell bash. También se conoce como el error bash. Permite a un atacante obtener el control sobre el equipo. Un tipo de variables en bash son las variables ambientales. Una vulnerabilidad en el bash se gana a través de esta variable ambiental. Aunque ciertas condiciones tienen que cumplirse para la explotación de la vulnerabilidad, una vez que su atacante tiene éxito puede hacerse con el control del servidor remoto.

En la figura 1 se esquematiza la vulnerabilidad ShellShock. En general, el código dentro de la función tendrá problemas en su ejecución, mientras que el código fuera de las llaves se ejecutará, esto es la vulnerabilidad CVE-2014-6271. El atacante puede acceder remotamente usando un payload, de ahí el nombre bashdoor.

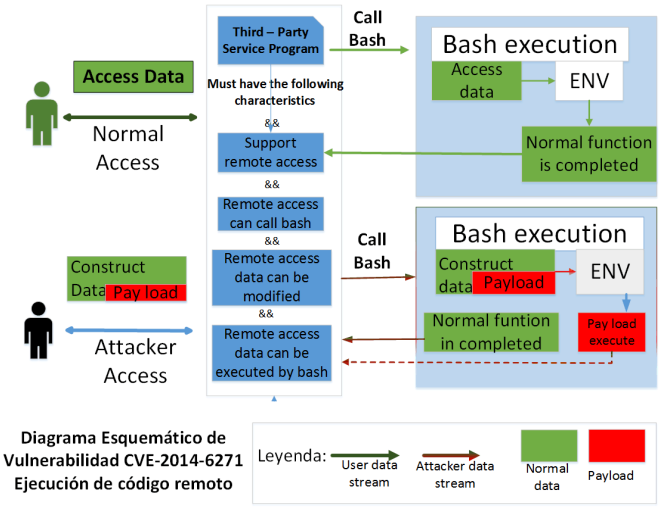

FIGURA 1. Vulnerabilidad ShellShock

Hoy en día existen algunas herramientas para realizar pruebas de penetración, una de ellas es Metasploit, la cual será utilizada para realizar la explotación de la vulnerabilidad en el Shell hacia un servidor Web, utilizando payload, para establecer una conexión remoto como la indicada en la figura 1.

III. CONFIGURACIÓN DEL EXPERIMENTO

A. *Diseño e Implementación topología de prueba*

Para realizar el experimento, se implementó un ambiente virtual experimental, utilizando VMware como hypervisor. A continuación, en la figura 2, se presenta la topología empleada:

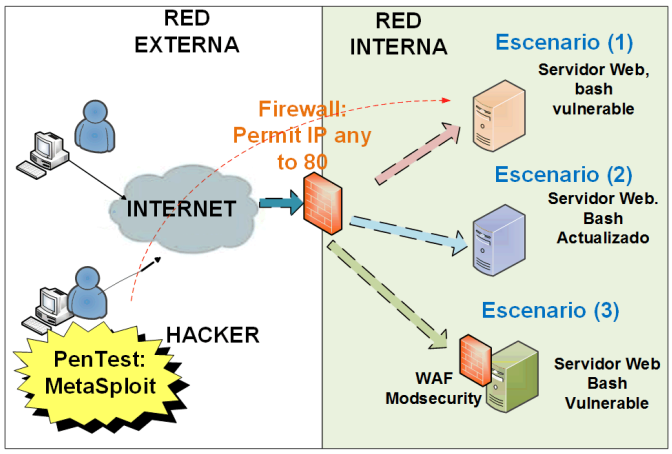

Figura 2. Ambiente Virtualizado de Experimentación

Como se aprecia en la figura 1, el ambiente virtualizado consta de los siguientes elementos: En la red interna o LAN: Un servidor Web, con Ubuntu 12, en el perímetro un firewall de capa 3 y en la red externa un equipo con la distribución de Linux Back Box.

El firewall de capa 3, está configurado de tal modo que permite el acceso desde usuarios de la red externa (PC-ATAQUE) a través del puerto 80 hacia el servidor Web (PC-VÍCTIMA) y también al puerto 22, para realizar actividades de administración.

Para el servidor Web se tienen tres escenarios, en todos se tiene el servidor web Apache, en el cual se habilitó CGI (Common Gateway Interface), para la ejecución de script CGI. En el primer escenario, se verificó que la versión del sistema operativo Ubuntu, tenga la vulnerabilidad en el Shell bash, *CVE*-2014-6271, para realizar la prueba de explotación. Para el segundo escenario, se tiene un servidor de similares características, pero con el parche para el Bash. El tercer escenario, es el mismo servidor que el primer escenario; no obstante, en este servidor se tiene instalado un servidor WAF.

En lo que respecta al equipo que realiza el ataque se utilizó la distribución de Linux Back Box, ya que cuenta con herramientas de ethical hacking preinstaladas; y, para la experimentación se utilizará la herramienta Metasploit.

B. Configuración de los componentes de experimentación

Como se indicó anteriormente, el firewall de capa 3, permite el acceso hacia el servidor Web por el puerto 80, esto se verifica accediendo al servidor desde un cliente utilizando un navegador web. Adicionalmente se habilita el CGI en el servidor Web, lo cual se comprueba ejecutando un script tipo CGI.

Seguido de esto, para el primer escenario, se realiza un escaneo de manera general a fin de identificar o corroborar que el servidor Web tenga la vulnerabilidad ShellSock, esto se lo realiza con el siguiente comando.

curl -A "() { :; }; echo; /bin/cat /etc/passwd" servidor-web/cgi-bin/script.sh > dat2.txt

Si el servidor tiene la vulnerabilidad, se ejecutará el comando "cat /etc/passwd" y dicha información se almacenará en el archivo dat2.txt.

Una vez verificada la vulnerabilidad, se procede a realizar la explotación, para lo cual se configura el Metasploit que tiene precargado un exploit para la vulnerabilidad *CVE*-2014-6271. En el exploit, se colocan parámetros tales como la dirección del servidor remoto - víctima, el directorio CGI con el acceso al script existente en servidor; adicionalmente, se configura el Payload, el mismo que permite establecer una conexión remota inversa entre el servidor víctima y el atacante; es decir, si se realiza el ataque satisfactoriamente, se inicia un túnel entre el PC atacante, desde donde se pueden ejecutar comandos de manera remota en el servidor Web.

C. Propuesta de Mitigación

A continuación se explican dos propuestas de mitigación para los ataques tipo ShellShock:

i) Actualización del bash del sistema operativo - Escenario 2. Los sistemas operativos tienen diferentes parches los mismos que sirven para corregir errores o agregar funcionalidades. En este sentido, existen parches para el bash, que permiten corregir la vulnerabilidad del bash evitando de esta manera los ataques del tipo ShellShock. Para verificar la mitigación propuesta, en el escenario 2, se realizará la actualización del bash del sistema operativo en el servidor víctima, después se procede a realizar un ataque tipo ShellShock con la herramienta MetaSploit, hacia el servidor Web.

ii) Implementación de un Web Application Firewall WAF – Escenario 3. Para mitigar el ataque tipo ShellShock hacia servidores web, se puede utilizar un Firewall a nivel de capa aplicación, a fin de bloquear los ataques de exploit. Para la experimentación se instaló un WAF basado en software libre denominado ModSecurity, el cual se integra con el servidor web vulnerable.

El resultado de estas propuestas de mitigación se expone a continuación en la sección IV

IV. Evaluación De Resultados Y Discusión

A. Escenarios y resultados de Experimentación.

Como se indicó anteriormente el objetivo de esta investigación es realizar la evaluación del ataque tipo ShellShock con un ambiente de experimentación virtualizado, considerando para esto la realización de una prueba de penetración aprovechando la vulnerabilidad del bash, para analizar la problemática de este tipo de ataque. A continuación se detallan los escenarios de experimentación:

Escenario (1): Como se indicó en el apartado 3.1, en el primer escenario, se verificó que el servidor víctima tiene la vulnerabilidad en el bash, con el comando:

env x='() { :;}; echo vulnerable' bash -c "echo Esta es una prueba"

El resultado de ese comando retorna:

vulnerable
Esta es un Prueba

Adicionalmente, se enviaron comandos básicos de Linux hacia el servidor web víctima, como por ejemplo: la

sentencia *curl -A "() { :; }; echo; /bin/ls" pc-víctima/cgi-bin/script.sh > dat.txt*

Con estas pruebas se pudo constatar que se puede obtener cualquier tipo de información, e incluso ejecutar comandos que puedan afectar a otros servidores tanto en la red interna como en la externa, utilizando como medio el servidor víctima, todo esto sin necesidad de utilizar herramientas avanzadas, lo cual demuestra la criticidad de esta vulnerabilidad.

Después se procedió a realizar la prueba de penetración, explotando la vulnerabilidad bash del servidor, utilizando Metasploit, obteniéndose como resultado el control del Shell remoto del servidor a través del puerto 80, utilizando el payload meterpreter. Cabe indicar que una vez que se tiene acceso al servidor, se puede ejecutar y tener acceso a determinados comandos y directorios, en función de los permisos con que se ejecute el CGI vulnerable, tal y como se indica en la figura 1.

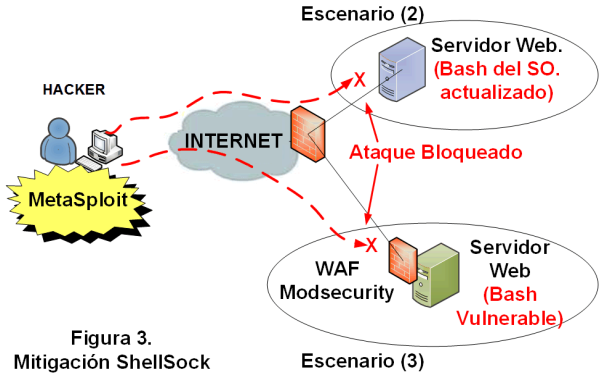

Figura 3.
Mitigación ShellSock

Escenario (2) Mitigación: En este escenario, se realizó la actualización del bash del sistema operativo Ubuntu, con los siguientes comandos "sudo apt-get update && sudo apt-get install bash"

Seguido de esto se verifica que el servidor víctima ya no tiene la vulnerabilidad en el bash, utilizando nuevamente el comando: *env x='() { :;}; echo vulnerable' bash -c "echo Esta es una Prueba"*

Ahora, cuando se ejecuta el comando, se obtiene como respuesta: *"Esta es una Prueba"*, sin la palabra *"vulnerable"*.

Para finalizar, se procede a realizar la prueba de penetración con Metasploit, constatando que ya no se tiene el acceso remoto con el exploit. Figura 3.

Escenario (3). Para este escenario se instaló un WAF en el servidor Web que tiene la vulnerabilidad en el Bash. El WAF utilizado es el Modsecurity, el mismo que tiene un conjunto de reglas que se pueden descargar desde su sitio web. Para verificar que el WAF esté habilitado en el servidor Ubuntu, se utilizó el siguiente comando: "sudo a2enmod mod-security"

Nuevamente se procedió a realizar la prueba de penetración para la vulnerabilidad ShellShock y se constató que no se puede establecer una conexión remota, usando el exploit de Metasploit, Figura 3. Adicionalmente, se revisaron los logs del WAF, en el cual se evidenció el reconocimiento del ataque (Apache-Handler: CGI-script), en el archivo modsec_audit.log

B. Discusión

Como se pudo apreciar en la prueba de penetración realizada, en el escenario (1) se tiene que la vulnerabilidad Shell Shock, es muy crítica, ya que básicamente se tiene acceso al Shell del servidor atacado, pudiendo acceder a información privilegiada éste, realizar cambios en las configuraciones de los archivos y principalmente convertirse en una maquina zombie, para producir ataques de DoS hacia otros servidores tanto internos como externos.

Se presentaron también dos formas de mitigación: una de ellas el mantener actualizado el sistema operativo Linux y el Shell bash; sin embargo, en la práctica existen empresas que tienen sistemas antiguos en los cuales no se pueda realizar dicha actualización. También se debe considerar que esta vulnerabilidad puede realizarse utilizando el protocolo SSH y con DHCP, esto en determinados equipos, como por ejemplo: routers y switch, que pueden estar sin soporte por parte de los fabricantes por lo que algunos de estos seguirán con la vulnerabilidad.

Como segunda alternativa de mitigación, un poco más compleja que la anterior, es la instalación de un servidor WAF, que para nuestro caso se integró al servidor Web, pero también se podría considerar el uso de WAF dedicados, los cuales servirían no solo para mitigar los ataques ShellShock, sino que también ayudaría a proteger al servidor de otro tipo de ataques.

V. TRABAJO RELACIONADO

La vulnerabilidad, hecha pública por el experto en seguridad Unix Stephane Chazelas, estuvo presente por más de 20 años y afecta a todas las versiones de bash hasta la 4.3

Robert Graham, experto en seguridad, considera que ShellShock pone en riesgo no sólo a los ordenadores y muchos de los servidores de la Web sino también en dispositivos o equipos que usan versiones modificadas de Linux como sistema operativo, como por ejemplo: las cámaras de vídeo IP podrían ser vulnerables ya que rara vez se actualizan.

En el trabajo realizado en [10]**¡Error! No se encuentra el rigen de la referencia.**, la evaluación del riesgo de vulnerabilidades en servidores Web, tanto para técnicos en seguridad como para usuarios no técnicos para escanear sus servidores Web y encontrar las implicaciones de las vulnerabilidades en sus sistemas. Esto mediante la construcción de una solución que realiza pruebas de concepto hacia las vulnerabilidades más críticas existentes, incluida la de ShellShock; no obstante, no se especifica el ambiente de experimentación.

En [7], Se realiza una categorización y análisis de los ataques de inyección de código, como por ejemplo SQL Injections, Cross Site Scritping y ShellSock, y se plantea una aplicación o herramienta experimental para detectar y explotar este tipo de ataques; no obstante, hoy en día ya se tienen herramientas similares que permiten mitigar este tipo de

ataques, aunque se debe tener en cuenta que estas tienen reglas que deben estar actualizándose constantemente a fin de mitigar nuevas vulnerabilidades.

También en [8], se realiza pruebas experimentales para indicar el impacto de los ataques tipo Heartbleed Bugs y los ataques tipo Bash Bug; sin embargo, en toda la experimentación se realizan pruebas únicamente de los ataques Heartbleed, quedando un vació en lo que se refiere a las pruebas con ShellShock.

En [9], se tiene que en el año 2015 los ataques a aplicaciones Web basados en ShellShock crecieron teniéndose cerca de 173 millones de ataques contra los clientes de Akamai. ShellShock también cambió significativamente el equilibrio de los ataques a través de http vs. https, en gran parte debido a que estos ataques se llevaron a cabo sobre todo a través de HTTPS. El error ShellShock fue anunciado por primera vez en septiembre de 2014 y recibió atención de los medios; como resultado de esto se espera que la mayoría de sistemas sean actualizados, por lo que el número de intentos de explotar esta vulnerabilidad vaya decreciendo. Por otro lado La proliferación de las redes robot construido a partir de dispositivos, como router, está causando un aumento de ShellShock mediante la explotación de las credenciales de inicio de sesión predeterminadas.

El National Vulnerability Database, recomienda como buena práctica, el tener un plan de mantenimiento, para actualizar parches para la vulnerabilidad Bash que están en constante actualización. Algunos creen que la solución todavía permite que ciertos caracteres que se inyecta en las versiones del bash vulnerables a través de variables de entorno especialmente diseñados. Los atacantes pueden crear nuevos métodos para eludir las restricciones de entorno y ejecutar comandos de Shell, métodos de derivación identificadas en los siguientes trabajos todavía funcionan tal como [5]: CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187.

En lo que se refiere a pruebas de penetración, en [11] se indica de manera generalizada los métodos para realizar estas pruebas para servidores Web utilizando Kali Linux. Aquí explican las formas de hacer reconocimiento de vulnerabilidades y diferentes ataques, incluidos SSL, XSS y otras técnicas de inyección de código, sin embargo, no se indican de manera específica las pruebas de explotación con ShellShock.

A diferencia de los trabajos antes mencionados, éste se centra principalmente en el ataque tipo ShellShock y se implementan dos mecanismos de mitigación, uno actualizando el bash del sistema operativo y otro mediante la utilización de un WAF.

VI. CONCLUSIONES

En el presente trabajo se pudo simular ataques hacia un servidor Web, utilizando herramientas de penetración, para explotar la vulnerabilidad ShellShock, de esta manera se constató la problemática que tiene este tipo de ataques, ya que se puede tomar el control de un equipo remotamente. A pesar de esto, se pudo ver que en la práctica existen principalmente dos opciones para mitigar esta vulnerabilidad en servidores Web, la una realizando actualizaciones al bash del sistema y otra instalando firewall a nivel de aplicación como los WAF, muchos de los cuales tienen reglas para detectar y bloquear esos ataques.

En lo que respecta a la experimentación futura, se podría utilizar los otros vectores de ataque que tiene ShellShock, SSH y DHCP, en dispositivos móviles o equipos de comunicación, para realizar ataques de DDoS. Una explotación de un servidor DHCP pueden configurar opciones y parámetros maliciosos, especialmente diseñados para que los clientes ejecuten ataques sin que se den cuenta afectando a otros clientes conectados en el mismo entorno de red.

REFERENCIAS

[1] «“ShellShock”, un peligro que se siente a distancia.,» 26 Noviembre 2014. [En línea]. Available: http://www.benditaess.com/projects/customer/etek/website/?p=45.

[2] J. Alborts, «#Shellshock, la grave vulnerabilidad en Bash – y todo lo que debes saber,» 26 Septiembre 2014. [En línea]. Available: http://www.welivesecurity.com/la-es/2014/09/26/shellshock-grave-vulnerabilidad-bash/.

[3] L. Lopresti, «Shellshock Bash Vulnerability.,» 25 Septiembre 2014. [En línea]. Available: http://www.securetia.com/shellshock-bash-vulnerability/.

[4] B. Bilbao, «Shellshock las cosas que debemos saber.,» 2 Octubre 2014. [En línea]. Available: http://sensorstechforum.com/es/shellshock-the-things-we-must-know/.

[5] NIST, «National Vulnerability Database. “Vulnerability Summary for CVE-2014-6271.” Last accessed,» 27 Septiembre 2014. [En línea]. Available: http://web.nvd.nist.gov/ view/vuln/detail?vulnId=CVE-2014-6271.2..

[6] Trend Micro Incorporated, «TrendLabs Security Intelligence Blog. “Heartbleed.”,» 27 Septiembre 2014. [En línea]. Available: http://blog.trendmicro.com/trendlabs-security-intelligence/?s=heartbleed&Submit=+Go+.

[7] Anastasios Stasinopoulos, «Commix: Detecting and exploiting command injection flaws. Department of Digital Systems, University of Piraeus,» [En línea].

[8] J. I. M. Secaira, «Niveles de Impacto: Heartbleed Bugs vs. Bash Bugs.,» Revista publicando, nº ISSN 1390-9304, pp. 65-77, 2(5). 2015.

[9] «Akamai’s [state of the internet] / security / Q3 2015 /,» 2015. [En línea]. Available: http://www.stateoftheinternet.com.

[10] B. Delamore, An Extensible Web Application Vulnerability Assessment and Testing Framework. Thesis University of Waikato,, 2015.

[11] J. A. Ansari, Web Penetration Testing with Kali Linux Second Edition.