

# **ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**



## **Facultad de Ingeniería en Electricidad y Computación Maestría en Seguridad Informática Aplicada**

**“ESQUEMA DE ANÁLISIS TEMPRANO DE  
VULNERABILIDADES DEL SERVIDOR DEL DEPARTAMENTO  
DE ADMISIÓN Y NIVELACIÓN DE LA UNIVERSIDAD DE SAN  
GREGORIO DE PORTOVIEJO”**

### **EXAMEN DE GRADO (COMPLEXIVO)**

PREVIO A LA OBTENCIÓN DEL GRADO DE:

### **MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA**

GONZALO ANTONIO ORDÓÑEZ RODRÍGUEZ

GUAYAQUIL – ECUADOR

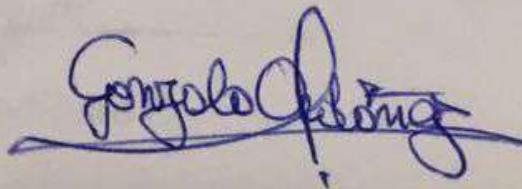
AÑO: 2016

## **AGRADECIMIENTO**

Agradezco a Dios por permitirme vivir y por todo lo que me ha dado, a mis padres por el apoyo que me dan y por ser mi ejemplo a seguir y por último y no menos importante a mi esposa y mi hijo por ser ellos la razón por la que me levanto día a día.

## DEDICATORIA

El presente proyecto de graduación se lo dedicó a mis padres, hermanos y sobre todo a mi esposa e hijo que son la razón por la cual me encuentro en esta etapa de mi vida.

A handwritten signature in blue ink, appearing to read 'Gonzalo P. Ponce', with a horizontal line underneath.

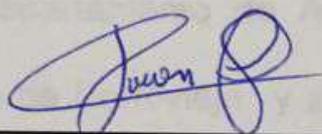
## TRIBUNAL DE SUSTENTACIÓN



---

Mgs. Lenin Freire

DIRECTOR DEL MSIA

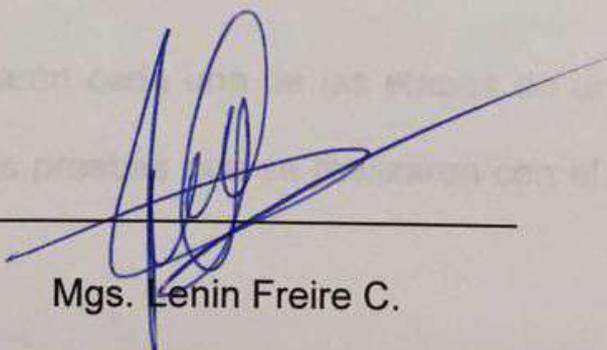


---

Mgs. Juan Carlos García

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



---

Mgs. Lenin Freire C.

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

## RESUMEN

En la actualidad la seguridad de la información es la parte primordial en todas las pequeñas, medianas y grandes empresas, con esto surge la necesidad de proteger dicha información en busca de siempre mantener la confidencialidad, la disponibilidad e integridad de la misma, por lo tanto el presente trabajo tiene como fin proponer la solución a las diferentes tipos de vulnerabilidades halladas al servidor del Departamento de Admisión y Nivelación de la Universidad de San Gregorio de Portoviejo y así tratar de mitigar que esta información caiga en manos de terceros.

En este trabajo se detallarán cada una de las etapas de un hacking ético y además también todas las pruebas que se realizaron con el análisis de cada una de éstas.

El análisis realizado se entregará a la Universidad de San Gregorio de Portoviejo para que el encargado de seguridad de dicho servidor aplique las

soluciones propuestas y así tratar de mitigar que la información caiga en manos de tercero o que la misma sea manipulada.

## ÍNDICE GENERAL

AGRADECIMIENTO .....	i
DEDICATORIA .....	ii
TRIBUNAL DE SUSTENTACIÓN .....	iii
RESUMEN .....	iv
ÍNDICE GENERAL.....	vi
ABREVIATURAS Y SIMBOLOGÍAS .....	ix
ÍNDICE DE FIGURAS.....	x
ÍNDICE DE TABLAS .....	xi
INTRODUCCIÓN .....	xii
CAPÍTULO 1.....	1
GENERALIDADES .....	1
1.1. ANTECEDENTES.....	1
1.2. DESCRIPCIÓN DEL PROBLEMA.....	2
1.3. SOLUCIÓN PROPUESTA.....	2
CAPÍTULO 2.....	4
ANÁLISIS DE VULNERABILIDADES A TRAVÉS DE LA IMPLEMENTACIÓN DE UN HACKING ÉTICO .....	4

2.1	DESCRIPCIÓN DEL ESCENARIO .....	4
2.2.	SISTEMAS OPERATIVOS Y HERRAMIENTAS A UTILIZAR .....	5
2.2.1	SISTEMAS OPERATIVOS .....	5
2.2.2	HERRAMIENTAS A UTILIZAR.....	5
2.3.	FASES DEL HACKING ÉTICO.....	6
2.3.1	FASE 1 RECONOCIMIENTO.....	6
2.3.1.1	OBJETIVOS .....	6
2.3.1.2	RESULTADOS .....	9
2.3.2	FASE 2 ESCANEO.....	9
2.3.2.1	OBJETIVOS .....	10
2.3.2.2	RESULTADOS .....	15
2.3.3	FASE 3 OBTENER ACCESO.....	16
2.3.3.1	OBJETIVOS .....	16
CAPÍTULO 3.....		22
ANÁLISIS DE RESULTADOS.....		22
3.1	ANÁLISIS DE LOS RESULTADOS DE LOS ATAQUES .....	22
3.2	PROPUESTA DE SOLUCIONES A LA VULNERABILIDADES ENCONTRADAS .....	23
CONCLUSIONES Y RECOMENDACIONES .....		24

BIBLIOGRAFÍA..... 26

## ABREVIATURAS Y SIMBOLOGÍAS

DoS	Denegación de Servicio
DAN – USGP	Departamento de Admisión y Nivelación de la Universidad de San Gregorio de Portoviejo
Host	Servidor
FIREWALL	Cortafuego diseñado para impedir el acceso no autorizado.
IP	Protocolo de Internet.
MSF	Metasploit Framework

## ÍNDICE DE FIGURAS

FIGURA 2. 1 IMAGEN DEL RESULTADO DEL RECONOCIMIENTO CON VISUAL IP TRACE 2009 .....	7
FIGURA 2. 2 PING A LA PÁGINA WEB DEL DAN - USGP .....	8
FIGURA 2. 3 RECONOCIMIENTO PASIVO A LA IP DEL HOST .....	8
FIGURA 2. 4 IMAGEN DEL ESCANEADO INTENSIVO AL HOST VICTIMA CON ZNMAP.....	11
FIGURA 2. 5 PUERTOS ABIERTOS CON LA HERRAMIENTA ZNMAP .....	12
FIGURA 2. 6 REPORTE DE RIESGO ALTO CON LA HERRAMIENTA OPENVAS.....	13
FIGURA 2. 7 REPORTE DE RIESGO MEDIO CON LA HERRAMIENTA OPENVAS.....	14
FIGURA 2. 8 IMAGEN DE ACCESO AL HOST REMOTO .....	17
FIGURA 2. 9 IMAGEN DEL SITIO WEB CON EL ATAQUE DoS.....	18
FIGURA 2. 10 DETENER EL SERVICIO IPTABLES .....	19
FIGURA 2. 11 IMAGEN DE LA LISTA DE REGLAS DEL IPTABLES.....	19
FIGURA 2. 12 EJECUCIÓN DEL SCRIPT SLOWLORIS.PL PARA PROVOCAR DoS.....	20
FIGURA 2. 13 SCRIPT SLOWLORIS.PL ENVIANDO MÚLTIPLES PAQUETES TCP .....	20
FIGURA 2. 14 IMAGEN DEL SITIO DEMORANDO EN RESPONDER.....	21

## ÍNDICE DE TABLAS

TABLA 1 RESULTADO DE ANÁLISIS CON ZNMAP .....	15
TABLA 2 RESULTADO DEL ANÁLISIS CON OPENVAS .....	15
TABLA 3 RESULTADO DEL ANÁLISIS CON MSF .....	21
TABLA 4 SOLUCIÓN PROPUESTAS POR LA HERRAMIENTA OPENVAS .....	23

## INTRODUCCIÓN

En el presente trabajo se detallan las etapas de un hacking ético como son el reconocimiento, el escaneo y obtener acceso para el análisis de vulnerabilidad del Departamento de Admisión y Nivelación de la Universidad San Gregorio de Portoviejo.

En las etapas de reconocimiento y escaneo se profundizará en conocer el origen físico del servidor, los puertos abiertos y servicios que estos escuchan.

De las etapas anteriores se recolectó la mayor parte de información para utilizar las herramientas adecuadas y obtener el acceso sin borrar las huellas para que las mismas sean revisadas por el encargado del manejo y seguridad del servidor, se plantearan las medidas de seguridad a tomar para tratar de disminuir los posibles ataques al servidor web del DAN – USGP.

# **CAPÍTULO 1**

## **GENERALIDADES**

### **1.1. ANTECEDENTES**

Se presentó la propuesta de realizar un análisis de vulnerabilidades de caja gris a la página web del Departamento de Admisión y Nivelación de la Universidad de San Gregorio de Portoviejo, la cual fue aceptada por el Rector de la Universidad, e inmediatamente se empezó a realizar el análisis de la misma.

El DAN tiene las siguientes funcionalidades planificar, organizar, inscribir e identificar a los futuros estudiantes; elaborar, administrar y calificar los test; publicar y responsabilizarse de los resultados [1]

## **1.2. DESCRIPCIÓN DEL PROBLEMA**

Con lo expuesto en el párrafo anterior podemos notar que este Departamento en su sitio web maneja información sensible de la universidad, para lo cual en este trabajo de tesis se plantea proponer la solución a las diferentes tipos de vulnerabilidades halladas y así tratar de mitigar que esta información caiga en manos de terceros.

## **1.3. SOLUCIÓN PROPUESTA**

En la actualidad las páginas web se han convertido en una herramienta muy importante en todas las empresas pequeñas, medianas y grandes, la educación no es una excepción ya que estas representan un medio para dar a conocer la misión, la visión, los alcances etc.

A través de la página web se pueden realizar consultas de notas, valor de matrículas, inicio de clases entre otras, se pueden subir apuntes, se realizan las inscripciones y se genera la orden de pago de la matrícula y pensiones.

Los docentes pueden establecer una comunicación dinámica y fluida con los estudiantes mediante los diferentes servicios desarrollados en las páginas como foros, chat en línea.

Entrando a la página web se conocen todos los servicios que Universidad presta en el campo de la educación, así toda la información está puesta allí para la comunidad de los usuarios.

Se planifica hacer un análisis externo de caja gris a la página web para detectar el sistema operativo y vulnerabilidades que puedan ser explotadas.

Para realizar este análisis se cumplió todas las etapas de un hacking ético las cuales son: reconocimiento, escaneo, obtener acceso, escribir informe y reportar.

El reporte que den como resultado los pasos antes realizado será proporcionado a la Universidad de San Gregorio de Puerto Viejo para que el personal encargado tome medidas cautelares y así tratar de mitigar que esta información sensible de los estudiantes sea manipulada o caiga en manos de terceros.

## **CAPÍTULO 2**

### **ANÁLISIS DE VULNERABILIDADES A TRAVÉS DE LA IMPLEMENTACIÓN DE UN HACKING ÉTICO**

#### **2.1 DESCRIPCIÓN DEL ESCENARIO**

Para realizar un hacking ético primero debemos de asegurarnos que el servidor al que queremos verificar las vulnerabilidades sea un hosting externo o uno propio de la Universidad San Gregorio de Portoviejo, para los cuales se utilizó una herramienta de traceroute visual, se contempló un solo escenario, el cual fue un análisis externo de caja gris el mismo que se realizó desde mi hogar. [2]

## **2.2. SISTEMAS OPERATIVOS Y HERRAMIENTAS A UTILIZAR**

### **2.2.1 SISTEMAS OPERATIVOS**

La ejecución del reconocimiento y escaneo se lo realizó en una máquina con sistema operativo Windows 10 de 64 bits, se tomó la decisión de virtualizar máquinas debido a que:

- Como se trata de un proyecto que realizó el aspirante previo a la obtención del título de Magister de Seguridad Informática, y en vista a la necesidad de tener varios sistemas operativos se optó por la virtualización usando el software gratuito Virtual Box, y así no tener la necesidad de montar un laboratorio con diferentes SO, y ahorrar gastos de hardware y software.

Los sistemas operativos que se utilizaron fueron:

- Windows XP
- Kali Linux

### **2.2.2 HERRAMIENTAS A UTILIZAR**

Las herramientas que se utilizaron fueron:

- Visual IP Trace 2009, es una herramienta comercial, para conocer la ubicación geográfica del objetivo que traza una dirección IP o el sitio web de nuevo a su origen.
- NMAP, es una herramienta que permite realizar explotación de una red o un host y auditoría de seguridad. Su versión principal era para Linux pero en la actualidad ya es multiplataforma. [3]
- OPENVAS, herramienta multiplataforma, para el análisis y gestión de las vulnerabilidades en la actualidad su interfaz gráfica ha mejorado.
- METASPLOIT, herramienta de explotación que proporciona información de vulnerabilidades y también realiza test de penetración [2]

## **2.3. FASES DEL HACKING ÉTICO**

### **2.3.1 FASE 1 RECONOCIMIENTO**

#### **2.3.1.1 OBJETIVOS**

- Verificar si el servidor al que se quiere realizar el escaneo de vulnerabilidades es propio de la Universidad o externo.

- Obtener la dirección ip del host en el cual se encuentra publicado el sitio web del Departamento de Admisión y Nivelación de la Universidad de San Gregorio de Portoviejo.

### Ejecución del software Visual IP Trace 2009

Con el propósito de obtener información de donde se encuentra ubicado el hosting del departamento de la Universidad de San Gregorio de Portoviejo, se ejecutó esta herramienta obteniendo como resultado que se encuentra localizado en Quito, Pichincha, Ecuador.

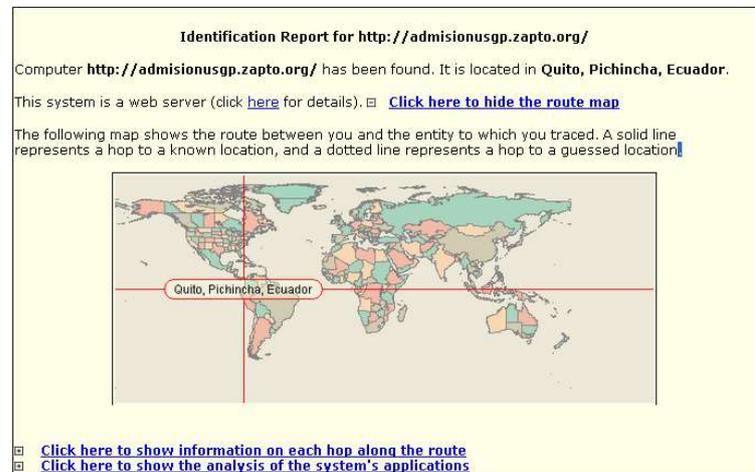


Figura 2. 1 Imagen del resultado del reconocimiento con Visual IP Trace 2009

Se realizó un ping al nombre del dominio para obtener la dirección IP del host la cual nos resolvió 186.42.197.151

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@kali:~# ping www.admisionusp.zapto.org
ping: unknown host www.admisionusp.zapto.org
root@kali:~# ping admisionusp.zapto.org
PING admisionusp.zapto.org (186.42.197.151) 56(84) bytes of data.
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=1 ttl=55 ti
me=136 ms
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=2 ttl=55 ti
me=91.0 ms
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=3 ttl=55 ti
me=213 ms
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=4 ttl=55 ti
me=159 ms
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=5 ttl=55 ti
me=133 ms
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=6 ttl=55 ti
me=243 ms
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=7 ttl=55 ti
me=247 ms
64 bytes from 151.pichincha.andinonet.net (186.42.197.151): icmp_req=8 ttl=55 ti

```

Figura 2. 2 Ping a la Página web del DAN - USGP

Con esta IP se realizó una búsqueda en google y como se puede observar en la siguiente imagen nos muestra como resultado que esta IP pública pertenece a Andinonet y que se encuentra ubicada en la provincia de El Oro, con esto podemos deducir que la página web se encuentra publicada en un servidor propio de la Universidad. [4]

IP address 186.42.197.151	
Address type	IPv4
Hostname	151.pichincha.andinonet.net
ISP	Universidad Particular San Gregorio De Portoviejo
Timezone	America/Guayaquil (UTC-5)
Local time	20:50:27
Country	Ecuador
State / Region	El Oro
City	San Gregorio
Coordinates	-3.35541, -80.284

Is the above data incorrect? Help us improve our database accuracy.  
Report a problem | © OpenStreetMap contributors

Figura 2. 3 Reconocimiento pasivo a la IP del host

### **2.3.1.2 RESULTADOS**

- Con la ejecución de la herramienta Visual IP Trace 2009 a la dirección web <http://admisionusgp.zapto.org/> se obtuvo la ubicación geográfica de nuestro objetivo la cual nos indica que se encuentra en Quito, Pichincha, Ecuador y que el proveedor que asigna la IP pública es Andinanet, con la IP podremos posteriormente en la etapa de escaneo ver puertos abiertos en este servidor.
- Existe conexión exitosa entre la máquina del atacante y el servidor utilizando la dirección ip obtenida anteriormente.

### **2.3.2 FASE 2 ESCANEO**

En la fase de escaneo vamos a identificar el sistema operativo y puertos abiertos con los respectivos servicios que se escuchan, en el servidor con IP 186.42.197.151, realizamos el escaneo de red en forma activa con la herramienta NMAP, para que nos permita conocer los puertos abiertos y servicios levantados en los mismos.

### **2.3.2.1 OBJETIVOS**

- Obtener los puertos abiertos en el servidor web y los servicios levantados.
- Obtener la versión del sistema operativo del servidor.

### **Ejecución de la herramienta ZNMAP**

Se realizó el escaneo con el comando de modo intensivo el cual nos dio como resultado:

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-01-11 22:46 ECT
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 22:46
Scanning 186.42.197.151 [4 ports]
Completed Ping Scan at 22:46, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:46
Completed Parallel DNS resolution of 1 host. at 22:46, 6.88s elapsed
Initiating SYN Stealth Scan at 22:46
Scanning 151.pichincha.andinanet.net (186.42.197.151) [1000 ports]
Discovered open port 80/tcp on 186.42.197.151
Discovered open port 22/tcp on 186.42.197.151
Completed SYN Stealth Scan at 22:46, 14.82s elapsed (1000 total ports)
Initiating Service scan at 22:46
Scanning 2 services on 151.pichincha.andinanet.net (186.42.197.151)
Completed Service scan at 22:47, 9.24s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 151.pichincha.andinanet.net (186.42.197.151)
Retrying OS detection (try #2) against 151.pichincha.andinanet.net (186.42.197.151)
Initiating Traceroute at 22:47
Completed Traceroute at 22:47, 0.02s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 22:47
Completed Parallel DNS resolution of 2 hosts. at 22:47, 6.55s elapsed
NSE: Script scanning 186.42.197.151.
Initiating NSE at 22:47
Completed NSE at 22:47, 3.67s elapsed
Nmap scan report for 151.pichincha.andinanet.net (186.42.197.151)
Host is up (0.0061s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 88:ce:59:73:eb:e3:0f:7a:el:f5:el:fe:1e:b3:19:fd (RSA)
|_ 256 63:a0:fd:15:22:eb:42:37:el:b4:5e:40:e8:30:40:f9 (ECDSA)
80/tcp    open  http     Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_ http-favicon: Unknown favicon MD5: D41D8CD98F00B204E9009999E6CF8427E
|_ http-generator: WordPress 4.3
|_ http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_ http-robots.txt: 1 disallowed entry
|_ /wp-admin/
|_ http-title: Departamento de Admisi\C3\xB3n y Nivelaci\C3\xB3n
443/tcp   closed https
Device type: general purpose|switch|specialized|VoIP phone
Running (JUST GUESSING): QEMU (91%), Bay Networks embedded (85%), NTI embedded (85%), Cabletron embedded (85%), Icom embedded (85%), Cisco embedded (85%), RAD Data Communications embedded (85%), Tyco embedded (85%)
OS CPE: cpe:/o:qemu:qemu cpe:/h:baynetworks:baystack_450 cpe:/h:cabletron:els100-24txm cpe:/h:icom:ic-7800 cpe:/h:cisco:catalyst_1900 cpe:/h:cisco:unified_ip_phone_7912
Aggressive OS guesses: QEMU user mode network gateway (91%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (85%), Bay Networks BayStack 450 switch (software version 4.2.0.16) (85%), NTI Environux-Mini environmental monitoring appliance (85%), Cabletron ELS100-24TXM Switch or Icom IC-7800 radio transceiver (85%), Cisco Catalyst 1900 switch or RAD IPMUX-1 TDM-over-IP multiplexer (85%), Tyco 24 Port SNMP Managed Switch (85%), Cisco IP Phone 7912-series (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=17 (Good luck!)
IP ID Sequence Generation: Incremental

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 1.88 ms 10.0.2.2
2 1.94 ms 151.pichincha.andinanet.net (186.42.197.151)

NSE: Script Post-scanning.
Initiating NSE at 22:47
Completed NSE at 22:47, 0.00s elapsed
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.15 seconds
Raw packets sent: 2060 (93.704KB) | Rcvd: 54 (4.144KB)
```

Figura 2. 4 Imagen del escaneo intensivo a la víctima con ZNMAP

## Escaneo de puertos y servicios abiertos en el servidor

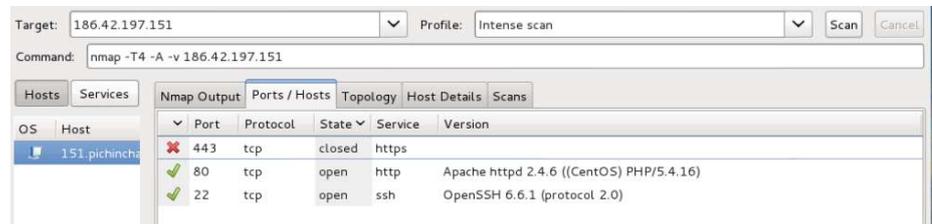


Figura 2. 5 Puertos abiertos con la herramienta ZNMAP

## Ejecución de la herramienta OPENVAS

Se realizó el escaneo con la herramienta OPENVAS el cual nos dio el siguiente resultado:

- Riesgo alto

High (CVSS: 8.5) NVT: OpenSSH Multiple Vulnerabilities
<p><b>Product detection result</b>  cpe:/a:openbsd:openssh:6.6.1  Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)</p>
<p><b>Summary</b>  This host is running OpenSSH and is prone to multiple vulnerabilities.   OID of test routine: 1.3.6.1.4.1.25623.1.0.806052</p>
<p><b>Vulnerability Detection Result</b>  Installed version: 6.6.1  Fixed version: 7.0</p>
<p><b>Impact</b>  Successful exploitation will allow an attacker to gain privileges, to conduct impersonation attacks, to conduct brute-force attacks or cause a denial of service.  Impact Level: Application</p>
<p><b>Solution</b>  Upgrade to OpenSSH 7.0 or later.  For updates refer to <a href="http://www.openssh.com">http://www.openssh.com</a></p>
<p><b>Vulnerability Insight</b>  Multiple flaws are due to:  - Use-after-free vulnerability in the 'mm_answer_pam_free_ctx' function in monitor.c in sshd.  - Vulnerability in 'kbdint_next_device' function in auth2-chall.c in sshd.  - vulnerability in the handler for the MONITOR_REQ_PAM_FREE_CTX request.</p>
<p><b>Vulnerability Detection Method</b>  Get the installed version with the help of detect NVT and check the version is vulnerable or not.  Details:OpenSSH Multiple Vulnerabilities  OID:1.3.6.1.4.1.25623.1.0.806052  Version used: \$Revision: 2058 \$</p>
<p><b>Product Detection Result</b> Product: cpe:/a:openbsd:openssh:6.6.1   Method: SSH Server type and version  OID: 1.3.6.1.4.1.25623.1.0.10267</p>
<p><b>References</b>  CVE: CVE-2015-6564, CVE-2015-6563, CVE-2015-5600  Other:  URL:<a href="http://seclists.org/fulldisclosure/2015/Aug/54">http://seclists.org/fulldisclosure/2015/Aug/54</a>  URL:<a href="http://openwall.com/lists/oss-security/2015/07/23/4">http://openwall.com/lists/oss-security/2015/07/23/4</a></p>

Figura 2. 6 Reporte de riesgo alto con la herramienta OPENVAS

- Riesgo medio

Medium (CVSS: 4.3) NVT: OpenSSH Security Bypass Vulnerability
<p><b>Product detection result</b>  cpe:/a:openbsd:openssh:6.6.1  Detected by SSH Server type and version (OID: 1.3.6.1.4.1.25623.1.0.10267)</p>
<p><b>Summary</b>  This host is running OpenSSH and is prone to security bypass vulnerability.</p> <p>OID of test routine: 1.3.6.1.4.1.25623.1.0.806049</p>
<p><b>Impact</b>  Successful exploitation will allow remote attackers to bypass intended access restrictions.  Impact Level: Application</p>
<p><b>Solution</b>  Upgrade to OpenSSH version 6.9 or later.  For updates refer to <a href="http://www.openssh.com">http://www.openssh.com</a></p>
<p><b>Vulnerability Insight</b>  The flaw is due to the refusal deadline was not checked within the x11_open_helper function.</p>
<p><b>Vulnerability Detection Method</b>  Get the installed version with the help of detect NVT and check the version is vulnerable or not.  Details:OpenSSH Security Bypass Vulnerability  OID:1.3.6.1.4.1.25623.1.0.806049  Version used: \$Revision: 2062 \$</p>
<p><b>Product Detection Result</b> Product: cpe:/a:openbsd:openssh:6.6.1  Method: SSH Server type and version  OID: 1.3.6.1.4.1.25623.1.0.10267</p>
<p><b>References</b>  CVE: CVE-2015-5352  Other:  URL:<a href="http://openwall.com/lists/oss-security/2015/07/01/10">http://openwall.com/lists/oss-security/2015/07/01/10</a></p>

Figura 2. 7 Reporte de riesgo medio con la herramienta OPENVAS

### 2.3.2.2 RESULTADOS

- Con la ejecución de la herramienta ZNMAP se pudo identificar :

TABLA 1 Resultado de análisis con ZNMAP

Puerto	Protocolo	Estado	Servicio	Versión
80	tcp	open	http	Apache httpd 2.4.6 (CentOS ) PHP /5.4.16)
22	tcp	open	ssh	OpenSSH 6.6.1 (protocol 2.0)

- Con la herramienta OPENVAS se pudo verificar que el servidor es vulnerable por el puerto 22 en el servicio openSSH:

TABLA 2 Resultado del análisis con OPENVAS

Riesgo	Impacto	Nivel	Solución
Alto	Permitirá al atacante obtener privilegios, para llevar a cabo: <ul style="list-style-type: none"> <li>• Ataques de suplantación</li> <li>• Ataques de fuerza bruta</li> <li>• Denegación de servicio</li> </ul>	Aplicación	Actualizar a OpenSSH 7.0 o posterior.

Medio	Permitirá al atacante <ul style="list-style-type: none"> <li>evitar las restricciones de acceso previstos.</li> </ul>	Aplicación	Actualizar a OpenSSH 6.9 o posterior.
-------	---	------------	---------------------------------------

### 2.3.3 FASE 3 OBTENER ACCESO

De acuerdo al resultado que se obtuvo en el punto anterior la fase de escaneo se pueden ver algunos tipos de ataques que se pueden realizar al DAN-USGP.

#### 2.3.3.1 OBJETIVOS

- Obtener acceso al host.
- Provocar DoS en un horario de la noche que se acordó con el encargado de la administración del host.

#### Ejecución de la herramienta MSF

Para poder explotar la vulnerabilidad del ataque de fuerza bruta se utilizó la herramienta MSF con el módulo ssh\_login, claro adaptando al diccionario de datos un conjunto de combinaciones de las abreviaturas del Departamento y las iniciales de la universidad, con el año.

[5]

Una vez identificado la clave del usuario root se procedió a ingresar al servidor como muestra la figura.

```

root@151:~# ssh root@186.42.197.151
root@186.42.197.151's password:
Last login: Sun Jan 10 21:22:48 2016 from 181.113.152.131
root@151 ~# ifconfig
eth2e8: flags=4096<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 186.42.197.151  netmask 255.255.255.0  broadcast 186.42.197.255
    inet6 fe80::eeaf:cbff:febf:1d19  prefixlen 64  scopeid 0x20<link>
    ether ec:80:18:1d:19  txqueuelen 1000  (Ethernet)
    RX packets 19081926  bytes 159469299 (1.8 GiB)
    RX errors 0  dropped 59732  overruns 0  frame 0
    TX packets 1623513  bytes 1268152976 (1.1 GiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=7344<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 0  (Local Loopback)
    RX packets 12258  bytes 2113283 (2.0 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 12258  bytes 2113283 (2.0 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=1999<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
    ether 52:54:00:09:19:45  txqueuelen 0  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
  
```

Figura 2. 8 Imagen de acceso al host remoto

Con el acceso al host remoto hemos explotado la vulnerabilidad de ataque de fuerza bruta utilizando el protocolo ssh.

Con la misma herramienta pero esta vez utilizando el módulo synflood se lo configuró para que la máquina del hacker envíe demasiadas solicitudes de SYN al host para que responda con el envío SYN-ACK, dejando al servidor a la espera del ACK final, provocando así un alto inicio de conexión que nunca son finalizados, por lo que consumirá recursos de forma desproporcionada.

En la siguiente imagen se muestra lentitud al momento de cargar la página, para obtener un resultado más preciso

es necesario que el atacante realice este tipo de ataques desde diferentes máquinas.

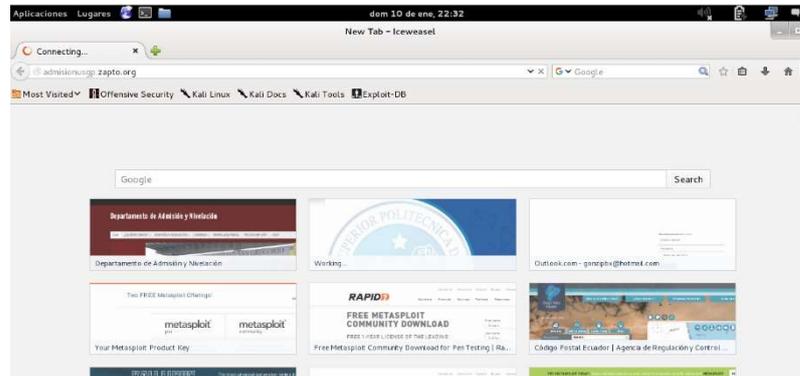


Figura 2. 9 Imagen del sitio web con el ataque DoS

Se accedió a la configuración del iptables de Linux del host víctima y ejecutando el comando `iptables -S` el cual nos permite desplegar la lista de reglas de la configuración del firewall manual, como muestra en la figura 2.11 podemos ver que este tiene configurado reglas para detener los ataques de denegación de servicio.

```

-A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i lo -j ACCEPT
-A FORWARD -j FORWARD_direct
-A FORWARD -j FORWARD_IN_ZONES_SOURCE
-A FORWARD -j FORWARD_IN_ZONES
-A FORWARD -j FORWARD_OUT_ZONES_SOURCE
-A FORWARD -j FORWARD_OUT_ZONES
-A FORWARD -p icmp -j ACCEPT
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
-A OUTPUT -o virbr0 -p udp -m udp --dport 68 -j ACCEPT
-A OUTPUT -j OUTPUT_direct
-A FORWARD_IN_ZONES -i enp2s0 -g FWDI_public
-A FORWARD_IN_ZONES -g FWDI_public
-A FORWARD_OUT_ZONES -o enp2s0 -g FWD0_public
-A FORWARD_OUT_ZONES -g FWD0_public
-A FWDI_public -j FWDI_public_log
-A FWDI_public -j FWDI_public_deny
-A FWDI_public -j FWDI_public_allow
-A FWD0_public -j FWD0_public_log
-A FWD0_public -j FWD0_public_deny
-A FWD0_public -j FWD0_public_allow
-A INPUT_ZONES -i enp2s0 -g IN_public
-A INPUT_ZONES -g IN_public
-A IN_public -j IN_public_log
-A IN_public -j IN_public_deny
-A IN_public -j IN_public_allow
-A IN_public_allow -p tcp -m tcp --dport 80 -m conntrack --ctstate NEW -j ACCEPT
-A IN_public_allow -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -j ACCEPT
-A IN_public_allow -p tcp -m tcp --dport 443 -m conntrack --ctstate NEW -j ACCEPT
root@151 sysconfig#

```

Figura 2. 10 Imagen de la lista de reglas del Iptables

Con el comando `service iptables stop`, procedemos a apagar el firewall manual

```

oot@kali:~# ssh root@186.42.197.151
root@186.42.197.151's password:
ast failed login: Mon Jan 11 23:20:26 ECT 2016 from 192.3.90.114 on ssh:notty
here were 10 failed login attempts since the last successful login.
ast login: Mon Jan 11 23:08:43 2016 from 186.47.191.91
root@151 ~)# services iptables status
ash: services: no se encontró la orden...
na orden similar es: 'service'
root@151 ~)# service iptables status
edirecting to /bin/systemctl status iptables.service
iptables.service - IPv4 firewall with iptables
Loaded: loaded (/usr/lib/systemd/system/iptables.service; disabled; vendor preset: disabled)
Active: inactive (dead)
root@151 ~)# service iptables stop
edirecting to /bin/systemctl stop iptables.service
root@151 ~)#

```

Figura 2. 11 Detener el servicio iptables

Una vez que hemos logrado detener el servicio podemos realizar una denegación de servicio utilizando un script realizado en el lenguaje perl `slowloris.pl` implementa una potente DoS enviando una gran cantidad de peticiones request a http y https, la manera es enviando cabeceras y más cabeceras al servidor de esta forma se fuerza a tener abiertas las conexiones activas y en algún momento el



De la misma manera que el primer ataque de DoS el servidor web no dejó de funcionar solo respondía cada vez más lento.

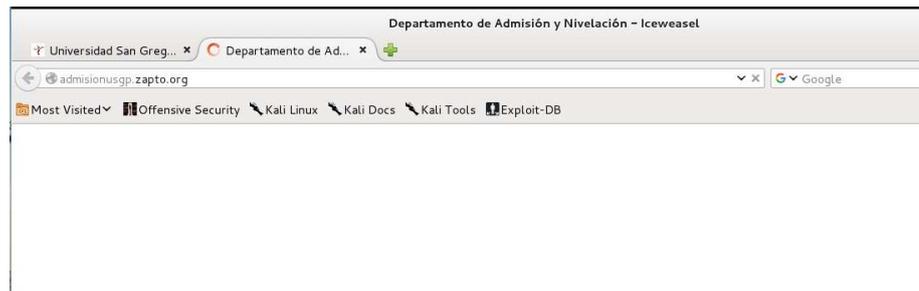


Figura 2. 14 Imagen del sitio demorando en responder.

Al final de realizar esta prueba se detuvo el script y se levantó nuevamente el servicio de iptables.

### 2.3.3.2 RESULTADOS

- Con la ejecución de la herramienta MSF se obtuvo lo siguiente:

TABLA 3 Resultado del análisis con MSF

Módulo	Vulnerabilidad	Estado
ssh_login	Ataques de fuerza bruta	Exitosa
synflood	Denegación de servicio	Exitosa

## **CAPÍTULO 3**

### **ANÁLISIS DE RESULTADOS**

#### **3.1 ANÁLISIS DE LOS RESULTADOS DE LOS ATAQUES**

- El ataque de fuerza bruta fue exitoso y con el mismo se puedo obtener un control total en el servidor web de aplicaciones
- La DoS que se realizó en este hacking ético solo provocó que el servidor se demore más en responder, esto se debe a que el aspirante al título realizó este ataque desde una computadora de hogar con la siguientes características core i5 y con una máquina virtual de Kali con solo 2 gb de memoria ran y además que la conexión a internet era vía wifi.

- No se realizó el borrado de huellas para que precisamente el encargado de la administración del servidor pueda evidenciar el ingreso a dicho servidor.

### 3.2 PROPUESTA DE SOLUCIONES A LA VULNERABILIDADES ENCONTRADAS

Las herramientas que se utilizaron para el análisis de las vulnerabilidades nos proporcionaron la solución a cada una de las vulnerabilidades encontradas las cuales fueron:

TABLA 4 Solución propuestas por la herramienta OPENVAS

<b>Vulnerabilidad</b>	<b>Servicio Actual</b>	<b>Solución</b>
<ul style="list-style-type: none"><li>• Ataques de fuerza bruta</li><li>• Denegación de servicio</li></ul>	OpenSSH 6.6.1	Actualizar a OpenSSH 7.0 o posterior.

## **CONCLUSIONES Y RECOMENDACIONES**

### **CONCLUSIONES**

1. El servidor del DAN – USGP se encuentra vulnerable a los ataques enumerados en el presente trabajo.
2. El personal encargado de la administración del servidor debe de estar en continua capacitación para sustentar cualquier amenaza en el futuro
3. La herramienta OpenSSH se encuentra desactualizada y la misma puede verse afectada por un ataque de fuerza bruta.

## RECOMENDACIONES

1. Se recomienda realizar un hardening a todos los servidores que son expuesto a la red pública y privada.
2. Se recomienda tener habilitada las actualización automática del SO para que los parches corrijan cualquier hueco de seguridad.
3. Se recomienda la adquisición de antivirus pagados debido a que estos tienen soporte y una correcta actualización
4. Establecer políticas de seguridad para que las contraseñas sean más robustas con el uso adecuado de caracteres especiales, letras, números y una longitud mínima de 10 caracteres.
5. Adquisición de un firewall y ubicación de los servidores publicados en una red DMZ, para impedir que un hacker pueda entrar a la red local y afectar a otros equipos y servidores
6. El administrador del servidor debe realizar de manera diaria la revisión de los logs del servidor.

## BIBLIOGRAFÍA

- [1] <http://admisionusgp.zapto.org/>.
- [2] K. Astudillo, Hacking Ético 101, Guayaquil, 2013.
- [3] <https://nmap.org/man/es/>.
- [4] <https://db-ip.com/186.42.197.151>.
- [5] <https://www.offensive-security.com/metasploit-unleashed/scanner-ssh-auxiliary-modules>.



USGP-R-0013-2016

UNIVERSIDAD  
**SAN GREGORIO**  
DE PORTOVIEJO

Portoviejo, 07 de enero de 2016

Ingeniero  
Sergio Flores  
**RECTOR DE LA UNIVERSIDAD POLITÉCNICA DEL LITORAL**  
Guayaquil.-

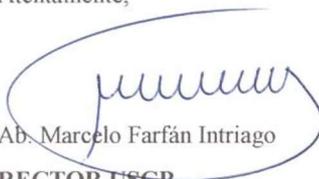
De mi consideración:

Por medio de la presente me permito comunicar a usted, que el Ingeniero Gonzalo Ordóñez, estudiante de una Maestría en Seguridad Informática V promoción de la ESPOL, desarrollará su trabajo de tesis denominado “Esquema de análisis temprano de vulnerabilidades del servidor del departamento de Admisión y Nivelación de la Universidad San Gregorio de Portoviejo”, como requisito previo a la obtención del título de Magister en Seguridad Informática Aplicada.

Particular que comunico a usted para los fines consiguientes.

Con sentimientos de consideración y estima.

Atentamente,

  
Ab. Marcelo Farfán Intriago

**RECTOR USGP**

*Pepi*

