Análisis de vulnerabilidades y riesgos

Este informe presenta el resultado de un análisis de vulnerabilidades realizado sobre un entorno controlado, con el objetivo de identificar brechas de seguridad, evaluar riesgos asociados y proponer controles de mitigación basados en las buenas prácticas de la norma ISO/IEC 27001.

La infraestructura de red de la organización infranet está constituida por dos servidores; uno de ellos destinado al alojamiento de sitios web y otro orientado a la prestación de servicios de correo electrónico donde encuentra configurado un firewall ASA que filtra el tráfico de red hacia los servidores y un servicio de en la nube.

La infraestructura de red implementa una segmentación lógica mediante VLANs, asignando redes independientes para las áreas de Administración, Contabilidad, Ventas y Logística, con el fin de optimizar el rendimiento, la seguridad y el control del tráfico interno. En la Ilustración 1 se detalla la topología de red y la configuración de la interfaz trunking, permitiendo la transmisión simultánea de múltiples VLANs a través de un único enlace físico, garantizando la correcta interconexión entre los distintos segmentos de red.

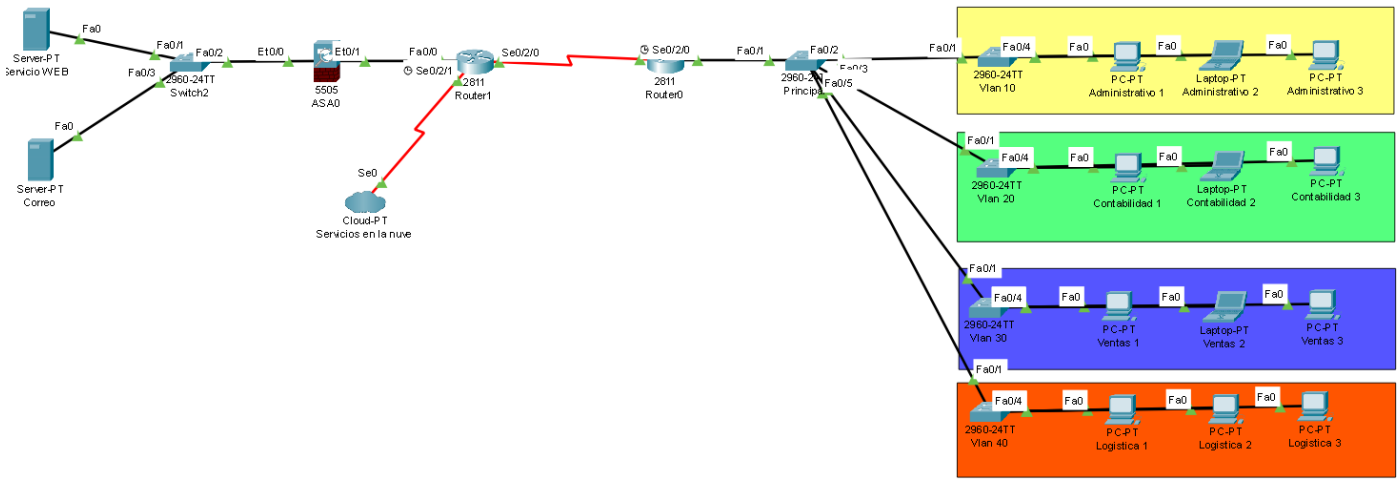

Ilustración 1. Infraestructura de red de infranet.

Identificada la segmentación y distribución de la red de la organización, Se realiza un escaneo de puertos para determinar que posibles vulnerabilidades podrían presentarse en los sistemas que componen la infraestructura de red, donde se identificó la apertura de dos puertos en el servidor web que se evidencia en la ilustración 2. Es importante analizar estos puertos para saber el nivel de riesgo que presenta.

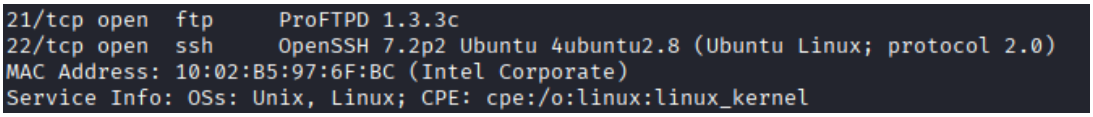

Ilustración 2.Puertos abiertos del servidor WEB.

Realizando una investigación a profundidad de los servicios que están presentes y en ejecución en los dos puertos 21 y 22, se identificó el servicio de ProFTPD y OpenSSH, Estos dos servicios de acuerdo a la base de datos de CVE, se identificó las siguientes vulnerabilidades descritas en la tabla 1.

Servicio	**Vulnerabilidades**	**Descripción**
ProFTPD	**CVE-2010-3867**	**Permite a usuarios autenticados remotamente crear, borrar, modificar y crear enlaces.**
OpenSSH	**CVE-2016-3115**	**Permite a usuarios remotos autenticarse eludiendo las restricciones de comando de Shell previstas.**

Tabla 1.. Identificación de las vulnerabilidades.

Para este caso se realiza una prueba de penetración para saber hasta donde es capaz un atacante acceder al sistema, para ello se identificó que la dirección ip del servidor es 192.168.1.17.

Utilizando varias herramientas que un atacante puede utilizar se logro acceder al servicio ftp del servidor, este acceso se puede evidenciar en la ilustración 2, donde se consigue acceder a diferentes directorios que están alojados en el servidor web.

```
listening on [any] 1234 ...
[+] Sending payload
[+] Activating the backdoor

connect to [192.168.1.13] from (UNKNOWN) [192.168.1.17] 36644
/bin/sh: 0: can't access tty; job control turned off
# ls -la
total 108
drwxr-xr-x  24 root root  4096 Oct 14 14:33 .
drwxr-xr-x  24 root root  4096 Oct 14 14:33 ..
drwxr-xr-x   2 root root  4096 Oct 14 14:29 bin
drwxr-xr-x   3 root root  4096 Oct 14 16:48 boot
drwxrwxr-x   2 root root  4096 Nov 14  2017 cdrom
drwxr-xr-x  19 root root  3960 Oct 14 14:30 dev
drwxr-xr-x 133 root root 12288 Oct 14 16:48 etc
drwxr-xr-x   3 root root  4096 Nov 14  2017 home
lrwxrwxrwx   1 root root    34 Oct 14 14:33 initrd.img → boot/initrd.img-4.15.0-142-generic
lrwxrwxrwx   1 root root    33 Oct 14 14:33 initrd.img.old → boot/initrd.img-4.15.0-99-generic
drwxr-xr-x  22 root root  4096 Nov 14  2017 lib
drwxr-xr-x   2 root root  4096 Oct 14 14:28 lib64
drwx------   2 root root 16384 Nov 14  2017 lost+found
drwxr-xr-x   3 root root  4096 Nov 16  2017 media
drwxr-xr-x   2 root root  4096 Aug  1  2017 mnt
drwxr-xr-x   2 root root  4096 Aug  1  2017 opt
dr-xr-xr-x 145 root root     0 Oct 14 12:50 proc
drwx------   5 root root  4096 Nov 14  2017 root
drwxr-xr-x  29 root root  1060 Oct 14 16:47 run
drwxr-xr-x   2 root root 12288 Oct 14 14:32 sbin
drwxr-xr-x   2 root root  4096 May 18  2020 snap
drwxr-xr-x   2 root root  4096 Aug  1  2017 srv
dr-xr-xr-x  13 root root     0 Oct 14 12:50 sys
drwxrwxrwt  10 root root  4096 Oct 14 18:17 tmp
drwxr-xr-x  11 root root  4096 Aug  1  2017 usr
drwxr-xr-x  15 root root  4096 Nov 16  2017 var
lrwxrwxrwx   1 root root    31 Oct 14 14:33 vmlinuz → boot/vmlinuz-4.15.0-142-generic
lrwxrwxrwx   1 root root    30 Oct 14 14:33 vmlinuz.old → boot/vmlinuz-4.15.0-99-generic
#
```

Ilustración 3. Archivos alojados en el servidor web.

Indagando mas en los directorios se encontró un directorio /etc/passwd, donde se valido varios usuarios y servicios que estaban en este directorio, para esta ocasión se puede validar esta información en la ilustración 4:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
```

Ilustración 4. Archivos y datos del directorio etc de la maquina víctima.

De acuerdo a la ilustración 4, se identifica un usuario particular llamado marlinspike, en el archivo passwd y que se puede comprobar en la ilustración 5, hasta el momento solo se identifica un usuario creado en el servidor web, lo que nos permite identificar que tiene acceso de privilegiado en el servidor.

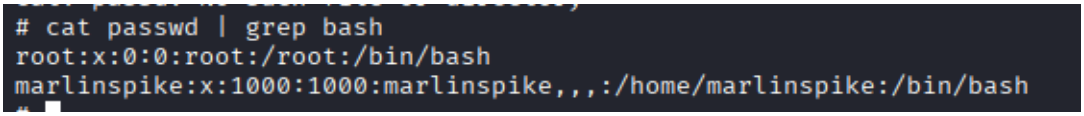

Ilustración 5. Usuario del servidor web.

Conforme la ilustración 5, se realizará un ataque de fuerza bruta para identificar la posible contraseña del usuario marlinspike. Para este caso usando herramientas de hacking, se valida con éxito la autenticación de usuario y contraseña, visualizándose la evidencia en la ilustración 6.

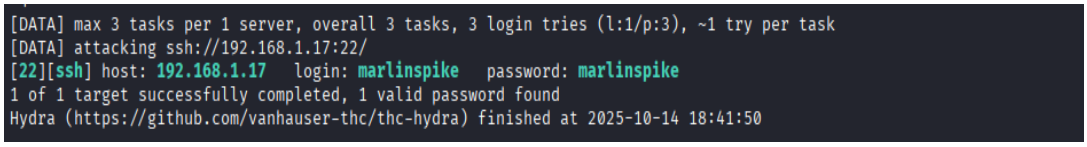

Ilustración 6. Contraseña de la maquina victima

Teniendo la evaluación de penetración en el entorno vulnerable “servidor web”, se plantea las siguientes amenazas principales que afectan gravemente la continuidad del negocio donde se describirán en la siguiente tabla 2:

Tipo	Descripción
Ransomware	**Se pude cifrar todos los volúmenes de datos almacenados en el server, comprometiendo la disponibilidad.**
Fuga de datos	**Se puede inspeccionar la base de datos donde se descarga, cambia y elimina datos comprometiendo la integridad y confidencialidad.**
Contraseñas débiles	**Se verifica conforme el test de penetración, que las contraseñas son demasiado débiles y muy comunes para un atacante.**

Tabla 2.Identificación de amenazas.

Amenazas conforme las vulnerabilidades detectadas

Amenazas	Vulnerabilidades	impacto	Justificación
Ransomware	**CVE-2016-3115**	**Alto**	**La falta de parches facilita la explotación de esta vulnerabilidad y el cifrado de los datos, afectando la continuidad del negocio.**
Fuga de datos	**CVE-2010-3867**	**Alto**	**La falta de parche permite explotar la vulnerabilidad, afectando la reputación de la organización**
Contraseñas débiles	**CVE-2016-3115 CVE-2010-3867**	**Alto**	**No se tiene contraseñas fuertes que cumpla con los 8 caracteres alfanuméricos.**

Tabla 3.Relación entre las amenazas conforme las vulnerabilidades encontradas.

Conforme el análisis de amenazas principales en el entorno tecnológico, se asocia las vulnerabilidades que están presentes en el servidor web y que un atacante podría aprovechar y se describen en la tabla 3.

Para mitigar estas amenazas que tiene el entorno tecnológico y así reducir el tiempo en que esas amenazas se materialicen y generen un riesgo, se plantea la siguiente tablas 4, donde se plantea controles para mitigar las amenazas.

Tipo	Control	Descripción
Técnico	**Prevención de fuga de datos**	**Se debe aplicar medidas correctivas para la prevención de fuga de datos en el sistema.**

Técnico	**Protección contra código malicioso**	**Se debe crear la política para gestionar la protección contra código malicioso, y la actualización de parches de seguridad a la versión más reciente y estable.**
Técnico	**Instalación de software en producción**	**Se crear la política para instalación y actualización de software en los sistemas de información.**
Técnico	**Gestión de vulnerabilidades técnicas**	**Se debe crear la política de gestión de vulnerabilidades para realizar y evaluar periódicamente la evaluación de vulnerabilidades para la mejora continua del sistema de gestión de seguridad de la información.**
Organizacional	**Autenticación de la información, gestión de identidad, autorización de acceso y eliminación de la información**	**Se debe realizar el debido cambio de las contraseñas en los servicios alojados en el servidor conforme la política establecida en la organización.**
Administrativos	**Política de seguridad de la información**	**Actualizar la política y agregar nuevas políticas conforme los controles establecidos anteriormente.**

Tabla 4.Controles de mitigación.

Finalmente se desarrolla la matriz de riesgo que permite evaluar el nivel de riesgo si se materializan las amenazas en el entorno tecnológico de la organización.

Riesgo	Probabilidad	Impacto	Nivel de riesgo
Ransomware	**Alto**	**Alto**	**Alto**
Fuga de datos	**Alto**	**Alto**	**Alto**
Contraseñas débiles	**Medio**	**Alto**	**Alto**

Tabla 5.Matriz de Riesgos.

Evaluando la Tabla 5, se concluye que es necesario implementar los controles lo antes posible para reducir la probabilidad de impacto y mitigar el nivel de riesgo, fortaleciendo así la postura de seguridad de la organización. Estas acciones contribuyen a disminuir el vector de ataque y garantizar el cumplimiento de los principios de confidencialidad, integridad y disponibilidad de la información.