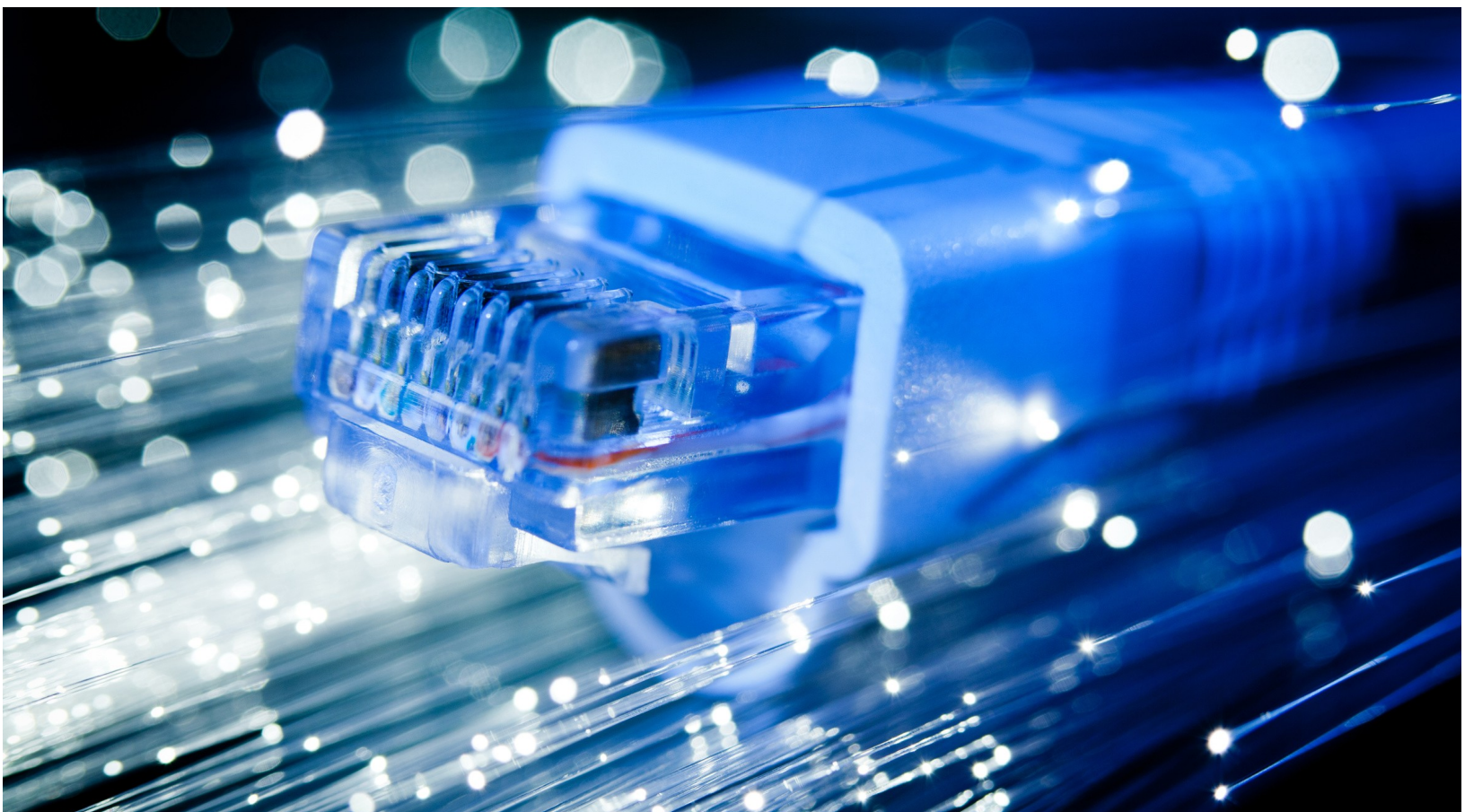


Reporte de pruebas de penetración



Este documento expone las vulnerabilidades encontradas, analizadas y/o explotadas, durante las pruebas realizadas al servidor *truerandom.bid*

Versión 0.1

Elaboración: Ferrusca Ortiz Jorge Luis

Resumen ejecutivo

Objetivo.....	
Introducción	
Descripción de niveles de seguridad.....	

Reporte

Escaneo de puertos	
Escaneo de servicios.....	
FTP.....	
MySQL.....	
Wordpress.....	
Conclusiones.....	

Objetivo

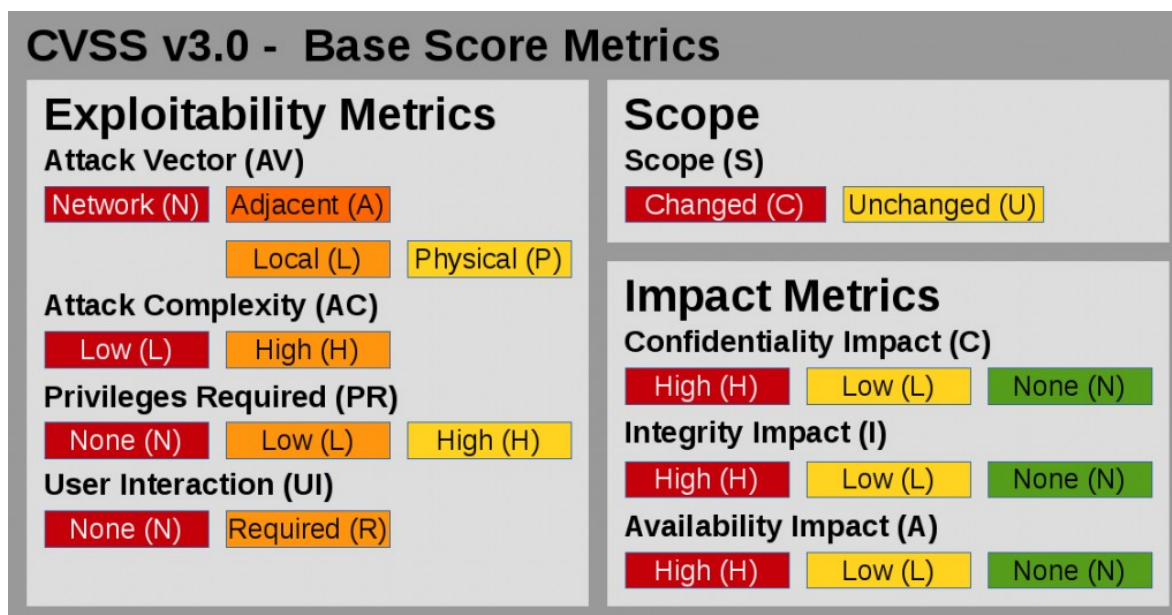
Este documento tiene como objeto, mostrar un panorama general acerca de los servicios que provee el sistema, en lo que respecta a sus vulnerabilidades y posibles soluciones, esto con la finalidad de proveer un enfoque en el que el cliente pueda mitigar las diversas vulnerabilidades que se enlistan.

Introducción

Para la realización de las pruebas de penetración, se utilizaron diversas herramientas vistas a lo largo del curso, desde la fase de reconocimiento y escaneo, hasta la explotación de las vulnerabilidades.

Descripción de niveles de seguridad

En las siguientes páginas se enlistarán los servicios que tienen vulnerabilidad, todos medidos a través de un puntaje base, que se encuentra definido en el Documento de Especificación CVSS 3.0. Dicho puntaje es calculado a través de una serie de métricas, las cuales son:



Las cuales se clasifican de la siguiente manera:

Rating	CVSS Score
None	0.0
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

Escaneo de puertos y servicios

Descripción

Dentro de esta fase, para iniciar solo se necesitaba la dirección IP del servidor, la cual se obtuvo y se empezaron a escanear los puertos, de los cuales se obtuvo la siguiente información:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-03-26 14:41 CST
Nmap scan report for 167.99.232.57
Host is up (0.077s latency).
Not shown: 90 closed ports
PORT      STATE      SERVICE      VERSION
21/tcp    open       ftp          vsftpd 2.0.8 or later
22/tcp    open       ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open       http         Apache httpd 2.4.29 ((Ubuntu))
135/tcp    filtered  msrpc
139/tcp    filtered  netbios-ssn
445/tcp    filtered  microsoft-ds
1025/tcp   filtered  NFS-or-IIS
3306/tcp   open       mysql        MySQL 5.7.25-0ubuntu0.18.04.2
8009/tcp   open       ajp13        Apache Jserv (Protocol v1.3)
8080/tcp   open       http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Con esta información, se comenzaron a tratar de obtener vulnerabilidades para los servicios una vez que conocidos

FTP

Descripción

FTP refiere al Protocolo de Transferencia de Archivos, uno de los protocolos dentro del protocolo TCP/IP. FTP hace posible transferir archivos de un host a otro.

Anonymous FTP es llamado así debido a que no se necesita tener identidad para acceder a los archivos, lo que permite acceder al servidor FTP con un login común (como “ftp” o “anonymous”) y cualquier password.

En este caso, utilizamos dicho usuario por defecto, para entrar al servidor:

```
10040 ○ ftp 167.99.232.57
Connected to 167.99.232.57.
220 Pistas en raiz del puerto 80
Name (167.99.232.57:chicoterry): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
```

Con eso se obtuvo acceso, sin embargo y algo que se pudo aprovechar fue el dar de alta una llave pública en `authorized_keys` para obtener acceso ahora desde Secure shell.

Solución

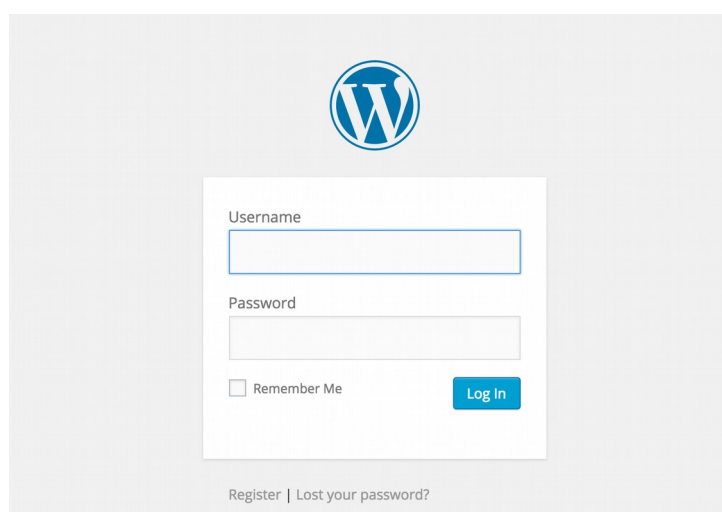
Se podría desactivar el acceso anónimo para evitar algún mal uso, o bien activar un login con una contraseña lo suficientemente fuerte para aquellos usuarios que tengan que acceder al servidor.

Wordpress

Descripción

WordPress es un sistema de gestión de contenido (CMS) de código abierto con licencia GPLv2.

Se cuenta con una pantalla de login similar a la siguiente, mediante la cual podemos acceder al panel de control de nuestro sistema

The image shows the WordPress login interface. At the top center is the WordPress logo, a blue 'W' inside a circle. Below the logo is a white rectangular box containing the login form. The form has two input fields: 'Username' and 'Password'. Below the 'Password' field is a checkbox labeled 'Remember Me'. To the right of the checkbox is a blue button with the text 'Log In'. At the bottom of the white box, there are two links: 'Register' and 'Lost your password?'. The entire form is centered on a light gray background.

El primer enfoque que se tuvo, fue de intentar acceder mediante contraseñas y usuarios conocidos, para ello existen diversas herramientas que nos pueden ayudar en ataques de diccionario, en este caso mediante Burp y archivos de contraseñas como rockyou.txt de kali por ejemplo, se intentan obtener las credenciales correctas

Results	Target	Positions	Payloads	Options				
Filter: Showing all items								
Request	Payload1	Payload2	Status	Error	Timeout	Length	Com	
67	root	pepper	200	<input type="checkbox"/>	<input type="checkbox"/>	7672		
37	root	trustno1	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
97	root	austin	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
132	root	jackson	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
142	root	peanut	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
209	root	fender	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
227	root	enter	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
229	root	chris	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
331	root	gemini	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
362	root	monica	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
363	root	elephant	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
424	root	nissan	200	<input type="checkbox"/>	<input type="checkbox"/>	5717		
4	root	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	5716		
8	root	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	5716		

Una vez teniendo usuario y contraseña, se accede directamente a la administración del sitio.

Solución

Existen diversos mecanismos que se pueden implementar, tales como:

- Habilitar el login desde direcciones IP específicas
- Limitar el número de intento de accesos

Sin embargo la más importante es requerir contraseñas lo suficientemente fuertes, y esto se puede lograr estableciendo, por ejemplo, contraseñas de longitud mayor a 7 caracteres, combinando upper y lowercase, caracteres alfanuméricos y al menos 1 símbolo

MySQL

Descripción

MySQL es un sistema gestor de base de datos relacional (RDBMS) de código abierto, MySQL es altamente asociado con las aplicaciones basadas en la web.

Mediante un script de enumeración de nmap es eventualmente posible obtener listas de usuarios para el manejador, por lo que se obtienen algunos resultados al ejecutar dicho script

```
10026 nmap --script=mysql-enum.nse 167.99.232.57

Starting Nmap 7.01 ( https://nmap.org ) at 2019-03-26 13:03 CST
Nmap scan report for 167.99.232.57
Host is up (0.081s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
1025/tcp  filtered NFS-or-IIS
3306/tcp  open  mysql

| mysql-enum:
| Valid usernames:
|   admin:<empty> - Valid credentials
|   root:<empty> - Valid credentials
|   webadmin:<empty> - Valid credentials
|   sysadmin:<empty> - Valid credentials
|   netadmin:<empty> - Valid credentials
|   test:<empty> - Valid credentials
|   user:<empty> - Valid credentials
|   web:<empty> - Valid credentials
|   administrator:<empty> - Valid credentials
```

Al emplear nombres conocidos, se puede facilitar la intrusión ya que ahora solo dependemos de la contraseña, para ello se pueden usar diversas herramientas, una de ellas vía metasploit, (scanner/mysql/mysql_login) mediante la cual nos intentamos autenticar:

```
ES))
[-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: root:123456789 (Incorrect: Access denied for user 'root'@'132.248.52.100')
d: YES))
[-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: root:password (Incorrect: Access denied for user 'root'@'132.248.52.100')
: YES))
[-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: root:iloveyou (Incorrect: Access denied for user 'root'@'132.248.52.100')
: YES))
[-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: root:princess (Incorrect: Access denied for user 'root'@'132.248.52.100')
: YES))
[-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: root:1234567 (Incorrect: Access denied for user 'root'@'132.248.52.100')
YES))
[-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: root:rockyou (Incorrect: Access denied for user 'root'@'132.248.52.100')
YES))
```

Nuevamente sabemos que el hecho de utilizar contraseñas comunes, abre la posibilidad de poder ingresar de manera mucho más rápida y sencilla a los servicios que tenemos.

Solución

Al igual que con wordpress, esto se puede solucionar utilizando contraseñas lo suficientemente fuertes, restringiendo el acceso a MySQL a determinadas direcciones IP si es en verdad necesario, o de ser posible, restringir el acceso únicamente de manera local.

Referencias

RFC 1635. *How to use anonymous FTP* <https://tools.ietf.org/html/rfc1635>

Nmap.org. *File mysql-enum*

First. Improving Security Together. *Common Vulnerability Scoring System Version 3.0 Calculator*