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

Reporte detallado

Objetivo

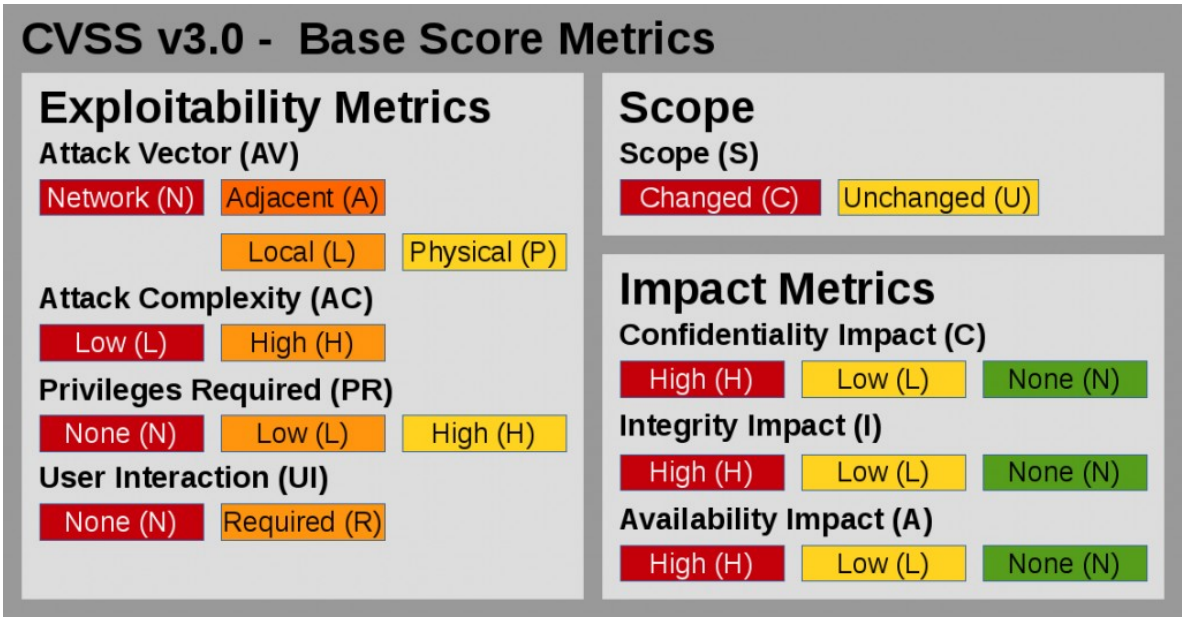
Este documento tiene como objeto, mostrar un panorama general acerca de los servicios que provee el sistema, en lo que respecta a sus vulnerabilidades y posibles soluciones, esto con la finalidad de proveer un enfoque en el que el cliente pueda mitigar las diversas vulnerabilidades que se enlistan.

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.

Wordpress

Referencias

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

X = E

Elaboró: Ferrusca Ortiz Jorge Luis