Puertos vulnerables a tener en cuenta

Hay más de 130,000 puertos TCP y UDP, pero algunos son más vulnerables que otros. En las pruebas de penetración, estos puertos se consideran frutas maduras, es decir, vulnerabilidades que son fáciles de explotar.

Muchos puertos tienen vulnerabilidades conocidas que puedes explotar cuando surgen en la fase de escaneo de tu prueba de penetración. Aquí hay algunos puertos vulnerables comunes que necesitas saber.

1. FTP (20, 21)

FTP significa Protocolo de Transferencia de Archivos. Los puertos 20 y 21 son únicamente puertos TCP que se utilizan para permitir a los usuarios enviar y recibir archivos desde un servidor a sus computadoras personales.

El puerto FTP es inseguro y está desactualizado y puede ser explotado usando:

Autenticación anónima. Puedes iniciar sesión en el puerto FTP con el nombre de usuario y la contraseña configurados como “anonymous”.

Secuencias de comandos entre sitios.

Ataques de fuerza bruta.

Ataques de salto de directorios.

2. SSH (22)

SSH significa Secure Shell. Es un puerto TCP utilizado para garantizar el acceso remoto seguro a los servidores. Puedes explotar el puerto SSH mediante la fuerza bruta de las credenciales SSH o utilizando una clave privada para obtener acceso al sistema de destino.

3. SMB (139, 137, 445)

SMB significa Bloque de Mensajes del Servidor. Es un protocolo de comunicación creado por Microsoft para brindar acceso compartido a archivos e impresoras a través de una red. Al enumerar el puerto SMB, encuentras la versión SMB y luego puedes buscar un exploit en Internet, Searchsploit o Metasploit.

El puerto SMB podría explotarse usando la vulnerabilidad EternalBlue, usando fuerza bruta para las credenciales de inicio de sesión de SMB, explotando el puerto SMB usando NTLM Capture y conectándose a SMB usando PSexec.

Un ejemplo de una vulnerabilidad SMB es la vulnerabilidad Wannacry que se ejecuta en EternalBlue

4. DNS (53)

DNS significa Sistema de Nombres de Dominio. Es un puerto TCP y UDP utilizado para transferencias y consultas respectivamente. Un exploit común en los puertos DNS es el ataque de denegación de servicio distribuido (DDoS).

5. HTTP/HTTPS (443, 80, 8080, 8443)

HTTP significa Protocolo de Transferencia de Hipertexto, mientras que HTTPS significa Protocolo de Transferencia de Hipertexto Seguro (que es la versión más segura de HTTP). Estos son los protocolos más populares y ampliamente utilizados en Internet y, como tales, son propensos a muchas vulnerabilidades. Son vulnerables a inyecciones de SQL, secuencias de comandos entre sitios, falsificación de solicitudes entre sitios, etc.

6. Telnet (23)

El protocolo Telnet es un protocolo TCP que permite a un usuario conectarse a computadoras remotas a través de Internet. El puerto Telnet ha sido reemplazado durante mucho tiempo por SSH, pero algunos sitios web todavía lo utilizan en la actualidad. Está desactualizado, es inseguro y vulnerable al malware. Telnet es vulnerable a la suplantación de identidad, la detección de credenciales y la fuerza bruta de credenciales.

7. SMTP (25)

SMTP significa Protocolo Simple de Transferencia de Correo. Es un puerto TCP utilizado para enviar y recibir correos. Puede ser vulnerable al correo no deseado y la suplantación de identidad si no está bien protegido.

8. TFTP (69)

TFTP significa Protocolo de Transferencia de Archivos Trivial. Es un puerto UDP que se usa para enviar y recibir archivos entre un usuario y un servidor a través de una red. TFTP es una versión simplificada del protocolo de transferencia de archivos. Debido a que es un puerto UDP, no requiere autenticación, lo que lo hace más rápido pero menos seguro.