Informe de Metasploit

Autor: Yorman Veloz

Índice

Introducción 3
Alcance 3
Enfoque y Estrategia 3
Fases del Pestenting 3
Vulnerabilidades Detectadas 3
Observaciones 4
Propuestas de Prevención 5
Análisis de Mitigación 5
Impacto Potencial 5
Conclusión 5

Introducción

El presente informe documenta el ejercicio de pentesting realizado sobre una máquina vulnerable (Metasploitable2. El objetivo es identificar vulnerabilidades explotables mediante técnicas de reconocimiento activo y análisis de servicios, con fines educativos y de entrenamiento profesional.

Alcance

El escaneo se centrará en la recopilación de información sobre los puertos, servicios y vulnerabilidades de la máquina objetivo**.** Se realizarán los siguientes escaneo utilizando nmap.

- Stealth scan (escaneo sigiloso - syn scan)
- Escaneo a los puertos comunes (1 - 1024)
- Escaneos para obtener la versión del servicio corriendo en ese puerto
- Escaneos para obtener la versión del sistema Operativo del Metasploitable 2
- El resultado sea almacenado en un archivo .txt llamado Mestasploitable2scan.txt
- Utilizar el script de vulnerabilidades de nmap para verificar las vulnerabilidades que tiene la máquina como tal (pista el argumento --script vuln)
- Hacer que el escaneo se ejecute lo más rápido posible (Pista, jugar con los parámetros T)

Toda la información recopilada se documentará para su posterior análisis en el contexto de una evaluación de seguridad.

Enfoque y Estrategia

Se aplicó una metodología estructurada basada en las fases clásicas del pentesting:

- Reconocimiento
- Análisis de vulnerabilidades
- Explotación
- Reporte

Fases del Pestenting

Herramientas Usadas:

- **Comando ejecutado**

  $ nmap -sS -p1-1024 -sV -O --script vuln -T4 -oN Metasploitable2scan.txt 10.0.1.9

Vulnerabilidades Detectadas

Puerto	Estado	Servicio	Versión	Vulnerabilidades	Severidad	Propuestas de Mitigación
21/tcp	Open	ftp	vsftpd 2.3.4	CVE-2011-2523	Alto	Parche vsftpd. https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
22/tcp	Open	Ssh	OpenSSH 4.7p1 Debian	CVE-2023-38408, CVE-2016-1908, CVE-2020-15778,	Alto	Actualizar OpenSSH. https://www.openssh.com/security.html

			8ubuntu1 (protocol 2.0)	CVE-2016-10012, CVE-2019-6110, CVE-2019-6109, CVE-2016-6515, CVE-2016-10708, CVE-2015-5600, CVE-2016-10009, CVE-2016-10010, CVE-2015-6564, CVE-2018-15473		
23/tcp	Open	telnet	Linux telnetd	No se especifican CVEs en el escaneo)	Medio	Actualizar servicio o Deshabilitar Telnet (usar SSH)
25/tcp	Open	smtp	Postfix smtpd	CVE-2014-3566 (POODLE), CVE-2015-4000 (Logjam)	Medio	Configurar TLS seguro. https://www.openssl.org/~bodo/ssl-poodle.pdf
53/tcp	Open	domain	ISC BIND 9.4.2	CVE-2021-25216, CVE-2020-8616, CVE-2016-1286, CVE-2012-1667, CVE-2015-5477, CVE-2014-8500, CVE-2017-3141, CVE-2015-5722, CVE-2023-50387, CVE-2023-4408, CVE-2021-25215	Alto	Actualizar BIND. https://www.isc.org/bind/
80/tcp	Open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)	CVE-2017-7679, CVE-2017-3167, CVE-2011-3192, CVE-2017-9798, CVE-2018-1303, CVE-2016-5387, CVE-2014-0226, CVE-2007-6750 (Slowloris), CVE-2009-3555, CVE-2017-9788, CVE-2021-40438, CVE-2022-31813, CVE-2022-22720	Alto	Actualizar Apache. https://httpd.apache.org/security/
111/tcp	Open	rpcbind	2 (RPC #100000)		Medio	. Actualizar servicio o Restringir acceso con firewall
139/tcp	Open	Netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	(No se especifican CVEs en el escaneo, pero versiones antiguas son vulnerables)	Alto	Actualizar Samba. https://www.samba.org/samba/security/
445/tcp	Open	Netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)	(No se especifican CVEs en el escaneo, pero versiones antiguas son vulnerables)	Alto	Actualizar Samba. https://www.samba.org/samba/security/
512/tcp	Open	exec	netkit-rsh rexecd	(Servicio obsoleto con riesgos conocidos)	Alto	Deshabilitar servicio.
513/tcp	Open	login	OpenBSD or Solaris rlogind	(Servicio obsoleto con riesgos conocidos)	Alto	Deshabilitar servicio.
514/tcp	Open	Shell	tcpwrapped	Servicio restringido	Bajo	Evaluar necesidad del servicio.

Observaciones

- FTP (21/tcp): Vulnerabilidad crítica con backdoor (CVE-2011-2523) que permite ejecución remota de comandos como root.
- SSH (22/tcp): Múltiples CVEs, algunos con alta criticidad. Versión muy antigua.
- HTTP (80/tcp): Apache 2.2.8 tiene decenas de vulnerabilidades, incluyendo DoS (Slowloris), XSS, y ejecución remota.
- SMB (139/445): Versiones antiguas de Samba pueden ser vulnerables a ataques como EternalBlue (aunque no se detectó en el escaneo).

- Servicios obsoletos: Telnet, rsh, rlogin son inseguros por diseño.

Propuestas de Prevención

- Aplicar controles de seguridad preventiva, como segmentación de red y cortafuegos.
- Establecer un programa de gestión de parches y actualizaciones periódicas.
- Deshabilitar servicios innecesarios antes de exponer sistemas.
- Realizar auditorías de configuración y escaneos automatizados regularmente.

Análisis de Mitigación

Las medidas recomendadas son de implementación técnica accesible y ampliamente documentadas. La aplicación efectiva de estos controles mitiga riesgos críticos como ejecución remota, denegación de servicio, y filtrado de credenciales. Requieren supervisión continua por parte del administrador del sistema.

Impacto Potencial

Implementar estas mitigaciones:

- Reduce la superficie de ataque
- Mejora el cumplimiento con normas como ISO 27001 y CIS Controls.
- Minimiza el riesgo de explotación automatizada o ataques dirigidos.
- Mejora la postura general de ciberseguridad.

Conclusión

El ejercicio demostró la importancia del reconocimiento temprano de vulnerabilidades, aún en entornos de laboratorio. La exposición de servicios desactualizados puede comprometer la seguridad de sistemas completos. La prevención y mitigación continua, combinadas con buenas prácticas de administración, son claves para la protección efectiva de activos informáticos.