

RECONOCIMIENTO DE UNA MÁQUINA VULNERABLE METASPLOITABLE

6 DE NOVIEMBRE DE 2024

1. Objetivos y alcance

El objetivo de esta auditoría fue realizar un reconocimiento de vulnerabilidades en la maquina con el sistema operativo metasploitable. Se realizaron escaneos de red para buscar la dirección ip objetiva, escaneos sobre versiones y sistemas operativos, enumeración de puertos y servicios del objetivo.

2. Herramientas y técnicas utilizadas

Se utilizara nmap para realizar dicha auditoría. Se utilizó el comando **nmap -sS -sV -O -p- 10.0.2.4** para obtener una lista de puertos, servicios activos y sistema operativo.

```
MAC Address: 08:00:27:3F:23:2B (Oracle VM
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-04 19:12 CET
Nmap scan report for 10.0.2.4
Host is up (0.00020s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:3F:23:2B (Oracle VirtualBox virtual NIC)
```

Se obtuvo una lista amplia de los puertos abiertos, sin embargo, no se obtuvieron versiones de los servicios corriendo en dichos puertos. Se detectó el sistema operativo Linux 2.6.9 - 2.6.33, lo cual es una información sensible para que un atacante pueda investigar posibles brechas en el sistema operativo.

3. Resultados de la vulnerabilidades

Para el escaneo de vulnerabilidades se ejecuto el script de nmap de vulnerabilidades comunes, utilizando el siguiente comando **nmap --script vuln -sS -p- 10.0.2.4**

```
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs: BID:48539 CVE:CVE-2011-2523
|       vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
3306/tcp  open  mysql
5432/tcp  open  postgresql
| ssl-dh-params:
|   VULNERABLE:
|     Diffie-Hellman Key Exchange Insufficient Group Strength
|       State: VULNERABLE
|       Transport Layer Security (TLS) services that use Diffie-Hellman group
|       of insufficient strength, especially those using one of a few commonl
|       shared groups, may be susceptible to passive eavesdropping attacks.
|       Check results:
|         WEAK DH GROUP 1
|           Cipher Suite: TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
|           Modulus Type: Safe prime
|           Modulus Source: Unknown/Custom-generated
|           Modulus Length: 1024
|           Generator Length: 8
|           Public Key Length: 1024
https://weakdh.org
| ssl-poodle:
|   VULNERABLE:
|     SSL POODLE information leak
|       State: VULNERABLE
|       IDs: BID:70574 CVE:CVE-2014-3566
|       The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|       products, uses nondeterministic CBC padding, which makes it easie
|       for man-in-the-middle attackers to obtain cleartext data via a
|       padding-oracle attack, aka the "POODLE" issue.
|       Disclosure date: 2014-10-14
|       Check results:
|         TLS_RSA_WITH_AES_128_CBC_SHA
|       References:
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
|         https://www.openssl.org/~bodo/ssl-poodle.pdf
|         https://www.imperialviolet.org/2014/10/14/poodle.html
|         https://www.securityfocus.com/bid/70574
| ssl-ccs-injection:
|   VULNERABLE:
|     SSL/TLS MITM vulnerability (CCS Injection)
|       State: VULNERABLE
|       Risk factor: High
|       OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h
|       does not properly restrict processing of ChangeCipherSpec messages,
|       which allows man-in-the-middle attackers to trigger use of a zero
|       length master key in certain OpenSSL-to-OpenSSL communications, and
|       consequently hijack sessions or obtain sensitive information, via
|       a crafted TLS handshake, aka the "CCS Injection" vulnerability.
```

```
513/tcp open  login
514/tcp open  shell
1099/tcp open  rmiregistry
| rmi-vuln-classloader:
|   VULNERABLE:
|   RMI registry default configuration remote code execution vulnerability
|   State: VULNERABLE
|   Default configuration of RMI registry allows loading classes from remote
|   URLs which can lead to remote code execution.
```

La vulnerabilidad más peligrosa fue la encontrada en el puerto 21/tcp ftp con el CVE-2011-2553 con un riesgo crítico(9.8). Esta vulnerabilidad permite que se ejecute una puerta trasera y se abra un shell en el puerto 6200/tcp. Lo cual garantiza acceso total al sistema de forma remota desde el ordenador atacante.

En el sistema pueden haber fugas de información debido a la vulnerabilidad CVE-2014-3566 en el puerto 5432/tcp esta vulnerabilidad en el protocolo SSL 3.0 en el OpenSSL permite que los atacantes realizar un ataque man-in-the-middle para obtener información no cifrada. Tiene un riesgo bajo (3.4) , sin embargo, no hay que ignorarla, la fuga de información puede contener datos sensible que puede llevar a un ataque mas peligroso.

4. Mitigación

Las recomendaciones para la mitigación de posibles ataques recae en mantener siempre los sistemas actualizados a la versiones más actuales. Para evitar una fuga de información através de un ataque de man in the middle se puede desactivar el soporte SSLv3 en las aplicaciones y en los servicios. Asegurar se obtener la versión más reciente de SSL/TLS para mejor encriptación.

La vulnerabilidad critica de ftp 21/tcp backdoor, se puede mitigar por completo actualizando a la versión mas reciente de VSFTPD y así evitar un control total de un usuario no autorizado.