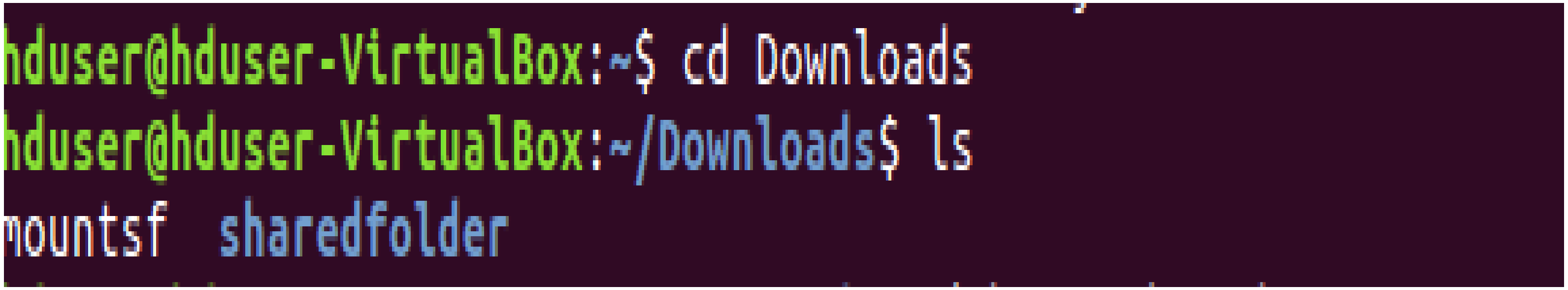
CYBER SECURITY MANAGEMENT

Agenda

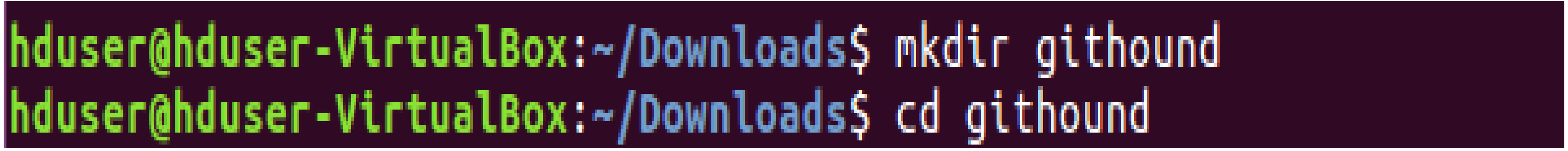
Githound steps

Step 1



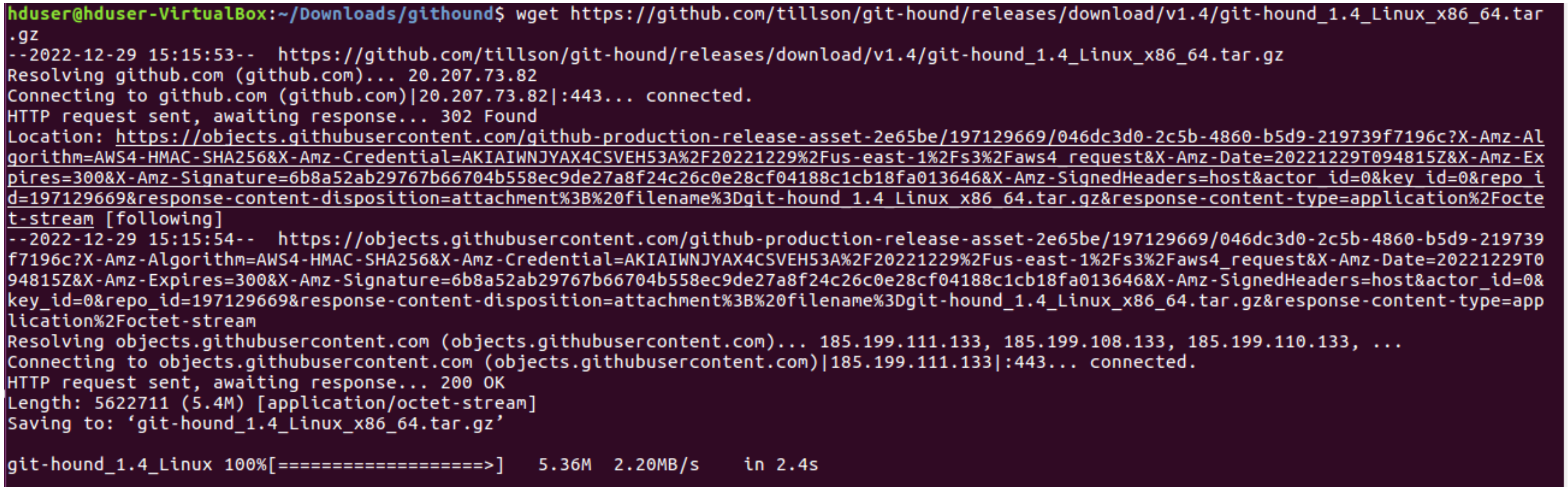
```
hduser@hduser-VirtualBox:~$ cd Downloads
hduser@hduser-VirtualBox:~/Downloads$ ls
mountsf  sharedfolder
```

Step 2



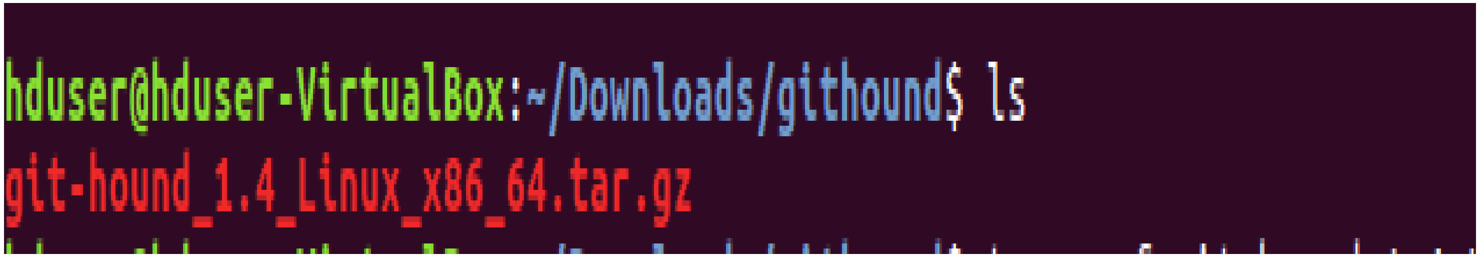
```
hduser@hduser-VirtualBox:~/Downloads$ mkdir githound
hduser@hduser-VirtualBox:~/Downloads$ cd githound
```

Step 3



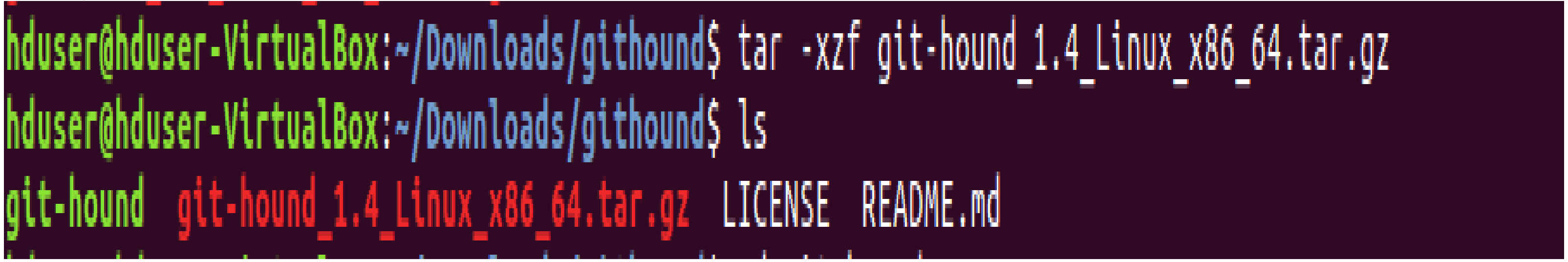
```
hduser@hduser-VirtualBox:~/Downloads/githound$ wget https://github.com/tillson/git-hound/releases/download/v1.4/git-hound_1.4_Linux_x86_64.tar
.gz
--2022-12-29 15:15:53--  https://github.com/tillson/git-hound/releases/download/v1.4/git-hound_1.4_Linux_x86_64.tar.gz
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://objects.githubusercontent.com/github-production-release-asset-2e65be/197129669/046dc3d0-2c5b-4860-b5d9-219739f7196c?X-Amz-Al
gorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20221229%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20221229T094815Z&X-Amz-Ex
pires=300&X-Amz-Signature=6b8a52ab29767b66704b558ec9de27a8f24c26c0e28cf04188c1cb18fa013646&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_i
d=197129669&response-content-disposition=attachment%3B%20filename%3Dgit-hound_1.4_Linux_x86_64.tar.gz&response-content-type=application%2Focte
t-stream [following]
--2022-12-29 15:15:54--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/197129669/046dc3d0-2c5b-4860-b5d9-219739
f7196c?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIWNJYAX4CSVEH53A%2F20221229%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20221229T0
94815Z&X-Amz-Expires=300&X-Amz-Signature=6b8a52ab29767b66704b558ec9de27a8f24c26c0e28cf04188c1cb18fa013646&X-Amz-SignedHeaders=host&actor_id=0&
key_id=0&repo_id=197129669&response-content-disposition=attachment%3B%20filename%3Dgit-hound_1.4_Linux_x86_64.tar.gz&response-content-type=app
lication%2Foctet-stream
Resolving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 185.199.110.133, ...
Connecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5622711 (5.4M) [application/octet-stream]
Saving to: ‘git-hound_1.4_Linux_x86_64.tar.gz’

git-hound_1.4_Linux 100%[===================>]   5.36M  2.20MB/s    in 2.4s
```

Step 4



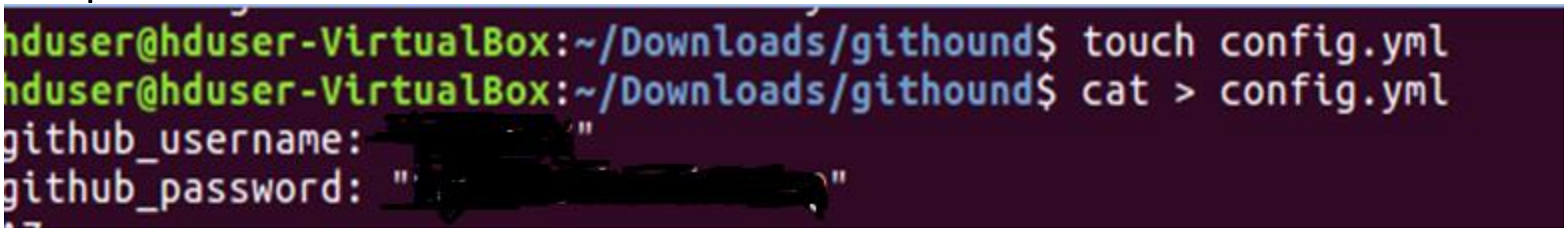
```
hduser@hduser-VirtualBox:~/Downloads/githound$ ls
git-hound_1.4_Linux_x86_64.tar.gz
```

Step 5



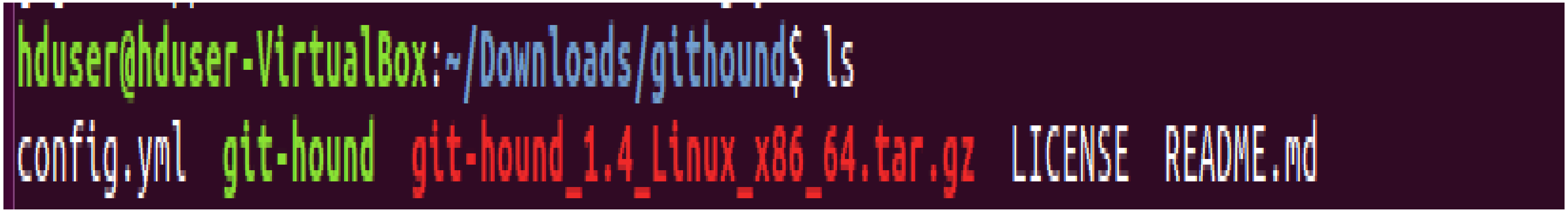
```
hduser@hduser-VirtualBox:~/Downloads/githound$ tar -xzf git-hound_1.4_Linux_x86_64.tar.gz
hduser@hduser-VirtualBox:~/Downloads/githound$ ls
git-hound  git-hound_1.4_Linux_x86_64.tar.gz  LICENSE  README.md
```

Step 6



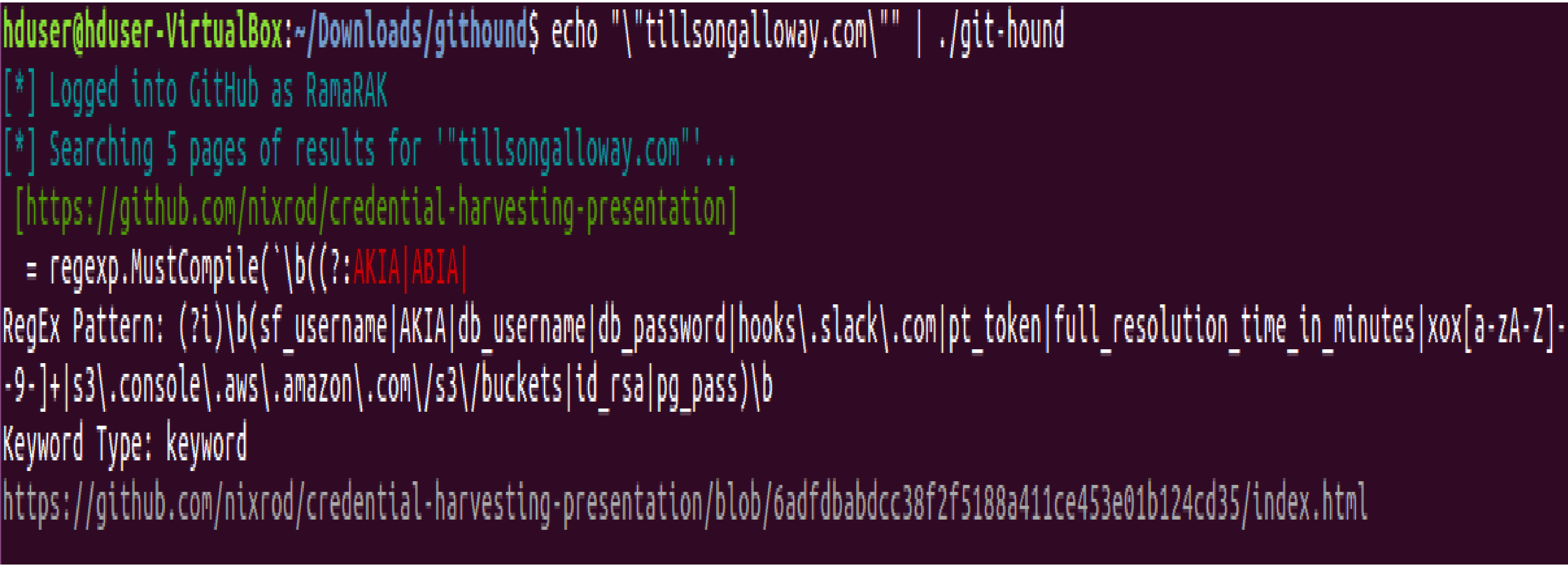
```
hduser@hduser-VirtualBox:~/Downloads/githound$ touch config.yml
hduser@hduser-VirtualBox:~/Downloads/githound$ cat > config.yml
github_username: [redacted]"
github_password: "[redacted]"
```

Step 7



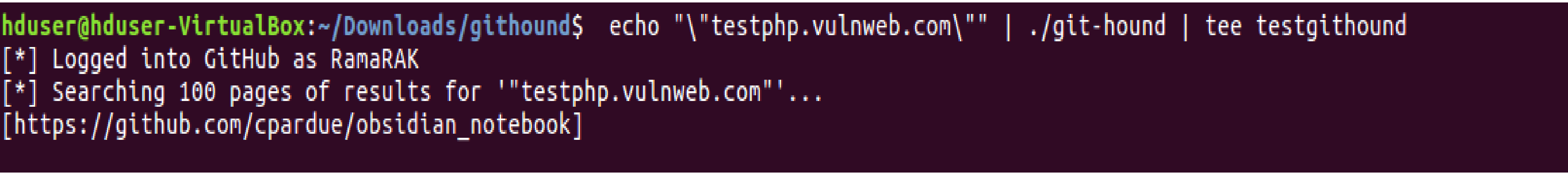
```
hduser@hduser-VirtualBox:~/Downloads/githound$ ls
config.yml  git-hound  git-hound_1.4_Linux_x86_64.tar.gz  LICENSE  README.md
```

Step 8



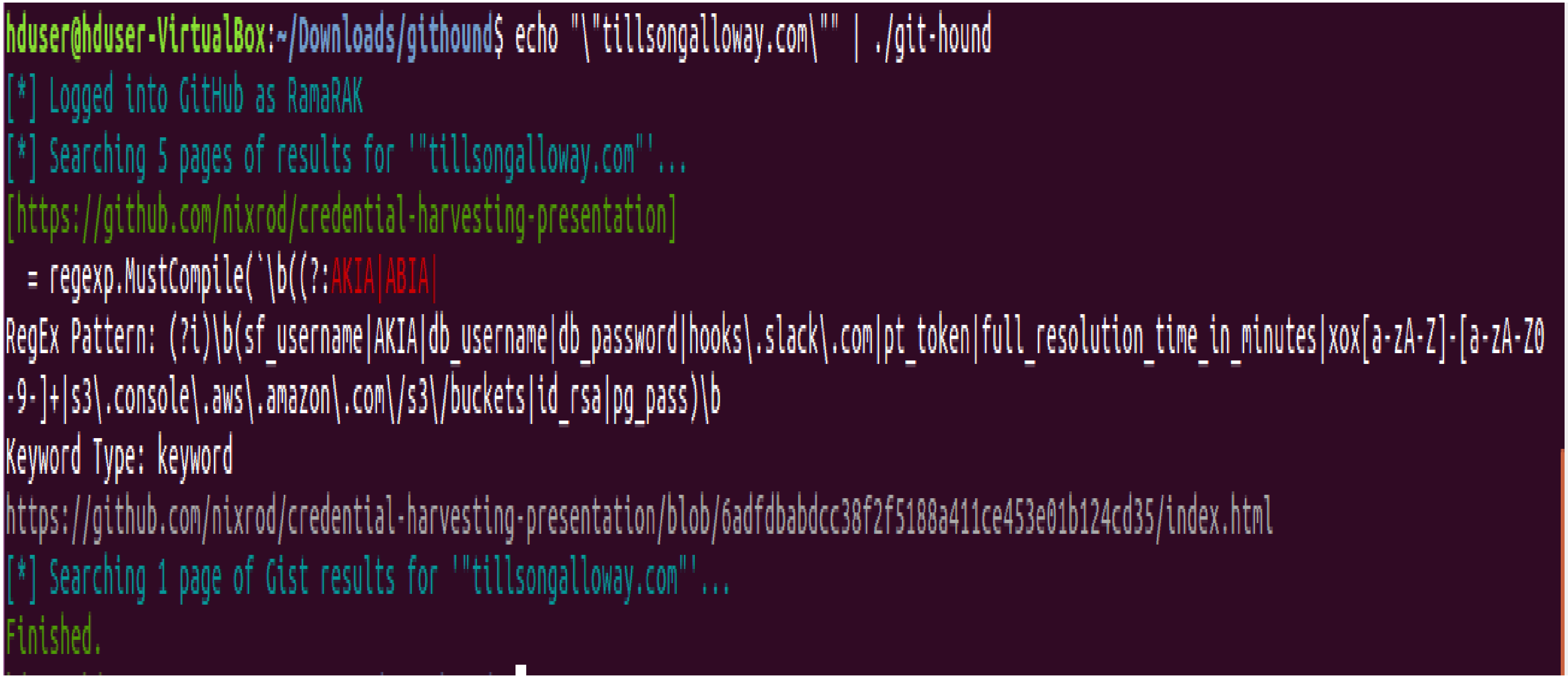
```
hduser@hduser-VirtualBox:~/Downloads/githound$ echo "\"tillsongalloway.com\"" | ./git-hound
[*] Logged into GitHub as RamaRAK
[*] Searching 5 pages of results for '"tillsongalloway.com"'...
 [https://github.com/nixrod/credential-harvesting-presentation]
  = regexp.MustCompile(`\b((?:AKIA|ABIA|
RegEx Pattern: (?i)\b(sf_username|AKIA|db_username|db_password|hooks\.slack\.com|pt_token|full_resolution_time_in_minutes|xox[a-zA-Z]-
-9-]+|s3\.console\.aws\.amazon\.com\/s3\/buckets|id_rsa|pg_pass)\b
Keyword Type: keyword
https://github.com/nixrod/credential-harvesting-presentation/blob/6adfdbabdcc38f2f5188a411ce453e01b124cd35/index.html
```

Step 9



```
hduser@hduser-VirtualBox:~/Downloads/githound$  echo "\"testphp.vulnweb.com\"" | ./git-hound | tee testgithound
[*] Logged into GitHub as RamaRAK
[*] Searching 100 pages of results for '"testphp.vulnweb.com"'...
[https://github.com/cpardue/obsidian_notebook]
```

```
echo "joor.com" | ./git-hound
```



```
hduser@hduser-VirtualBox:~/Downloads/githound$ echo "\"tillsongalloway.com\"" | ./git-hound
[*] Logged into GitHub as RamaRAK
[*] Searching 5 pages of results for '"tillsongalloway.com"'...
[https://github.com/nixrod/credential-harvesting-presentation]
  = regexp.MustCompile(`\b((?:AKIA|ABIA|
RegEx Pattern: (?i)\b(sf_username|AKIA|db_username|db_password|hooks\.slack\.com|pt_token|full_resolution_time_in_minutes|xox[a-zA-Z]-[a-zA-Z0
-9-]+|s3\.console\.aws\.amazon\.com\/s3\/buckets|id_rsa|pg_pass)\b
Keyword Type: keyword
https://github.com/nixrod/credential-harvesting-presentation/blob/6adfdbabdcc38f2f5188a411ce453e01b124cd35/index.html
[*] Searching 1 page of Gist results for '"tillsongalloway.com"'...
Finished.
```

References

- https://github.com/tillson/git-hound