Hack The Box walkthrough: Netmon

PUBLISHED: JUN 29, 2019
AUTHOR: BENJAMIN · 8 MIN READ

#HACKTHEBOX #PENTESTING #CTF #PRTG #FTP

Today, the virtual machine “Netmon” on Hack The Box retired. In this walkthrough, we show one way to retrieve the “user.txt” and “root.txt” files.

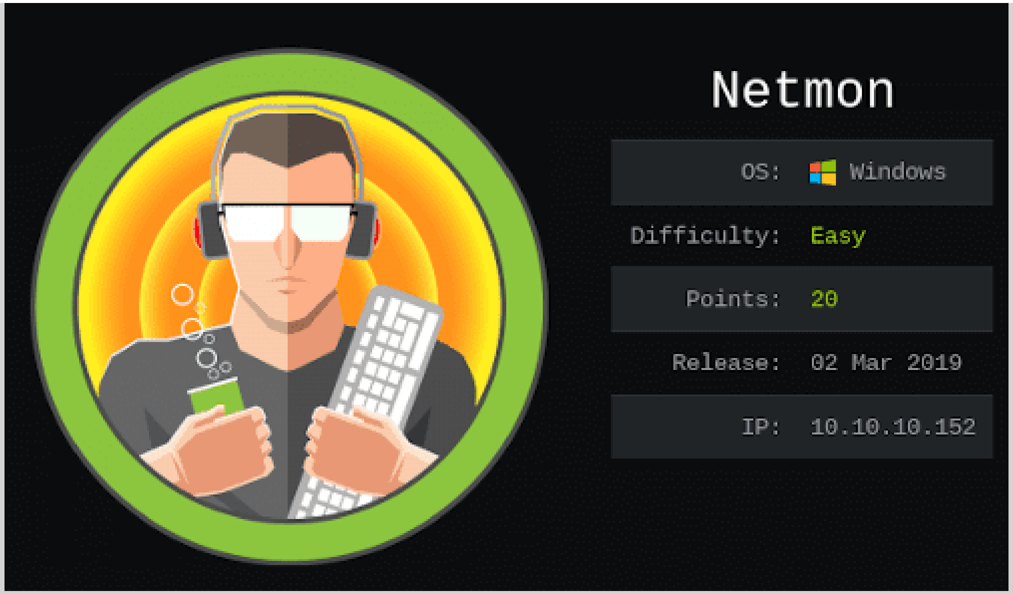
Contents

Note

If you are totally new to Hack The Box, read the short description on our page about our Hack The Box series.

General information about "Netmon"

On hackthebox.eu, we get general information about the target. It runs "Windows" and is rated "easy". There are more than 17,000 user owns (user.txt) and more than 10,000 system owns (root.txt). We also see that this machine can likely be exploited using publicly-known vulnerabilities.

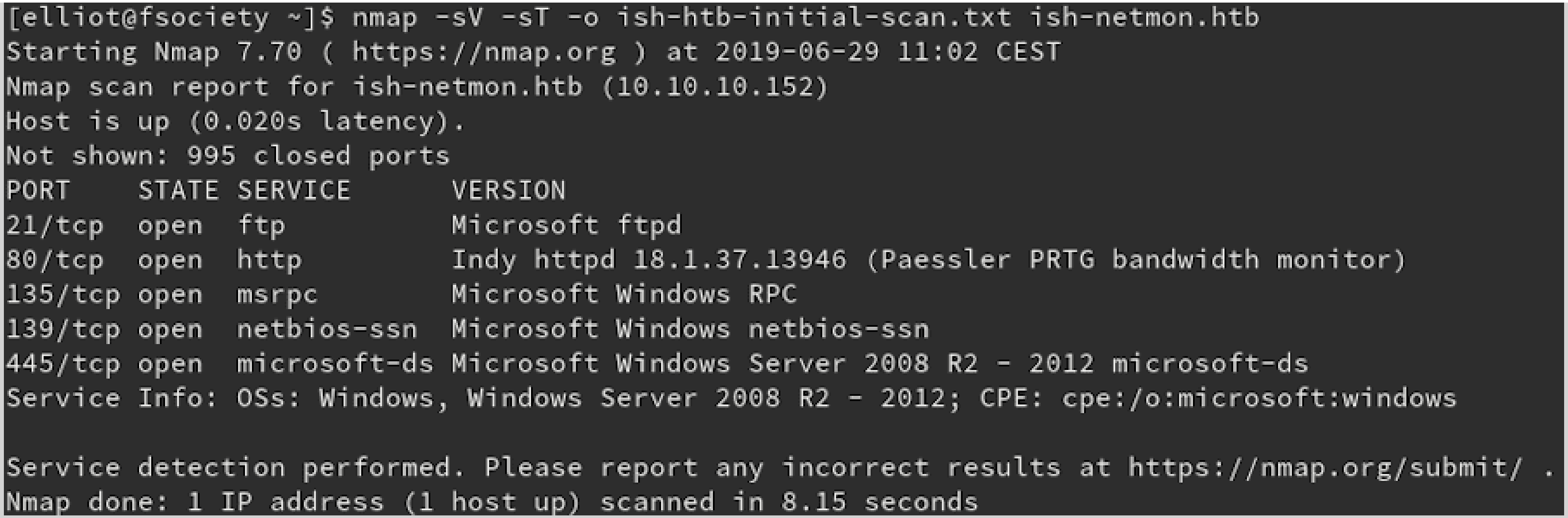


The Netmon card on Hack The Box. (🔍 Zoom in)

Step 1: Initial nmap scan

After connecting to the HTB VPN and adding the machine's IPv4 address to our "/etc/hosts" file (ish-netmon.htb), we conduct our initial nmap scan: `nmap -sV -sT -o ish-htb-initial-scan.txt ish-netmon.htb`.

- `-sV` : Probe open ports to determine service/version info.
- `-sT` : Do a TCP Connect Scan.
- `-o ish-htb-initial-scan.txt` : Save the output to this file.
- `ish-netmon.htb` : Scan this machine.



```
[elliot@fsociety ~]$ nmap -sV -sT -o ish-htb-initial-scan.txt ish-netmon.htb
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-29 11:02 CEST
Nmap scan report for ish-netmon.htb (10.10.10.152)
Host is up (0.020s latency).
Not shown: 995 closed ports
PORT    STATE SERVICE      VERSION
21/tcp  open  ftp          Microsoft ftpd
80/tcp  open  http         Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.15 seconds
```

Open ports based on our initial nmap scan. (Zoom in)

This scan results in the following open ports:

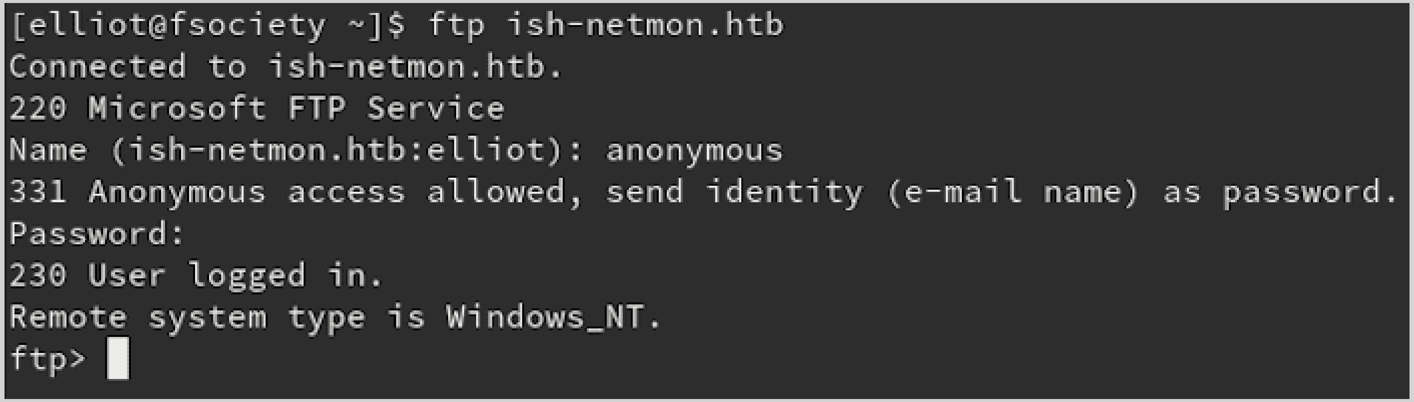
- 21/tcp: Microsoft ftpd
- 80/tcp: Indy httpd 18.1.37.13946 (Paessler PRTG bandwidth monitor)
- 135/tcp: Microsoft Windows RPC
- 139/tcp: Microsoft Windows netbios-ssn
- 445/tcp: Microsoft Windows Server 2008 R2 - 2012 microsoft-ds

Besides, the operating system is either “Windows Server 2008 R2” or “Windows Server 2012”.

Step 2: Check if FTP allows anonymous login

So, there is FTP on port 21. If configured insecurely, servers may allow anonymous FTP access. This feature was originally introduced to allow people to access archive sites, as described in RFC 1635 (May 1994). However, the server may allow people to access secret data if enabled.

First, we check if anonymous login is possible: `ftp ish-netmon.htb`. The server asks for a name ("Name (ish-netmon.htb:elliot):"). We just enter `anonymous`, and get the reponse: "331 Anonymous access allowed, send identity (e-mail name) as password."



```
[elliot@fsociety ~]$ ftp ish-netmon.htb
Connected to ish-netmon.htb.
220 Microsoft FTP Service
Name (ish-netmon.htb:elliot): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> 
```

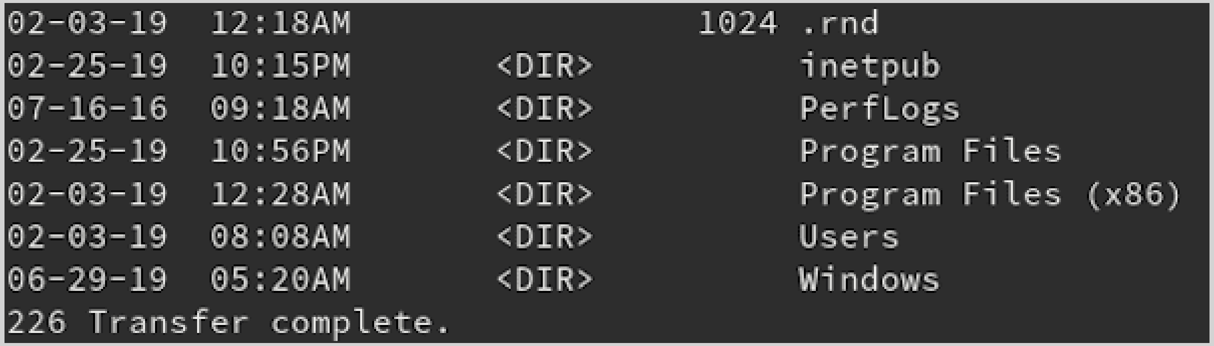
We are able to access FTP anonymously. (🔍 Zoom in)

So, anonymous access is enabled and we can use FTP to learn about the system now.

Step 3: Checking files and folders using FTP

While still connected to the machine via FTP, we enter `dir` to list the visible contents of the current folder. (We use `dir` instead of `ls` since it is a Windows machine.) We see the following folders:

- inetpub
- PerfLogs
- Program Files
- Program Files (x86)
- Users
- Windows



```
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
06-29-19  05:20AM       <DIR>          Windows
226 Transfer complete.
```

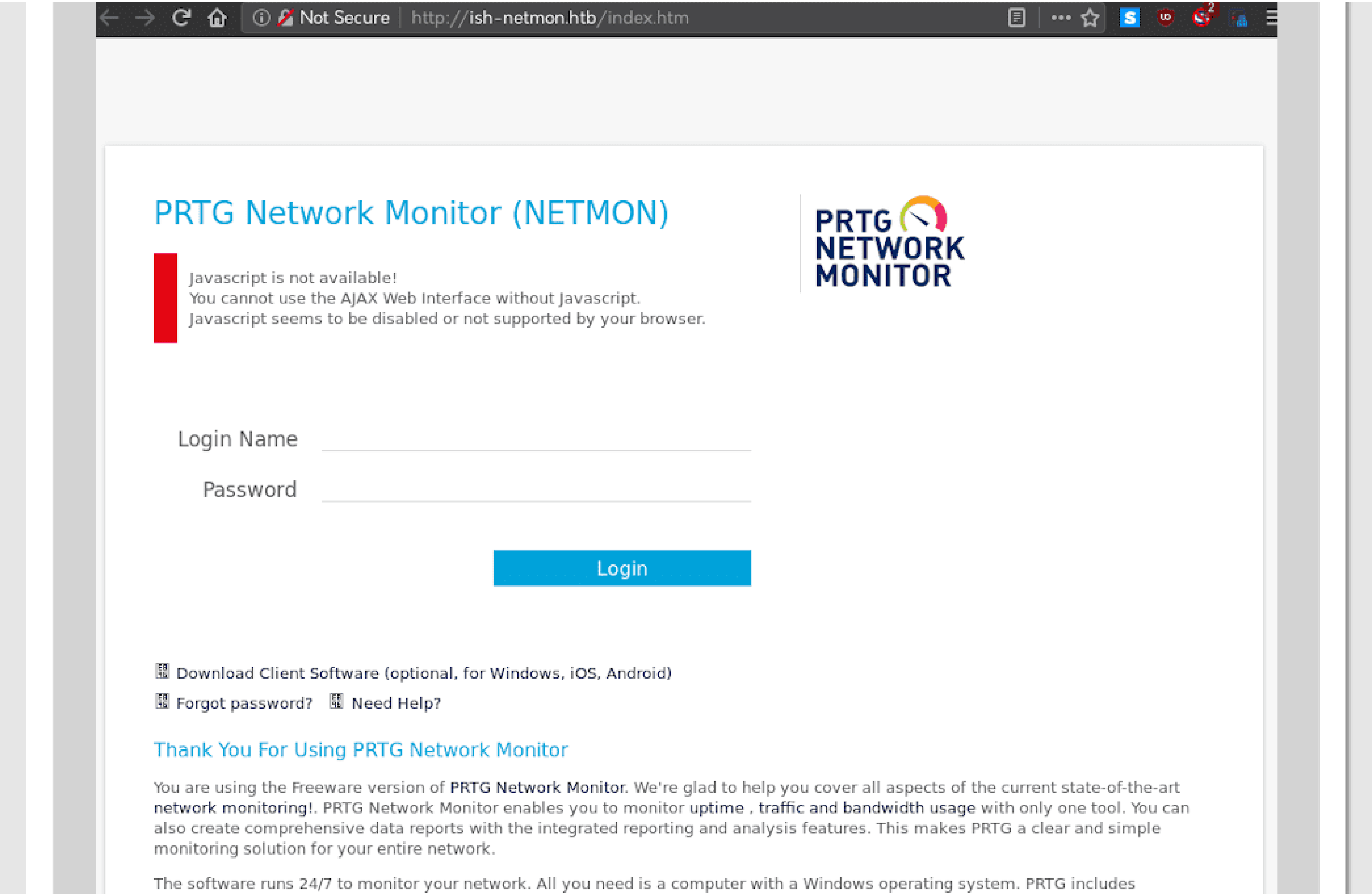
All visible folders in C: on the remote machine. (🔍 Zoom in)

So, we are obviously on the C: drive. In “Program Files”, we see Internet Explorer, VMware, Windows Defender, WindowsPowerShell, and WinPcap. In “Program Files (x86)”, there is additionally Microsoft.NET, and PRTG Network Monitor. We already know that PRTG Network Monitor runs on this server as reported by nmap.

If we go to “Users”, there are the folders “Administrator” and “Public”. Trying to access the “Administrator” folder, results in “550 Access is denied.” If we access the “Public” folder, we already see the “user.txt” file. This was quite easy. We use `get user.txt` to retrieve the file. Now, we have to find the “root.txt” file. It is likely located in the “Administrator” folder that can’t be accessed via FTP. Time to choose another strategy. We `quit` FTP for now.

Step 4: Checking PRTG Network Monitor

nmap already reported that there is “PRTG Network Monitor” running on port 80. nmap also reported its version number: 18.1.37.13946. If we go to “ish-netmon.htb” using a normal web browser, we see the login page of PRTG Network Monitor. In the footer section, it also shows “PRTG Network Monitor 18.1.37.13946”.



PRTG Network Monitor (NETMON)

Javascript is not available!
You cannot use the AJAX Web Interface without Javascript.
Javascript seems to be disabled or not supported by your browser.

Login Name

Password

Login

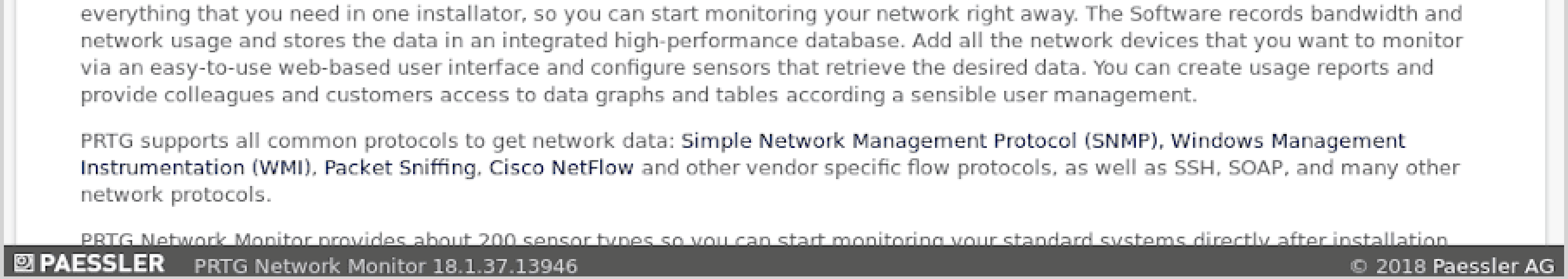
Download Client Software (optional, for Windows, iOS, Android)

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.

PRTG Network Monitor provides about 200 sensor types so you can start monitoring your standard systems directly after installation.

The login page of PRTG Network Monitor. We still need credentials. (Zoom in)

As always, version information is valuable for attackers. So, we are looking for publicly-known vulnerabilities in this version. Of course, there is no guarantee that the web application is vulnerable. Our favorite search engine lists “PRTG < 18.2.39 Command Injection Vulnerability” and “PRTG Network Monitor 18.2.38 - (Authenticated) Remote Code Execution”. Both vulnerabilities look interesting but we need credentials for the administrator of PRTG Network Monitor to exploit them.

One way is to use brute force. The Burp Suite provides the “Intruder” (attack type “Sniper”) for this purpose. This may work if the administrator chose a weak or known password. However, brute-force attacks can become extremely time-consuming.

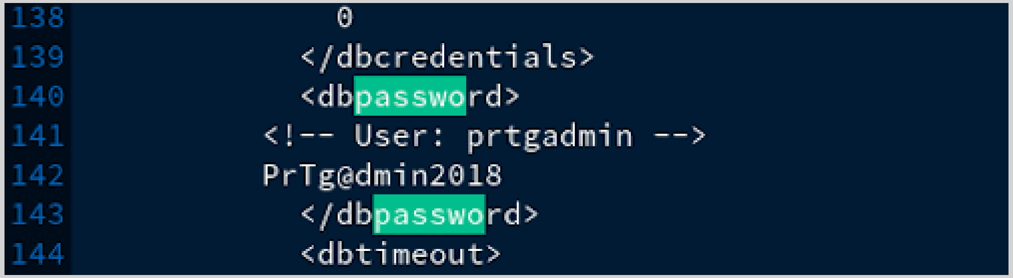
The better way is to find any cleartext credentials since we are already able to access the remote system using anonymous FTP. Sometimes—and contrary to best practices—web applications store credentials like passwords in cleartext. If we look for “PRTG cleartext credentials” on the internet, we get a hit on Reddit: “PRTG exposes Domain accounts and passwords in plain text.” There is an excerpt of an e-mail from Paessler, reporting “[a]n internal PRTG Network Monitor error caused some passwords to be written to the PRTG Configuration.dat file in plain text.”

If we look at the documentation of PRTG Network Monitor, we learn that the admin’s username is “prtgadmin”. The configuration is stored in XML in “PRTG Configuration.dat”. The data directory on Windows Server 2008 or 2012 is “%programdata%\Paessler\PRTG Network Monitor”. Let’s go back to FTP to check this folder:

1. `ftp ish-netmon.htb`
2. `cd "ProgramData\Paessler\PRTG Network Monitor"`
3. `dir`

Interestingly, there are three configuration files: “PRTG Configuration.dat”, “PRTG Configuration.old”, and “PRTG Configuration.old.bak”. We retrieve all of them using `get`. Could one of these files contain the password as mentioned in the Reddit post?

In “PRTG Configuration.dat” and “PRTG Configuration.old”, we look for “password” and only find `<encrypted/>`. However, in “PRTG Configuration.old.bak”, we get `<!-- User: prtgadmin --> PrTg@dmin2018`. Bingo!



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

The password 'PrTg@dmin2018' is actually included in a backup file. (🔍 Zoom in)

We go back to the web browser and enter username `prtgadmin` and password `PrTg@dmin2018`, resulting in “Your login has failed. Please try again!”. However, the admin was lazy. We enter `PrTg@dmin2019` and have full admin access to PRTG Network Monitor.

Step 5: Exploiting CVE-2018-9276 in PRTG Network Monitor

So far, we retrieved the “user.txt” file, got admin access to PRTG Network Monitor, and we know that the installed version is likely vulnerable to CVE-2018-9276 as described in “PRTG < 18.2.39 Command Injection Vulnerability” and “PRTG Network Monitor 18.2.38 – (Authenticated) Remote Code Execution”.

The blog post on codewatch.org (“PRTG < 18.2.39 Command Injection Vulnerability”) describes that you can simply add arbitrary commands to a file name in the notifications settings. Normally, PRTG Network Monitor should only execute the file, but the vulnerability allows injecting commands.

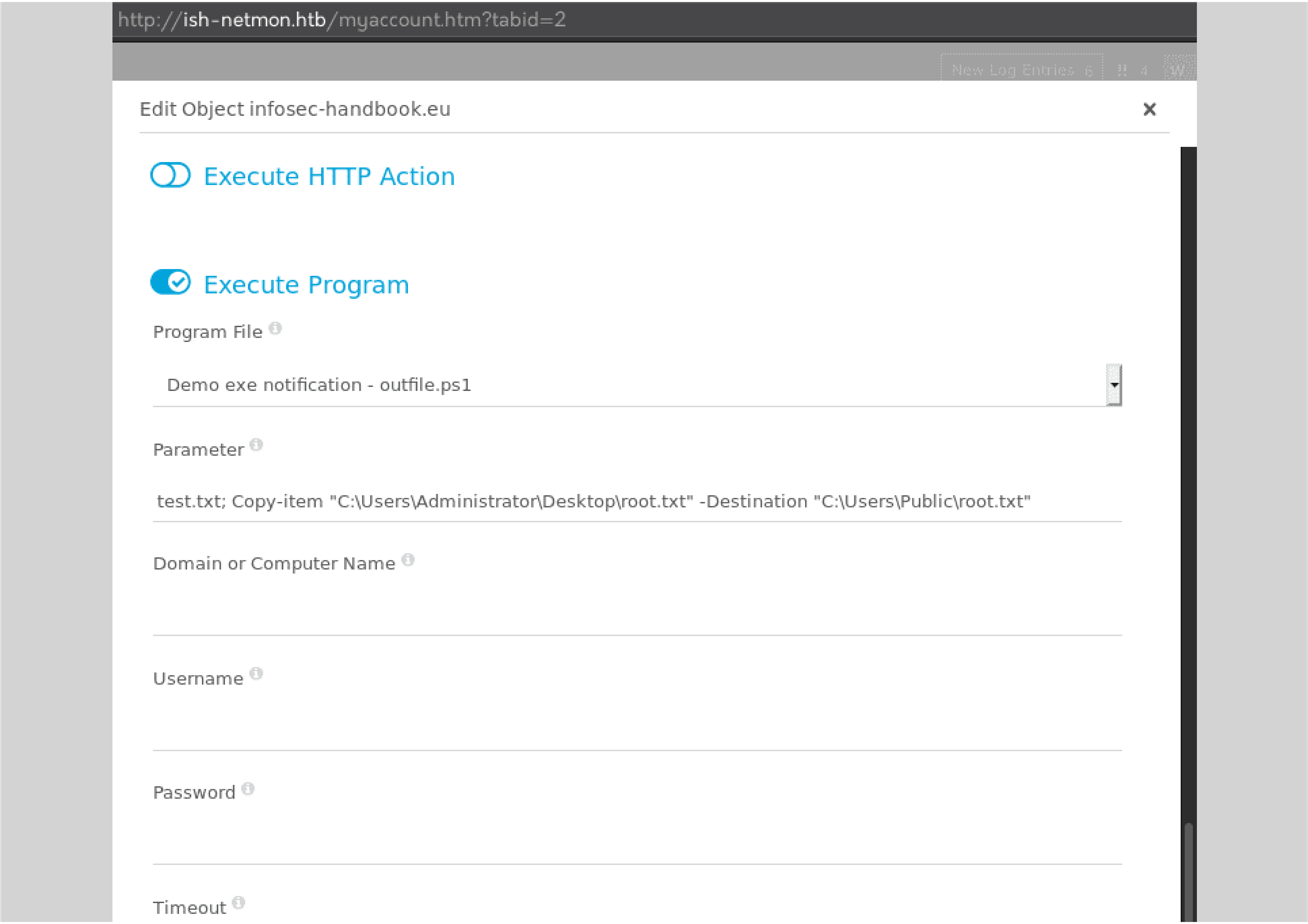
What do we need? We already know that there is a folder “Administrator” and it looks like the “root.txt” is oftentimes directly in the “Desktop” folder (as written in many other walkthroughs). So, the path to the “root.txt” is likely “C:\Users\Administrator\Desktop\root.txt”. We also know that there is PowerShell running on the server. So, maybe we only need a PowerShell script that copies the “root.txt” file to a folder that can be accessed using FTP (like Users\Public).

According to docs.microsoft.com, there is the command “Copy-Item”. We have to use the following syntax: `Copy-Item [-Path] <String[]> [[-Destination] <String>]`. So, our script looks like `Copy-Item [path\root.txt] -Destination [accessible-path]`.

We need to go to the notifications settings on our web browser, as described in the blog post on codewatch.org:

1. Click “Setup”
2. Click “Notifications” in “Account Settings”
3. Click “Add new notification”
4. Enable “Execute Program”
5. Select “Demo exe notification – outfile.ps1” as the “Program File”
6. Enter `test.txt; Copy-item "C:\Users\Administrator\Desktop\root.txt" -Destination "C:\Users\Public\root.txt"` as the “Parameter”

7. Then, switch “Notification Summarization” to “Always notify ASAP, never summarize”
8. “Save” the notification
9. Click “Send test notification”



http://ish-netmon.htb/myaccount.htm?tabid=2

Edit Object infosec-handbook.eu

○ Execute HTTP Action

● Execute Program

Program File: Demo exe notification - outfile.ps1

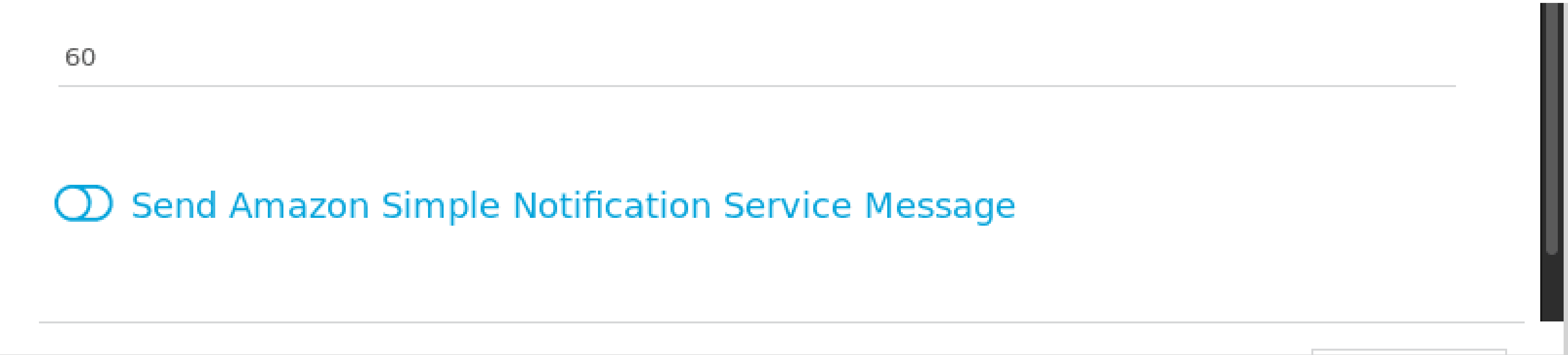
Parameter: test.txt; Copy-item "C:\Users\Administrator\Desktop\root.txt" -Destination "C:\Users\Public\root.txt"

Domain or Computer Name

Username

Password

Timeout


60

Send Amazon Simple Notification Service Message

We have to create a useless notification to exploit the vulnerability. The notification actually executes an injected command (our PowerShell script). (Zoom in)

In theory, this should create a test notification. Then, the test notification should execute the program, resulting in execution of our PowerShell script. The script copies “root.txt” to a folder that is accessible via FTP.

So, we have to check if it actually worked. We switch back to FTP `ftp ish-netmon.htb` and go to the accessible folder as before `cd Users/Public`. Then we use `dir`. Now, there is a file called “root.txt”. We `get` it and look at its contents. It’s actually the root flag. Done.

- “user.txt”: `d…5`
- “root.txt”: `3…c`

“*Everything has beauty, but not everyone sees it.*” — Confucius

Follow us on Mastodon:
@infosechandbook

Summary

In this walkthrough, we showed one way to own “Netmon” using FTP anonymous access and command injection. There may be other ways to own the machine. As shown in step 1, there are more open ports (135, 139, 445). Read other walkthroughs on the internet to learn about alternative ways to own the machine.

“Netmon” demonstrates the risks of anonymous FTP access and outdated software running on a public server. If you manage any servers, either disable FTP anonymous login or disable FTP completely and switch to secure alternatives. Furthermore, always keep your software up-to-date and delete unnecessary server-side backup files.

OLDER

GDPR: How to identify incomplete privacy policies?

NEWER

Web server security – Part 0: How to start

LATEST ACTIVITY

PRIVACY

ECSM 2019: Tips for your cyber hygiene

OCT 13, 2019 · NEW

MONTHLY REVIEW

Monthly review – September 2019

SEP 30, 2019 · NEW

HOME NETWORK SECURITY

Home network security – Part 2: HTTPS and TLS hardening

JUL 23, 2018 · UPDATED

PRIVACY

GnuPG for e-mail encryption and signing

SEP 1, 2019 · NEW

MONTHLY REVIEW

Monthly review – August 2019

AUG 31, 2019 · NEW

CATEGORIES

authentication (4)

discussion (6)

hack-the-box (1)

home-network-security (6)

knowledge (2)

limits (3)

monthly-review (2)

myths (5)

privacy (11)

tutorial (3)

vulnerability (1)

web-server-security (9)

TAG CLOUD

2fa ad-blocking afwall android apache appeals assessment audit blogging bluetooth caa camera capec career certifications cms comptia cryptcheck csp ct ctf cve cvss cwe dejablue dns dnssec doh dot e-foundation e-mail e2ee ecsm2019 encryption ethics exif fail2ban federation fido2 firewall ftp gdm gdpr gnupg hackthebox hardenize https hugo hygiene ips joomla keybase knob kresd lan lets-encrypt lineageos lnav logging malvertising mastodon matrix metadata minisign modsecurity monitoring nas nextcloud nginx nitrokey observatory ocsp open-source owasp pam password pdfex pentesting photo phpbb policy privacy privacy-policy privacyscore privacytools prtg remote-access rom router server-security signal simjacker software-security ssh standard tls tor tracking turris-omnia u2f ultravnc verification vnc waf web-server webauthn webbkoll wibattack wlan wordpress wpa2 xmpp yubikey

RSS/Atom · Privacy policy · Security policy · Changelog · Copyright

Mirror (dat protocol)