

# Whctf - OLDDRIVER - Writeup

转载

baikeng3674 于 2017-09-18 09:25:00 发布 219 收藏 2

原文链接: <http://www.cnblogs.com/WangAoBo/p/7541536.html>

版权

## Whctf - OLDDRIVER - Writeup

转载请标明出处<http://www.cnblogs.com/WangAoBo/p/7541536.html>

### 题目:

```
{{"c": "7366067574741171461722065133242916080495505913663250330082747465383676893970411476550748394841437418105312353971095003424322679616940371123028982189502042, "e": 10, "n": 25162507052339714421839688873734596177751124036723831003300959761137811490715205742941738406548150240861779301784133652165908227917415483137585388986274803}, {"c": "2196282532330046915179592028988688656279094277154685850084217980656643576710380397888514877213930548431968824936899503784441507383476095946258011317951461, "e": 10, "n": 2397685958990441979832081209768185865232547379189123271043199720289781958063493707900625213218095330766877190212418023297341732808839488308551126409983193}, {"c": "6569689420274066957835983390583585286570087619048110141187700584193792695235405077811544355169290382357149374107076406086154103351897890793598997687053983, "e": 10, "n": 18503782836858540043974558035601654610948915505645219820150251062305120148745549065675486501918320908234828526043464783353378450107671922605361848703623}, {"c": "450824616804451351845249388271353639063674154155180582179033897379761597127186724858437981311412547819528469269592866894553625483179633266057122967547052, "e": 10, "n": 23383087478545512218713157932934746110721706819077423418060220083657713428503582801909807142802647367994289775015595100541168367083097506193809451365010723}, {"c": "229661056702912823355888430182441615527644863731179428659669040761911223734354255327674393881768672955471431549481892275388019894589722422137268427611672, "e": 10, "n": 31775649089861428671057909076144152870796722528112580479442073365053916012507273433028451755436987054722496057749731758475958301164082755003195632005308493}, {"c": "17963313063405045742968136916219838352135561785389534381262979264585397896844470879023686508540355160998533122970239261072020689217153126649390825646712087, "e": 10, "n": 22246342022943432820696190444155665289928378653841172632283227888174495402248633061010615572642126584591103750338919213945646074833823905521643025879053949}, {"c": "1652417534709029450380570653973705320986117679597563873022683140800507482560482948310131540948227797045505390333146191586749269249548168247316404074014639, "e": 10, "n": 25395461142670631268156106136028325744293358436617528677967249347353524924655001151849544022201772500033280822372661344352607434738696051779095736547813043}, {"c": "158577173448835103945663139404049775956867942951061921976619178080767536174185929049073245112648776648126779759368428205194684721516497026290981786239352, "e": 10, "n": 3205650889274418490128941328728039891303832311548608141088227876326753674154124775132776928481935378184756756785107540781632570295330486738268173167809047}, {"c": "8965123421637694050044216844523379163347478029124815032832813225050732558524239660648746284884140746788823681886010577342254841014594570067467905682359797, "e": 10, "n": 5284976626954182747422818942882064857416253959598539592261649809907435742263020551050642688903339287717357281169159984125315046021998681796461970736553}, {"c": "135609457565430230085293881084469408471378530384370952445730358885312885773708290656663200693978983948484847030321018915638381833935580958342719988978247, "e": 10, "n": 3041598480030757893294639998755908896835638354344823359397204419191241802721772499486615661699080998502439901585573950889047918537906687840725005496238621}}
```

### 分析:

给了10组RSA的加密信息, 共有10个公钥, 并且所有的n都是互质的, 因此想到了低加密指数广播攻击  
放两个学习链接:

<http://bobao.360.cn/learning/detail/3058.html> (低加密指数广播攻击)

<http://www.bystudent.com/?p=86> (Code300)

### 步骤:

知道了原理就很简单了, 直接放脚本

```
1 import libnum
2 import gmpy2
3 dic = [{"c":
73660675747411714617220651332429160804955059136632503300827474653836768939704114765507483948414374181053
12353971095003424322679616940371123028982189502042, "e": 10, "n":
25162507052339714421839688873734596177751124036723831003300959761137811490715205742941738406548150240861
779301784133652165908227917415483137585388986274803},
4 {"c":
21962825323300469151795920289886886562790942771546858500842179806566435767103803978885148772139305484319
68824936899503784441507383476095946258011317951461, "e": 10, "n":
2397685958990441979832081209768185865232547379189123271043199720289781958063493707900625213218095330766
877190212418023297341732808839488308551126409983193},
5 {"c":
65696894202740669578359833905835852865700876190481101411877005841937926952354050778115443551692903823571
```

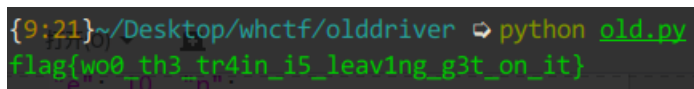
```

49374107076406086154103351897890793598997687053983, "e": 10, "n":
18503782836858540043974558035601654610948915505645219820150251062305120148745545906567548650191832090823
482852604346478335353784501076761922605361848703623},
6 {"c":
45082461680445135184524938827135363906367415415518058217903389737976159712718672485843798131141254781952
84692695928668946553625483179633266057122967547052, "e": 10, "n":
23383087478545512218713157932934746110721706819077423418060220083657713428503582801909807142802647367994
289775015595100541168367083097506193809451365010723},
7 {"c":
22966105670291282335588843018244161552764486373117942865966904076191122337435542553276743938817686729554
714315494818922753880198945897222422137268427611672, "e": 10, "n":
31775649089861428671057909076144152870796722528112580479442073365053916012507273433028451755436987054722
496057749731758475958301164082755003195632005308493},
8 {"c":
17963313063405045742968136916219838352135561785389534381262979264585397896844470879023686508540355160998
533122970239261072020689217153126649390825646712087, "e": 10, "n":
22246342022943432820696190444155665289928378653841172632283227888174495402248633061010615572642126584591
103750338919213945646074833823905521643025879053949},
9 {"c":
16524175347090294503805706539737053209861176795975638730226831408005074825604829483101315409482277970455
05390333146191586749269249548168247316404074014639, "e": 10, "n":
25395461142670631268156106136028325744393358436617528677967249347353524924655001151849544022201772500033
280822372661344352607434738696051779095736547813043},
10 {"c":
15585771734488351039456631394040497759568679429510619219766191780807675361741859290490732451112648776648
126779759368428205194684721516497026290981786239352, "e": 10, "n":
32056508892744184901289413287728039891303832311548608141088227876326753674154124775132776928481935378184
756756785107540781632570295330486738268173167809047},
11 {"c":
89651234216376940500442168445233791633474780291248150328328132250507325585242396606487462848841407467888
23681886010577342254841014594570067467905682359797, "e": 10, "n":
52849766269541827474228189428820648574162539595985395992261649809907435742263020551050064268890333392877
173572811691599841253150460219986817964461970736553},
12 {"c":
13560945756543023008529388108446940847137853038437095244573035888531288577370829065666320069397898394848
484847030321018915638381833935580958342719988978247, "e": 10, "n":
30415984800307578932946399987559088968355638354344823359397204419191241802721772499486615661699080998502
439901585573950889047918537906687840725005496238621}]
13 n = []
14 C = []
15 for i in dic:
16     n.append(i["n"])
17     C.append(i["c"])
18
19 # for i in n:
20     # for j in n:
21         # if i == j:
22             # continue
23         # else:
24             # if gmpy2.gcd(i, j) != 1:
25                 # print i, j
26 N = 1
27 for i in n:
28     N *= i
29
30 Ni = []
31 for i in n:
32     Ni.append(N / i)
33
34 T = []

```

```
35 for i in xrange(10):
36     T.append(long(gmpy2.invert(Ni[i], n[i])))
37
38 X = 0
39 for i in xrange(10):
40     X += C[i] * Ni[i] * T[i]
41
42 m10 = X % N
43 m = gmpy2.iroot(m10, 10)
44 print libnum.n2s(m[0])
```

运行得到flag



```
{9:21}~/Desktop/whctf/olddriver ➤ python old.py
flag{wo0_th3_tr4in_i5_leaving_g3t_on_it}
```

转载于:<https://www.cnblogs.com/WangAoBo/p/7541536.html>