Whctf - OLDDRIVER - Writeup

转载

weixin_30478619 于 2017-09-18 09:25:00 发布 723 收藏 3
原文链接：http://www.cnblogs.com/WangAoBo/p/7541536.html

Whctf - OLDDRIVER - Writeup

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

题目：


```
[{"c": 73660675747411714617220651332429160804955059136632503300827474653836768939704114765507483948414374181053123539710950034243226796169403711230289821895020 42, "e": 10,
"n": 25162507052339714421839688873734596177751124036723831003300959761137811490715205742941738406548150240861779301784133652165908227917415483137585388986274803},
{"c": 21962825323300469151795920289886886562790942771546858500842179806566435767103803978885148772139305484319688249368999503784441507383476095946258011317951461, "e": 10,
"n": 23976859589904419798320812097681858652325473791891232710431997202897819580634937070900625213218095330766877190212418023297341732808839488308551126409983193},
{"c": 65696894202740669578359833905835852865700876190481101411877005841937926952354050778115443551692903823571493741070764060861541033518978907935989976870539 83, "e": 10,
"n": 18503782836858540043974558035601654610948915505645219820150251062305120148745545906567548650191832090823482852604346478335353784501076761922605361848703623},
{"c": 45082461680445135184524938827135363906367415415518058217903389737976159712718672485843798131141254781952846926959286689465536254831796332660571229675470 52, "e": 10,
"n": 23383087478545512218713157932934746110721706819077423418060220083657713428503582801909807142802647367994289775015595100541168367083097506193809451365010723},
{"c": 22966105670291282335588843018244161552764486373117942865966904076191122337435542553276743938817686729554714315494818922753880198945897222422137268427611672, "e": 10,
"n": 31775649089861428671057909076144152870796722528112580479442073365053916012507273433028451755436987054722496057749731758475958301164082755003195632005308493},
{"c": 17963313063405045742968136916219838352135561785389534381262979264585397896844470879023686508540355160998533122970239261072020689217153126649390825646712087, "e": 10,
"n": 22246342022943432820696190444155665289928378653841172632283227888174495402248633061010615572642126584591103750338919213945646074833823905521643025879053949},
{"c": 16524175347090294503805706539737053209861176795975638730226831408005074825604829483101315409482277970455053903331461915867492692495481682473164040740146 39, "e": 10,
"n": 25395461142670631268156106136028325744393358436617528677967249347353524924655001151849544022201772500033280822372661344352607434738696051779095736547813043},
{"c": 15585771734488351039456631394040497759568679429510619219766191780807675361741859290490732451112648776648126779759368428205194684721516497026290981786239352, "e": 10,
"n": 32056508892744184901289413287728039891303832311548608141088227876326753674154124775132776928481935378184756756785107540781632570295330486738268173167809047},
{"c": 89651234216376940500442168445233791633474780291248150328328132250507325585242396606487462848841407467888236818860105773422548410145945700674679056823597797, "e": 10,
"n": 52849766269541827474228189428820648574162539595985395992261649809907435742263020551050064268890333392877173572811691599841253150460219986817964461970736553},
{"c": 13560945756543023008529388108446940847137853038437095244573035888531288577370829065666320069397898394848484847030321018915638381833935580958342719988978247, "e": 10,
"n": 30415984800307578932946399987559088968355638354344823359397204419191241802721772499486615661699080998502439901585573950889047918537906687840725005496238621}]
```

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
77930178413365216590822791741548313758538898627480 3},
 4 {"c":
21962825323300469151795920289886886562790942771546858500842179806566435767103803978885148772139305484319
68824936899950378444150738347609594625801131795146 1, "e": 10, "n":
23976859589904419798320812097681858652325473791891232710431997202897819580634937070900625213218095330766
87719021241802329734173280883948830855112640998319 3},
 5 {"c":
65696894202740669578359833905835852865700876190481101411877005841937926952354050778115443551692903823571
```

```
4937410707640608615410335189789079359899768705398 3, "e": 10, "n":
1850378283685854004397455803560165461094891550564521982015025106230512014874554590656754865019183209082348285260434647833535378450107676192260536184870362 3},
 6 {"c":
4508246168044513518452493882713536390636741541551805821790338973797615971271867248584379813114125478195284692695928668946553625483179633266057122967547052, "e": 10, "n":
2338308747854551221871315793293474611072170681907742341806022008365771342850358280190980714280264736799428977501559510054116836708309750619380945136501072 3},
 7 {"c":
2296610567029128233558884301824416155276448637311794286596690407619112233743554255327674393881768672955471431549481892275388019894589722242213726842761167 2, "e": 10, "n":
3177564908986142867105790907614415287079672252811258047944207336505391601250727343302845175543698705472249605774973175847595830116408275500319563200530849 3},
 8 {"c":
1796331306340504574296813691621983835213556178538953438126297926458539789684447087902368650854035516099853312297023926107202068921715312664939082564671208 7, "e": 10, "n":
2224634202294343282069619044415566528992837865384117263228322788817449540224863306101061557264212658459110375033891921394564607483382390552164302587905394 9},
 9 {"c":
1652417534709029450380570653973705320986117679597563873022683140800507482560482948310131540948227797045505390333146191586749269249548168247316404074014639, "e": 10, "n":
2539546114267063126815610613602832574439335843661752867796724934735352492465500115184954402220177250003328082237266134435260743473869605177909573654781304 3},
10 {"c":
1558577173448835103945663139404049775956867942951061921976619178080767536174185929049073245111264877664812677975936842820519468472151649702629098178623935 2, "e": 10, "n":
3205650889274418490128941328772803989130383231154860814108822787632675367415412477513277692848193537818475675678510754078163257029533048673826817316780904 7},
11 {"c":
8965123421637694050044216844523379163347478029124815032832813225050732558524239660648746284884140746788823681886010577342254841014594570067467905682359797, "e": 10, "n":
5284976626954182747422818942882064857416253959598539599226164980990743574226302055105006426889033339287717357281169159984125315046021998681796446197073655 3},
12 {"c":
1356094575654302300852938810844694084713785303843709524457303588853128857737082906566632006939789839484848484703032101891563838183393558095834271998897824 7, "e": 10, "n":
3041598480030757893294639998755908896835563835434482335939720441919124180272177249948661566169908099850243990158557395088904791853790668784072500549623862 1},]
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_leav1ng_g3t_on_it}
```

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