

```
print
```

发表于 2021-05-21 分类于 [Challenge](#), [2020](#), [XCTF 高校网络安全专题挑战赛](#), [鲲鹏计算专场](#), [Reverse](#)
[Challenge](#) | [2020](#) | [XCTF 高校网络安全专题挑战赛](#) | [鲲鹏计算专场](#) | [Reverse](#) | [print](#)

[点击此处](#)获得更好的阅读体验

*WriteUp*来源

官方WP

题目描述

题目考点

解题思路

通过逆向提供的binary文件"print", 可以知道里面实现了一个brainfuck引擎, 提取出其中的brainfuck程序, [见a.bf](#)

将a.bf程序转化为相同功能的c代码, 见a.cpp

对a.cpp代码进行人工分析,最后计算得到输入的password为R3veRSe_C0d3.

通过连接远程运行的服务得到最终的flag,运行命令为

```
1 print -c "R3veRSe C0d3" | nc localhost 6666
```

a.bf 请将下面两个代码块合并

[illegible][illegible]

a.cpp 请将下面三个代码块合并

"

```

1 ptr = &[6];
2 while(*ptr){
3     *ptr = 1;
4     *ptr = &[30];
5     *ptr = 1;
6     ptr = &[0];
7     *ptr = 1;
8     ptr = &[6];
9 }
10 ptr = &[0];
11 while(*ptr){
12     *ptr = 1;
13     ptr = &[6]
14     *ptr = 1;
15     ptr = &[0];
16 }
17 ptr = &[2];
18 while(*ptr){
19     *ptr = 1;
20     ptr = &[31];
21     *ptr = 1;
22     ptr = &[0];
23     *ptr = 1;
24     ptr = &[2];
25 }
26 ptr = &[0];
27 while(*ptr){
28     *ptr = 1;
29     ptr = &[2];
30     *ptr = 1;
31     ptr = &[0];
32 }
33 ptr = &[9];
34 while(*ptr){
35     *ptr = 1;
36     *ptr = &[31];
37     *ptr = 1;
38     ptr = &[0];
39     *ptr = 1;
40     ptr = &[9];
41 }
42 ptr = &[0];
43 while(*ptr){
44     *ptr = 1;
45     ptr = &[9];
46     *ptr = 1;
47     ptr = &[0];
48 }
49 ptr = &[16];
50 while(*ptr){
51     *ptr = 1;
52     ptr = &[31];
53     *ptr = 1;
54     ptr = &[0];
55     *ptr = 1;
56     ptr = &[16];
57 }
58 ptr = &[0];
59 while(*ptr){
60     *ptr = 1;
61     *ptr = 1;
62     ptr = &[0];
63 }
64 ptr = &[23];
65 while(*ptr){
66     *ptr = 1;
67     ptr = &[31];
68     *ptr = 1;
69     ptr = &[0];
70     *ptr = 1;
71     ptr = &[23];

```

```

73 }
74 ptr = &_ [0];
75 while(*ptr){
76     *ptr -= 1;
77     ptr = &_ [23];
78     *ptr += 1;
79     ptr = &_ [0];
80 }
81 ptr = &_ [30];
82 while(*ptr){
83     *ptr -= 1;
84     ptr = &_ [31];
85     *ptr += 1;
86     ptr = &_ [0];
87     *ptr += 1;
88     ptr = &_ [30];
89 }
90 ptr = &_ [0];
91 while(*ptr){
92     *ptr -= 1;
93     ptr = &_ [30];
94     *ptr += 1;
95     ptr = &_ [0];
96 }
97 ptr = &_ [25];
98 while(*ptr){
99     *ptr -= 1;
100    ptr = &_ [32];
101    *ptr += 1;
102    ptr = &_ [0];

103    *ptr += 1;
104    ptr = &_ [25];
105 }
106 ptr = &_ [0];
107 while(*ptr){
108     *ptr -= 1;
109     ptr = &_ [25];
110     *ptr += 1;
111     ptr = &_ [0];
112 }
113 ptr = &_ [20];
114 while(*ptr){
115     *ptr -= 1;
116     ptr = &_ [32];
117     *ptr += 1;
118     ptr = &_ [0];
119     *ptr += 1;
120     ptr = &_ [20];
121 }
122 ptr = &_ [0];
123 while(*ptr){
124     *ptr -= 1;
125     ptr = &_ [20];
126     *ptr += 1;
127     ptr = &_ [0];
128 }
129 ptr = &_ [15];
130 while(*ptr){
131     *ptr -= 1;
132     ptr = &_ [32];
133     *ptr += 1;
134     ptr = &_ [0];
135     *ptr += 1;
136     ptr = &_ [15];
137 }
138 ptr = &_ [0];
139 while(*ptr){
140     *ptr -= 1;
141     ptr = &_ [15];
142     *ptr += 1;
143     ptr = &_ [0];
144 }
145 ptr = &_ [10];
146 while(*ptr){
147     *ptr -= 1;
148     ptr = &_ [32];
149     *ptr += 1;
150     ptr = &_ [0];
151     *ptr += 1;
152     ptr = &_ [10];
153 }
154 ptr = &_ [0];
155 while(*ptr){
156     *ptr -= 1;
157     ptr = &_ [10];
158     *ptr += 1;
159     ptr = &_ [0];
160 }
161 ptr = &_ [5];
162 while(*ptr){
163     *ptr -= 1;
164     ptr = &_ [32];
165     *ptr += 1;
166     ptr = &_ [0];
167     *ptr += 1;
168     ptr = &_ [5];
169 }
170 ptr = &_ [0];
171 while(*ptr){
172     *ptr -= 1;
173     ptr = &_ [5];
174     *ptr += 1;
175     ptr = &_ [0];
176 }
177 ptr = &_ [13];
178 while(*ptr){

179     *ptr -= 1;
180     ptr = &_ [33];
181     *ptr += 1;
182     ptr = &_ [0];
183     *ptr += 1;
184     ptr = &_ [13];
185 }
186 ptr = &_ [0];
187 while(*ptr){
188     *ptr -= 1;
189     ptr = &_ [13];
190     *ptr += 1;
191     ptr = &_ [0];
192 }
193 ptr = &_ [8];
194 while(*ptr){

```

```

194 while(*ptr){
195     *ptr -= 1;
196     ptr = &_ [33];
197     *ptr += 1;
198     ptr = &_ [0];
199     *ptr += 1;
200     ptr = &_ [8];
201 }
202 ptr = &_ [0];
203 while(*ptr){
204     *ptr -= 1;
205     ptr = &_ [8];
206     *ptr += 1;
207     ptr = &_ [0];
208 }
209 ptr = &_ [3];
210 while(*ptr){
211     *ptr -= 1;
212     ptr = &_ [33];
213     *ptr += 1;
214     ptr = &_ [0];
215     *ptr += 1;
216     ptr = &_ [3];
217 }
218 ptr = &_ [0];
219 while(*ptr){
220     *ptr -= 1;
221     ptr = &_ [3];
222     *ptr += 1;
223     ptr = &_ [0];
224 }
225 ptr = &_ [22];
226 while(*ptr){
227     *ptr -= 1;
228     ptr = &_ [33];
229     *ptr += 1;
230     ptr = &_ [0];
231     *ptr += 1;
232     ptr = &_ [22];
233 }
234 ptr = &_ [0];
235 while(*ptr){
236     *ptr -= 1;
237     ptr = &_ [22];
238     *ptr += 1;
239     ptr = &_ [0];
240 }
241 ptr = &_ [30];
242 while(*ptr){
243     *ptr -= 1;
244     ptr = &_ [33];
245     *ptr += 1;
246     ptr = &_ [0];
247     *ptr += 1;
248     ptr = &_ [30];
249 }
250 ptr = &_ [0];
251 while(*ptr){
252     *ptr -= 1;
253     ptr = &_ [30];
254     *ptr += 1;
255     ptr = &_ [0];
256 }
257 ptr = &_ [7];
258 while(*ptr){
259     *ptr -= 1;
260     ptr = &_ [34];
261     *ptr += 1;
262     ptr = &_ [0];
263     *ptr += 1;
264     ptr = &_ [7];
265 }
266 ptr = &_ [0];
267 while(*ptr){
268     *ptr -= 1;
269     ptr = &_ [7];
270     *ptr += 1;
271     ptr = &_ [0];
272 }
273 ptr = &_ [2];
274 while(*ptr){
275     *ptr -= 1;
276     ptr = &_ [34];
277     *ptr += 1;
278     ptr = &_ [0];
279     *ptr += 1;
280     ptr = &_ [2];
281 }
282 ptr = &_ [0];
283 while(*ptr){
284     *ptr -= 1;
285     ptr = &_ [2];
286     *ptr += 1;
287     ptr = &_ [0];
288 }
289 ptr = &_ [21];
290 while(*ptr){
291     *ptr -= 1;
292     ptr = &_ [34];
293     *ptr += 1;
294     ptr = &_ [0];
295     *ptr += 1;
296     ptr = &_ [21];
297 }
298 ptr = &_ [0];
299 while(*ptr){
300     *ptr -= 1;
301     ptr = &_ [21];
302     *ptr += 1;
303     ptr = &_ [0];
304 }
305 ptr = &_ [28];
306 while(*ptr){
307     *ptr -= 1;
308     ptr = &_ [34];
309     *ptr += 1;
310     ptr = &_ [0];
311     *ptr += 1;
312     ptr = &_ [28];
313 }
314 ptr = &_ [0];
315 while(*ptr){
316     *ptr -= 1;

```

```

317 ptr = &_[28];
318 *ptr += 1;
319 ptr = &_[0];
320 }
321 ptr = &_[17];
322 while(*ptr){
323     *ptr -= 1;
324     ptr = &_[34];
325     *ptr += 1;
326     ptr = &_[0];
327     *ptr += 1;
328     ptr = &_[17];
329 }
330 ptr = &_[0];

331 while(*ptr){
332     *ptr -= 1;
333     ptr = &_[17];
334     *ptr += 1;
335     ptr = &_[0];
336 }
337 ptr = &_[8];
338 while(*ptr){
339     *ptr -= 1;
340     ptr = &_[35];
341     *ptr += 1;
342     ptr = &_[0];
343     *ptr += 1;
344     ptr = &_[8];
345 }
346 ptr = &_[0];
347 while(*ptr){
348     *ptr -= 1;
349     ptr = &_[8];
350     *ptr += 1;
351     ptr = &_[0];
352 }
353 ptr = &_[15];
354 while(*ptr){
355     *ptr -= 1;
356     ptr = &_[35];
357     *ptr += 1;
358     ptr = &_[0];
359     *ptr += 1;
360     ptr = &_[15];
361 }
362 ptr = &_[0];
363 while(*ptr){
364     *ptr -= 1;
365     ptr = &_[15];
366     *ptr += 1;
367     ptr = &_[0];
368 }
369 ptr = &_[22];
370 while(*ptr){
371     *ptr -= 1;
372     ptr = &_[35];
373     *ptr += 1;
374     ptr = &_[0];
375     *ptr += 1;
376     ptr = &_[22];
377 }
378 ptr = &_[0];
379 while(*ptr){
380     *ptr -= 1;
381     ptr = &_[22];
382     *ptr += 1;
383     ptr = &_[0];
384 }
385 ptr = &_[29];
386 while(*ptr){
387     *ptr -= 1;
388     ptr = &_[35];
389     *ptr += 1;
390     ptr = &_[0];
391     *ptr += 1;
392     ptr = &_[29];
393 }
394 ptr = &_[0];
395 while(*ptr){
396     *ptr -= 1;
397     ptr = &_[29];
398     *ptr += 1;
399     ptr = &_[0];
400 }
401 ptr = &_[6];
402 while(*ptr){
403     *ptr -= 1;
404     ptr = &_[35];
405     *ptr += 1;
406     ptr = &_[0];

407     *ptr += 1;
408     ptr = &_[6];
409 }
410 ptr = &_[0];
411 while(*ptr){
412     *ptr -= 1;
413     ptr = &_[6];
414     *ptr += 1;
415     ptr = &_[0];
416 }
417 ptr = &_[7];
418 while(*ptr){
419     *ptr -= 1;
420     ptr = &_[36];
421     *ptr += 1;
422     ptr = &_[0];
423     *ptr += 1;
424     ptr = &_[7];
425 }
426 ptr = &_[0];
427 while(*ptr){
428     *ptr -= 1;
429     ptr = &_[7];
430     *ptr += 1;
431     ptr = &_[0];
432 }
433 ptr = &_[20];
434 while(*ptr){
435     *ptr -= 1;
436     ptr = &_[36];
437     *ptr += 1;

```

```

438 ptr = &_ [0];
439 *ptr += 1;
440 ptr = &_ [20];
441 }
442 ptr = &_ [0];
443 while (*ptr) {
444   *ptr -= 1;
445   ptr = &_ [20];
446   *ptr += 1;
447   ptr = &_ [0];
448 }
449 ptr = &_ [3];
450 while (*ptr) {
451   *ptr -= 1;
452   ptr = &_ [36];
453   *ptr += 1;
454   ptr = &_ [0];
455   *ptr += 1;
456   ptr = &_ [3];
457 }
458 ptr = &_ [0];
459 while (*ptr) {
460   *ptr -= 1;
461   ptr = &_ [3];
462   *ptr += 1;
463   ptr = &_ [0];
464 }
465 ptr = &_ [17];
466 while (*ptr) {
467   *ptr -= 1;
468   ptr = &_ [36];
469   *ptr += 1;
470   ptr = &_ [0];
471   *ptr += 1;
472   ptr = &_ [17];
473 }
474 ptr = &_ [0];
475 while (*ptr) {
476   *ptr -= 1;
477   ptr = &_ [17];
478   *ptr += 1;
479   ptr = &_ [0];
480 }
481 ptr = &_ [30];
482 while (*ptr) {
483   *ptr -= 1;
484   ptr = &_ [36];
485   *ptr += 1;
486   ptr = &_ [0];
487   *ptr += 1;
488   ptr = &_ [30];
489 }
490 ptr = &_ [0];
491 while (*ptr) {
492   *ptr -= 1;
493   ptr = &_ [30];
494   *ptr += 1;
495   ptr = &_ [0];
496 }
497 ptr = &_ [37];
498 while (*ptr) {
499   *ptr -= 1;
500 }
501 *ptr = 53;
502 ptr = &_ [38];
503 while (*ptr) {
504   *ptr -= 1;
505 }
506 *ptr = 228;
507 ptr = &_ [39];
508 while (*ptr) {
509   *ptr -= 1;
510 }
511 *ptr = 5;
512 ptr = &_ [40];
513 while (*ptr) {
514   *ptr -= 1;
515 }
516 *ptr = 158;
517 ptr = &_ [41];
518 while (*ptr) {
519   *ptr -= 1;
520 }
521 *ptr = 73;
522 ptr = &_ [42];
523 while (*ptr) {
524   *ptr -= 1;
525 }
526 *ptr = 123;
527 ptr = &_ [31];
528 while (*ptr) {
529   *ptr -= 1;
530   ptr = &_ [37];
531   *ptr -= 1;
532   ptr = &_ [0];
533   *ptr += 1;
534   ptr = &_ [31];
535 }
536 ptr = &_ [0];
537 while (*ptr) {
538   *ptr -= 1;
539   ptr = &_ [31];
540   *ptr += 1;
541   ptr = &_ [0];
542 }
543 ptr = &_ [32];
544 while (*ptr) {
545   *ptr -= 1;
546   ptr = &_ [38];
547   *ptr -= 1;
548   ptr = &_ [0];
549   *ptr += 1;
550   ptr = &_ [32];
551 }

```

```

1 ptr = &_ [0];
2 while (*ptr) {
3   *ptr -= 1;
4   ptr = &_ [32];
5   *ptr += 1;
6   ptr = &_ [0];

```

```

6     ptr = &_ [0];
7 }
8 ptr = &_ [33];
9 while(*ptr){
10     *ptr -= 1;
11     ptr = &_ [39];
12     *ptr -= 1;
13     ptr = &_ [0];
14     *ptr += 1;
15     ptr = &_ [33];
16 }
17 ptr = &_ [0];
18 while(*ptr){
19     *ptr -= 1;
20     ptr = &_ [33];
21     *ptr += 1;
22     ptr = &_ [0];
23 }
24 ptr = &_ [34];
25 while(*ptr){
26     *ptr -= 1;
27     ptr = &_ [40];
28     *ptr -= 1;
29     ptr = &_ [0];
30     *ptr += 1;
31     ptr = &_ [34];
32 }
33 ptr = &_ [0];
34 while(*ptr){
35     *ptr -= 1;
36     ptr = &_ [34];
37     *ptr += 1;
38     ptr = &_ [0];
39 }
40 ptr = &_ [35];
41 while(*ptr){
42     *ptr -= 1;
43     ptr = &_ [41];
44     *ptr -= 1;
45     ptr = &_ [0];
46     *ptr += 1;
47     ptr = &_ [35];
48 }
49 ptr = &_ [0];
50 while(*ptr){
51     *ptr -= 1;
52     ptr = &_ [35];
53     *ptr += 1;
54     ptr = &_ [0];
55 }
56 ptr = &_ [36];
57 while(*ptr){
58     *ptr -= 1;
59     ptr = &_ [42];
60     *ptr -= 1;
61     ptr = &_ [0];
62     *ptr += 1;
63     ptr = &_ [36];
64 }
65 ptr = &_ [0];
66 while(*ptr){
67     *ptr -= 1;
68     ptr = &_ [36];
69     *ptr += 1;
70     ptr = &_ [0];
71 }
72 ptr = &_ [43];
73 while(*ptr){
74     *ptr -= 1;
75 }
76 *ptr = 48;
77 ptr = &_ [37];
78 while(*ptr){
79     *ptr = 0;
80     ptr = &_ [43];
81     *ptr += 1;

82     ptr = &_ [37];
83     while(*ptr){
84         *ptr -= 1;
85     }
86 }
87 ptr = &_ [38];
88 while(*ptr){
89     *ptr = 0;
90     ptr = &_ [43];
91     *ptr += 1;
92     ptr = &_ [38];
93     while(*ptr){
94         *ptr -= 1;
95     }
96 }
97 ptr = &_ [39];
98 while(*ptr){
99     *ptr = 0;
100     ptr = &_ [43];
101     *ptr += 1;
102     ptr = &_ [39];
103     while(*ptr){
104         *ptr -= 1;
105     }
106 }
107 ptr = &_ [40];
108 while(*ptr){
109     *ptr = 0;
110     ptr = &_ [43];
111     *ptr += 1;
112     ptr = &_ [40];
113     while(*ptr){
114         *ptr -= 1;
115     }
116 }
117 ptr = &_ [41];
118 while(*ptr){
119     *ptr = 0;
120     ptr = &_ [43];
121     *ptr += 1;
122     ptr = &_ [41];
123     while(*ptr){
124         *ptr -= 1;
125     }
126 }
127 ptr = &_ [42];
128 while(*ptr){

```

```

128 while(*ptr){
129     *ptr = 0;
130     ptr = &_ [43];
131     *ptr += 1;
132     ptr = &_ [42];
133     while(*ptr){
134         *ptr -= 1;
135     }
136 }
137 ptr = &_ [44];
138 *ptr = getchar();
139 ptr = &_ [45];
140 *ptr = getchar();
141 ptr = &_ [46];
142 *ptr = getchar();
143 ptr = &_ [47];
144 *ptr = getchar();
145 ptr = &_ [48];
146 *ptr = getchar();
147 ptr = &_ [49];
148 *ptr = getchar();
149 ptr = &_ [50];
150 while(*ptr){
151     *ptr -= 1;
152 }
153 *ptr = 101;
154 ptr = &_ [51];
155 while(*ptr){
156     *ptr -= 1;
157 }

158 *ptr = 95;
159 ptr = &_ [52];
160 while(*ptr){
161     *ptr -= 1;
162 }
163 *ptr = 67;
164 ptr = &_ [53];
165 while(*ptr){
166     *ptr -= 1;
167 }
168 *ptr = 48;
169 ptr = &_ [54];
170 while(*ptr){
171     *ptr -= 1;
172 }
173 *ptr = 100;
174 ptr = &_ [55];
175 while(*ptr){
176     *ptr -= 1;
177 }
178 *ptr = 51;
179 ptr = &_ [44];
180 while(*ptr){
181     *ptr -= 1;
182     ptr = &_ [50];
183     *ptr -= 1;
184     ptr = &_ [0];
185     *ptr += 1;
186     ptr = &_ [44];
187 }
188 ptr = &_ [0];
189 while(*ptr){
190     *ptr -= 1;
191     ptr = &_ [44];
192     *ptr += 1;
193     ptr = &_ [0];
194 }
195 ptr = &_ [45];
196 while(*ptr){
197     *ptr -= 1;
198     ptr = &_ [51];
199     *ptr -= 1;
200     ptr = &_ [0];
201     *ptr += 1;
202     ptr = &_ [45];
203 }
204 ptr = &_ [0];
205 while(*ptr){
206     *ptr -= 1;
207     ptr = &_ [45];
208     *ptr += 1;
209     ptr = &_ [0];
210 }
211 ptr = &_ [46];
212 while(*ptr){
213     *ptr -= 1;
214     ptr = &_ [52];
215     *ptr -= 1;
216     ptr = &_ [0];
217     *ptr += 1;
218     ptr = &_ [46];
219 }
220 ptr = &_ [0];
221 while(*ptr){
222     *ptr -= 1;
223     ptr = &_ [46];
224     *ptr += 1;
225     ptr = &_ [0];
226 }
227 ptr = &_ [47];
228 while(*ptr){
229     *ptr -= 1;
230     ptr = &_ [53];
231     *ptr -= 1;
232     ptr = &_ [0];
233     *ptr += 1;

234     ptr = &_ [47];
235 }
236 ptr = &_ [0];
237 while(*ptr){
238     *ptr -= 1;
239     ptr = &_ [47];
240     *ptr += 1;
241     ptr = &_ [0];
242 }
243 ptr = &_ [48];
244 while(*ptr){
245     *ptr -= 1;
246     ptr = &_ [54];
247     *ptr -= 1;
248     ptr = &_ [0];
249     *ptr += 1;

```

```

250     ptr = &_ [48];
251 }
252 ptr = &_ [0];
253 while(*ptr){
254     *ptr -= 1;
255     ptr = &_ [48];
256     *ptr += 1;
257     ptr = &_ [0];
258 }
259 ptr = &_ [49];
260 while(*ptr){
261     *ptr -= 1;
262     ptr = &_ [55];
263     *ptr -= 1;
264     ptr = &_ [0];
265     *ptr += 1;
266     ptr = &_ [49];
267 }
268 ptr = &_ [0];
269 while(*ptr){
270     *ptr -= 1;
271     ptr = &_ [49];
272     *ptr += 1;
273     ptr = &_ [0];
274 }
275 ptr = &_ [50];
276 while(*ptr){
277     *ptr = 0;
278     ptr = &_ [43];
279     *ptr += 1;
280     ptr = &_ [50];
281     while(*ptr){
282         *ptr -= 1;
283     }
284 }
285 ptr = &_ [51];
286 while(*ptr){
287     *ptr = 0;
288     ptr = &_ [43];
289     *ptr += 1;
290     ptr = &_ [51];
291     while(*ptr){
292         *ptr -= 1;
293     }
294 }
295 ptr = &_ [52];
296 while(*ptr){
297     *ptr = 0;
298     ptr = &_ [43];
299     *ptr += 1;
300     ptr = &_ [52];
301     while(*ptr){
302         *ptr -= 1;
303     }
304 }
305 ptr = &_ [53];
306 while(*ptr){
307     *ptr = 0;
308     ptr = &_ [43];
309     *ptr += 1;
310     ptr = &_ [53];
311     while(*ptr){
312         *ptr -= 1;
313     }
314 }
315 ptr = &_ [54];
316 while(*ptr){
317     *ptr = 0;
318     ptr = &_ [43];
319     *ptr += 1;
320     ptr = &_ [54];
321     while(*ptr){
322         *ptr -= 1;
323     }
324 }
325 ptr = &_ [55];
326 while(*ptr){
327     *ptr = 0;
328     ptr = &_ [43];
329     *ptr += 1;
330     ptr = &_ [55];
331     while(*ptr){
332         *ptr -= 1;
333     }
334 }
335 ptr = &_ [43];
336 putchar(*ptr);
337 }

```

Flag

1

- 本文作者：CTFHub
- 本文链接：<https://writeup.ctfhub.com/Challenge2020/XCTF高校网络安全专题挑战赛/鲲鹏计算专场/Reverse/ihB3d4tEzw4Q5EcUkt6QBM.html>
- 版权声明： 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！

#Challenge #2020 #Reverse #XCTF高校网络安全专题挑战赛 # 鲲鹏计算专场
[mips](#)
[babyphp](#)