

[VulnHub] Brainpan: 1

Date: 31/Aug/2019

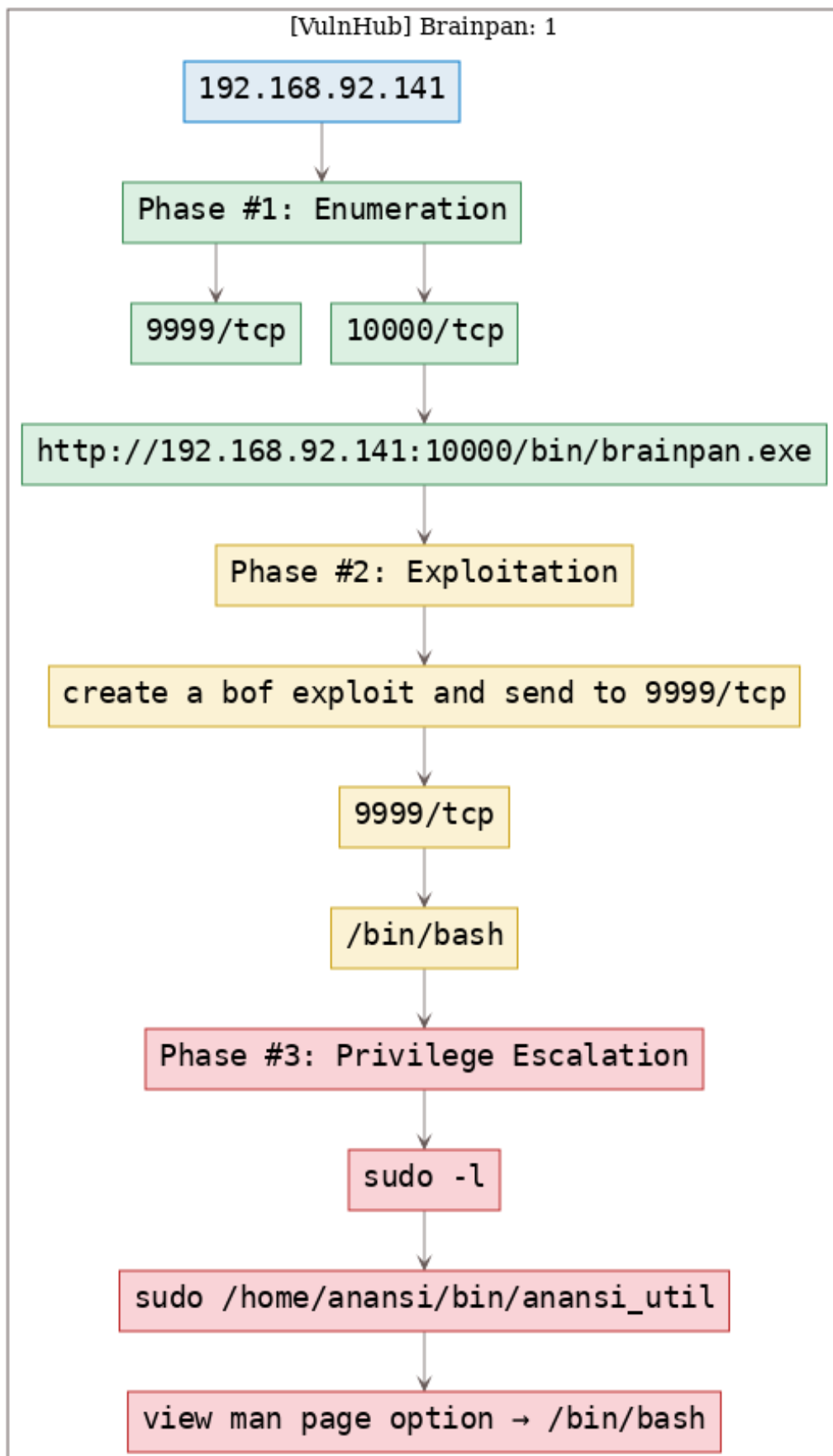
Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [exploit_bof](#), [privesc_anansi](#), [privesc_sudo](#)

Overview

This is a writeup for VulnHub VM [Brainpan: 1](#). Here's an overview of the `enumeration` → `exploitation` → `privilege escalation` process:

Killchain



TTPs

1. 9999/tcp/abyss?: [privesc_anansi](#), [privesc_sudo](#)
2. 10000/tcp/http/SimpleHTTPServer 0.6 (Python 2.7.3): [exploit_bof](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```

1 # Nmap 7.70 scan initiated Wed Jul 31 15:33:35 2019 as: nmap -vv --reason -Pn -sV -sC
2   --version-all -oN
3   /root/toolbox/vulnhub/brainpan/results/192.168.92.141/scans/_quick_tcp_nmap.txt -oX
4   /root/toolbox/vulnhub/brainpan/results/192.168.92.141/scans/xml/_quick_tcp_nmap.xml
5   192.168.92.141
6 Nmap scan report for 192.168.92.141
7 Host is up, received arp-response (0.00077s latency).
8 Scanned at 2019-07-31 15:33:36 PDT for 44s
9 Not shown: 998 closed ports
10 Reason: 998 resets
11
12 PORT      STATE SERVICE REASON      VERSION
13 9999/tcp  open  abyss?  syn-ack ttl 64
14 | fingerprint-strings:
15 |   NULL:
16 |
17 |_ _ _ _ _
18 |_ _ _ _ _
19 |_ _ _ _ _
20 |_ _ _ _ _
21 |_ _ _ _ _
22 |_ _ _ _ _
23 |_ _ _ _ _
24 |_ _ _ _ _
25 |_ _ _ _ _
26 |_ _ _ _ _
27 |_ _ _ _ _
28 |_ _ _ _ _
29 |_ _ _ _ _
30 |_ _ _ _ _
31 |_ _ _ _ _
32 |_ _ _ _ _
33 |_ _ _ _ _
34 |_ _ _ _ _
35 |_ _ _ _ _
36 |_ _ _ _ _
37 |_ _ _ _ _
38 |_ _ _ _ _
39 |_ _ _ _ _
40 |_ _ _ _ _
41 |_ _ _ _ _
42 |_ _ _ _ _
43 |_ _ _ _ _
44 |_ _ _ _ _
45 |_ _ _ _ _
46 |_ _ _ _ _
47 |_ _ _ _ _
48 |_ _ _ _ _
49 |_ _ _ _ _
50 |_ _ _ _ _
51 |_ _ _ _ _
52 |_ _ _ _ _
53 |_ _ _ _ _
54 |_ _ _ _ _
55 |_ _ _ _ _
56 |_ _ _ _ _
57 |_ _ _ _ _
58 |_ _ _ _ _
59 |_ _ _ _ _
60 |_ _ _ _ _
61 |_ _ _ _ _
62 |_ _ _ _ _
63 |_ _ _ _ _
64 |_ _ _ _ _
65 |_ _ _ _ _
66 |_ _ _ _ _
67 |_ _ _ _ _
68 |_ _ _ _ _
69 |_ _ _ _ _
70 |_ _ _ _ _
71 |_ _ _ _ _
72 |_ _ _ _ _
73 |_ _ _ _ _
74 |_ _ _ _ _
75 |_ _ _ _ _
76 |_ _ _ _ _
77 |_ _ _ _ _
78 |_ _ _ _ _
79 |_ _ _ _ _
80 |_ _ _ _ _
81 |_ _ _ _ _
82 |_ _ _ _ _
83 |_ _ _ _ _
84 |_ _ _ _ _
85 |_ _ _ _ _
86 |_ _ _ _ _
87 |_ _ _ _ _
88 |_ _ _ _ _
89 |_ _ _ _ _
90 |_ _ _ _ _
91 |_ _ _ _ _
92 |_ _ _ _ _
93 |_ _ _ _ _
94 |_ _ _ _ _
95 |_ _ _ _ _
96 |_ _ _ _ _
97 |_ _ _ _ _
98 |_ _ _ _ _
99 |_ _ _ _ _
100 |_ _ _ _ _
101 |_ _ _ _ _
102 |_ _ _ _ _
103 |_ _ _ _ _
104 |_ _ _ _ _
105 |_ _ _ _ _
106 |_ _ _ _ _
107 |_ _ _ _ _
108 |_ _ _ _ _
109 |_ _ _ _ _
110 |_ _ _ _ _
111 |_ _ _ _ _
112 |_ _ _ _ _
113 |_ _ _ _ _
114 |_ _ _ _ _
115 |_ _ _ _ _
116 |_ _ _ _ _
117 |_ _ _ _ _
118 |_ _ _ _ _
119 |_ _ _ _ _
120 |_ _ _ _ _
121 |_ _ _ _ _
122 |_ _ _ _ _
123 |_ _ _ _ _
124 |_ _ _ _ _
125 |_ _ _ _ _
126 |_ _ _ _ _
127 |_ _ _ _ _
128 |_ _ _ _ _
129 |_ _ _ _ _
130 |_ _ _ _ _
131 |_ _ _ _ _
132 |_ _ _ _ _
133 |_ _ _ _ _
134 |_ _ _ _ _
135 |_ _ _ _ _
136 |_ _ _ _ _
137 |_ _ _ _ _
138 |_ _ _ _ _
139 |_ _ _ _ _
140 |_ _ _ _ _
141 |_ _ _ _ _
142 |_ _ _ _ _
143 |_ _ _ _ _
144 |_ _ _ _ _
145 |_ _ _ _ _
146 |_ _ _ _ _
147 |_ _ _ _ _
148 |_ _ _ _ _
149 |_ _ _ _ _
150 |_ _ _ _ _
151 |_ _ _ _ _
152 |_ _ _ _ _
153 |_ _ _ _ _
154 |_ _ _ _ _
155 |_ _ _ _ _
156 |_ _ _ _ _
157 |_ _ _ _ _
158 |_ _ _ _ _
159 |_ _ _ _ _
160 |_ _ _ _ _
161 |_ _ _ _ _
162 |_ _ _ _ _
163 |_ _ _ _ _
164 |_ _ _ _ _
165 |_ _ _ _ _
166 |_ _ _ _ _
167 |_ _ _ _ _
168 |_ _ _ _ _
169 |_ _ _ _ _
170 |_ _ _ _ _
171 |_ _ _ _ _
172 |_ _ _ _ _
173 |_ _ _ _ _
174 |_ _ _ _ _
175 |_ _ _ _ _
176 |_ _ _ _ _
177 |_ _ _ _ _
178 |_ _ _ _ _
179 |_ _ _ _ _
180 |_ _ _ _ _
181 |_ _ _ _ _
182 |_ _ _ _ _
183 |_ _ _ _ _
184 |_ _ _ _ _
185 |_ _ _ _ _
186 |_ _ _ _ _
187 |_ _ _ _ _
188 |_ _ _ _ _
189 |_ _ _ _ _
190 |_ _ _ _ _
191 |_ _ _ _ _
192 |_ _ _ _ _
193 |_ _ _ _ _
194 |_ _ _ _ _
195 |_ _ _ _ _
196 |_ _ _ _ _
197 |_ _ _ _ _
198 |_ _ _ _ _
199 |_ _ _ _ _
200 |_ _ _ _ _
201 |_ _ _ _ _
202 |_ _ _ _ _
203 |_ _ _ _ _
204 |_ _ _ _ _
205 |_ _ _ _ _
206 |_ _ _ _ _
207 |_ _ _ _ _
208 |_ _ _ _ _
209 |_ _ _ _ _
210 |_ _ _ _ _
211 |_ _ _ _ _
212 |_ _ _ _ _
213 |_ _ _ _ _
214 |_ _ _ _ _
215 |_ _ _ _ _
216 |_ _ _ _ _
217 |_ _ _ _ _
218 |_ _ _ _ _
219 |_ _ _ _ _
220 |_ _ _ _ _
221 |_ _ _ _ _
222 |_ _ _ _ _
223 |_ _ _ _ _
224 |_ _ _ _ _
225 |_ _ _ _ _
226 |_ _ _ _ _
227 |_ _ _ _ _
228 |_ _ _ _ _
229 |_ _ _ _ _
230 |_ _ _ _ _
231 |_ _ _ _ _
232 |_ _ _ _ _
233 |_ _ _ _ _
234 |_ _ _ _ _
235 |_ _ _ _ _
236 |_ _ _ _ _
237 |_ _ _ _ _
238 |_ _ _ _ _
239 |_ _ _ _ _
240 |_ _ _ _ _
241 |_ _ _ _ _
242 |_ _ _ _ _
243 |_ _ _ _ _
244 |_ _ _ _ _
245 |_ _ _ _ _
246 |_ _ _ _ _
247 |_ _ _ _ _
248 |_ _ _ _ _
249 |_ _ _ _ _
250 |_ _ _ _ _
251 |_ _ _ _ _
252 |_ _ _ _ _
253 |_ _ _ _ _
254 |_ _ _ _ _
255 |_ _ _ _ _
256 |_ _ _ _ _
257 |_ _ _ _ _
258 |_ _ _ _ _
259 |_ _ _ _ _
260 |_ _ _ _ _
261 |_ _ _ _ _
262 |_ _ _ _ _
263 |_ _ _ _ _
264 |_ _ _ _ _
265 |_ _ _ _ _
266 |_ _ _ _ _
267 |_ _ _ _ _
268 |_ _ _ _ _
269 |_ _ _ _ _
270 |_ _ _ _ _
271 |_ _ _ _ _
272 |_ _ _ _ _
273 |_ _ _ _ _
274 |_ _ _ _ _
275 |_ _ _ _ _
276 |_ _ _ _ _
277 |_ _ _ _ _
278 |_ _ _ _ _
279 |_ _ _ _ _
280 |_ _ _ _ _
281 |_ _ _ _ _
282 |_ _ _ _ _
283 |_ _ _ _ _
284 |_ _ _ _ _
285 |_ _ _ _ _
286 |_ _ _ _ _
287 |_ _ _ _ _
288 |_ _ _ _ _
289 |_ _ _ _ _
290 |_ _ _ _ _
291 |_ _ _ _ _
292 |_ _ _ _ _
293 |_ _ _ _ _
294 |_ _ _ _ _
295 |_ _ _ _ _
296 |_ _ _ _ _
297 |_ _ _ _ _
298 |_ _ _ _ _
299 |_ _ _ _ _
300 |_ _ _ _ _
301 |_ _ _ _ _
302 |_ _ _ _ _
303 |_ _ _ _ _
304 |_ _ _ _ _
305 |_ _ _ _ _
306 |_ _ _ _ _
307 |_ _ _ _ _
308 |_ _ _ _ _
309 |_ _ _ _ _
310 |_ _ _ _ _
311 |_ _ _ _ _
312 |_ _ _ _ _
313 |_ _ _ _ _
314 |_ _ _ _ _
315 |_ _ _ _ _
316 |_ _ _ _ _
317 |_ _ _ _ _
318 |_ _ _ _ _
319 |_ _ _ _ _
320 |_ _ _ _ _
321 |_ _ _ _ _
322 |_ _ _ _ _
323 |_ _ _ _ _
324 |_ _ _ _ _
325 |_ _ _ _ _
326 |_ _ _ _ _
327 |_ _ _ _ _
328 |_ _ _ _ _
329 |_ _ _ _ _
330 |_ _ _ _ _
331 |_ _ _ _ _
332 |_ _ _ _ _
333 |_ _ _ _ _
334 |_ _ _ _ _
335 |_ _ _ _ _
336 |_ _ _ _ _
337 |_ _ _ _ _
338 |_ _ _ _ _
339 |_ _ _ _ _
340 |_ _ _ _ _
341 |_ _ _ _ _
342 |_ _ _ _ _
343 |_ _ _ _ _
344 |_ _ _ _ _
345 |_ _ _ _ _
346 |_ _ _ _ _
347 |_ _ _ _ _
348 |_ _ _ _ _
349 |_ _ _ _ _
350 |_ _ _ _ _
351 |_ _ _ _ _
352 |_ _ _ _ _
353 |_ _ _ _ _
354 |_ _ _ _ _
355 |_ _ _ _ _
356 |_ _ _ _ _
357 |_ _ _ _ _
358 |_ _ _ _ _
359 |_ _ _ _ _
360 |_ _ _ _ _
361 |_ _ _ _ _
362 |_ _ _ _ _
363 |_ _ _ _ _
364 |_ _ _ _ _
365 |_ _ _ _ _
366 |_ _ _ _ _
367 |_ _ _ _ _
368 |_ _ _ _ _
369 |_ _ _ _ _
370 |_ _ _ _ _
371 |_ _ _ _ _
372 |_ _ _ _ _
373 |_ _ _ _ _
374 |_ _ _ _ _
375 |_ _ _ _ _
376 |_ _ _ _ _
377 |_ _ _ _ _
378 |_ _ _ _ _
379 |_ _ _ _ _
380 |_ _ _ _ _
381 |_ _ _ _ _
382 |_ _ _ _ _
383 |_ _ _ _ _
384 |_ _ _ _ _
385 |_ _ _ _ _
386 |_ _ _ _ _
387 |_ _ _ _ _
388 |_ _ _ _ _
389 |_ _ _ _ _
390 |_ _ _ _ _
391 |_ _ _ _ _
392 |_ _ _ _ _
393 |_ _ _ _ _
394 |_ _ _ _ _
395 |_ _ _ _ _
396 |_ _ _ _ _
397 |_ _ _ _ _
398 |_ _ _ _ _
399 |_ _ _ _ _
400 |_ _ _ _ _
401 |_ _ _ _ _
402 |_ _ _ _ _
403 |_ _ _ _ _
40
```

```

49 SF:THE\x20PASSWORD\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
50 SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\n\n\x2
51 SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x
52 SF:20\x20\x20\x20\x20\x20\x20\x20>>\x20");
53 MAC Address: 00:0C:29:4F:0B:E6 (VMware)
54
55 Read data files from: /usr/bin/./share/nmap
56 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
57 # Nmap done at Wed Jul 31 15:34:20 2019 -- 1 IP address (1 host up) scanned in 45.02 seconds

```

2. Downloaded file from <http://192.168.92.141:10000/bin/brainpan.exe>.

Findings

Open Ports

```

1 9999/tcp | abyss? |
2 10000/tcp | http | SimpleHTTPServer 0.6 (Python 2.7.3)

```

Files

```

1 http://192.168.92.141:10000/bin/brainpan.exe

```

Phase #2: Exploitation

1. BoF in a vulnerable service running on 9999/tcp. File for the vulnerable service is available for download via a HTTP server running on 10000/tcp. Analyze the service, create exploit and gain remote access to VM.

[illegible]

Figure 2: writeup.exploitation.steps.1.1

Phase #2.5: Post Exploitation

```

1 puck@brainpan> id
2 uid=1002(puck) gid=1002(puck) groups=1002(puck)
3 puck@brainpan>
4 puck@brainpan> uname
5 Linux brianpan 3.5.0-25-generic #39-Ubuntu SMP Mon Feb 25 19:02:34 UTC 2013 i686 i686 i686
   ↪ GNU/Linux
6 puck@brainpan>
7 puck@brainpan> ifconfig
8 eth0 Link encap:Ethernet HWaddr 00:0c:29:4f:0b:e6
9      inet addr:192.168.92.141 Bcast:192.168.92.255 Mask:255.255.255.0
10      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
11      RX packets:10919 errors:0 dropped:0 overruns:0 frame:0
12      TX packets:342 errors:0 dropped:0 overruns:0 carrier:0
13      collisions:0 txqueuelen:1000
14      RX bytes:742406 (742.4 KB) TX bytes:39258 (39.2 KB)
15 puck@brainpan>
16 puck@brainpan> users
17 reynard
18 anansi
19 puck

```

Phase #3: Privilege Escalation

1. There's a binary, `anansi_util` that allows `sudo` access. Running the service, we see that it has 3 options, one of which is to view `man` page for any command. We use this option to escape to shell.

```
puck@brainpan:/home/puck$ sudo /home/anansi/bin/anansi_util manual test
sudo /home/anansi/bin/anansi_util manual test
No manual entry for manual
WARNING: terminal is not fully functional
- (press RETURN)/bin/bash
Cannot seek to that file position (press RETURN)
Pattern not found (press RETURN)!/bin/sh
#!/bin/sh
#

# id
id
uid=0(root) gid=0(root) groups=0(root)
#

# uname -a
uname -a
Linux brainpan 3.5.0-25-generic #39-Ubuntu SMP Mon Feb 25 19:02:34 UTC 2013 i686 i686 i686 GNU/Linux
#
```

Figure 3: writeup.privesc.steps.1.1

Loot

Hashes

```
1 root:$6$m20VT7lw$172.XYFP3mb9Fbp/┘  
  ↪ IgxPQJJkDgd0hg34jZD5sxVMix3dKq.DBwv.mw3HgCmRd0QcN4TCzaUtmx4C5DvZa.....  
2 reynard:$6$h54J.qxd$yL5md3J4d0NwNl.36┘  
  ↪ iA.mkcabQqRMmeZ0VFKxIVpXeNpfK.mvmYpYsx8W0Xq02zH8bqo2K.mkQzz55U2H.....  
3 anansi:$6$hblZfTkV$vmZoctrS1nmcdQCk5gjlmcLUb18xvJa3efaU6cpw9ho0XC/┘  
  ↪ kHupYqQ2qz50.ekVE.SwMfvRnf.QcB1lyD.....  
4 puck:$6$A/┘  
  ↪ mZxJX0$Zmgb3T6SAq.Fx01gEmbIcBF90i7q2eAi0TMMq0hg0pjdgDjBrOp2NBpIRqs40IEZB4op6ueK888lh07gc.....
```

References

- [+] <https://www.vulnhub.com/entry/brainpan-1,51/>
- [+] <https://isroot.nl/2019/05/12/vulnhub-write-up-brainpan-1/>
- [+] <https://d7x.promiselabs.net/2018/03/04/ctf-brainpan-1-ctf-walkthrough-introduction-to-exploit-development-part-i/>