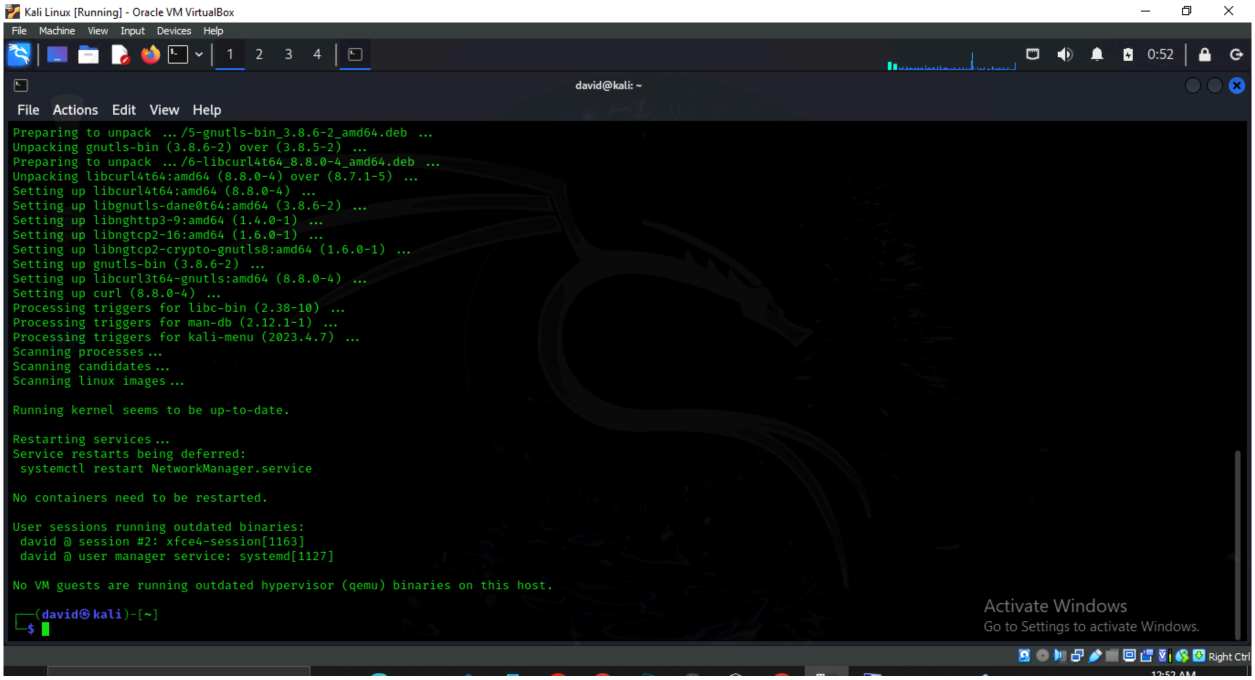
LAB 10:

How to use the Curl tool for manual information gathering.

Tool: Kali Linux

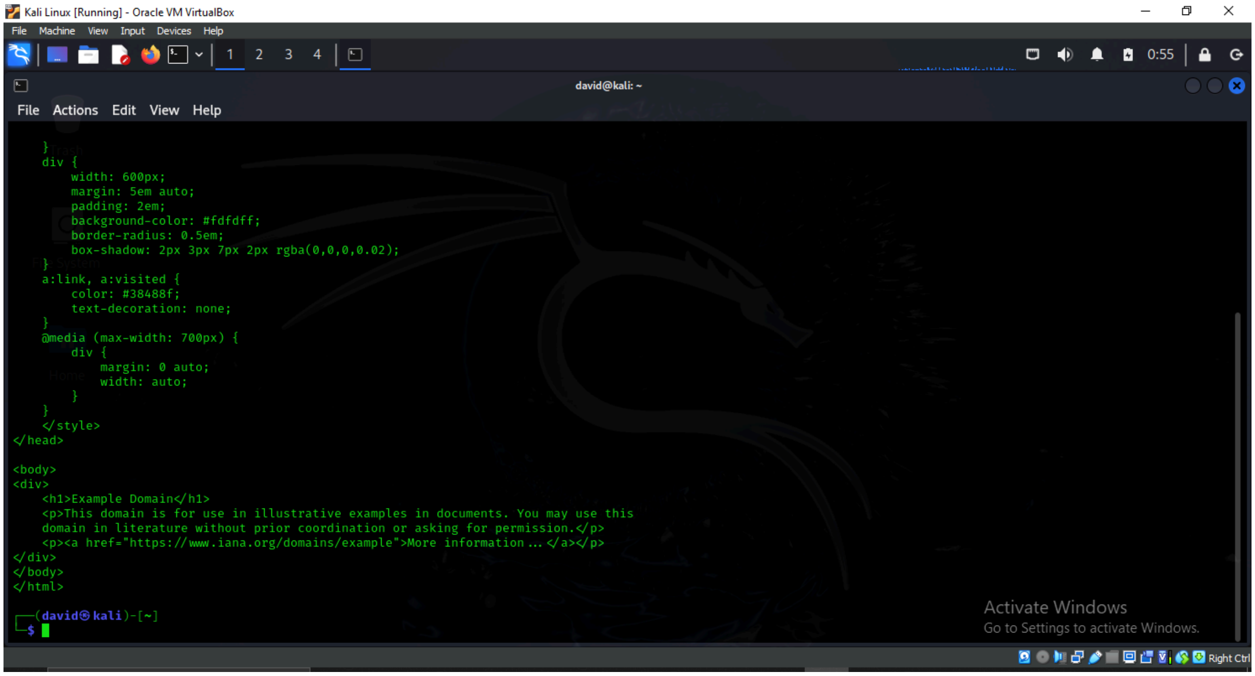
Task 1: Curl can be installed on Linux using the following command:
sudo apt-get install curl



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
0:52
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
Preparing to unpack .../5-gnutls-bin_3.8.6-2_amd64.deb ...
Unpacking gnutls-bin (3.8.6-2) over (3.8.5-2) ...
Preparing to unpack .../6-libcurl4t64_8.8.0-4_amd64.deb ...
Unpacking libcurl4t64:amd64 (8.8.0-4) over (8.7.1-5) ...
Setting up libcurl4t64:amd64 (8.8.0-4) ...
Setting up libgnutls-dane0t64:amd64 (3.8.6-2) ...
Setting up libnghttp3-9:amd64 (1.4.0-1) ...
Setting up libngtcp2-16:amd64 (1.6.0-1) ...
Setting up libngtcp2-crypto-gnutls8:amd64 (1.6.0-1) ...
Setting up gnutls-bin (3.8.6-2) ...
Setting up libcurl3t64-gnutls:amd64 (8.8.0-4) ...
Setting up curl (8.8.0-4) ...
Processing triggers for libc-bin (2.38-10) ...
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for kali-menu (2023.4.7) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...
Service restarts being deferred:
 systemctl restart NetworkManager.service

No containers need to be restarted.

User sessions running outdated binaries:
 david @ session #2: xfce4-session[1163]
 david @ user manager service: systemd[1127]

No VM guests are running outdated hypervisor (qemu) binaries on this host.

┌──(david㉿kali)-[~]
└─$ 
```

Task 2: open a terminal and type the following:
curl https://example.com



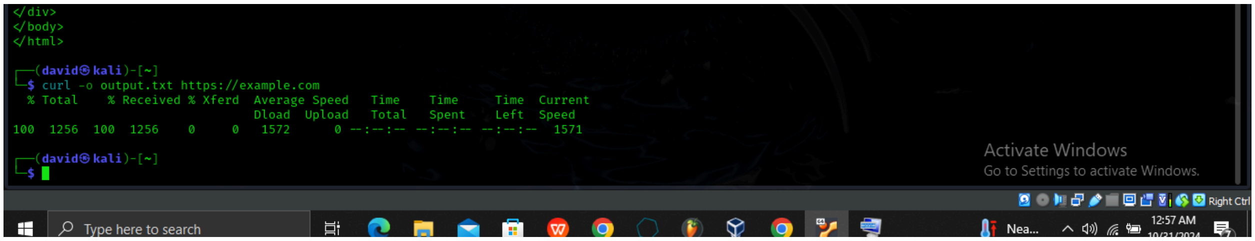
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
0:55
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
    }
    div {
        width: 600px;
        margin: 5em auto;
        padding: 2em;
        background-color: #fdfdff;
        border-radius: 0.5em;
        box-shadow: 2px 3px 7px 2px rgba(0,0,0,0.02);
    }
    a:link, a:visited {
        color: #38488f;
        text-decoration: none;
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may use this
    domain in literature without prior coordination or asking for permission.</p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></p>
</div>
</body>
</html>

┌──(david㉿kali)-[~]
└─$ 
```

To save this output to a file, we will use either the “-o” or “-O” option. The lowercase option saves the file with a predefined filename, while the uppercase option saves the file with its original filename.

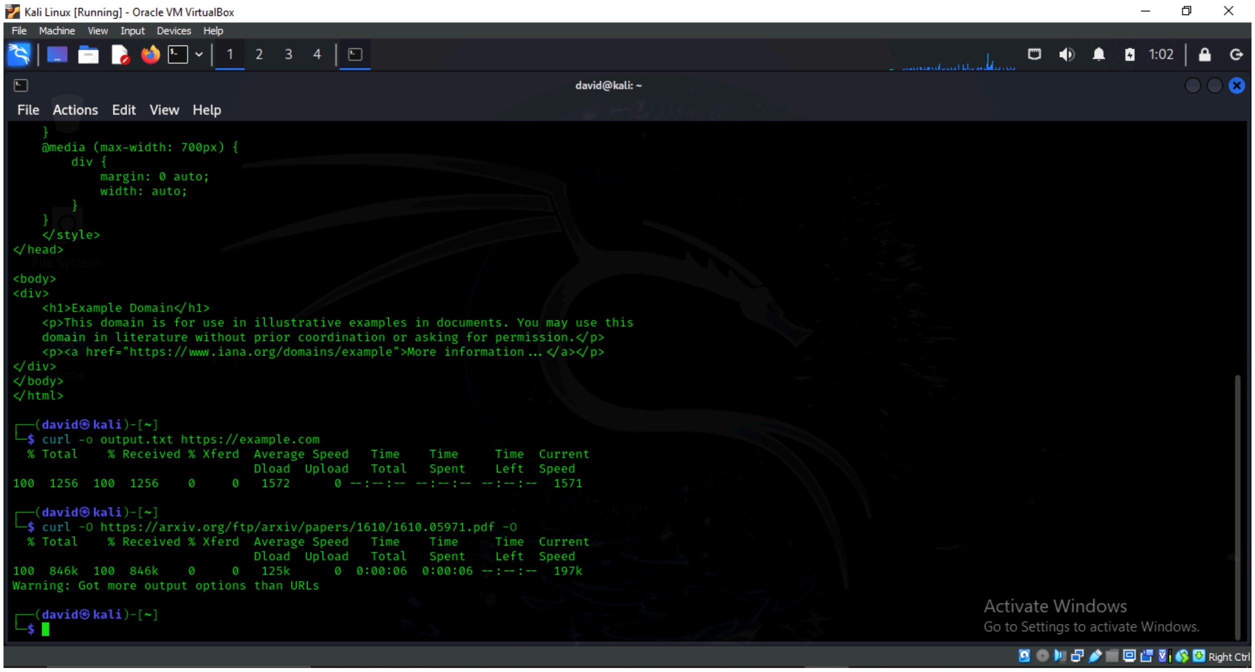
Type the following to save your output:

curl -o output.txt https://example.com



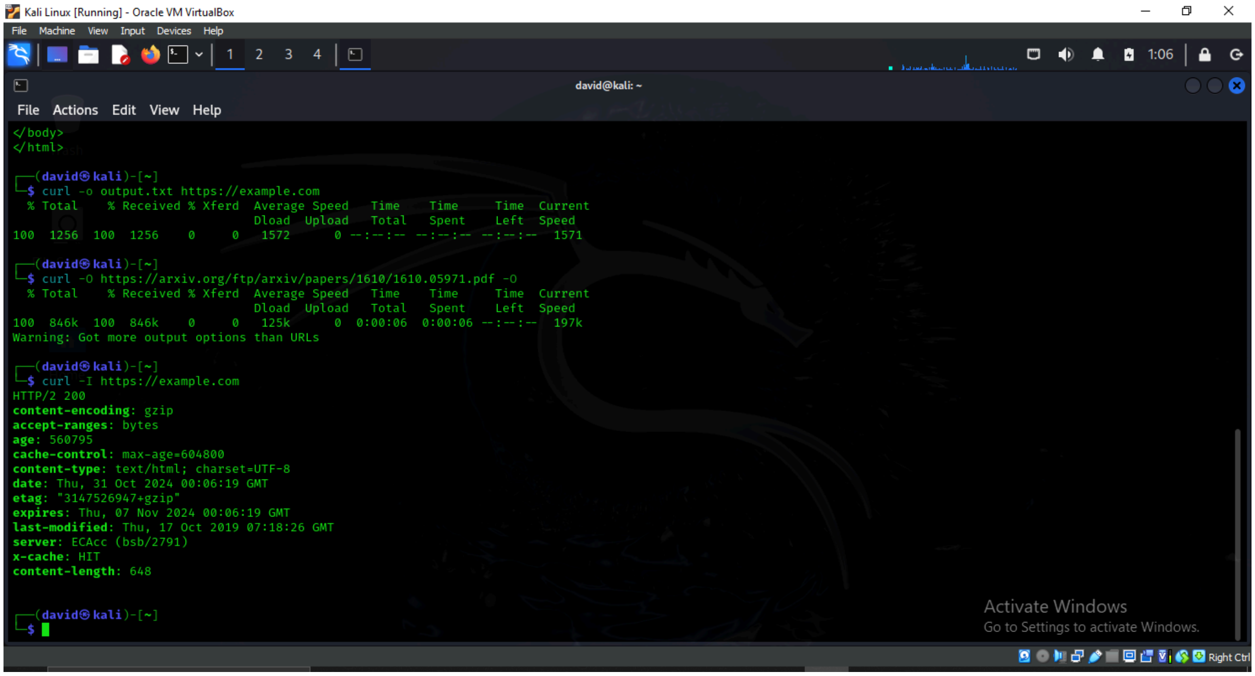
```
</div>
</body>
</html>

┌──(david㉿kali)-[~]
└─$ curl -o output.txt https://example.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1256  100  1256    0     0   1572      0 --:--:-- --:--:-- --:--:--  1571

┌──(david㉿kali)-[~]
└─$ 
```

Task 3: Curl also provides you with the ability to download multiple files at once. To do this, use multiple -O options, followed by the URL of the file you want to download. For example:
curl -O https://arxiv.org/ftp/arxiv/papers/1610/1610.05971.pdf -O


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:02
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

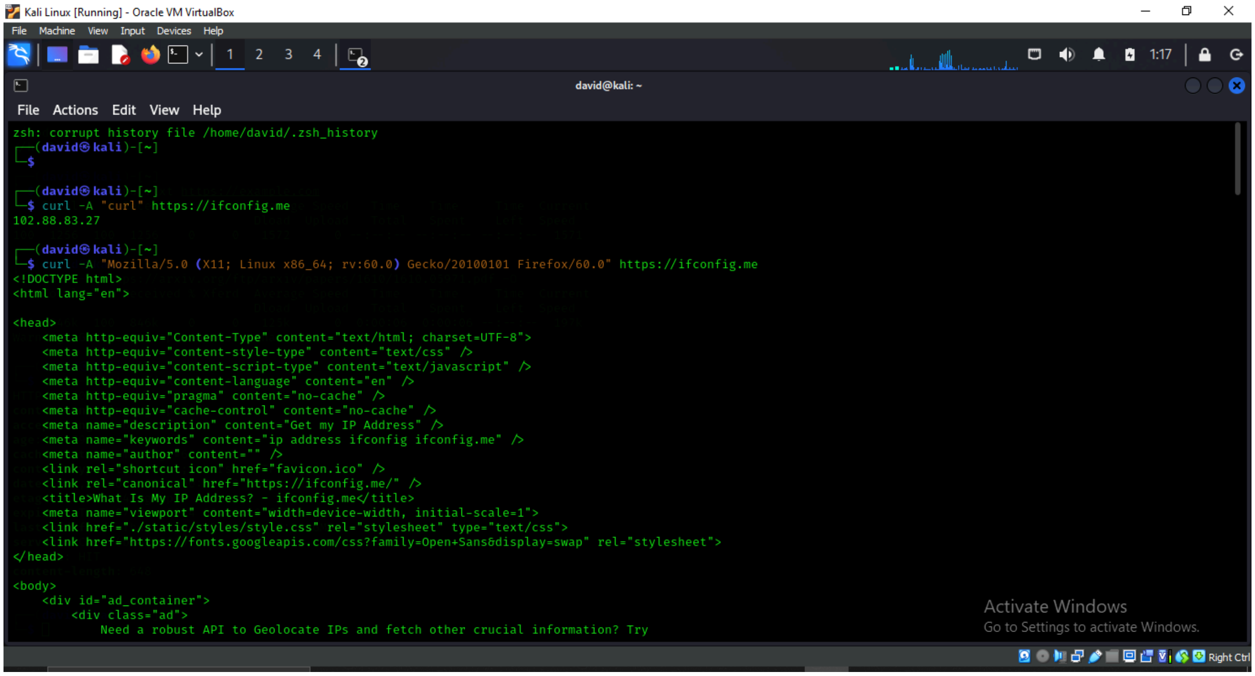
```
    }
    @media (max-width: 700px) {
        div {
            margin: 0 auto;
            width: auto;
        }
    }
    </style>
</head>

<body>
<div>
    <h1>Example Domain</h1>
    <p>This domain is for use in illustrative examples in documents. You may use this
    domain in literature without prior coordination or asking for permission.</p>
    <p><a href="https://www.iana.org/domains/example">More information...</a></p>
</div>
</body>
</html>

┌──(david㉿kali)-[~]
└─$ curl -o output.txt https://example.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1256  100  1256    0     0   1572      0 --:--:-- --:--:-- --:--:--  1571

┌──(david㉿kali)-[~]
└─$ curl -O https://arxiv.org/ftp/arxiv/papers/1610/1610.05971.pdf -O
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  846k  100  846k    0     0   125k      0  0:00:06  0:00:06 --:--:--  197k
Warning: Got more output options than URLs

┌──(david㉿kali)-[~]
└─$ 
```

Task 4: Curl can also be useful for downloading HTTP headers, which is useful when testing a site. To do this,use the following command: curl -I https://example.com


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:06
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

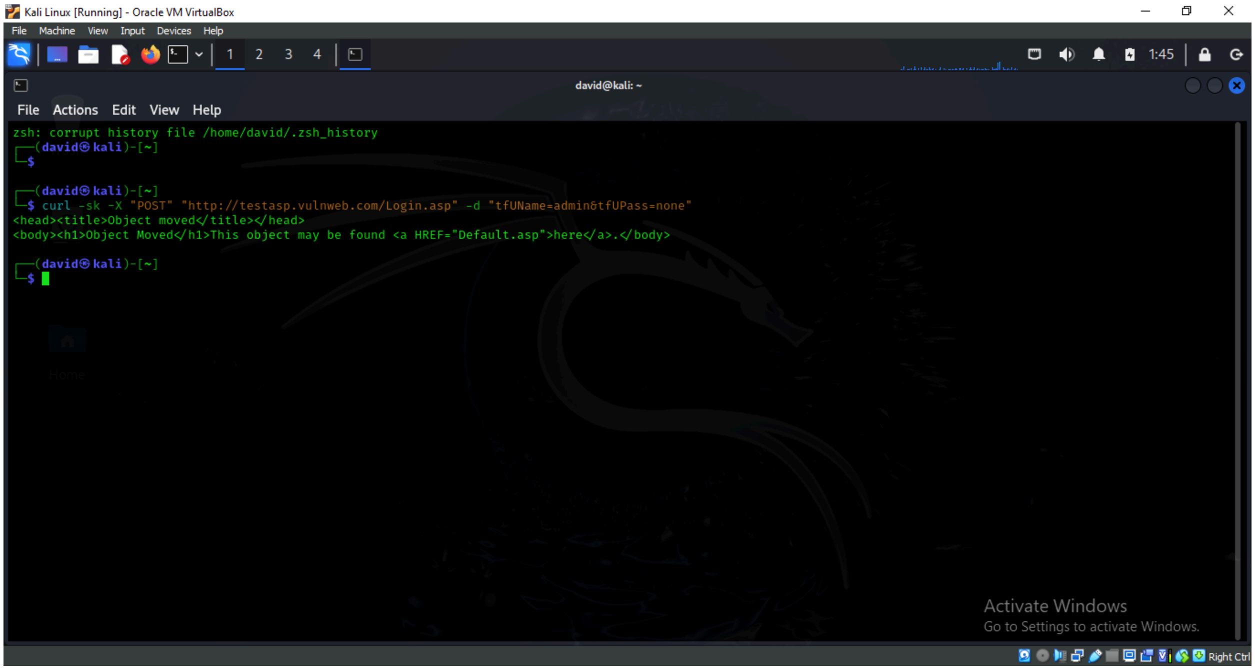
```
</body>
</html>

┌──(david㉿kali)-[~]
└─$ curl -o output.txt https://example.com
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  1256  100  1256    0     0   1572      0 --:--:-- --:--:-- --:--:--  1571

┌──(david㉿kali)-[~]
└─$ curl -O https://arxiv.org/ftp/arxiv/papers/1610/1610.05971.pdf -O
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  846k  100  846k    0     0   125k      0  0:00:06  0:00:06 --:--:--  197k
Warning: Got more output options than URLs

┌──(david㉿kali)-[~]
└─$ curl -I https://example.com
HTTP/2 200
content-encoding: gzip
accept-ranges: bytes
age: 560795
cache-control: max-age=604800
content-type: text/html; charset=UTF-8
date: Thu, 31 Oct 2024 00:06:19 GMT
etag: "3147526947+gzip"
expires: Thu, 07 Nov 2024 00:06:19 GMT
last-modified: Thu, 17 Oct 2019 07:18:26 GMT
server: ECAcc (bsb/2791)
x-cache: HIT
content-length: 648


┌──(david㉿kali)-[~]
└─$ 
```

Task 5: When attempting to download a file or gather other information using curl, you may discover that the target site may be designed to block curl. In this case, it is useful to emulate a browser, such as Firefox, to return the information you are looking for. To do this, use the following command:
curl -A “curl” https://ifconfig.me
curl -A “Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0” https://ifconfig.me


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:17
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
zsh: corrupt history file /home/david/.zsh_history
┌──(david㉿kali)-[~]
└─$

┌──(david㉿kali)-[~]
└─$ curl -A "curl" https://ifconfig.me
102.88.83.27

┌──(david㉿kali)-[~]
└─$ curl -A "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0" https://ifconfig.me
<!DOCTYPE html>
<html lang="en">

<head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <meta http-equiv="content-style-type" content="text/css" />
    <meta http-equiv="content-script-type" content="text/javascript" />
    <meta http-equiv="content-language" content="en" />
    <meta http-equiv="pragma" content="no-cache" />
    <meta http-equiv="cache-control" content="no-cache" />
    <meta name="description" content="Get my IP Address" />
    <meta name="keywords" content="ip address ifconfig ifconfig.me" />
    <meta name="author" content="" />
    <link rel="shortcut icon" href="favicon.ico" />
    <link rel="canonical" href="https://ifconfig.me/" />
    <title>What Is My IP Address? - ifconfig.me</title>
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="./static/styles/style.css" rel="stylesheet" type="text/css">
    <link href="https://fonts.googleapis.com/css?family=Open+Sans&display=swap" rel="stylesheet">
</head>

<body>
    <div id="ad_container">
        <div class="ad">
            Need a robust API to Geolocate IPs and fetch other crucial information? Try
```

Task 6: Curl can also be used for sending HTTP POST data to FORM pages. In this example, we are sending two parameters, “tfUName” and “tfUPass”, with attached values to “http://testasp.vulnweb.com/Login.asp”.



Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
1:45
david@kali: ~
File Actions Edit View Help
Activate Windows
Go to Settings to activate Windows.
Right Ctrl

```
zsh: corrupt history file /home/david/.zsh_history
┌──(david㉿kali)-[~]
└─$

┌──(david㉿kali)-[~]
└─$ curl -sk -X "POST" "http://testasp.vulnweb.com/Login.asp" -d "tfUName=admin&tfUPass=none"
<head><title>Object moved</title></head>
<body><h1>Object Moved</h1>This object may be found <a HREF="Default.asp">here</a>.</body>

┌──(david㉿kali)-[~]
└─$
```