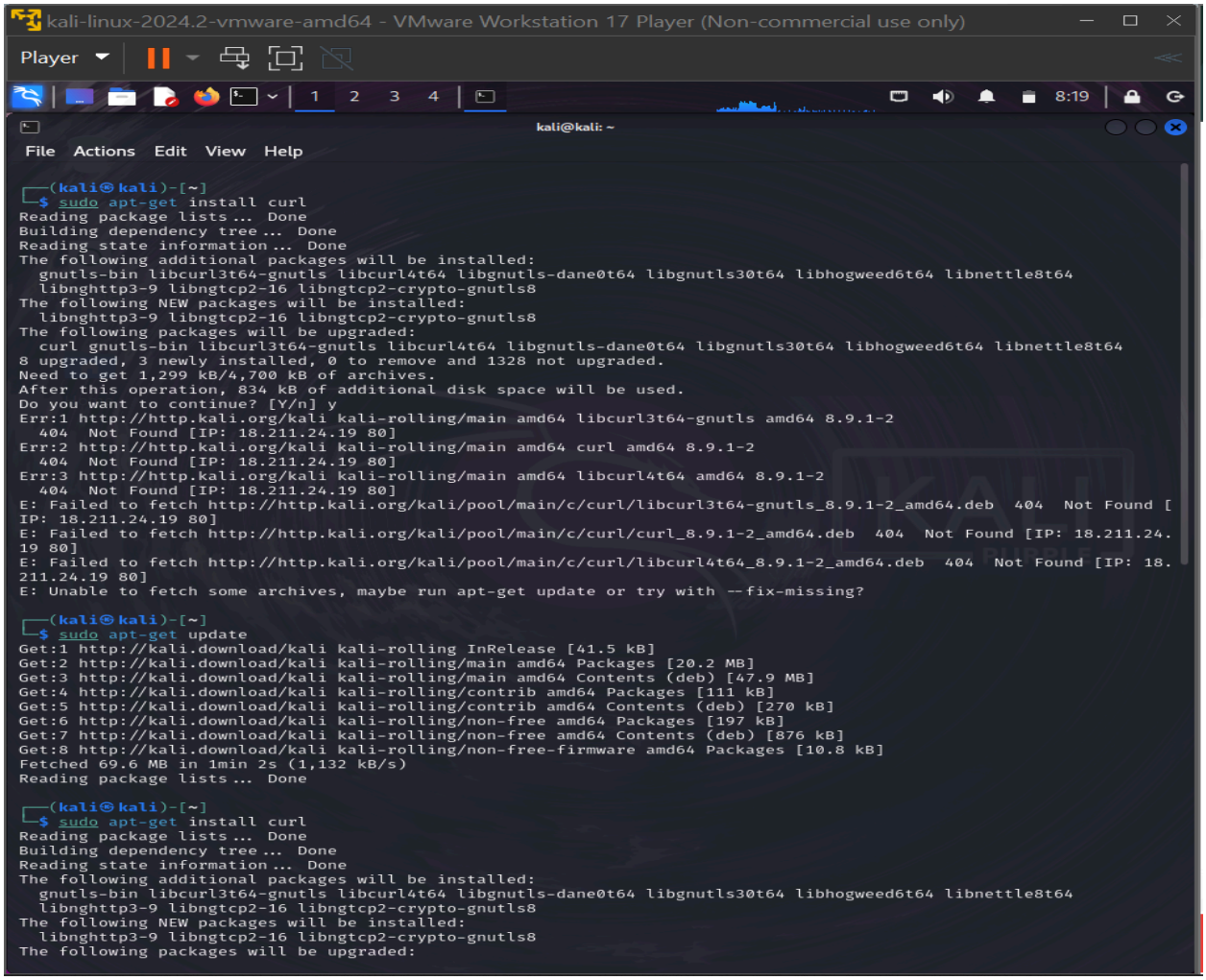
USING CURL TOOL FOR MANUAL INFORMATION GATHERING

Tools : KALI LINUX [CURL]
Project-Site : https://example.com, http://testasp.vulnweb.com

The `curl` tool is a command-line utility used to transfer data to or from a server using various protocols, including HTTP, HTTPS, FTP, and more. It's commonly used for testing APIs, downloading files, or sending data in web requests.

Input from Kali : CURL



kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player

1 2 3 4 8:20

kali@kali: ~

File Actions Edit View Help

```
The following packages will be upgraded:
  curl gnutls-bin libcurl3t64-gnutls libcurl4t64 libgnutls-dane0t64 libgnutls30t64 libhogweed6t64 libnettle8t64
8 upgraded, 3 newly installed, 0 to remove and 1431 not upgraded.
Need to get 964 kB/4,365 kB of archives.
After this operation, 517 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libcurl3t64-gnutls amd64 8.10.1-2 [360 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 curl amd64 8.10.1-2 [252 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 libcurl4t64 amd64 8.10.1-2 [352 kB]
Fetched 964 kB in 3s (333 kB/s)
(Reading database ... 406050 files and directories currently installed.)
Preparing to unpack .../libnettle8t64_3.10-1_amd64.deb ...
Unpacking libnettle8t64:amd64 (3.10-1) over (3.9.1-2.2) ...
Setting up libnettle8t64:amd64 (3.10-1) ...
(Reading database ... 406050 files and directories currently installed.)
Preparing to unpack .../libhogweed6t64_3.10-1_amd64.deb ...
Unpacking libhogweed6t64:amd64 (3.10-1) over (3.9.1-2.2) ...
Setting up libhogweed6t64:amd64 (3.10-1) ...
(Reading database ... 406050 files and directories currently installed.)
Preparing to unpack .../libgnutls-dane0t64_3.8.6-2_amd64.deb ...
Unpacking libgnutls-dane0t64:amd64 (3.8.6-2) over (3.8.5-2) ...
Preparing to unpack .../libgnutls30t64_3.8.6-2_amd64.deb ...
Unpacking libgnutls30t64:amd64 (3.8.6-2) over (3.8.5-2) ...
Setting up libgnutls30t64:amd64 (3.8.6-2) ...
Selecting previously unselected package libnghttp3-9:amd64.
(Reading database ... 406050 files and directories currently installed.)
Preparing to unpack .../0-libnghttp3-9_1.4.0-1_amd64.deb ...
Unpacking libnghttp3-9:amd64 (1.4.0-1) ...
Selecting previously unselected package libngtcp2-16:amd64.
Preparing to unpack .../1-libngtcp2-16_1.6.0-1_amd64.deb ...
Unpacking libngtcp2-16:amd64 (1.6.0-1) ...
Selecting previously unselected package libngtcp2-crypto-gnutls8:amd64.
Preparing to unpack .../2-libngtcp2-crypto-gnutls8_1.6.0-1_amd64.deb ...
Unpacking libngtcp2-crypto-gnutls8:amd64 (1.6.0-1) ...
Preparing to unpack .../3-libcurl3t64-gnutls_8.10.1-2_amd64.deb ...
Unpacking libcurl3t64-gnutls:amd64 (8.10.1-2) over (8.7.1-5) ...
Preparing to unpack .../4-curl_8.10.1-2_amd64.deb ...
Unpacking curl (8.10.1-2) over (8.7.1-5) ...
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_8.10.1-2_amd64.deb ...
Unpacking libcurl4t64:amd64 (8.10.1-2) over (8.7.1-5) ...
Setting up libcurl4t64:amd64 (8.10.1-2) ...
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 (8.10.1-2) ...
Setting up curl (8.10.1-2) ...
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) ...

┌──(kali㉿kali)-[~]
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player

1 2 3 4 8:53

kali@kali: ~

File Actions Edit View Help

```
Processing triggers for man-db (2.12.1-1) ...
Processing triggers for kali-menu (2023.4.7) ...

┌──(kali㉿kali)-[~]
└─$ curl https://example.com
<!doctype html>
<html>
<head>
    <title>Example Domain</title>

    <meta charset="utf-8" />
    <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1" />
    <style type="text/css">
    body {
        background-color: #f0f0f2;
        margin: 0;
        padding: 0;
        font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI", "Open Sans", "Helvetica Neue", Helvet
ica, Arial, sans-serif;

    }
    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>

┌──(kali㉿kali)-[~]
└─$
```

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)

Player

1 2 3 4 8:59

kali@kali: ~

File Actions Edit View Help

```
    <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>

┌──(kali㉿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    213      0  0:00:05  0:00:05 --:--:--   271

┌──(kali㉿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  70908      0  0:00:12  0:00:12 --:--:--  129k
Warning: Got more output options than URLs

┌──(kali㉿kali)-[~]
└─$ curl -O https://arxiv.org/ftp/arxiv/papers/1610/1610.05971.pdf -O https://arxiv.org/pdf/2103.08624.pdf
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  846k  100  846k    0     0   196k      0  0:00:04  0:00:04 --:--:--  196k
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   249  100   249    0     0    712      0 --:--:-- --:--:-- --:--:--   713

┌──(kali㉿kali)-[~]
└─$ curl -C- -O https://arxiv.org/pdf/2103.08624.pdf
** Resuming transfer from byte position 249
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0   249    0     0    0     0      0      0 --:--:--  0:00:03 --:--:--     0

┌──(kali㉿kali)-[~]
└─$ curl -I https://example.com
HTTP/2 200
content-encoding: gzip
accept-ranges: bytes
age: 584184
cache-control: max-age=604800
content-type: text/html; charset=UTF-8
date: Thu, 24 Oct 2024 12:58:45 GMT
etag: "3147526947+gzip"
expires: Thu, 31 Oct 2024 12:58:45 GMT
last-modified: Thu, 17 Oct 2019 07:18:26 GMT
server: ECAcc (bsb/278E)
x-cache: HIT
content-length: 648

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ curl -k "http://192.168.1.1"
curl: (28) Failed to connect to 192.168.1.1 port 80 after 134322 ms: Could not connect to server

┌──(kali㉿kali)-[~]
└─$ curl -u "username:pwd" "ftp://mirrors.sonic.net/knoppix/live.iso"

curl: (67) Access denied: 530

┌──(kali㉿kali)-[~]
└─$
```

```
└─$ curl -s -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>

┌──(kali㉿kali)-[~]
└─$
```

RESULT AND PROCEDURES ON HOW TO USE THE CURL TOOL.

Here we used the CURL tool for manual information gathering. CURL stands for Client URL. It is a command line tool for getting and sending data including files using URL syntax.

The general syntax for using curl is the following:

Curl [options] URL

This is a basic syntax that makes the tool quite simple to use. To get some more information on curl and how it is used, type curl –help to display the information screen.

We began by installing CURL with the following command [sudo apt-get install curl], then we performed our first task that is getting the source code of a site by entering the following [curl https://example.com], in the first picture we can see a raw html output, 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. Basically, the lowercase option allows us to specify a file name. This is a useful option if the webpage we are trying to inspect is preventing us from right clicking on the page to view the source code in the browser. Type the following to save your output:[curl -o output.txt https://example.com]. In
Image 4 we can see some brief statistical data on this output.

Curl can also be used to provide us with the ability to download multiple files at once. To do this, we are going to use multiple -O options, followed by the URL of the file you want to download. To do this we would enter the following command [curl -O https://arxiv.org/ftp/arxiv/papers/1610/1610.05971.pdf -O https://arxiv.org/pdf/2103.08624.pdf]. If connections drop while

downloading a file, we can resume the download with the -C- option. This is a useful feature when downloading large sized files, ex DVD ISO files, or mp4 video files. This way, if your connection drops when downloading a file, you can resume the download instead of starting from scratch, using curl [-C- -O https://arxiv.org/pdf/2103.08624.pdf].

Curl can also be useful for downloading HTTP headers, which is useful when testing a site. We can use the following commands to do that for example [curl -I https://example.com] This will display many useful pieces of information, such as server info, content type, and content encoding.

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 “Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0” https://ifconfig.me]

Another important feature of curl is its ability to transfer files. This is useful when interacting with servers through the command line, particularly if you are trying to take advantage of potential vulnerabilities. To access a protected FTP server, we would use the -u option to specify the username and password: [curl -u “username:pwd” “ftp://mirrors.sonic.net/knoppix/live.iso”]

To upload a file to the server, we can use the -T option: [curl -T file.zip -u “username:password” ftp://mirrors.sonic.net/]. Here we can see that curl denied connecting to sites which have invalid SSL certificates. To connect without blocking and getting a warning message, we can use the “–k” option, for example: [curl -k http://192.168.1.1/]

Curl can also be configured to use a proxy. To do this, use the -x option followed by the proxy URL. For example:[curl -x 192.168.0.1:8080 http://example.com/].

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”. We can use the following command for that [curl -sK -X “POST” “http://testasp.vulnweb.com/login.asp” -d “tfUName=admin&tfUPass=none”]. Our results are in the last image.