Pentesting Fundamentals

Learn the important ethics and methodologies behind every pentest.

Task 2 Penetration Testing Ethics

Question	Answer
You are given permission to perform a security audit on an organisation; what type of hacker would you be?	white hat
You attack an organisation and steal their data, what type of hacker would you be?	black hat
What document defines how a penetration testing engagement should be carried out?	Rules of Engagement

Task 3 Penetration Testing Methodologies

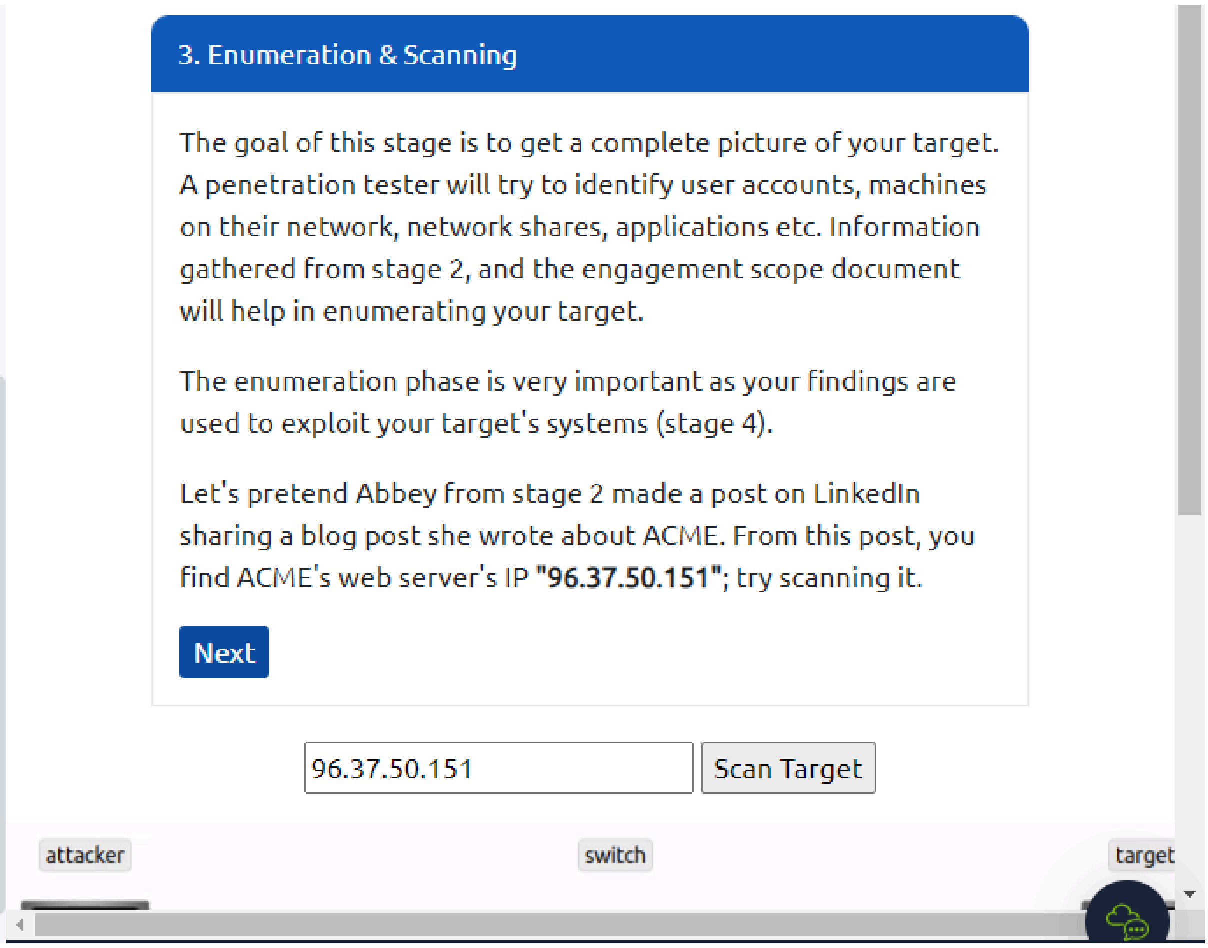
Question	Answer
What stage of penetration testing involves using publicly available information?	Information Gathering
If you wanted to use a framework for pentesting telecommunications, what framework would you use? Note: We're looking for the acronym here and not the full name.	OSSTMM
What framework focuses on the testing of web applications?	OWASP

Task 4 Black box, White box, Grey box Penetration Testing

Question	Answer
You are asked to test an application but are not given access to its source code - what testing process is this?	Black box
You are asked to test a website, and you are given access to the source code - what testing process is this?	white box

Task 5 Practical: ACME Penetration Test

- ➔ I clicked on the “View Site” button
- ➔ I read through and clicked on next
- ➔ On getting to Enumeration and scanning, i entered the ip address



3. Enumeration & Scanning

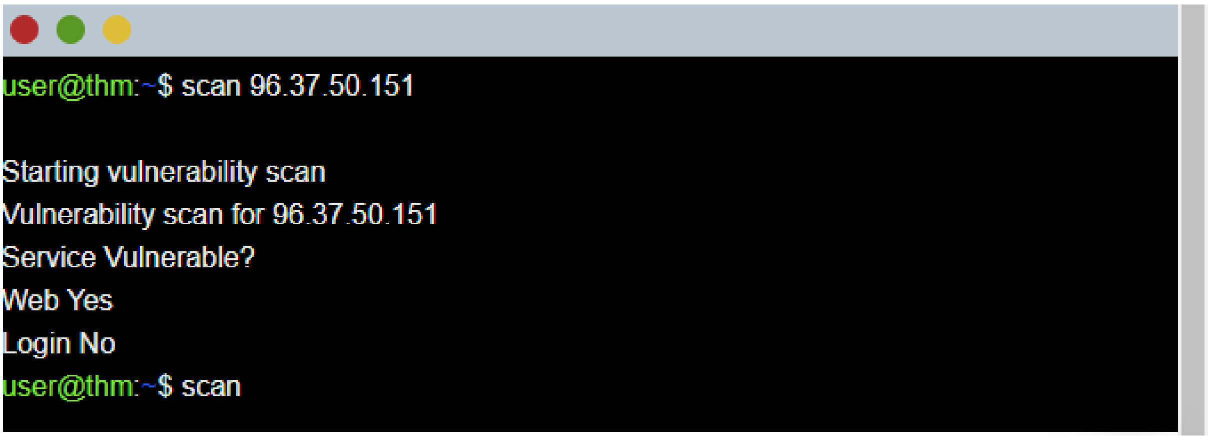
The goal of this stage is to get a complete picture of your target. A penetration tester will try to identify user accounts, machines on their network, network shares, applications etc. Information gathered from stage 2, and the engagement scope document will help in enumerating your target.

The enumeration phase is very important as your findings are used to exploit your target's systems (stage 4).

Let's pretend Abbey from stage 2 made a post on LinkedIn sharing a blog post she wrote about ACME. From this post, you find ACME's web server's IP **"96.37.50.151"**; try scanning it.

96.37.50.151

➔ My scan result shows vulnerabilities in its web service

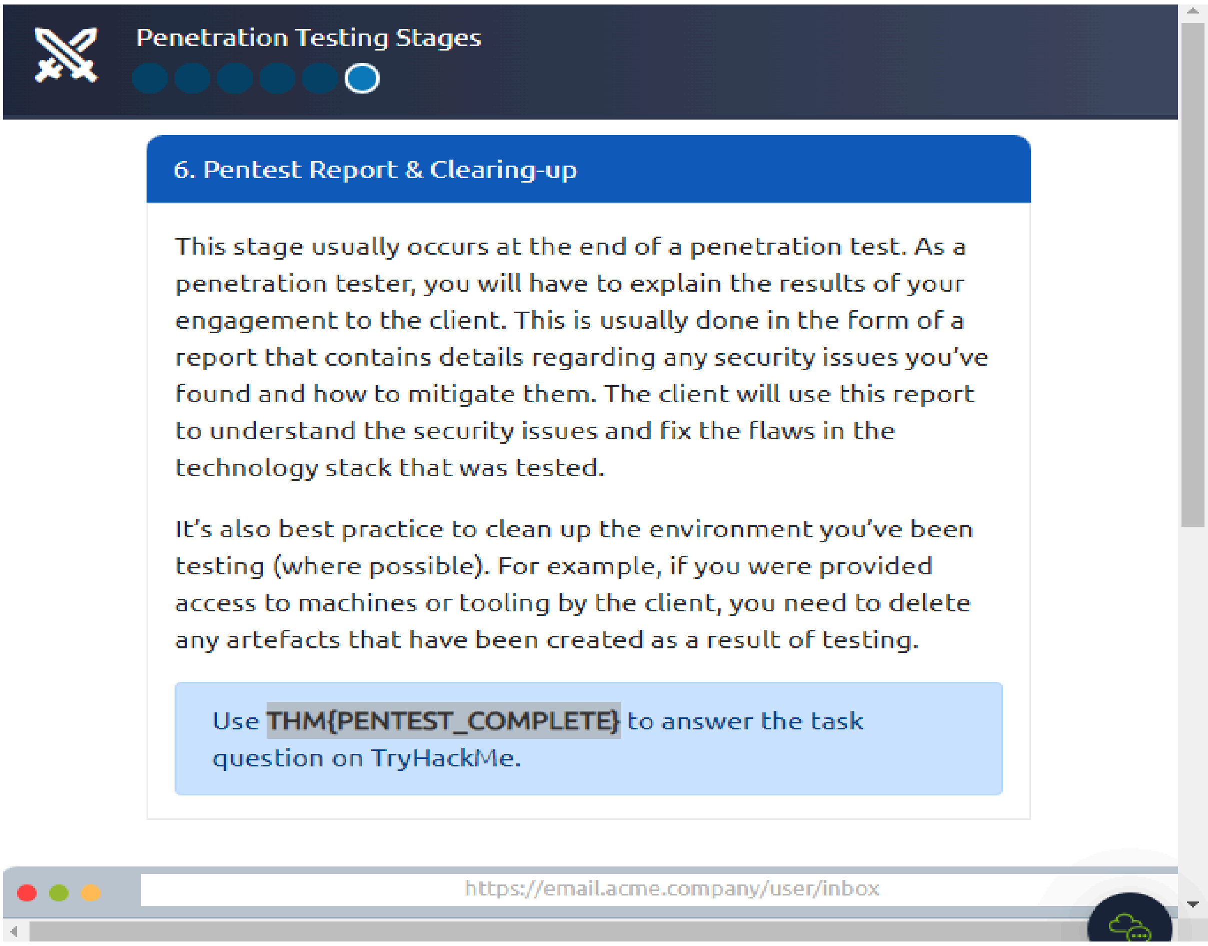


```
user@thm:~$ scan 96.37.50.151

Starting vulnerability scan
Vulnerability scan for 96.37.50.151
Service Vulnerable?
Web Yes
Login No
user@thm:~$ scan
```

➔ I read through and clicked on next until i got the flag

Answer/Flag:THM{PENTEST_COMPLETE}



Penetration Testing Stages

6. Pentest Report & Clearing-up

This stage usually occurs at the end of a penetration test. As a penetration tester, you will have to explain the results of your engagement to the client. This is usually done in the form of a report that contains details regarding any security issues you've found and how to mitigate them. The client will use this report to understand the security issues and fix the flaws in the technology stack that was tested.

It's also best practice to clean up the environment you've been testing (where possible). For example, if you were provided access to machines or tooling by the client, you need to delete any artefacts that have been created as a result of testing.

Use THM{PENTEST_COMPLETE} to answer the task question on TryHackMe.

END!!!