# Exercise: Penetration testing strategy

## Introduction

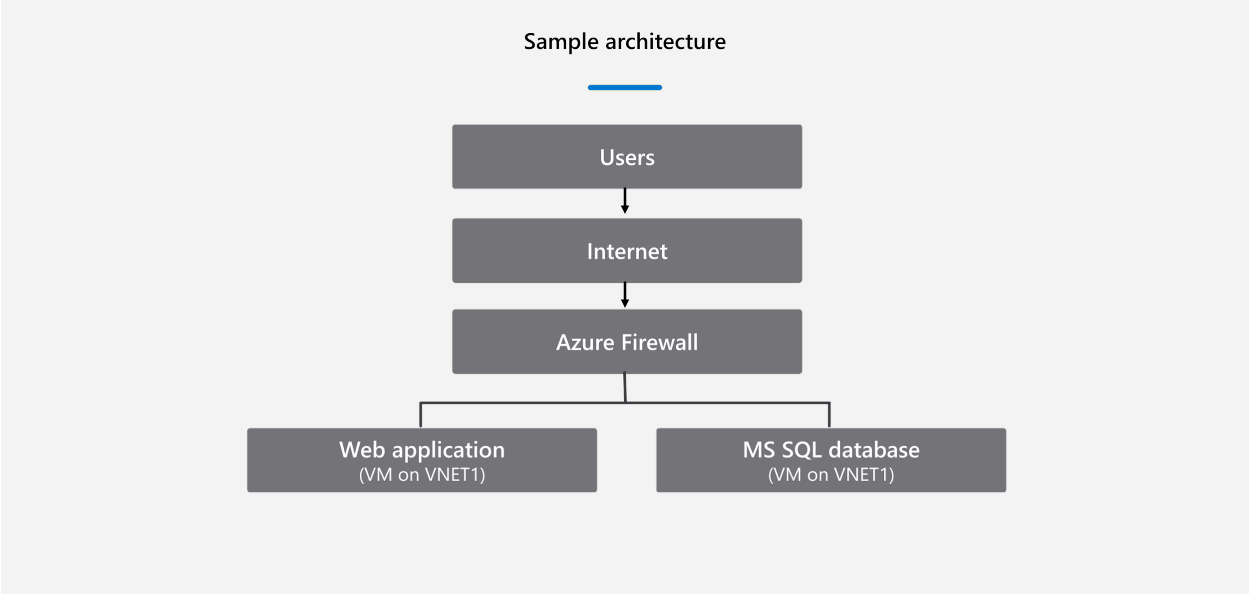
Throughout your learning journey, you have gained valuable insights into the significance of penetration testing in evaluating and improving the security of digital systems. You have explored different methodologies, stages, and techniques to identify vulnerabilities and fortify defenses against potential cyber threats.

Now it's time to put your knowledge into practice with a real-world scenario. In this exercise, your objective is to develop a penetration testing strategy that encompasses the various stages and tasks aligned with the given case study.

By completing this exercise, you will strengthen your skills in penetration testing and reinforce your understanding of the methodologies and techniques involved.

## Case study

Sam's Scoops is a popular online ice cream retailer that has built its eCommerce platform on a virtual machine (VM) hosted on Microsoft Azure. The company stores its customer and product data in a Microsoft SQL Server database, which runs on another Azure VM. To enhance the security of their infrastructure, Sam's Scoops has implemented Azure Firewall and Web Application Firewall (WAF).




## Architecture overview

### Virtual machine 1: eCommerce platform

This VM hosts Sam's Scoops' eCommerce platform, which handles customer orders, product catalog, and website functionalities. It is connected to a virtual network (VNet 1) in Azure to enable communication with other resources.

Azure Firewall and WAF will be deployed to protect this VM and monitor incoming traffic.

### Virtual machine 2: MS SQL Server

This VM hosts the Microsoft SQL Server database that stores customer information, order details, and product inventory for the eCommerce platform. It is connected to the same VNet as the eCommerce VM to allow secure communication between the two.

### Azure Firewall

Azure Firewall is deployed as a network security service that provides inbound and outbound traffic filtering and network address translation (NAT). It serves as the main gateway for the eCommerce VM and MS SQL Server VM, controlling access to and from the internet.
Azure Firewall rules is configured to allow necessary traffic and block unauthorized access attempts. Web Application Firewall (WAF) The WAF component is integrated with Azure Firewall and provides an additional layer of security specifically for web applications. It helps protect the eCommerce platform from common web application vulnerabilities and provides real-time threat intelligence. WAF rules will be configured to detect and block malicious web traffic, such as SQL injection or cross-site scripting (XSS) attacks.
By implementing Azure Firewall and WAF, Sam's Scoops aims to enhance the security posture of its Azure infrastructure. The combination of these services allows for robust network security, protection against web application attacks, and improved control over inbound and outbound traffic.
The next steps for Sam's Scoops involves conducting reconnaissance, enumeration, exploitation, and escalation testing to identify and address any vulnerabilities in its infrastructure, followed by reporting and remediation based on the penetration testing findings.

# Instructions

Your task is to create a comprehensive testing strategy that outlines the steps and tools for implementing a penetration test. Additionally, you need to classify the type of testing involved as black box testing, grey box testing, or white box testing.

# Guidelines: Creating the strategy

Preparing a task list for the penetration testing strategy requires careful planning and consideration of the penetration testing stages.
Follow the guidelines below for creating an effective and structured testing strategy.

### Understand the scenario

To begin, familiarize yourself with the provided case study:

- Take note of the organization's name (Sam's Scoop) and the Azure infrastructure details.
- Review the architecture overview, including the involved virtual machines (eCommerce Platform and MS SQL Server) and security components (Azure Firewall and WAF).

### Review penetration testing stages

Refresh your understanding of the penetration testing stages mentioned in the situation. You can revisit the following resources should you require further assistance:

- Stage 1 - Reconnaissance

- Stage 2 –Enumeration
- Stage 3 – Exploitation
- Stage 4 –Escalation
- Stage 5 – Report and remediation

## Define task categories

Divide the task list into categories corresponding to each stage of the penetration testing process:

- Create categories for reconnaissance, enumeration, exploitation, escalation, and reporting and remediation.

## Identify stage-specific tasks

Under each category, list specific tasks that align with the respective penetration testing stage. For example, under reconnaissance, tasks may include passive reconnaissance, active reconnaissance, and gathering specific information.

## Specify tools and techniques

For each task, identify the tools and techniques that can be used to accomplish it. Consider the tools mentioned in the fictional situation and those you have learned or researched.

## Add classification of testing type

Determine whether the type of testing involved is black box testing, grey box testing, or white box testing based on the level of knowledge and access provided.
You can revisit the following resources should you require further assistance:

- Black box testing
- White box testing
- Grey box testing

## Consider logical flow

Arrange the tasks in a logical order that follows the natural progression of a penetration test. Typically, reconnaissance comes first, followed by enumeration, exploitation, escalation, and reporting/remediation.

## Validate task list

Review the task list to ensure it covers all essential steps and aligns with the given scenario.
**Tip**: Check that the tools and techniques mentioned are appropriate for each task.

## Provide clear instructions

Write clear and concise instructions for each task to ensure they are easily understood and actionable. Include any specific requirements, restrictions, or considerations to guide the participants effectively.

## Test and refine

If possible, test the penetration testing strategy yourself or with a small group to identify any ambiguities or areas that need improvement.

## Conclusion

By completing this exercise on creating a penetration testing strategy, you will enhance your skills in penetration testing, reinforce your understanding of the methodologies and techniques involved, and gain hands-on experience in assessing and enhancing the security of digital sys