Comprehensive Penetration Testing Plan for Sam's Scoops Microsoft Azure Environment

Introduction

Demonstration in planning a white box penetration test on a Microsoft Azure environment and identifying vulnerabilities and weaknesses within the Azure infrastructure. Allowing me to have a deeper understanding of penetration testing, encompassing the various stages such as reconnaissance, enumeration, exploitation, escalation, and ultimately, reporting and remediation. The penetration tests were conducted in a simulated Microsoft Azure environment to evaluate the security posture of the infrastructure and applications. Adhering to ethical hacking principles, the aim was to identify vulnerabilities and security weaknesses within the scope of the Azure infrastructure components described in the scenario.

Scenario

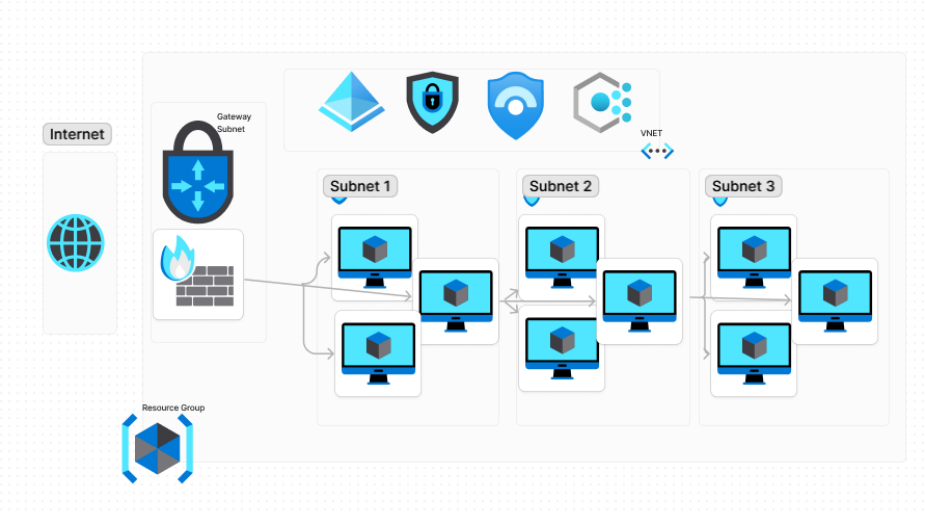
A white box penetration test for Sam's Scoops to be carried out inside an Azure environment. In order to allow Sam to feel confident that their infrastructure is up to the task.

The primary objective of this exercise was to formulate a comprehensive penetration testing plan and craft a Network Architecture Diagram which included an explanation of its key components and structure.

Azure infrastructure components

- Virtual machine(VM)
- Virtual network (VNet)
- Subnets
- Network security groups (NSG)
- Private IP range
- Resource groups
- Role-based access control (RBAC)
- Azure Firewall
- Virtual Private Network (VPN)
- Azure Security Center (New Name – Defender for Cloud)
- Microsoft Sentinel and Log Analytics
- Azure Security Policy
- Azure Active Directory (Azure AD)

Network architecture diagram



Comprehensive Penetration Testing Plan for Sam's Scoops Microsoft Azure Environment

Diagram of correct network architecture

The provided diagram illustrates a robust network architecture within Microsoft Azure, leveraging key components to enhance security and scalability. Here are the essential elements:

1. **Firewall Deployment**: The firewall is strategically placed in the gateway subnet, meticulously inspecting all incoming and outgoing traffic. This proactive measure safeguards the network against unauthorized access and potential malicious threats.
2. **Subnet Isolation**: Multiple subnets are employed to segregate distinct types of traffic and resources. For instance:
    - **Subnet 1**: Dedicated to web servers.
    - **Subnet 2**: Reserved for database servers.
    - **Subnet 3**: Allocated for development servers. This isolation ensures that each resource type remains protected from both external threats and internal interactions.
3. **Network Security Groups (NSGs)**: NSGs are applied to each subnet, allowing fine-grained control over traffic flow to and from the virtual machines (VMs). For example:
    - The NSG on **Subnet 1** can be configured to permit internet traffic specifically for web servers while restricting access to database servers.
4. **Key Benefits**:
    - **Security**: The combined use of firewalls, subnets, and NSGs fortifies the network against unauthorized intrusions and malicious activities.
    - **Scalability**: The architecture easily accommodates scaling by adding or removing VMs across different subnets.
    - **Manageability**: NSGs simplify traffic management, ensuring efficient control over communication between VMs.
    - **Visibility**: Microsoft Sentinel enhances visibility by providing insights into security events across the network.
    - **Compliance**: Organizations can align with security regulations using this well-structured network architecture.

In summary, this comprehensive design integrates firewalls, subnets, NSGs, Azure Policy, and Microsoft Sentinel, resulting in a secure and scalable Azure network solution.

Penetration Testing Strategy

Step 1: Reconnaissance

Tools:

- Azure CLI
- Powershell
- Open-source intelligence (OSNIT) sources

Techniques:

- Use Azure CLI, PowerShell, and Open-source intelligence (OSINT) sources to gather information about Azure resources, endpoints, and configurations.

Explanation:

- This step is crucial in understanding potential vulnerabilities and entry points. It helps to build a comprehensive picture of the target environment, which is essential for planning subsequent steps of the penetration test.

Targeted workload:

- Azure Active Directory
- Virtual machines

Step 2: Enumeration

Methodology:

- Employ automated scanning tools such as Nmap and OWASP ZAP.

Vulnerability scanning:

- Identify vulnerabilities in Azure resources using Azure Security Center.

Manual testing:

- Manually verify vulnerabilities, configurations, and access controls.

Explanation:

- This step involves identifying live hosts, open ports, and services running on those ports. The significance of thorough enumeration is to identify potential weaknesses that can be exploited.

Targeted workload

- Azure Firewall
- Azure VPN Gateway
- Azure Active Directory

Step 3: Exploitation

Ethical approach:

- Ensure all actions adhere to ethical hacking principles.

Proof of Concept (PoC):

- Exploit vulnerabilities to demonstrate their impact without causing harm using Metasploit and OWASP WebGoat.

Exploit frameworks:

- Use ethical hacking frameworks to simulate attacks.

Explanation:

- This phase involves attempting to exploit the identified vulnerabilities. The purpose of PoC is to demonstrate the potential impact of the vulnerabilities without causing harm. Ethical conduct during this phase is crucial to ensure the integrity of the system and data.

Targeted workload:

- Azure Firewall
- Azure VPN Gateway
- Azure Active Directory
- Virtual Machine

Step 4: Escalation

Privilege escalation:

- Attempt to escalate privileges using known techniques.

Data Exfiltration:

- To spotlight data security risks without compromising sensitive information ethically exfiltrate data from the system.

Explanation:

- This step involves attempting to gain higher-level privileges, such as admin access, which can be used to exploit the system further. It's significant in assessing the extent to which an attacker can escalate privileges. Use of established techniques such as privilege escalation vulnerabilities and social engineering may be used to escalate privileges.

Targeted workload:

- Azure Firewall
- Azure VPN Gateway
- Azure Active Directory
- Virtual Machine

Step 5: Reporting and Remediation

Documentation:

- Record all findings, including vulnerabilities and exploitation methods.

Prioritization:

- Prioritize vulnerabilities based on their criticality.

Recommendations:

- Provide recommendations for remediation.

Collaboration:

- Collaborate with stakeholders to address identified issues.

Explanation:

- This final step involves documenting the findings, prioritizing the vulnerabilities based on their severity, and providing recommendations for remediation. Collaboration with stakeholders is crucial at this stage to ensure the identified vulnerabilities are addressed, and security is enhanced.

Conclusion

Conducting a white box penetration test on Sam's Scoops Azure environment allows for the assessment of the system's security resilience and provides a roadmap for future enhancements to the network. The system has now had a comprehensive evaluation spanning many strategies from reconnaissance to reporting. The collaborative remediation efforts underscore the commitment to strengthening the overall security of Sam's Scoops systems allowing Sam to fortify his business' Azure environment against potential threats.