Penetration Testing Strategy: Sam’s Scoops

Sam’s Scoops is a ice cream retail business that has expanded to several stores over the years. Due to expanding operations, Sam’s Scoops incorporated the cloud infrastructure with their respective on-premises infrastructure. As an online icecream retailer, Sam’s Scoops have an e-platform that deal with all the online orders. The e-platform deals with sensitive information related to customer such as customer name, email, payment info, and orders etc. All this data is stored on SQL server. Both the e-platform and SQL server are hosted on two separate Azure VMs in the Azure environment. The network to these monitors is monitored and protected by an Azure firewall. Moreover, Sam’s Scoops have also employed Web App Firewall that protects and filter the http traffic between the internet and the app.

Penetration Strategy

Penetration testing involves the following five stages:

1. Reconnaissance

The main focus of this stage is to collect as much information as possible about Sam’s Scoops. This step includes collecting information such the name of target in this case Sam’s Scoops and other relevant info from various sources. Moreover, the info related to Sam’s Scoops digital presence will be analyzed. It will include info such as websites and social media presence. The information about the potential attack surface and entry points is gathered. It also includes steps such as probing the network for open ports, services and vulnerabilities.

a. Tools:

- **Maltego:** aggregates information from various sources such as social media platforms, public databases, and online records.

b. Techniques:

- **Data mining and visualization**
- **Collection**

2. Enumeration

This step involves the assessment of the target system to gain valuable sights. During this step the information about the OS systems, software versions, IP addresses and open ports etc.

a. Tools

- **Nmap:** can identify hosts on a network, detect open ports, and determine the services running on those ports.
- **OpenVAS:** provides a comprehensive set of vulnerability tests for networks and web applications
- **Wireshark:** capture and analyze network traffic

b. Techniques

- **TCP SYN, UDP, and ICMP scans**
- **OS fingerprinting**
- **Service version detection**
- **Banner grabbing**
- **Input validation**
- **Resource development**

3. Exploitation

This step involves the exploiting the identified vulnerabilities to gain unauthorized access to the system.

a. Tools

- **Burp Suite:** toolkit specifically designed for web application testing. Intercept proxy feature allow to intercept and modify https traffic. Intruder module is another feature that can be used to automate fuzzing tasks
- **Metasploit:** pre-built exploits, payloads, and auxiliary modules

b. Techniques

- **SQL injections**
- **Credential access**
- **Cross-site scripting**
- **Injecting payloads**

4. Escalation

Once the system has been exploited, it is all about escalating the privileges. This step involves targeting the accounts or systems with privileged accesses. It also involves persistence.

a. Tools

- **Metasploit:** post-exploitation module can be used for privilege escalagtion

b. Techniques

- **Lateral movement**
- **Command and control**
- **Backdoors**
- **Modify registry**

5. Reporting and remediation

The final step of penetration testing is to report all the findings. It includes steps like listing of vulnerablities found, vulnerability assessment and its impacts, and remediation.

a. Tools:

- **QualysGuard**
- **Executive summary**
- **Appendix**
- **Vulnerability assessment**

b. Techniques:

- **Be clear and concise**
- **Be specific**
- **Testing the remediation process**