Penetration test for Sam's Scoops

Sam's Scoops has an eCommerce platform that is hosted on Microsoft Azure on a virtual machine. The company stores customer and product data on a Microsoft SQL server that is on another virtual machine on Azure. Sam's Scoops has implemented an Azure Firewall and Web Application Firewall in between the internet and the web application and SQL database to protect proprietary and customer data. A white-box penetration test will be performed to identify and remediate possible vulnerabilities in Sam's Scoops eCommerce platform, the virtual machine it is running on, and the firewalls in place to protect the platform and SQL server. It is a white-box test because the system architecture as well as the security configurations put in place are known to the tester.

Stage 1: Reconnaissance

- Perform passive reconnaissance by searching Sam's Scoops in a search engine to find employee names, emails, and relevant company information. Searching employees on social media can uncover additional information.
- Perform active reconnaissance through tools such as Nmap to identify network hosts, open ports, and services running on those ports.
- Maltego can also be used as active reconnaissance to aggregate data about employees, domains, and IP addresses from social media, online databases, and public records.
- Shodan can be used as active reconnaissance to find potential vulnerabilities by analyzing internet devices such as routers, webcams, servers, and IoT devices to gather information about open ports, banners, system configurations and misconfigurations, credentials, and unpatched software.

Stage 2: Enumeration

- In addition to the information gathered through active reconnaissance tools used in stage 1, tools such as Nessus to provide both unauthenticated and authenticated scans, gaining deeper insight into potential vulnerabilities such as through open ports and services running on those ports as well as getting a detailed report about vulnerabilities and their severities.

Stage 3: Exploitation

- Since Sam's Scoops is an eCommerce platform on a virtual machine with a connected MS SQL server on another virtual machine, it is assumed that XSS and SQL injection attacks are a concern. During this phase, tools such as BurpSuite can be used to identify flaws in the WAF and Azure Firewall configurations to prevent XSS and SQL injection attacks.

Stage 4: Escalation

- Once an injection vulnerability is found or a security misconfiguration of the WAF and Azure Firewall, such as using a SQL injection attack to bypass security authorizations and gain access to user accounts, tools such as Metasploit can be used to escalate account privilege, move laterally throughout the network to discover previously inaccessible data, and exfiltrate said data.

Stage 5: Report and Remediation

- If flaws are found in security configurations of the firewalls, virtual machines, or internet-connected devices such as weak passwords or encryption, vulnerabilities to injection attacks, or misconfigured inbound/outbound traffic rules on the firewalls, a detailed report would be made by identifying the vulnerability, its severity, and then how to remediate the vulnerability. For example, to prevent SQL injections, software patches or input validation may be required. To prevent unauthorized network traffic, inbound traffic rules may need to be reconfigured in the Azure firewall and WAF.