ISIN 335 – AWS Penetration Testing Plan
Instructor: Gerald Emerick

Amazon AWS Penetration Test Plan

You have been asked to design and plan a penetration test against the AWS three tier architecture you have designed. Using Kali Linux as your general toolset, list and describe the tools and methods you will use to complete the penetration test including reconnaissance, scanning, and vulnerability analysis. Exploitation and post-exploitation are out of scope. In addition, identify and describe at least two AWS Security services including AWS Inspector that you would include in your penetration test that would compliment your Kali toolset. Your document must follow this outline:

a. **Scope of Penetration Test** – List the IP ranges and briefly describe the targeted 3 tier architecture.

The scope of the Penetration Test focuses on the three separate tiers of the architecture: the web server tier, the application server tier, and the database tier.

- Public Subnets: 10.0.0.0/24, 10.0.2.0/24 (Web Server 1 & 2)
- Private Subnets: 10.0.1.0/24, 10.0.3.0/24 (Application Server 1 & 2)
- Database Subnets: 10.0.4.0/24, 10.0.5.0/24 (RDS Instance and Read Replica)

The three-tiered architecture in AWS has two availability zones designed for high availability along with fault tolerance. The web servers are located in the public subnets, the application servers are located in the private subnets, and the database server along with the read replica are in separate private subnets. The architecture utilizes ALBs for distributing traffic to mitigate overload. The NAT gateways allow for internet access in the private subnets. Amazon S3 is located in the AWS Cloud as well for hosting static content. The architecture also utilizes a VPN gateway to allow connection from the organization's data center.

b. **Reconnaissance and Scanning** – List the chosen Kali tools, methods, and purpose of each tool.

The main Kali tools I chose for reconnaissance and scanning are Nmap, nslookup, Nikto, and dirbuster. Nmap's purpose would be to identify open ports, services, and live targets at the intended IP ranges. Utilizing 'nmap -sS -A -Pn' along with the range such as 10.0.0.0/16 or 10.0.1.0/24 would search for TCP SYN port scan, version detection, and OS detection. Nslookup's purpose would be to identify if

the domains www.store.com and www.otherstore.com have any DNS records associated with specific IP addresses and configuration issues. Nslookup can be ran with 'nslookup www.store.com'. Nikto's purpose would be to scan the web servers for any outdated software/services, vulnerabilities, and/or misconfigurations. Nikto can be ran with 'nikto -h http://www.store.com'. Dirbuster's purpose would be to find any hidden files or directories using a brute force approach on the web servers. Dirbuster can be ran with the address 'www.store.com' through Kali.

c. **Vulnerability Analysis** - List the chosen Kali tools, methods, and purpose of each tool.

The tools in Kali that I have chosen for vulnerability analysis is metasploit, SQLmap, and Burp Suite. Metasploit Framework would be able to list currently known vulnerabilities in the web servers and application servers based on information from the reconnaissance & scanning section. Metasploit can be ran with 'msfconsole', then with a search command for certain services such as 'search ftp', then a module can be chosen and configured to set an exploit. SQLmap's purpose would be to test for SQL injection vulnerabilities on the RDS database web servers. A sample command for this could be, 'sqlmap -u "http://www.store.com/product?id=1" --dbs'. Burp Suite's purpose would be to identify cross-site scripting vulnerabilities on the web servers, or locate insecure session management.

d. **AWS Security Services** – Identify and describe the two AWS Security services you have chosen.

The AWS security services that would be most beneficial for this plan would be Amazon Inspector and AWS Config. Amazon Inspector would provide automated vulnerability assessments for the instances deployed. This would look at known CVEs along with misconfigurations such as inadequate security group rules. AWS Config would act as a continuous monitoring agent to evaluate resource usage based on best security practices by AWS.