VMware NSX Advanced Load Balancer : Web Application Firewall Security

Course Outline

1. Course Introduction
- Introductions and course logistics
- Course objectives

2. Introduction to NSX Advanced Load Balancer
- Introduce NSX Advanced Load Balancer
- Discuss NSX Advanced Load Balancer use cases and benefits
- Explain NSX Advanced Load Balancer architecture and components
- Explain the management, control, data, and consumption planes and their respective functions

3. Introduction to NSX ALB Web Application Firewall
- Introduce the NSX Advanced Load Balancer Web Application Firewall (WAF)
- Discuss NSX Advanced Load Balancer WAF use cases and benefits

4. Virtual Services Configuration Concepts
- Explain Virtual Service components
- Explain Virtual Service types
- Explain and configure basic virtual service components such as Application Profiles, Network Profiles, Pools, and Health Monitors

5. Attacking and Defending Web Applications
- Introduce the processes and methodologies used when attacking and defending web applications
- Introduce the tools used to attack web applications
- Explain with examples terminology such as Reflected XSS and SQL injection

6. Profiles and Policies
- Explain and deep dive on Advanced Virtual Service creation
- Explain and deep dive on Application Profiles and Types such as L4, DNS, Syslog, and HTTP
- Explain and configure advanced application HTTP Profile options
- Deep dive on Network Profiles and Types
- Explain and configure SSL Profiles and Certificates
- Explain and configure HTTP and DNS policies

7. DDoS Protection
- Introduce the NSX Advanced Load Balancer rate limiting functionality
- Explain the NSX Advanced Load Balancer rate limiting functionality
- Hands-on examples of rate limiting in action

8. Customizing Application Delivery with Datascripts

- Introduce the concept of datascripts to manipulate data
- Explain the various components and inspection points

9. iWAF Deep Dive

- Describe the building blocks of the iWAF implementation
- Explain the various iWAF components
- Introduce both Positive and Negative security models
- Explain the iWAF Policies, profiles, and rule sets

10. iWAF Core Rule Set

- Explain the history and rationale of the core rule set
- Describe the NSX ALB (Avi) Core Rule Set

11. iWAF Custom Rules

- Describe the power and complexity available via custom rules
- Explain the rule language
- Implement various use cases
- Explain common errors and possible solutions

12. iWAF Operations

- Describe the iWAF application onboarding process
- Tuning the iWAF policies
- Working with iWAF logs and analytics
- Explaining false positive mitigation tactics

13. iWAF Best Practices

- Provide guidance on how to get the best results with iWAF