

دوره , TShoot هوره , LTM , AWAF

مروری بر دوره

این دوره جامع دوره قصد دارد تا ادمین ها، اپراتورها و مهندسین شبکه را با عملکرد سیستم BIG-IP آشنا سازد. دانشجویان این دوره علاوه بر آشنایی با چگونی و نحوه مدیریت سیستم BIG-IP، پیکربندی Object ها، پردازش ترافیک و همچنین چگونگی نحوه مدیریت و انجام عملیات مرتبط با این سیستم را خواهد آموخت. پرداختن به موضوع مهم و حیاتی عیب یابی در این سیستم و Advanced Web Application Firewall در کنار

AWAF)) از جمله دیگر سرفصل های این دوره خواهند بود.

آنچه در این دوره خواهید آموخت

- آشنایی با انواع یلتفرمهای ۴۵
- ساختار سیستمعامل TMOS
- مفهوم Multi-tenancy به واسطه قابلیت
 - انواع روشهای استقرار تجهیزات ADC
- نحوه فعالسازی License و انجام Resource Provisioning هریک از ماژولهای مختلف،
- آشنایی با پیکربندی مفاهیم پایه ارتباطی شبکه بر روی تجهیزات ۴۵ شامل Trunk, VLAN, Self-IP, آشنایی با Node, Pool Member, Monitor, Server Pool, Virtual شامل TMOS شاهیم پایه در سیستمعامل Server, Profile, NAT/SNAT
 - آشنایی با نحوه پیکربندی و پیادهسازی معماری Half-proxy و Full-proxy
 - آشنایی با معماری High-availability بر روی تجهیزات ه
 - آشنایی با نحوه استفاده از دستورات TMSH
 - انواع روشهای استقرار تجهیزات ADC در زیرساخت شبکه (Deployment Models)
 - مفاهیم پایه و کاربردی در سیستم عامل TMOS با تمرکز بر روی ماژول •





- نحوه پیکربندی زیرساخت شبکه شامل Trunk, VLAN, Self-IP, Route
- مفهوم Route Domain (VRF) و ارتباط آن با Administrative Partition
- مديريت بهينه و سطح بالاي ترافيک HTTP به واسطه LTP (Local Traffic Policy) و iRule Scripts
- بررسی و بهینهسازی مفاهیم بنیادین TCP Profile به عنوان پرکاربردترین و مهم ترین Profile در سیستمعامل TMOS
- نحوه انتخاب صحیح تکنیکهای توزیع ترافیک (Load-balancing Methods) تحت شرایط انواع مختلفی از سناریوها
 - نحوه پیادهسازی معماری Half-proxy و Full-proxy
- اعمال Traffic Tuning به واسطه سرور مجازی (Virtual Server) به ازای انواع مختلفی از سرویسها با هدف انتخاب Virtual Server Type بهینه و کاربردی در هر سناریو
 - آشنایی با نحوه پیکربندی صحیح انواع روشهای پیادهسازی مکانیزمهای Failover (Failover Methods) Active/Standby میباشد.
 - آشنایی با ماهیت عملکرد یروتکل HTTP و جایگاه تجهیزات
 - آشنایی با ریسکهای امنیتی OWASP TOP-۱۰ Risks
 - آشنایی با تهدیدات امنیتی OWASP Automated Threats
 - نحوه استقرار تجهیزات WAF در لایه سرویس با تمرکز بر روی ماژولهای F۵-ASM و F۵-AWAF، مقدمهای بر ماژولهای F۵-ASM و بیان تفاوتهای فنی بین این دو ماژول
 - آشنایی با نحوه بهروزرسانی و مدیریت انواع Signatureها و Databaseهای تجهیز شامل Asm/AWAF Attack Signatures، Threat Campaign Signatures، Behavioral WAF Signatures، Browser Challenge Database، Server Technology Database، Geo-location Database و Credential Stuffing Database، BOT Signatures
 - آشنایی با نحوه پیکربندی و اعمال Security Tuning بر روی تک تک Security Entityها شامل ,File Type, Parameter, Header
- بررسی و نحوه اعمال Tuning بر روی Learning Suggestionهای متعلق به Correlation Engine و Behavioral Analytic Engine
- پیکربندی و اعمال Tuning بر روی قابلیتهای امنیتی شامل –Tuning بر روی قابلیتهای امنیتی





force Attacks Protection, WEB Scraping Attacks Protection, Session Tracking, Session Hijacking Protection, Session Awareness, CSRF Protection, Information Leakage Protection

- پیادهسازی مفهوم Micro-services، پیکربندی و بهینهسازی Micro-services، پیکربندی و بهینهسازی Lv BOTs Protection
- پیادهسازی معماری HSL (High-speed Logging) با هدف بهینهسازی فرمت و نحوه ارسال Logهای امنیتی
 - همچنین آشنایی با نحوه بررسی Logging و Reporting تجهیزات ASM/AWAF، میباشد.

سرفصل ها

Admin & TShoot

- Getting started with the BIG-IP system
- Traffic processing with BIG-IP Local Traffic Manager (LTM)
- Using TMSH (TMOS Shell) command line interface
- Using NATs and SNATs
- Monitoring application health and managing object status
- Modifying traffic behavior with profiles, including SSL offload and reencryption
- Modifying traffic behavior with persistence, including source address affinity and cookie persistence
- Troubleshooting the BIG-IP system, including logging (local, high-speed, and legacy remote logging), and using TCPDUMP
- User roles and administrative partitions
- vCMP concepts
- Configuring high availability (including active/standby and connection and persistence mirroring)





Local Traffic Manager (LTM)

- BIG-IP initial setup (licensing, provisioning, and network configuration)
- A review of BIG-IP local traffic configuration objects
- Using dynamic load balancing methods
- Modifying traffic behavior with persistence (including SSL, SIP, universal, and destination address affinity persistence)
- Processing traffic with virtual servers (including network, forwarding, and reject virtual servers)
- Processing traffic with SNATs (including SNAT pools and SNATs as listeners)
- Modifying traffic behavior with profiles (including TCP profiles, advanced HTTP profile options, caching, compression, and One Connect profiles)
- Advanced BIG-IP LTM configuration options (including VLAN tagging and trunking, SNMP features, packet filters, and route domains)
- Deploying application services with iApps
- Customizing application delivery with iRules and local traffic policies
- Securing application delivery using BIG-IP LTM

Advance Web Application Firewall

Chapter \: Introducing the BIG-IP System

- Initially Setting Up the BIG-IP System
- Archiving the BIG-IP System Configuration
- Leveraging Fa Support Resources and Tools





Chapter Y: Traffic Processing with BIG-IP

- Identifying BIG-IP Traffic Processing Objects
- Understanding Profiles
- Overview of Local Traffic Policies
- Visualizing the HTTP Request Flow

Chapter v. Overview of Web Application Processing

- Web Application Firewall: Layer y Protection
- Layer v Security Checks
- Overview of Web Communication Elements
- Overview of the HTTP Request Structure
- Examining HTTP Responses
- How F
 Δdvanced WAF Parses File Types, URLs, and Parameters
- Using the Fiddler HTTP Proxy

Chapter 4: Overview of Web Application Vulnerabilities

- A Taxonomy of Attacks: The Threat Landscape
- Common Exploits Against Web Applications

Chapter a: Security Policy Deployments: Concepts and Terminology

- Defining Learning
- Comparing Positive and Negative Security Models
- The Deployment Workflow
- Assigning Policy to Virtual Server
- Deployment Workflow: Using Advanced Settings





- Configure Server Technologies
- Defining Attack Signatures
- Viewing Requests
- Security Checks Offered by Rapid Deployment

Chapter 9: Policy Tuning and Violations

- Post-Deployment Traffic Processing
- How Violations are Categorized
- Violation Rating: A Threat Scale
- Defining Staging and Enforcement
- Defining Enforcement Mode
- Defining the Enforcement Readiness Period
- Reviewing the Definition of Learning
- Defining Learning Suggestions
- Choosing Automatic or Manual Learning
- Defining the Learn, Alarm and Block Settings
- Interpreting the Enforcement Readiness Summary
- Configuring the Blocking Response Page

Chapter V: Using Attack Signatures and Threat Campaigns

- Defining Attack Signatures
- Attack Signature Basics
- Creating User-Defined Attack Signatures
- Defining Simple and Advanced Edit Modes
- Defining Attack Signature Sets
- Defining Attack Signature Pools





- Understanding Attack Signatures and Staging
- Updating Attack Signatures
- Defining Threat Campaigns
- Deploying Threat Campaigns

Chapter A: Positive Security Policy Building

- Defining and Learning Security Policy Components
- · Defining the Wildcard
- Defining the Entity Lifecycle
- Choosing the Learning Scheme
- How to Learn: Never (Wildcard Only)
- How to Learn: Always
- How to Learn: Selective
- Reviewing the Enforcement Readiness Period: Entities
- Viewing Learning Suggestions and Staging Status
- Defining the Learning Score
- Defining Trusted and Untrusted IP Addresses
- How to Learn: Compact

Chapter 9: Securing Cookies and other Header Topics

- The Purpose of F∆ Advanced WAF Cookies
- Defining Allowed and Enforced Cookies
- Securing HTTP headers

Chapter VI: Visual Reporting and Logging





- Viewing Application Security Summary Data
- Reporting: Build Your Own View
- Reporting: Chart based on filters
- Brute Force and Web Scraping Statistics
- Viewing Resource Reports
- PCI Compliance: PCI-DSS v..
- · Analyzing Requests
- Local Logging Facilities and Destinations
- Viewing Logs in the Configuration Utility
- Defining the Logging Profile
- Configuring Response Logging

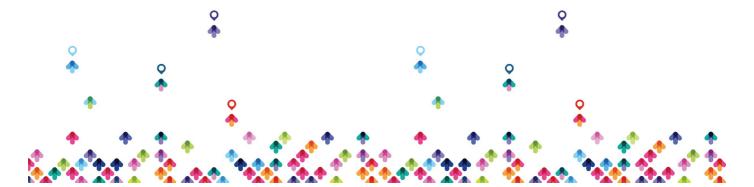
Chapter ۱۱: Lab Project ۱

Chapter 17: Advanced Parameter Handling

- Defining Parameter Types
- Defining Static Parameters
- Defining Dynamic Parameters
- Defining Parameter Levels
- Other Parameter Considerations

Chapter 17: Automatic Policy Building

- Defining Templates Which Automate Learning
- Defining Policy Loosening
- Defining Policy Tightening
- Defining Learning Speed: Traffic Sampling
- Defining Track Site Changes





Chapter 14: Integrating with Web Application Vulnerability Scanners

- Integrating Scanner Output
- Importing Vulnerabilities
- Resolving Vulnerabilities
- Using the Generic XML Scanner XSD file

Chapter 1a: Deploying Layered Policies

- Defining a Parent Policy
- Defining Inheritance
- Parent Policy Deployment Use Cases

Chapter 19: Login Enforcement and Brute Force Mitigation

- Defining Login Pages for Flow Control
- Configuring Automatic Detection of Login Pages
- Defining Brute Force Attacks
- Brute Force Protection Configuration
- Source-Based Brute Force Mitigations
- Defining Credential Stuffing
- Mitigating Credential Stuffing

Chapter 17: Reconnaissance with Session Tracking

- Defining Session Tracking
- Configuring Actions Upon Violation Detection

Chapter NA: Layer Y Denial of Service Mitigation





- Defining Denial of Service Attacks
- Defining the DoS Protection Profile
- Overview of TPS-based DoS Protection
- Creating a DoS Logging Profile
- Applying TPS Mitigations
- Defining Behavioral and Stress-Based Detection

Chapter 19: Advanced Bot Defense

Classifying Clients with the Bot Defense Profile

Defining Bot Signatures

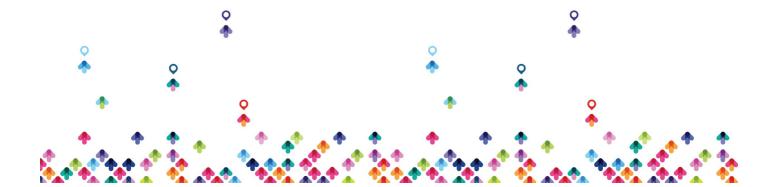
Defining Fa Fingerprinting

Defining Bot Defense Profile Templates

پیش نیاز ها

اشنایی با

- OSI model encapsulation
- Routing and switching
- Ethernet and ARP
- TCP/IP concepts
- IP addressing and subnetting
- NAT and private IP addressing





- Default gateway
- Network firewalls
- LAN vs. WAN

