خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره F۵ Admin & TShoot , 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 LTM در کنار Advanced Web Application Firewall (AWAF) از جمله دیگر سرفصل های این دوره خواهند بود.

آنچه در این دوره خواهید آموخت

- آشنایی با انواع پلتفرم‌های F۵
- ساختار سیستم‌عامل TMOS
- مفهوم Multi-tenancy به واسطه قابلیت vCMP
- 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 F۵ شامل Trunk, VLAN, Self-IP, ...، آشنایی با مفاهیم پایه در سیستم‌عامل TMOS شامل Node, Pool Member, Monitor, Server Pool, Virtual Server, Profile, NAT/SNAT, ...
- آشنایی با نحوه پیکربندی و پیاده‌سازی معماری Half-proxy و Full-proxy
- آشنایی با معماری High-availability بر روی تجهیزات F۵
- آشنایی با نحوه استفاده از دستورات TMSH
- انواع روش‌های استقرار تجهیزات ADC در زیرساخت شبکه (Deployment Models)
- مفاهیم پایه و کاربردی در سیستم‌عامل TMOS با تمرکز بر روی ماژول LTM

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- نحوه پیکربندی زیرساخت شبکه شامل Trunk, VLAN, Self-IP, Route , ...
- مفهوم VRF (Route Domain) و ارتباط آن با Administrative Partition
- مدیریت بهینه و سطح بالای ترافیک HTTP به واسطه LTP (Local Traffic Policy) و iRule Scripts
- بررسی و بهینه‌سازی مفاهیم بنیادین TCP Profile به عنوان پرکاربردترین و مهم‌ترین 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) به‌صورت Active/Active و Active/Standby می‌باشد.
- آشنایی با ماهیت عملکرد پروتکل HTTP و جایگاه تجهیزات WAF
- 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 F۵-AWAF 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 URL, 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 Brute-Forceful Browsing Protection,

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

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 L۷ (D)DoS Attacks Protection، پیکربندی و بهینه‌سازی L۷ 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 re-encryption
- 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)

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

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)
- Monitoring application health with Layer ۳, Layer ۴, and Layer ۷ monitors (including transparent, scripted, and external monitors)
- 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 ۱: Introducing the BIG-IP System

- Initially Setting Up the BIG-IP System
- Archiving the BIG-IP System Configuration
- Leveraging F۵ Support Resources and Tools

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Chapter ۲: Traffic Processing with BIG-IP

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

Chapter ۳: Overview of Web Application Processing

- Web Application Firewall: Layer ۷ Protection
- Layer ۷ Security Checks
- Overview of Web Communication Elements
- Overview of the HTTP Request Structure
- Examining HTTP Responses
- How F۵ Advanced WAF Parses File Types, URLs, and Parameters
- Using the Fiddler HTTP Proxy

Chapter ۴: Overview of Web Application Vulnerabilities

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

Chapter ۵: 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

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

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

Chapter ۶: 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 ۷: 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

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ - ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

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

Chapter ۸: 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 ۹: Securing Cookies and other Header Topics

- The Purpose of F۵ Advanced WAF Cookies
- Defining Allowed and Enforced Cookies
- Securing HTTP headers

Chapter ۱۰: 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 ۳.۰
- 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 ۱۲: Advanced Parameter Handling

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

Chapter ۱۳: Automatic Policy Building

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

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Chapter ۱۴: Integrating with Web Application Vulnerability Scanners

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

Chapter ۱۵: Deploying Layered Policies

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

Chapter ۱۶: 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 ۱۷: Reconnaissance with Session Tracking

- Defining Session Tracking
- Configuring Actions Upon Violation Detection

Chapter ۱۸: Layer ۷ Denial of Service Mitigation

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

- 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 ۱۹: Advanced Bot Defense

Classifying Clients with the Bot Defense Profile
Defining Bot Signatures
Defining F۵ Fingerprinting
Defining Bot Defense Profile Templates

پیش نیاز ها

آشنایی 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