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

کارگاه آموزشی امنیت در ساختار محصول VMware vSphere

شرح مختصر

بررسی راهکارها و آموزش پیاده سازی امنیت در زیر ساخت مجازی سازی VMware vSphere

مروری بر دوره

مروری بر دوره

امروزه محصولات و تکنولوژی های مختلف مجازی سازی ، علی الخصوص مجازی سازی مراکز داده (Datacenter Virtualization) در داخل کشور به شکل همه گیردرحال استفاده هستند و دوره های آموزشی مختلفی برای نصب و راه اندازی، مدیریت ، بهینه سازی و طراحی در حال برگزاری است. ولیکن دغدغه ای از مدت ها پیش ذهن مدیران و کارشناسان فناوری اطلاعات سازمانها و شرکتهای مختلفی دولتی و خصوصی را مشغول نموده و اکنون نیز بخشنامه های سفت و سختی از طرف نهادهای امنیتی کشور نیز ارسال گردیده است،و آن دغدغه چیزی نیست جز موضوع امن سازی ساختارهای مجازی سازی ؛موضوعی که تا به حال به صورت مجتمع به آن پرداخته نگردیده است. ما در این کارگاه آموزشی قصد داریم سرفصلهای امنیتی محصول VMware vSphere را بر اساس نسخه ۶.۵, ۶.۷به صورت کامل بررسی نماییم و نحوه امن سازی و Hardening این ساختار را با Best Practice های امنیتی شرکت VMware بررسی و تا حد امکان در محیط لابراتواری اجرا نماییم.

آنچه در این دوره خواهید آموخت

آنچه خواهید آموخت

- امن سازی ، Hardening و Best Practice های امنیتی در Esxi Hypervisor
- امن سازی ، Hardening و Best Practice های امنیتی ساختار vCenter و سرویس های وابسته
- امن سازی ، Hardening و Best Practice های امنیتی محیط Virtual Machine ها
- نحوه Encrypt کردن Virtual Machine ها و استفاده از KMS Server
- امن سازی ، Hardening و Best Practice های امنیتی در لایه Virtual Networking

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

- بررسی Permissions & Privileges) vSphere Role base access control)
- امن سازی لایه ISCSI,NSF,FC) Virtual Storage)

سرفصل ها (حضوری)

سرفصل ها

۱- Securing & Hardening Esxi Hosts

- Limit Esxi Access
- General ESXi Security Recommendations
- Use named users and least privilege
- Minimize the number of open ESXi firewall ports
- Automate ESXi host management (Host Profile)
- Take advantage of lockdown mode
- Check VIB package integrity
- Manage ESXi certificates
- Consider Smart card authentication
- Consider ESXi account lockout
- UEFI Secure Boot for ESXi Hosts
- ESXi Log Files
- Using the ESXi Shell
- Using Active Directory to Manage ESXi Users
- Using vSphere Authentication Proxy
- Hardening Esxi Host guide

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

۲- Securing & Hardening vCenter Server systems

- vCenter Server Security Best Practices
- Secure VCSA
- Secure Windows based vCenter
- Verify Thumbprints for Legacy ESXi Hosts
- Verify that SSL Certificate Validation Over Network File Copy Is Enabled
- vSphere Certificate Management
- Required Ports for vCenter Server and Platform Services Controller
- Additional vCenter Server TCP and UDP Ports
- vCenter Server systems Hardening guide

۳- Securing & Hardening Virtual Machines

- Enable or Disable UEFI Secure Boot for a Virtual Machine
- Limit Informational Messages From Virtual Machines to VMX Files
- Prevent Virtual Disk Shrinking
- Virtual Machine Security Best Practices
- Secure vMotion & FT Logging
- Configure Windows VM for use with Credential Guard and Virtual TPM
- Secure Windows Guest OS with Virtualization Based Security (VBS)

۴- Virtual Machine Encryption

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

- How vSphere Virtual Machine Encryption Protects Your Environment
- vSphere Virtual Machine Encryption Components
- Encryption Process Flow
- Virtual Disk Encryption
- Prerequisites and Required Privileges for Encryption Tasks
- Encrypted vSphere vMotion
- Encryption Best Practices, Caveats, and Interoperability
- Set up the Key Management Server Cluster
- Create an Encryption Storage Policy
- Enable Host Encryption Mode Explicitly
- Disable Host Encryption Mode
- Create an Encrypted Virtual Machine
- Clone an Encrypted Virtual Machine
- Encrypt an Existing Virtual Machine or Virtual Disk
- Decrypt an Encrypted Virtual Machine or Virtual Disk
- Change the Encryption Policy for Virtual Disks
- Resolve Missing Key Issues
- vSphere Virtual Machine Encryption and Core Dumps

۵- **Securing vSphere Networking**

- Introduction to vSphere Network Security
- Securing the Network With Firewalls
- Secure the Physical Switch
- Securing Standard Switch Ports with Security Policies

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

- Securing vSphere Standard Switches
- Standard Switch Protection and VLANs
- Secure vSphere Distributed Switches and Distributed Port Groups
- Securing Virtual Machines with VLANs
- Creating Multiple Networks Within a Single ESXi Host
- Internet Protocol Security
- Ensure Proper SNMP Configuration
- vSphere Networking Security Best Practices

۶- **Permissions & Privileges** (**vSphere Role based access control**)

- Understanding Authorization in vSphere
- Managing Permissions for vCenter Components
- Global Permissions
- Using Roles to Assign Privileges
- Best Practices for Roles and Permissions
- Required Privileges for Common Tasks
- Alarms Privileges
- Auto Deploy and Image Profile Privileges
- Certificates Privileges
- Content Library Privileges
- Cryptographic Operations Privileges
- Datacenter Privileges
- Datastore Privileges
- Datastore Cluster Privileges

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

- Distributed Switch Privileges
- ESX Agent Manager Privileges
- Extension Privileges
- Folder Privileges
- Global Privileges
- Host CIM Privileges
- Host Configuration Privileges
- Host Inventory
- Host Local Operations Privileges
- Host vSphere Replication Privileges
- Host Profile Privileges
- Network Privileges
- Performance Privileges
- Permissions Privileges
- Profile-driven Storage Privileges
- Resource Privileges
- Scheduled Task Privileges
- Sessions Privileges
- Storage Views Privileges
- Tasks Privileges
- Transfer Service Privileges
- Virtual Machine Configuration Privileges
- Virtual Machine Guest Operations Privileges
- Virtual Machine Interaction Privileges
- Virtual Machine Inventory Privileges
- Virtual Machine Provisioning Privileges

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

- Virtual Machine Service Configuration Privileges
- Virtual Machine Snapshot Management Privileges
- Virtual Machine vSphere Replication Privileges
- dvPort Group Privileges
- vApp Privileges
- vServices Privileges
- vSphere Tagging Privileges

۷- **Securing vSphere Virtual Storage**

- Secure ISCSCI storage
- Secure FC Storage
- Secure NFS Storage
- Encrypt vSAN Datastore

مخاطبان دوره

مخاطبان دوره

- این دوره را برای تمامی کارشناسان ساختار مجازی سازی VMware vSphere که در حال کار با محصول مذکور در شرکتهای و سازمانهای مختلف می باشند ، توصیه می نماییم.

پیش نیاز ها

پیش نیازها

- گذراندن حداقل دوره ,VMware vSphere : Install

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

Configure, Manage ۶-۶.۵-۶.۷

برای حضور در این کارگاه الزامی می باشد.