

Virtual Infrastructure & Security: 'VMware Hacking'

VMware vSphere and Virtual Infrastructure Security Securing the Virtual Environment

Inleiding

'Veel bedrijven denken bij hun drang naar virtualisatie niet na over de beveiliging'

De sterke drang van bedrijven naar virtualisatie zorgt ervoor dat zij steken laten vallen bij de beveiliging van de data. Dit komt onder andere doordat bij virtualisatie een fysieke harde schijf wordt omgezet in een bestand op een gedeelde server. Deze server is voor veel personen toegankelijk wat beveiligingsproblemen kan opleveren. In de oude situatie werd dit probleem opgelost binnen het eigen fysieke datacenter, maar tegenwoordig bevindt veel informatie zich nu op slecht beveiligde storagelocaties en gegevensdiefstal is dus veel eenvoudiger geworden.

Voor de isolatie en beveiliging van fysieke servers vertrouwen we al jaren op firewalls en VLAN's. Helaas is deze methode niet echt geschikt voor virtuele omgevingen. In een dynamische virtuele omgeving kunnen VM's immers van de ene naar de andere fysieke server migreren. Wat nu als een van die servers niet adequaat is beveiligd? Voor je er erg in hebt, staat die bedrijfskritische VM doodleuk in een onveilige omgeving te draaien.

Deze en andere uitdagingen worden behandeld in de nieuwe training 'VMware Hacking' van StarTel. In de training Virtual Infrastructure & Security: VMware Hacking worden kandidaten in 4 dagen ingewijd in de mogelijkheden die er zijn om de virtuele VMware omgeving optimaal te beveiligen: 'It goes beyond the typical security protocols administrators use to secure their environments and delves much deeper into the actual working (and shortcomings) of the VMware environment. Students will take a 360 degree look at the potential threats, how to defend and defeat them, and establish a solid foundation to build secure virtual data centers from the ground up'..

Cursusinhoud

- Viewing virtualization from the attacker's perspective ('If you want to stop hackers from invading your network, first you've got to invade their minds'), and understanding the new security problems it can introduce;
- Discovering which security threats the vmkernel does (& doesn't) address;
- Learning how VMsafe enables third-party security tools to access the vmkernel API;

- Understanding the security implications of VMI, paravirtualization, and VMware Tools;
- Securing virtualized storage: authentication, disk encryption, virtual storage networks, isolation, & more;
- Protecting clustered virtual environments that use VMware High Availability, Dynamic Resource Scheduling, Fault Tolerance, vMotion, and Storage vMotion;
- Securing the deployment & management of virtual machines across the network;
- Mitigating risks associated with backup, performance management, & other day-to-day operations;
- Using multiple security zones & other advanced virtual network techniques.

Doelgroep

System Administrators and Security Administrators using virtualization software.

Voorkennis

VMware Infrastructure 3 Install & Configure or equivalent. In lieu of hands-on classroom training, an in-depth knowledge of VMware's ESX virtualization environment is required.

Cursusduur

4 dagen

Cursusmateriaal

Bij de training wordt gebruik gemaakt van het cursusboek 'VMware vSphere and Virtual Infrastructure Security. Securing the Virtual Environment' van Edward L. Haletky. Dit boek wordt aangevuld met speciaal voor de training samengesteld lesmateriaal. De training wordt verzorgd door een VMware Certified Instructor (VCI) gespecialiseerd in IT Security.