Common Virtualization Vulnerabilities and How to Mitigate Risks

pentestlab.blog/category/external-submissions

February 25, 2013

Virtualization has eased many aspects of IT management but has also complicated the task of cyber security.The nature of virtualization introduces a new threat matrix, and administrators need to address the resulting vulnerabilities in their enterprise environments.

Critical Virtualization Vulnerabilities

Some attacks against virtual machine, or VM, environments are variations of common threats such as denial of service. Others are still largely theoretical but likely approaching as buzz and means increase. Keep an eye on these critical weaknesses:

VM sprawl:VMs are easy to deploy, and many organizations view them as hardware-like tools that don't merit formal policies.This has led to VM sprawl, which is the unplanned proliferation of VMs.Attackers can take advantage of poorly monitored resources.More deployments also mean more failure points, so sprawl can cause problems even if no malice is involved.

Hyperjacking: Hyperjacking takes control of the hypervisor to gain access to the VMs and their data. It is typically launched against type 2 hypervisors that run over a host OS although type 1 attacks are theoretically possible. In reality, hyperjackings are rare due to the difficulty of directly accessing hypervisors.However, hyperjacking is considered a real-world threat, and administrators should take the offensive and plan for it.

VM escape:A guest OS escapes from its VM encapsulation to interact directly with the hypervisor.This gives the attacker access to all VMs and, if guest privileges are high enough, the host machine as well. Although few if any instances are known, experts consider VM escape to be the most serious threat to VM security.

Denial of service: These attacks exploit many hypervisor platforms and range from flooding a network with traffic to sophisticated leveraging of a host's own resources.The availability of botnets continues to make it easier for attackers to carry out campaigns against specific servers and applications with the goal of derailing the target's online services.

Incorrect VM isolation: To remain secure and correctly share resources,VMs must be isolated from each other.Poor control over VM deployments can lead to isolation breaches in which VMs communicate.Attackers can exploit this virtual drawbridge to gain access to multiple guests and possibly the host.

Unsecured VM migration: This occurs when a VM is migrated to a new host, and security policies and configuration are not updated to reflect the change.Potentially, the host and other guests could become more vulnerable.Attackers have an advantage in that administrators are likely unaware of having introduced weaknesses and will not be on alert.

Host and guest vulnerabilities: Host and guest interactions can magnify system vulnerabilities at several points.Their operating systems, particularly Windows, are likely to have multiple weaknesses.Like other systems, they are subject to vulnerabilities in email, Web browsing, and network protocols.However, virtual linkages and the co-hosting of different data sets make a serious attack on a virtual environment particularly damaging.

How to Mitigate Risk

Fortunately, security engineers can take several steps to minimize risk.The first task is to accurately characterize all deployed virtualization and any active security measures beyond built-in hypervisor controls on VMs.Security controls should be compared against industry standards to determine gaps.Coverage should include anti-virus, intrusion detection, and active vulnerability scanning.Additionally, consider these action steps:

VM traffic monitoring: The ability to monitor VM backbone network traffic is critical.Conventional methods will not detect VM traffic because it is controlled by internal soft switches.However, hypervisors have effective monitoring tools that should be enabled and tested.

Administrative control: Secure access can become compromised due to VM sprawl and other issues.Ensure that authentication procedures, identity management, and logging are ironclad.

Customer security: Outside of the VM, make sure protection is in place for customer-facing interfaces such as websites.

VM segregation: In addition to normal isolation, strengthen VM security through functional segregation.For example, consider creating separate security zones for desktops and servers.The goal is to minimize intersection points to the extent feasible.

Conclusion

Virtualization threats can seem abstract but are no more so than other attacks. Motives and methods are fundamentally the same, and administrators must counter with similar proven techniques.

This is a guest blog from James Younger, Lead Instructor at TrainACE. TrainACE is a Cyber Security Training organization located in the Washington D.C. metro. James carries many certifications including CISSP, CASP, CEH, CHFI, CCNA, Security+, MCSE, and PMP. For more information, follow them on twitter @pentesttraining.