EC-Council Licensed Penetration Tester

Methodology: Virtual Machine Penetration Testing

Penetration Tester:			
Organization:			
Date:		**Location:**	

Test 1: Scan for virtual environments

Target Organization	
URL	
Host Machine	
Detected Virtual Environments	
Services Created on Specific Ports by Virtual Platforms	1. 2. 3.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Search for virtual environments

Target Organization	
URL	
Discovered Virtual Environments	
List of Computers, Routers, and Servers discovered Using Variety of Filters	1. 2. 3. 4. 5.
Tools/Services Used	
	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Check if a documented policy exists for creating new virtual machines

Target Organization		
URL		
Host Machine		
Documented Policy Available to Create New Virtual Machines	☐ YES	☐ NO
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 4: Create inventory of virtual machines

Target Organization		
URL		
Host Machine		
Inventory (List of All Virtual Machines)		
Online VMs	**Offline VMs**	**Rouge VMs**
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 5: Check patch status of host and guest operating systems

Target Organization	
URL	
Patch Status of Host Operating Systems	
Patch Status of Guest Operating Systems	
List all Unpatched Host and Guest Operating Systems	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Check VM configuration for unused emulated hardware

Target Organization	
URL	
Analyzed VM Configuration Settings	
List of All Unused Emulated Hardware	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Check IP addressing information on virtual NICs

Target Organization	
URL	
Host Operating System	
Information Gathered from the Host Operating System's Virtual NIC on the Untrusted Network	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Check the network bandwidth limit per VM

Target Organization		
URL		
Outbound Traffic From a Virtual Machine		**Inbound Traffic To a Virtual Machine**
□ Average Size:		□ Average Size:
□ Peak Size:		□ Peak Size:
□ Burst Size:		□ Burst Size:
Tools/Services Used	1. _____ 2. _____ 3. _____ 4. _____ 5. _____	

Results Analysis:

Test 9: Check virtual switches for promiscuous mode

Target Organization		
URL		
Promiscuous Mode Enabled on Virtual Switches and on Virtual Distributed Switches	□ Yes	□ No
Enabled ESX Hypervisor	□ True	□ False
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 10: Perform virtual machines stress testing

Target Organization	
URL	
Memory Reliability	
Input/output Performance of VMs	
Network Performance of the Virtual Machines	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 11: Try to exploit hypervisors using automated exploit tools

Target Organization	
URL	
Exploited Hypervisors	
Results of the Exploit	
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Try to break out of guest VM

Target Organization	
URL	
Host Operating System	
Guest Virtual Machine	
Exploited VMware Workstation	
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____

Results Analysis:

Test 13: Perform vulnerability assessment of virtual environment

Target Organization	
URL	
Findings from Vulnerability Assessment of Virtual Environment	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: