

EC-Council Licensed Penetration Tester

Methodology: Virus and Trojan Detection

Penetration Tester:			
Organization:			
Date:		Location:	



Test 1: Check for suspicious open ports

Target Organization	
URL	
Detected Suspicious Connections	<div>1. <hr/></div> <div>2. <hr/></div> <div>3. <hr/></div> <div>4. <hr/></div> <div>5. <hr/></div>
Command Used	<div>1. <hr/></div> <div>2. <hr/></div> <div>3. <hr/></div> <div>4. <hr/></div> <div>5. <hr/></div>
Tools/Services Used	<div>1. <hr/></div> <div>2. <hr/></div> <div>3. <hr/></div> <div>4. <hr/></div> <div>5. <hr/></div>

Results Analysis:

Test 2: Check Windows Task Manager

Target Organization	
URL	
Programs and Processes Running on the Computer	<div>1. <hr/></div> <div>2. <hr/></div> <div>3. <hr/></div> <div>4. <hr/></div> <div>5. <hr/></div>
Detected Suspicious Processes	<div>1. <hr/></div> <div>2. <hr/></div> <div>3. <hr/></div> <div>4. <hr/></div> <div>5. <hr/></div>
Tools/Services Used	<div>1. <hr/></div> <div>2. <hr/></div> <div>3. <hr/></div> <div>4. <hr/></div> <div>5. <hr/></div>

Results Analysis:

Test 3: Scan for suspicious running processes

Target Organization	
URL	
Active Scanning Programs	1. 2. 3. 4. 5.
Suspicious Running Processes	1. 2. 3. 4. 5.
Unknown .exe files Detected	1. 2. 3. 4. 5.
Suspicious open Ports Detected by Program	1. 2. 3. 4. 5.
Suspicious Network Activities Detected	1. 2. 3.

	4.
	5.
Tools/Services Used	1.
	2.
	3.
	4.
	5.

Results Analysis:

Test 4: Scan for suspicious registry entries

Target Organization	
URL	
Suspicious Registry Entries	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Test 5: Scan for suspicious device drivers

Target Organization	
URL	
Scanned Suspicious Device Drivers	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Test 6: Scan for suspicious Windows services

Target Organization	
URL	
Detected the Trojans or Viruses from Windows Services	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Test 7: Scan for suspicious startup programs

Target Organization	
URL	
Startup Programs Scanned	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Test 8: Scan for suspicious files and folders

Target Organization	
URL	
Computing MD5 or SHA1 Cryptographic Hashes	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Test 9: Scan for suspicious network activity

Target Organization	
URL	
Network Traffic is Monitored	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Test 10: Check whether anti-virus and anti-Trojan programs are working

Target Organization	
URL	
Enabled Anti-Virus and Anti-Trojans	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis:

Test 11: Detect the boot-sector virus

Target Organization	
URL	
Commands Used	<div>1. _____</div> <div>2. _____</div> <div>3. _____</div> <div>4. _____</div> <div>5. _____</div>
Reports Generated	<div>1. _____</div> <div>2. _____</div> <div>3. _____</div> <div>4. _____</div> <div>5. _____</div>
Tools/Services Used	<div>1. _____</div> <div>2. _____</div> <div>3. _____</div> <div>4. _____</div> <div>5. _____</div>

Results Analysis:

Test 12: Use HijackThis to scan for spyware

Target Organization	
URL	
Scanned for Spyware to Analyze and fix Computer	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>
Tools/Services Used	<div>1.</div> <div>2.</div> <div>3.</div> <div>4.</div> <div>5.</div>

Results Analysis: