EC-Council Licensed Penetration Tester

Methodology: Log Management Penetration Testing

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

PENETRATION

LICENSED

TESTER

Test 1: Add a new line/plain text into the log files

Target Organization	
URL	
Scanned Log Files	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 2: Add separators (single pipe/multiple pipe characters) into the log files

Target Organization	
URL	
Inserting Single or Multiple pipe characters	1. 2. 3. 4. 5.
Log files discovered	1. 2. 3. 4. 5.
Tools Used	1. 2. 3. 4. 5.

Results Analysis:

Test 3: Timestamp injection

Target Organization	
URL	
Inserting or Modifying Log Files	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Adding a Timestamp Between the Corresponding Timestamps	1. 2. 3. 4. 5. 6. 7. 8. 9.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 4: Wrapping words and creating unusual log entries

Target Organization	
URL	
Log Entries Created	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 5: Add HTML tags into a log (HTML injection)

Target Organization	
URL	
Executing the script and Compromises the HTML Reports	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 6: Check the log viewing interface (terminal injection)

Target Organization	
URL	
Using Terminal Emulation to Interpret Character Sequence	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 7: Scan for log files

Target Organization	
URL	
Scanned Log Files	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 8: Try to flood syslog servers with bogus log data

Target Organization	
URL	
Syslog hosts	1. 2. 3. 4. 5.
Syslog Server Logs	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 9: Try malicious syslog message attack (buffer overflow)

Target Organization		
URL		
Buffer Overflow Condition Occurred	□ Yes	□ No
Tools/Services Used	1. 2. 3. 4. 5.	

Results Analysis:

Test 10: Perform man-in-the-middle attack

Target Organization		
URL		
Syslog Client Checks for the Server's Identity	□ Yes	□ No
Tools/Services Used	1. ____ 2. ____ 3. ____ 4. ____ 5. ____	

Results Analysis:

Test 11: Check whether logs are encrypted

Target Organization	
URL	
Sensitive Information Recovered	1. 2. 3. 4. 5.
System Configurations	1. 2. 3. 4. 5.
Security Weakness	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 12: Check whether the arbitrary data can be injected remotely into the Microsoft ISA Server log file

Target Organization	
URL	
Server Address	1. 2. 3. 4. 5.
HTTP Request Sent	1. 2. 3. 4. 5.
Modified Destination Host Parameter in Log File	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 13: Perform DoS attack against the Check Point FW-1 syslog daemon

Target Organization	
URL	
Enabling the Firewall Object	1. 2. 3. 4. 5.
Listening Syslog Daemon	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis:

Test 14: Send syslog messages containing escape sequences to the syslog daemon of Check Point FW-1 NG FP3

Target Organization	
URL	
Remotely receiving syslogs	1. 2. 3. 4. 5.
Tools/Services Used	1. 2. 3. 4. 5.

Results Analysis: