Client-Side Penetration Test Report

Introduction

This report presents the results of client-side penetration tests conducted by CORE Impact Professional. Unlike remote network attacks, client-side attacks require an end user to perform an action to trigger a compromise of their computer. The report includes detailed information on deployed social engineering attacks such as those that launch exploits via malicious web servers and emails. These attack vectors attempt to compromise end-user systems by exploiting known client-side vulnerabilities or by taking advantage of gaps in end-user security awareness. Once a computer is compromised, an attacker can establish a beachhead to infiltrate further into the organization’s back-end network.

Client-side attacks are arguably the most difficult to protect against because they take advantage of the human element in a network. In addition to maintaining computers at the current patch level, the best way to protect against these types of attacks is to educate end users on the latest social engineering attack trends and to continuously raise security awareness by testing the end-user community with controlled client-side penetration tests.

Workspace Summary

Name: Report 3
Started: 5/1/2012 12:04:24PM
Finished: 5/1/2012 1:00:00PM
Exact Time: 56 minutes 36 seconds
Running Time: 42 minutes 45 seconds

All successful client-side attacks

- Total number of hosts and mobiles compromised through email-borne attacks: 0
- Total number of hosts and mobiles compromised through malicious web server attacks: 1
- Total number of unique hosts and mobiles compromised through client-side attacks: 1
- Total number of compromised hosts and mobiles using decouple: 0

Summary of email-borne attacks

- Total number of email addresses targeted: 0
- Total number of emails sent: 0
- Total number of hosts and mobiles compromised through email-borne attacks: 0
- Percentage of successful email-borne attacks: 0.00%

Summary of malicious web server attacks

- Total number of malicious web sites deployed: 1
- Total number of unique user hits on the malicious web sites: 6
- Total number of hosts and mobiles compromised through malicious web server attacks: 0
- Number of malicious web server attacks: 4
- Number of successful malicious web server attacks: 0
- Percentage of successful malicious web server attacks: 0.00%
Summary of exploited client-side vulnerabilities

Total number of client-side vulnerabilities successfully exploited: 2
Total number of unique client-side vulnerabilities successfully exploited: 2
Total number of hosts and mobiles successfully exploited by client-side vulnerabilities: 1

Successful client-side exploits per operating system

<table>
<thead>
<tr>
<th>Operating System &amp; Version</th>
<th>Exploits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>2</td>
</tr>
<tr>
<td>unknown</td>
<td>2</td>
</tr>
</tbody>
</table>

*Unknown operating systems are not shown

Most successful email-borne attacks

- No successful email-borne attacks.
Most successful malicious web server attacks

Web Sites with Highest Number of Compromised Hosts and Mobiles

<table>
<thead>
<tr>
<th>Unit</th>
<th>Exploit accessed</th>
<th>Exploit successful</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*The number of successful exploit attempts is, at most, equal to the number of exploit access attempts, never greater.*

Details of non-trojan based email-borne attacks

No email templates used.

Details of trojan-based email-borne attacks

No email templates used.

Details of malicious web server attacks

**Web site:** http://10.44.11/packs0e/cNS1eojYSBzCzrKKY2gaa

**Exploits:**

- **NOCVE-9999-9999: One Link Multiple Clientsides Exploit.**

  Total number of compromised hosts and mobiles: 0

  List of hosts and mobiles that were compromised: None

  **Vulnerability description**

  Not available.

  **Additional exploit information**

  http://www.securityfocus.com/bid/13097
  http://xforce.iss.net/xforce/xfdb/20059
  http://www.securityfocus.com/archive/1/395515

  Total number of unique hits on the URL: 1
  Total number of exploits accessed: 1
  Browsers identified: msie 6.0.
Details of Phishing attacks

No phishing attacks deployed.

Unique email messages sent

*Exploit Name:* NOCVE-9999-9999: One Link Multiple Clientsides Exploit.

**Subject:** Online games

```html
<html>
<head>
  <%headinsert%>
</head>
<body>
  <%bodyinsert%>
  <p class="MsoNormal" style="text-align: center; align="center">b><span style="font-size: 18pt; color: rgb(153, 0, 0);">ONLINE GAMES: PLAY FOR FREE</span></b></p>
  <span style="font-size: 12pt; font-family: "Times New Roman";">Bored of your job? Need a break? Not allowed to install games on your company's workstation?<br>
  We have the solution for you! Click on the link below and start playing games online, no installation required!!!<br><br>
  <p align="center">Click To Play</p><br><br>
  Afraid your boss might come back and see you goofing around? Don't worry! <br>
  >From our game page you are just a click away from your predefined "escape" page!
  Nobody will ever notice!</span>
</body>
</html>
```
# Index

<table>
<thead>
<tr>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Workspace Summary (Report 3)</td>
<td>1</td>
</tr>
<tr>
<td>Successful client-side exploits per operating system</td>
<td>2</td>
</tr>
<tr>
<td>Most successful email-borne attacks</td>
<td>2</td>
</tr>
<tr>
<td>Most successful malicious web server attacks</td>
<td>3</td>
</tr>
<tr>
<td>Details of non-trojan based email-borne attacks</td>
<td>3</td>
</tr>
<tr>
<td>Details of trojan-based email-borne attacks</td>
<td>3</td>
</tr>
<tr>
<td>Details of malicious web server attacks</td>
<td>4</td>
</tr>
<tr>
<td>Details of Phishing attacks</td>
<td>4</td>
</tr>
<tr>
<td>Unique email messages sent</td>
<td>4</td>
</tr>
</tbody>
</table>