

## Table of Contents

<b>Introduction</b>	<b>3</b>
<b>Generate Shellcode</b>	<b>5</b>
<b>MSFVENOM</b>	<b>6</b>
<b>Shellcode Execution</b>	<b>9</b>
<b>Classic</b>	<b>9</b>
<b>EnumChildWindows</b>	<b>15</b>
<b>EnumWindows</b>	<b>18</b>
<b>VirtualAlloc Implementation</b>	<b>20</b>
<b>XOR</b>	<b>30</b>
<b>AES</b>	<b>38</b>
<b>Pointer Way</b>	<b>41</b>
<b>Timer</b>	<b>43</b>
<b>Process Shellcode Injection</b>	<b>47</b>
<b>Thread Hijacking</b>	<b>52</b>
<b>Conclusions</b>	<b>62</b>