

# Obsah

<b>Úvod</b>	<b>7</b>
<b>O autorovi</b>	<b>7</b>
<b>Předmluva autora</b>	<b>7</b>
<b>O této knize</b>	<b>7</b>
Co se v knize dozvíte	8
Popis nástrojů	9
Porozumění zápisu příkazů	9
<b>Co je Sysinternals</b>	<b>9</b>
<b>FAQ o Sysinternals</b>	<b>10</b>
Volný překlad EULA	11
<b>Sysinternals Forum</b>	<b>13</b>
<b>Balík Sysinternals</b>	<b>14</b>
Systémové proměnné	15
<b>Sysinternals Live</b>	<b>16</b>
<b>Další informace o Sysinternals</b>	<b>16</b>
<b>Využití nástrojů Sysinternals</b>	<b>17</b>
Troubleshooting	17
KAPITOLA 1	
<b>Souborové a diskové nástroje</b>	<b>19</b>
<b>Contig</b>	<b>20</b>
<b>Disk Usage (DU)</b>	<b>23</b>
<b>DiskView</b>	<b>24</b>
<b>NTFSInfo</b>	<b>25</b>
<b>FindLinks</b>	<b>26</b>
<b>Junction</b>	<b>29</b>
<b>Streams</b>	<b>30</b>
<b>Sync</b>	<b>33</b>
<b>Disk2vhd</b>	<b>34</b>
<b>PageDefrag</b>	<b>35</b>
<b>MoveFile a PendMoves</b>	<b>37</b>
<b>DiskMon</b>	<b>38</b>
<b>DiskExt</b>	<b>39</b>

<b>EFSDump</b>	<b>41</b>
<b>VolumeID</b>	<b>42</b>
<b>LDMDump</b>	<b>43</b>
<b>CacheSet</b>	<b>45</b>
<b>Chkdsk</b>	<b>46</b>
<b>BCDboot</b>	<b>48</b>
<b>BCDedit</b>	<b>49</b>
KAPITOLA 2	
<b>Síťové utility</b>	<b>51</b>
<b>AdExplorer</b>	<b>52</b>
<b>AdInsight</b>	<b>54</b>
<b>AdRestore</b>	<b>55</b>
<b>Nltest</b>	<b>56</b>
<b>PipeList</b>	<b>57</b>
<b>PsFile</b>	<b>59</b>
<b>TCPView</b>	<b>60</b>
<b>Netstat</b>	<b>62</b>
<b>Whols</b>	<b>65</b>
<b>Netsh</b>	<b>67</b>
<b>Ping, Tracert, PathPing</b>	<b>70</b>
<b>Route a ARP</b>	<b>74</b>
<b>Mrinfo</b>	<b>78</b>
<b>Nslookup</b>	<b>79</b>
KAPITOLA 3	
<b>Procesní nástroje</b>	<b>83</b>
<b>Handle</b>	<b>84</b>
<b>ListDLLs</b>	<b>87</b>
<b>PortMon</b>	<b>89</b>
<b>ProcDump</b>	<b>91</b>
<b>Process Explorer</b>	<b>94</b>
<b>Shutdown</b>	<b>112</b>
<b>Process Monitor</b>	<b>115</b>
<b>PsGetSid</b>	<b>128</b>
<b>PsList</b>	<b>129</b>
<b>TaskList</b>	<b>132</b>

<b>PsKill</b>	<b>133</b>
<b>TaskKill</b>	<b>134</b>
<b>PsService</b>	<b>136</b>
<b>PsSuspend</b>	<b>138</b>
<b>VMMMap</b>	<b>139</b>
<b>Mem</b>	<b>142</b>

## KAPITOLA 4

<b>Bezpečnostní nástroje</b>	<b>143</b>
<b>AccessChk</b>	<b>144</b>
<b>AccessEnum</b>	<b>146</b>
<b>Autologon</b>	<b>149</b>
<b>Autoruns</b>	<b>150</b>
<b>Msconfig</b>	<b>154</b>
<b>LogonSessions</b>	<b>155</b>
<b>PsExec</b>	<b>157</b>
<b>PsLoggedOn</b>	<b>159</b>
<b>PsLogList</b>	<b>161</b>
<b>RootkitRevealer</b>	<b>165</b>
<b>SDelete</b>	<b>168</b>
<b>ShareEnum</b>	<b>169</b>
<b>ShellRunas</b>	<b>170</b>
<b>Runas</b>	<b>172</b>
<b>SigCheck</b>	<b>173</b>
<b>SigVerif</b>	<b>175</b>
<b>Verifier</b>	<b>176</b>

## KAPITOLA 5

<b>Systemové nástroje</b>	<b>179</b>
<b>Coreinfo</b>	<b>180</b>
<b>ProcFeatures</b>	<b>181</b>
<b>PsInfo</b>	<b>181</b>
<b>RAMMap</b>	<b>183</b>
<b>WinObj</b>	<b>184</b>
<b>LoadOrder</b>	<b>186</b>
<b>ClockRes</b>	<b>187</b>
<b>LiveKd</b>	<b>187</b>

<b>Msinfo32</b>	<b>190</b>
<b>GetMac</b>	<b>191</b>
<b>IPconfig</b>	<b>191</b>
<b>Systeminfo</b>	<b>194</b>
KAPITOLA 6	
<b>Ostatní nástroje</b>	<b>197</b>
<b>PsTools</b>	<b>198</b>
<b>Hex2Dec</b>	<b>199</b>
<b>Desktops</b>	<b>200</b>
<b>ZoomIt</b>	<b>201</b>
<b>Strings</b>	<b>202</b>
<b>BglInfo</b>	<b>204</b>
<b>Reg a Regedit</b>	<b>206</b>
<b>RegJump</b>	<b>218</b>
<b>RegDelNull</b>	<b>219</b>
<b>DebugView</b>	<b>220</b>
<b>Ctrl2Cap</b>	<b>221</b>
<b>BlueScreen</b>	<b>222</b>
<b>Clip</b>	<b>222</b>
<b>RecDisk</b>	<b>223</b>
<b>Mrt (Malicious Removal Tool)</b>	<b>223</b>
<b>Choice</b>	<b>224</b>
<b>Makecab</b>	<b>224</b>
<b>Cmdkey</b>	<b>227</b>
<b>Winsat</b>	<b>228</b>
<b>Wusa</b>	<b>230</b>
PŘÍLOHY	231
<b>Slovník</b>	<b>231</b>
<b>Klávesové zkratky</b>	<b>236</b>
<b>Systemové konzole</b>	<b>236</b>
<b>Ovládací panely</b>	<b>238</b>
<b>Systemové proměnné</b>	<b>240</b>
REJSTŘÍK	243