

# How to Cheat at Securing Windows 2000 TCP/IP

Copyright 2003 by Syngress Publishing,  
all rights reserved

*How to Cheat at Being a Windows 2000 System Administrator* \_\_ *Error! Bookmark not defined.*

<b>TOPIC 1: A TCP/IP Primer</b> _____	<b>5</b>
<b>IP Address Classes and Subnets</b> _____	<b>5</b>
<b>Subnets and Routing</b> _____	<b>5</b>
<b>TOPIC 2: The OSI Model</b> _____	<b>7</b>
<b>Seven Layers of the Networking World</b> _____	<b>7</b>
<b>TOPIC 3: The TCP/IP Protocol Suite</b> _____	<b>8</b>
<b>TCP/IP Core Protocols</b> _____	<b>9</b>
TCP _____	9
UDP _____	9
<b>IP</b> _____	<b>9</b>
<b>The Three-Way Handshake</b> _____	<b>10</b>
ARP _____	10
ICMP _____	11
IGMP _____	11
<b>TCP/IP Applications</b> _____	<b>11</b>
<b>TOPIC 4: Windows 2000 TCP/IP Stack Enhancements</b> _____	<b>13</b>
<b>NetBT and WINS</b> _____	<b>13</b>
DHCP _____	14
DNS _____	14
SNMP _____	14
<b>TOPIC 5: Using TCP/IP Utilities</b> _____	<b>15</b>
<b>ARP</b> _____	<b>15</b>
<b>Hostname</b> _____	<b>15</b>
<b>Ipconfig</b> _____	<b>15</b>
<b>Nbtstat</b> _____	<b>16</b>
<b>Netstat</b> _____	<b>16</b>
<b>Nslookup</b> _____	<b>17</b>

<b>Ping</b>	<b>17</b>
<b>Route</b>	<b>18</b>
<b>Tracert</b>	<b>18</b>
<b>Pathping</b>	<b>19</b>
<b>Netdiag</b>	<b>20</b>
<b>SNMP</b>	<b>21</b>
How Does SNMP Work?	21
Installing the Agent	22
<b><i>TOPIC 6: Using Windows 2000 Monitoring Tools</i></b>	<b>24</b>
<b>Basic Monitoring Guidelines</b>	<b>24</b>
<b>Performance Logs and Alerts</b>	<b>24</b>
<b>Counters</b>	<b>25</b>
<b>Log File Format</b>	<b>25</b>
<b>Alerts</b>	<b>25</b>
<b>Network Monitor</b>	<b>26</b>
Filtering	26
Security Issues	26
Using Network Monitor	26
Capture Window Panes	26
Buffer	27
Collecting Data	27
Filtered Captures	28
Filtering by Address Pairs	28
Display Filters	29
<b><i>TOPIC 7: Secure Sockets Layer</i></b>	<b>30</b>
<b>How a Secure SSL Channel Is Established</b>	<b>30</b>
<b>Symmetric and Asymmetric Encryption</b>	<b>31</b>
Symmetric Encryption	31
Asymmetric Encryption	32
Hash Algorithms	33
Digital Certificates	33
Certificate Authorities	33
SSL Implementation	34
<b><i>TOPIC 8: Secure Communications over Virtual Private Networks</i></b>	<b>35</b>
<b>Tunneling Basics</b>	<b>35</b>
<b>VPN Definitions and Terminology</b>	<b>35</b>
<b>How Tunneling Works</b>	<b>35</b>
IP Addressing	36

<b>Security Issues Pertaining to VPNs</b>	<b>36</b>
Encapsulation	36
User Authentication	36
<b>Data Security</b>	<b>36</b>
<b>Windows 2000 Security Options</b>	<b>37</b>
<b>Common VPN Implementations</b>	<b>38</b>
<b>Remote User Access Over the Internet</b>	<b>38</b>
<b>Connecting Networks Over the Internet</b>	<b>38</b>
Sharing a Remote Access VPN Connection	38
Using a Router-to-Router Connection	39
<b>Tunneling Protocols and the Basic Tunneling Requirements</b>	<b>39</b>
<b>Windows 2000 Tunneling Protocols</b>	<b>39</b>
Point to Point Tunneling Protocol (PPTP)	39
Layer 2 Tunneling Protocol (L2TP)	39
Using PPTP with Windows 2000	39
How to Configure a PPTP Device	40
Using L2TP with Windows 2000	40
How to Configure L2TP	40
How L2TP Security Differs from PPTP	41
<b>Interoperability with Non-Microsoft VPN Clients</b>	<b>41</b>
<b><i>TOPIC 9: IPSec for Windows 2000</i></b>	<b>42</b>
<b>Overview of IPSec Cryptographic Services</b>	<b>42</b>
Message Integrity	42
Hashing Messages	43
<b>Message Authentication</b>	<b>43</b>
Preshared Key Authentication	43
Kerberos Authentication	44
Public Key Certificate-Based Digital Signatures	44
<b>Confidentiality</b>	<b>44</b>
<b>IPSec Security Services</b>	<b>44</b>
Authentication Header (AH)	44
Encapsulating Security Payload (ESP)	45
<b><i>TOPIC 10: Security Associations and IPSec Key Management Procedures</i></b>	<b>46</b>
<b>IPSec Key Management</b>	<b>46</b>
Phase 1: Establishing the ISAKMP SA	46
Phase 2: Establishing the IPSec SA	47
<b><i>TOPIC 11: Deploying IPSec</i></b>	<b>48</b>
<b>Building Security Policies with Customized IPSec Consoles</b>	<b>48</b>
Building an IPSec MMC Console	48

<b>Flexible Security Policies</b>	<b>48</b>
<b>Rules</b>	<b>49</b>
Filter Actions	49
<b>Flexible Negotiation Policies</b>	<b>50</b>
<b>Filters</b>	<b>50</b>
<b>Creating a Security Policy</b>	<b>51</b>
<b>Making the Rule</b>	<b>51</b>