



# Contents

<b>1</b>	<b>Introduction</b> .....	<b>7</b>
1.1	Connecting Tubes	7
1.2	Intended Audience	7
1.3	Free for Students	8
1.4	Thanks and Contact Information	8
<b>2</b>	<b>The Basics</b> .....	<b>9</b>
2.1	Network Requirements	9
2.2	Linux Server Convention	9
2.3	Linux BASH aliases	9
2.4	Windows Doskey Macros (aka Windows aliases)	10
2.5	Commands Overview	12
2.5.1	SSH Server .....	12
2.5.2	SSH Client .....	12
2.5.3	Netcat .....	13
2.5.4	nmap .....	14
2.5.5	proxychains .....	14
2.6	Networking Basics	14
2.6.1	Network Interface Cards .....	14
2.6.2	House Analogy .....	14
<b>3</b>	<b>SSH -L Port Forward to 127.0.0.1</b> .....	<b>17</b>
3.1	Overview	17
3.2	First Connection	17

3.3	Netcat Chat	18
3.4	Netcat Shell	19
3.5	Gophish Admin Panel	19
3.6	Ghost Blog Admin Panel	21
<b>4</b>	<b>SSH -L Port Forward to Remote Targets</b> .....	<b>23</b>
4.1	Overview	23
4.2	Netcat Chat	24
4.3	SSH to Linux Target	24
4.4	SSH Tunnels, within Tunnels, within Tunnels	25
4.5	Remote Desktop Protocol through a Jumpbox	27
4.6	Web Browsing	29
4.7	Throwing Exploits	31
<b>5</b>	<b>SSH -R Remote Port Forward Listening on 127.0.0.1</b> .....	<b>35</b>
5.1	Overview	35
5.2	First Connection	35
5.3	Netcat Chat	36
5.4	Scantron Agent Tunnels	37
<b>6</b>	<b>SSH -R Remote Port Forward Listening on ens33</b> .....	<b>41</b>
6.1	Overview	41
6.2	Netcat Chat	41
6.3	WWW Server to 127.0.0.1	42
6.4	Exploit Callbacks Using -R	43
<b>7</b>	<b>SSH -D SOCKS Proxy</b> .....	<b>47</b>
7.1	Overview	47
7.2	Installing proxychains	47
7.3	Netcat Chat	47
7.4	Web Browsing	49
7.4.1	Firefox .....	50
7.4.2	Chrome .....	50
7.5	curl	51
7.6	nmap Scanning	52
7.7	Wfuzz Web Directory Brute Forcing	53
<b>8</b>	<b>Advanced Topics</b> .....	<b>55</b>
8.1	Overview	55
8.2	Linux Redirector - redir	55
8.3	Linux Redirector - rinetd	56
8.4	Windows Redirector - netsh	57

8.5	netsh + Meterpreter = <3	59
8.6	Windows Redirector - fpipe	60
8.7	Windows Redirector - winrelay	61
8.8	Shadowsocks - An SSH -D Alternative	62
8.9	Sharing Port Forwards and SOCKS Proxies	64
8.10	Meterpreter portfwd Module	65
8.11	Metasploit SOCKS Proxies	67
8.12	Privilege Escalation	71
<b>9</b>	<b>Credits</b> .....	<b>77</b>
9.1	Book Cover Artwork	77
9.2	LaTeX Template	77
9.3	Chapter Photos	77
9.4	Change Log	78
	<b>Index</b> .....	<b>79</b>