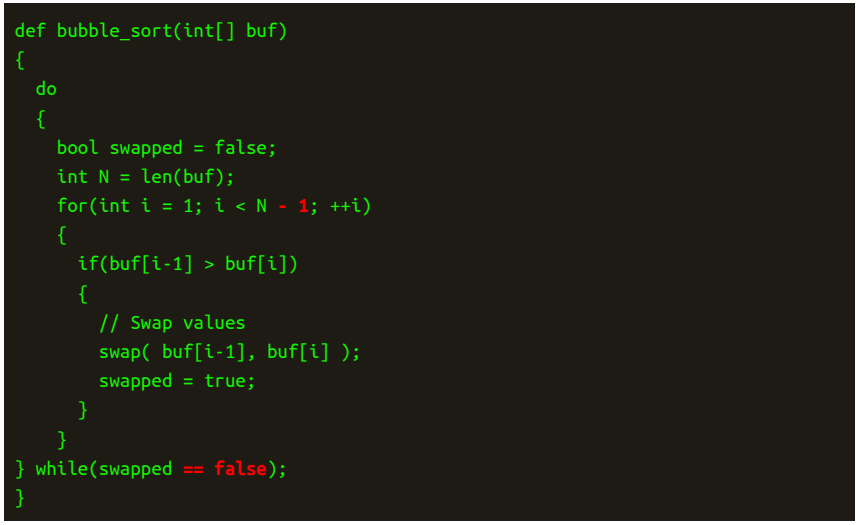
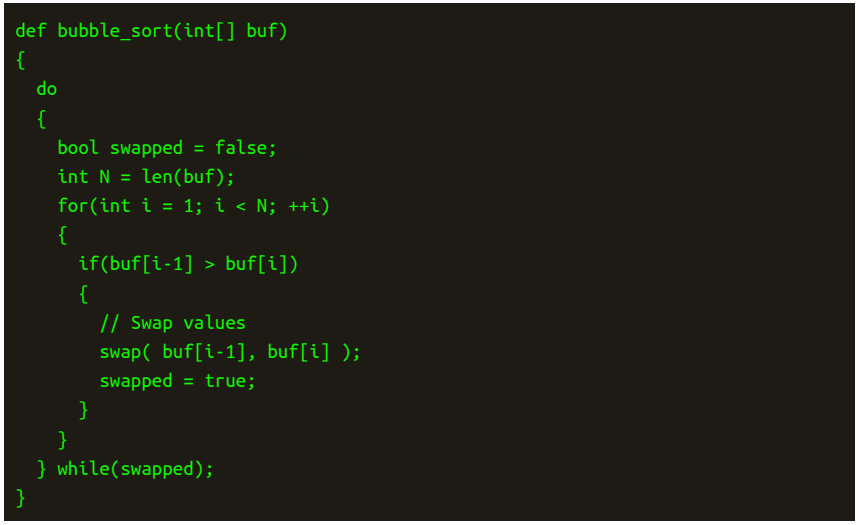
Attacking Network Protocols

A Hacker's Guide to Capture, Analysis, and Exploitation

by James Forshaw

errata updated to print 7

Page	Error	Correction	Print corrected
3	This layer contains network protocols, such as the *HyperText Transport Protocol (HTTP)*, which transfers web page contents; the *Simple Mail Transport Protocol (SMTP)*, which transfers email; and the *Domain Name System (DNS)* protocol, which converts a name to a node on the network.	This layer contains network protocols, such as the *HyperText Transport Protocol (HTTP)*, which transfers web page contents; the *Simple Mail Transport Protocol (SMTP)*, which transfers email; and the *Domain Name System (DNS)* protocol, which converts a name to **an address of** a node on the network.	Print 2
6	Ethernet uses a **64**-bit value called a Media Access Control	Ethernet uses a **48**-bit value called a Media Access Control	Print 2
28–29	The Windows system proxy supports only SOCKS version 4 proxies, which means it will resolve **only local hostnames**.	The Windows system proxy supports only SOCKS version 4 proxies, which means it will resolve **hostnames locally**.	Print 2
42	Because the Internet RFCs invariably use big endian as the preferred type for all network protocols they specify (unless there are legacy reasons for doing otherwise), big endian is referred as network order.	Because the Internet RFCs invariably use big endian as the preferred type for all network protocols they specify (unless there are legacy reasons for doing otherwise), big endian is referred **to** as network order.	Print 2
60	If percent encoding was used to encode the value in Figure 3-18, you would get %06%E3**%58**.	If percent encoding was used to encode the value in Figure 3-18, you would get %06%E3**X**.	Print 2
137	If you look at the files distributed with a .NET application, you'll see files with *.exe* and ***.ddl*** extensions, and you'd be forgiven for assuming they're just native executables.	If you look at the files distributed with a .NET application, you'll see files with *.exe* and ***.dll*** extensions, and you'd be forgiven for assuming they're just native executables.	Print 2
169	One advantage to this model is that because only public key information is ever distributed, it's possible to provide **component** certificates to users via public networks.	One advantage to this model is that because only public key information is ever distributed, it's possible to provide **root** certificates to users via public networks.	Print 2
217	In the C language, this usually results in an error value being returned from the allocation functions (usually a **NUL** pointer); in other languages, it might result in the termination of the environment or the generation of an exception.	In the C language, this usually results in an error value being returned from the allocation functions (usually a **NULL** pointer); in other languages, it might result in the termination of the environment or the generation of an exception.	Print 2

Page	Error	Correction	Print corrected
224			Print 2
253	As an example, consider the networked application shown in Listing **107**.	As an example, consider the networked application shown in Listing **10-7**.	Print 2
264	The addresses of the two strings with the final **NUL** (which is represented by a 0) are then pushed onto the stack in reverse order.	The addresses of the two strings with the final **NULL** (which is represented by a 0) are then pushed onto the stack in reverse order.	Print 2
264	Next, a single **NUL** is pushed on the stack for the environment array . . .	Next, a single **NULL** is pushed on the stack for the environment array . . .	Print 2
264			Print 2