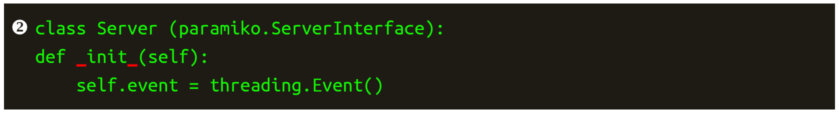
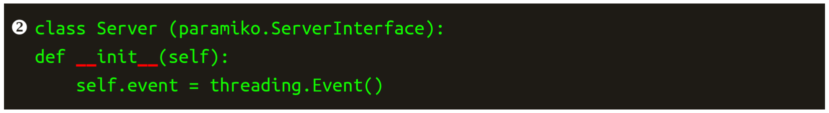
Black Hat Python, 2nd edition

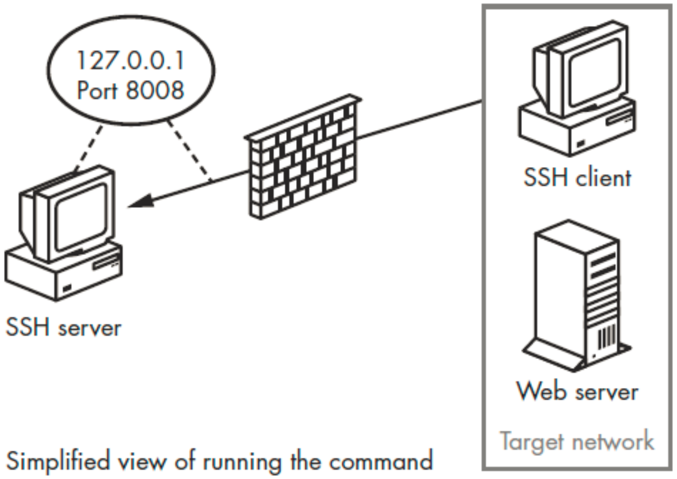
Python Programming for Hackers and Pentesters

by Justin Seitz & Tim Arnold

errata updated to print 4

Page	**Error**	**Correction**	**Print corrected**
4	Deletion	~~You can search for packages and install them into your virtual environment with `pip`:~~ ~~`(venv3) tim@kali: ~/bhp: pip search hashcrack`~~	Print

28	
	`❷ class Server (paramiko.ServerInterface):`
	`  def _init_(self):`
	`      self.event = threading.Event()`
		
		`❷ class Server (paramiko.ServerInterface):`
		`  def __init__(self):`
		`      self.event = threading.Event()`
			Print 4

31	Figure replacement	 127.0.0.1 Port 8008 SSH client SSH server Web server Target network Simplified view of running the command `ssh justin@sshserver -R 8008:webserver:80` *Figure 2-2: SSH reverse tunneling*	Print 4

37	. . . on the network **interface.An** *input/output control (IOCTL)* is a means . . .	. . . on the network **interface. An** *input/output control (IOCTL)* is a means . . .	Print 4
39	("ihl", c_ubyte, 4), # 4 bit unsigned char ("version", c_ubyte, 4), # 4 bit unsigned char	("version", c_ubyte, 4), # 4 bit unsigned char ("ihl", c_ubyte, 4), # 4 bit unsigned char	Print 2

107	self._callbacks.includeInScope(java_url)
	          else:
	            print('Empty response from Bing.: %s'
	                % bing_query_string)
	         return
		self._callbacks.includeInScope(java_url)
		      else:
		        print('Empty response from Bing.: %s'
		            % bing_query_string)
		     return
			Print 4

113	def display_wordlist(self):
	    print ("#!comment: BHP Wordlist for site(s) %s" % ", ".join(self.hosts)) ❸
	
	    for word in sorted(self.wordlist):
	        for password in self.mangle(word):
	            print password
	
	    return
		def display_wordlist(self):
		    print("#!comment: BHP Wordlist for site(s) %s" % ", ".join(self.hosts)) ❸
		
		    for word in sorted(self.wordlist):
		        for password in self.mangle(word):
		            print(password)
		
		    return
			Print 4

129	windll.user32.GetWindowTextA(hwnd, byref(window_title), 512)
	   try:
	       self.current_window = window_title.value.decode()
	   except UnicodeDecodeError as e:
	       print(f'{e}: window name unknown')
	
	  ❻ print('\n', process_id,
	         executable.value.decode(), self.current_window)
	
	   windll.kernel32.CloseHandle(hwnd)
	   windll.kernel32.CloseHandle(h_process)
		windll.user32.GetWindowTextA(hwnd, byref(window_title), 512)
		 try:
		     self.current_window = window_title.value.decode()
		 except UnicodeDecodeError as e:
		     print(f'{e}: window name unknown')
		
		❻ print('\n', process_id,
		       executable.value.decode(), self.current_window)
		
		 windll.kernel32.CloseHandle(hwnd)
		 windll.kernel32.CloseHandle(h_process)
			Print 4