

Ethical Hacking

A Hands-on Introduction to Breaking In

by Daniel G. Graham

errata updated to print 2

Page	Error	Correction	Print corrected
3	Insertion	When installing VirtualBox on Windows, users will need to install the VirtualBox Extensions.	Print 2
5	Insertion	When installing the new version of pfSense, readers will need to select the Auto (UFS) BIOS option.	Print 2
10	Open the Kali Linux virtual machine in VirtualBox. If your Kali Linux displays nothing but a black screen, make sure the PAE/ NK checkbox is selected.	Open the Kali Linux virtual machine in VirtualBox. If your Kali Linux displays nothing but a black screen, make sure the PAE/ NX checkbox is selected.	Print 2
10	Deletion	On the left side of the page, you should see a folder icon. Click it and select your downloaded OVA file.	Print 2
41	<pre>ip.src == 192.168.1.101 ip.dst == 192.168.1.101</pre>	<pre>ip.src == 192.168.1.101 ip.dst == 192.168.1.101</pre>	Print 2
91	TLS uses HASHA @hashbased message authentication codes (HMACs) to verify messages.	TLS uses hashbased message authentication codes (HMACs) to verify messages.	Print 2

Page	Error	Correction	Print corrected
94	Figure 6-5 replacement	<p>Figure 6-5: The path of official certificates</p>	Print 2
100	<p>Let's use the HKDF function to derive a key and encrypt a file:</p> <pre>kali@kali:~\$ openssl enc -aes-256-ctr -hkdf -e -a -in plain.txt -out encrypted.txt -pass file:AliceSharedSecret.bin</pre>	<p>Let's use a key derivation function to derive a key and encrypt a file. Instead of using HKDF we will use the PBKDF2 function supported by openssl.</p> <pre>kali@kali:~\$ openssl enc -aes-256-ctr -pbkdf2 -e -a -in plain.txt -out encrypted.txt -pass file:AliceSharedSecret.bin</pre>	Print 2