

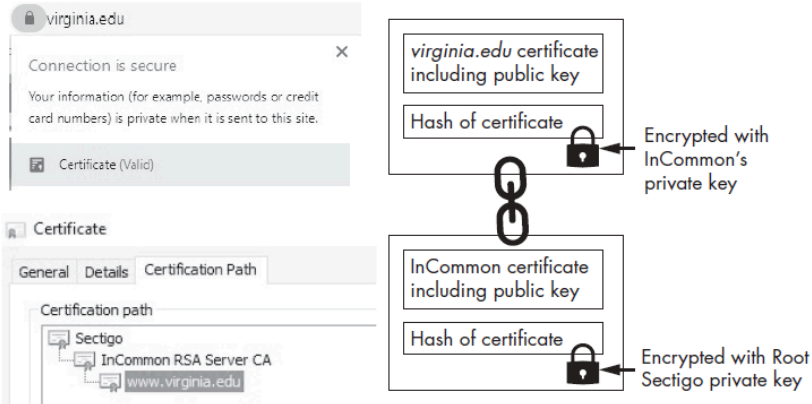
Ethical Hacking

A Hands-on Introduction to Breaking In

by Daniel G. Graham

errata updated to print 4

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
8	<pre>LAN (lan) -> em1 -> v4: 192.1689.100.1/24</pre>	<pre>LAN (lan) -> em1 -> v4: 192.168.100.1/24</pre>	Print 3
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
78	4. Use the <i>extended Euclidean</i> algorithm to compute the public key (d) by choosing an integer d such that $ed \bmod z = 1$.	4. Use the <i>extended Euclidean</i> algorithm to compute the private key (d) by choosing an integer d such that $ed \bmod z = 1$.	Print 3
91	TLS uses HASHA @ <i>hashbased message authentication codes (HMACs)</i> to verify messages.	TLS uses <i>hashbased message authentication codes (HMACs)</i> 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
163	Then comes the 16-bit <i>Client TLS Version</i> , which is the version of TLS that the client is currently running, and the 32-bit <i>Client Random</i> , a nonce supplied during the TLS exchange.	Then comes the 16-bit <i>Client TLS Version</i> , which is the version of TLS that the client is currently running, and the 32-byte <i>Client Random</i> , a nonce supplied during the TLS exchange.	Print 3
166	<pre>0x00, 0x40 # Payload length 64KB</pre>	<pre>0x40, 0x00 # Payload length 64KB</pre>	Print 4
194-195	postint	postinst	Print 4
195	<pre>touch ~/Desktop/Malware/trojans/mailTrojan/postint</pre>	<pre>touch ~/Desktop/Malware/trojans/mailTrojan/DEBIAN/postinst</pre>	Print 4
254	<pre>kali@kali:~\$ sqlmap -u "http://<Metasploitable-IP>/mutillidae/index.php?page= → user-info.php&username=&password=&" --sqlmap-shell sqlmap-shell></pre>	<pre>kali@kali:~\$ sqlmap -u "http://<Metasploitable-IP>/mutillidae/index.php?page= → user-info.php&username=user&password=123&user-info-php-submit-button= → view+Account+Details" --shell sqlmap-shell></pre>	Print 4

Page	Error	Correction	Print corrected
254	<pre>sqlmap-shell> --dbs [16:16:04] [INFO] testing connection to the target URL</pre>	<pre>sqlmap-shell> --dbs --skip="user,page,user-info-php-submit-button" -p password [16:16:04] [INFO] testing connection to the target URL</pre>	Print 4
304	<pre>msfadmin@metasploitable:~\$ iptables -t nat -A POSTROUTING -s 10.0.0.0/24 -o eth1 -j MASQUERADE</pre> <p>Check to see whether you can access the outside world by pinging the pfSense firewall from your Ubuntu virtual machine in the private LAN:</p> <pre>victim@ubuntu:~\$ ping 192.168.1.1</pre>	<pre>msfadmin@metasploitable:~\$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE</pre> <p>Run the following command to allow forwarding from eth1 to eth0:</p> <pre>msfadmin@metasploitable:~\$ sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT</pre> <p>Check to see whether you can access the outside world by pinging the pfSense firewall from your Ubuntu virtual machine in the private LAN:</p> <pre>victim@ubuntu:~\$ ping 192.168.1.1</pre> <p>To enable DNS, edit the <code>/etc/resolv.conf</code> file and set the <code>nameserver</code> to <code>10.0.0.1</code>.</p>	Print 4