Linux Basics for Hackers

Getting Started with Networking, Scripting, and Security in Kali

by OccupyTheWeb

updated to print 10

Page	Error	Correction	Print corrected
xxiii	Text insertion	Beginning with Kali 2020 and later versions, Kali provides you a username and password set to Kali.	Print 7
xxxvi	Text insertion	If you are using Kali 2020 or later, you will need to use the `sudo` before any command that requires root privileges. These later versions of Kali will respond with `'command not found'` when the command requires root privileges. Simply precede the command with `sudo`.	Print 7
7	• You would use `..` to move up one level. • You would use `.. ..` to move up two levels. • You would use `.. .. ..` to move up three levels, and so on. So, for example, to move up two levels, enter `cd` followed by two sets of double dots with a **space** in between: `kali >cd .. ..`	• You would use `..` to move up one level. • You would use `../..` to move up two levels. • You would use `../../..` to move up three levels, and so on. So, for example, to move up two levels, enter `cd` followed by two sets of double dots with a **forward slash** in between: `kali >cd ../..`	Print 2
12	`kali >find /etc -type f --name apache2.*`	`kali >find /etc -type f -name apache2.`	Print 5
23	`kali >nl /etc/snort.conf | grep output`	`kali >nl /etc/snort/snort.conf | grep output`	Print 2
27	1. Navigate to ***/usr/share/wordlists/metasploit***. This is a directory of multiple wordlists that can be used to brute force passwords in various password-protected devices using Metasploit, the most popular pentesting and hacking framework. 2. Use the `cat` command to view the contents of the file ***passwords.lst***. 3. Use the `more` command to display the file ***passwords.lst***. 4. Use the `less` command to view the file ***passwords.lst***. 5. Now use the `nl` command to place line numbers on the passwords in ***passwords.lst***. There should be around 88,396 passwords. 6. Use the `tail` command to see the last 20 passwords in ***passwords.lst***. 7. Use the `cat` command to display ***passwords.lst*** and pipe it to find all the passwords that contain *123*.	1. Navigate to ***/usr/share/metasploit-framework/data/wordlists***. This is a directory of multiple wordlists that can be used to brute force passwords in various password-protected devices using Metasploit, the most popular pentesting and hacking framework. 2. Use the `cat` command to view the contents of the file ***password.lst***. 3. Use the `more` command to display the file ***password.lst***. 4. Use the `less` command to view the file ***password.lst***. 5. Now use the `nl` command to place line numbers on the passwords in ***password.lst***. There should be around 88,396 passwords. 6. Use the `tail` command to see the last 20 passwords in ***password.lst***. 7. Use the `cat` command to display ***password.lst*** and pipe it to find all the passwords that contain *123*.	Print 2
99	`kali >dd if=/dev/media of=/root/flashcopy bs=4096 conv:noerror`	`kali >dd if=/dev/media of=/root/flashcopy bs=4096 conv=noerror`	Print 5
158	The syntax here is straightforward: simply plug in **`airdump-ng`**, . . .	The syntax here is straightforward: simply plug in **`airodump-ng`**, . . .	Print 10
159	`aireplay-ng --deauth 100 -a 01:01:AA:BB:CC:22 -c A0:A3:E2:44:7C:E5 wlan0mon`	`aireplay-ng --deauth 100 -a 01:02:CC:DD:03:CF -c A0:A3:E2:44:7C:E5 wlan0mon`	Print 5
189	`HackersAriseDictionary = {'name': 'OccupyTheWeb', 'value' : 27)`	`HackersAriseDictionary = {'name': 'OccupyTheWeb', 'value' : 27}`	Print 5