Cheatography

Aircrack Suite - Kali Linux Cheat Sheet

by [deleted] via cheatography.com/22164/cs/4465/

Linux basics

pwd	Specifies your current directory
ls	List contents of the current directory
rm *words.txt*	removes the file *words.txt*
rm -r *folder*	Recursively removes the directory *folder*
ctrl+c	End a program
ifconfig	List network interfaces
man *application*	Opens the help manual for the specified application

airmon-ng

airmon-ng	Show current interfaces
airmon-ng start *wlan#*	Start monitoring on the specified interface
airmon-ng stop *wlan#*	Stop monitoring on the specified interface

airodump-ng

airodump-ng <options> <mon#>	
airodump-ng -w *prac* mon0	Start a collecton called *prac* on mon0
airodump-ng --channel *8* mon0	Start a collecton on channel *8* using mon0
airodump-ng --output-format *pcap* mon0	Start a collection, outputting to a *.pcap* file using mon0
Available formats are:	pcap, ivs, csv, csv, gps, kismet and/or netxml
airodump-ng --bssid *##:##:##:##:##:##* mon0	Starts collecting on BSSID *##:##:##:##:##:##* using mon0
airodump-ng --essid *Redback* mon0	Starts collecting on ESSID *Redback* using mon0
airodump-ng -a mon0	Starts collecting on mon0 while excluding unassociated clients

aircrack-ng

aircrack-ng <options> <.cap/.ivs file>	
aircrack-ng prac.cap	Attemtps to crack the WEP encryption on prac.cap
aircrack-ng -l *password.txt* prac.cap	Attemtps to crack the WEP encryption on prac.cap and saves it to *password.txt*
aircrack-ng -w darkc0de.lst prac.cap	Attemtps to crack the WPA encryption on prac.cap using the darkc0de.lst dictionary

airdecap-ng

airdecap-ng <options> <.pcap file>	
airdecap-ng -e *Redback* -w ##:##:##:##:## prac.cap	Decrypts WEP data from the *Redback* network using cracked key *##:##:##:##:##*
airdecap-ng -e *Redback* -p *password* prac.cap	Decrypts WPA data from the *Redback* network using the password *password*

Sponsored by **Readable.com**
Measure your website readability!
https://readable.com