

São Carlos, 19 de Maio de 2010

Prática 5 - Sniffing

1. Introdução

Sniffing é um procedimento de captura de pacotes em determinada rede através de alguma ferramenta (*sniffer*). Estas ferramentas também são conhecidas como analisadores de rede e analisadores de protocolo.

Este procedimento pode ser utilizado tanto para gerenciamento da rede, como para propósitos maliciosos. Tipicamente, administradores de rede utilizam estas ferramentas para entender quais os recursos da rede mais utilizados, enquanto, hackers utilizam para interceptar informações sigilosas trocadas pelos usuários da rede.

Nesta prática utilizaremos faremos o *sniffing* das redes wireless do campus II. Como as redes internas utilizam criptografia WPA, criaremos uma nova rede (com outro AP) para analisar o tráfego gerado.

2. Materiais

Utilizaremos os seguintes materiais:

- Notebook com interface Ethernet
- Linux BT4 (Live CD)
- Kismet
- Wireshark

3. Descrição da Prática

Os alunos se dividirão em grupos de 4 pessoas, e cada grupo receberá um notebook. Em seguida anote o número do notebook na folha de presença na frente do nome.

3.1 Kismet

O Kismet é uma ferramenta de sniffing de pacotes em redes wireless. Para configurá-lo basta editar a seguinte linha no arquivo `/etc/kismet/kismet.conf`

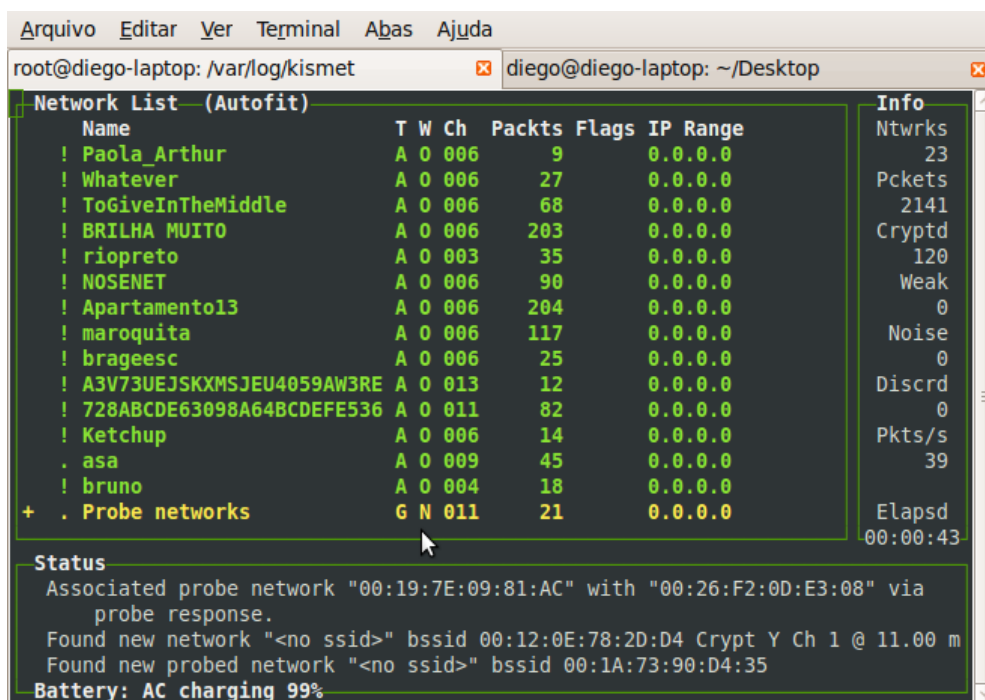
source=none,none,none

para

source=nome_do_driver_da_interface,nome_da_interface,alias

Os notebooks do lab utilizam interface de rede da Intel com o chipset 5100. O (provável) nome do driver é `ipw5100`. O segundo parâmetro é **wlan0**, e o terceiro é apenas um nome que vai aparecer no kismet (escolha qualquer coisa!).

Abra o Kismet (digite `kismet` no terminal), e será exibida uma tela similar a esta:



The screenshot shows the Kismet terminal interface. At the top, there are menu options: Arquivo, Editar, Ver, Terminal, Abas, Ajuda. Below that, the terminal title bar shows the current directory: `root@diego-laptop: /var/log/kismet` and the user's location: `diego@diego-laptop: ~/Desktop`.

The main display is divided into two sections. The top section is titled "Network List (Autofit)" and contains a table with the following columns: Name, T, W, Ch, Packts, Flags, and IP Range. The data rows are as follows:

Name	T	W	Ch	Packts	Flags	IP Range
! Paola_Arthur	A	0	006	9		0.0.0.0
! Whatever	A	0	006	27		0.0.0.0
! ToGiveInTheMiddle	A	0	006	68		0.0.0.0
! BRILHA MUITO	A	0	006	203		0.0.0.0
! riopreto	A	0	003	35		0.0.0.0
! NOSENET	A	0	006	90		0.0.0.0
! Apartamento13	A	0	006	204		0.0.0.0
! maroquita	A	0	006	117		0.0.0.0
! brageesc	A	0	006	25		0.0.0.0
! A3V73UEJSKXMSJEU4059AW3RE	A	0	013	12		0.0.0.0
! 728ABCDE63098A64BCDEF536	A	0	011	82		0.0.0.0
! Ketchup	A	0	006	14		0.0.0.0
. asa	A	0	009	45		0.0.0.0
! bruno	A	0	004	18		0.0.0.0
+ . Probe networks	G	N	011	21		0.0.0.0

The right side of the terminal shows an "Info" panel with the following statistics: Ntwrks: 23, Pckets: 2141, Cryptd: 120, Weak: 0, Noise: 0, Discrd: 0, Pkts/s: 39, and Elapsed: 00:00:43.

The bottom section is titled "Status" and contains the following text: "Associated probe network "00:19:7E:09:81:AC" with "00:26:F2:0D:E3:08" via probe response." "Found new network "<no ssid>" bssid 00:12:0E:78:2D:D4 Crypt Y Ch 1 @ 11.00 m" "Found new probed network "<no ssid>" bssid 00:1A:73:90:D4:35". At the very bottom, it says "Battery: AC charging 99%".

O Kismet armazenará automaticamente os pacotes capturados na pasta `/var/log/kismet`.

Para exibir o menu de ajuda da ferramenta digite *h*.

1) Forneça o SSID, BSSID, o padrão utilizado (*carrier*), o canal utilizado, a quantidade de clientes conectados e o tipo de encriptação (caso exista) para duas redes detectadas pelo kismet.

Em seguida utilizaremos o Wireshark para analisar os pacotes capturados. Abaixo segue a interface gráfica do Wireshark:

Abra o arquivo com a extensão *.dump* gerado pelo Kismet e responda as seguintes perguntas.

2) Dentre os pacotes capturados qual a proporção dos pacotes de dados?

3) Podemos interceptar informações importantes com o kismet/wireshark?

4) Um administrador de rede pode detectar a presença de um sniffer em uma rede cabeada? E para o caso de redes Wireless?

5) Quais procedimentos gerenciais um administrador de redes pode executar com o auxílio de sniffers?

6) Quais medidas você adotaria para evitar sniffers em redes cabeadas e wireless?