Aircrack-ng (Hack-WiFi) на пенсии
Аудит WiFi сетей / MikroTik Радар

Начало статьи https://crimea-karro.ru/download/Aircrack_ng_to_RouterOS.pdf

Использование MikroTik как базу, для нужд и анализа WiFi сетей, дело весьма удобное. Малые габариты и мобильность позволят использовать роутер как точку сбора информации (сканирования) в любом месте и в любое время автоматически. Для этого создадим простейший скрипт (вы должны знать базу по работе с скриптами в MikroTik)…

```
# Message/Date/SysTime
:log info "Log WiFi-Center Sended to email...";
:local date [/system clock get date];
:local sysname [/system identity get name];
:local months ("jan","feb","mar","apr","may","jun","jul","aug","sep","oct","nov","dec");
:local month ([:find $months [:pick $date 0 3 ]] + 1);
:if ($month < 10) do={:set month ("0" . $month);};
:local sysver [/system package get system version];
:local name "$[/system identity get name].$[:pick $date 7 11].$month.$[:pick $date 4 6].backup";

#Scan WiFi
/interface wireless scan wlan1 rounds=1 save-file=$name
:delay 30s;

#Send email
/tool e-mail send to="it@crimea-karro.ru" subject="$[/system identity get name]  WiFi Scaner" \
body="$[/system clock get date] WiFi Scan File / Bunker-01" file=$name

#Delete file
:delay 10s;
/file remove $name

:log info "Log WiFi- Center Sended...";
```

Скрипт довольно прост:

```
# Message/Date/SysTime

:log info "Log WiFi-Center Sended to email...";
:local date [/system clock get date];
:local sysname [/system identity get name];
:local months ("jan","feb","mar","apr","may","jun","jul","aug","sep","oct","nov","dec");
:local month ([:find $months [:pick $date 0 3 ]] + 1);
:if ($month < 10) do={:set month ("0" . $month);};
:local sysver [/system package get system version];
:local name "$[/system identity get name].$[:pick $date 7 11].$month.$[:pick $date 4 6].backup";
```

Пишем в лог файл роутера информацию о создании отчета, определяем имя файла (переменные) по дате сканирования.

#Scan WiFi

```
/interface wireless scan wlan1 rounds=1 save-file=$name
:delay 30s;
```

Выполняем сканирование доступной зоны, rounds=1 это один проход сканирования, который не мешает рабочей точке доступа в роутере и не отсоединит клиентов (при условии рабочего не мобильного роутера), записываем данные в файл, ожидание 30 секунд после всех действий (возможно CPU роутера загружен).

#Send email

```
/tool e-mail send to="it@karro.ru" subject="$[/system identity get name]  WiFi Scaner" \
body="$[/system clock get date] WiFi Scan File / Bunker-01" file=$name
```

Описание электронного письма, адрес, тело и заголовки (обратите внимание, у вас должна быть настроена отправка данных на Email).

#Delete file

```
:delay 10s;
/file remove $name
:log info "Log WiFi- Center Sended...";
```

Ожидаем 10 секунд после всех действий (возможно CPU роутера загружен), удаляем созданный файл отчета из памяти роутера (возможно у вас достаточно памяти роутера для хранения, хотя смысла хранения нет). Пишем в лог файл роутера информацию о создании отчета.

Не забывайте о schedule (график выполнения задач и скриптов).
Установите время и цикл для скрипта сканирования…

Start Time - 20:00:00
Interval - 1d 00:00:00
On Event - /system script run script1_scan_wifi (имя выше созданного скрипта).

Пример отчета:

Bunker-01.2018.10.10.backup

```
EC:43:F6:D6:15:1E,'Sev_Love',2412/20-Ce/gn,-79,802.11,privacy,
10:A4:BE:F3:8D:6E,'YICarCam_F38D6E',2412/20/gn,-86,802.11,privacy,
70:4F:57:F4:44:6C,'TP-Link_446C',2412/20-Ce/gn,-90,802.11,privacy,
14:CC:20:3E:12:52,'Traveller',2422/20-Ce/gn,-90,802.11,privacy,
A4:2B:B0:E4:40:5C,'TP-LINK_405C',2452/20-eC/gn,-53,802.11,privacy,
2C:AB:25:0A:A2:6A,'natali',2457/20/gn,-78,802.11,privacy,
34:08:04:81:D5:45,'DLink',2462/20/g,-74,802.11,privacy,
```