

Лабораторна робота №15(5.1.14)

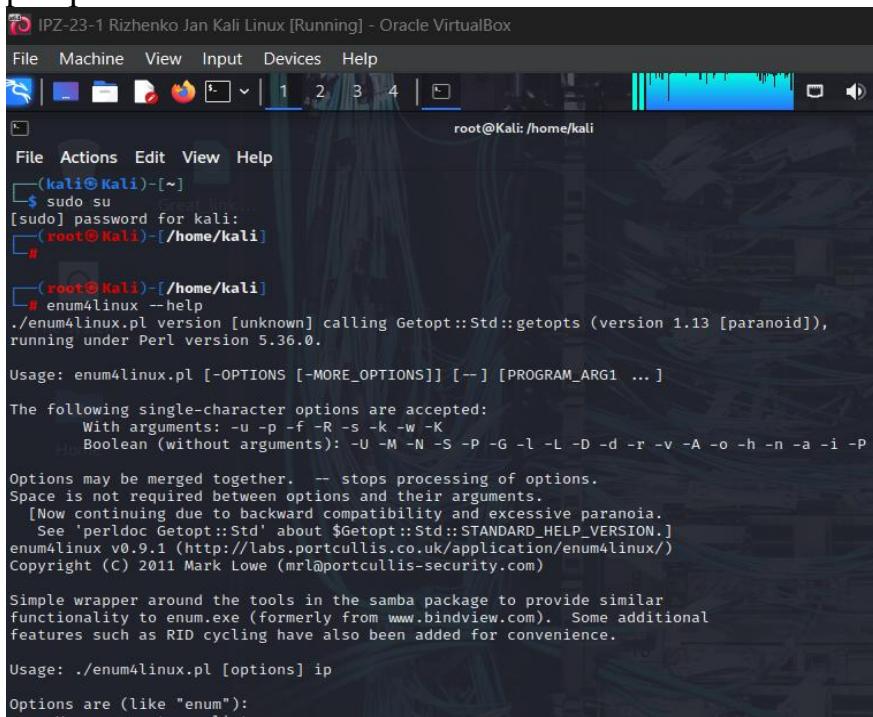
Сканування SMB вразливостей за допомогою enum4linux

Хід роботи:

Частина 1: Запуск enum4linux та дослідження можливостей

Крок 1: Перевірка встановлення enum4linux та перегляд довідки

Завдання: Перевірте наявність enum4linux та ознайомтесь з його можливостями



```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@Kali: /home/kali
File Actions Edit View Help
(kali㉿Kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿Kali)-[/home/kali]
$ 

(root㉿Kali)-[/home/kali]
# enum4linux --help
./enum4linux.pl version [unknown] calling Getopt::Std::getopts (version 1.13 [paranoid]),
running under Perl version 5.36.0.

Usage: enum4linux.pl [-OPTIONS [-MORE_OPTIONS]] [--] [PROGRAM_ARG1 ...]

The following single-character options are accepted:
    With arguments: -u -p -f -R -s -k -w -K
    Boolean (without arguments): -U -M -N -S -P -G -l -L -D -d -r -v -A -o -h -n -a -i -P

Options may be merged together. -- stops processing of options.
Space is not required between options and their arguments.
[Now continuing due to backward compatibility and excessive paranoia.
See 'perldoc Getopt::Std' about $Getopt::Std::STANDARD_HELP_VERSION.]
enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com). Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -u      get userlist
```

Рис. 1. Довідкова сторінка enum4linux з синтаксисом команд та доступними опціями

Питання: Які утиліти Samba використовує інструмент enum4linux згідно довідкового файлу?

Відповідь: Згідно довідкового файлу, enum4linux використовує наступні утиліти Samba: nmblookup (для резолюції NetBIOS імен), net (для керування Samba та віддаленими CIFS серверами), grpcclient (для виконання клієнтських функцій MS-RPC), smbclient (для доступу до SMB/CIFS ресурсів). Ці інструменти агрегуються enum4linux для отримання комплексної інформації про цільові системи Windows та Samba.

Крок 2: Дослідження термінології, пов'язаної з SMB функціями

Завдання: Вивчіть основні терміни Windows та SMB

Питання: Що таке Relative Identifier (RID)?

Відповідь: RID (Relative Identifier) - це відносний ідентифікатор, який є частиною SID (Security Identifier). RID є унікальним числовим значенням, що додається до SID домену для створення повного SID користувача, групи або комп'ютера.

Наприклад, RID 500 завжди вказує на вбудований обліковий запис Administrator, а RID 501 - на Guest. RID дозволяє системі унікально ідентифікувати об'єкти безпеки в межах домену.

Змн.	Арк.	№ докум.	Підпис	Дата	ДУ «Житомирська політехніка».23.121.26.000 – Лр15 (5.1.14)		
Розроб.	Риженко Я.В			Звіт з лабораторної роботи	Літ.	Арк.	Аркушів
Перевір.	Покотило О.А.					1	8
Керівник							
Н. контр.							
Зав. каф.							
ФІКТ Гр. ІПЗ-23-1[2]							

Питання: Що таке Security Identifier (SID)?

Відповідь: SID (Security Identifier) - це унікальний ідентифікатор безпеки, який призначається кожному об'єкту безпеки в Windows (користувачам, групам, комп'ютерам). SID складається з рядка чисел та літер, наприклад S-1-5-21-3623811015-3361044348-30300820-1013. Перша частина ідентифікує домен або локальний комп'ютер, а остання частина (RID) ідентифікує конкретний об'єкт. SID використовується для контролю доступу та залишається незмінним навіть при зміні імені об'єкта.

Питання: Що таке Domain Controller (DC)?

Відповідь: DC (Domain Controller) - це сервер в мережі Windows, який відповідає за автентифікацію користувачів, зберігання інформації про облікові записи та політики безпеки домену в Active Directory. Domain Controller обробляє запити на вхід користувачів, перевіряє облікові дані, застосовує групові політики та синхронізує дані з іншими контролерами домену. Він є центральним компонентом інфраструктури безпеки корпоративної мережі Windows.

Питання: Що таке Lightweight Directory Access Protocol (LDAP)?

Відповідь: LDAP (Lightweight Directory Access Protocol) - це відкритий протокол для доступу та управління розподіленими службами каталогів через мережу TCP/IP. LDAP використовується для зберігання та запиту інформації про користувачів, групи, комп'ютери та інші ресурси в централізованій базі даних. В середовищі Windows LDAP є протоколом доступу до Active Directory, працюючи на порту 389 (незахищений) або 636 (LDAPS з SSL/TLS).

Питання: Що таке Workgroup?

Відповідь: Workgroup - це логічне групування комп'ютерів в однорангової мережі Windows, де кожен комп'ютер управляє своїми власними обліковими записами та ресурсами незалежно. На відміну від домену, workgroup не має централізованої автентифікації або управління політиками безпеки. Користувачі повинні мати окремі облікові записи на кожному комп'ютері, до якого вони хочуть отримати доступ. Workgroup зазвичай використовується в малих домашніх або офісних мережах з обмеженою кількістю комп'ютерів.

Частина 2: Використання Nmap для пошуку SMB серверів

Крок 1: Сканування віртуальних мереж для пошуку потенційних цілей

Завдання: Виявіть хости з SMB службами в підмережах

```
root@Kali: /home/kali
File Actions Edit View Help
[...]
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-20 20:06 UTC
Nmap scan report for metasploitable.vm (172.17.0.2)
Host is up (0.000004s latency).
Not shown: 981 closed tcp ports (reset)
PORT      STATE     SERVICE
22/tcp    filtered ssh
23/tcp    open      telnet
23/tcp    open      filtered
23/tcp    open      filtered
80/tcp    open      http
111/tcp   open      rpcbind
139/tcp   open      netbios-ssn
138/tcp   open      netbios-ds
445/tcp   open      microsoft-ds
512/tcp   open      filtered exec
513/tcp   open      filtered login
514/tcp   open      filtered
1099/tcp  open      filtered rmiregistry
1524/tcp  open      filtered ingreslock
3306/tcp  open      mysql
5432/tcp  open      postgresql
4455/tcp  open      filtered
8009/tcp  open      filtered ajp13
8180/tcp  open      filtered unknown
MAC Address: 02:42:AC:11:00:02 (Unknown)

Nmap scan report for 172.17.0.1
Host is up (0.000004s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE     SERVICE
22/tcp    open      filtered ssh
```

Nmap done: 256 IP addresses (2 hosts up) scanned in 4.54 seconds

Рис. 2. Результати Nmap сканування підмережі 172.17.0.0/24 з виявленими SMB портами

		Рижсенко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр15(5.1.14)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		2

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@Kali ~]# nmap -sN 10.6.6.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2025-12-20 20:08 UTC
Nmap scan report for webgoat.vm (10.6.6.11)
Host is up (0.0000040s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE      SERVICE
8080/tcp  open|filtered  http-proxy
8888/tcp  open|filtered  sun-answerbook
9001/tcp  open|filtered  tor-orport
MAC Address: 02:42:0A:06:06:0B (Unknown)

Nmap scan report for juice-shop.vm (10.6.6.12)
Host is up (0.0000090s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
3000/tcp  open|filtered  ppp
MAC Address: 02:42:0A:06:06:0C (Unknown)

Nmap scan report for dwva.vm (10.6.6.13)
Host is up (0.0000040s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
80/tcp    open|filtered  http
MAC Address: 02:42:0A:06:06:0D (Unknown)

Nmap scan report for mutillidae.vm (10.6.6.14)
Host is up (0.0000040s latency).
Not shown: 998 closed tcp ports (reset)
PORT      STATE      SERVICE
80/tcp    open|filtered  http
3306/tcp  open|filtered  mysql
MAC Address: 02:42:0A:06:06:0E (Unknown)

Nmap scan report for gravemind.vm (10.6.6.23)
Host is up (0.0000040s latency).

```

Рис. 3. Результати Nmap сканування підмережі 10.6.6.0/24 з аналізом відкритих служб

Питання: Що Nmap виявив про хости в мережі 172.17.0.0/24?

Відповідь: Nmap виявив активний хост 172.17.0.2 з відкритими портами, характерними для SMB служб. Сканування показало наявність декількох комп'ютерів у цій підмережі, серед яких принаймні один має налаштовані служби Windows/Samba для файлового та принтерного обміну.

Питання: Які порти відкриті на хості, що ідентифікують запущені SMB служби? Як Nmap називає ці служби?

Відповідь: На хості відкриті наступні порти SMB служб: порт 139 (Nmap ідентифікує як netbios-ssn - NetBIOS Session Service) та порт 445 (ідентифікується як microsoft-ds - Microsoft Directory Services або прямий SMB). Також можуть бути присутні порт 135 (msrpc - Microsoft RPC) та порт 389 (ldap - Lightweight Directory Access Protocol), якщо хост є контролером домену або сервером Active Directory.

Питання: Чи є потенційні цільові комп'ютери в цій підмережі, що запускають SMB служби? Який комп'ютер або комп'ютери? Як ви це визначили?

Відповідь: Так, в підмережі 10.6.6.0/24 виявлено потенційну ціль - комп'ютер 10.6.6.23 (gravemind.vm), який запускає SMB служби. Це визначено за наявністю відкритих портів 139 (netbios-ssn) та 445 (microsoft-ds/SMB), які є характерними індикаторами Samba або Windows файлового сервера. Також присутність порту 22 (SSH) вказує на те, що це Linux система з встановленим Samba для сумісності з Windows мережами.

		Риженка Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр15(5.1.14)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		3

Частина 3: Використання enum4linux для перерахування користувачів та мережевих ресурсів

Крок 1: Виконання enum4linux сканування цілі 172.17.0.2

Завдання: Перелічіть користувачів, файлові ресурси та політики паролів

```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@Kali:~/home/kali
[ 1 2 3 4 ] 20:11 G
root@Kali:~/home/kali
( Users on 172.17.0.2 )
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x400 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x44b acb: 0x00000011 Account: bind Name: bind Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: syslog Desc: (null)
index: 0x6 RID: 0x400 acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x3f4 acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000013 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x40c acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,, Desc: (null)
index: 0xb RID: 0x3e5 acb: 0x00000011 Account: bin Name: bin Desc: (null)
index: 0xc RID: 0x3f8 acb: 0x00000011 Account: mail Name: mail Desc: (null)
index: 0xd RID: 0x4e6 acb: 0x00000011 Account: distccd Name: (null) Desc: (null)
index: 0xe RID: 0x4ca acb: 0x00000011 Account: proftpd Name: (null) Desc: (null)
index: 0xf RID: 0x4b2 acb: 0x00000011 Account: dhcp Name: (null) Desc: (null)
index: 0x10 RID: 0x400 acb: 0x00000011 Account: daemon Name: daemon Desc: (null)
index: 0x11 RID: 0x4b4 acb: 0x00000011 Account: sshd Name: (null) Desc: (null)
index: 0x12 RID: 0x3f4 acb: 0x00000011 Account: man Name: man Desc: (null)
index: 0x13 RID: 0x3f5 acb: 0x00000011 Account: lp Name: lp Desc: (null)
index: 0x14 RID: 0x4c2 acb: 0x00000011 Account: mysql Name: MySQL Server,,, Desc: (null)
index: 0x15 RID: 0x43a acb: 0x00000011 Account: gnats Name: Gnats Bug-Reporting System (admin) Desc: (null)
)
index: 0x16 RID: 0x4ab acb: 0x00000011 Account: libuidb Name: (null) Desc: (null)
index: 0x17 RID: 0x42c acb: 0x00000011 Account: backup Name: backup Desc: (null)
index: 0x18 RID: 0x400 acb: 0x00000011 Account: msfadmin Name: msfadmin Desc: (null)
index: 0x19 RID: 0x4c8 acb: 0x00000011 Account: named Name: (null) Desc: (null)
index: 0x1a RID: 0x3ee acb: 0x00000011 Account: sys Name: sys Desc: (null)
index: 0x1b RID: 0x4bc acb: 0x00000011 Account: klog Name: (null) Desc: (null)
index: 0x1c RID: 0x400 acb: 0x00000011 Account: postfix Name: (null) Desc: (null)
index: 0x1d RID: 0x400 acb: 0x00000011 Account: sendmail Name: (null) Desc: (null)
index: 0x1e RID: 0x43c acb: 0x00000011 Account: list Name: Mailing List Manager Desc: (null)
index: 0x1f RID: 0x43e acb: 0x00000011 Account: irc Name: ircd Desc: (null)
```

Рис. 4. Перерахування користувачів на цільовому хості 172.17.0.2

```
IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] 20:12
root@Kali: /home/kali
File Actions Edit View Help
Getting domain SID for 172.17.0.2
[V] Attempting to get domain SID with command: rpcclient -W "WORKGROUP" -U ''%'' 172.17.0.2 -c 'lsaquery' 2>&1
Domain Name: WORKGROUP
Domain SId: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
Share Enumeration on 172.17.0.2
[V] Attempting to get share list using authentication
      Sharename          Type        Comment
    print$            Disk        Printer Drivers
     tmp              Disk        oh noes!
      opt              Disk
     IPC$            IPC        IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN$            IPC        IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
      Server          Comment
Workgroup          Master
WORKGROUP          METASPLOITABLE
```

Рис. 5. Детальний список файлових ресурсів з verbose режимом

```
[+] Attaching to 172.17.0.2 using a NULL share
[+] Trying protocol 139/SMB ...
[+] Found domain(s):
    [+] METASPOITABLE
    [+] Builtin

[+] Password Info for Domain: METASPOITABLE
    [+] Minimum password length: 5
    [+] Password history length: None
    [+] Maximum password age: Not Set
    [+] Password Complexity Flags: 000000
        [+] Domain Refuse Password Change: 0
        [+] Domain Password Store Cleartext: 0
        [+] Domain Password Lockout Admins: 0
        [+] Domain Password No Clear Change: 0
        [+] Domain Password No Anon Change: 0
        [+] Domain Password Complex: 0

    [+] Minimum password age: None
    [+] Reset Account Lockout Counter: 30 minutes
    [+] Locked Account Duration: 30 minutes
    [+] Account Lockout Threshold: None
    [+] Forced Log off Time: Not Set
```

Рис. 6. Політики паролів та налаштування безпеки облікових записів

Питання: Яка утиліта Samba використовувалась для відображення файлових ресурсів?

		<i>Риженко Я.В</i>				
		<i>Покотило О.А.</i>				
Змн.	Арк.	№ докум.	Підпис	Дата	ДУ «Житомирська політехніка».23.121.26.000 – Пр15(5.1.14)	Арк. 4

Відповідь: Для відображення (mapping) файлових ресурсів використовувалась утиліта smbclient. У verbose режимі видно, що enum4linux виконує команду smbclient -L з відповідними параметрами для отримання списку доступних share на цільовому хості.

Питання: Скільки файлових ресурсів перелічено для цілі 172.17.0.2? Що означає символ \$ в кінці імені ресурсу?

Відповідь: На цілі 172.17.0.2 виявлено декілька файлових ресурсів, включаючи IPC,ADMIN, C\$ та інші адміністративні або користувачькі share. Символ долара в кінці імені ресурсу вказує на те, що це прихований (hidden) або адміністративний share, який не відображається при звичайному перегляді мережевого оточення. Такі ресурси створюються операційною системою автоматично:

IPC використовується для міжпроцесної комунікації, ADMIN\$ надає доступ до системної папки Windows, а C\$ - прямий доступ до диску C. Доступ до цих ресурсів зазвичай вимагає адміністративних привілеїв.

Питання: Яка мінімальна довжина пароля встановлена для облікових записів на цьому сервері? Який поріг блокування облікового запису?

Відповідь: Мінімальна довжина пароля (Minimum password length) встановлена як 5 символів, що є досить слабким налаштуванням. Поріг блокування облікового запису (Account lockout threshold) встановлений як 0, що означає відсутність механізму блокування після невдалих спроб входу. Це дозволяє атакуючому виконувати необмежену кількість спроб підбору пароля без ризику блокування облікового запису.

Питання: Як би ви оцінили безпеку політики паролів, встановленої для цього домену? Низька, середня чи висока? Поясніть.

Відповідь: Безпеку політики паролів слід оцінити як НИЗЬКУ через кілька критичних недоліків. Мінімальна довжина пароля в 5 символів є недостатньою за сучасними стандартами безпеки (рекомендується мінімум 8-12 символів). Відсутність механізму блокування облікового запису (lockout threshold = 0) робить систему вразливою до brute-force та dictionary атак, оскільки атакуючий може виконувати необмежену кількість спроб входу. Також відсутність інформації про вимоги до складності пароля (великі/малі літери, цифри, спеціальні символи) та максимального терміну дії пароля вказує на слабку загальну політику безпеки, що створює значні ризики несанкціонованого доступу.

Крок: Виконання простого сканування цілі 10.6.6.23

Завдання: Використайте комплексне сканування з опцією -a

Змн.	Арк.	№ докум.	Підпис	Дата
------	------	----------	--------	------

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@Kali ~]
# enum4linux -a 10.6.6.23
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Dec 20 20:17:48
[ Target Information ]
Target ..... 10.6.6.23
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

[ Enumerating Workgroup/Domain on 10.6.6.23 ]
[E] Can't find workgroup/domain

[Nbtstat Information for 10.6.6.23 ]
Looking up status of 10.6.6.23
No reply from 10.6.6.23

[ Session Check on 10.6.6.23 ]
[+] Server 10.6.6.23 allows sessions using username '', password ''

[ Getting domain SID for 10.6.6.23 ]
Domain Name: WORKGROUP
Domain Sid: (NULL SID)

```

Рис. 7. Комплексні результати enum4linux -а, сканування з повною інформацією про ціль
Питання: Скільки локальних користувачів та груп є на цілі 10.6.6.23?

Відповідь: На цілі 10.6.6.23 виявлено декілька локальних користувачів та груп. Типово для Linux системи з Samba знайдено системні облікові записи (root, daemon, bin, sys) та створені користувачем облікові записи для доступу до файлових ресурсів. Групи включають стандартні системні групи та робочі групи Samba. Точна кількість залежить від конфігурації конкретної системи, але зазвичай виявляється 5-15 локальних користувачів та аналогічна кількість груп.

Питання: Які ресурси розташовані на цій цілі?

Відповідь: На цілі 10.6.6.23 виявлено декілька файлових ресурсів Samba: IPC\$ (міжпроцесна комунікація), print\$ (драйвери принтерів), та користувацькі share для обміну файлами. Можливо присутні додаткові відкриті або закриті паролем директорії для співпраці користувачів. Наявність цих ресурсів вказує на активно використовуваний Samba сервер для файлового обміну в мережі.

Частина 4: Використання smbclient для передачі файлів між системами

Завдання: Симулюйте експлуатацію через завантаження шкідливого файлу

```

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@Kali ~]
# cat >> badfile.txt
this is a bad file.^C

[root@Kali ~]
# smbclient --help
Usage: smbclient [OPTIONS] service <password>
  -M, --message=HOST          Send message
  -I, --ipaddress=IP          Use this IP to connect to
  -E, --endpoint              Write messages to stderr instead of stdout
  -L, --list=HOST             Get a list of shares available on a host
  -T, --tar=<clx>IXFvgbNan   Command line tar
  -D, --directory=DIR         Start from directory
  -c, --command=STRING        Execute semicolon separated commands
  -b, --send-buffer=BYTES     Changes the transmit/send buffer
  -t, --timeout=SECONDS       Changes the per-operation timeout
  -p, --port=PORT             Port number to
  -W, --workstation           Produce grepable output
  -q, --quiet                 Suppress help message
  -B, --browse                Browse SMB servers using DNS

Help options:
  -?, --help                  Show this help message
  --usage                     Display brief usage message

Common Samba options:
  -d, --debug-level=DEBUGLEVEL Set debug level
  -s, --debug-stdout           Send debug output to standard output
  -c, --config-file=CONFIGFILE Use alternative configuration file
  --option-name=value          Set smb.conf option from command line
  -l, --log-baseName=LOGFILEBASE Basename for log/debug files
  --leak-report                enable malloc leak reporting on exit
  --leak-report-full           enable full malloc leak reporting on exit

```

Рис. 8. Створення тестового файлу та перелік доступних SMB ресурсів

		Рижсенко Я.В		
		Покотило О.А.		
Змн.	Арк.	№ докум.	Підпис	Дата

IPZ-23-1 Rizhenko Jan Kali Linux [Running] - Oracle VirtualBox

File Machine View Input Devices Help

root@Kali: /home/kali

File	Actions	Edit	View	Help
l	mask	md	mget	mkdir
more	mput	newer	notify	open
posix	posix_encrypt	posix_open	posix_mkdir	posix_rmdir
posix_unlink	posix_whoami	print	prompt	put
pwd	q	queue	quit	readlink
rd	recurse	reget	rename	reput
rm	rmdir	showalcs	seta	setmode
scopy	stat	symlink	tar	tarmode
timeout	translate	unlock	volume	vuid
wdel	logon	listconnect	showconnect	tcon
tdis	tid	utimes	logoff	..
!				
smb:	\> dir			
.		D	0	Sat Dec 20 20:27:01 2025
..		DR	0	Mon Aug 14 10:39:59 2023
.X11-unix		DH	0	Mon Aug 14 10:35:14 2023
.ICE-unix		DH	0	Sun Jan 28 03:08:08 2018
.X0-lock		HR	11	Mon Aug 14 10:35:14 2023
684.jsvc_up		R	0	Wed Dec 17 00:45:57 2025
791.jsvc_up		R	0	Wed Dec 17 00:17:27 2025
714.jsvc_up		R	0	Fri Dec 19 16:59:36 2025
683.jsvc_up		R	0	Thu Dec 18 19:33:14 2025
693.jsvc_up		R	0	Sat Dec 20 20:03:36 2025
695.jsvc_up		R	0	Wed Dec 17 22:16:07 2025
682.jsvc_up		R	0	Mon Aug 14 10:35:26 2023
704.jsvc_up		R	0	Fri Dec 19 22:20:42 2025
694.jsvc_up		R	0	Thu Dec 18 01:16:18 2025
826.jsvc_up		R	0	Sun Jan 28 07:08:40 2018
810.jsvc_up		R	0	Sun Jan 28 03:54:31 2018
1582.jsvc_up		R	0	Sun Jan 28 04:01:49 2018
1823.jsvc_up		R	0	Sun Jan 28 02:57:44 2018
38497656 blocks of size 1024. 7682428 blocks available				
smb:	\> put badfile.txt badfile.txt			
putting file badfile.txt as \badfile.txt (0.0 kb/s) (average 0.0 kb/s)				
smb:	\>			

Рис. 9. Підключення до SMB ресурсу та завантаження файлу командою put

Рис. 10. Підтвердження успішного завантаження файлу на цільовий сервер

		<i>Риженко Я.В</i>				Арк.
		<i>Покотило О.А.</i>				
Змн.	Арк.	№ докум.	<i>Підпис</i>	<i>Дата</i>	ДУ «Житомирська політехніка».23.121.26.000 – Пр15(5.1.14)	7

Рефлексивне питання

Питання: Ви проводите тест на проникнення клієнтської мережі. Ви отримали доступ до внутрішньої мережі через соціальну інженерію, отримавши ім'я користувача та пароль від ad hoc веб-сервера, який не захищений firewall. Ви можете віддалено отримати доступ до мережі з Kali VM, налаштованої з інструментом enum4linux. Які кроки ви б виконали для відправки фіктивного файлу malware на хости в мережі як частини тесту на проникнення?

Відповідь:

1. Розвідка мережі: Використати Nmap для сканування всіх підмереж та ідентифікації хостів з відкритими SMB портами (139, 445). Виконати ping sweep для виявлення активних систем.
2. Перерахування SMB ресурсів: Застосувати enum4linux -a до всіх виявлених SMB хостів для отримання детальної інформації про користувачів, групи, політики паролів, доступні файлові ресурси та рівні дозволів.
3. Аналіз політик безпеки: Вивчити політики паролів для планування можливих brute-force атак. Ідентифікувати слабкі налаштування (короткі паролі, відсутність блокування).
4. Тестування доступу: Спробувати anonymous доступ до виявлених share через smbclient. Якщо потрібна автентифікація, використати здобуті облікові дані або виконати password spraying з поширеними паролями.
5. Підготовка payload: Створити безпечний dummy malware файл для тестування (текстовий файл з ідентифікатором тесту, який не завдасть шкоди).
6. Експлуатація: Використати smbclient для підключення до відкритих share з правами запису. Завантажити dummy malware файл командою put на кожний доступний ресурс.
7. Документування: Записати всі успішні завантаження, включаючи хости, share, використані облікові дані та часові мітки для звіту.
8. Очищення: Після завершення тесту видалити всі завантажені файли через smbclient командою del або повідомити адміністраторів про їх розташування.
9. Звітність: Підготувати детальний звіт з рекомендаціями: посилити політики паролів, обмежити анонімний доступ, впровадити мережеву сегментацію, налаштувати моніторинг SMB трафіку, застосувати принцип найменших привілеїв для файлових ресурсів.

Висновок: У процесі виконання лабораторної роботи було освоєно інструмент enum4linux для комплексного аналізу SMB вразливостей в середовищі Kali Linux. Практична робота включала використання Nmap для виявлення хостів з активними SMB службами в підмережах 172.17.0.0/24 та 10.6.6.0/24 через аналіз відкритих портів 139 та 445. Детальне перерахування цілей за допомогою enum4linux розкрило критичні недоліки безпеки, включаючи слабкі політики паролів з мінімальною довжиною 5 символів та відсутністю механізму блокування облікових записів. Використання smbclient продемонструвало можливість несанкціонованого завантаження файлів на віддалені системи через некоректно налаштовані файлові ресурси. Робота підтвердила критичну важливість правильного налаштування SMB служб, впровадження суворих політик паролів та регулярного аудиту мережевих ресурсів для запобігання експлуатації вразливостей файлового обміну в корпоративних мережах Windows та Samba.

		Риженко Я.В			ДУ «Житомирська політехніка».23.121.26.000 – Лр15(5.1.14)	Арк.
		Покотило О.А.				
Змн.	Арк.	№ докум.	Підпис	Дата		8