# 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

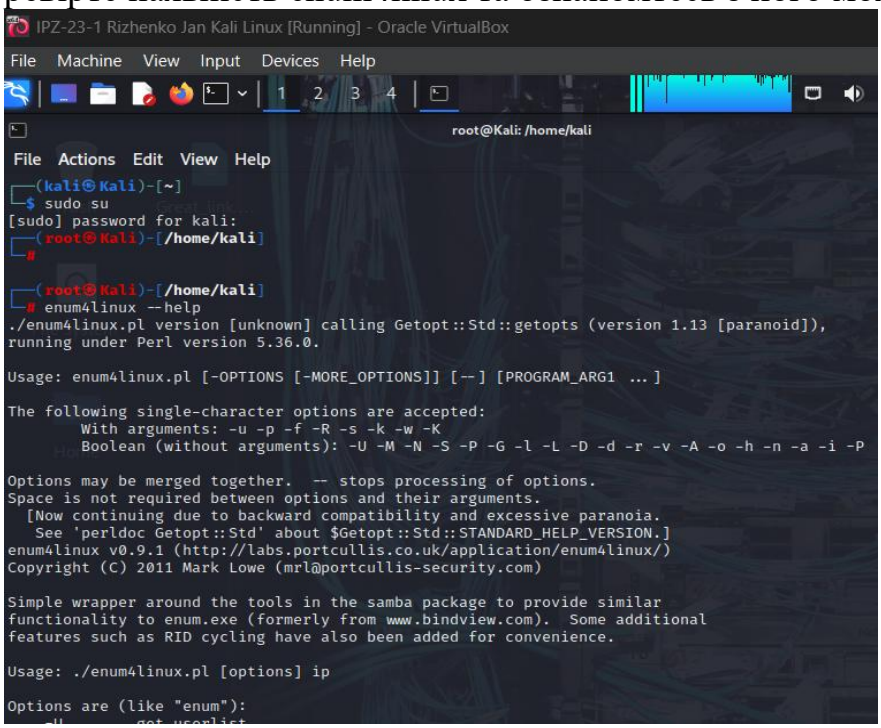


Рис. 1. Довідкова сторінка enum4linux з синтаксисом команд та доступними опціями

**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), rpcclient (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.

**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

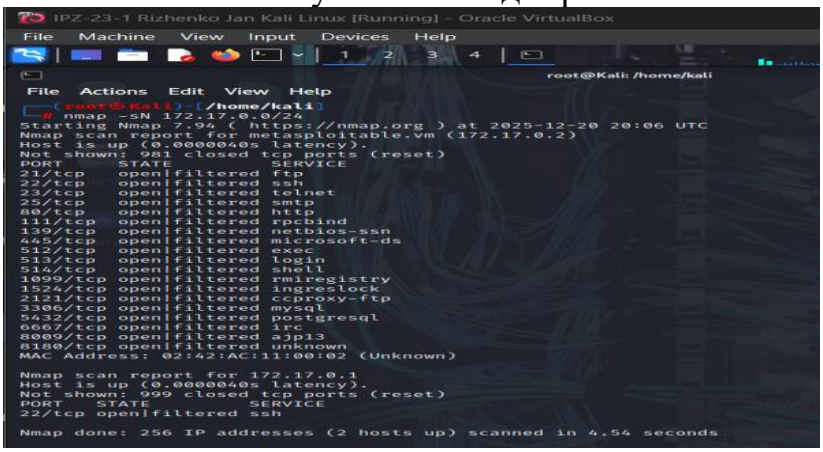

Рис. 2. Результати Nmap сканування підмережі 172.17.0.0/24 з виявленими SMB портами

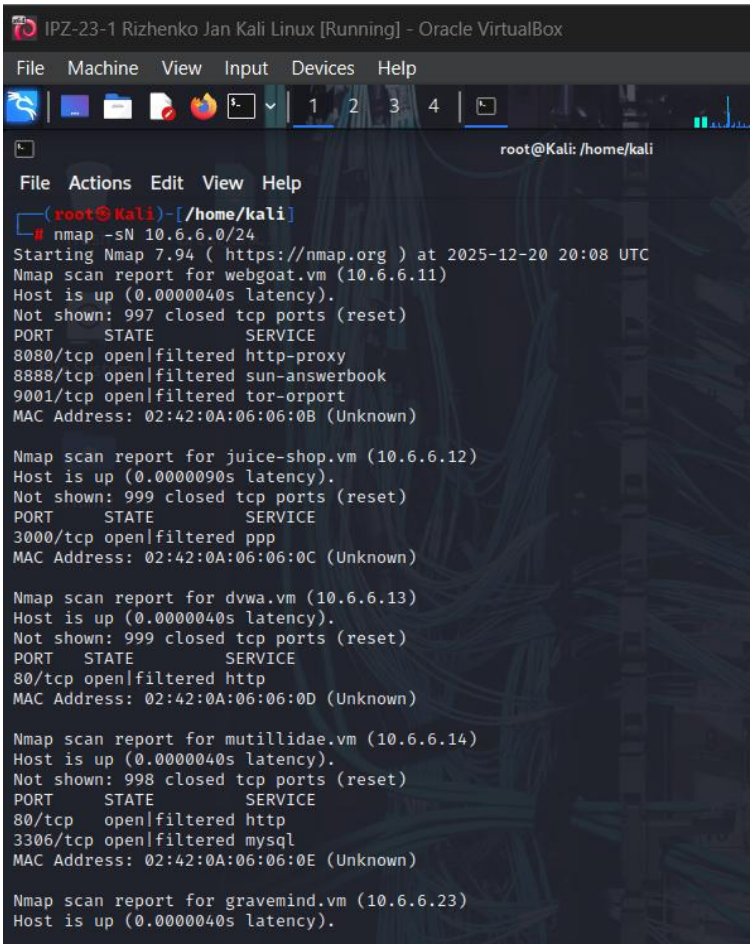


Рис. 3. Результати Nmap сканування підмережі 10.6.6.0/24 з аналізом відкритих служб

**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.

**Частина 3:** Використання enum4linux для перерахування користувачів та мережевих ресурсів

**Крок 1:** Виконання enum4linux сканування цілі 172.17.0.2

**Завдання:** Переліччіть користувачів, файлові ресурси та політики паролів

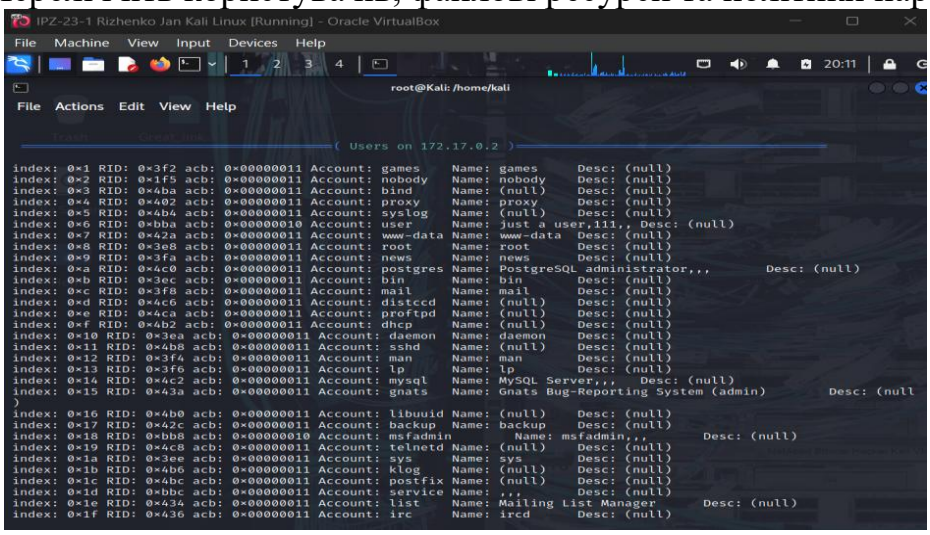


Рис. 4. Перерахування користувачів на цільовому хості 172.17.0.2

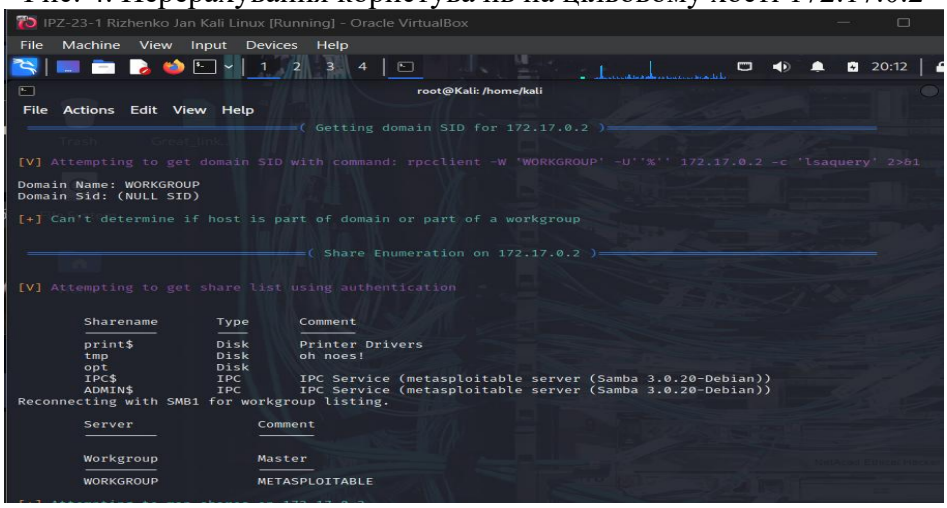


Рис. 5. Детальний список файлових ресурсів з verbose режимом

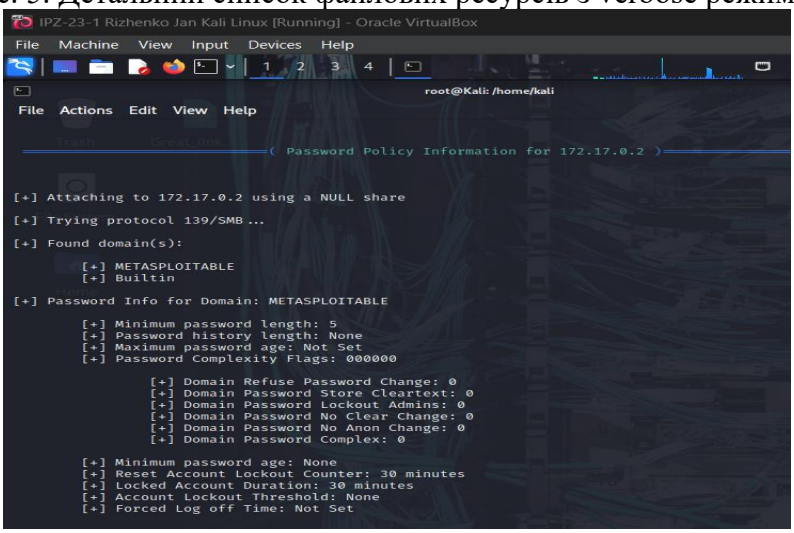


Рис. 6. Політики паролів та налаштування безпеки облікових записів

**Питання: Яка утиліта Samba використовувалась для відображення файлових ресурсів?**

**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 користувацькі 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

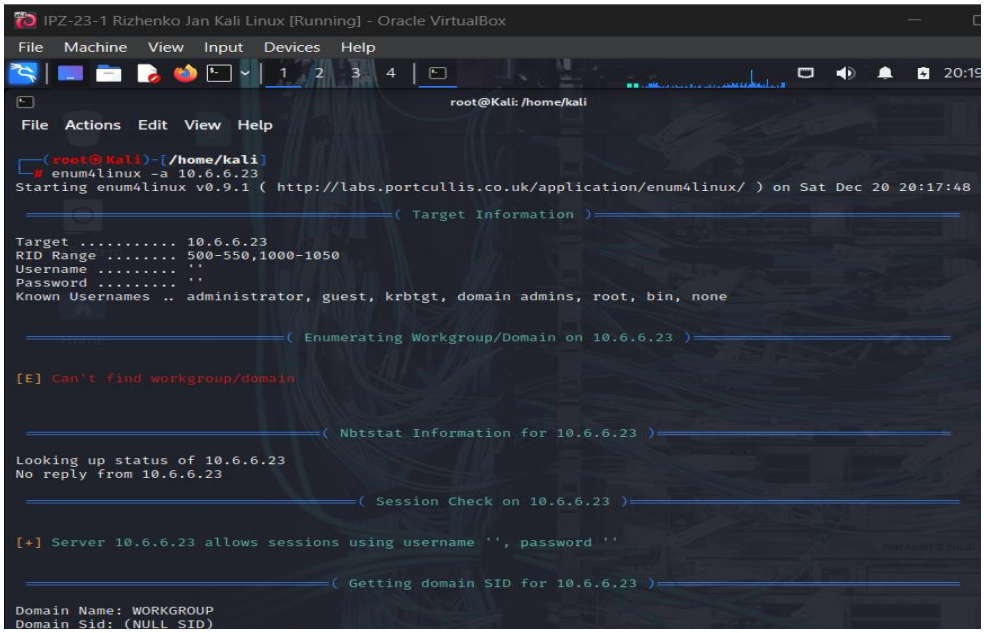


Рис. 7. Комплексні результати enum4linux -a, сканування з повною інформацією про ціль

**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

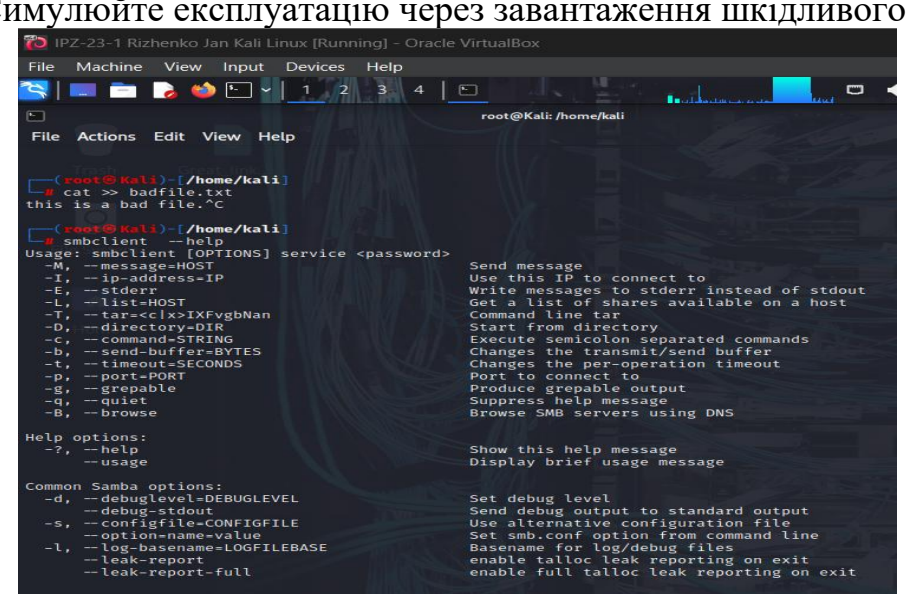


Рис. 8. Створення тестового файлу та перелік доступних SMB ресурсів

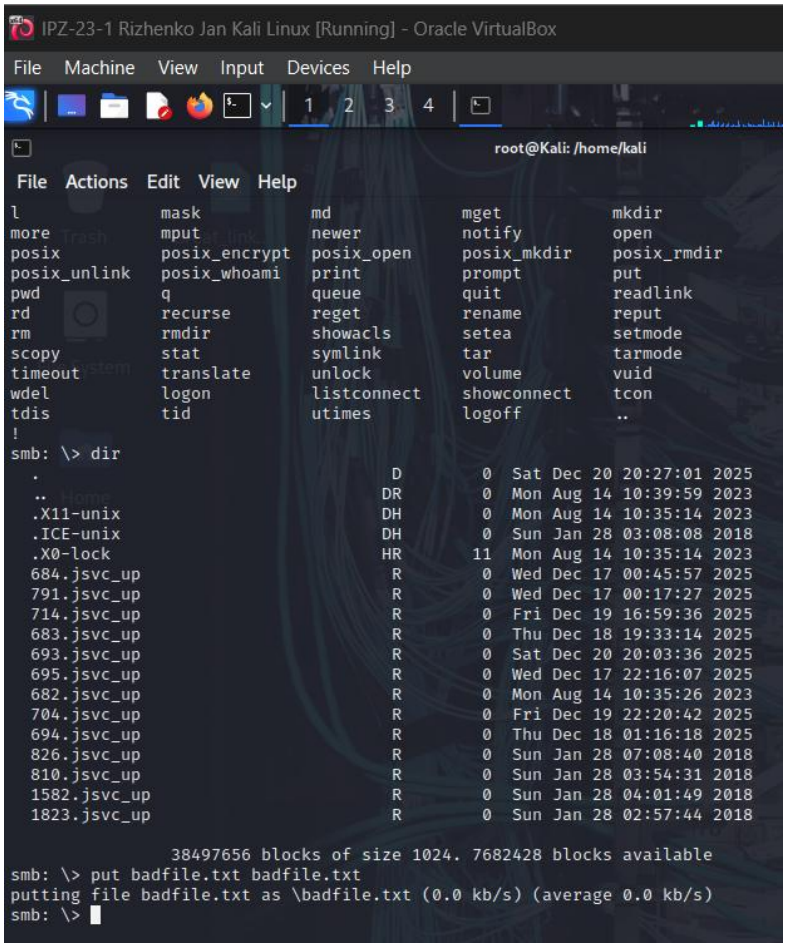


Рис. 9. Підключення до SMB ресурсу та завантаження файлу командою put

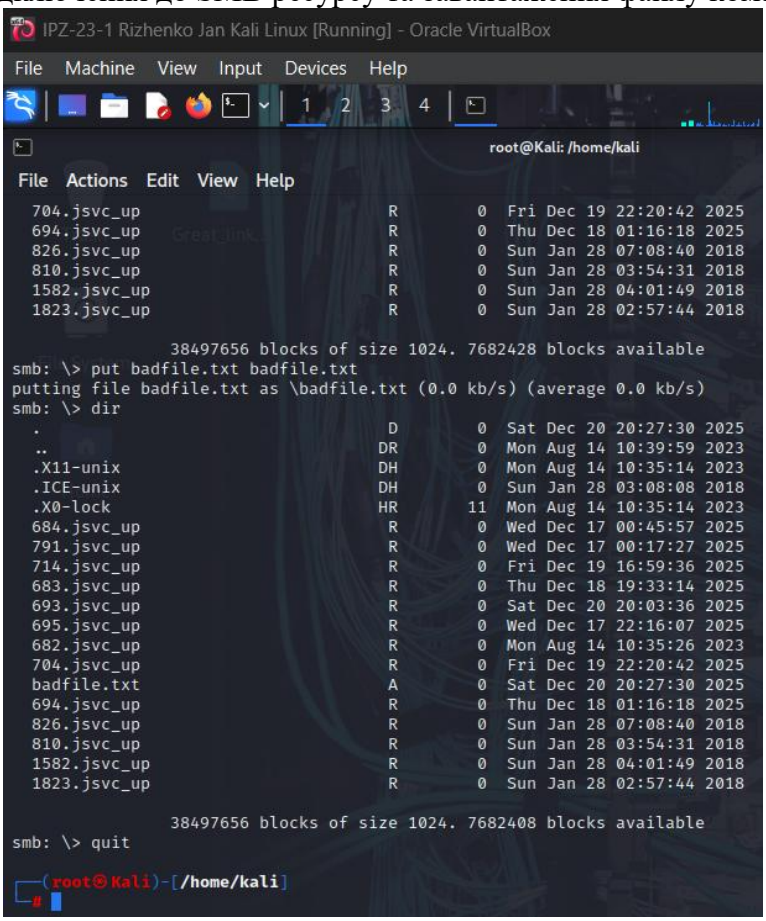


Рис. 10. Підтвердження успішного завантаження файлу на цільовий сервер

**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.