УДК 004.021
DOI: 10.31673/2409-7292.2023.020005

Мужанова Т. М. Лавровський І. М.

АНАЛІЗ СУЧАСНИХ ЗАСОБІВ ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ

Тестування на проникнення – це перевірка безпеки, яка виконується організацією, під час якої експерт намагається знайти, вторгнутися та використати слабкі місця в комп'ютерній системі або мережах організації. Основна мета – знайти будь-яку потенційну слабкість. Це також допомагає організаціям підтримувати та дотримуватися встановлених стандартів щодо захисту конфіденційності своїх клієнтів. У статті досліджуються програмні засоби, які можуть бути використані для здійснення тестування на проникнення.

Ключові слова: кібербезпека, тестування на проникнення, етичний хакінг, засоби злому.

Вступ

Інтернет став фундаментальною частиною глобальної економіки. Усі організації використовують комп'ютерні технології для повсякденної діяльності, від багатомільярдних корпорацій до малих приватних фірм. Це ставить багатьох людей під загрозу зловмисного програмного забезпечення, кіберзлочинців і хакерів, якщо не вжити належних заходів. Однак навіть у найбільш попереджувальних заходах є вразливості та лазівки – ось тут і з'являється тестування на проникнення.

Формулювання проблеми

Тестування на проникнення, широко відоме як проба пера або етичний хакінг, – це санкціонована імітаційна кібератака, націлена на комп'ютерну мережу з метою оцінки будь-яких недоліків у безпеці мережі. Тестування на проникнення використовується при розподілі бюджету для надання кількісної та якісної інформації про стан безпеки системи. Тести на проникнення можуть бути автоматизовані або проведені вручну етичними хакерами. З іншого боку, автоматизоване тестування на проникнення виконується за допомогою спеціального програмного забезпечення.

Метою даної статті є проведення огляду спеціального програмного забезпечення, яке може бути використано для тестування на проникнення.

Викладення основного матеріалу

Ключові обов'язкові функції програмного забезпечення для тестування на проникнення визначаються технічними можливостями сканерів в т.ч. щодо злому паролів, мультисистемністю та зручністю для користувача (рис. 1):

1. *Детальні та вичерпні звіти*

Хороше програмне забезпечення для тестування на проникнення має бути в змозі надавати докладні та вичерпні звіти. Тестування на проникнення не закінчується лише пошуком уразливостей у мережі. Оператор або адміністратор повинен вміти розуміти проблеми в мережі. Без цих знань було б складно спланувати наступні дії. Звіт про тестування має описувати, надавати докази та оцінювати ризик, а також рекомендувати вирішення будь-якої виявленої вразливості.

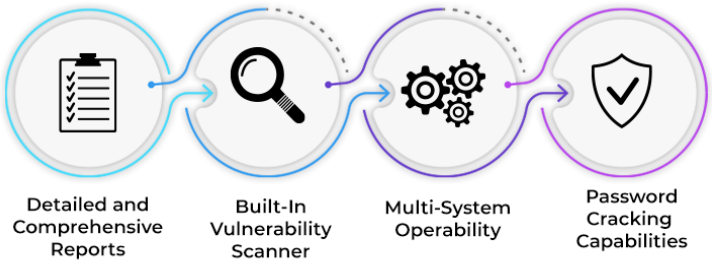


Рис. 1. Ключові функції засобів для тестування на проникнення [1]

2. *Вбудований сканер вразливостей*

Сканер уразливостей постачається разом із більшістю комерційних інструментів тестування на проникнення. Мета сканування вразливостей полягає в тому, щоб виявити будь-яку помилку в апаратному чи програмному забезпеченні, яка пізніше може виявитися маршрутом атаки на систему. Сканери вразливостей виконують сканування на основі опублікованої бази даних загальних вразливостей і вразливостей (CVE), що робить регулярні оновлення дуже важливими. Сканування також включає автоматичне сканування, яке можна налаштувати для запуску в певних програмах.

3. *Мультисистемна працездатність*

Неодмінною особливістю хорошого програмного забезпечення для тестування на проникнення є його можливість використовувати на різних пристроях. Більшість програмного забезпечення для проникнення сумісні з операційними системами Linux, деякі з них уже попередньо встановлені в ОС. Однак інші пристрої, що працюють під керуванням операційних систем Windows, macOS і мобільних телефонів Android, також потребують інструментів тестування на проникнення для перевірки вразливостей. Це зробило програмне забезпечення для тестування, яке сумісне з декількома пристроями, користуватись великим попитом.

4. *Можливості злому паролів*

Паролі є однією з найслабкіших ланок будь-якої організації чи комп'ютерної мережі. Люди часто використовують найпростішу комбінацію символів, щоб захистити доступ до важливої інформації. Ось чому тести на проникнення часто включають оцінку надійності пароля. Таким чином, програмне забезпечення для тестування на проникнення повинно мати можливість зламувати паролі. Вони використовують комбінацію таких функцій, як атаки грубої сили, атаки криптоаналізу та атаки за словником, щоб оцінити надійність пароля.

Розглянемо найкращі інструменти для тестування на проникнення у 2022 році.

Aircrack-ng – це стандартний, добре відомий інструмент, який використовується для оцінки, аналізу та злому безпроводових мереж. Він був створений в 2010 році і використовувався для тестування безпроводових мереж за стандартами 801.11.

Aircrack-ng – це інструмент тестування безпроводової мережі, який може розшифровувати паролі WEP і WPA PSK, що вказує на важливу слабку область. Aircrack-ng може контролювати певну мережу WiFi. Він захоплює пакети даних, а потім експортує їх у текстові файли для подальшого аналізу мережі. Як і будь-який інструмент для етичного хакінгу, Aircrack-ng може здійснювати атаки з відтворенням, установлювати підроблені точки доступу, а також вводити пакети в мережу. Коли Aircrack-ng було випущено вперше, він був розроблений для роботи в ОС Linux. Це було розширено, щоб включити ОС Windows, серед іншого. Aircrack-ng є одним із старіших варіантів програмного забезпечення для тестування на проникнення. Він добре відомий із широко доступним вихідним кодом. Aircrack-ng – безкоштовний інструмент, доступний для завантаження.

Aircrack-ng – це набір інструментів, який зосереджується на різних аспектах WiFi і може використовуватися для моніторингу безпеки Wi-Fi. Однак ви не можете використовувати його в проводових мережах.

Burp Suite – це інструмент тестування на проникнення на основі Java, розроблений PortSwigger web security. Це комбінований інструмент тестування та сканування вразливостей, розроблений для веб-додатків.

Burp Suite має сканер із широким охопленням, структурований для тестування сучасних веб-додатків із різними API та порівняння із задокументованими вразливими місцями. Burp Suite може визначати та декодувати шифрування, що використовується під час передачі пакетів даних через мережу. Крім того, він може кодувати подібні дані в мережі. Важливість тестування безпеки полягає в розумінні

можливих недоліків. Burp Suite створює докладні звіти, які можна легко зрозуміти. Burp Suite доступний у трьох версіях, і всі версії працюють на комп'ютерах з ОС Linux, macOS і Windows із правильними характеристиками. Окрім тестування на проникнення та сканування вразливостей, Burp Suite дозволяє вам пасивно сканувати під час перегляду. Професійне видання Burp Suite для одного користувача коштує 399 доларів на рік.

Burp Suite є одним із провідних інструментів кібербезпеки на ринку. Однак ціни на професійну та корпоративну версії інструменту досить високі.

Cain and Abel – інструмент тестування на проникнення, створений у 2014 році. Це інструмент, який використовує різні методи відновлення пароля та аналізу пакетів у Microsoft Windows.

Ключові особливості Cain and Abel включають запис VoIP. І хоча це не основна функція, запис VoIP також можна використовувати для тестування мережі. Cain and Abel – це головним чином інструмент злому паролів, який може відновлювати різні типи паролів за допомогою грубої сили, атак за словником і криптоаналізу. Cain and Abel можуть відстежувати або перехоплювати мережеві пакети даних. Потім ці пакети захоплюються та аналізуються для отримання важливої інформації про мережу. Це інструмент, створений для роботи в операційних системах Microsoft Windows від Vista до найновішої ОС Windows. Cain and Abel – це високошвидкісний інструмент для відновлення паролів, який розкриває найскладніші паролі. Інструмент тестування на проникнення Cain and Abel є безкоштовним.

Це хороший інструмент, якщо вам цікаво, чи можуть хакери легко розшифрувати ваші паролі. Однак джерелом занепокоєння є відсутність вихідного коду.

CANVAS by Immunity – є одним із провідних інструментів оцінки безпеки, доступних для комерційного використання. Розроблений компанією Immunity, це індійська компанія, яка використовується для тестування на проникнення та дослідження експлойтів.

Основні функції Canvas включають раннє оновлення Canvas – це важлива функція, яка забезпечує життєздатність проектів, що потребують часу, завдяки щохвилинному доступу до нещодавно випущених уразливостей. Функція імунітету ретельно вибирає вразливості, включені до складу Canvas Exploits. Найважливіші з них мають нові та дорогоцінні вразливості. Canvas Strategic дозволяє команді, яка працює над Canvas з різних комп'ютерів, ділитися, контролювати та координувати прогрес і досягнення. Canvas може повністю працювати на системах з операційними системами Windows або Linux. Він також може працювати на мобільних телефонах Android в обмеженому обсязі. Одним з унікальних аспектів Canvas є його адаптивний відкритий дизайн, який дозволяє користувачам відповідно налаштовувати програмне забезпечення. Imunity Canvas коштує 32 480 доларів за річну ліцензію.

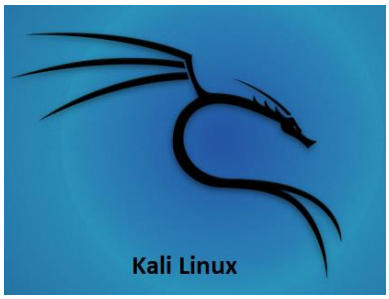
Canvas допомагає тестувальникам проникнення розробляти та використовувати продукти безпеки сторонніх розробників, такі як DSquare, D2 exploitation pack тощо. Однак його дизайн може дещо заплутати нових користувачів.

John the Ripper – опублікований у 2013 році, є одним із найпоширеніших інструментів злому паролів. Він збирає багато методів зламу або відновлення паролів в одному пакеті.

Ключові особливості John the Ripper включають атаки грубою силою: під час використання грубої сили для злому паролів інструмент перевіряє кожну можливу комбінацію паролів у межах заданого набору параметрів. John the Ripper також може використовувати атаки за словником, щоб розкрити пароль. Він використовує випадкові слова зі словника та порівнює їх із системою. Інструмент може

отримати доступ до паролів, які були зашифровані. John the Ripper можна використовувати в кількох операційних системах. Як правило, він працює на базі ОС Unix, а також macOS, ОС Windows і ОС Kerberos. Серед кількох інструментів тестування на проникнення John the Ripper – це спеціалізоване програмне забезпечення для злому паролів, до якого можна отримати безкоштовний доступ. Професійна версія John the Ripper коштує $39,95 без підтримки електронною поштою.

За допомогою John the Ripper користувачі та організації можуть перевірити надійність своїх поточних паролів. Однак ви не можете використовувати цей інструмент для перевірки вразливості мережі, окрім паролів.



Kali Linux – це інструмент, розроблений Offensive Security, який є частиною загального пакета операційної системи Linux.

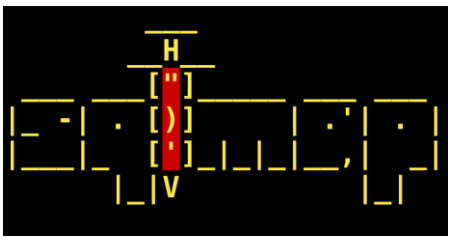
Kali Linux пропонує добре задокументовану інформацію для новачків і експертів у цій галузі, включаючи поради та вказівки. Kali NetHunter – це функція, яка дозволяє телефонам Android мати програму тестування на проникнення. Він містить програму, магазин додатків і контейнер Kali. Kali Linux не потрібно зберігати лише в комп'ютерній системі. Його також можна використовувати безпосередньо з USB-накопичувача. Kali Linux дозволяє користувачам створювати оптимізовану та персоналізовану версію програми відповідно до їхніх потреб. Це важливо для спеціалістів із безпеки. Kali Linux – це не просто безкоштовний інструмент тестування на проникнення для експертів. Завдяки новим функціям він також доступний для людей із вадами зору. Kali Linux – це безкоштовний ресурс, автоматично доступний у всіх системах Linux.

Kali Linux допомагає тестувальникам проникнення бути оснащеними для наступальних і оборонних цілей. Однак це програма не призначена для новачків або повсякденного використання.

Metasploit – це програма, створена для пошуку, використання та вивчення подробиць про можливі вразливості системи. Він включає як Metasploit pro, так і фреймворк Metasploit.

Metasploit захищає компанії та малий бізнес від кібератак. Завдяки спрощеному інтерфейсу, як експерти, так і новачки можуть отримати доступ до інструменту. Metasploit дозволяє користувачеві сканувати слабкі місця та вразливості в комп'ютерній мережі за допомогою сканування для виявлення. Користувачі також можуть сканувати імпортовані дані. Користувачі можуть використовувати фреймворк Metasploit для налаштування та розробки інструментів безпеки або написання нових кодів експлойтів для виявлення невиявлених уразливостей. Metasploit сумісний із комп'ютерами Linux, macOS і Windows із мінімум 4 ГБ оперативної пам'яті та 1 ГБ пам'яті. Metasploit попередньо встановлено в системі Kali Linux і містить антикриміналістичні інструменти. Фреймворк Metasploit є безкоштовним, тоді як Metasploit Pro коштує 15 000 доларів США на рік.

Metasploit допомагає тестувальникам проникнення оцінювати мережі щодо нових і існуючих недоліків. Однак дізнатися про його використання може бути складно, а в разі неправильного використання може призвести до втрати даних.



SQLmap заснована Даніеле Беллуччі в 2006 році, – це програмне забезпечення для тестування на проникнення з відкритим кодом, яке використовується для пошуку та використання недоліків впровадження SQL, тобто коли введення користувача може змінити виконання запиту SQL.

SQLmap можна використовувати як інструмент злому паролів. Він автоматично розпізнає формати хешу пароля та

використовує техніку атаки на основі словника. SQLmap може дозволити користувачеві шукати певну інформацію в системі бази даних. Пошук може здійснюватися для бази даних або окремих стовпців у кількох базах даних. SQLmap допомагає віддалено виконувати довільні інструкції та отримувати доступ до результату, якщо системою бази даних є MySQL, Microsoft SQL Server тощо. SQLmap можна повністю використовувати на багатьох платформах баз даних, таких як MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, SQLite, Firebird тощо. SQLmap – це унікальний інструмент тестування на проникнення для систем керування базами даних (СУБД), який попередньо встановлено на Kali Linux. SQLmap є безкоштовним продуктом із відкритим кодом.

SQLmap допомагає тестувальникам проникнення оцінити міцність бази даних. Однак він має дещо високий ступінь помилкових спрацьовувань, що вимагає додаткового ручного тестування повідомлених уразливостей.

W3af розшифровується як Web Application Attack and Audit Framework. Це сканер безпеки веб-додатків, який надає інформацію про слабкі місця веб-додатків і був розроблений у 2007 році.

Сканер W3af може шукати у веб-програмі вразливості. Він також має два інтерфейси, графічний інтерфейс користувача та інтерфейс командного рядка. Детальні вичерпні звіти: диспетчер виводу має кілька методів написання виводу. Результати можна надіслати електронною поштою або записати у CSV, HTML тощо. W3af постачається з декількома плагінами, які виконують свої функції та можуть спілкуватися один з одним. Приклади включають плагін аудиту, використання та виявлення. Генерація запитів вручну – це функція, яка діє як проксі-сервер «людина посередині» для полегшення ручного тестування веб-додатків. W3af має величезну кількість функцій, і це тому, що він дозволяє розробникам розширювати його за допомогою кількох плагінів. W3af – це безкоштовний інструмент із відкритим вихідним кодом, доступний для широкої громадськості.

За допомогою W3af користувачі можуть знайти понад 200 уразливостей у веб-додатках. Однак він має той недолік, що час від часу дає хибно негативні результати, що може призвести до непомічених недоліків.

Wireshark є одним із найпопулярніших аналізаторів мережевих протоколів. Це міжплатформний інструмент із відкритим вихідним кодом, який дозволяє користувачам мікроскопічно переглядати свою мережу та вирішувати проблеми.

Wireshark використовує API перехоплення та перехоплення пакетів для перехоплення пакетів даних. В UNIX/Linux це називається libpcap, що означає Promiscuous Library Capture. Wireshark також може перехоплювати голос через Інтернет-протокол пакетів даних або викликів, зроблених через мережу, надаючи користувачеві доступ до даних. Wireshark надає результати тестів, проведених у мережі, у форматі, зрозумілому будь-якому оператору. Wireshark можна використовувати в таких операційних системах, як Linux OS, macOS, Solaris, Windows OS та інших операційних системах, схожих на UNIX. Цей інструмент дозволяє глибоко аналізувати мережевий трафік і може читати та записувати багато різних форматів захоплених файлів. Wireshark – це програма з відкритим кодом, яку можна завантажити безкоштовно.

Wireshark може допомогти користувачам усунути неполадки в мережі та тестувати програмне забезпечення, аналізуючи вміст пакетів у мережі. Однак він не використовує знайдені вразливості.

Порівняльний аналіз засобів тестування на проникнення наведено у Таблиці 1.

© Мужанова, Т. М., & Лавровський, І. М. (2023). Аналіз сучасних засобів для тестування на проникнення. Сучасний захист інформації, 2(54), 35–40. https://doi.org/10.31673/2409-7292.2023.020005.

Таблиця 1

Порівняльний аналіз засобів тестування на проникнення

Назва продукту	Можливість зламу паролів	Призначення, можливість здійснення атаки	Операційна система	Вартість
Aircrack-ng	WEP і WPA PSK у Wi-Fi	Атаки з відтворенням, впровадження підроблених точок доступу	Linux, Windows	Безкоштовний з відкритим кодом
Burp Suite	Криптоаналіз	Активне тестування сучасних веб-додатків із різними API	Linux, Windows	$399 доларів на рік
Cain and Abel	Брутфорс, атака за словником, криптоаналіз	Перехоплення мережевих пакетів даних	Windows	Безкоштовний
Canvas	–	Тестування на проникнення та дослідження експлойтів	Windows, Linux, Android	$32 480 за річну ліцензію
John the Ripper	Брутфорс, атака за словником, криптоаналіз	Активне тестування на проникнення	Unix, macOS, Windows, Kerberos	$39,95
Kali Linux	–	Сканування для виявлення уразливостей. Наступальні і оборонні завдання	Linux	Безкоштовний
Metasploit	–	Сканування для виявлення уразливостей	Linux, macOS, Windows	$15 000 на рік
SQLmap	Атака за словником, криптоаналіз	Виконання довільних інструкцій віддалено	Windows, Linux,	Безкоштовний з відкритим кодом
W3af	–	Пошук вразливостей у веб-додатку	Windows, Linux,	Безкоштовний з відкритим кодом
Wireshark	–	Перехоплення пакетів даних з використанням API	Linux, macOS, Solaris, Windows	Безкоштовний з відкритим кодом

Висновок

Тестування на проникнення тепер має важливе значення для кібербезпеки типового підприємства. Згідно зі звітом Core Security про тестування на проникнення за 2021 рік, 85% компаній проводять тестування принаймні раз на рік, а 99% вважають, що інструменти тестування пера є важливими для їхніх ініціатив щодо відповідності. Інвестуючи в правильні інструменти та програмне забезпечення, підприємства можуть оснастити фахівців з кібербезпеки останніми інноваціями, які не поступаються передовим кібератакам, тож ви можете бути на крок попереду хакерів і кіберзлочинців.

Перелік посилань

1. Chiradeep Basu Mallick. Top 10 Penetration Testing Tools in 2022. https://www.spiceworks.com/it-security/vulnerability-management/articles/best-penetration-testing-tools/.

2. Bacudio, Aileen & Yuan, Xiaohong & Chu, Bill & Jones, Monique. (2011). An Overview of Penetration Testing. International Journal of Network Security & Its Applications. 3. 19-38. 10.5121/ijnsa.2011.3602.

3. Jai Narayan Goel, B.M. Mehtre, Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology, Procedia Computer Science, Volume 57, 2015, Pages 710-715, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2015.07.458.

Надійшла: 28.02.2023 Рецензент: д.т.н., професор Савченко В.А.