КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.18.3948
УДК 004.056

Тишик Іван Ярославович
кандидат технічних наук, доцент кафедри захисту інформації
Національний університет "Львівська політехніка", м. Львів, Україна
ORCID ID 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

ТЕСТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА НЕСАНКЦІОНОВАНИЙ ДОСТУП

Анотація. В сучасному світі з року в рік збільшується кількість кібератак. Ці атаки несуть за собою масові втрати конфіденційних даних, виведення зі стану працездатності критично важливої інфраструктури. Кількість кібератак лише підвищилась з початком пандемії і несе за собою значні фінансові та репутаційні ризики для будь яких компаній. В роботі розглянуті можливі методи проведення тестування безпеки корпоративної мережі організації на несанкціоноване проникнення. Проведено моделювання тестування на несанкціонований доступ до вибраних інформаційних ресурсів та охарактеризовано можливі атаки після здобуття такого доступу. Наведено найбільш типові методи експлуатації можливих вразливостей у корпоративних мережах. Вибрано дистрибутив Kali Linux, оскільки він містить багато інструментів для тестування на проникнення, що дозволяє проводити як періодичні тестування мереж та вузлів, так і аудит безпеки корпоративної мережі з метою виявлення існуючих уразливостей, недоліків налаштування та закриття їх ще до можливого використання зловмисниками. У ході дослідження виявлено, що кожна система по-своєму унікальна через використання різного типу сигнатур та застосувань. Таке подання вимагає поглиблених знань про атаки та документації конкретної системи від розробника для налаштування самої системи щодо спостереження за специфічними додатками. Проведені моделювання процесу виявлення мережевих атак на основі утиліт ОС Kali Linux показали, що даний засіб є практичним вибором для адміністратора безпеки і дозволяє йому своєчасно виявити загрози інформаційній системі та проводити ефективний моніторинг операційного середовища в реальному часі. Саме завдяки утилітам запропонованої системи, на основі яких реалізується мережева атака на об’єкт захисту, можна нівелювати певного виду вразливості інформаційної системи чи її складових частин, що унеможливить реалізацію багатьох видів атак. Напрямки подальших досліджень можуть бути спрямовані на розробку мережевих утиліт для реалізації захисту різного типу операційних систем від несанкціонованих втручань та наступної їх інтеграції у систему утиліт для відповідного операційного середовища , а також підвищити ефективність моніторингу інформаційної системи в цілому на предмет виявлення різного роду вразливостей на її активи, що покращить її захист від багатьох видів мережевих атак.

Ключові слова: інформаційна система, вектори атаки, несанкціонований доступ, сервіси хмарних обчислень, тестування на проникнення

ВСТУП

Більшість сучасних автоматизованих систем обробки інформації є розподіленими, побудованими на стандартних мережевих архітектурах, які використовують типові набори мережевих сервісів і прикладного програмного забезпечення. Корпоративні мережі «успадковують» всі «традиційні» для локальних обчислювальних систем способи несанкціонованого втручання. Крім того, для них характерні і специфічні канали проникнення та несанкціонованого доступу до інформації, зумовлені використанням мережевих технологій.

Безпека інформаційної мережі включає захист обладнання, програмного забезпечення, даних і персоналу. Мережева безпека складається з положень і політики, прийнятої адміністратором мережі, щоб запобігти і контролювати несанкціонований доступ, неправильне використання, зміни або відмови в комп'ютерній мережі та мережі доступних ресурсів. Мережева безпека включає в себе дозвіл на доступ до даних в мережі, який надається адміністратором мережі. Користувачі вибирають або їм призначаються ідентифікатор і пароль або інші перевірки автентичності інформації, що дозволяє їм здійснити доступ до інформаційних ресурсів у рамках своїх повноважень.

Мережева безпека охоплює різні комп'ютерні мережі, як державні, так і приватні, які використовуються в повсякденних робочих місцях для здійснення угод і налагодження зв'язків між підприємствами, державними установами та приватними особами. Мережі можуть бути приватними, такими як всередині компанії або відкритими, для публічного доступу. При цьому, найбільш поширений і простий спосіб захисту мережевих ресурсів від несанкціонованих втручань є присвоєння їм унікального імені та відповідного паролю. Проте, на цей час існує низка технік та методик щодо несанкціонованого доступу до таких "запаролених" мережевих ресурсів. З огляду на сказане, виникає потреба аналізу вразливостей мережевих ресурсів на несанкціоновані втручання [1].

Тестування на проникнення, пентестинг чи етичний злом − це процес оцінки програми чи інфраструктури на наявність вразливостей, тобто, намагання використати ці вразливості та обійти або пошкодити компоненти системи безпеки за допомогою ручного тестування. Такі вразливості, як правило, мають місце через неправильну конфігурацію, незахищений код, погано розроблену архітектуру чи розкриття конфіденційної інформації. Результатом є діючий звіт, який пояснює кожну вразливість або ланцюжок вразливостей, які використовуються для отримання доступу до цілі з кроками, вжитими для їх експлуатації, а також описом способу їх усунення та подальшими рекомендаціями превентивних дій щодо їх нівелювання. Кожній виявленій вразливості присвоюється рейтинг ризику, який використовується для покращення безпеки тестованої системи [1-2].

Постановка проблеми. Проблеми забезпечення інформаційної безпеки в корпоративних комп’ютерних мережах зумовлені загрозами безпеки локальних робочих станцій, локальних мереж і атаками на інформаційні ресурси корпорації, які мають вихід в загальнодоступні мережі передачі даних. Мережеві атаки на стільки ж різноманітні, як і системи, проти яких вони спрямовані. Деякі атаки відрізняються високою складністю. Іншого виду атаки здатен втілити навіть звичайний оператор, який не підозрює про наслідки, причиною яких може стати його діяльність. З точки зору безпеки розподілені системи характеризуються перед усім наявністю віддалених атак, оскільки компоненти розподілених систем, зазвичай, використовують відкриті канали передачі даних і порушник може не тільки проводити пасивне прослуховування інформації, що передається, а й модифікувати цей трафік (активна взаємодія). І якщо активний вплив на трафік може бути зафіксовано, то пасивний практично не піддається виявленню. Складність виявлення факту проведення віддаленої атаки забезпечує такому виду неправомірних дій перше місце за ступенем важливості, оскільки труднощі з виявленням перешкоджає своєчасному реагування на здійснювану загрозу, в результаті чого у порушника збільшуються шанси на успішну реалізацію атаки.

Аналіз останніх досліджень і публікацій. Атаки на інформаційну систему як правило вимагають попередні знання про мережі та її хостах атаки. Наприклад, для проведення ICMP-атаки Smurf потрібно знайти проміжну мережу з великою кількістю хостів, що відповідають на ехо-запити, при цьому така мережа повинна бути досяжна

для пакетів з широкомовною адресою цієї мережі, які були надіслані з мережі зловмисника, безумовно, повинна бути відома IP- адреса комп'ютера атаки. Для атаки ICMP / UDP-затопленням потрібно знати адреси хостів проміжної мережі, а також номери пасивних портів цих хостів; для атаки ICMP / chargen / echo-затопленням - адреси хостів проміжної мережі з активними портами 7 і 19, і т. д. [3]

Якщо зловмисник хоче задіяти мережу ботів, заражених вірусом певного типу, то йому знадобиться просканувати велику кількість комп'ютерів на відгук за певним портом, який використовується цим вірусом для отримання команд від контролера атаки. Віруси намагаються поширитися на якмога більшу кількість комп'ютерів, але заздалегідь не можна сказати, чи буде успішним таке впровадження для якогось певного хоста, - це залежить від конфігурації засобів захисту та параметрів ОС хоста. Тому зловмисник заздалегідь не знає, які хости він може використовувати в якості членів мережі ботів, і тому йому потрібно зібрати відомості про заражених комп'ютерах [4].

Тому майже будь-яку атаку передує мережева розвідка, при якій зловмисник намагається зібрати необхідні для атаки відомості. Конкретний набір відомостей залежить від типу атаки, але частіше за все мережева розвідка включає збір таких даних: IP-адреси активних (тобто включених, що відповідають на мережевий трафік) хостів; номера активних TCP-портів; номера активних і пасивних UDP-портів хостів; тип і версії ОС і додатків [5].

Виявлення IP-адрес активних хостів мережі називають скануванням мережі (network scanning). Сам термін «сканування» говорить про те, що зловмисник тестує один за одним всі можливі значення IP-адрес деякої підмережі (наприклад, для підмережі з маскою / 24 це 254 значення) або номера портів (65 535 для TCP і стільки ж для UDP). Для сканування мережі та портів використовуються більш витончені засоби, ніж утиліта ping або стандартна процедура встановлення TCP-з'єднання, які легко блокуються фаєрволами. До одного з публічно доступних портів, найчастіше до порту 80 (порт веб-сервера), який з великим ступенем ймовірності (але, звичайно, не обов'язково) відкритий для зовнішнього доступу. Якщо хост відповідає пакетом SYN / ACK, то сканер вважає, що хост активний, і завершує TCP-з'єднання пакетом з ознакою RST [6].

Схожі методи застосовуються і для сканування портів. Тут перевага віддається SYN-скануванню протоколу TCP, оскільки перевіряються десятки тисяч портів (по 65 535 портів для TCP і UDP). Сканування портів часто здійснюється за допомогою тих же спеціалізованих програмних засобів, що і для інвентаризації мережі та аудиту її захищеності. (Metasploit, Nmap) [5, 7].

Системи виявлення вторгнень дозволяє виявити атаки, а саме трасування мережі, сканування портів, стеків TCP, атаки відмови в обслуговуванні, впровадження вірусів, атаки на вразливості операційної системи чи окремих додатків. В мережі організації може бути декілька таких систем. При одночасній роботі вони працюють узгоджено, пересилаючи повідомлення про підозрілий трафік в центральний сервер системи, який у свою чергу збирає та систематизує ці дані, а також повідомляє адміністратора.

Системи виявлення сигнатур можна розділити на дві категорії: ті, що працюють на основі перевірки сигнатур і ті, що працюють на основі виявлення аномалій. Система, що працює на основі перевірки сигнатур, веде базу даних сигнатур атак. Кожна сигнатура – це набір правил, які описують способи боротьби з вторгненнями. Дана система аналізує кожен пакет, що проходить через неї, порівнюючи його вміст з сигнатурами бази даних. Якщо пакет співпадає з сигнатурою, то генерується попередження. Недоліком такого підходу є те, що система безсильна проти незареєстрованих атак.

Система, що працює на основі виявлення аномалій, створює профіль надійного трафіку, який спостерігається у штатному режимі. Після цього вона відстежує такі

потоки пакетів, які мають статичні «дивацтва». Наприклад, непропорціональне збільшення пакетів, або різний скачок інтенсивності сканування портів. Переагою таких систем є те, що вони можуть відстежувати нові, ще не описані атаки [4-7].

Пошук уразливостей − важлива частина завдання забезпечення безпеки. Ця робота включає в себе регулярне тестування інформаційної системи. У будь-який момент часу для будь-якої системи можна вказати безліч різних видів уразливостей, наприклад, для операційних систем і прикладних програм нові уразливості з'являються мало не щодня; виявляти їх вручну є дуже трудомістким завданням. Тому для автоматизації пошуку уразливостей використовують різні програмні інструменти − засоби сканування уразливостей, такі, наприклад, як GFI LANguard, Nessus, OpenVAS, SPARTA, Lynis, Maltego та інші [8−10].

Мета статті. Насичення ринку IT різноманітними інформаційними системами ставить перед користувачем термінову необхідність вибору оптимального способу виявлення атак та запобігання несанкціонованому вторгненню до його системи, поданні йому відповідної методології тестування на проникнення. Метою роботи є формування та подання користувачеві методик щодо вибору систем, які позиціонуються як IDS (Intrusion Detection System − Система виявлення атак (вторгнень), що надаватиме йому можливість отримати цілісну картину про загрози безпеці його інформаційної системи незалежно від використовуваного в ній операційного середовища. Це дозволить вжити превентивних заходів щодо підвищення ефективності засобів захисту інформаційної системи в цілому.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проведення тестування на несанкціонований доступ до організації розпочато з процедури збору інформації для прогнозування можливих векторів атак та способі отримання несанкціонованого доступу. Для моделювання процесу збору інформації досліджено офіційний веб-сайт diia.gov.ua. (рис.1). На зображенні поданого рисунку можна помітити знайдену інформацію про організацію в соціальній мережі Linkedin. Під час збору інформації на ресурсах сайту Міністерства цифрової трансформації України знайдено дані людей, які працюють у цій організації, а також формат електронної пошти використовуваний в організації.

Рис.1. Вибір урядового сайту для моделювання процесу збору інформації

На рис.2., відображена знайдена інформація про організацію за допомогою утиліти Email Hunter. Одержана інформація являє собою список електронних поштових скриньок працівників цієї організації.

ISSN 2663 - 4023

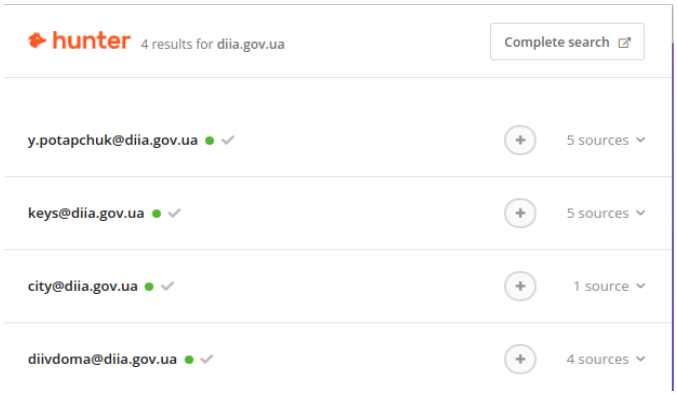

Рис.2. Знайдені утилітою Email Hunter електронні скриньки працівників організації

Ці дані можуть знадобитися для проведення атак методами соціальної інженерії при уособленні криптоаналітика одним з працівників даної організації.

Для подальшого збору інформації використано утиліту Maltego, яка формує граф на основі аналізу зв'язків знайденої інформації. Таке програмне забезпечення застосовується в онлайн-розслідуваннях для автоматизації процесу і пошуку зв'язків між шматками інформації, які розміщені на різних джерелах мережі інтернет. В результаті сканування домену diia.go.ua отримано результат, поданий на рис. 3. У цьому випадку видно фізичні адреси розташування серверів AWS (сервіси хмарних обчислень), на яких хоститься веб сайт Дії, а також сервери пов'язані з київським офісом Дії.

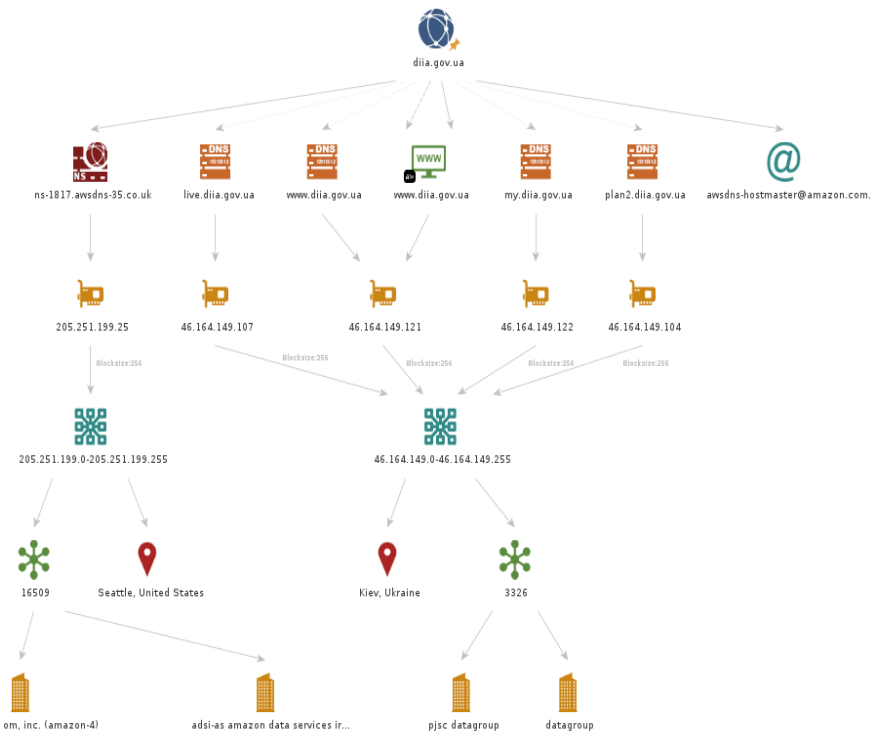

Рис.3. Зображення отриманого в результаті роботи утиліти Maltego графу

ISSN 2663 - 4023

Досліджену інформацію можна використовувати для визначення пріоритетних векторів атак, а також наявність цієї інформації надає можливість проводити атаки методом соціальної інженерії. Після дослідження поданим методом сайту, було зібрано достатню кількість інформації для визначення векторів можливих атак. Цей етап триваліший і чим більше та докладніше буде зібрано інформації, тим вищий шанс знайти вразливість.

Для прикладу в роботі досліджено вразливість домену vns.lpnu.ua з використанням утиліти Nikto, яка виконала основне сканування порту 80 для даного домену та надала повний звіт на основі виконаних сканувань, поданих на рис.4.

У результаті сканування порта 80 отримано детальну інформацію про нашу ціль, таку як IP адреса хоста, порт, а також дату початку сканування. Також сканер надав список потенційних вразливостей сканованої цілі. Можна побачити сесійну "кукі" створену без HttpOnly прапора, що є доволі небезпечно для власника сайту. Також сканер надав підказки про файли на сайті, які потенційно можуть тримати в собі конфінденційну інформацію.

```
sasha@sasha-VirtualBox:~$ nikto -h vns.lpnu.ua
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          178.212.110.23
+ Target Hostname:    vns.lpnu.ua
+ Target Port:        80
+ Start Time:         2022-05-01 14:54:59 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.37 (centos) OpenSSL/1.1.1c
+ Cookie MoodleSession created without the httponly flag
+ Retrieved x-powered-by header: PHP/7.3.29
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-redirect-by' found, with contents: Moodle
+ Root page / redirects to: https://vns.lpnu.ua/login/index.php
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to
XST
+ /config.php: PHP Config file may contain database IDs and passwords.
+ Uncommon header 'x-accel-buffering' found, with contents: no
+ OSVDB-3092: /html/: This might be interesting...
+ Uncommon header 'x-ua-compatible' found, with contents: IE=edge
+ Uncommon header 'content-script-type' found, with contents: text/javascript
+ Uncommon header 'content-style-type' found, with contents: text/css
+ Uncommon header 'x-frame-options' found, with contents: sameorigin
+ OSVDB-3092: /login/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ Server leaks inodes via ETags, header found with file /INSTALL.txt, fields: 0
x298 0x5da84d33bc080
+ OSVDB-3092: /INSTALL.txt: Default file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6544 items checked: 0 error(s) and 17 item(s) reported on remote host
+ End Time:           2022-05-01 15:00:03 (GMT3) (304 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Рис. 4. Сканування домену vns.lpnu.ua за портом 80

Nikto Domain Scan. Для доменів з увімкненим HTTPS потрібно вказати прапор -ssl для сканування порта 443:

У результаті сканування порта 443 ми отримано більш детальну інформацію про домен, вдобавок до стандартної інформації додалась ще інформація про SSL сертифікат сайта.

Також сканер надав список потенційних вразливостей домену, наприклад, можна побачити, що сайт використовує wildcard сертифікат, а це означає, що його секретний ключ лежить всюди, де використовується цей сертифікат, що може бути потенційною вразливістю.

ISSN 2663 - 4023

```
sasha@sasha-VirtualBox: $ nikto -h vns.lpnu.ua -ssl
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          178.212.110.23
+ Target Hostname:    vns.lpnu.ua
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject: /C=UA/ST=Lvivska oblast/O=Lviv Polytechnic National
 University/CN=*.lpnu.ua
                   Ciphers: TLS_AES_256_GCM_SHA384
                   Issuer:  /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Lim
ited/CN=Sectigo RSA Organization Validation Secure Server CA
+ Start Time:         2022-05-01 15:02:01 (GMT3)
---------------------------------------------------------------------------
+ Server: Apache/2.4.37 (centos) OpenSSL/1.1.1c
+ Cookie MoodleSession created without the httponly flag
+ Retrieved x-powered-by header: PHP/7.3.29
+ The anti-clickjacking X-Frame-Options header is not present.
+ Uncommon header 'x-redirect-by' found, with contents: Moodle
+ Root page / redirects to: https://vns.lpnu.ua/login/index.php
+ Server is using a wildcard certificate: '*.lpnu.ua'
+ Server leaks inodes via ETags, header found with file /, fields: 0x30c0b 0x5c
5c7fdeec240
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to
XST
+ Uncommon header 'content-script-type' found, with contents: text/javascript
+ Uncommon header 'content-style-type' found, with contents: text/css
+ Uncommon header 'x-ua-compatible' found, with contents: IE=edge
+ Uncommon header 'x-frame-options' found, with contents: sameorigin
```

Рис. 5. Результат сканування домену за протоколом https

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного тестування виявлено значну кількість вразливостей інформаційних ресурсів. Зібрана тестувальником інформація про вразливості допоможе компаніям визначити поточний рівень захисту їхньої інформаційної системи, ідентифікувати вразливості та пріоритезувати їх за рівнем критичності, а також скласти план реакції на подальші кібератаки.

У ході дослідження було виявлено, що кожна система по-своєму унікальна через використання різного типу правил (сигнатур) та застосувань. Таке подання вимагає поглиблених знань про атаки та документації конкретної системи від розробника для налаштування самої системи щодо спостереження за специфічними (нестандартними) додатками.

Вибрано дистрибутив Kali Linux, оскільки він містить багато інструментів для тестування на проникнення, що дозволяє проводити як періодичні тестування мереж та вузлів, так і аудит безпеки корпоративної мережі з метою виявлення існуючих вразливостей, недоліків налаштування та закриття їх ще до можливого використання зловмисниками.

Напрямки подальших досліджень можуть бути спрямовані на розробку мережевих утиліт для реалізації захисту різного типу операційних середовищ від несанкціонованих втручань та наступної їх інтеграції у цілісну систему утиліт під управлінням операційної системи, а також підвищення ефективності моніторингу інформаційної системи в цілому єна предмет виявлення різного роду вразливостей на її активи. Це покращить їх захист від багатьох видів мережевих атак.

ISSN 2663 - 4023

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Parasram, S. V. N., Samm, A., Boodoo, D., Johansen, G., Allen, L., Heriyanto, T., Ali, S. (2018). Kali Linux 2018: Assuring Security by Penetration Testing Fourth Edition. *Packt Publishing*.

2 *Penetration testing*. IT Governance - Governance, Risk Management and Compliance for Information Technology. https://www.itgovernance.co.uk/penetration-testing.

3 *OWASP foundation, the open source foundation for application security | OWASP foundation*. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org.

4 Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

5 Positive Technologies. (2019). *Penetration testing of corporate information systems: statistics and findings, 2019*. Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions. https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019.

6 Parasram, S. (2020). Digital Forensics With Kali Linux - Second Edition. *Packt Publishing*.

7 Stoykov, A., (2021). *Metasploitable 2 Full Walkthrough*. MATRIX Labs. https://matrixlabsblog.wordpress.com/2019/04/02/metasploitable-2-full-walkthrough

8 *Homepage*. Homepage - Maltego. https://www.maltego.com

9 *Download Nessus Vulnerability Assessment | Nessus®* Tenable®. https://www.tenable.com/products/nessus

10 *Burp Suite - Kali Linux Tools.* (2021). Kali.tools. https://kali.tools/?p=1589.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (18), 2022
ISSN 2663 - 4023

Ivan Tyshyk
Ph.D, Docent, Associate Professor at the Department of Information Security National University "Lviv Polytechnic", Lviv, Ukraine
ORCID ID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

TESTING THE ORGANIZATION'S CORPORATE NETWORK FOR UNAUTHORIZED ACCESS

Abstract. In today's world, the number of cyber attacks is increasing every year. These attacks lead to massive loss of confidential data, disruption of critical infrastructure. The number of cyberattacks has only increased since the beginning of the pandemic and carries with it significant financial and reputational risks for any company. The work considers possible methods of testing the security of the organization's corporate network against unauthorized penetration. Simulation of testing for unauthorized access to selected information resources was carried out and possible attacks after obtaining such access were characterized.
The most typical methods of exploitation of possible vulnerabilities in corporate networks are given. The Kali Linux distribution was chosen because it contains many tools for penetration testing, which allows for periodic testing of networks and nodes, as well as corporate network security audits in order to identify existing vulnerabilities, configuration flaws and close them before they can be used by attackers. During the study, it was found that each system is unique in its own way due to the use of different types of signatures and applications. Such a representation requires in-depth knowledge of attacks and system-specific documentation from the developer to configure the system itself to monitor specific applications. Conducted simulations of the process of detecting network attacks based on the Kali Linux OS utilities showed that this tool is a practical choice for a security administrator and allows him to detect threats to the information system in a timely manner and conduct effective monitoring of the operating environment in real time. Thanks to the utilities of the proposed system, on the basis of which a network attack on the object of protection is implemented, it is possible to eliminate a certain type of vulnerability of the information system or its constituent parts, which will make it impossible to implement many types of attacks. The directions of further research can be aimed at the development of network utilities to implement the protection of various types of operating systems against unauthorized interventions and their subsequent integration into the system of utilities for the appropriate operating environment, as well as to increase the effectiveness of monitoring the information system as a whole for the purpose of detecting various types of vulnerabilities on its assets , which will improve its protection against many types of network attacks.

Keywords: information system, attack vectors, unauthorized access, Amazon Web Services, penetration testing

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Parasram, S. V. N., Samm, A., Boodoo, D., Johansen, G., Allen, L., Heriyanto, T., Ali, S. (2018). Kali Linux 2018: Assuring Security by Penetration Testing Fourth Edition. *Packt Publishing*.
2 *Penetration testing*. IT Governance - Governance, Risk Management and Compliance for Information Technology. https://www.itgovernance.co.uk/penetration-testing.
3 *OWASP foundation, the open source foundation for application security | OWASP foundation*. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org.
4 Official PCI Security Standards Council Site - Verify PCI Compliance, Download Data Security and Credit Card Security Standards. https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
5 Positive Technologies. (2019). *Penetration testing of corporate information systems: statistics and findings, 2019*. Positive Technologies - vulnerability assessment, compliance management and threat analysis solutions. https://www.ptsecurity.com/ww-en/analytics/corp-vulnerabilities-2019.

6 Parasram, S. (2020). Digital Forensics With Kali Linux - Second Edition. *Packt Publishing*.
7 Stoykov, A., (2021). *Metasploitable 2 Full Walkthrough*. MATRIX Labs. https://matrixlabsblog.wordpress.com/2019/04/02/metasploitable-2-full-walkthrough
8 *Homepage*. Homepage - Maltego. https://www.maltego.com
9 *Download Nessus Vulnerability Assessment | Nessus®* Tenable®. https://www.tenable.com/products/nessus
10 *Burp Suite - Kali Linux Tools.* (2021). Kali.tools. https://kali.tools/?p=1589.