УДК 004.7

Цевчук В.С., магістрант
Бродський Ю.Б., к.т.н., доцент
Державний університет «Житомирська політехніка»

ПРОЄКТУВАННЯ HONEYPOT-ПІДСИСТЕМИ ДЛЯ ЗАХИСТУ ПУБЛІЧНИХ ПОРТІВ КОРПОРАТИВНИХ МЕРЕЖ

Сучасні тенденції розвитку цифрових мереж в Україні передбачають суттєве посилення захисту публічних портів корпоративних мереж. Концепція Honeypot використовується для створення оманливих сервісів, в яких ключова роль відводиться проактивному моніторингу та блокуванню загроз. Саме проєктна реалізація Honeypot з інтеграцією в MS Active Directory є важливим чинником підвищення безпеки, оскільки традиційні методи (фаєрволи, IDS/IPS) не забезпечують проактивного моніторингу та збору threat intelligence. Згідно з даними звіту Cybersecurity Ventures, кількість кібератак на корпоративні мережі зросла на 50% у 2024 році, що підкреслює необхідність інноваційних рішень, таких як Honeypot, для збору даних про атаки в реальному часі. У контексті українських підприємств, де MS Active Directory є поширеним інструментом управління, відсутність адаптованих honeypot-підсистем призводить до вразливостей у публічних портах, як SSH, Telnet, HTTP/HTTPS, що експлуатуються для несанкціонованого доступу.

У мережах на базі MS Active Directory публічні порти (SSH, Telnet, HTTP/HTTPS) вразливі до несанкціонованого доступу, що призводить до компрометації домену та витоку даних. Проблема посилюється відсутністю інтегрованих honeypot-підсистем з блокуванням IP, обмеженням віртуальним середовищем, браком кількісного аналізу ефективності та фокусу на сучасних загрозах (AI-driven attacks, zero-day exploits). Аналіз застосування схожих технологій виявив сильні сторони в теорії та реалізації, але слабкості в емпіричних даних.

Тому метою дослідження є розробка honeypot-підсистеми для виявлення і блокування зловмисних IP-адрес на публічних портах мережі на базі MS Active Directory, підвищивши рівень кібербезпеки через моніторинг загроз.

Модель прототипу підсистеми розроблялася в середовищі VirtualBox на базі програмного забезпечення Oracle VirtualBox як гіпервізора, Ubuntu Server як шлюзу, Windows Server для MS Active Directory, Cowrie для емуляції SSH/Telnet, Honeyhttpd для HTTP/HTTPS та Kali Linux для симуляції атак, застосовуючи методи експериментального тестування та аналізу логів JSON та Fail2Ban.

В результаті проєктування отримана модель honeypot-підсистеми з інтеграцією в AD через Ubuntu-шлюз з iptables для блокування IP. Прототип розробленої підсистеми є результативним і дійсно виконує функцію виявлення атак (SSH/HTTP) з низьким відсотком помилкових спрацювань.

Таким чином, у доповіді буде представлено модель яка відображає прототип honeypot-підсистеми для мереж MS Active Directory.

Теоретична та практична значимість проведеного дослідження полягає в розширенні знань про застосування honeypot, обґрунтовуючи віртуальну інтеграцію для моніторингу загроз та розвитку теорії кібербезпеки з акцентом на емуляцію сервісів і аналіз threat intelligence, а також у запропонованих рекомендаціях щодо налаштування інструментів Cowrie, Honeyhttpd та Fail2Ban, що суттєво зменшує ризики без значних витрат ресурсів. Запропоновану модель доцільно впроваджувати в корпоративні мережі, що забезпечить на погляд авторів підвищення ефективності виявлення атак, блокування IP-адрес та оптимізації політик Active Directory. Практична значимість полягає в

В перспективі подальше дослідження буде орієнтуватися на масштабування до реальних продуктивних мереж з інтеграцією традиційних IDS/IPS систем, на розширення на додаткові протоколи (FTP, RDP), а також тестування в хмарних середовищах, таких як Azure AD.

Список використаних джерел:

1. Honeypots: tracking hackers. Boston : Addison-Wesley, 2002. 452 с.
2. Blue team handbook: incident response edition : a condensed field guide for the cyber security incident responder. 2-ге вид. CreateSpace Independent Publishing Platform, 2014. 146 с.
3. Public-Facing infrastructure – threatng security - external attack surface management (EASM) - digital risk protection - security ratings. ThreatNG Security. URL: https://www.threatngsecurity.com/glossary/public-facing-infrastructure.
4. Cybercrime To Cost The World $9.5 Trillion USD Annually In 2024. Cybersecurity Ventures. URL: https://cybersecurityventures.com/cybercrime-to-cost-the-world-9-trillion-annually-in-2024/