УДК 004.03+004.056

Кульчицький Б. В.
Куперштейн Л. М.

АНАЛІЗ ІНСТРУМЕНТАЛЬНИХ ЗАСОБІВ ЗДІЙСНЕННЯ DDOS-АТАК

Вінницький національний технічний університет

Анотація
В роботі розглянуто інструменти для реалізації DDoS-атак. Проаналізовано їх параметри, можливості та методи на яких вони базуються.
Ключові слова: DDoS-атака, інструмент, мережева безпека.

Abstract
The paper considers tools for implementing DDoS-attacks. Their parameters, possibilities and methods on which they are based are analyzed
Keywords: DDoS-attack, tool, network security.

Вступ

DDoS-атаки запускаються через добре організовану, розподілену і віддалену керовану мережу таким чином, щоб скомпрометовані комп'ютери (зомбі або боти) могли бути використані для передачі великого обсягу безперервних і одночасних запитів до цільової системи.

DDoS-атаки головним чином викликають незвичайну поведінку у вигляді недоступності, неможливості доступу до конкретного веб-сайту або послуги та уповільнення продуктивності мережі. В результаті цільові системи реагують повільно або повністю відмовляють [1].

В останні роки DDoS-атаки були збільшені в силі, частоті та складності. Зловмисники постійно вдосконалюють свої навички та змінюють свій режим роботи і використовують новітні технології для запуску різноманітних DDoS-атак. Незважаючи на те, що дослідники запропонували багато рішень для виявлення чи запобігання DDoS-атак, зловмисники постійно розробляють нові методи і засоби, щоб обійти ці контрзаходи. Доступно цілий ряд інструментів, які можуть генерувати подібний легітимний трафік, а також трафік атак які легко обходять існуючі рішення захисту від DDoS.

Метою даного дослідження є аналіз існуючих програмних засобів якими здійснюють DDoS-атаки, щоб дослідники мали змогу проектувати експерименти у реальному часі для перевірки розробленого захисту.

Результати дослідження

Результати дослідження висвітлюють ключові технічні особливості інструментів для здійснення DDoS-атак, які використовуються зловмисниками для запуску DDoS-атак. Ця інформація допоможе дослідникам вибрати відповідні інструменти для їх експериментів у реальному часі та розробленню нових рішень для постійно зростаючої проблеми DDoS-атак [2].

Широкий вибір безкоштовних інструментів для проведення DDoS-атаки доступний в Інтернеті. Більшість з них дуже потужні і руйнівні, вони можуть легко зірвати цільову мережу та веб-додатки з точки зору пропускної спроможності та вичерпання ресурсів [3]. З таких програм LOIC, Xoic, RUDY і HULK які зможуть генерувати легітивний HTTP трафік. Хоча Trinoo, Stacheldraht, Shaft, Mstream і Trinity мають можливості для запуску потужних DDoS-атак, але вони сьогодні застарілі і недостатньо потужні в порівнянні з іншими інструментами для реалізації атаки у списку.

Усі популярні інструменти атаки порівнюються на основі ключових особливостей, які показано в таблиці 1. Основні можливості включають підтримуванні операційні системи, ціль атаки, можливість створити ботнету та типу протоколу.

Таблиця 1 – Порівняння різних програмних засобів для здійснення DDoS-атак

Назва	ОС	Ціль атаки	Можливість створити ботнет	Тип протоколу	Можливості
HULK	Windows, Linux	Ресурс	Ні	TCP, HTTP	• Обхід кешування. • Генерування унікального та заплутаного трафіку. • Генерування великого обсягу трафіку на веб-сервері.
Tor's Hammer	Linux, MacOS	Пропускна здатність, ресурс	Так	HTTP	• Використовуючи разом з Tor складний для виявлення. • Атака може бути здійснена на Apache та ISS сервери.
Slowloris	Windows, Linux	Пропускна здатність, ресурс	Ні	TCP, HTTP	• Відправляє авторизований HTTP трафік до сервера. • Атака намагається створити максимальну кількість відкритих з'єднань, яке досягається за рахунок відповідних запитів. • Атака намагається тримати з'єднання максимально довгим.
LOIC	Windows, Linux, MacOS, Android	Ресурс	Так	TCP, UDP, ICMP, HTTP	• Можливо здійснювати атаку на основі URL чи IP-адреси сервера. • Не приховує IP-адресу.
Xoic	Windows	Ресурс	Так	TCP, UDP, ICMP	• Просте у використанні. • Надає три режими атаки: тестування, нормальний, змішаний.
DDoSim	Linux	Ресурс	Так	TCP, UDP, HTTP, SMTP	• Атакує сервер відтворюючи багато зомбі хостів. • Може виконувати HTTP DDoS-атаку використовуючи дійсні запити. • Може виконувати DDoS-атаку використовуючи недійсні запити.
RUDY	Linux	Ресурс	Ні	HTTP	• Інтерактивне меню консолі. • Можливість вибору форми з URL для POST DDoS-атаки.
Pyloris	Windows, Linux, MacOS	Ресурс	Так	TCP, UDP, HTTP, SMTP, IMAP, TELNET	• Простий у використані графічний інтерфейс. • Безпосередньо здійснює атаку на сервер.

Hulk – програмний засіб, що може вивести сервера з роботи через хвилину, оскільки він безпосередньо впливає на завантаження сервера [4]. Він генерує flood TCP SYN і багатопотоковий flood HTTP GET. Також має можливість відправляти різні шаблони запитів атаки, які можуть заплутати реферера для кожного запиту. Tor's Hammer [4] – програмний засіб розроблений на Python який базується на повільному POST запиту, який проходить через TOR мережі. Tor's Hammer використовує випадкові джерела IP-адрес ускладнюючи відслідкування джерело атакуючого. Slowloris – створює flood TCP SYN запити до жертви. Містить як графічний інтерфейс так і командний рядок [5]. LOIC – програмний засіб з відкритим кодом який розроблений Praetox Technologies [6]. LOIC спрямований на виснаження ресурсів жертви таких як CPU, пам'яті та інше. Xoic – виконує DDoS-атаку на будь-який сервер з визначеною IP-адресою, з обраним портом та з обраним протоколом [7]. Розроблений за допомогою мови програмування C# та використовує модель IRC. DDoSim – використовує випадкові IP-адреси для стимулювати декількох ботів з повним TCP з'єднанням [8]. Інтерфейс командний рядок який реалізований мовою програмування C++ та виснажує ресурси жертви. Rudy – програмне забезпечення розроблене на основі Python для реалізації повільної DDoS-атаки для повалення веб-серверу [9]. Pyloris – інструмент на основі скрипту, який

використовується для тестування вразливостей певного класу атак [10]. Використовується вбудовані методи Slowloris та тест на готовність сервера витримати ботнет.

Висновки

Розглянуто інструменти для реалізації DDoS-атак. Проаналізовано параметри та можливості які вони надають. Всі розглянуті інструменти є у відкритому доступі. Вибір відповідного надасть змогу розробнику засобу захисту протестувати його ефективність в реальному часі, що в свою чергу пришвидшить її налагодження.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Voytovych O. P. Denial-of- Service attacks investigation / Voytovych O. P., Kolibabchuk E. I., Kupershtein L. M. // Вісник ХНУ: серія Технічні науки. - №3. -2016. - С. 129-133.
2. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с
3. Voitovych O. Investigation of simple Denial-of-Service attacks / O. Voitovych, Y. Baryshev, E. Kolibabchuk and L. Kupershtein // 2016 Third International Scientific-Practical Conference “Problems of Infocommunications Science and Technology (PIC S&T)”, Kharkiv, Ukraine, 2016, pp. 145-148.
4. Packet Storm, DDoS Attack Tools, [назва з екрану]. – Режим доступу до джерела: http://packetstormsecurity.org
5. Sourceforge, DDoS Attack Tools [назва з екрану]. – Режим доступу до джерела: http://sourceforge.net/projects/slowloris
6. Low Orbit Ion Cannon (LOIC) [назва з екрану]. – Режим доступу до джерела: https://github.com/NewEraCracker/LOIC
7. Sourceforge, Xoic Tool to make (D)DoS attacks [назва з екрану]. – Режим доступу до джерела: https://sourceforge.net/directory/os:windows/?q=xoic
8. Sourceforge, DDOSIM - Layer 7 DDoS Simulator [назва з екрану]. – Режим доступу до джерела: https://sourceforge.net/projects/ddosim/
9. Sourceforge, R-U-Dead-Yet? (RUDY) [назва з екрану]. – Режим доступу до джерела: https://sourceforge.net/projects/ r-u-dead-yet/
10. Sourceforge, Pyloris a protocol agnostic application layer denial of service attack. [назва з екрану]. – Режим доступу до джерела: https://sourceforge.net/projects/pyloris/
11. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни „Основи науково-дослідної роботи/ Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44 с.

Кульчицький Богдан Володимирович – студент групи БС-18м, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна

Куперштейн Леонід Михайлович – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна

Kulchytskyi Bogdan V. – Student of Information Technologies and Computer Engineering epartment, Vinnytsia National Technical University, Vinnytsia, Ukraine

Kupershtein Leonid M. – PhD., Assoc. Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, Ukraine