переваги в боротьбі зі злочинцями. Для цього у вищих навчальних закладах системи МВС України повинні створюватися центри підготовки поліграфологів з урахуванням специфіки роботи поліції. Навчання у таких центрах дозволить поліцейським:

– отримати спеціальні знання в області природничо-наукових основ проведення досліджень на поліграфі;

– отримати знання в області спеціальної термінології;

– отримати знання в області правових основ та організаційних особливостей проведення тестів з використанням поліграфа;

– освоїти технічні пристрої, що використовуються при проведенні досліджень;

– освоїти ефективні методики і тести;

– освоїти специфіку аналізу результатів тестів на поліграфі і складання висновку експерта.

Одержано 16.04.2019

УДК 004.056.53

Ярослав Віталійович ОСІПОВ,
курсант групи Ф4-302 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

DDOS-АТАКИ ЯК ОСНОВНИЙ ВИД ЗЛОЧИНУ В КІБЕРСФЕРІ

Розподілена атака типу «відмова в обслуговуванні» (Distributed Denial of Service attack) – це зловмисна спроба порушити нормальний трафік цільового сервера, служби або мережі, перевантажуючи мета або навколишнє інфраструктуру потоком інтернет-трафіку. DDoS-атаки досягають ефективності, використовуючи кілька скомпрометованих комп'ютерних систем в якості джерел трафіку атаки.

У більшості випадків зловмисник використовує мережу з комп'ютерів, заражених вірусом. Вірус дозволяє отримувати необхідний і достатній віддалений доступ до зараженого комп'ютера. Мережа з таких комп'ютерів називається ботнет. Як правило, в ботнетах присутній координуючий сервер. Вирішивши реалізувати атаку, зловмисник відправляє команду сервера, який в свою чергу дає сигнал кожному боту розпочати виконання шкідливих мережевих запитів.

Різні вектори DDoS-атак націлені на різні компоненти мережевого підключення. Щоб зрозуміти, як працюють різні DDoS-атаки, необхідно знати, як здійснюється з'єднання з мережею. Майже всі DDoS-атаки включають в себе перевантаження цільового пристрою або мережі трафіком. Атаки можна розділити на три категорії: атаки прикладного рівня, протокольні атаки, та об'ємні атаки. Зловмисник може використовувати один або кілька різних

векторів атаки або циклічні вектори атаки, потенційно засновані на контрзаходи, зроблених метою.

Атаки прикладного рівня. Мета цих атак полягає в тому, щоб вичерпати ресурси цілі. Таки атаки важко захистити, так як трафік може бути важко помітити як шкідливий.

Протокольні атаки викликають збої в роботі служби, оскільки використовують всю доступну ємність таблиці станів серверів веб-додатків або проміжних ресурсів, таких як брандмауери і балансувальник навантаження. Протокольні атаки використовують слабкості на рівні 3 і рівні 4 стека протоколів, щоб зробити ціль недоступною. SYN Flood атака використовує рукостискання TCP, відправляючи цільового об'єкту велика кількість пакетів SYN «Початковий запит з'єднання» TCP з підробленими IP-адресами джерела. Цільова машина відповідає на кожен запит на підключення, а потім чекає останнього кроку рукостискання, який ніколи не відбувається, виснажуючи ресурси мети в процесі.

Об'ємні атаки. Ця категорія атак намагається створити перевантаження, споживаючи всю доступну пропускну здатність між ціллю та Інтернетом. Великі обсяги даних відправляються на ціль з використанням форми посилення або іншого засобу створення великого трафіку, такого як запити з ботнету.

Посилення DNS. Відправляючи запит на відкритий DNS- сервер з підробленим IP-адресом (реальний IP-адресу цілі), цільової IP-адреса потім отримує відповідь від сервера. Зловмисник структурує запит так, щоб DNS-сервер відповідав на ціль великою кількістю даних. В результаті ціль отримує посилення початкового запиту атакуючого.

У висновку необхідно відзначити, що атаки DDOS відбуваються щодня. Тому, якщо у вас є ресурси в мережі, то необхідно звернутися до фахівців з безпеки в Інтернеті. Але послуги фахівців можуть бути дорогими, і програмне забезпечення, яке вам потрібно, може бути ще дорожче, але ви ніколи не знаєте, коли вам може знадобитися захист.

Одержано 11.04.2019

УДК 681.3.06

Олексій В'ячеславович ПЕРЕЦЬ,
курсант групи Ф4-102 ХНУВС
Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКУ ЧЕРЕЗ СМАРТФОН

Мобільний телефон просто незамінним для кожної сучасної людини. Але, хоча такий зв'язок і має безліч позитивних якостей, її безпека все ж викликає чималі сумніви. Річ у тому, що сигнали, передаванні смартфонами, цілком можна перехопити та розшифрувати. Смартфон також схильний до вірусних атак. В цьому випадку, навіть якщо смартфон просто лежить на столі,