УДК 004.056.53

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0003-4794-743X;
Андрій Олександрович ЛАЩЕНКО,
студент 2 курсу групи Кб-дср-17-1 факультету № 6
Харківського національного університету внутрішніх справ

ОСОБЛИВІ ПИТАННЯ РЕАГУВАННЯ НА DOS ТА DDOS АТАКИ

Відокремлено в ряду загроз безпеки стоять вразливості DOS – Denial Of Service (відмова в обслуговуванні). Як правило, до цього класу нападів належать події, описувані в новинах «Хакери атакували сайт X, порушивши його роботу. Сайт не працював протягом Y годин». Тобто це саме «атака@, а не «злом». На сервер надходять запити, які він не може (не встигає) обробити, в результаті чого він не встигає обробити запити звичайних відвідувачів і виглядає для них як непрацюючий. Ці атаки не мають на меті викрасти дані, але можуть допомогти почати інші види атак, тобто звільнити шлях [1].

Коли користувач заходе в Інтернет мережу, неважливо як через Wi-Fi, через мобільний Інтернет чи через комп'ютерну мережу він отримуєте IP-адресу. IP-адреса це ідентифікатор (унікальний числовий номер) мережевого рівня, який використовується для адресації комп'ютерів чи пристроїв у мережах, які побудовані з використанням протоколу TCP/IP (наприклад Інтернет). Ця адреса може бути динамічна або статична, якщо динамічна то адреса буде періодично змінюватись, а якщо статична то тільки тоді коли власник цієї адреси захоче її змінити.

Під час моніторингу сайтів користувач обов’язково залишає свій IP-адрес, тому зловмисники можуть знайти користувача за цією адресою через спеціалізовані сайти, а також зробити хакерську атаку (Dos-атака) на відмову в обслуговуванні. Розподілена атака на відмову в обслуговуванні це – напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена. Іншими словами коли відбувається Dos-атака у мережі Інтернет у потерпілого користувача на комп’ютері вимикається і може перестати робити операційна система (ОС). Для такого типу атак зловмисники використовують Linux Kali (це ОС для перевірки різних систем на слабкі місця), а також спеціальні команди в його терміналі.

Для захисту від таких видів атак користувачам рекомендують використовувати VPN (англ. Virtual Private Network – віртуальна приватна мережа) – узагальнена назва технологій, що дозволяють

забезпечити одне або кілька мережних з'єднань (логічну мережу) поверх іншої мережі (наприклад, Інтернет), а також виставити динамічний IP-адрес [2].

Зміна IP-адреси і повне «знеособлення» користувача VPN дозволяє отримати максимальну анонімність при використанні Інтернету, стійке шифрування всіх відправлених і отриманих даних, захист від перехоплення паролів, онлайн-листування, платіжної інформації та ін., а також має можливість «телепортації» Інтернету в іншу країну та знімає будь-які географічні обмеження поточного місця виходу в мережу.

В якості висновку можна підкреслити що VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному клієнту бути повноцінним учасником віддаленої мережі та користуватись її сервісами – внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет.

Слід розглянути інший вид розповсюджених атак, таку як Ddos – атака. Ризниця Dos та Ddos атак в тому, що Dos – атаки проводяться як правило з одного комп'ютера користувача на слабкі веб-сайти з точки зору їх захисту де немає доменів захисту від цих атак, а Ddos-атаки використовують порти різних пристроїв які можуть бути просто приєднані до Інтернет мережі. Наприклад коли ми заходимо на сайт або переходимо по його вкладках ми відправляємо йому запит у розмірі 10~50 кб.

При Ddos – атаках користуються слабкими місцями Memcached (комп'ютерна програма, сервіс хешування даних в оперативній пам'яті на основі парадигми розподіленої хеш-таблиці) яка за допомогою клієнтської бібліотеки дозволяє хешувати дані в ОЗП одного або декількох серверів. Розподіл даних реалізується за значенням хеш-ключа). Зловмисники як правило використовують платний сервіс Shodan який надає порти пристроїв через які можна зробити Ddos-атаку. Далі через спеціальну програму вони відправляють запити на ці порти та через них переходять на вибраний для атаки сайт, тим самим збільшують пакети з 10 ~ 50 кб до 50 мб цим самим роблять величезне навантаження на сайт і таких пристроїв може бути безліч.

Наприклад, нещодавно була зроблена DDOS-атака на сайт GitHub де швидкість DDOS файлів була зафіксована близько 1,7 Tb/s більшість пристроїв які були там зафіксовані є системи домашньої автоматизації (англ. Smart home - системи домашніх пристроїв, здатних виконувати дії і вирішувати певні повсякденні завдання без участі людини) тобто їх власники не знали що через їх пристрої була зроблена Ddos-атака, і все це через те що в цих пристроях був відкритий порт 11211.

Висновок. Виходячи із вищенаведеного memcached використовує порт 11211 за замовчуванням. Так як в memcached немає вбудованих механізмів аутентифікації, то виходить, що будь-хто може приєднатися ззовні і використовувати його в своїх цілях. Щоб

уникнути цього, користувачі можуть або закрити порт 11211 за допомогою фаєрвола, або настроїти memcached-сервер, щоб він міг використовуватися тільки з локального хоста.

Список бібліографічних посилань

1. Виды взломов сайтов и их предотвращение // Captcha.Ru. URL: http://captcha.ru/articles/antihack/ (дата звернення: 10.10.2018).

2. Виды хакерских атак // Хакерские Атаки URL: https://sites.google.com/site/hakerskieataki/home/vidyhakerskih-atak (дата звернення: 10.10.2018).

Одержано 30.10.2018

УДК 343.9

Дмитро Юрійович УЗЛОВ,
кандидат технічних наук,
начальник Управління інформаційно-аналітичної підтримки
ГУНП в Харківській області;
ORCID: https://orcid.org/0000-0003-3308-424X;
Володимир Михайлович СТРУКОВ,
кандидат технічних наук, доцент
завідуючий кафедри інформаційних технологій факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
ORCID: http://orcid.org/0000-0003-4722-3159;
Олексій В'ячеславович ВЛАСОВ,
заступник начальника Управління інформаційно-аналітичної підтримки
ГУНП в Харківській області

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ У ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ЗЛОЧИННОСТІ

Інформаційний злочин – це навмисні дії, спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань. Інформаційні злочини включають до себе досить широкий спектр протиправної діяльності:

– шахрайство;

– незаконне копіювання;

– поширення шкідливих вірусів;

– злом паролів;

– крадіжка номерів банківських карт і інших банківських реквізитів;

– фішинг;

– поширення протиправної інформації (наклепу, матеріалів порнографічного характеру, матеріалів, що збуджують міжнаціональну та міжрелігійну ворожнечу і т.п.);

– зміна комп'ютерних даних;

– комп'ютерний саботаж або шкідливе втручання через комп'ютерні мережі в роботу різних систем;