УДК 004.057:681.3.064
DOI: 10.31673/2409-7292.2019.045262

Ю.С. Антонов, П.В. Римар, О.Г. Антонова

ПРОБЛЕМА DoS / DDoS АТАК НАВЧАЛЬНИХ РЕСУРСІВ СТУДЕНТАМИ

У роботі досліджено проблему DoS / DDoS атак на навчальні ресурси зі сторони студентів. Сформульовано причини, що можуть спонукати студентів до здійснення кібератак на ЗВО або навчальні ресурси. Розглянуто приклад реальної DoS атаки автоматизованої системи контролю знань студентом, та способи виявлення особи кіберхулігана. Запропоновано певні заходи з упередження та протидії атакам.

Ключові слова: кіберзагроза, кібератака, DoS, DDoS, запобіжні заходи, студент, навчальний ресурс, сканування портів, моніторинг активності, сертифікат, nmap, netstat, Apache Benchmark, Linux, iptables.

Вступ і постановка задачі

Сучасна освіта дуже активно використовує різноманітні ІТ-технології. Це дуже добре, оскільки дозволяє розширити можливості навчального процесу, полегшити роботу та спростити комунікацію між викладачами та студентами. Разом з цим викладачі стикаються з новими ризиками та загрозами у кіберпросторі, в тому числі DoS / DDoS атаками [1, 2, 3, 4, 5, 6]. Оскільки не всі викладачі за освітою є ІТ-фахівцями, а ІТ-фахівці можуть мати різну спеціалізацію, завжди будуть актуальними методи та методики підвищення захисту комп'ютерних систем від кіберзлочинців та підвищення загального освітнього рівня у сфері ІТ-технологій та кібербезпеці. Цю роботу присвячено проблемі попередження та удосконалення захисту від DoS / DDoS атак навчальних ресурсів, розробці організаційних та програмних заходів щодо запобігання, оперативного виявлення та реагування на атаки.

Аналіз останніх досліджень

На даний час проблема кіберзагроз та протидії ним є дуже гострою. В останні роки відзначається збільшення кількості кібератак, у тому числі DoS / DDoS [2, 7, 8, 9]. Так у 2018 році [8] частка атак на деякі галузі була наступною: державні установи – 19% , медичні установи – 11%, фінансова галузь – 10%, освітні установи – 7%, ІТ-компанії – 5%, телекомунікаційні компанії – 2%. У роботі [2] наводиться статистика, що свідчить про щорічне збільшення DDoS-атак у вересні, де в першу чергу страждає освітня система, а найбільш гучною була атака на сайт Единбурзького університету (один з провідних ЗВО Англії). Все частіше для здійснення DDoS атак використовуються специфічні пристрої: роутери, веб-камери, принтери та різноманітні пристрої зі світу IoT [10]. Проблема виявлення та захисту від DoS / DDoS атак розглядалась у роботах [12, 13, 14].

Метою статті є розгляд причин, що можуть спонукати студентів до здійснення кібератак на ЗВО або навчальні ресурси. Вивчення, удосконалення, розробка та узагальнення заходів щодо забезпечення інформаційної безпеки та протидії DoS / DDoS-атакам.

Основна частина

Під час навчального процесу в одному місці збирається дуже велика кількість людей, переважну більшість яких складає молодь від 16 до 25 років, що за всіма показниками є достатньо активною, дуже різною за характером і темпераментом, ставленням до навчального процесу та світу в цілому. Таким чином, перед нами достатньо потужна вибухова суміш, що може проявити себе будь-якої хвилини, і нехтувати нею у жодному випадку не можна [2, 3, 4, 5, 6]. Каталізатором для кібератаки може бути дуже багато причин, ось деякі з них:

неправильна, з точки зору студента, оцінка його знань, умінь або навичок;
відсутність бажання або не готовність студента складати іспит, залік, тест, тощо
особисті образи або проблеми комунікації з викладачем / однокурсниками;
бажання принизити викладача або навчальний заклад;
проблеми у коханні / особистому житті;
бажання перевірити щойно отримані знання (не обов'язково на лекціях);
помста;
бажання заробити гроші або створити собі певну репутацію.

Об’єктами атак у цьому випадку можуть бути:
навчальні ресурси, які належать ЗВО або викладачам особисто;
поштові скриньки викладачів;
електронні журнали;
корпоративні облікові записи;
месенджери;
стаціонарні ПК, ноутбуки, планшети, телефони;
та інші.
Для досягнення своєї мети, кіберзлочинці можуть використовувати:
DoS та DDoS атаки;
фішинг;
mailbombing або спам;
соціальний інжиніринг;
фізичний доступ до системи.

У цій роботі ми більш детально зупинимось на проблематиці DoS / DDoS атак. Для цього спочатку розглянемо реальний приклад. Одразу попередимо, що реальні IP-адреси, доменні імена, назви підприємств, тощо не будуть наводитись з етичних та інших міркувань. Більше того, на момент написання статті не всі учасники зазначених подій ліквідували недоліки своїх систем, що може привести до повторного використання вразливостей їх систем вже третіми особами.

Так студенти однієї групи мали проходити тестування за допомогою автоматизованої системи контролю знань (АСКЗ) A.S.T.S.. У зв’язку із певними труднощами, на той момент в якості серверу виступав NAS (CPU: AMD E350D; RAM 4Gb; LAN: 1000 Mbit; HDD: 2TB+2TB+3TB; OS: Linux Debian 9), який, окрім своїх прямих обов’язків, був змушений виконувати додаткові функції.

Сеанс тестування було призначено поза навчальним часом, а саме на 19:00. Все йшло за планом, студенти та викладач були готові до проведення тестування (з мови програмування C#). Через декілька хвилин після початку тестування переглядаємо поточні результати тестування та дізнаємось, хто із студентів не розпочав сеанс. Спочатку все йде добре, але згодом виникають ознаки некоректної роботи системи, а саме: достатньо повільне оновлення сторінки, відображення помилки про роботу з БД. Враховуючи режим експлуатації системи, стає зрозумілим, що є три причини такої поведінки:

активне використання NAS за прямим / цільовим призначенням;
відмова / перевантаження апаратної частини (CPU, HDD);
спроба зовнішнього втручання.

Моніторинг локальної мережі та апаратної частини показав, що з першими двома пунктами все гаразд, тому залишився виключно останній пункт – зовнішнє втручання. Одразу виникає декілька запитань:

Які саме компоненти системи атаковані?
Чи зміг зловмисник потрапити до системи?
Втручання зовнішнє чи це хтось «свій»?
Чому була атакована система?

Спробуємо знайти відповіді на наші запитання.

За допомогою утиліти top визначаємо, що найбільше навантаження у системі припадає на Apache та MySQL і складає приблизно 20 та 50 відсотків відповідно. Усі інші процеси знаходяться у межах норми. Далі намагаємось з’ясувати, звідки відбувається ця атака.

За допомогою програми netstat визначаємо статистику доступу до нашої системи (лістинг 1) та отримуємо результат зображений на рис 1. З наведених даних видно, що на одну IP-адресу припадає понад 700 підключень, у той час, як з інших IP-адрес – 2-3 з’єднання у середньому. Можна зробити висновок, що ця IP-адреса і є адресою, з якої здійснюється атака на нашу систему, оскільки:

кількість студентів не перевищує 33 особи;

вони не знаходяться територіально в одному місці;

студенти інших груп не брали участь у тестуванні.

Наступним кроком є аналіз та перевірка log файлів сервера apache2 за допомогою наступної команди:

grep 193.2**.***.*** */var/log/apache2/access.log.4*

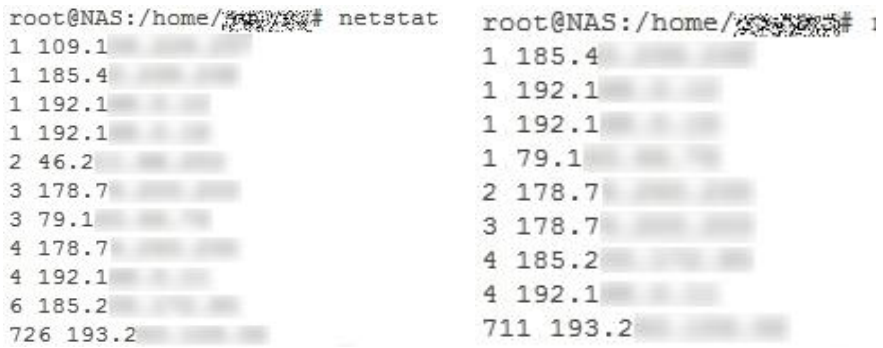

Рис. 1. Аналіз мережевої активності

Фрагмент отриманого результату наведено у лістингу 1. Зміст фрагменту свідчить про те, що запити до системи генеруються утилітою Apache Benchmark. Паралельно запускаємо програму nmap для сканування портів та визначення ОС на вузлі з якого здійснюється атака. Взагалі, після завершення атаки було знайдено 2,178 млн. рядків, які відповідають IP-адресі кіберзлочинця.

Лістинг 1.

Фрагмент log файлу доступу до веб серверу.

```
1: 193.2**.***.*** - - [16/May/2019:18:58:17 +0300] "GET / HTTP/1.1" 200 1121 "-"
2: 193.2**.***.*** - - [16/May/2019:18:58:18 +0300] "GET ..... HTTP/1.1" 200 1224
3: 193.2**.***.*** - - [16/May/2019:18:58:33 +0300] "POST / HTTP/1.1" 200 1394
4: 193.2**.***.*** - - [16/May/2019:19:02:31 +0300] "GET / HTTP/1.0" 200 1997 "-"
                "ApacheBench/2.3"
5: 193.2**.***.*** - - [16/May/2019:19:02:31 +0300] "GET / HTTP/1.0" 200 1997 "-"
                "ApacheBench/2.3"
6: 193.2**.***.*** - - [16/May/2019:19:02:34 +0300] "GET / HTTP/1.0" 200 1996 "-"
                "ApacheBench/2.3"
```

Намагаємось визначити, хто нас атакує: свій чи чужий. На користь того, що атакує свій, свідчить те, що доступ до системи реалізовано за допомогою технології *port forwarding* і відкривається виключно за необхідності. Це означає, що ризик визначення системи ботами існує, але зведений до мінімуму (значно менший), оскільки система використовується три рази на семестр. Тому відкриваємо власний журнал доступу АСКЗ і перевіряємо, чи були активні підключення з цієї IP-адреси (рис 2).

На підставі даних наведених на рис. 1, рис. 2 та лістингу 1 можна зробити висновок, що з визначеної нами IP-адреси здійснюється тестування та одночасна спроба провести DoS атаку на систему, та бачимо ПІБ ймовірного підозрюваного. Зазначимо одразу, що вважати цю особу винним в інциденті поки що зарано, бо його обліковий запис міг бути скомпрометований.

На цьому етапі інформується другий викладач, про спробу втручання в нормальну роботу системи (рис. 3). Він не був попереджений, тому невідкладно зв’язується із студентами. Підозрюваний №1 повідомляє, що не зміг пройти тест, паралельно він звинувачує в цьому іншу особу, яка автоматично стає Підозрюваним №2. Таким чином, ми маємо двох підозрюваних, кожного з яких треба максимально перевірити. Перевіряючи по

базах GEO-IP адреси підозрюваних встановлюємо, що адреси Підозрюваного №2 відносяться до однієї з мобільних мереж країни, а Підозрюваного №1 знаходиться у тому самому місті та відноситься до домену однієї з установ цього міста evilhost.example-backdoor.vn.ua.

```
MariaDB [ASTS]> SELECT DISTINCT people_id, [redacted]
+-----------+----------------+
| people_id | ip             |
+-----------+----------------+
|      1517 | 193.2[redacted] |
+-----------+----------------+
1 row in set (0.02 sec)

MariaDB [ASTS]> SELECT DISTINCT people_id,[redacted]
+-----------+----------------+------------+--------------------------+----------------+
| people_id | fname          | name       | sname                    | ip             |
+-----------+----------------+------------+--------------------------+----------------+
|      1517 | P[redacted]    | [redacted] | [redacted]               | 193.2[redacted] |
+-----------+----------------+------------+--------------------------+----------------+
1 row in set (0.01 sec)
```

Рис. 2. Аналіз сесій у АСКЗ A.S.T.S.

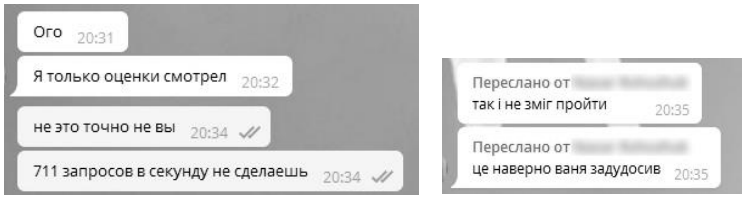

Рис. 3. Листування з колегами та студентами

Максимальну кількість інформації зібрано. Оскільки нападникам може бути відомо про те, що ми знаємо про зовнішнє втручання, блокуємо доступ до сервера і чекаємо завершення сканування портів.

Після того, як сканування системи evilhost.example-backdoor.vn.ua. завершено, приступаємо до аналізу результатів, що наведені у табл. 1.

Таблиця 1.

Порти відкриті на вузлі зловмисника.

Port	State	Service	Port	State	Service
80/tcp	open	http	14680/tcp	closed	unknown
443/tcp	open	https	15980/tcp	open	unknown
11322/tcp	open	unknown			

З наведених результатів видно, що на системі evilhost.example-backdoor.vn.ua відкриті порти 80 та 443, які за замовченням відповідають веб-серверу та протоколам HTTP та HTTPS відповідно. Після цього за допомогою браузера намагаємось з'ясувати, що саме розташовано на цьому веб-сервері, переходимо за посиланнями http://evilhost.example-backdoor.vn.ua (рис. 4) та https://evilhost.example-backdoor.vn.ua (рис. 5).

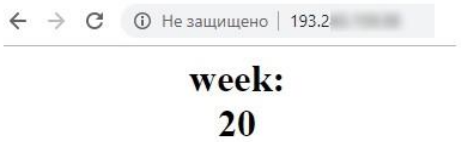

Рис. 4. Результат http запиту на вузел кіберзлочинця

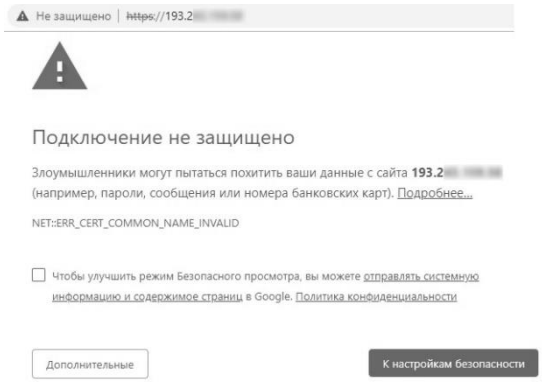

Рис. 5. Результат https запиту на вузел кіберзлочинця

Як видно з рис. 4, за першим посиланням цікава для нас інформації відсутня, а зміст сайту дуже схожий на дитячу забавку. Перехід за другим посиланням недосвідченого користувача / фахівця теж не містить цікавої інформації, але не для нас. Подібне повідомлення може виникати в тих випадках, коли сертифікат, що розташований на сервері, не призначений для цього сервера, а це для нас є дуже актуальним та цікавим, тому натискаємо кнопку «Дополнительно», після чого бачимо інформацію зображену на рис. 6. В отриманому повідомлені можна знайти адресу, для якої створювався цей сертифікат. Ця інформація для нас є дуже важливою, оскільки дозволяє продовжити пошуки.

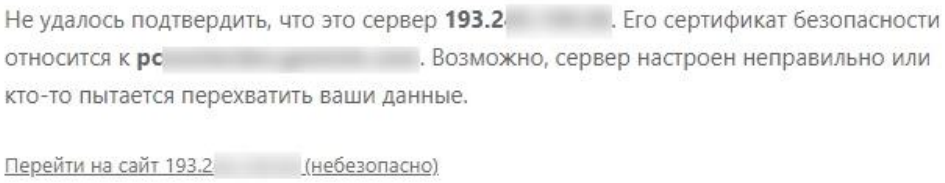

Рис. 6. Аналіз помилки пов’язаної з сертифікатом

Намагаємось перейти за новою адресою https://pcdev.evil-company.com, але все, що можна побачити – це повідомлення ***«502 Bad Gateway nginx 1.2.1»***. Ми не зупиняємось на цьому і намагаємось перейти на домен другого рівня за адресою https://evil-company.com. Нарешті ми бачимо професійно розроблений сайт однієї з міжнародних компаній з розробки програмного забезпечення, що має свій філіал у місті. На сторінці цієї компанії у соціальній мережі бачимо інформацію про її діяльність та фотографії працівників. Після 10 хвилин перегляду, знаходимо групову фотографію працівників цієї компанії (біля 40 осіб), де присутній наш Підозрюваний №1. З вірогідністю 90% відсотків можна стверджувати, що Підозрюваний №1 та невідомий кіберхуліган – це одна й та сама особа.

Слід відзначити, що Підозрюваний №1 не вважав свої дії злочином, для нього це було більше жартом або забавкою, жодних асоціацій з кримінальною або адміністративною відповідальністю в нього не виникало, хоча на відповідному навчальному курсі проблема кіберзлочинів та їх наслідків розглядалась не одноразово. Основними причинами цієї DoS атаки були цікавість та не знання матеріалу.

Таким чином, внаслідок дій нашого кіберхулігана було:

здійснено зрив тестування групи;

скомпрометовано вузел evilhost.example-backdoor.vn.ua та установу, якій належить відповідне доменне ім’я (example-backdoor.vn.ua);

скомпрометовано та завдано шкоди репутації, як філіалу так і компанії, де він працює;

скомпрометовано вузел pcdev.evil-company.com;

скомпрометовано вузел evil-company.com.

В розглянутому прикладі частину удару на систему прийняв на себе роутер, який був

відповідним чином налаштований. Кількість процесорних ресурсів, що припадала на Apache та MySQL пов'язана з науково-технічним експериментом з аналізу даних, отриманих під час тестування [11]. Не дивлячись на те, що технічно була можливість одразу припинити атаку на сервер, це не було зроблено з декількох причин:

залишався запас ресурсів (CPU, RAM);

миттєве від'єднання зловмисника могло навести його на думку, що його напад або дії викриті, і він би почав знищувати ознаки свого втручання;

збір доказів ще не було завершено.

На жаль чарівної палички, яка могла б захистити сервер на 100% для цього виду атак не існує, але протидіяти таким явищам обов'язково треба. На даний момент існує велика кількість рекомендацій з протидії різноманітним кіберзагрозам у тому числі DoS / DDoS атакам [12, 14, 13, 15, 16].

З метою запобігання подібним явищам, особливо в освітньому просторі, можна рекомендувати проведення деяких організаційних та технічних заходів, які вже оприлюднювались раніше [17, 14, 15, 16]:

1) поширення інформації про проблему кібербезпеки у суспільстві;

2) зміна законодавства, статутів та правил поведінки в організаціях та установах, тощо;

3) постійний моніторинг та аналіз кіберзагроз та ризиків;

4) підвищення кваліфікації та щорічний інструктаж IT персоналу,

5) розробка обов'язкових для всіх співробітників процедур, що будуть виконуватись для запобігання кіберзагрозам;

6) розробка процедур, що будуть виконуватись під час кібератаки усіма співробітникам підприємства / відділу;

7) своєчасне створення резервних копій коду та даних;

8) використання хмарних технологій або інших можливостей, що надаються провайдерами послуг для запобігання DoS атакам (наприклад ClaudFlare);

9) максимально можливе використання апаратного захисту на всіх рівнях;

10) правильне налаштування операційної системи для протидії атакам;

11) своєчасне та правильне налаштування кожного сервісу, що використовується;

12) створення скриптів або сценаріїв, що дозволяють реагувати на загрозу.

Зауважимо, що використання виключно хмарних технологій не може вважатись панацеєю від DoS / DDoS атаки. Якщо тарифним планом передбачено автоматичне збільшення потужностей у разі потреби, то під час атаки ці ресурси будуть використані. Сервер витримає атаку, але рахунок, який буде отримано за послуги, може вдарити по фінансах, і одразу виникає питання "Хіба не цього хотіли зловмисники?".

З особистого досвіду хотілося б додати наступні рекомендації:

1) розширення форматів наукових та фахових конференцій шляхом залучення певної кількості "не фахівців" у якості слухачів;

2) збільшення кількості різноманітних конкурсів та олімпіад з кібербезпеки та захисту інформації;

3) здійснювати щорічний детальний інструктаж студентів та викладачів, відносно правил інформаційної та кібербезпеки, з ознайомленням під розпис;

4) використання на серверах лише дійсно необхідного програмного забезпечення;

5) обережна робота з оновленнями;

6) обмеження доступу до важливих ресурсів ззовні (виключно інтранет мережа);

Зупинимось більш детально на деяких пунктах.

Щорічний інструктаж викладачів та студентів потрібен з декількох причин:

ця категорія людей складає найбільшу частку від загальної кількості, а людський фактор завжди є найбільш вразливим і потенційно небезпечним;

частина студентів ще є неповнолітніми, та навіть деякі повнолітні особи у душі ще є дітьми, тому вони дуже часто ставляться до всього, що стосується кіберпростору, як до іграшки, забавки, чогось не зовсім реального, а оскільки воно не реальне, то і за наслідки не

треба хвилюватись;

інколи викладачам стає шкода студента і вони ідуть йому назустріч, нехтуючи при цьому, правилами особистої та корпоративної кібербезпеки, можливо, навіть не усвідомлюючи це;

ці дві категорії людей мають доступ до системи з середини і випадково можуть надати третім особам інформацію про системи захисту та політики безпеки у ЗВО, або знаходити та самостійно використовувати слабкі місця у захисті.

Такий інструктаж має охоплювати усі елементи ІТ-інфраструктури навчального закладу. Наполегливо рекомендується чітко та явно зазначати які дії є забороненими для студентів/викладачів навчального закладу, наприклад:

передача логіна та пароля третій особі;

підключення особистих пристроїв до дротових мереж без згоди уповноважених ІТ фахівців;

використання різноманітних сканерів, сніферів та інших апаратно-програмних засобів у дротових та бездротових мережах;

передача інформації про ІТ-інфраструктури навчального закладу

Що стосується пункту 5, то під обережною роботою з оновленнями мається на увазі наступне:

оновлення є важливими, і у контексті даної роботи існують для того, щоб закрити певні проблеми у безпеці (і ми цього не заперечуємо);

оновлення, як і інше програмне забезпечення, також може містити проблеми з безпекою;

оновлення може з’явитись лише через декілька років або не з’явитись взагалі;

оновлення може призвести до нестабільної роботи системи взагалі або до проблеми з окремими її компонентами.

Тому, якщо у Вас є можливість, то було б доцільним мати клон реальної системи, на якому системні адміністратори мали б можливість перевіряти роботу системи з тим чи іншим оновленням, і вже після цього встановлювати його на «бойових» серверах.

Пункт 6 може здаватись дуже дивним, але, на нашу думку, він є достатньо важливим та дієвим. З одного боку сервери (назвемо їх Master), що знаходяться у внутрішній мережі, будуть недоступними ззовні, але з іншого, боку їх не можливо буде атакувати ззовні, тим самим підвищити рівень безпеки. Якщо доступ до якогось ресурсу буде потрібен ззовні необхідно буде активувати DMZ, де і будуть розташовані додаткові сервери (ESlave). Далі буде необхідно реалізувати оновлення на серверах ESlave так, щоб вони отримували лише ту інформацію з Master серверів, до якої дійсно не потрібен доступ з інтернет мережі. Наприклад, ЗВО використовує якусь АСКЗ для оцінки знань студентів, при цьому ця система розташована на одному сервері. У разі, якщо доступ до системи буде можливий з будь-якої точки світу, існує великий ризик здійснення DoS / DDoS атаки на АСКЗ під час іспиту, заліку тощо. До того ж, можливість проходити тестування без нагляду викладачів може буде логічною лише під час вивчення матеріалу та самостійної роботи над ним, складати іспит таким чином неможливо, бо не буде прозорості та об’єктивності процесу.

Так свого часу одним з авторів було розроблено декілька сценаріїв, що дозволяють певним чином реагувати на зовнішню атаку. При написанні скриптів використовувались мови програмування bash та PHP (перший варіант був написаний виключно на bash). Використання мови PHP є непринциповим її можна успішно замінити на C/C++, Python або будь-яку іншу, за необхідності. Так у лістингу 2 наведено bash скрипт, що запускається за розкладом автоматично кожні декілька хвилин та відповідає за запуск основної програми.

Лістинг 2.

DoSDetectionDemon.sh.

```
1: #!/bin/sh
2: cd /home/dDoSguard
```

```
3: php DoSDetectionDemon.php >>DoSlog.txt
```

У лістингу 3 наведено bash скрипт, що визначає кількість підключень для кожної IP-адреси, та виводить їх у порядку зменшення кількості підключень, мінімальна кількість підключень задається відповідним параметром. Скрипт, що виводить детальну інформацію про підключення для заданої IP-адреси наведено у лістингу 4.

Лістинг 3.

DoSDetectionLog.sh.

```
1: #!/bin/sh
2: LastCommand='$1>'${1}'{print $1 " " $2}'
3: netstat -ntu | awk '{print $5 $4}' | grep -vE "(Address|servers|127.0.0.1)" | cut -d: -f1 | sort | uniq -c | sort -rn| sed 's/^[ \t]*//' | awk "$LastCommand"
```

Лістинг 4.

DoSIPDetails.sh.

```
1: #!/bin/sh
2: netstat -ntu | awk '{print $5 ":" $4}' | grep $1 | cut -d: -f1,4 --output-delimiter='=>' | sort | uniq -c | sort -rn| sed 's/^[ \t]*//'
```

Принцип роботи головної програми (лістинг 5) полягає у підключенні файлу конфігурації (6), отриманні поточної дати та часу у відповідному форматі (7-8), перевірці підключень, що можуть являти собою загрозу (9) та безпосередній реакції на загрозу , якщо така існує (10-26). Реакція на загрозу являє собою форматування та запис у файли журналів інформації про мережеві аномалії (11-14) та активність процесів в операційній системі (15-17). Після цього відбувається відправлення зібраних даних на електронну пошту вказану у файлі конфігурації (18-22), виклик функції getDoSDetails та відправлення ще одного листа з більш детальною інформацією саме за цією адресою (23-26).

Лістинг 5.

DoSDetectionDemon.php.

```
1: <?php
2: /***
3: * copyright Антонов Юрий Сергеевич
4: * 2008-2019
5: */
6: include_once 'config.php';
7: $currentDate=date('Y_m_d_H_i_s');
8: $curDate=date('Y-m-d H:i:s');
9: $res=exec("./DoSDetectLog.sh $cnf['MinimalDoSLevel']}", $resData);
10: if(count($resultData)>0) {
11:    $result=implode("\n",$resData);
12:    $logFileName="${currentDate}_DoS_log.txt";
13:    $topFileName="${currentDate}_DoS_top.txt";
14:    file_put_contents($logFileName,$result);
15:    $res=exec("top -b -n 1",$topData);
16:    $result=implode("\n",$topData);
17:    file_put_contents($topFileName,$result);
18:    $command="mutt ${cnf['DefaultEmail']}";
```

```
19:    if(isset($cnf['AlternativeEmail']))
20:         $command.=" -c ${cnf['AlternativeEmail']} ";
21:    $command2=$command."-s \"DoS attack detected on
       ${cnf['ServerName']} at $curDate\" -a ${topFileName} < $logFileName";
22:    exec($command2);
23:    $ipFileName=getDoSDetails($resData,$currentDate,$cnf);
24:    $command3=$command."-s \"DoS attack details on
         ${cnf['ServerName']} at $curDate\"< $ipFileName";
25:      exec($command3);
26: }
27: function GetDoSDetails($data,$curDate,$cnf) {
28:      $ipFileName="${curDate}_DoS_IPDetails.txt";
29:      $whiteList=$cnf['WhiteList'];
30:    foreach($data as $record) {
31:      $rec=explode(" ",$record);
32:      exec("./DoSIPDetails.sh ${rec[1]}",$resData);
33:      $result=implode("\n",$resData);
34:      file_put_contents($ipFileName,$result,FILE_APPEND);
35:      if(true==$whiteList[$rec[1]]) {
36:        file_put_contents($ipFileName,"\nThe host ${rec[1]} is whitelisted, but possible host
         compromised!",FILE_APPEND);
37:        continue;  }
38:      if($rec[0]>$cnf['CriticalDoSLevel']) {
39:         $commands=['incoming'=>"${cnf['iptables']} -A INPUT -s ${rec[1]} -j DROP"
     ,'outgouing'=>"${cnf['iptables']} -A INPUT -d ${rec[1]} -j DROP"];
40:       foreach($commands as $key=>$cmd) {
41:         file_put_contents("banIP.sh",$cmd."\n", FILE_APPEND);
42:         $lastLine=system($cmd,$retVal);
43:         if(0===$retVal)
44:           $msg="\nHost ${rec[1]} banned, all $key packets will be dropped!";
45:         else $msg="\nError: host ${rec[1]} not banned, exit code$retVal!";
46:         file_put_contents($ipFileName,$msg,FILE_APPEND);}
47: } }
48:      return $ipFileName; }
```

Функція getDoSDetails (27-48) під час своєї роботи перебирає усі підозрілі адреси (30-47) формує файл журналу з детальною інформацією про підключення (32-34). Якщо поточна IP-адреса належить до “білого списку”, то робиться відповідний запис та перехід до наступної адреси (35-37), у протилежному випадку при перевищені критичного порогу підключень (38) відбувається повне блокування адреси зловмисника (39-47). У лістингу 6 можна побачити файл конфігурації для цієї програми.

Лістинг 6.

config.php.

```
1: <?php
2: /***
3: * copyright Антонов Юрий Сергеевич 2008-2019
4: */
5: $config=[  'ServerName'=>'A.S.T.S Elite-110'
6:          ,'MinimalDoSLevel'=>'10'
7:          ,'CriticalDoSLevel'=>'50'
8:          ,'DefaultEmail'=>'admin@mydomain.net'
```

```
9:      ,'AlternativeEmail'=>'support@mydomain.net'
10:     ,'iptables'=>'/sbin/iptables'
11:     ,'WhiteList'=>['192.168.0.55'=>true,'192.168.0.100'=>true] ];
```

Наведений у лістингах код був трохи змінений для збереження деяких “комерційних” таємниць, але він повністю працездатний. У тому вигляді, в якому код наведено у лістингах, йому буде важко протидіяти атакам, де використовуються такі інструменти як Slowloris або R-U-Dead-Yet. Враховуючи це можна рекомендувати здійснювати не лише аналіз мережевої активності, а й одночасний моніторинг використання таких ресурсів як процесор, оперативна пам’ять тощо. Таким чином за другорядними ознаками, можна виявляти зовнішній вплив на систему та відповідним чином реагувати на нього.

Зауважимо, що велика кількість студентів може створити ефект подібний до DoS / DDoS атаки по відношенню до викладача або ресурсу цілком законними способами. Наприклад, викладач читає лекційні заняття на декількох курсах і кількість слухачів становить від 100 до 300 осіб. Якщо усі студенти відправлять лектору 2-4 електронних листа, то йому прийдеться переглянути від 200 до 1200 електронних листів. Таке явище може трапитись само по собі. Наприклад на першому курсі, коли студенти мало обізнані та недостатньо організовані. З іншого боку якщо викладач дуже надокучив студентам під час семестру, то ніщо не заважає їм домовитись, та писати “листи щастя” викладачеві на протязі залікового тижня усім потоком. Дотримування правил етики та ввічливості у листах, завадить відмовити такому кореспондентові. У будь-якому випадку робота викладача буде паралізована (ускладнена). Єдине, що можна порадити у цій ситуації, це мати дві поштові скриньки. Першу використовувати для листування з колегами, наукової діяльності, тощо. Другу виключно для роботи зі студентами. Аналогічним чином, якщо 5000 студентів відвідують сайт і оновлюють сторінку 5 разів на хвилину, то у в результаті отримаємо 25 тис. запитів на хвилину. При цьому жодних протизаконних дій ніхто не здійснює.

Висновки

Як показали дослідження, ймовірність кібератак навчальних ресурсів з боку студентів дійсно існує та не може ігноруватись. Забезпечення якісного захисту у першу чергу має починатись зі зміни світогляду, відповідального ставлення до рекомендацій з підвищення захисту комп’ютерних систем, запобігання та протидії різного роду атакам, використання усіх наявних організаційних, програмних та апаратних засобів. Також слід враховувати, що як студенти, так і викладачі мають інформацію, яка може бути дуже цікавою для кіберзлочинців.

Перелік посилань

1. Смит П. Оптимизация и защита Linux-сервера своими руками / П. Смит. – СПб.: Наука и Техника, 2006. – 576 с.

2. Купреев О. DDoS-атаки в третьем квартале 2018 года [Електронный ресурс] / О. Купреев, Е. Бадовская, А. Гутников // - Режим доступа: https://securelist.ru/dDoS-report-in-q3-2018/92512/ (28.07.2019)

3. Студент устроил DDoS-атаку на школьную систему в США [Електронный ресурс] // - Режим доступа: https://threatpost.ru/student-ustroil-dDoS-ataku-na-shkolnuyu-sistemu-v-ssha/8504/ (23.08.2019)

4. DDoS во время экзаменационной сессии [Електронный ресурс] // - Режим доступа: https://threatpost.ru/dDoS_vo_vremja_ekzamenatsionnoj_sessii/8466/ (23.08.2019)

5. DDoS attack downs University of London learning platform [Електронный ресурс] // - Режим доступа: https://www.theregister.co.uk/2015/05/22/university_of_london_dDoS_attack (23.08.2019)

6. DoS-атака на сервер [Електронный ресурс] // - Режим доступа: https://i-exam.ru/node/542 (23.08.2019)

7. SAM COOK DDoS attack statistics and facts for 2018-2019 [Електронный ресурс] // - Режим доступа: https://www.comparitech.com/blog/information-security/dDoS-statistics-facts/ (23.08.2019)

8. Актуальные киберугрозы — 2018. Тренды и прогнозы Дата публикации 12 марта 2019 [Електронный ресурс] // - Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2018/ (23.08.2019)

9. Купреев О. DDoS-атаки во втором квартале 2019 года [Електронный ресурс] О. Купреев, Е. Бадовская, А. Гутников // - Режим доступа: https://securelist.ru/dDoS-report-q2-2019/94452/ (23.08.2019)

10. Гресько А.О. Загальний комплексний опис проблем інформаційної безпеки в "Інтернеті речей" / А.О. Гресько, Ю.М. Щебланін // Сучасний захист інформації. - 2016. - № 1. - с. 69-73.

11. Антонов Ю.С. Оцінка повноти відповідей в автоматизованих системах контролю знань / Ю.С. Антонов // Наукові праці Донецького національного технічного університету. Сер.: Інформатика, кібернетика та обчислювальна техніка. - 2012. - № 15. - С.113-117.

12. Смоктій О.Д. Анализ механизма и последствий воздействия DDoS-атак на эталонную модель взаимодействия открытых систем OSI / О.Д. Смоктій, К.В. Смоктій, О.В. Іванченко // Системи управління, навігації та зв'язку. - 2017. - № 1. - с.33-37.

13. Види DDoS-атак та алгоритм виявлення DDoS-атак типу flood-attack / [Н.В. Багнюк, В.М. Мельник, О.В. Клеха, І.А. Невідомський] // Комп'ютерно-інтегровані технології: освіта, наука, виробництво. - 2015. - № 18. - С.6-12.

14. Защита от DDoS атак своими руками [Електронный ресурс] // - Режим доступа: https://geekelectronics.org/linux/zashhita-ot-dDoS-atak-svoimi-rukami.html (23.08.2019)

15. Борсуковський Ю.В. Базові напрямки забезпечення кібербезпеки державного та приватного секторів / Ю.В. Борсуковський, В.Л. Бурячок, В.Ю. Борсуковська // Сучасний захист інформації. - 2017. - № 2. - с.85-89.

16. Ільїн О.О. Аналіз уразливості інформаційного ресурсу вищого навчального закладу та класифікація загроз інформаційної безпеки / О.О. Ільїн, С.О. Сєрих, В.В. Вишнівський // Сучасний захист інформації. - 2017. - № 1. - с.66—72.

17. Плахтий М. Как пережить DDoS-атаку — опыт и советы билетного оператора Karabas.com [Електронный ресурс] / М. Плахтий // - Режим доступа: https://ain.ua/2019/04/08/karabas-protiv-dDoS-kolonka/ (23.08.2019)

Надійшла: 21.10.2019 Рецензент: д.т.н., доцент Гайдур Г.І.