Краснобрижий І.В.
кандидат юридичних наук
(Дніпропетровський державний університет внутрішніх справ)

УДК 62-52

ПРАКТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ ВИЯВЛЕННЯ ТА БОРОТЬБИ З DoS ТА DDoS-АТАКАМИ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ ПОРУШЕННЯ НОРМАЛЬНОГО ФУНКЦІОНУВАННЯ ДЕРЖАВНИХ КОНТЕНТІВ

Розглянуто питання пошуку методики виявлення та боротьби з Dos, DDos-атаками, які використовуються для порушення нормального функціонування державних контентів у мережах Internet, Ethernet.

***Ключові слова**: контент, Dos, DDos, сервіси, міжмережеві екрани, сервер, TCP/IP, трафік, порт, IPMP, UDP, PING-пакет, HTTP.*

Постановка проблеми. Вже три роки триває антитерористична операція на Сході України, однією із складових частин якої є ведення так званої «інформаційної війни» з боку країни-агресора – Російської Федерації, що потребує активізації діяльності держави у напрямку розробки концептуальних засад забезпечення кібернетичної безпеки, визначення алгоритму здійснення заходів з метою захисту вітчизняного кібернетичного простору.

За таких умов формування і безперебійне функціонування національних інформаційних ресурсів є однією з ключових проблем становлення та розвитку національного інформаційного простору України [1, с. 94]. Загальновідомо, що саме інформаційні ресурси є важливою складовою стратегічних ресурсів держави, значення якої зростає із розвитком інформаційно-комунікаційних технологій та їх використанням в усіх сферах суспільного життя. Саме тому ефективний захист державних інформаційних ресурсів є важливою умовою забезпечення кібернетичної безпеки та реалізації виваженої державної політики у сфері інформатизації.

Численні атаки на державні інформаційні ресурси з боку російських мережевих сегментів, внаслідок яких інформаційні ресурси стають недоступними цільовим користувачам, надають підстави стверджувати, що існуюча система державного управління кібернетичною безпекою має певні недоліки, не спроможна своєчасно реагувати на кіберзагрози, працювати на упередження мережевих кібернетичних атак на вітчизняний кібернетичний простір, особливо в умовах «гібридної» війни з РФ, і потребує оптимізації.

Аналіз публікацій, в яких започатковано розв'язання даної пробле-

ми. Дослідження проблем забезпечення інформаційної безпеки держави досліджували: А. Марущак, В. Панченко, В. Петрик, В. Ліпкан та інші фахівці. Проблемні питання забезпечення кібернетичної безпеки розглядали у своїх працях: В. Бурячок, А. Бабенко, В. Бутузов, В. Гавловский, В. Голубєв, С. Гнатюк, Д. Дубов, О. Корченко, В. Номоконов, В. Петров, І. Рязанцева, В. Тулупов, В. Шеломенцев. Висвітлення проблемних питань підготовки фахівців у сфері забезпечення кібербезпеки певною мірою здійснювали: О. Баранов, В. Богуш, Ю. Онищенко, О. Орлов та ін.

Мета даної статті полягає у поширенні інформації про реальні практичні методики виявлення та боротьби з Dos, DDos-атаками, які використовуються для порушення нормального функціонування державних контентів у мережах Internet, Ethernet, серед співробітників інформаційно-технічних державних структурних підрозділів, діяльність яких направлена на захист вищевказаних контентів.

Виклад основного матеріалу. DoS-атака (від англ. Denial of Service – відмова в обслуговуванні) і DDoS-атака (від англ. Distributed Denial of Service – розподілена атака типу «відмова в обслуговуванні») – атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких легітимні (правомірні) користувачі системи не можуть одержати доступ до надаваних системою ресурсів, або цей доступ стає ускладненим.

Небезпека більшості Dos та DDoS-атак – у їхній абсолютній прозорості й «нормальності», тому що помилка у програмному забезпеченні завжди може бути виправлена, то повне вичерпання ресурсів – явище майже повсякденне. З ними зіштовхуються багато адміністраторів, коли ресурсів машини (ширини каналу) стає недостатньо, або web-сайт піддається слешдот-ефекту (потужному сплеску відвідуваності веб-сайту) – як приклад можна навести випадок із сайтом twitter.com, що став недоступним уже через кілька хвилин після першої звістки про смерть Майкла Джексона. І якщо різати трафік і ресурси для усіх підряд, то врятуєшся від DDoS, але втратиш добру половину клієнтів [2].

Виходу із цієї ситуації фактично немає, однак наслідки DDoS-атак і їхню ефективність можна істотно знизити за рахунок правильного настроювання маршрутизатора, брандмауера й постійного аналізу аномалій у мережевому трафіку. Виходячи із цього, нижче ми послідовно розглянемо:

1) методи боротьби з конкретними типами DDoS-атак;

2) універсальні поради, які допоможуть підготуватися до DoS-атаки й знизити її ефективність;

3) способи розпізнавання початку DDoS-атаки;

4) що необхідно робити, коли почалася DDoS-атака.

1. Отже, існує два типи DoS, DDoS-атак, і найпоширеніша з них заснована на ідеї флуда (flood – повінь, англ.), тобто завалювання жертви величезною кількістю пакетів. Флуд буває різним: ICMP-flood, SYN-flood, UDP-flood і HTTP-flood. Сучасні DoS-боти можуть використовувати усі ці види атак одночасно, тому варто заздалегідь подбати про адекватний захист від кожної з

них.

ICMP-flood

Дуже примітивний метод забивання смуги пропущення й створення навантажень на мережевий стек через монотонну посилку запитів ICMP ECHO (ping). Легко виявляється за допомогою аналізу потоків трафіка в обидва боки: під час атаки типу ICMP-flood вони практично ідентичні. Майже безболісний спосіб абсолютного захисту заснований на відключенні відповідей на запити ICMP ECHO:

```
# sysctl net.ipv4.icmp_echo_ignore_all=1
```

або за допомогою брандмауера:

```
# iptables -A INPUT -p icmp -j DROP ---i icmp-type 8
```

SYN-flood

Один із розповсюджених способів не тільки забити канал зв'язку, але й увести мережевий стек операційної системи в такий стан, коли він уже не зможе приймати нові запити на підключення. SYN-flood заснований на спробі ініціалізації великого числа одночасних TCP-з'єднань через посилку SYN-пакета з неіснуючою зворотною адресою. Після декількох спроб відіслати відповідний ACK-пакет на недоступну адресу більшість операційних систем ставлять невстановлене з'єднання в чергу. І тільки після n-ої спроби закривають з'єднання. Тому що потік ACK-пакетів дуже великий, незабаром виявляється, що черга є заповненою і ядро дає відмову на спроби відкрити нове з'єднання. Найбільш розумні DoS-боти ще й аналізують систему перед початком атаки, щоб слати запити тільки на відкриті життєво важливі порти. Ідентифікувати таку атаку просто: досить спробувати підключитися до одного із сервісів [3, с. 104]. Оборонні заходи звичайно містять у собі:

Збільшення черги «напіввідчинених» TCP-з'єднань:

```
# sysctl -w net.ipv4.tcp_max_syn_backlog=1024
```

Зменшення часу втримання «напіввідчинених» з'єднань:

```
# sysctl -w net.ipv4.tcp_synack_retries=1
```

Включення механізму TCP syncookies:

```
# sysctl -w net.ipv4.tcp_syncookies=1
```

Обмеження максимального числа «напіввідчинених» з'єднань із одного IP до конкретного порту:

```
# iptables -I INPUT -p tcp ---isyn ---idport 80 -m iplimit ---i iplimit-above 10 -j DROP
```

UDP-flood

Типовий метод захаращення смуги пропущення. UDP-flood заснований на нескінченній посилці UDP-пакетів на порти різних UDP-сервісів. Легко усувається за рахунок відрізання таких сервісів від зовнішнього світу й установки ліміту на кількість з'єднань в одиницю часу до DNS-сервера на стороні шлюзу:

```
# iptables -I INPUT -p udp ---idport 53 -j DROP -m iplimit ---i iplimit-above 1
```

HTTP-flood

Один з найпоширеніших на сьогодні способів флуда. HTTP-flood заснований на нескінченній посилці HTTP-повідомлень GET на 80-й порт із метою завантажити web-сервер настільки, щоб він не зміг обробляти усі інші запити. Часто метою флуда стає не корінь web-сервера, а один зі скриптів, що виконує ресурсномісткі завдання або працюючий з базою даних. У кожному разі індикатором атаки, що почалася, буде слугувати аномально швидке зростання логов web-сервера.

Методи боротьби з HTTP-flood-ом містять у собі тюнінг (відновлення) web-сервера й бази даних з метою знизити ефект від атаки, а також відсіювання DoS-ботів за допомогою різних прийомів. По-перше, варто збільшити максимальне число конектів (підключень) до бази даних одночасно. По-друге, установити перед web-сервером Apache легкий і продуктивний nginx (HTTP-сервер, почтовий і зворотний прокси-сервер, працюючий на Unix-подібних операційних системах) – він буде кешувати запити й віддавати статику. Це рішення зі списку "must have" (повинне бути – англ.), що не тільки знизить ефект DoS-атак, але й дозволить серверу витримати величезні навантаження. Невеликий приклад:

```
# vi /etc/nginx/nginx.conf
# Збільшуємо максимальну кількість використовуваних файлів
worker_rlimit_nofile 80000;
events {
# Збільшуємо максимальну кількість з'єднань
worker_connections 65536;
# Використовуємо ефективний метод epoll для обробки з'єднань
use epoll;
}
http {
gzip off;
# Відключаємо таймаут на закриття keep-alive з'єднань
keepalive_timeout 0;
# Не віддавати версію nginx у заголовку відповіді
server_tokens off;
# Скидати з'єднання по таймауту
reset_timedout_connection on;
}
# Стандартні настроювання для роботи в якості проксі
server {
listen 111.111.111.111 default deferred;
```

```
server_name host.com www.host.com;
log_format IP $remote_addr;
location / {
proxy_pass http://127.0.0.1/;
}
location ~* \.(jpeg|jpg|gif|png|css|js|pdf|txt|tar)$ {
root /home/www/host.com/httpdocs;
}
}
```

Якщо буде потреба, можна задіяти nginx-модуль ngx_http_limit_req_module, що обмежує кількість одночасних підключень із однієї адреси. Ресурсномісткі скрипти можна захистити від ботів за допомогою затримок, кнопок «натисни мене», виставляння кукісов і інших прийомів, спрямованих на перевірку «людяності».

2. Універсальні поради:

Щоб не потрапити в безвихідне становище під час обвалення DDoS-шторму на системи, необхідно ретельним чином підготувати їх до такої ситуації:

- усі сервери, що мають прямий доступ у зовнішню мережу, повинні бути підготовлені до простого й швидкого віддаленого ребуту (reboot – перезавантаження, англ.), використовуючи сервіс sshd. Великим плюсом буде наявність другого, адміністративного, мережевого інтерфейсу, через який можна одержати доступ до сервера у випадку переповнення основного каналу;

- програмне забезпечення, використовуване на сервері, завжди повинно перебувати в актуальному стані. Всі дірки – пропатчено, відновлення встановлено (проста порада, якою багато нехтують). Це захистить нас від DoS-атак, що експлуатують баги (помилки) у сервісах;

- усі слухаючі мережеві сервіси, призначені для адміністративного використання, повинні бути блоковані брандмауером від усіх, хто не повинен мати до них доступ. Тоді атакуючий не зможе використовувати їх для проведення DoS-атаки або брутфорса (brute force – груба сила, англ.);

- на підходах до сервера (найближчому маршрутизаторі) повинна бути встановлена система аналізу трафіка (наприклад – NetFlow), що дозволить вчасно довідатися про атаку, що починається, і вчасно вжити заходів по її запобіганню.

Також бажано додати в /etc/sysctl.conf такі рядки:

```
# vi /etc/sysctl.conf
 # Захист від спуфинга
net.ipv4.conf.default.rp_filter = 1
# Перевіряти TCP-з'єднання щохвилини. Якщо на іншій стороні – легальна
```

```
машина, вона відразу відповість. Дефолтове значення – 2 години.
net.ipv4.tcp_keepalive_time = 60
# Повторити спробу через десять секунд
net.ipv4.tcp_keepalive_intvl = 10
# Кількість перевірок перед закриттям з'єднання
net.ipv4.tcp_keepalive_probes = 5
```

Слід зазначити, що усі наведені прийоми спрямовані на зниження ефективності DDoS-атак, що ставлять своєю метою витрату ресурсів машини. Від флуда, що забиває канал сміттям, захиститися практично неможливо, і єдино правильний, але не завжди можливий спосіб боротьби полягає у тому, щоб «позбавити атаку сенсу». Якщо ми одержимо у своє розпорядження дійсно широкий канал, що легко пропустить трафік невеликого ботнета, вважайте що від 90 % атак наш сервер захищений. Є більш витончений спосіб захисту. Він заснований на організації розподіленої обчислювальної мережі, що включає в себе безліч дублюючих серверів, які підключені до різних магістральних каналів. Коли обчислювальні потужності або пропускна здатність каналу закінчуються, усі нові клієнти перенаправляються на інший сервер (або поступово "розмазуються" по серверах за принципом round-robin – алгоритм вирівнювання навантаження розподіленої обчислювальної системи методом перебору її елементів по круговому циклу). Це неймовірно дорога, але дуже стійка структура, ефективно атакувати яку практично неможливо.

Інше більш-менш ефективне рішення полягає в покупці дорогих систем Cisco Traffic Anomaly Detector і Cisco Guard. Працюючи у зв'язці, вони можуть придушити атаку, що починається, але як і більшість інших рішень, заснованих на навчанні й аналізі становищ, дають збої. Тому варто гарненько подумати перед тим, як витрачати сотні тисяч гривень на такий захист.

3. Способи розпізнавання початку DDoS-атаки.

Перед безпосереднім початком атаки боти «розігріваються», поступово нарощуючи потік пакетів на сервер, що атакується. Важливо піймати момент і почати активні дії. Допоможе в цьому постійне спостереження за маршрутизатором, підключеним до зовнішньої мережі (аналіз графіків NetFlow). На сервері-жертві визначити початок атаки можна підручними засобами.

Наявність SYN-flood-а встановлюється легко – через підрахунок числа "напіввідчинених" TCP-з'єднань:

```
# netstat -na | grep ":80\ " | grep SYN_RCVD
```

У звичайній ситуації їх не повинно бути зовсім (або дуже невелика кількість: максимум 1–3). Якщо це не так – ти атакований, терміново переходь до блокування атакуючих.

З HTTP-flood-ом трохи складніше. Для початку потрібно підрахувати кількість процесів Apache і кількість з’єднань на 80-й порт (HTTP-flood):

```
# ps aux | grep httpd | wc -l
# netstat -na | grep ":80\ " | wc -l
```

Значення, що у кілька разів перевищують середньостатистичні, дають підстави замислитися. Далі варто переглянути список IP-адрес, з яких ідуть запити на підключення:

```
# netstat -na | grep ":80\ " | sort | uniq -c | sort -nr | less
```

Однозначно ідентифікувати DoS-атаку не можна, можливо лише підтвердити свої здогади про її наявність – якщо одна адреса повторюється в списку занадто багато разів (та й то, це може говорити про відвідувачів, що сидять за NAT'ом). Додатковим підтвердженням буде аналіз пакетів за допомогою tcpdump:

```
# tcpdump -n -i eth0 -s 0 -w output.txt dst port 80 and host IP-Сервера
```

Показником слугує великий потік одноманітних (які не містять корисної інформації) пакетів від різних IP, спрямованих на один порт/сервіс (наприклад, корінь web-сервера або певний cgi-скрипт).

4. Що необхідно робити, коли почалася DDoS-атака.

Остаточно визначившись, починаємо блокувати непрошених по IP-адресах (буде набагато більше ефекту, якщо ми зробимо це на маршрутизаторі):

```
# iptables -A INPUT -s xxx.xxx.xxx.xxx -p tcp ---i destination-port http -j DROP
```

Або відразу по підмережах:

```
# iptables -A INPUT -s xxx.xxx.0.0/16 -p tcp ---i destination-port http -j DROP
```

Це дасть нам деяку фору (зовсім маленьку, найчастіше IP-адреса джерела зміниться), яку ми повинні використати для того, щоб звернутися до провайдера/хостера (із прикладеними до повідомлення логами web-сервера, ядра, брандмауера й списком виявлених нами IP-адрес). Більшість із них, звичайно, проігнорують це повідомлення (а хостинги з оплатою трафіка ще й порадіють – DoS-атака принесе їм прибуток) або просто відключать наш сервер. Але в кожному разі це варто зробити обов'язково, – ефективний захист від DDoS можливий тільки на магістральних каналах. Поодинці ми впораємося із дрібними нападками, спрямованими на виснаження ресурсів сервера, але опинимося беззахисними перед більш-менш серйозним DDoS-ом.

На сьогоднішній момент велику популярність має використання на серверах операційної системи FreeBSD [4, с. 91]. У зв'язку із чим пропонуємо деякі прийоми настроювання цієї системи для збільшення стійкості її до DoS, DDoS атак:

Зменшуємо час очікування відповідного пакета на запит SYN-ACK (захист від SYN-flood):

```
# sysctl net.inet.tcp.msl=7500
```

Перетворюємо сервер у чорну діру. Так ядро не буде слати відповідні пакети при спробі підключитися до незайнятих портів (знижує навантаження на машину під час DDoS-а на випадкові порти):

```
# sysctl net.inet.tcp.blackhole=2  # sysctl net.inet.udp.blackhole=1
```

Обмежуємо число відповідей на ICMP-Повідомлення 50-ю в секунду (захист від ICMP-flood):

```
# net.inet.icmp.icmplim=50
```

Збільшуємо максимальну кількість підключень до сервера (захист від усіх видів DDoS):

```
# sysctl kern.ipc.somaxconn=32768
```

Включаємо DEVICE_POLLING – самостійне опитування мережевого драйвера ядром на високих навантаженнях (істотно знижує навантаження на систему під час DDoS-а):

- Перезбираємо ядро з опцією «options DEVICE_POLLING»;
- Активуємо механізм поллінга: «sysctl kern.polling.enable=1»;
- Додаємо запис «kern.polling.enable=1» в /etc/sysctl.conf.

Висновок. Наведені практичні методики виявлення та протидії DoS та DDoS-атакам є загальними, але разом з тим дуже ефективними та можуть бути використані державними адміністраторами навіть середнього рівня підготовки. Використання цих шаблонів настроювання операційних систем значно знизить імовірність несанкціонованого втручання в нормальне функціонування державних автоматизованих систем, на яких знаходяться різноманітні інформаційні контенти. Але разом з цим слід зазначити гостру необхідність поліпшення контролю за кібернетичним простором України з боку державних організацій, функція яких полягає в тому числі й у слідкуванні за інформаційною безпекою. Доцільно, на нашу думку, створити державний підрозділ, функція якого полягала б у проведенні постійного інформаційного аудиту захищеності державних автоматизованих систем.

Бібліографічні посилання

1. Нестеряк Ю.В. Державна інформаційна політика та управління національними інформаційними ресурсами / Ю.В. Нестеряк // Державне управління та місцеве самоврядування : зб. наук. праць. – Дніпропетровськ; ДРІДУ НАДУ. – 2013. – Вип. 1(16). – С. 94–104

2. Савин Л.В. Сетецентричная и сетевая война. Введение в концепцию / Л.В. Савин. – М. : Евразийское движение, 2011.

3. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / Бурячок В.Л. // Сучасна спеціальна техніка. – 2011. – № 3 (26). – С. 104–114.

4. Панченко В.М. Зарубіжний досвід формування систем захисту критичної інфраструктури від кіберзагроз / Панченко В.М. // Інформаційна безпека людини, суспільства, держави. – 2012. – № 3 (10). – С. 91.

Краснобрыжий И.В. Практические аспекты организации выявления и борьбы с Dos и DDoS-атаками, которые используются для нарушения нормального функционирования государственных контентов. Рассмотрены вопросы поиска методики выявления и борьбы с Dos, DDos-атаками, которые используются для нарушения нормального функционирования государственных контентов в сетях Internet, Ethernet.

Ключевые слова: *контент, Dos, DDos, сервисы, межсетевые экраны, сервер, TCP/IP, трафик, порт, IPMP, UDP, PING-пакет, HTTP.*

Krasnobryzhyy I.V. Practical aspects of detection and fight DoS and DDoS attacks are used to affect normal functioning of the state contents. The article deals with the question of finding methods of detection and fight against Dos, DDos attacks used to disruption of normal functioning of public content networks Internet, Ethernet. This requires the activation of the state towards the development of conceptual basis to ensure cyber security, the definition of the algorithm of measures implementation to protect national cyber space. The author pays attention to the need of state information resources protection by creation a governmental unit the function of which is to hold regular information security audits of state automated systems.

Keywords*: content, Dos, DDos, services, firewalls, server, TCP / IP, traffic, port, IPMP, UDP, PING-pack, HTTP.*

Надійшла до редакції 12.10.2016

Плетенець В.М.
кандидат юридичних наук, доцент
(*Дніпропетровський державний університет внутрішніх справ)*

УДК 343.98

ОСОБЛИВОСТІ ВСТАНОВЛЕННЯ ПСИХОЛОГІЧНОГО КОНТАКТУ ПРИ ДОПИТАХ ЗА УЧАСТЮ ЗАХИСНИКА

Розглянуто організаційно-тактичні особливості встановлення психологічного контакту при проведенні допитів, в яких бере участь захисник. Зосереджено увагу на факторах, які позитивно впливають на встановлення психологічного контакту.

Ключові слова: *допит, слідча (розшукова) дія, психологічний контакт. тактичний прийом, розслідування, захисник.*

Постановка проблеми. Встановленню психологічного контакту з різними категоріями осіб при проведенні їх допитів приділяло увагу багато вчених. У той же час поза увагою залишилися особливості встановлення психологічного контакту з допитуваним за участі захисника. У практичній діяльності дана проблема вирішення так і не набула. Це обумовлює необхідність приділення цьому питанню окремої уваги з боку науковців.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. Проблемам встановлення психологічного контакту при проведенні допиту приділяли увагу: В. П. Бахін, Р. С. Бєлкін, В.Д. Берназ, О.М. Васильєв,