ПРИЛОЖЕНИЕ НА КИБЕРАТАКАТА С ОТКАЗ НА УСЛУГИ DOS (DENIAL OF SERVICE) СРЕЩУ ИНФОРМАЦИОННИТЕ РЕСУРСИ НА НАЦИОНАЛНИ ДЪРЖАВНИ АГЕНЦИИ И АКАДЕМИЧНИ ИНСТИТУЦИИ

Илин САВОВ*
Петър БОЯНОВ**

In this paper an implementation of the Denial of Service (DoS) cyber attack Against the National Cyber Security System is made.

Въведение

Кибератаката с отказ на услуги DoS (Denial of Service) се характеризира с това, че е атака, изцяло насочена към компютърна машина или компютърна мрежа с цел намаляване на производителността или изцяло блокиране на работата на компютърната машина. По този начин тези кибератаки предотвратяват възможността на оторизирани и легитимни потребители да си получат достъпа до компютъра или компютърната мрежа. Симптомите на кибератаките с отказ на услуги са свързани с невъзможност за достъп до определен уебсайт или всички определени уебсайтове, увеличаване на количеството на получените фалшиви електронни писма и прекалено бавна мрежова производителност [1; 2: 249 – 259; 4; 6: 465; 7: 34 – 41; 8: 1 – 6].

* Авторът е професор, доктор, декан на Учебно-научен център „Национална сигурност и обществен ред“ във Висше училище по сигурност и икономика – Пловдив.
** Авторът е доцент, доктор, инженер в Шуменски университет „Епископ Константин Преславски“.

Изложение

Повечето киберпрестъпници прилагат кибератака с разпределен отказ на услуги DDoS (Distributed Denial of Service), която използва голям брой от компрометирани хостове (зомбита), на които им е наредено да атакуват отдалечената компютърна машина на жертвата [2: 249 – 259; 3: 36 – 47; 4; 5: 414; 6: 465; 9: 104 – 111; 13: 1 – 22, 1 – 52; 14: 1 – 22; 15]. Кибератаките с отказ на услуги се разделят на:

- кибератаки, насочени към ширината на честотната лента;
- кибератаки с наводняване със заявки към системни услуги;
- кибератаки с изпращане пакети с активиран флаг „SYN“;
- кибератаки с наводняване на ICMP протокола;
- кибератаки към клиенти с равноправен достъп и др.

След като киберпрестъпникът осъществи тази атака, тогава последиците за организацията могат да бъдат следните:

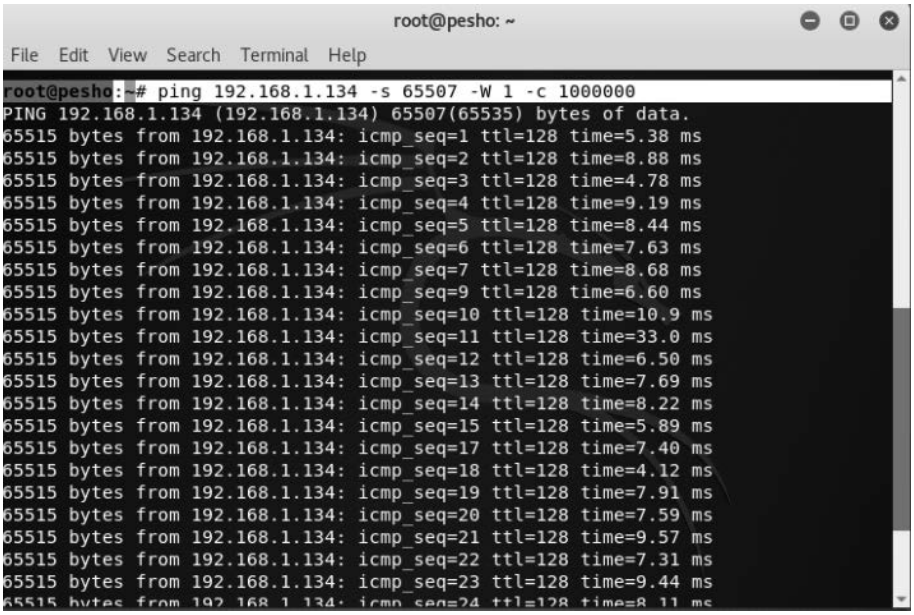
- причиняване на големи финансови загуби;
- изцяло спиране или блокиране на интернет връзката на организацията;
- изцяло изолиране на организацията от интернет пространството [9: 104 – 111; 10: 72 – 79; 11: 18 – 23; 12: 58 – 64; 16: 302; 17: 359; 18: 1 – 12].

Наводняването с изпращане на безброй много ICMP заявки е една от най-сериозните кибератаки от тип отказ на услуги. На *Фигура 1* е показана кибератаката с наводняване с безброй много заявки с протокола ICMP. Тази атака е известна още с името „ping на смъртта“. Параметрите на кибератака са конфигурирани по следния начин:

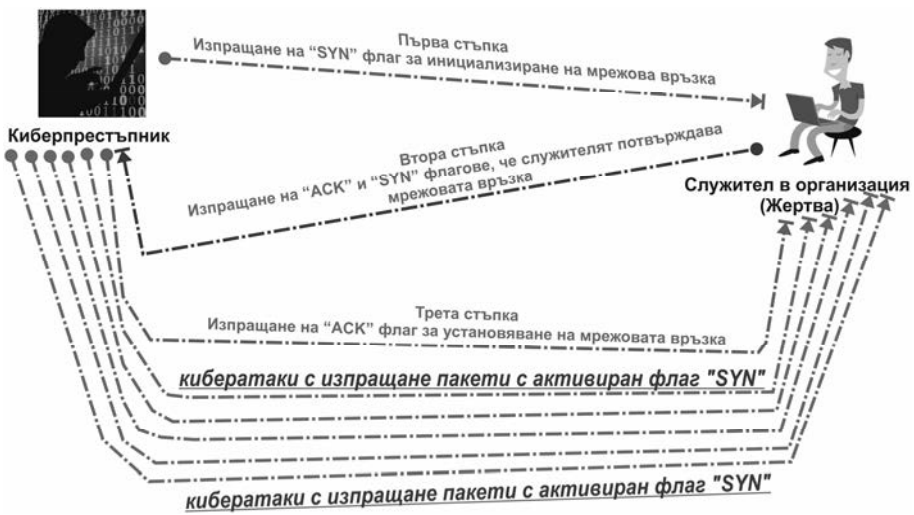
- IPv4 адрес на компютърната жертва – 192.168.1.134;
- размер на всеки пакет – 65 507 байта;
- време на изчакване на заявките – до 1 милисекунда;
- общ брой на заявките, които трябва да бъдат изпратени – 1 000 000. Атаката е стартирана под Linux базирана операционна система.

Последиците, които могат да доведат в компютърната машина на жертвата, са блокиране на мрежовата карта и необходимо рестартиране на цялата компютърна машина. Ако тази атака се прави изключително често, е възможно да доведе до пълно блокиране на мрежовата карта [1; 2: 249 – 259; 4; 5: 414; 6: 465; 7: 34 – 41; 8: 1 – 6; 9: 104 – 111].

Фигура 1. ***Стартиране на кибератаката „ping на смъртта“***



Фигура 2. ***Кибератаки с изпращане на пакети с активиран флаг „SYN“***



Кибератаки с изпращане на пакети с активиран флаг „SYN“ целят да препълнят мрежовия буфер с мрежови пакети с активиран флаг „SYN“. Това означава, че процесът на трипътно ръкостискане по TCP протокола е завършено, но киберпрестъпникът продължава да изпраща пакети с активен синхронизиращ флаг към машината жертва. Ако тази атака се съчетае с изпращане на безброй много заявки по ICMP протокола, тогава машината жертва може да се блокира още бързо. Това е показано на *Фигура 2.*

В компютърното пространство едни от най-зловредните софтуерни програми, които се използват за осъществяване на кибератаките от тип отказ на услуги, са:

- Sprut
- DoS HTTP
- PHP DoS
- Janidos
- Supernove
- BanglaDoS.

Забележка: *Всичките експерименти и изследвания в тази статия са направени в специализирани компютърни лаборатории в Шуменския университет „Епископ Константин Преславски“ и във Висшето училище по сигурност и икономика – Пловдив. Всичко илюстрирано и обяснено в тази статия е с научноизследователска цел и авторите не носят отговорност в случаи на злоупотреба с него.*

Чл. 319а. (Нов – ДВ, бр. 92 от 2002 г.) (1) (Изм. – ДВ, бр. 38 от 2007 г.) „Който копира, използва или осъществи достъп до компютърни данни в компютърна система без разрешение, когато се изисква такова, се наказва с глоба до три хиляди лева.“ // Наказателен кодекс, чл. 319а. (Нов – ДВ, бр. 92 от 2002 г.) (1) (Изм. – ДВ, бр. 38 от 2007 г.).

Заключение

Служителите по сигурността на автоматизираните информационни системи и мрежи (АИС/М), както и администраторът по сигурността трябва да предприемат и направят следните защитни действия:

- изключване на всички ненужни системни услуги от операционната система;
- деинсталиране на всички неизползваеми софтуерни програми;
- сканиране на файлове, получени от външни източници на организацията;

• конфигуриране на няколко защитни стени в демилитаризираната зона (фермата със сървъри) на организацията и конфигуриране на няколко системи за откриване на проникванията след демилитаризираната зона;

• използване на специални софтуерни анализатори за откриване на уязвимости и слабости в конфигурацията и настройките на операционната система на служителя.

Също трябва да се сканира и мрежовата операционна система на маршрутизаторите в организацията. Най-полезните анализатори, които могат да се използват, са:

• Advanced Mail Bomber
• Apache JMeter
• GFI LanGuard
• Mail Bomber
• Nessus
• Nmap
• Webserver Stress Tool и др.

Литература

1. **Боянов,** П. Кибератаки и противодействие. Монография. Шумен: Епископ Константин Преславски, 2017. ISBN 978-619-201-206-9.

2. **Савов,** И. Относно някои аспекти от процедурите по използване на трафичните данни в Република България и някои европейски страни. – В: *Международна* конференция „Противодействие на радикализацията и тероризма“, Академия на МВР, април 2017 г. ISBN 978-954-348-145-3.

3. **Савов,** И. Един поглед върху същността на киберпрестъплението. – В: *Политика* и сигурност, ВУСИ, 2017. ISSN 2535-0358.

4. **Досев,** Н., Г. Томов. Кибертероризъм и противодействие. Учебник за дистанционно обучение. Велико Търново: Национален военен университет „Васил Левски“, 2014. ISBN 978-954-753-207-6.

5. **Allen,** L. Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide. Birmingham, UK: Packt Publishing, 2012. ISBN 978-1-84951-774-4.

6. **Bodmer,** S., M. Kilger, Gr. Carpenter, J. Jones. Reverse Deception: Organized Cyber Threat Counter-Exploitation. McGraw-Hill Education, 2012. ISBN 978-0-07-177250-1.

7. **Boyanov,** P. Educational exploiting the information resources and invading the security mechanisms of the operating system Windows 7 with the exploit Eternalblue and Backdoor Doublepulsar. – In: *Scientific* and Applied Research, Konstantin Preslavsky University Press, Vol. 14, 2018. ISSN 1314-6289. [online]. *http://www.rst-tto.com/publication.html.*

8. **Hristov,** H. Scanning for vulnerabilities in the security mechanisms of the hosts in the academic institutions and government agencies. – In: *Mathematical* and Software Engineering, Vol. 4, No. 1, 2018. ISSN 2367-7449. [online]. *http://varepsilon.com/.*

9. **Hristov,** Hr. Development of warfare and counter-terrorism. – In: *Science* Education Innovation, Vol. 3, 2014. ISSN 1314-9784.

10. **Hristov,** Hr. A modern survey on problems of business organization's security. – In: *Scientific* and Applied Research, Konstantin Preslavsky University Press, Vol. 7, 2015. ISSN 1314-6289. [online]. *http://www.rst-tto.com/publication.html.*

11. **Kahya-Özyirmidokuz,** E., A. Gezer, C. Ciflikli. Characterization of Network Traffic Data: A Data Preprocessing and Data Mining Application. – In: *Data* Analytics. The First International Conference on Data Analytics, September, 2012. ISBN 978-1-61208-242-4.

12. **Kaur,** R., G. Singh, Analysing, Port Scanning Tools and Security Techniques. – In: *International* Journal of Electrical Electronics & Computer Science Engineering, Vol. 1, Issue 5, October 2014. ISSN 2348 2273.

13. **Meyers,** C., S. Powers, D. Faissol. Probabilistic Characterization of Adversary Behavior in Cyber Security. No. LLNL-TR-419023. – In: *Lawrence* Livermore National Laboratory (LLNL), Livermore, CA, 2009.

14. **Meyers,** C., S. Powers, D. Faissol. Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches. – In: *Lawrence* Livermore National Laboratory, Livermore, CA, April 2009, Vol. 7.

15. **Nachev,** A., S. Zhelezov. Assessing the efficiency of information protection systems in the computer systems and networks. – In: *Information* Technology and Security, No. 1(3), 2013.

16. **Oram,** A., J. Viega. Beautiful Security. – In: *O'Reilly* Media, 2009. ISBN 978-0-596-52748-8.

17. **Shimeall,** T. J., J. M. Spring. Introduction to Information Security: A Strategic-Based Approach. Syngress, 2014. ISBN: 978-1-59749-969-9.

18. **Simmons,** C., S. Shiva, D. Dasgupta, Q. Wu. AVOIDIT: A cyber attack taxonomy. University of Memphis. – In: *Proceedings* of the 9th Annual Symposium on Information Assurance (ASIA '14), Albany, NY, USA, June 3 – 4, 2014.