2. Kostecka S, Solomia F., Yuriy S. Implementation of electronic document processing at enterprises. INFORMATION, COMMUNICATION, SOCIETY (ICS-2019) 16-18 MAY 2019, CHYNADIYOVO, UKRAINE
3. Nedoshytko I., Patriak O., Electronic Document Management and Its Value for Business. DOI: 10.31866/2617-796X.5.2.2022.270142
4. THE LAW OF UKRAINE. About electronic documents and electronic document flow. Available at https://zakon.rada.gov.ua/laws/show/851-15#Text
5. THE LAW OF UKRAINE. About electronic trust services. Available at https://zakon.rada.gov.ua/laws/show/2155-19
6. Zhovnirchyk, Martseniuk.ELECTRONIC GOVERNANCE AND ELECTRONIC WORKFLOW IN THE PROCESS OF ADOPTION MANAGEMENT DECISIONS . DOI:10.34132/pard2019.06.05
7. The Ministry of Digital took part in the presentation of the Digital Transformation Index 2021. https://thedigital.gov.ua/news/mintsifra-vzyala-uchast-u-prezentatsii-indeksu-tsifrovoi-transformatsii-2021
8. diia.Signature meets EU requirements.. Available at https://diia.gov.ua/news/revolyucijne-onovlennya-diyapidpis-vidpovidaye-vimogam-yes-doluchajtesya-do-beta-testu
9. Sharapova, Onoprienko, Chirva, Naranovych. CHARACTERISTICS OF THE IMPLEMENTATION OF ELECTRONIC DOCUMENT TREATMENT IN ITALY UNDER THE INFLUENCE OF EU LEGISLATION. DOI: https://doi.org/10.36074/grail-of-science.17.06.2022.015
10. Arkhypova Ye.O., Dmytrenko N.O. EXPERIENCE OF INTRODUCTION OF E-GOVERNANCE IN ESTONIAAND ITS IMPLEMENTATION IN UKRAINE. «Young Scientist» • No 11 (26) • Part 3 • november, 2015
11. Liudmyla Stryzheus, Alla Tendiuk. MANAGEMENT OF ADAPTATION OF THE ORGANIZATION'S PERSONNEL IN THE PERSONNEL MANAGEMENT SYSTEM . DOI: 10.36910/6775-2308-8559-2022-4-14
12. CURRENT LABOR MARKET DEVELOPMENT TRENDS IN THE CONDITIONS OF DIGITALIZATION OF THE ECONOMY DOI: 10.32782/2415-3583/26.11

CLASSIFICATION OF DDOS ATTACKS AND THEIR IMPLEMENTATION

Averbakh D.M., student,

Suknov M.P., PhD, Associate Professor,

Kharkiv National University of Radio Electronics

Keywords: DDoS attack, SYN flood, UDP flood.

DDoS attacks ("distributed denial-of-service") - is an attempt to disrupt normal server traffic. They aim to overwhelm the devices, services, or network the intended target with fake Internet traffic, making them unavailable to users.

A DDoS attack is like an unexpected traffic jam on the highway, preventing normal traffic from to its destination.

With the help of networks of computers connected to the Internet, DDoS attacks are carried out.

These networks, consisting of different network devices, are infected with malware, allowing an attacker to control them remotely. These different devices are called bots, and a group of such bots is called a botnet.

Even after a botnet is formed, an attacker is able to direct an attack by sending remote instructions to each bot.

The moment a network or server is made the target of a botnet, each bot sends requests to the victim's IP address. This can congest the server or network, causing a denial of Service to normal traffic.

Separating attack traffic from legitimate traffic can be quite difficult, since any bot is considered a legitimate Internet device.

So how do you identify a DDoS attack? There are several points that will help distinguish such an attack.

- Questionable amounts of traffic sent from a single IP address or spectrum of IP addresses;

- Traffic flow from users with the same type of device, geolocation, or version of web browser;

- Unexplained bursts of requests to the same page;

- Unnatural traffic modifications (e.g., bursts every 5 minutes).

Attacks can be divided into several categories:

- Volume attacks. When a huge amount of traffic is sent to overload network bandwidth.
- Protocol attacks. These are the ones that are more focused and exploit vulnerabilities in server resources.
- Application attacks. These attacks are the most sophisticated form of DDoS attacks, targeting specific web applications.
- SYN flooding.

- UDP flooding.

What is a SYN flood attack? SYN flooding (semi-open attack) is a type of DDoS attack. By using absolutely all available server resources, SYN flood attack tries make the server unavailable for legitimate traffic.

SYN flood attacks work using the TCP connection handshake procedure. Under standard conditions, a TCP connection applies three different processes to establish a connection.

1. First, the client sends a SYN packet to the server to initiate the connection.

2. The server then replies to this initial packet with a SYN/ACK packet to verify the connection.

Finally, the client returns the ACK packet with the intention of acknowledging the receipt of the packet from the server. Already at the end of this sequence of sending and receiving packets, the TCP connection opens and can send and receive data.

UDP flooding is a type of DDoS attack in which large numbers of UDP requests are sent to a target server in order to suppress that device's ability to process and respond.

The firewall that protects the target server can, in turn, fail due to UDP flooding, resulting in denial of service for legitimate traffic.

UDP flooding works mainly by exploiting the steps a server takes when it responds to a UDP packet sent to one of its ports. Under normal circumstances, when a server receives a UDP packet on a particular port, it takes two steps in response:

1. First, the server checks to see if any programs that are currently listening for requests on the specified port.

2. If no programs are receiving packets on that port, the server responds with a packet ICMP(ping) packet to inform the sender that the destination is unreachable.

When the server receives each new UDP packet, it goes through the request processing steps, using server resources in the process. When transmitting UDP packets, each packet will include the IP address of the source device. During this type of DDoS attack, the attacker typically does not use his own real IP address, but instead spoofs the source IP address of the UDP packets, preventing disclosure of the

attacker's true location and potential saturation response packets from the target.

As a result of the target server using resources to verify and then respond to each UDP packet received, the target's resources can be quickly depleted when receiving a large UDP packet stream, resulting in denial of service for normal traffic.

References

1. DDoS-атаки. Причины возникновения, классификация и защита от DDoS-атак. [Электронный ресурс]. Режим доступа: http://efsol.ru/articles/ddos-attacks.html/ (дата обращения: 13.05.2023).

MOST IMPORTANT KNOWLEDGE FOR AN IT SPECIALIST

Suvorov D.S., student,

Gerasymchuk T.V., Associate Professor,

Kharkiv National University of Radio Electronics

This article will give you some essential information about IT industry nowadays and an overview of important skills for this area with additional advice.

Whether you are just starting out in the field or looking to take your career to the next level, the information below can help you stand out and succeed in a rapidly changing industry.

To start with, it must be said that the IT industry is one of the most rapidly growing fields. Employment in computer and information technology occupations is projected to grow 11% to 2029, much faster than the average for all occupations.

Naturally, there are a lot of key pieces of information that should be known by well-qualified IT specialists to remain competitive.

But what are those most important areas of knowledge for IT guys to focus on?

This article will provide you with three main areas that can make all the difference in an IT specialist’s career: technical skills, soft skills and business acumen. So, let is get started.

Technical skills are needed for any IT specialist, regardless of their particular specialization. Each IT field has its own unique features, and it is important to understand the specific technical skills required for your area of expertise. But you